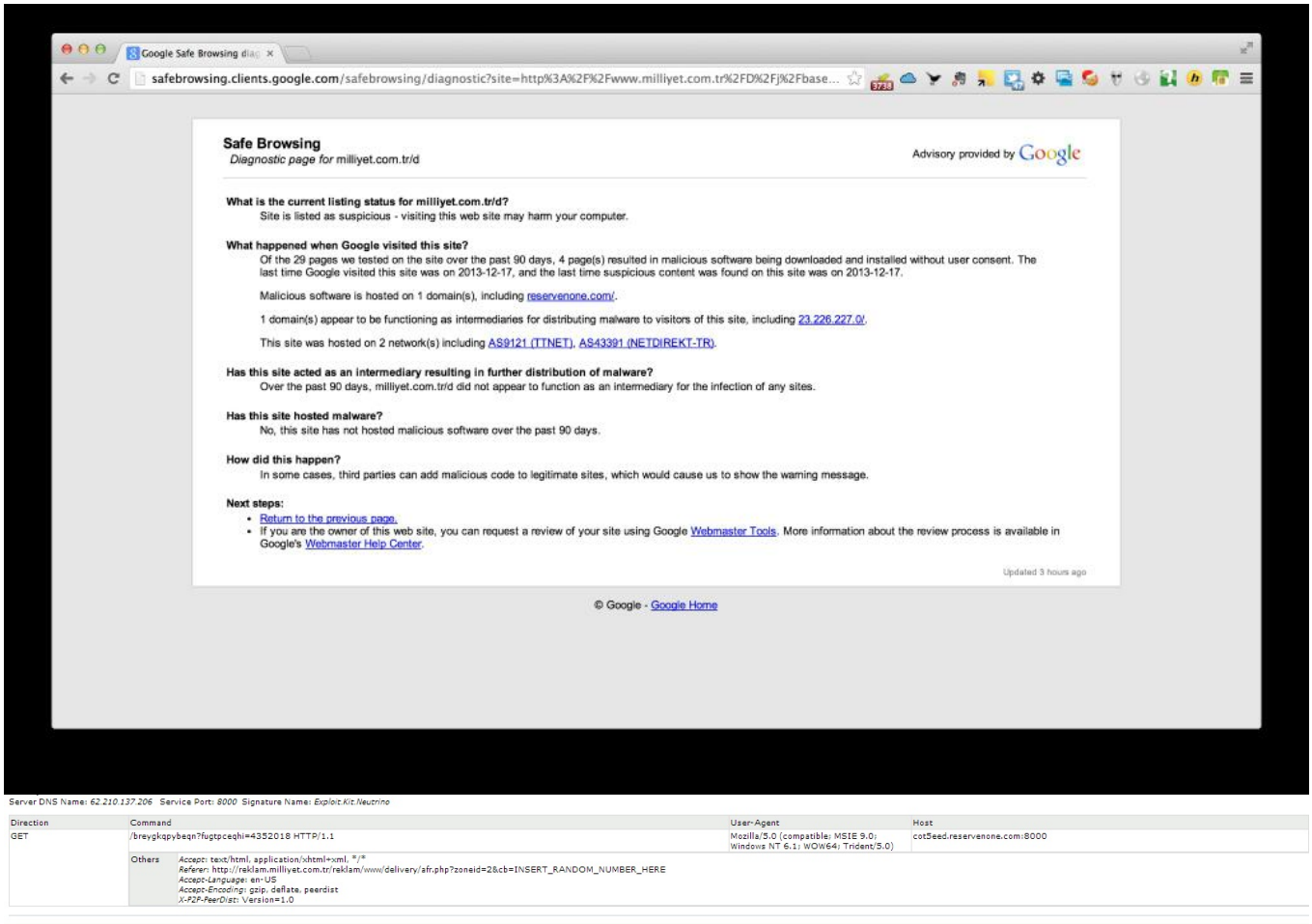
VirusTotal Proxy

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 ile 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.



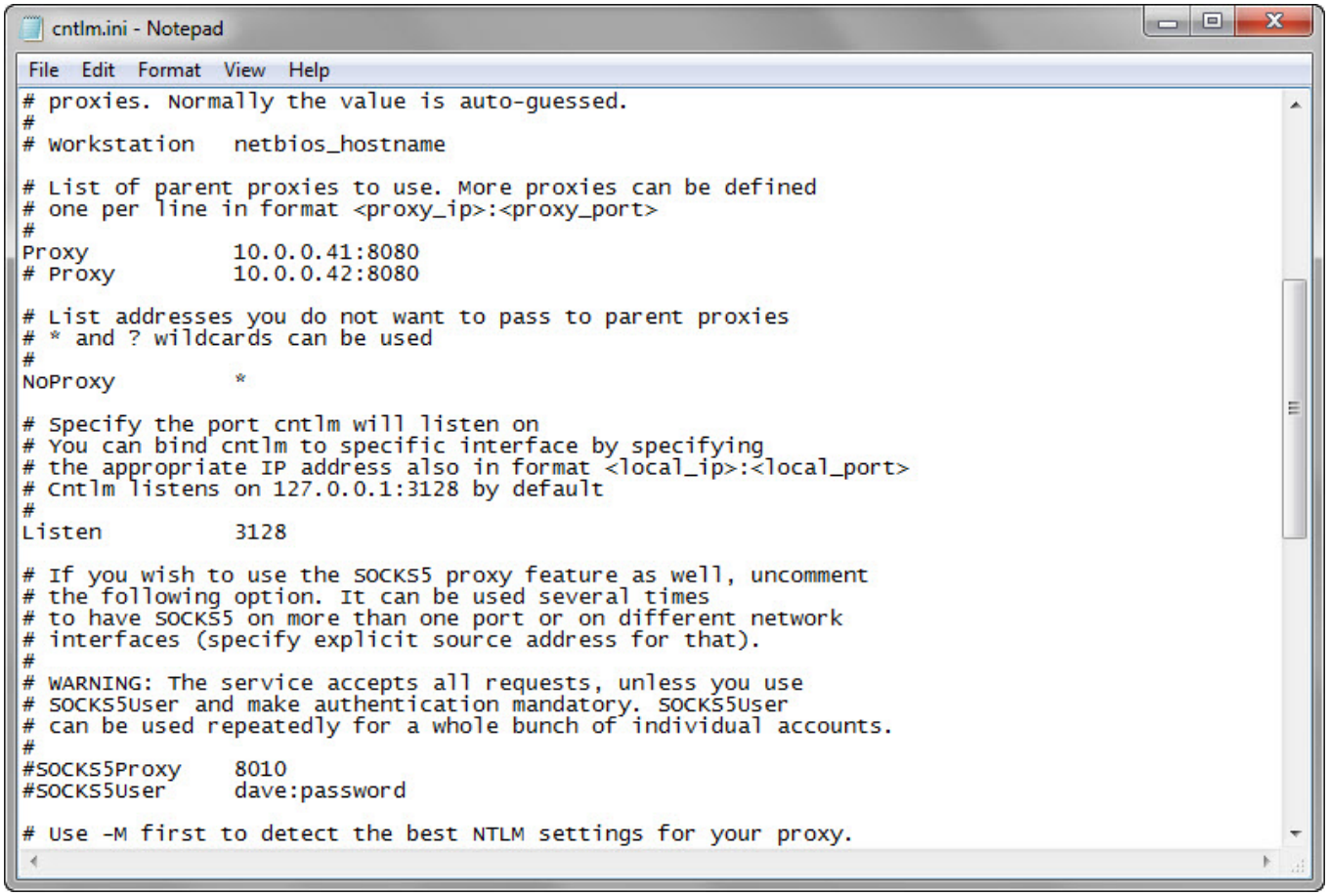
Elinizde en son teknoloji bir cihaz da olsa, Chrome gibi akıllı bir internet

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.

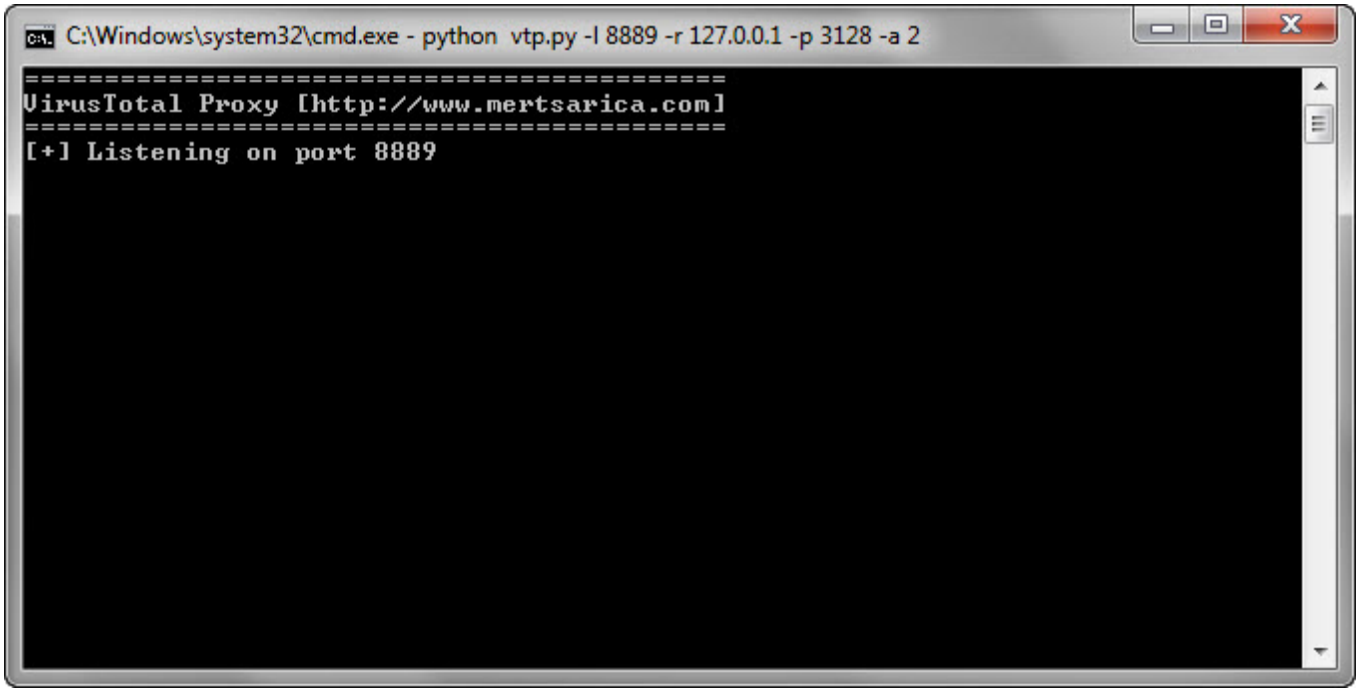
Bildiğiniz gibi VirusTotal, sadece zararlı yazılım analizi yapmakla kalmayıp ayrıca 52 farklı kaynak üzerinden zararlı URL, kod analizi gerçekleştirip, raporlayabiliyor. Çorbada tuzum olsun, kullanıcılar, güvenlik uzmanları, bu tehditlerden daha kısa sürede haberdar olabilsinler diye VirusTotal ile entegre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

Adına VirusTotal Proxy dediğim bu aracı, internet tarayıcısı ve sistem üzerinde çalışan bir proxy aracı (örnek: CNTLM) arasında konumlandırdım. Internet 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.

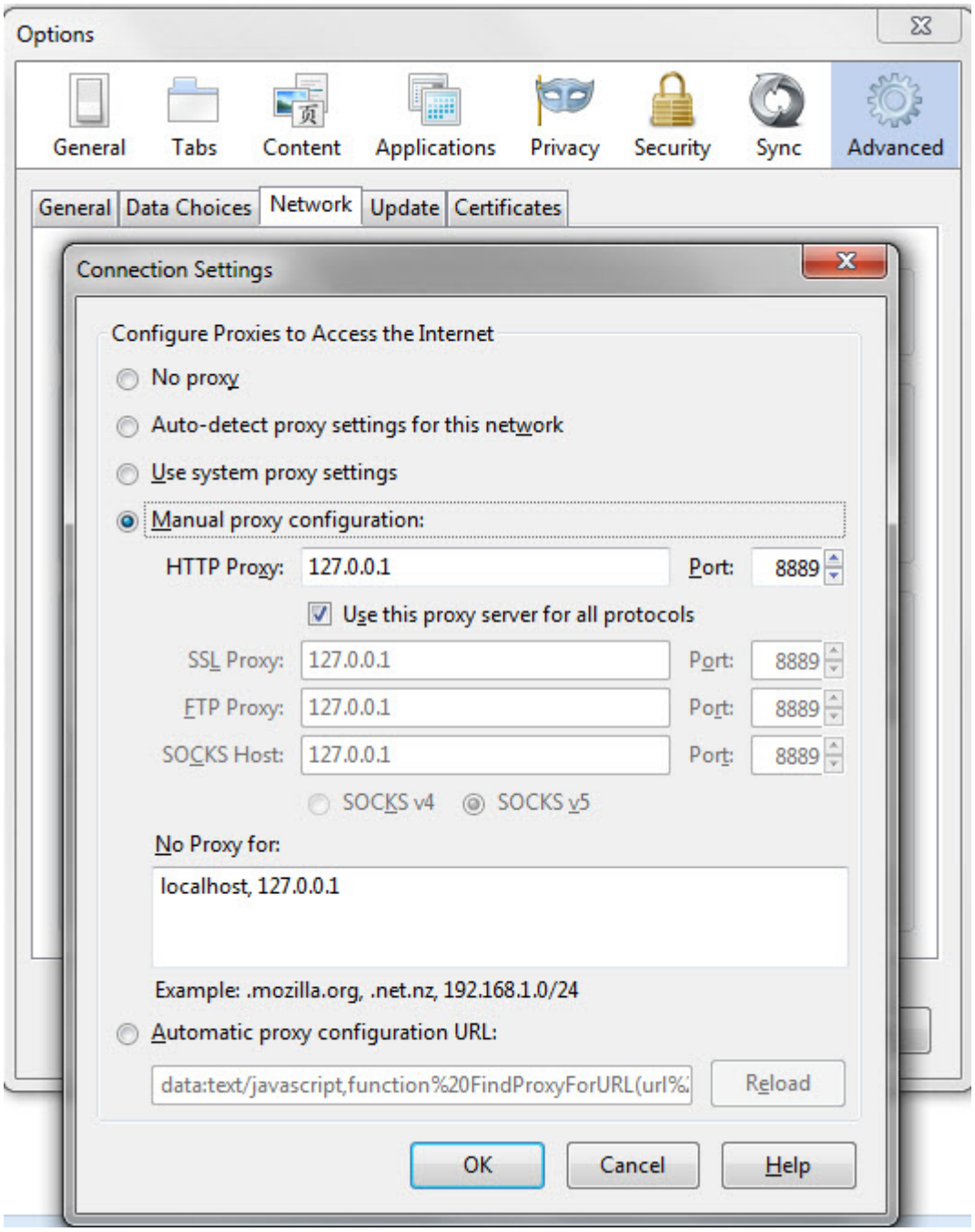
Aracın kullanımına geçmeden önce, sistem üzerinde mutlaka bir proxy aracının çalışması gerekiyor. Bunun için kendi sistemim üzerine açık kaynak kodlu CNTLM proxy aracını kurdum ve tüm trafik için proxy vazifesi görebilmesi adına ayar dosyasındaki (cntlm.ini) NoProxy ayarını * olarak değiştirdim ve 3128.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



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 kaçı zararlı kod tespit ederse sesli alarm üretmesi gerektiğini belirtiyorsunuz. (-a 2 ile 2 tane kaynak zararlı kod tespit ederse sesli alarm ver gibi)



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.


Options
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
General
Data Choices
Network
Update
Certificates
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
127.0.0.1
Port:
8889
Use this proxy server for all protocols
SSL Proxy:
127.0.0.1
Port:
8889
FTP Proxy:
127.0.0.1
Port:
8889
SOCKS Host:
127.0.0.1
Port:
8889
SOCKS v4
SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
data:text/javascript,function%20FindProxyForURL(url%
Reload
OK
Cancel
Help

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.