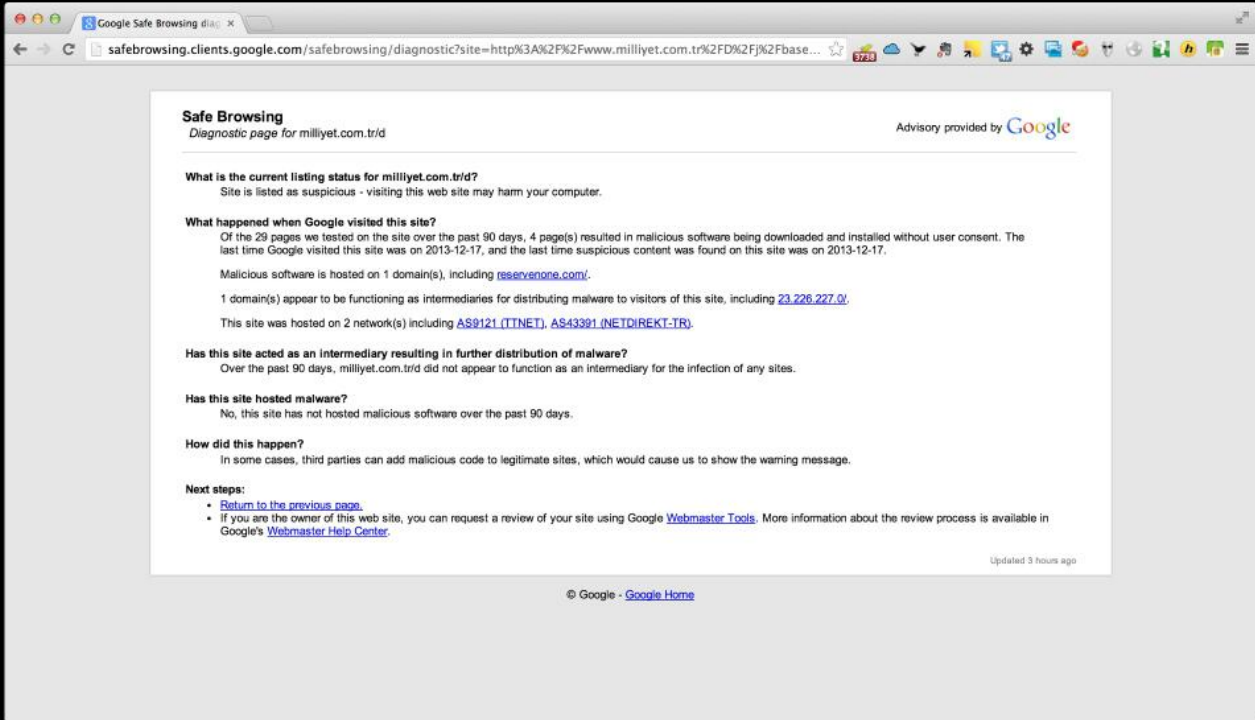


VirusTotal Proxy

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.



Safe Browsing
Diagnostic page for milliyet.com.tr?id

Advisory provided by Google

What is the current listing status for milliyet.com.tr?id?
Site is listed as suspicious - visiting this web site may harm your computer.

What happened when Google visited this site?
Of the 29 pages we tested on the site over the past 90 days, 4 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2013-12-17, and the last time suspicious content was found on this site was on 2013-12-17.
Malicious software is hosted on 1 domain(s), including [reservnone.com/](#).
1 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, including [23.226.227.0/](#).
This site was hosted on 2 network(s) including [AS8121 \(TTNET\)](#), [AS43391 \(NETDIREKT-TR\)](#).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, milliyet.com.tr?id did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?
No, this site has not hosted malicious software over the past 90 days.

How did this happen?
In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

Next steps:

- [Return to the previous page.](#)
- If you are the owner of this web site, you can request a review of your site using Google [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

Updated 3 hours ago

© Google - [Google Home](#)

Server DNS Name: 62.210.137.206 Service Port: 8000 Signature Name: Exploit.Kit.Neutrino

Direction	Command	User-Agent	Host
GET	/breygkopybeq7fugtpceqhi=4352018 HTTP/1.1	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	cotSeed.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-P2P-Feeder: Version=1.0	

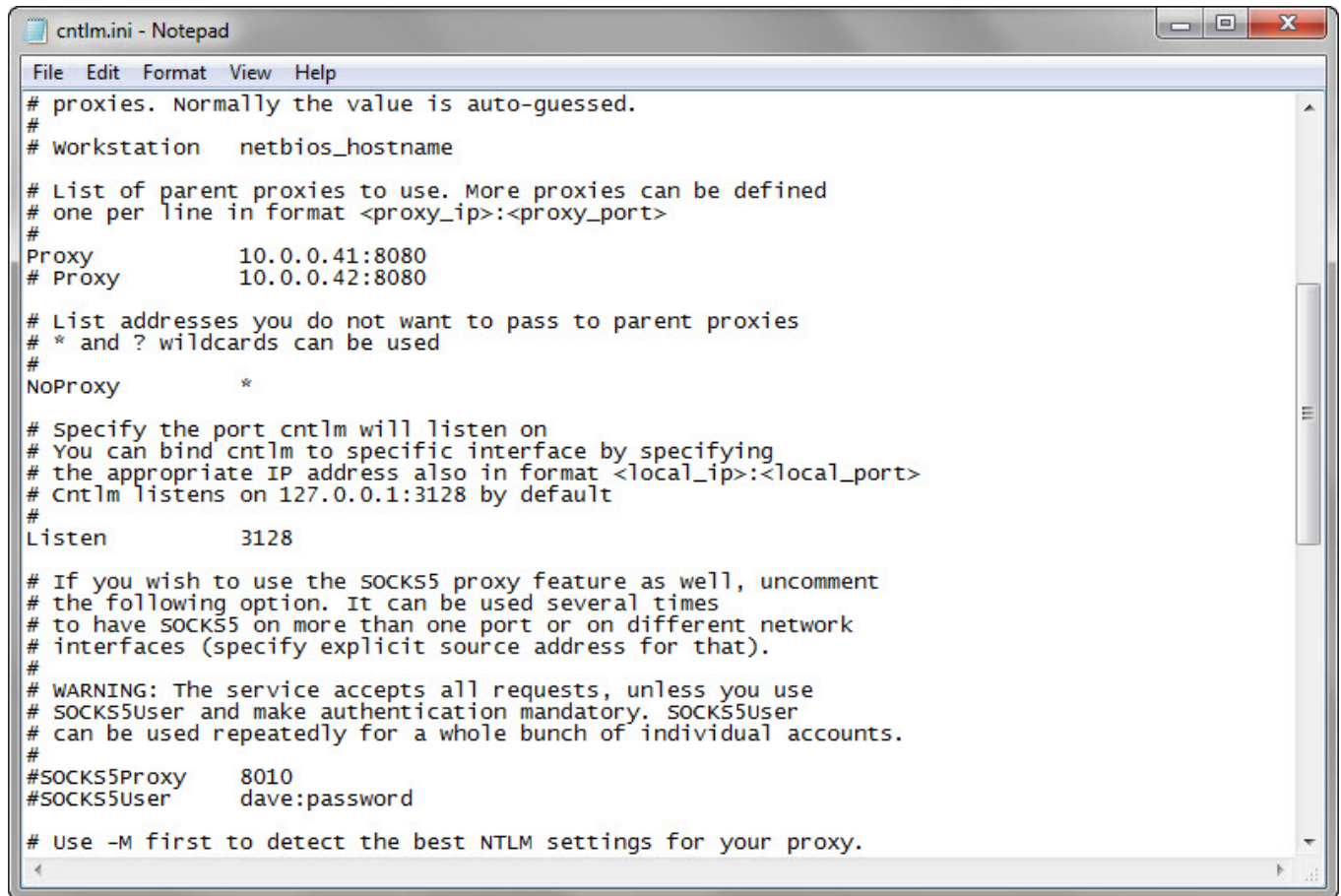
Elinizde en son teknoloji bir cihaz da olsa, Chrome gibi akıllı bir internet

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.

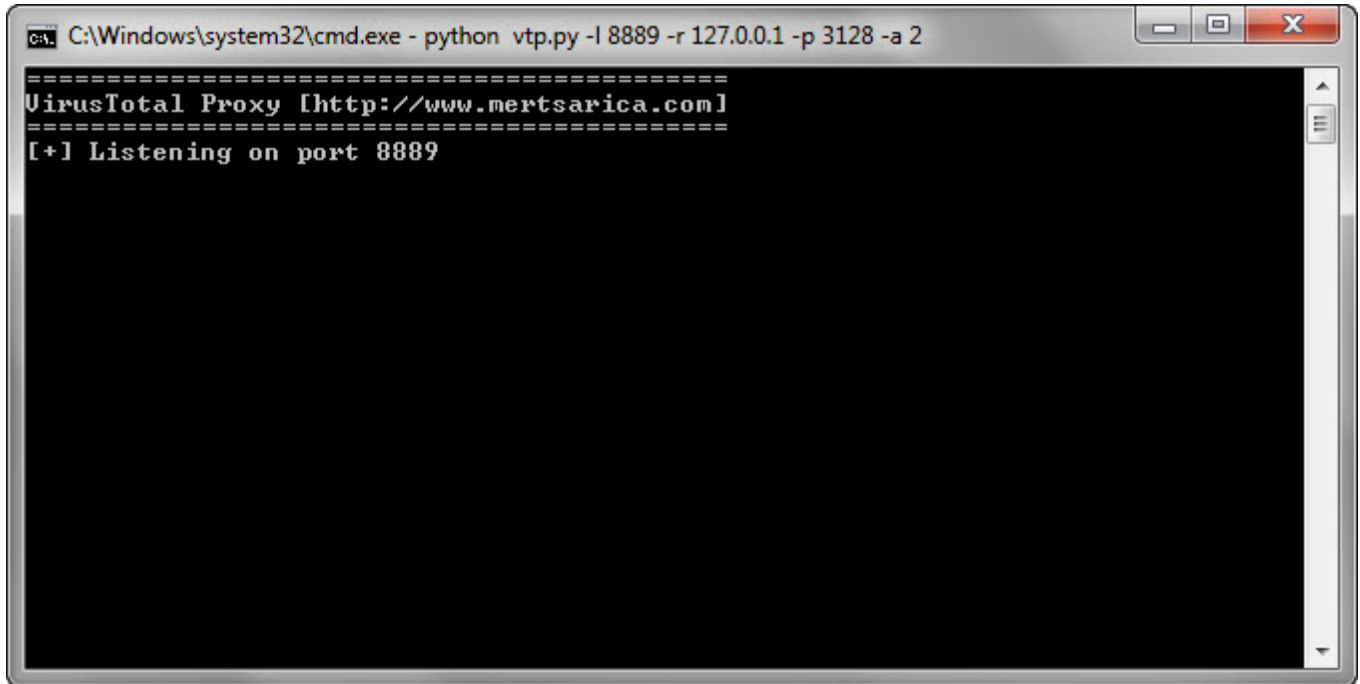
Adına VirusTotal Proxy dediğim bu aracı, internet tarayıcısı ve sistem üzerinde çalışan bir proxy aracı (örnek: CNTLM) arasında konumlandırımdı. İnternet tarayıcısı ile kullanıcı herhangi bir siteye bağlanmaya çalıştığı zaman bu araç kullanıcının bağlanmaya çalıştığı adresi paralelde alarak VirusTotal 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.



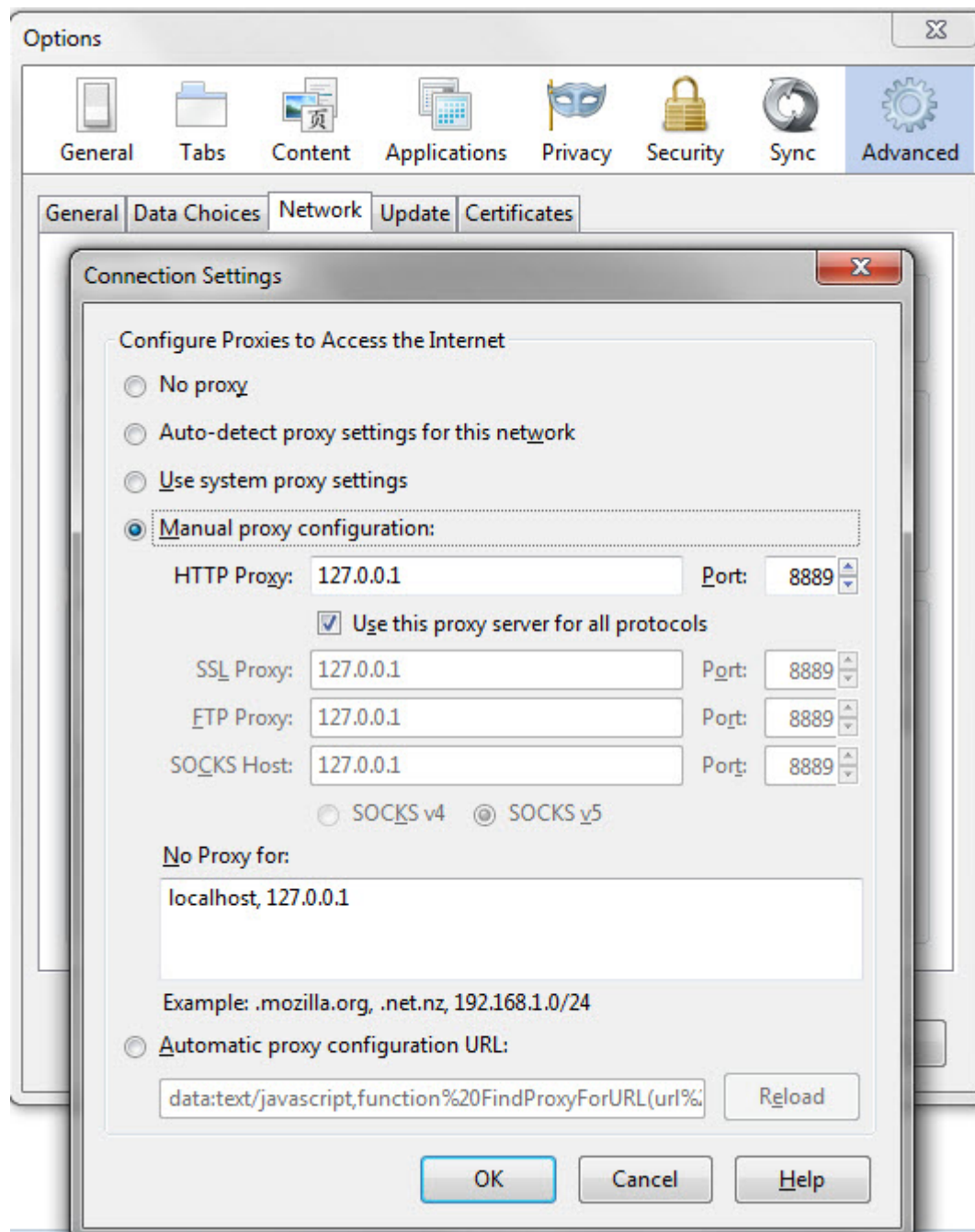
```
File Edit Format View Help
# proxies. Normally the value is auto-guessed.
#
# workstation netbios_hostname
#
# List of parent proxies to use. More proxies can be defined
# one per line in format <proxy_ip>:<proxy_port>
#
Proxy          10.0.0.41:8080
# Proxy        10.0.0.42:8080
#
# List addresses 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.
```

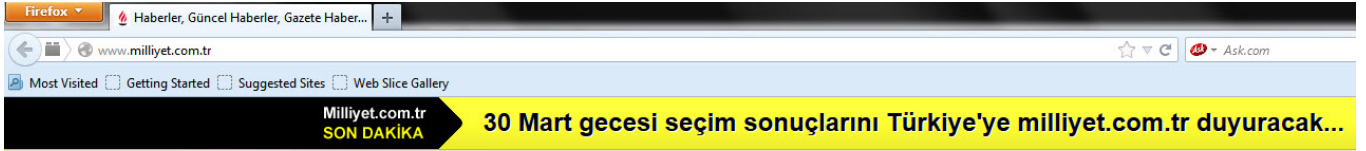
Aracın kullanımı ise oldukça basit. Aracı çalıştırmak için biri opsiyonel olmak üzere 4 adet parametre kullanmanız gerekiyor. -l parametresi ile aracın sistem üzerinde hangi bağlantı noktası üzerinde internet tarayıcısından gelecek bağlantı isteklerini dinleyeceğini belirtiyorsunuz. -r parametresi ile 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)

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe' followed by the command 'python vtp.py -l 8889 -r 127.0.0.1 -p 3128 -a 2'. The command prompt displays the output of the script: '=====
VirusTotal Proxy [http://www.mertsarica.com]
=====
[+] Listening on port 8889'. The rest of the window is black.

```
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 Her yerde

Milliyet Arşiv

Favorilerime ekle

Ana sayfam yap

Künye

Kampanyalar

28 Mart 2014, Cuma Bizi izleyin: [f](#) [t](#) [s](#) Üyelik CANLI BORSA BIST 68.438 2,07 ▲ EURO 3,0080 -0,08 ▼ USD 2,1910 0,23 ▲ ALTIN 91,3900 0,64 ▲

Milliyet.com.tr

BAŞINDA GÜVEN

Türkiye'nin lider haber sitesi

kelime ya da haber **Ara**

ADAYINIZI DESTEKLEMELİK İÇİN

Son Dakika Yazarlar Siyaset Ekonomi Finans **Spor SKORER** Dünya Gündem Magazin Cadda **Milliyet TV** SKORER TV Tüm

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://www.milliyet.com.tr
Connecting to: http://stats.g.doubleclick.net
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/submit/force=1&url=http://pubads.g.doubleclick.net/&token=318233978c58aa6cbbd1d1dc64ea0e07f074da619b27hd3539be1624253ffc

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/submit/force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdc0bfcf448757561bf370ab5215d

Date: 28-3-2014 14:38:18 Domain: http://cdn.tccdn.com Detection Ratio: 0 / 52
Report URL: https://www.virustotal.com/en/url/submit/force=1&url=http://cdn.tccdn.com
```

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

```
vtp.bt
1 28-3-2014 14:36:44|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdc0bfcf448757561bf370ab5215d
2 28-3-2014 14:36:45|http://www.adobe.com| 1 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://www.adobe.com/&token=271188595d1eb0ff961fe72d6a9dc68ecaa67275665e03a0a1dd0ef29
3 28-3-2014 14:36:45|http://www.googleadservices.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://www.googleadservices.com/&token=beff218cbd227963674a82025a64d0f0492
4 28-3-2014 14:36:45|https://ssl.google-analytics.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=https://ssl.google-analytics.com/&token=a8b594e6530c0c32736401fc5760b
5 28-3-2014 14:36:45|http://stats.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://stats.g.doubleclick.net/&token=a583ab723e2fae001c56e9919b177884e52
6 28-3-2014 14:36:46|http://icube.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://icube.milliyet.com.tr/&token=id56082a74642d140d0b9c4023a6470caa3f0a965
7 28-3-2014 14:36:47|https://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submit/force=1&url=https://sb.scorecardresearch.com/&token=ef497eebdc853f81a9c9b2dd13bf2903361
8 28-3-2014 14:36:48|http://www.milliyet.com.tr| 2 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://www.milliyet.com.tr/&token=712de7e2ddf2799b59a00edd424b4fd60bdea9e63b554
9 28-3-2014 14:36:48|http://partner.googleadservices.com| 2 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://partner.googleadservices.com/&token=fe489cb9a13e78687836879eaaf0f
10 28-3-2014 14:36:48|http://icdncube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://icdncube.milliyetemlak.com/&token=1200741e97d127eeadabd6cd599ef40f
11 28-3-2014 14:38:18|http://pubads.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://pubads.g.doubleclick.net/&token=310233978c58aa6cbbd1d1dc64ea0e07f074da619b27hd3539be1624253ffc
12 28-3-2014 14:38:18|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdc0bfcf448757561bf370ab5215d
13 28-3-2014 14:38:18|http://cdn.tccdn.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://cdn.tccdn.com/&token=ca7731c5d28ff9d59ab392fb2a1e59596bac1549df6d5f247dd697241
14 28-3-2014 14:38:18|https://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submit/force=1&url=https://sb.scorecardresearch.com/&token=ef497eebdc853f81a9c9b2dd13bf2903361
15 28-3-2014 14:38:19|http://subi.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://subi.milliyet.com.tr/&token=418609c31e43ff0b4f762c2f4ea703473c2d5d9a0d67
16 28-3-2014 14:38:19|http://live.sporx.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://live.sporx.com/&token=2167fa5c88f05148c422cb2a7be5516bc5b39e7421d53f4a1af2e169
17 28-3-2014 14:38:19|http://pagead2.googlesyndication.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://pagead2.googlesyndication.com/&token=e0c64fb1689d05b0b5d9ebf790
18 28-3-2014 14:38:19|http://icdncube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://icdncube.milliyetemlak.com/&token=712de7e2ddf2799b59a00edd424b4fd60bdea9e63b554
19 28-3-2014 14:41:20|http://icdncube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://icdncube.milliyetemlak.com/&token=1200741e97d127eeadabd6cd599ef40f
20 28-3-2014 14:41:20|http://csi.gstatic.com| 0 / 52|https://www.virustotal.com/en/url/submit/force=1&url=http://csi.gstatic.com/&token=3466e7ec9094b2789ff436f10f18b9e5234c39999d4d065deb10e4
```

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.