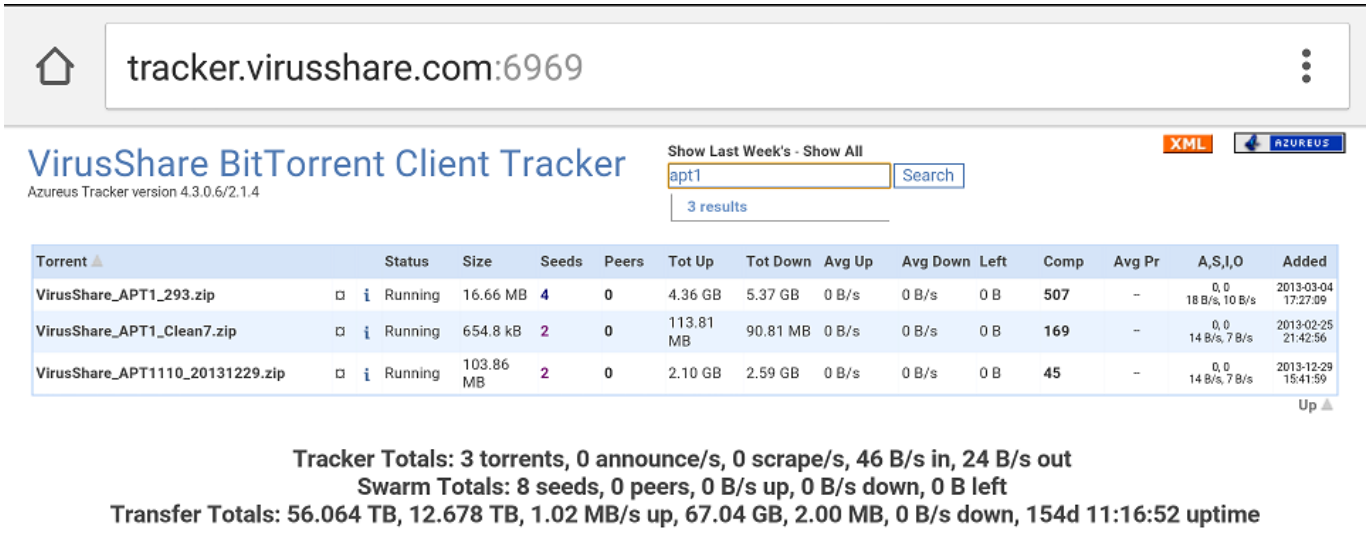
Bilinen Tehditlere Karşı Antivirüslerin Durumu

written by Mert SARICA | 1 June 2015

Son kullanıcı, sistem güvenlik yöneticisi, bilişim güvenliği uzmanı da olsanız, zaman zaman şu soruyu kendinize sorduğunuz oluyordur; Hangi antivirüs yazılımını kullanmalıyım ? Bilindiği üzere antivirüs yazılımlarının temelinde imza tabanlı bir teknoloji yatmaktadır bu nedenle yeni çıkan tehditlere karşı antivirüs yazılımı üreticisinin kısa bir süre içinde imza oluşturması ve bunu dünya genelindeki kullanıcılarına yaygınlaştırması, kullanıcıları açısından bilinen tehditlere karşı sistemlerini koruyabilme adına büyük bir öneme sahiptir. Dolayısıyla bir antivirüs yazılımını değerlendirirken, onlarca önemli kriterden bir tanesi de, bu antivirüs yazılımının veritabanının, bilinen tehditlerin ne kadarını tespit edebildiği, ne kadar güncel olduğudur.

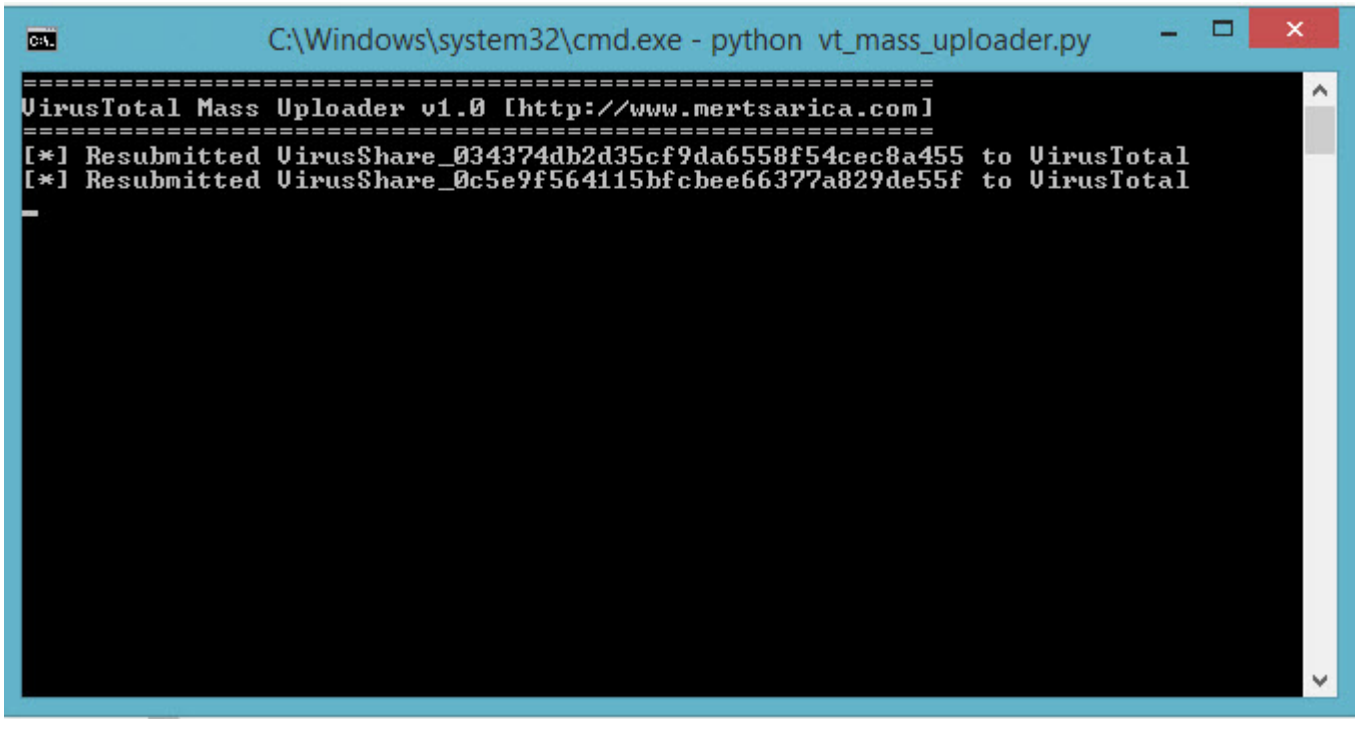
Evvel zaman içinde, sistem ve bellek üzerinden ileri seviye bilinmeyen zararlı yazılımları imzasız, davranışsal analiz yaparak tespit edebilen bir güvenlik ürününü değerlendirmek için çeşitli testler (POC – proof of concept) yaparken, antivirüs yazılımınlarının yetersiz olduğu noktalarda bu ürünün katma değerini ortaya çıkarmaya çalışıyordum. Bunun için de antivirüs yazılımlarının tespit edemediği fakat bu ürün tarafından davranışsal analiz ile tespit edilen ileri seviye zararlı yazılımlara ihtiyaç duymuştum.

Bu çalışmanın akabininde, antivirüs yazılımlarının bu zamana kadar tespit edilmiş olan APT zararlı yazılımlarını tespit etmede ne kadar başarılı olup olmadıklarını da öğrenmeye karar verdim. Mevzu bahis ileri seviye zararlı yazılımlar olunca aklıma hemen Mandiant'ın 2013 yılının Şubat ayında yayınlamış olduğu ve 2006 yılından raporun yayınlanmasına kadar geçen sürede Çinliler tarafından gerçekleştirilen ve ileri seviye saldırıları konu alan APT-1 raporu gelmişti. Mandiant sağolsun bu raporun yanında tespit ettikleri zararlı yazılımların md5 hash bilgilerini (1007 tane) de ek rapor olarak paylaşmıştı. 1007 tane zararlı yazılıma, testlerde kullanmak için ulaşmak pek mümkün olmasa da VirusShare sitesi sayesinde 293 tanesine ulaşmak mümkün olmuştu.

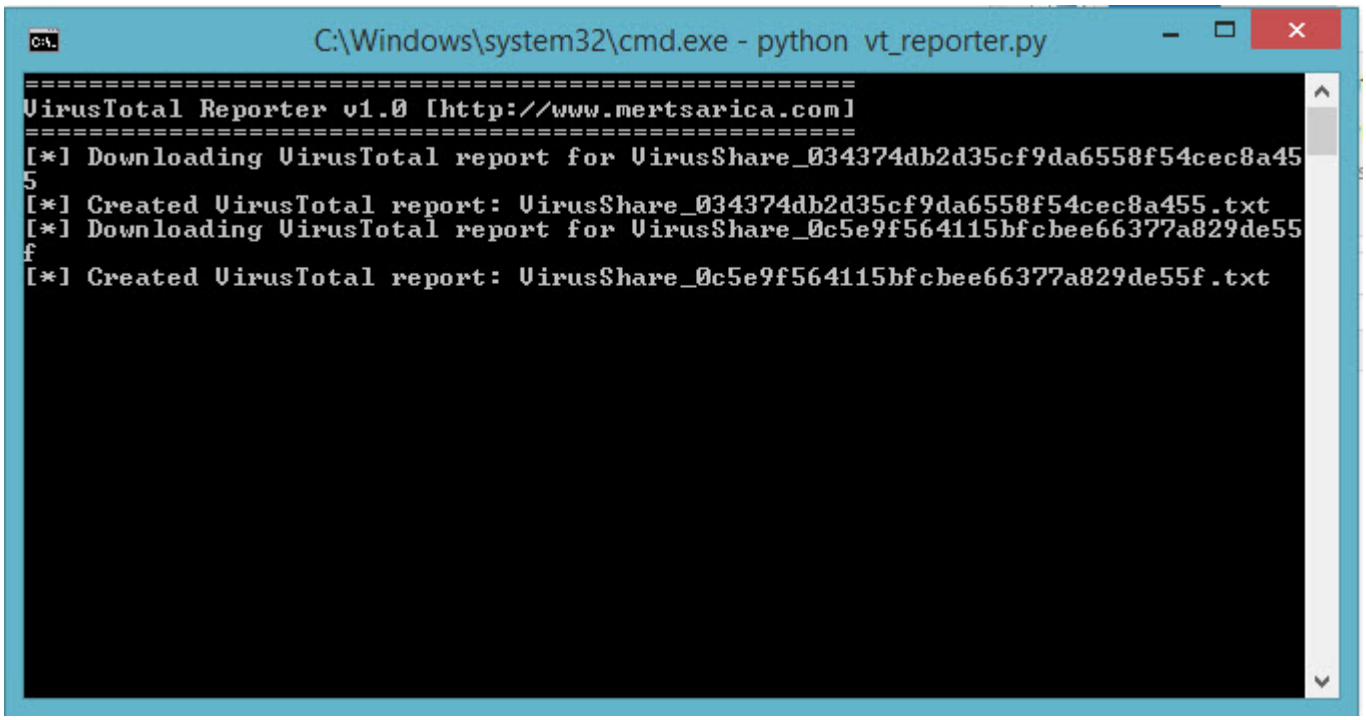


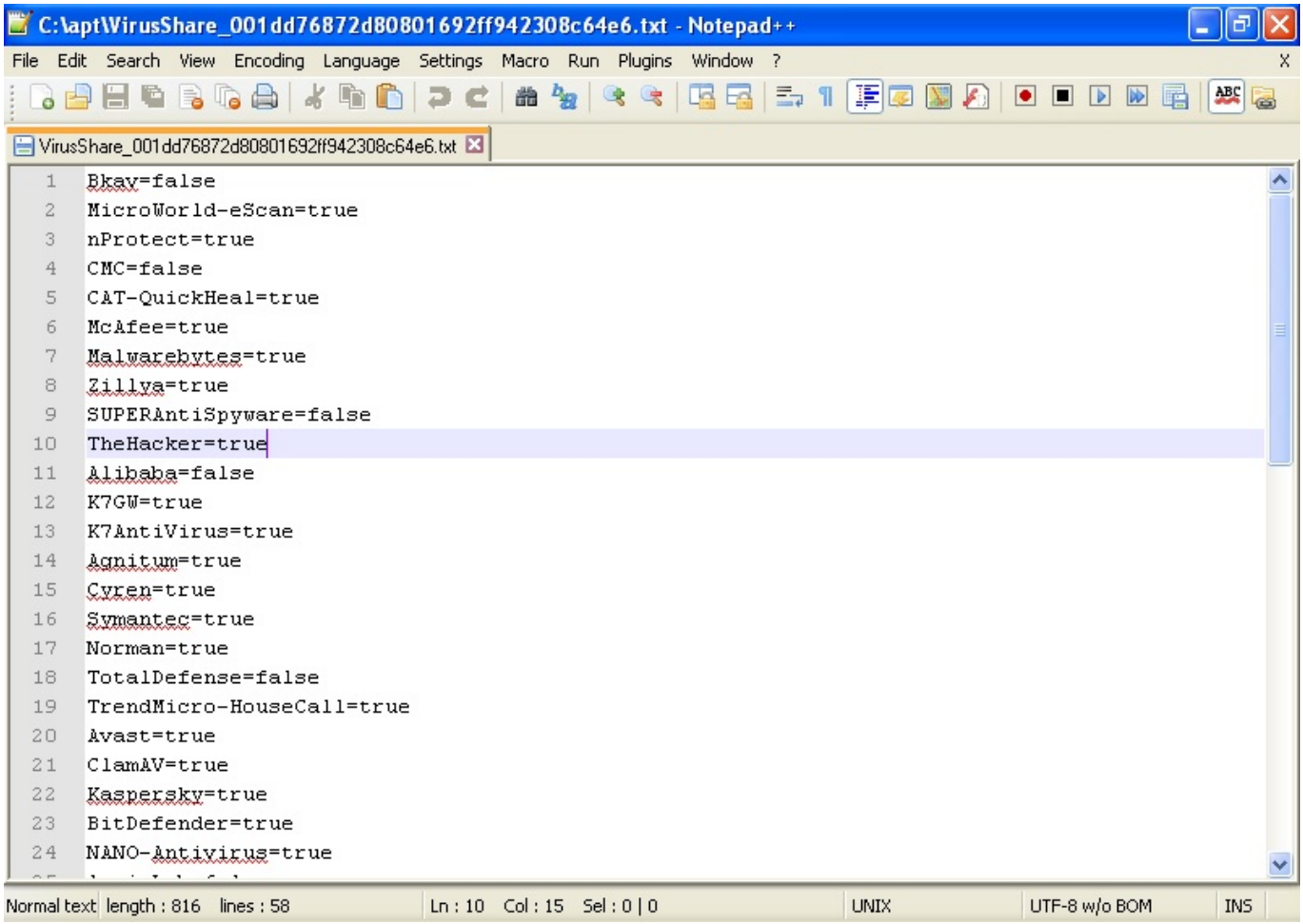
Tabii 293 tane zararlı yazılımı teker teker VirusTotal sitesine yüklemek ve her birinin sonucuna bakmak pratikte mümkün olamayacağı için hem merakımı gidermek hem de benzer nedenlerden ötürü bu tür bir çalışmaya ihtiyaç duyanları da düşünerek Python ile iki tane araç hazırlamaya karar verdim.

Hazırladığım ilk araç olan Virustotal Mass Uploader (vt_mass_uploader.py) aracı ile elinizde bulunan birden fazla zararlı yazılımı VirusTotal sitesine yükleyebiliyorsunuz. Bunun için aracın bulunduğu klasörde malwares adında bir klasör oluşturmanız ve yüklenmesini istediğiniz zararlı yazılımları bu klasöre kopyalamanız yeterli oluyor.

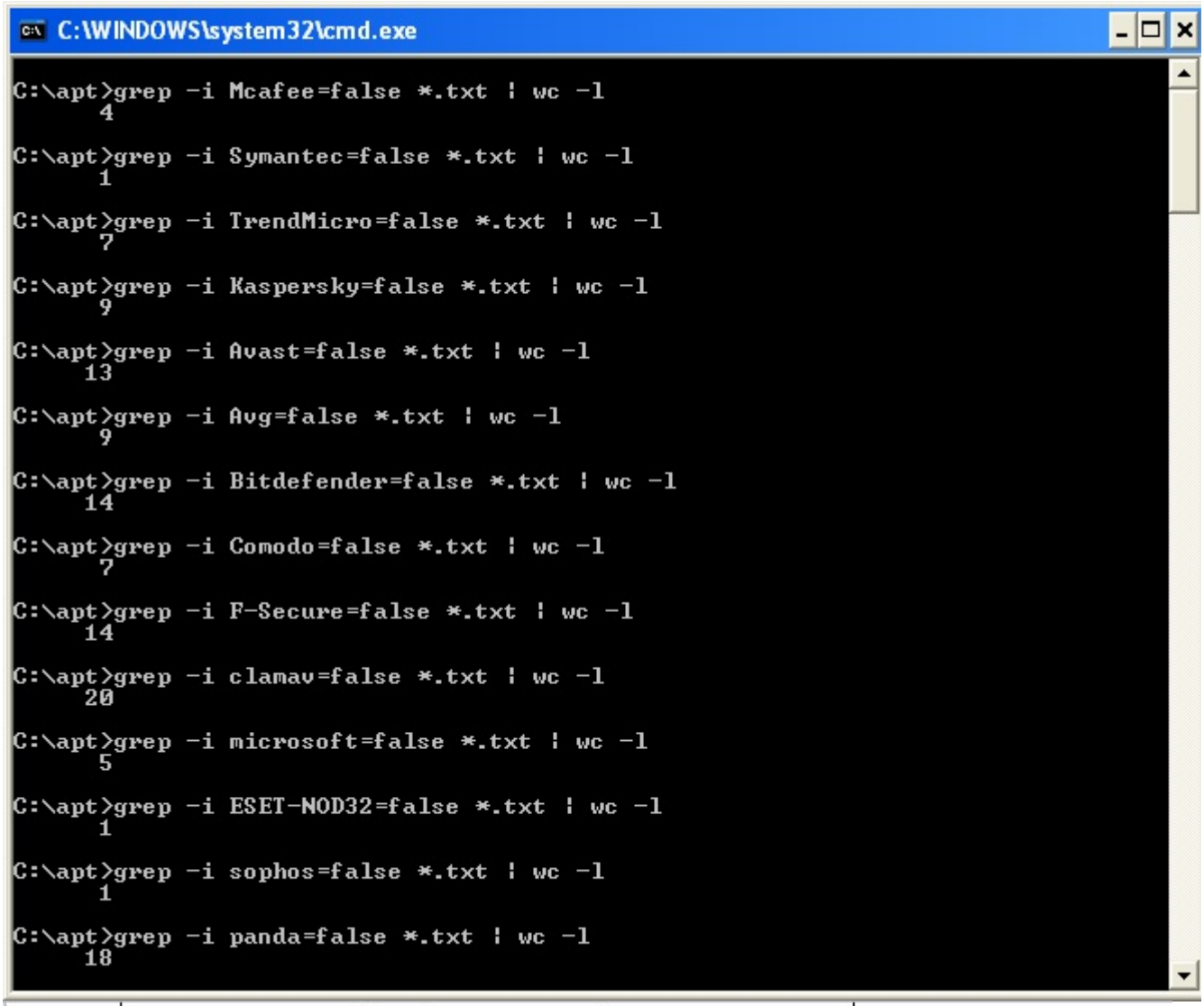


Hazırladığım ikinci araç olan VirusTotal Reporter (vt_reporter.py) aracı ise VirusTotal Mass Uploader aracının çıktısı olan vt_report.txt dosyasını okuyarak VirusTotal'a yüklenen zararlı yazılımların raporlarını zararlı yazılımın adı.txt olarak diske yazmaktadır. Bu dosyalardan hangi antivirüs yazılımının ilgili zararlı yazılımı tespit edip edemediği görülebilmektedir.





Mandiant'ın 2013 yılında yayınlanan APT raporunda yer alan 293 zararlı yazılımı yukarıdaki araçlar ile VirusTotal'a yükleyip, popüler antivirüs yazılımlarının hangilerini tespit edip edemediğine baktığımda ortaya çıkan tablo beni biraz şaşırttı.



Mandiant's APT-1 Malwares		
Vendor	**Failed Detection Rate (x/293)***	**Percentage**
Symantec	1	99,66%
ESET-NOD32	1	99,66%
Sophos	1	99,66%
Mcafee	4	98,63%
Microsoft	5	98,29%
TrendMicro	7	97,61%
Comodo	7	97,61%
Kaspersky	9	96,93%
AVG	9	96,93%
Avast	13	95,56%
F-Secure	14	95,22%
BitDefender	14	95,22%
Panda	18	93,86%
ClamAV	20	93,17%
* Lower is better at detection		

Mandiant's APT1 Report (18.02.2013): http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Digital Appendix & Indicators: http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip

2 sene önce yayınlanan bir rapora rağmen antivirüs yazılımlarından bazılarının 25.05.2015 tarihi itibariyle hala bu zararlı yazılımları tespit edemediği açıkça görülüyor. Örneğin Clamav antivirüs yazılımı 293 tane zararlı yazılımdan 20 tanesini, Panda ise 18 tanesini, Bitdefender ve F-Secure ise 14 tanesini tespit edemiyor. Tabii bu zararlı yazılımlardan bir tanesinin ip ve port taramak için kullanılan Angry IP Scanner olduğunu söylemem lazım dolayısıyla 293/293 tespit eden bir antivirüs yazılımı olsaydı bu defa da çok doğru bir sonuç olmayacaktı. Bu örneklem sonucunda ortaya çıkan tabloya göre Symantec, ESET-NOD32 ve Sophos'un diğer antivirüs yazılımlarına göre imza ile bilinen tehditleri tespit etmede daha başarılı olduğunu söylersek yanlış olmayacaktır.

Yaptığım bu çalışmanın antivirüs yazılımlarını değerlendirmek isteyenlere, hangi antivirüs yazılımını kullanmalıyım sorusuna yanıt arayanlara yol göstereceğini ümit ederek, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.