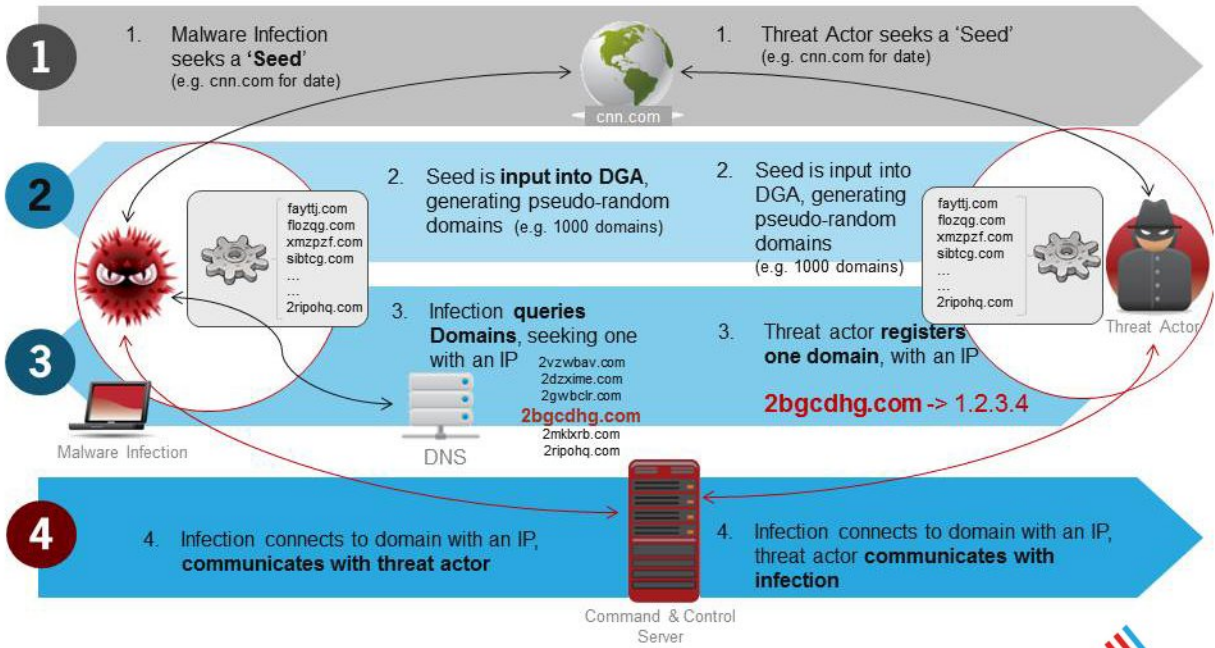


Hesperbot DGA Analizi

written by Mert SARICA | 1 October 2014

Alan adı üretme algoritması (DGA), zararlı yazılımlar tarafından yeni bir alan adı üretmek amacıyla kullanılan algoritmalar. Zararlı yazılım geliştiricileri, bu algoritma sayesinde geliştirmiş oldukları zararlı yazılımın haberleştiği komuta kontrol merkezinin şikayet üzerine ve/veya güvenlik firmaları tarafından yapılan müdahale üzerine (sinkhole) kapatılması durumunda tekrar zararlı yazılımı kontrol edebilmektedirler.

How Domain Generation Algorithms (DGA) Work



packets_20130913_020904.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 127.0.0.2 and ip.addr eq 127.0.0.1) and (udp.port eq 2308 and ...) Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
31	145.489203	127.0.0.2	127.0.0.1	DNS	58	Standard query 0x02c9 A www.bing.com
723	218.013488	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x0cfe A kvbqkztz1hryolzmomqwcqheoov.net
583	202.891744	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x13e4 A swijdm1jofmrskoeohzgjnnr.ru
351	178.726997	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x17db A abmciduijg1fuhqoknktw.info
1227	272.201407	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x1a9e A upnkf1bmkzmbpzhrstxdipjei.biz
555	199.867395	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x1be9 A eahrkeuemlmzhainkjmbljyhon.net
751	221.037837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x1bf8 A qijdeapkzhexyqctcuyxnjgeso.ru
485	192.306523	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x1eed A vkgyfvsjhjbxohatgldamkjdwpr.com
513	195.330872	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x21ee A usfugqfbbmrmkfmcywkaivlrzpr.com
1423	293.231647	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x2293 A aqwgqkuki zoznzaufmyxprkmb.ru
1255	275.205727	127.0.0.2	127.0.0.1	DNS	70	Standard query 0x249f A xozammrhacmt1hiznfxkh.ru
863	233.115203	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x26f0 A hyvxgusqscacqhycwkrhmnrp.info
625	207.428267	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x28e0 A ojyhpndraqbaqcpapfzdtucgu.org
891	236.129538	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2af2 A ugrcusd1bdqquuhehtwldrwb1.net
695	214.989139	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2efd A ivhpnjzlhutfedscxwvvgag.info
737	219.525663	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x2fff A obzpjbrojfhxvskfvmvjnsonvv.biz
267	169.663965	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x32de A ggeuibzfwsvwjzjinydlhy1xg.net
457	189.282175	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x35d3 A hbeiffydekzjbpwpcpeapfzdtucgu.org
1073	255.677647	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3787 A hygqppjusibxvhyghvghxcunjjb.com
989	246.664687	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x3789 A vciithyrkdbmdblclvgexc.com
1171	266.192767	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3a9c A aqdeufircjvfejbtzuovkdeazh.ru
231	166.649631	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3adc A xgficegmkvwoxkptmjcyrckwgt.ru
1311	281.214367	127.0.0.2	127.0.0.1	DNS	80	Standard query 0x3c9b A hahizprusxwfqqczlydswmiphcu.info
1395	290.227327	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3e92 A ffilso1nzhthfxzxrkdicujbl.net
597	204.403919	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x3ee6 A ypcifaxweaskcihoxhkmjntbhy.biz
653	210.452616	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x42e3 A vgcqr1xgmvetcpvlvbyzhztptjx.com
877	234.617363	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x42f1 A twnjtsqsgsxkixkzpcyptlf.biz
1339	284.218687	127.0.0.2	127.0.0.1	DNS	66	Standard query 0x4c96 A fdxhkjbireylzhnr.ru
253	168.161805	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x4ddd A futjni2torctclhhi2ydfixgby.com
611	205.916093	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x4fe7 A xkonfizpgpailjeyatamjfykbt.net
541	198.355221	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x51e8 A jrmrzxgkreyomovxozeurwaer.cp.org
471	190.794349	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x51ed A xgbukvukzdcmoncigybuizpeujr.info
1451	296.245981	127.0.0.2	127.0.0.1	DNS	71	Standard query 0x52ad A tdlppzpeulfxdmhlvpjpf.net
527	196.843047	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x53ef A qoqcaekrlzxqoytuoopbdixyvojf.biz
1437	294.733807	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x54ac A hggubuijmbvczh1lhtgvcpbukv.biz
1213	270.699247	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x569e A ofypozxxppnduovdofaedydqdyuw.org
779	224.062186	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x57fb A xojbqczlzwcepnwhaeiibip.net
147	157.576584	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x59c7 A hqgkvxhukwscaxaxoldutshy1by.ru
69	150.025727	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x59ca A xkbagejntccqami jvoxrwnknyld.com
421	186.267840	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x61d0 A vdiuceqwmzhpozsvsorqcinrg.com
1143	263.188447	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x6283 A hmeiaqprmojskhhxhikfmydy.info
295	172.688314	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x64d9 A gusofadlfpnlrvxcxwrfmqadnr.info
1185	267.694927	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x669d A tzxoqsrqtpyxdagauoppfvif.com
835	230.090855	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x66f7 A amontwfgidinvsoxotdmsggagy.ru
1199	269.197087	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x689e A inqomfnvjbytgztovcidjvlcvg.info
1269	276.707887	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x6b98 A hulgtqazgrmzldqbovlffj.com
919	239.143872	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x738d A fcqjfmfampvzpzaurbzmydijai.ru
681	213.476965	127.0.0.2	127.0.0.1	DNS	71	Standard query 0x73fd A tohejnrduoofeurbggepp.com
337	177.224837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x76db A dergdatxctgqwuwlzqxjtsqpv.com
1297	279.712207	127.0.0.2	127.0.0.1	DNS	73	Standard query 0x779a A jcapcivrgeqlzqsirwceid.biz
203	163.625282	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x7ac3 A ibhulbthubjbmnrzddiqajitgucp.net
365	180.239171	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x80db A pfdecapbplvuhcmheofgutgjn.org
667	211.964791	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x80fc A hhmigeqyvkqsgfqsclkbj.ru
1283	278.210047	127.0.0.2	127.0.0.1	DNS	79	Standard query 0x8498 A vgcxvzhbqhapijypnbllvctwqouc.net
1381	288.725167	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x8f91 A emsoxqcekzchmduy1xiffud.org
1353	285.720847	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x9497 A uknjdidatdaeytm1gadupvg.com

File: "C:\Users\RBashir\Downloads\mal\mal..." Packets: 1464 · Displayed: 204 (13.9%) · Load time: 0:00.044

Örneğin 2008 yılında MS08-67 zafiyetini istismar ederek dünyayı kasıp kavuran Conficker.A solucanı, barındırdığı DGA sayesinde günde 250 tane yeni alan adı üretiyordu. Aynı solucanın 2009 yılındaki güncellenmiş olan C varyantı ise günde 500 ile 50.000 alan adı üretecek bir DGA'ya sahipti. Conficker zararlı yazılımı ile mücadele esnasında, zararlı yazılımın oluşturduğu trafiği izlemek ve zararlı yazılım bulaşmış olan sistemleri tespit etmek amacıyla conficker çalışma grubu tarafından günde 500 adet alan adı kayıt ediliyor ve analiz sistemlerine (sinkhole) yönlendiriliyordu.

Günümüz zararlı yazılımlarında ise DGA, çoğunlukla ana haberleşme yönteminden ziyade yedek yöntem olarak kullanılmaktadır. Örneğin GameOver Zeus zararlı yazılımı DGA'yı, kullandığı ilk iki yöntem çalışmadığı takdirde üçüncü yöntem olarak kullanılmaktadır. DGA'nın birincil yöntem olarak kullanılmamasının temel sebebi, zararlı yazılım analistleri, siber güvenlik uzmanları tarafından kod analizi ile zararlı yazılımda tespit edilen DGA'nın yani alan adlarının,

yazılım geliştiriciden önce kayıt edilebilmesine imkan tanınmasıdır. Bu sayede uzmanlar, Conficker örneğinde olduğu gibi zararlı yazılımlar ile ilgili çeşitli bilgileri toplayabilmekte, kimi zaman ise zararlı yazılımları kontrol altına alabilmektedirler.

Gündemi, analiz yazılarını takip edenler, ileri seviye Hesperbot bankacılık zararlı yazılımının, 1.5 yıldır ülkemizin ve vatandaşlarımızın üzerinde kara bulut gibi dolaştığını biliyordur. Geçtiğimiz ayın başında Tübitak, Hesperbot ile ilgili yeni bir yazı yayınlayarak bu zararlı yazılımın ülkemizde hala aktif olduğunu ve vatandaşımız için ciddi bir tehdit olduğunu açıkladı.

Bu vesileyle Tübitak Bilgem Siber Güvenlik Enstitüsü'ne, Hesperbot ile mücadele adına verdiği emeklerinden dolayı teşekkür etmek isterim.

5 Eylül tarihinde INTEL RAD ekibi, Hesperbot'un hedef aldığı bankalara ait kural dosyasını ve ilave modüllerini indirmek için kullandığı alan adına (followtweetertag.com) siber operasyon düzenledi. Bu operasyon sonrasında Hesperbot zararlı yazılımı bulaşmış tüm sistemler, ilgili alan adına sahip web sitesine erişemedikleri için (http durum kodu 502) Hesperbot'un DGA'sı tarafından üretilen alan adları ile bağlantı kurmaya başladı.

Hesperbot, kural dosyası olmadan kullanıcının internet tarayıcısı ile internet bankacılığı sunucusunun arasındaki trafiğe müdahale edememektedir.

THIS DOMAIN IS SEIZED BY MUTUAL COOPERATION BETWEEN

DUE TO ILLEGAL FRAUDULENT ACTIVITY.

[EN] This domain name as well as its respective owners are found to be involved in a large-scale financial fraud campaign targeting on financial institutions and their clients. To prevent from any further loss or damage that may be faced, PRODAFT CYBER INTELLIGENCE LLC. has hereby seized this domain according to the ethics of good business practice. In line with our cyber investigation, we would like to inform you that all responsible governmental authorities are notified about IP address and relevant credentials of responsible cyber-criminals.

[TR] Bu alan adı ve işişi bulunan yetkililerin, bankacılık kurumlarını ve müşterilerini hedef alan geniş kapsamlı bir siber dolandırıcılık operasyonu ile bağlantılı oldukları tespit edilmiştir. Etik değerlerimiz gereğince, hedef alınan taraflarca uğranılabilecek zararın daha da büyümesi adına PRODAFT Siber İstihbarat Ltd. Şti. işbu alan adına el koymuş bulunmaktadır. Yürütmekte olduğumuz soruşturma çerçevesinde, tüm yetkili kurumlara, bu siber-dolandırıcılık operasyonunu yürüten şahıslara ait IP ve diğer bağlayıcı veriler iletilmiş bulunmaktadır.

[RU] Данный домен и его владелец связаны с обширной атакой на банковские учреждения и их клиентов. В соответствии с нашей этикой, в целях предотвращения роста подобной атаки в будущем, мы как фирма PRODAFT Cyber Intelligence LLC, вынуждены забронировать данное доменное имя. В рамках расследования, которое мы проводим, IP адреса и другие данные связанные с атакующими были переданы уполномоченным учреждениям.

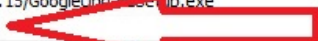
USTA
LULUBAL SİBER TEHDİT AŞI

GPACT

Contact info@prodaft.com for more info and compromised host list
Daha fazla bilgi ve etkilenen IP listesi için lütfen bizimle iletişime geçiniz: info@prodaft.com

Seized domains:
dksqlojlsmsizjrdllqjqt.ru
addytwteeter.com
followtweetertag.com
xdomainhelp.ru
xklovvyouahost.ru
twcbsitedesign.ru
zdomainstore.ru
airbwsbocqnhu.ru
xdomainssupport.ru
xwebsiteshosting.ru
xsolartechology.com
xsolarenergy.com

#	Result	Protocol	Host	URL
356	200	HTTP	Tunnel to	www.yahoo.com:443
357	200	HTTPS	www.yahoo.com	/
358	200	HTTP	tools.google.com	/service/update2?w=6:EFH2B5jVGzF8R2tTLHZGsVhFz0shG_-IACVF03N
359	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
360	502	HTTP	Tunnel to	followtweetertag.com:443
361	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
362	301	HTTP	yahoo.com	/
363	200	HTTP	Tunnel to	www.yahoo.com:443
364	200	HTTP	Tunnel to	www.yahoo.com:443
365	200	HTTPS	www.yahoo.com	/
366	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
367	502	HTTP	Tunnel to	followtweetertag.com:443
368	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
369	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
370	301	HTTP	microsoft.com	/
371	200	HTTP	www.microsoft.com	/
372	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
373	502	HTTP	Tunnel to	followtweetertag.com:443
374	302	HTTP	google.com	/
375	200	HTTP	www.google.com.tr	?gfe_rd=cr&ei=sq4JVMFHsao8wfiuGADA
376	502	HTTP	Tunnel to	followtweetertag.com:443
377	301	HTTP	yahoo.com	/
378	200	HTTP	Tunnel to	www.yahoo.com:443
379	200	HTTP	Tunnel to	www.yahoo.com:443
380	200	HTTPS	www.yahoo.com	/
381	502	HTTP	Tunnel to	followtweetertag.com:443
382	301	HTTP	yahoo.com	/
383	200	HTTP	Tunnel to	www.yahoo.com:443
384	200	HTTP	Tunnel to	www.yahoo.com:443
385	200	HTTPS	www.yahoo.com	/
386	502	HTTP	Tunnel to	followtweetertag.com:443
387	301	HTTP	wikipedia.org	/
388	200	HTTP	www.wikipedia.org	/
389	502	HTTP	Tunnel to	followtweetertag.com:443
390	301	HTTP	microsoft.com	/
391	200	HTTP	www.microsoft.com	/
392	502	HTTP	Tunnel to	followtweetertag.com:443
393	301	HTTP	yahoo.com	/
394	200	HTTP	Tunnel to	www.yahoo.com:443
395	200	HTTP	Tunnel to	www.yahoo.com:443
396	200	HTTPS	www.yahoo.com	/
397	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
398	200	HTTP	Tunnel to	iahapemwionkmti.ru:443
399	200	HTTPS	iahapemwionkmti.ru	/g



[Home](#) » [Reverse IP Lookup](#) » 94.126.178.17

94.126.178.17 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains

[Lookup tips](#) ⓘ**LOOKUP**

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — 56 domains hosted on IP address 94.126.178.17

Domain	View Whois Record	Screenshots
1. 11617em1rcuykcs49lo1x9whsv.biz		
2. 16m4ethimpjre119w61x1g5bgjy.biz		
3. 190hi6ljstut1qu0ezxzxqxl9.biz		

AND 53 other domains...

Bildiğiniz gibi hem işim gereği hem de ilgi alanıma girmesinden dolayı Hesperbot üzerinde zaman zaman çalışma fırsatı yakalıyor ve ilginç bulduğum noktaları sizlerle paylaşıyorum. Hesperbot'un DGA'sı da uzun zamandan beri merakımı cezbediyordu fakat DGA ile ilgili fonksiyona hata ayıklayıcının donmasından dolayı çok defa deneyip ulaşamayınca, havlu attığım zamanlar oldu. İnadım inat, gel zaman, git zaman, günün birinde bunun analiz için kullandığım sistemden kaynaklı olabileceğini düşünerek bu defa üzerinde sadece üzerine hata ayıklayıcı yüklü olan tertemiz bir Windows XP ile analizi gerçekleştirmeye karar verdim ve herhangi bir sorun yaşamadığımı görünce Yeni Zelanda'nın HAKA dansını yapmaya başladım :)

DGA fonksiyonunu aramamdaki temel amaç en kısa sürede Hesperbot'un üreteceği alan adlarına ve hangilerininin Hesperbot geliştiricileri tarafından kayıt

edildiđi bilgisine en kısa srede ulařmaktı. Fonksiyona ulařamadıđım taktirde izleyeceđim yol, Hesperbot'un ncelikle ilgili komuta kontrol merkezi adresine bađlanmasını beklemek, ardından bađlanamamasını sađlamak ve reteceđi alan adlarını teker teker kayıt altına almak olacaktı. Hesperbot'un ilk adrese bađlanmaya alıřması (followtweetertag.com) ve bađlanamaması durumunda, yeni alan adını retmesi iin belli bir sre ve bađlantı isteđinin adet bazında gemesini beklemesinden tr bu yntem, saatler belki gnler srebilirdi.

DGA'nın fonksiyonunu bulup incelediđimde ve dallanıp budaklanan alt fonksiyonlarını grdđmde nmde izlemem gereken iki yol vardı. Birincisi ya tm fonksiyonların ve komutların zerinden teker teker geecektim ve DGA'ya gre alan adı reten bir kod yazacaktım veya DGA fonksiyonunu yamayarak (patching), limit ve adet kontrollerini devre dıřı bırakarak seri bir řekilde Hesperbot'un yeni alan adlarını retmesini sađlayacaktım. řayet zararlı yazılım analisti olsaydım ve attıđım tařın rkteceđi kurbađaya deyeceđine inansaydım kesinlikle birinci yolu seerdim dolayısıyla pratik ve kısa yolu semeye karar verdim.

The screenshot displays the Immunity Debugger interface for Explorer.EXE. The assembly view shows instructions such as `MOV ESI,ESI` at address `02415374`. A red arrow highlights this instruction. Below the assembly view, a memory dump is shown with columns for Address, Hex, dump, and ASCII. Two red arrows point to specific memory locations in the dump, likely indicating the location of the DGA function or its arguments.

Hesperbot paketlenmiş (packed) bir zararlı yazılım olduğu için DGA fonksiyonunu yamamak için ya paketini açıp, çalışabilir hale getirecek ve gerekli değişiklikleri (patching) disk üzerindeki yapacaktım ya da bellekte çalışır haldeyken yapacaktım. Yine fazla zahmete girmek yerine (sanırım tembelim) ikinci yolu, bellek üzerinde değişik yapmayı seçtim. Bellek manipülasyonu için eskiden pydbg aracını kullanıyordum fakat zaman içinde geliştirmesine ara verilmesi nedeniyle yeni araçlara doğru yelken açtım ve kısa bir araştırmadan sonra aradığım aracı buldum, WinAppDbg.

WinAppDbg, Windows işletim sistemi için geliştirilmiş ve Python ile yazılmış bir hata ayıklayıcısıdır.

WinAppDbg modülü ile DGA fonksiyonunda gerekli değişiklikleri yapan ufak bir araç hazırladıktan sonra Hesperbot'un çalıştığı bir sistemde aracı çalıştırdım ve Hesperbot'un kısa bir süre içinde yeni alan adlarını

üretmesini sağlayarak mutlu sona ulaştım. (Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için bazı kısımlar sansürlenmiştir.)

```
C:\WINDOWS\system32\cmd.exe
=====
Hesperbot DGA Patch [http://www.mertsarica.com]
=====
[*] Searching Hesperbot DGA... <1/2>

[*] Possible matches!
[+] Address: 00F60E2B Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 00F80443 Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 0248B2AB Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 0394048B Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Searching Hesperbot DGA... <2/2>

[*] Possible matches!
[+] Address: 00F6106D Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 00F80685 Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 039406CD Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>


C:\Documents and Settings\Administrator\Desktop>_
```


🔒 4260	502	HTTP
🔒 4261	200	HTTP
📄 4262	200	HTTP
📄 4263	200	HTTP
🔒 4264	200	HTTP
🔒 4265	502	HTTP
🔒 4266	200	HTTP
🔒 4267	200	HTTP
🔒 4268	502	HTTP
🔒 4269	502	HTTP
🔒 4270	502	HTTP
🔒 4271	502	HTTP
🔒 4272	502	HTTP
🔒 4273	502	HTTP
🔒 4274	502	HTTP
🔒 4275	502	HTTP
🔒 4276	502	HTTP
🔒 4277	502	HTTP
🔒 4278	502	HTTP
🔒 4279	502	HTTP
🔒 4280	502	HTTP
🔒 4281	502	HTTP
🔒 4282	502	HTTP
🔒 4283	502	HTTP
🔒 4284	502	HTTP
🔒 4285	502	HTTP
🔒 4286	502	HTTP
🔒 4287	502	HTTP
🔒 4288	502	HTTP
🔒 4289	502	HTTP
🔒 4290	502	HTTP
🔒 4291	502	HTTP
🔒 4292	502	HTTP
🔒 4293	502	HTTP
🔒 4294	502	HTTP
🔒 4295	502	HTTP
🔒 4296	502	HTTP
🔒 4297	502	HTTP
🔒 4298	502	HTTP
🔒 4299	502	HTTP
🔒 4300	502	HTTP
🔒 4301	502	HTTP
🔒 4302	502	HTTP

Tunnel to	followtweettag.com:443
Tunnel to	lahapemwionkmti.ru:443
www.download.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/authrootseq.txt
www.download.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Tunnel to	lahapemwionkmti.ru:443
Tunnel to	dksqlojglsmsizjrdllgiqt.ru:443
Tunnel to	mquyuledcyic.ru:443
Tunnel to	mquyuledcyic.ru:443
Tunnel to	obqpdmjn.ru:443
Tunnel to	jatpvjafbwpptyag.ru:443
Tunnel to	ueizvrpmwmdyejmhkycig.ru:443
Tunnel to	debyixoc.ru:443
Tunnel to	xbkyvofc.ru:443
Tunnel to	bbhghuku.ru:443
Tunnel to	psfrnlmdpkr.ru:443
Tunnel to	mvpwppgsujt.ru:443
Tunnel to	qhreuqyk.ru:443
Tunnel to	wjikevjm.ru:443
Tunnel to	agxqstwoc.ru:443
Tunnel to	trzxvhsbthwccgo.ru:443
Tunnel to	oibldgaj.ru:443
Tunnel to	hxxjpbah.ru:443
Tunnel to	hkpjfcip.ru:443
Tunnel to	gstbidaxyepi.ru:443
Tunnel to	rbmccpnyjismhg.ru:443
Tunnel to	qfqyqwzqqxmevjtwrmssg.ru:443
Tunnel to	ytdgmjmkhmaavjpyfimro.ru:443
Tunnel to	uxzusbcu.ru:443
Tunnel to	ejmlcqdjjizfzfn.ru:443
Tunnel to	difnjbmlezxkiwyjhqknja.ru:443
Tunnel to	qcnqcqiy.ru:443
Tunnel to	phplstknzpvzxaakybc.ru:443
Tunnel to	xcofeihllcuzyvbsduugpjl.ru:443
Tunnel to	luamnbo.ru:443
Tunnel to	jaxvaxwdfsdpzgsuprga.ru:443
Tunnel to	yjubrrfpkjadsevaqz.ru:443
Tunnel to	bgjmnsqg.ru:443
Tunnel to	epztnxcjaldvqa.ru:443
Tunnel to	rysiakzkrkwyxhxlqdnkd.ru:443
Tunnel to	kivhkgvsephj.ru:443
Tunnel to	yvncjmqkr.ru:443
Tunnel to	sykrqgfhkgtpipi.ru:443
Tunnel to	mdftmsx.ru:443

lahapemwionkmti.ru  

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link) ...

Biliş Tarihi	22.08.2015
Oluşturulma Tarihi	22.08.2014
NS Sunucu 1	ns1.reg.ru
NS Sunucu 2	ns2.reg.ru
IP Adresi	94.126.178.17
Durum Bilgisi	REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkəsi	 Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.nipn.net
IP / Sunucu Bilgileri	IP 94.126.178.17 Ülke  Danimarka Registry Whois Sunucu whois.nipe.net

[Registru Whois Kaydı](#) [IP Whois Kaydı](#)



Registry Whois Kaydı

By submitting a query to RIPE's Whois Service you agree to abide by the following terms of use:
<http://www.ripe.net/about/servpol.html#3.2> (in Russian)
<http://www.ripe.net/about/en/servpol.html#3.2> (in English).


```

domain: LAHAPEMWIONKMTI.RU
nserver: ns1.reg.ru
nserver: ns2.reg.ru
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created: 2014.08.22
paid-till: 2015.08.22
free-date: 2015.09.22

```

Dksqlojglsmsizjrdllgiqt.ru  

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link) ...

Biliş Tarihi	28.08.2015
Oluşturulma Tarihi	28.08.2014
NS Sunucu 1	ns1.reg.ru
NS Sunucu 2	ns2.reg.ru
IP Adresi	179.43.160.25
Durum Bilgisi	REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkəsi	 Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.nipn.net
IP / Sunucu Bilgileri	Registru Whois Kaydı IP Whois Kaydı

Registry Whois Kaydı



By submitting a query to RIPE's Whois Service you agree to abide by the following terms of use:
<http://www.ripe.net/about/servpol.html#3.2> (in Russian)
<http://www.ripe.net/about/en/servpol.html#3.2> (in English).

```



domain: DKSQLOJGLSMSIZJRDLLGIQT.RU
nserver: ns1.reg.ru
nserver: ns2.reg.ru
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created: 2014.08.28
paid-till: 2015.08.28
free-date: 2015.09.28
source: TC1

```

Last updated on 2014.09.08 12:31:32 MSK

Mquyuledcyic.ru  

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link) ...

Biliş Tarihi	01.09.2015
Oluşturulma Tarihi	01.09.2014
NS Sunucu 1	ns1.reg.ru
NS Sunucu 2	ns2.reg.ru
IP Adresi	193.124.18.187
Durum Bilgisi	REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkəsi	 Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.nipn.net
IP / Sunucu Bilgileri	IP 193.124.18.187 Ülke  Rusya Federasyonu Registry Whois Sunucu whois.nipe.net

[Registru Whois Kaydı](#) [IP Whois Kaydı](#)

Registry Whois Kaydı

By submitting a query to RIPE's Whois Service you agree to abide by the following terms of use:
<http://www.ripe.net/about/servpol.html#3.2> (in Russian)
<http://www.ripe.net/about/en/servpol.html#3.2> (in English).

```

domain: MQUYULEDCYIC.RU
nserver: ns1.reg.ru
nserver: ns2.reg.ru
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created: 2014.09.01
paid-till: 2015.09.01
free-date: 2015.10.02

```

Obqpdmjn.ru  

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

.ru Uzantı Ülkesi	 Rusya Federasyonu
Registry Whois Sunucu	whois.ripn.net
Registrv Whois Kaydı	

Registry Whois Kaydı

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

No entries found for the selected source(s).

Last updated on 2014.09.08 16:01:34 MSK
```

Jatpvjafbwpptyag.ru  

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

.ru Uzantı Ülkesi	 Rusya Federasyonu
Registry Whois Sunucu	whois.ripn.net
Registry Whois Kaydı	

Registry Whois Kaydı

```
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

No entries found for the selected source(s).

Last updated on 2014.09.08 15:56:33 MSK
```

Kurban Bayramı'nızı en içten dileklerle kutlar, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.