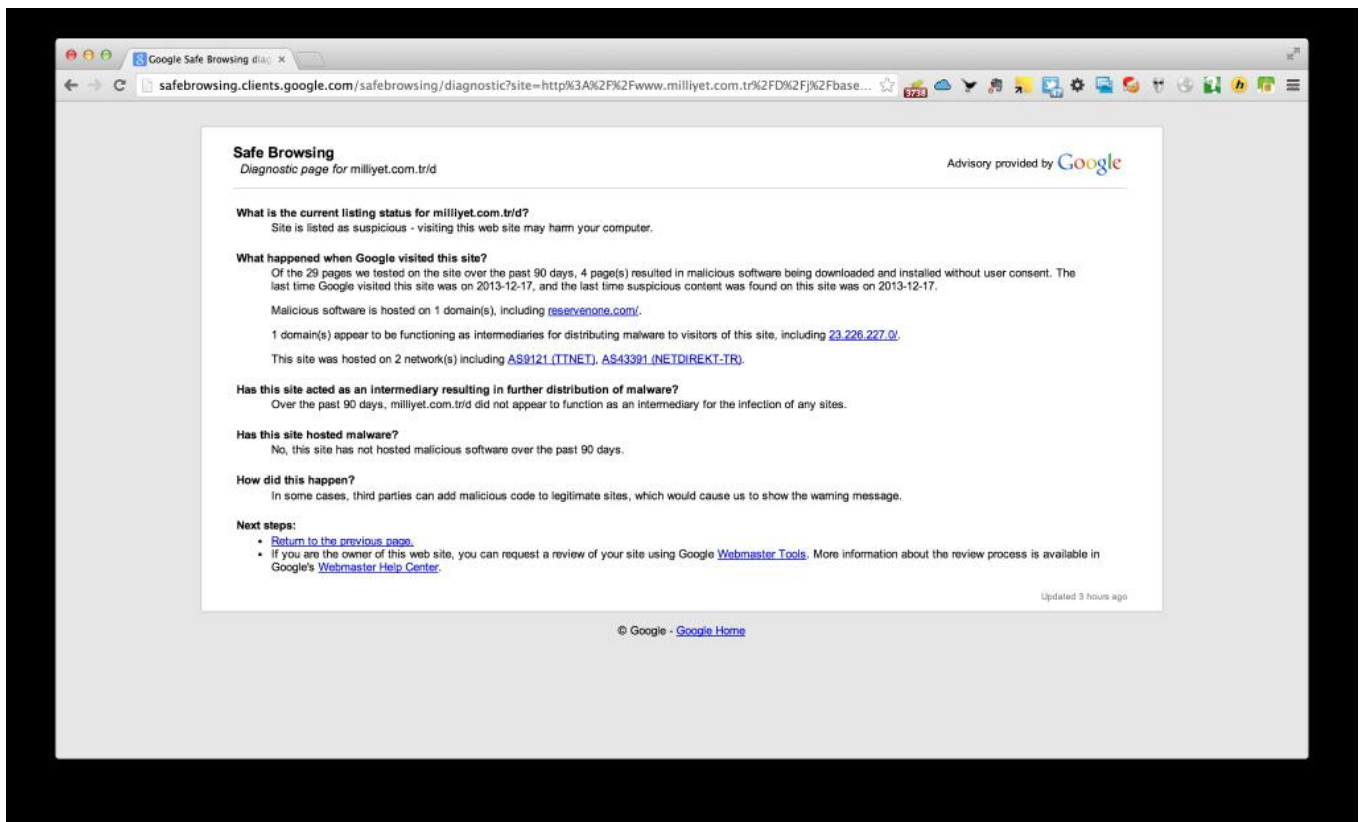


VirusTotal Proxy

written by Mert SARICA | 1 April 2014

Art niyetli kişilerin istismar kitleri sayesinde yaması eksik olan (java, flash, pdf, internet tarayıcısı vs.) sistemleri kontrol altına aldıklarına ve bu sistemlere uzaktan yönetime imkan tanıyan zararlı yazılımlar yüklediklerine son yıllarda sıklıkla rastlıyoruz. Özellikle medya, oyun, haber siteleri gibi hit sayısı oldukça fazla olan siteler, istismar kitlerini yüklemek için art niyetli kişilerin son zamanlarda hedefi haline geliyorlar.

17 Aralık 2013 tarihinde Milliyet'in internet sitesini Chrome internet tarayıcısı ile ziyaret edenler bir güvenlik uyarısı ile karşılaştılar. Bu uyarıda Google'ın siteyi en son ziyaret ettiğinde zararlı bir içerikle karşılaştığını ve bu nedenle siteyi kara listeye aldığı belirtiliyordu. Ağ üzerinden zararlı yazılım tespiti yapabilen cihazlar kullanan kurumlar ise o esnada Milliyet'i ziyaret eden kullanıcılarının tam olarak ne ile karşı karşıya olduklarını tespit edebildiler. Bu, Neutrino adında bir istismar kitiydi.



Server DNS Name: 62.210.137.205 Service Port: 8000 Signature Name: ExploitKit/Neutrino

Direction	Command	User-Agent	Host
GET	/breygkopybeqn7fugtpeqhi=4352018 HTTP/1.1	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	cot5eed.reservnone.com:8000
	Others	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*; Accept-Language: en-US; Accept-Encoding: gzip, deflate, peerdist; X-PZP-FeedDist: Version=1.0	

Elinizde en son teknoloji bir cihaz da olsa, Chrome gibi akıllı bir internet

tarayıcısı da kullanıyor olsanız kimi zaman bu tehditler karşısında uyarı/alarm alana dek, sisteminiz veya kurumunuzun sistemleri çoktan art niyetli kişilerin kontrolü altına girmiş olabiliyor. Zararlı yazılım analizi ile ilgilenen biriyseniz de analiz için çoğu zaman zararlı yazılıma/koda erişmeniz bu uyarılarla karşılaştıktan sonra sunucuya/koda erişimin yasaklanması/kaldırılması nedeniyle pek mümkün olamayabiliyor.

Bildiğiniz gibi VirusTotal, sadece zararlı yazılım analizi yapmakla kalmayıp ayrıca 52 farklı kaynak üzerinden zararlı URL, kod analizi gerçekleştirip, raporlayabiliyor. Çorbada tuzum olsun, kullanıcılar, güvenlik uzmanları, bu tehditlerden daha kısa sürede haberdar olabilsinler diye VirusTotal ile entegre çalışabilen bir araç hazırlamaya karar verdim.

Adına VirusTotal Proxy dediğim bu aracı, internet tarayıcısı ve sistem üzerinde çalışan bir proxy aracı (örnek: CNTLM) arasında konumlandırıdım. İnternet tarayıcısı ile kullanıcı herhangi bir siteye bağlanmaya çalıştığı zaman bu araç kullanıcının bağlanmaya çalıştığı adresi paralelde alarak VirusTotal sitesine gönderiyor ve kullanıcıya 52 farklı kaynak üzerinden bu site üzerinde zararlı bir kod olup olmadığı konusunda bilgi veriyor. Sadece bilgi vermekle kalmayıp ayrıca belirtilen alarm seviyesine göre uyarı sesi de veriyor.

Aracın kullanımına geçmeden önce, sistem üzerinde mutlaka bir proxy aracının çalışması gerekiyor. Bunun için kendi sistemim üzerine açık kaynak kodlu CNTLM proxy aracını kurdum ve tüm trafik için proxy vazifesi görebilmesi adına ayar dosyasındaki (cntlm.ini) NoProxy ayarını * olarak değiştirdim ve 3128. bağlantı noktasında (port) çalıştırdım.

```
cntlm.ini - Notepad
File Edit Format View Help
# proxies. Normally the value is auto-guessed.
#
# workstation netbios_hostname

# List of parent proxies to use. More proxies can be defined
# one per line in format <proxy_ip>:<proxy_port>
#
Proxy          10.0.0.41:8080
# Proxy        10.0.0.42:8080

# List addresses you do not want to pass to parent proxies
# * and ? wildcards can be used
#
NoProxy        *

# Specify the port cntlm will listen on
# You can bind cntlm to specific interface by specifying
# the appropriate IP address also in format <local_ip>:<local_port>
# cntlm listens on 127.0.0.1:3128 by default
#
Listen         3128

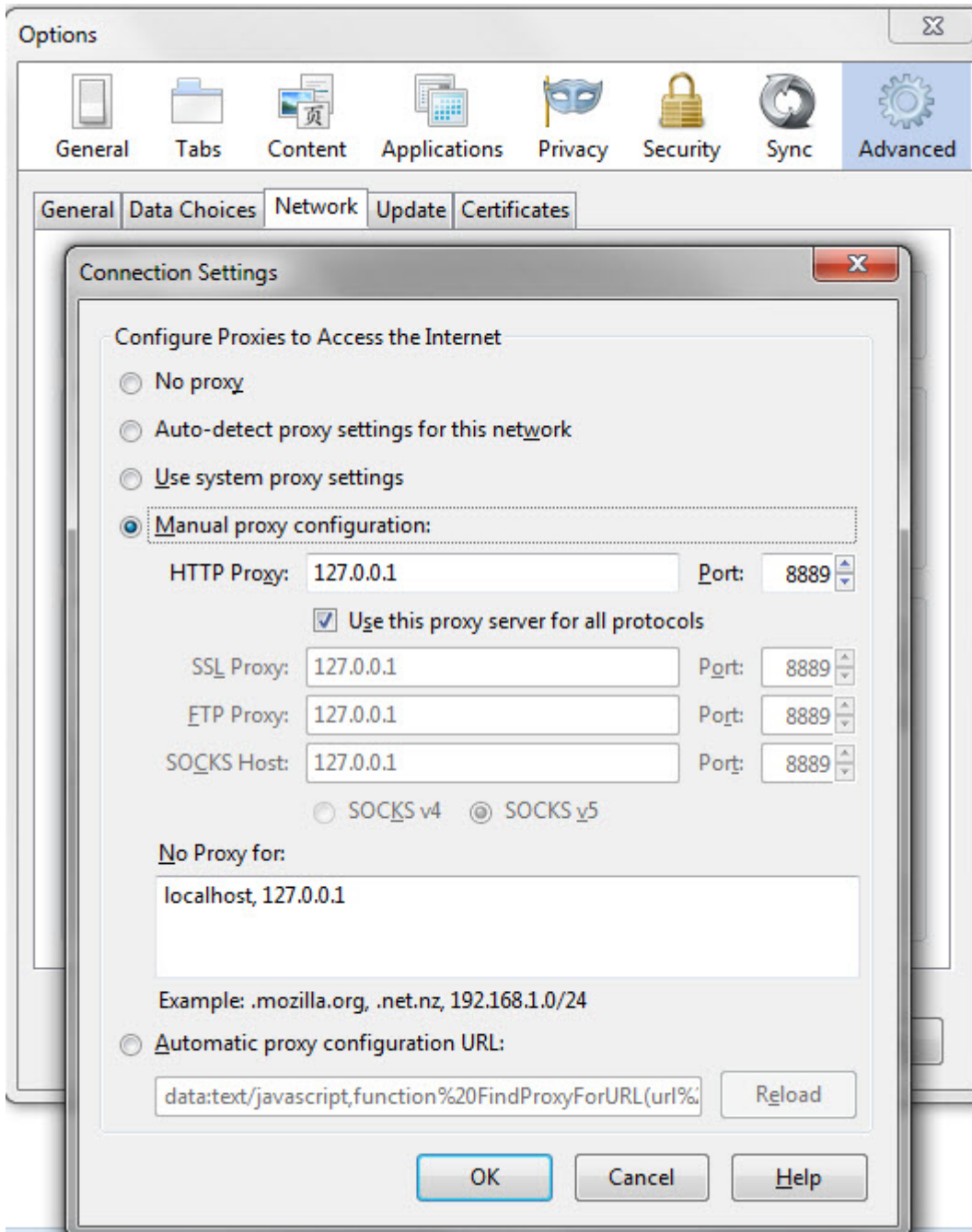
# If you wish to use the SOCKS5 proxy feature as well, uncomment
# the following option. It can be used several times
# to have SOCKS5 on more than one port or on different network
# interfaces (specify explicit source address for that).
#
# WARNING: The service accepts all requests, unless you use
# SOCKS5User and make authentication mandatory. SOCKS5User
# can be used repeatedly for a whole bunch of individual accounts.
#
#SOCKS5Proxy   8010
#SOCKS5User    dave:password

# Use -M first to detect the best NTLM settings for your proxy.
```

Aracın kullanımını ise oldukça basit. Aracı çalıştırmak için biri opsiyonel olmak üzere 4 adet parametre kullanmanız gerekiyor. -l parametresi ile aracın sistem üzerinde hangi bağlantı noktası üzerinde internet tarayıcısından gelecek bağlantı isteklerini dinleyeceğini belirtiyorsunuz. -r parametresi ile ister kendi sisteminizde çalışan ister başka bir sistem üzerinde çalışan ve internet bağlantısı kuracak olan proxy sunucusunun ip adresini belirtiyorsunuz. -p parametresi ile de haberleşilecek olan proxy sunucusunun hangi bağlantı noktası üzerinde çalıştığını belirtiyorsunuz. Opsiyonel olan -a parametresi ile de VirusTotal Proxy aracının VirusTotal üzerindeki 52 farklı kaynaktan kaç tane zararlı kod tespit ederse sesli alarm üretmesi gerektiğini belirtiyorsunuz. (-a 2 ile 2 tane kaynak zararlı kod tespit ederse sesli alarm ver gibi)

```
C:\Windows\system32\cmd.exe - python vtp.py -l 8889 -r 127.0.0.1 -p 3128 -a 2
=====
VirusTotal Proxy [http://www.mertsarica.com]
=====
[+] Listening on port 8889
```

Son adımda ise internet tarayıcınızın ağ ayarlarında, proxy adresi olarak VirusTotal Proxy aracının dinlediği ip adresini ve bağlantı noktasını belirtiyorsunuz ve ardından VirusTotal Proxy aracını (vtp.py) çalıştırıyorsunuz ve web sitelerini gezmeye başlıyorsunuz. VirusTotal Proxy aracı siz web sitelerini gezerken arka planda tüm haberleştiğiniz siteleri VirusTotal'a gönderecek ve hem ekrana hem de vtp.txt dosyasına hangi sitede, kaç tane zararlı kod tespit edildiğini, rapor adresleri ile birlikte kayıt altına alacaktır.



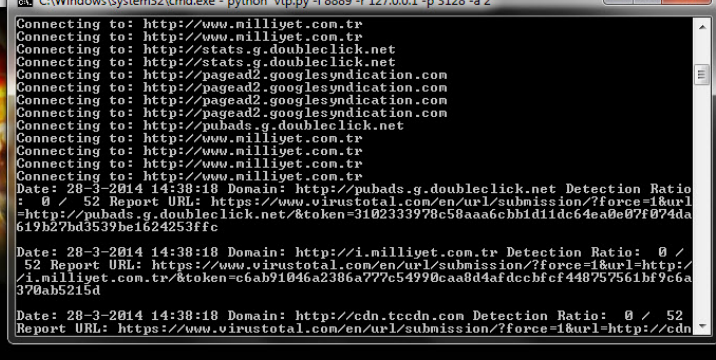
Detaylı bilgi ve rezervasyon için:
444 0 329
www.touristica.com.tr

touristica
tatil aşkına

Bugünkü Gazete
Milliyet Emlak
Milliyet Heryerde
Milliyet Arşiv

Favorilerime ekle
Ana sayfam yap
Künye
Kampanyalar

FLAŞ



```
C:\Windows\system32\cmd.exe - python vtp.py -l 8889 -r 127.0.0.1 -p 3128 -a 2
Connecting to: http://www.milliyet.com.tr
Connecting to: http://stats.g.doubleclick.net
Connecting to: http://pagead2.googlesyndication.com
Connecting to: http://pagead2.googlesyndication.com
Connecting to: http://pagead2.googlesyndication.com
Connecting to: http://pubads.g.doubleclick.net
Connecting to: http://www.milliyet.com.tr
Connecting to: http://www.milliyet.com.tr
Connecting to: http://www.milliyet.com.tr
Connecting to: http://www.milliyet.com.tr
Date: 28-3-2014 14:38:18 Domain: http://pubads.g.doubleclick.net Detection Ratio: 0 / 52
Report URL: https://www.virustotal.com/en/url/submission/?force=1&url=http://pubads.g.doubleclick.net/&token=3102333978c58aa6cbb1d1dc64ea0e7f874619b27hd3539be1624253ffc
Date: 28-3-2014 14:38:18 Domain: http://i.milliyet.com.tr Detection Ratio: 0 / 52
Report URL: https://www.virustotal.com/en/url/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4fdccbf4407f1859e3a370ah5215d
Date: 28-3-2014 14:38:18 Domain: http://cdn.tccdn.com Detection Ratio: 0 / 52
Report URL: https://www.virustotal.com/en/url/submission/?force=1&url=http://cdn
```

SON DAKİKA... SON DAKİKA... SON DAKİKA... G.Saray'a nester! 5 isim volcu...

```
vp bt
1 28-3-2014 14:36:44|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4fdccbf4407f1859e3a370ah5215d
2 28-3-2014 14:36:45|http://www.adobe.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.adobe.com/&token=271188595d1eb0f1961fe72d6a9dc068ecaa67275665e03a0a11d0ef29
3 28-3-2014 14:36:45|http://www.googleadservices.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.googleadservices.com/&token=be2f218cb2d27983674a82025a6440f0492
4 28-3-2014 14:36:45|http://ssl.google-analytics.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://ssl.google-analytics.com/&token=ae653a0c327364a01fc74db
5 28-3-2014 14:36:45|http://stats.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://stats.g.doubleclick.net/&token=563a8b723e2fae00c4f5e6919b177848e52
6 28-3-2014 14:36:46|http://cube.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://cube.milliyet.com.tr/&token=id56082a746427d140db9c4023a6470caa93ba95
7 28-3-2014 14:36:47|http://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://sb.scorecardresearch.com/&token=e497eebdc85f81a9c9b2dd13bf2903361
8 28-3-2014 14:36:48|http://www.milliyet.com.tr| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.milliyet.com.tr/&token=712de7e2ddf279959a00ed424b4fd60bea9e63b554
9 28-3-2014 14:36:48|http://partner.googleadservices.com| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://partner.googleadservices.com/&token=fe48cb9a13a8987836879ea5f0
10 28-3-2014 14:36:48|http://icdncube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://icdncube.milliyetemlak.com/&token=1200741e97d127eaaab6dc6d599ef0f
11 28-3-2014 14:38:18|http://pubads.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://pubads.g.doubleclick.net/&token=3102333978c58aa6cbb1d1dc64ea0e7f874619b27hd3539be1624253ffc
12 28-3-2014 14:38:18|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4fdccbf4407f1859e3a370ah5215d
13 28-3-2014 14:38:18|http://cdn.tccdn.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://cdn.tccdn.com/&token=ca7731c5d28ff9d59a392fb2a1e9596bac15496fd5f247dd697241
14 28-3-2014 14:38:18|http://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://sb.scorecardresearch.com/&token=e497eebdc85f81a9c9b2dd13bf2903361
15 28-3-2014 14:38:19|http://subi.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://subi.milliyet.com.tr/&token=418609c31e43ff0b4f762c2f4ea703473c2d5d9a0e67
16 28-3-2014 14:38:19|http://live.spox.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://live.spox.com/&token=2167fa5c88fc148c422cb2a7be516bc5b39e7421d53f4a1af2e169
17 28-3-2014 14:38:19|http://pagead2.googlesyndication.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://pagead2.googlesyndication.com/&token=e0c64fb1694050b5d9ebf790
18 28-3-2014 14:38:18|http://www.milliyet.com.tr| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.milliyet.com.tr/&token=712de7e2ddf279959a00ed424b4fd60bea9e63b554
19 28-3-2014 14:41:20|http://icdncube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://icdncube.milliyetemlak.com/&token=1200741e97d127eaaab6dc6d599ef0f
20 28-3-2014 14:41:20|http://csi.gstatic.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://csi.gstatic.com/&token=3466e7ec9094b2789ff436f10f18b95e234c39999d406d5eb10e4
```

Hem sıradan kullanıcıların hem de siber güvenlik uzmanlarının faydalanabileceği bir araç olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.

- Not #1: VirusTotal Proxy aracını buradan indirebilirsiniz.
- Not #2: Programın ihtiyaç duyduğu Twisted Python kütüphanesini buradan indirebilirsiniz.
- Not #3: VirusTotal, otomatize işlemler için API'lerinin kullanılmasını rica ediyor dolayısıyla VirusTotal Proxy aracını şüphelendiğiniz siteleri kontrol amaçlı kullanmanızı rica ederim. VirusTotal API'sine buradan ulaşabilirsiniz.