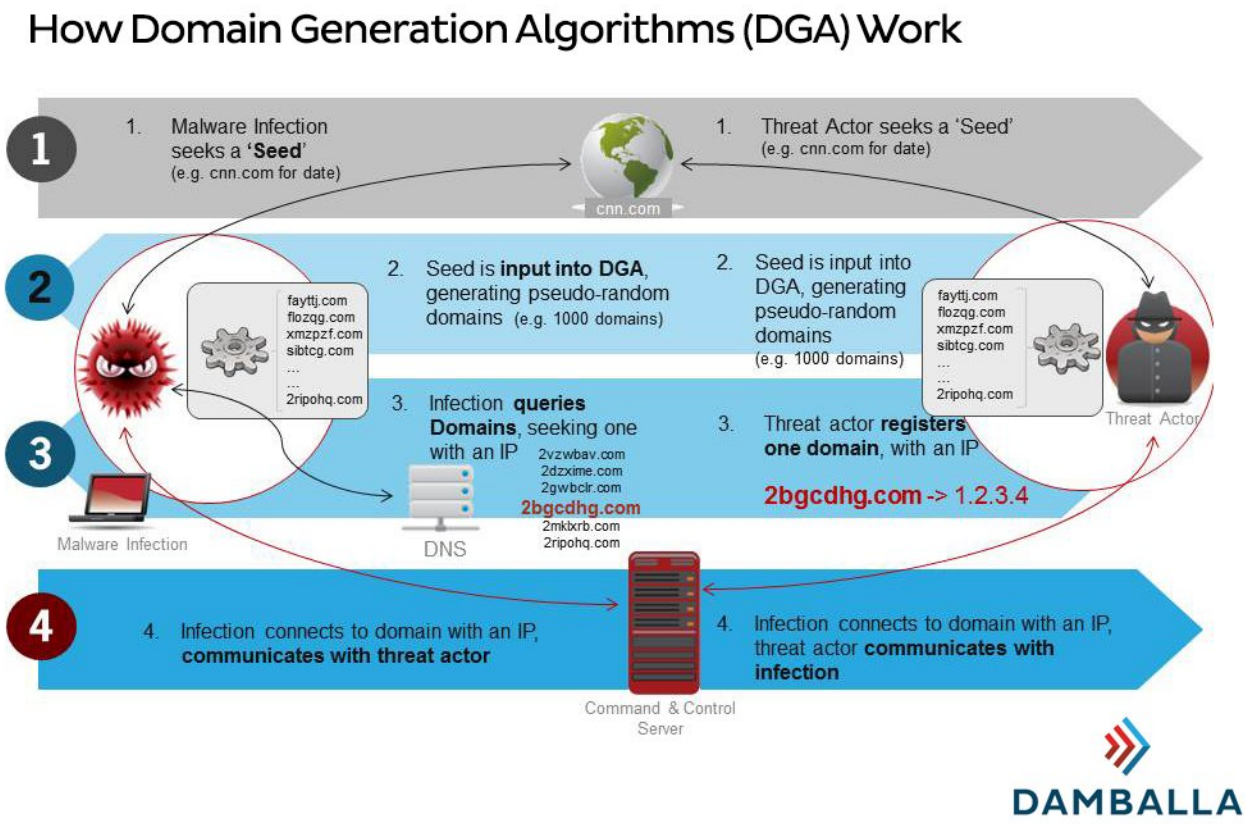
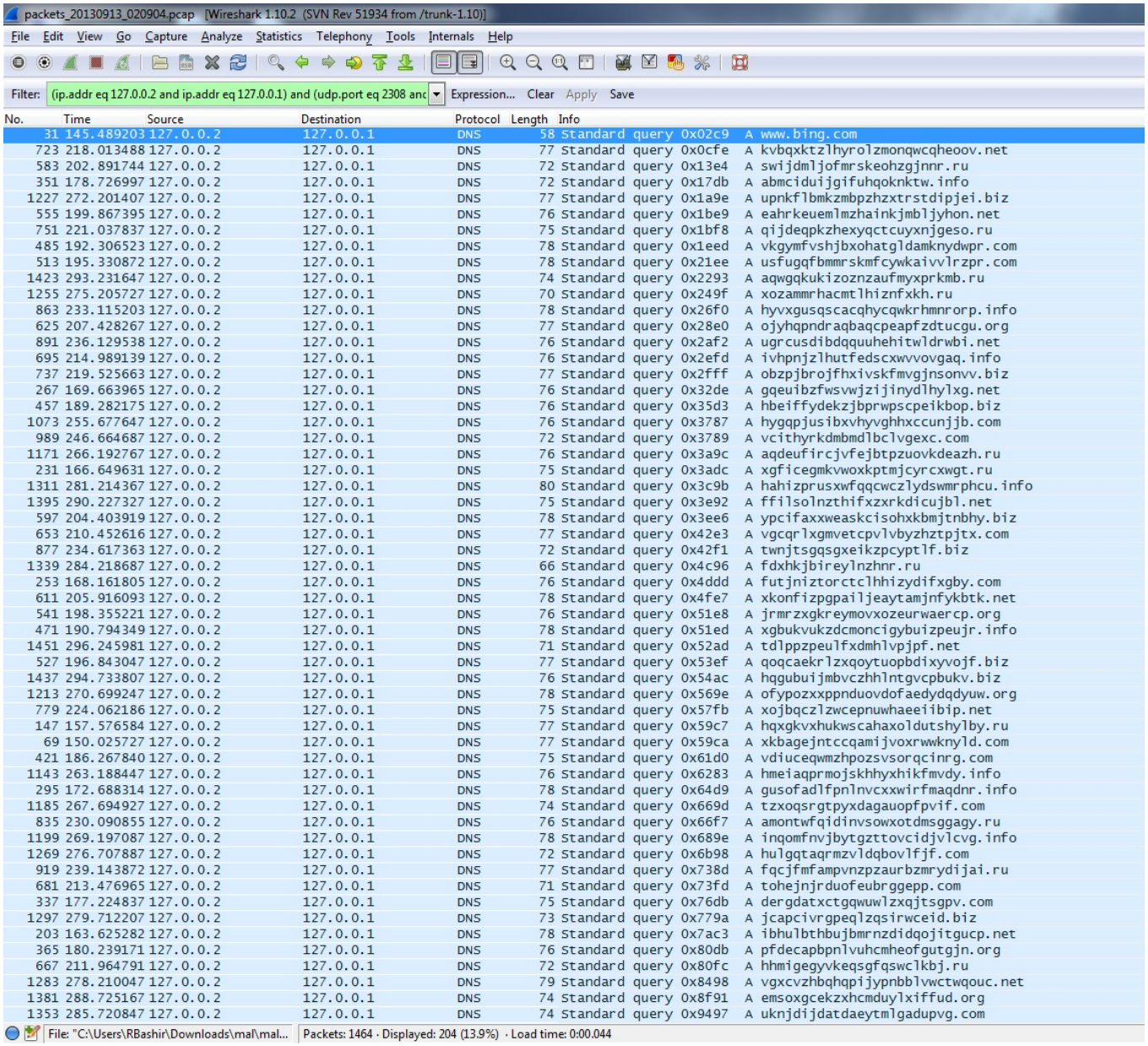
Hesperbot DGA Analizi

written by Mert SARICA | 1 October 2014

Alan adı üretme algoritması (DGA), zararlı yazılımlar tarafından yeni bir alan adı üretmek amacıyla kullanılan algoritmalardır. 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.





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 taktirde üçüncü yöntem olarak kullanmaktadır. 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,

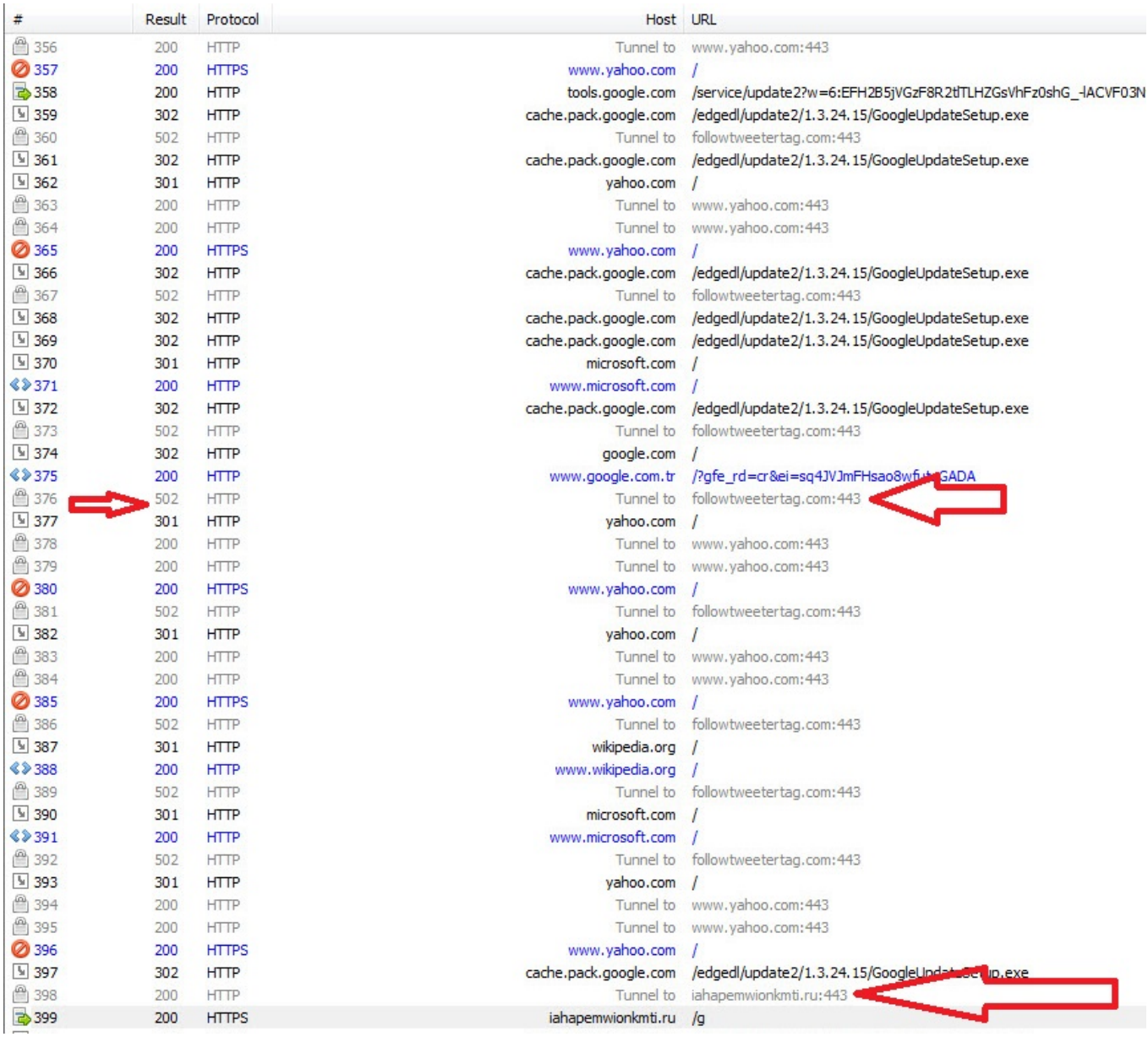
yazılım geliştiricinden önce kayıt edilebilmesine imkan tanımasıdır. Bu sayede uzmanlar, Conficker örneğinde olduğu gibi zararlı yazılımlar ile ilgili çeşitli bilgileri toplayabilmekte, kimi zaman ise zararlı yazılımları kontrol altına alabilmektedirler.

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.

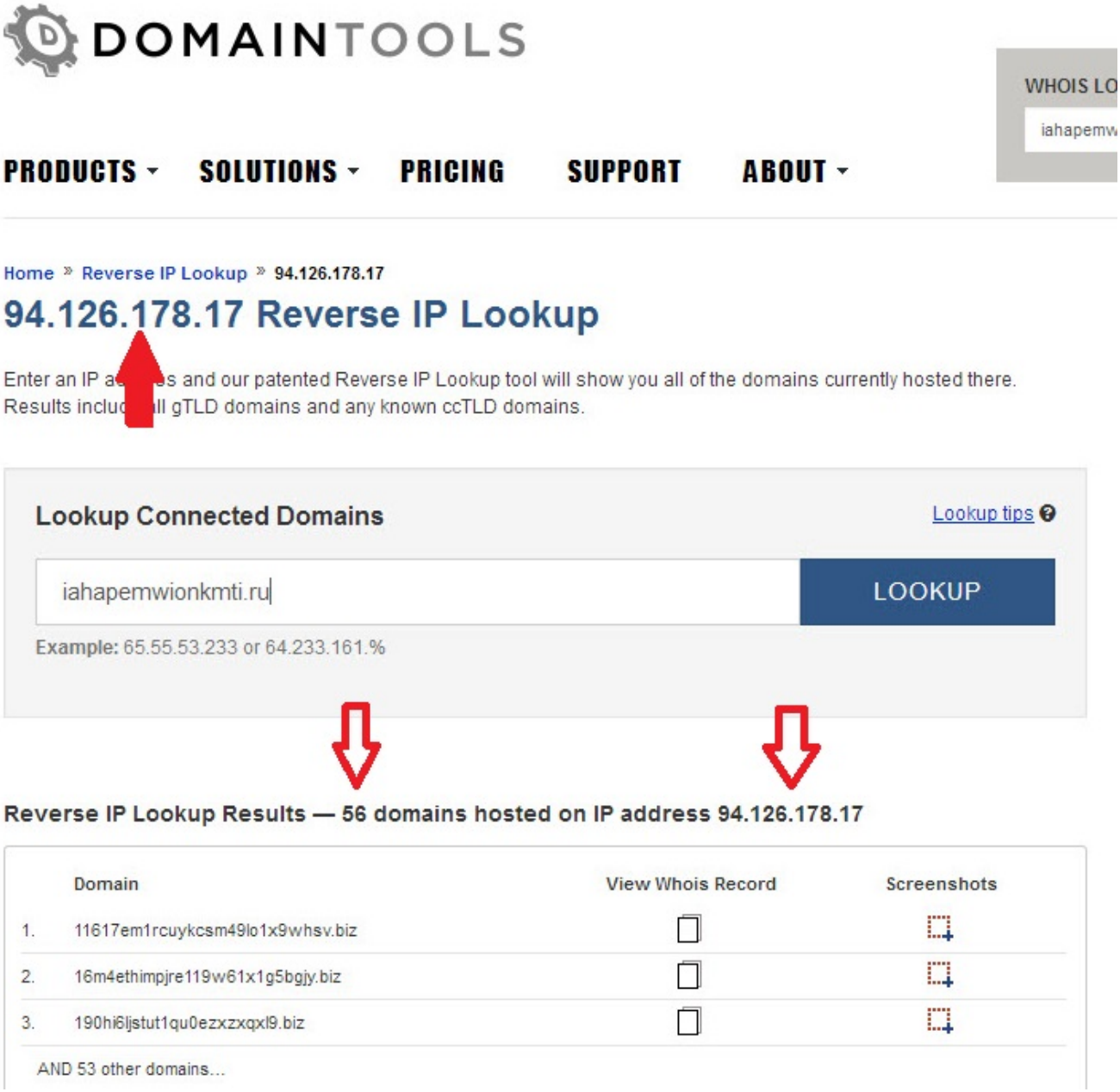
Bu vesileyle Tübitak Bilgem Siber Güvenlik Enstitüsü'ne, Hesperbot ile mücadele adına verdiği emeklerinden dolayı teşekkür etmek isterim.

5 Eylül tarihinde INTELRAD 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.



#	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:EFH2B5jVGzF8R2tlTLHZGsVhFz0shG_-lACVF03N
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=sq4JVJmFHsao8wfu
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

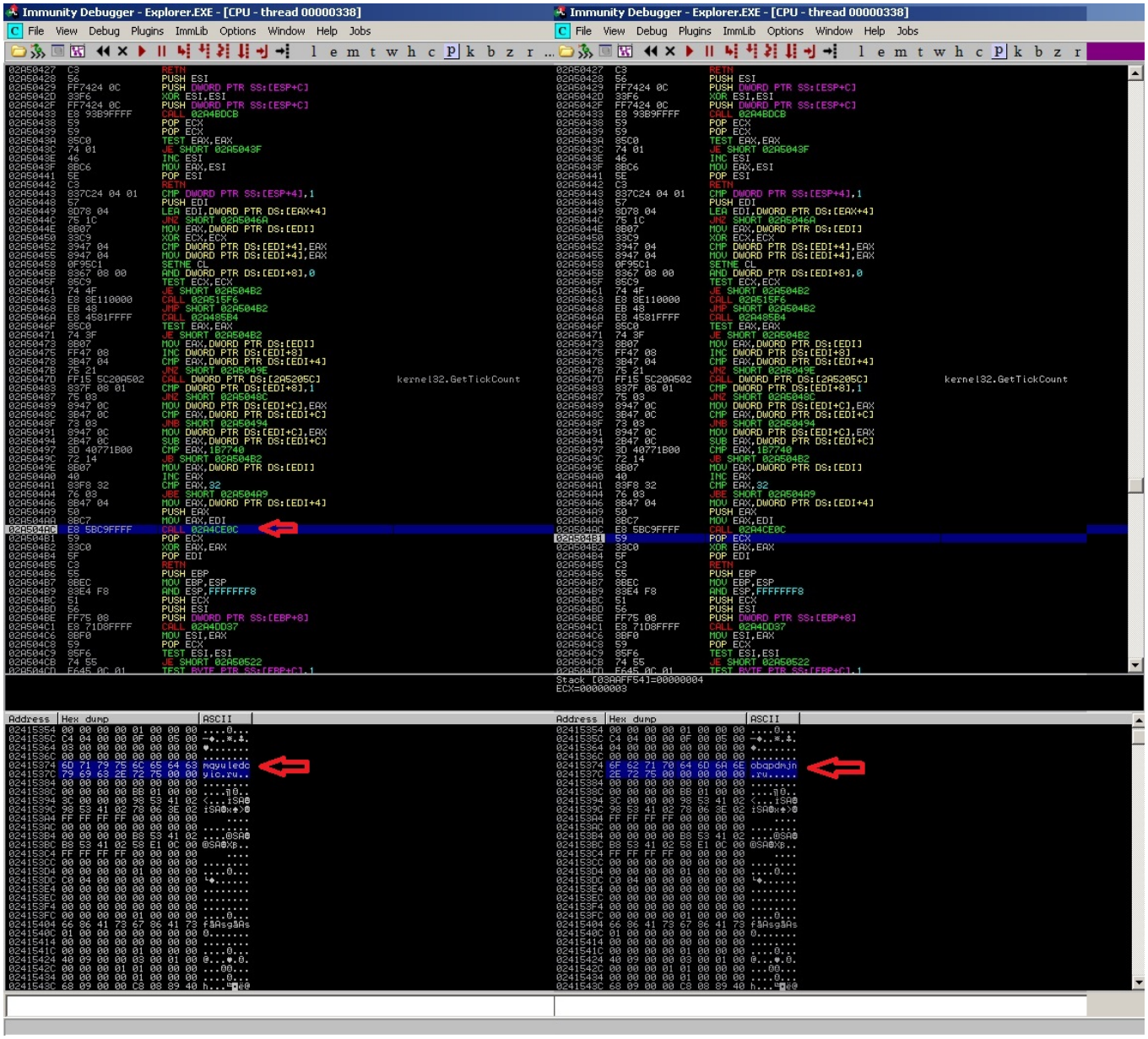


Bildiğiniz gibi hem işim gereği hem de ilgi alanıma girmesinden dolayı Hesperbot üzerinde zaman zaman çalışma fırsatı yakalıyor ve ilginç bulduğum noktaları sizlerle paylaşıyorum. Hesperbot'un DGA'sı da uzun zamandan beri merakımı cezbediyordu fakat DGA ile ilgili fonksiyona hata ayıklayıcının donmasından 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 üzerince 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 hangilerinin Hesperbot geliştiricileri tarafından kayıt

edildiği bilgisine en kısa sürede ulaşmaktı. Fonksiyona ulaşamadığım taktirde izleyeceğim yol, Hesperbot'un öncelikle ilgili komuta kontrol merkezi adresine bağlanmasını beklemek, ardından bağlanamamasını sağlamak ve üreteceği alan adlarını teker teker kayıt altına almak olacaktı. Hesperbot'un ilk adrese bağlanmaya çalışması (followtweetertag.com) ve bağlanamaması durumunda, yeni alan adını üretmesi için belli bir süre ve bağlantı isteğinin adet bazında geçmesini beklemesinden ötürü bu yöntem, saatler belki günler sürebilirdi.

DGA'nın fonksiyonunu bulup incelediğimde ve dallanıp budaklanan alt fonksiyonlarını gördüğümde önümde izlemem gereken iki yol vardı. Birincisi ya tüm fonksiyonların ve komutların üzerinden teker teker geçecektim ve DGA'ya göre alan adı üreten bir kod yazacaktım veya DGA fonksiyonunu yamayarak (patching), limit ve adet kontrollerini devre dışı bırakarak seri bir şekilde Hesperbot'un yeni alan adlarını üretmesini sağlayacaktım. Şayet zararlı yazılım analisti olsaydım ve attığım taşın ürküteceği kurbağaya deyeceğine inansaydım kesinlikle birinci yolu seçerdim dolayısıyla pratik ve kısa yolu seçmeye karar verdim.

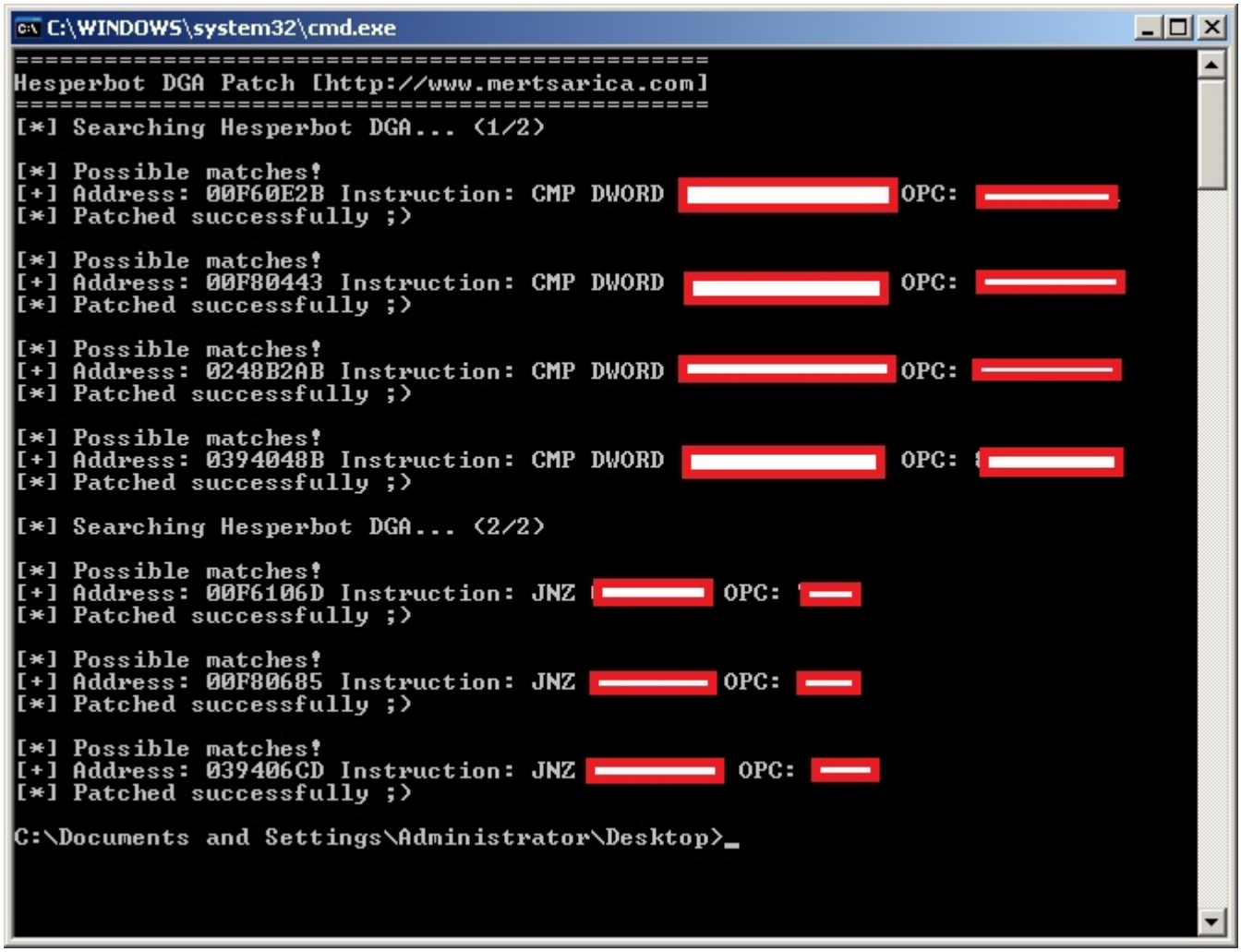


Hesperbot paketlenmiş (packed) bir zararlı yazılım olduğu için DGA fonksiyonunu yamamak için ya paketini açıp, çalışabilir hale getirecek ve gerekli değişiklikleri (patching) disk üzerindeyken yapacaktım ya da bellekte çalışır haldeyken yapacaktım. Yine fazla zahmete girmek yerine (sanırım tembelim)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

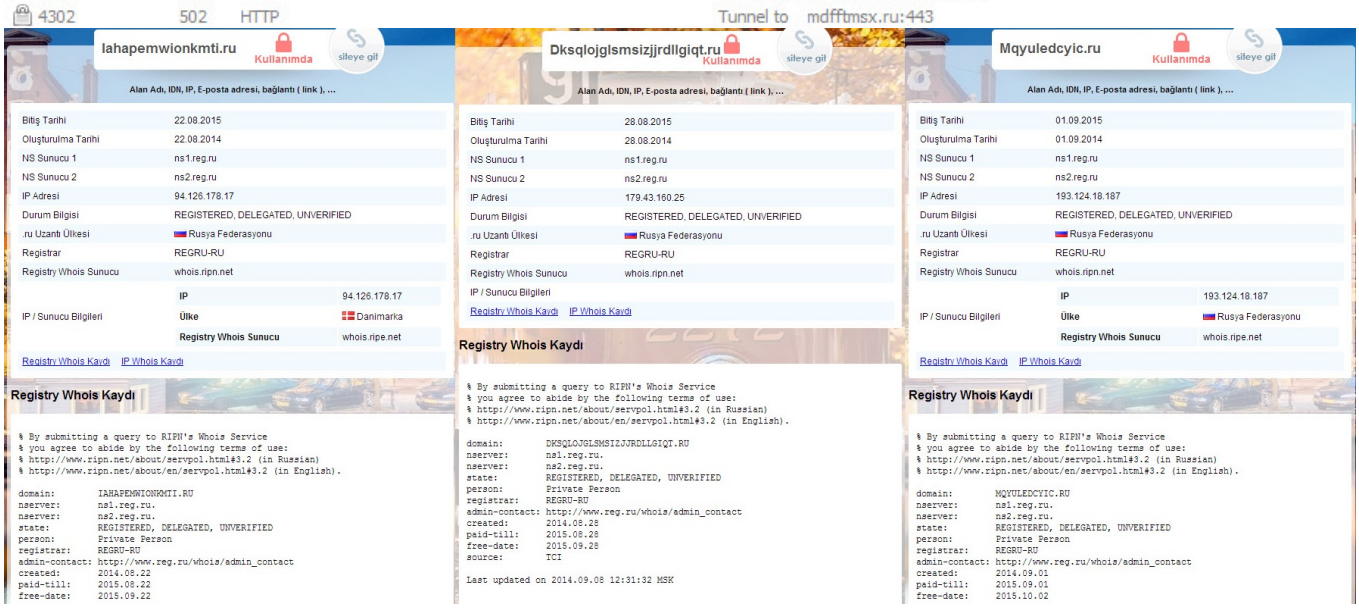
WinAppDbg, Windows işletim sistemi için geliştirilmiş ve Python ile yazılmış bir hata ayıklayıcısıdır.

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.)



4260	502	HTTP		Tunnel to	followtweetertag.com:443
4261	200	HTTP		Tunnel to	iahapemwionkmti.ru:443
4262	200	HTTP	www.download.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/authrootseq.txt	
4263	200	HTTP	www.download.windowsupdate.com	/msdownload/update/v3/static/trustedr/en/authrootstl.cab	
4264	200	HTTP		Tunnel to	iahapemwionkmti.ru:443
4265	502	HTTP		Tunnel to	dksqlojglsmsizjjrdllgiqt.ru:443
4266	200	HTTP		Tunnel to	mqyuledcyic.ru:443
4267	200	HTTP		Tunnel to	mqyuledcyic.ru:443
4268	502	HTTP		Tunnel to	obqpdmjn.ru:443
4269	502	HTTP		Tunnel to	jatpvjafbwptyag.ru:443
4270	502	HTTP		Tunnel to	ueizvrprmwmdyejmhkycig.ru:443
4271	502	HTTP		Tunnel to	debyixoc.ru:443
4272	502	HTTP		Tunnel to	xbkyvofc.ru:443
4273	502	HTTP		Tunnel to	bbhghuku.ru:443
4274	502	HTTP		Tunnel to	psfrnlmdpkzr.ru:443
4275	502	HTTP		Tunnel to	mvpwppgsujt.ru:443
4276	502	HTTP		Tunnel to	qhreuqyk.ru:443
4277	502	HTTP		Tunnel to	wjikevjm.ru:443
4278	502	HTTP		Tunnel to	agxqstwcoc.ru:443
4279	502	HTTP		Tunnel to	trzxvhstxnthwccego.ru:443
4280	502	HTTP		Tunnel to	oibldgaj.ru:443
4281	502	HTTP		Tunnel to	hkxjpbah.ru:443
4282	502	HTTP		Tunnel to	hkpjfcip.ru:443
4283	502	HTTP		Tunnel to	gstbidaxyepl.ru:443
4284	502	HTTP		Tunnel to	rbmccpnyjjsmhg.ru:443
4285	502	HTTP		Tunnel to	qfqyqwzqqxmevjjtwrmsgsg.ru:443
4286	502	HTTP		Tunnel to	ytigdmjmkhmaavjpyfimro.ru:443
4287	502	HTTP		Tunnel to	uxzusbcu.ru:443
4288	502	HTTP		Tunnel to	ejmlcqdjjixzfn.ru:443
4289	502	HTTP		Tunnel to	difnjbmlrezxkiwyjhqknja.ru:443
4290	502	HTTP		Tunnel to	qcnqcqiy.ru:443
4291	502	HTTP		Tunnel to	phplstknpzvzxaakybc.ru:443
4292	502	HTTP		Tunnel to	xcofeihllcuzdvbsduugpjl.ru:443
4293	502	HTTP		Tunnel to	luamnnbo.ru:443
4294	502	HTTP		Tunnel to	jaxvaxwdfsdpzgsuprga.ru:443
4295	502	HTTP		Tunnel to	yjubrrfpkjadsevaqz.ru:443
4296	502	HTTP		Tunnel to	bgjmnsqg.ru:443
4297	502	HTTP		Tunnel to	epztnxcjaldvqa.ru:443
4298	502	HTTP		Tunnel to	rysiakzkrkwyxhzxlqidnekd.ru:443
4299	502	HTTP		Tunnel to	kivhkjgvsephj.ru:443
4300	502	HTTP		Tunnel to	yvncjjmqkrt.ru:443
4301	502	HTTP		Tunnel to	sykrqgfhekgtplpi.ru:443
4302	502	HTTP		Tunnel to	mdfftmsx.ru:443



Iahapemwionkmti.ru — Kullanımda — sileye git

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

Bitiş 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 Ülkesi	Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.ripn.net
IP / Sunucu Bilgileri	IP: 94.126.178.17
	Ülke: Danimarka
	Registry Whois Sunucu: whois.ripe.net

Registry Whois Kaydı | IP 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).

domain:        IAHAPEMWIONKMTI.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
```

Dksqlojglsmsizjjrdllgiqt.ru — Kullanımda — sileye git

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

Bitiş 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 Ülkesi	Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.ripn.net
IP / Sunucu Bilgileri	

Registry Whois Kaydı | IP 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).

domain:        DKSQLOJGLSMSIZJJRDLLGIQT.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:       2014.08.25
paid-till:     2015.08.28
free-date:     2015.09.28
source:        TCI

Last updated on 2014.09.08 12:31:32 MSK
```

Mqyuledcyic.ru — Kullanımda — sileye git

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

Bitiş 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 Ülkesi	Rusya Federasyonu
Registrar	REGRU-RU
Registry Whois Sunucu	whois.ripn.net
IP / Sunucu Bilgileri	IP: 193.124.18.187
	Ülke: Rusya Federasyonu
	Registry Whois Sunucu: whois.ripe.net

Registry Whois Kaydı | IP 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).

domain:        MQYULEDCYIC.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
```

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