VAD (Vbulletin Attachment Downloader)

written by Mert SARICA | 17 September 2010

Geçtiğimiz Temmuz ayında Stuxnet adındaki zararlı yazılım (malware) .lnk ve .pif kısayol dosyalarındaki güvenlik açığından faydalanarak sistemler arasında yayılması nedeniyle bir anda dünyanın gündemine oturdu. Zararlı yazılımın başarıya ulaşmasındaki en büyük etkenlerden biri 0day güvenlik açığı istismar ediyor olmasıydı fakat geçtiğimiz günlerde Symantec tarafından yayınlanan bir yazı analizlerin halen devam ettiğini ve bu analizler neticesinde zararlı yazılımın aslında 1 değil tamı tamına 4 adet 0day güvenlik açığını istismar ettiğini ortaya koyuyordu.

Görünen o ki art niyetli kişiler her geçen gün çıtayı bir seviye daha yükseltiyor, güvenlik uzmanları için işler biraz daha zorlaşıyor, analizler biraz daha karmaşık bir hal alıyor ve bu nedenle bu tür saldırılara ve olay sonrası incelemelere hazırlıklı olmak için ne kadar çok zararlı yazılım incelenirse gerçek bir saldırıya o kadar hazırlıklı olunuyor.

Bu nedenden ötürü yerli ve yabancı hacking forumlarını zaman zaman gezerek yayınlanan zararlı yazılımları incelemeye gayret ediyorum. Geçtiğimiz günlerde yine bir hacking forumunu gezerken dikkatimi daha önce dikkat etmediğim bir ibare çekti, “http://novirusthanks.org dışındaki tarama sitelerinde taratmayın diyoruz taratıyorsunuz! 100 kere söylenmesine karşın!”

Zararlı yazılım oluşturan art niyetli kişilerin en çok çekindikleri konu yazılımlarının gerçek zamanlı virüs taraması gerçekleştiren web siteleri (virustotal, novirusthanks vb.) üzerinde taratılmalarıdır. Nedeni ise bu siteler üzerinde taratılan tüm yazılımlar antivirüs üreticilerine gönderilmektedir. Örnek olarak Virustotal ve Novirusthanks sitelerinin kullanım şartlarına bakacak olursak bunu açıkça ifade ettiklerini görebiliyoruz.

http://www.novirusthanks.org/terms.php

We may store (temporarily) the files that you send in our online-virus-scanner and the files that you submitted can be shared with Anti-Malware and Security Companies that participate in our project generally if the file is detected by at least one Antivirus Software that is present in the list of

the engines.

http://www.virustotal.com/terms.html
Collection and use of submitted files and personal information
When you submit a file to VirusTotal for scanning, we may store it and share it with the anti-malware and security industry (normally the companies that participate in VirusTotal receive the samples that their engines do not detect and are catalogued as malware by at least one other engine). The samples can be analysed by automatic tools and security analysts to detect malicious code and to improve antivirus engines.

Teker teker hacking forumlarını gezmek ve zararlı yazılımları indirmek vakit alan bir iş olduğu için geçtiğimiz günlerde Python ile bu işi otomatikleştirecek ufak bir program hazırlamaya karar verdim. Takip ettiğim forumların çoğu VBulletin forum kullandığı, eklenti modülü aktif olduğu ve ayrıca Vbulletin'de eklentileri listeleyen ayrı bir sayfa olduğu için hazırlayacağım programa forum adresinin belirtilmesi durumunda kullanıcı adı ve şifre ile giriş yapması, eklenti sayfalarını teker teker gezmesi ve exe, zip, rar uzantılarına sahip eklentileri tespit etmesi durumunda diske kaydetmesi yeterli olacaktı fakat buna ilaveten opsiyonel olarak birde virus tarama sitelerinden bir tanesine bu eklentileri yüklemesi ve sonucu kayıt altına almasının herkes için çok daha iyi olacağı düşüncesiyle bunların tamamını gerçekleştiren bir program hazırlamaya başladım.

Saatlerce programın üzerinde çalıştıktan sonra tamamlanmasına yakın bir zaman kala Python'da yer alan cookielib modülünün isteklerimi karşılamadığını farkettim. Urllib ile foruma belirttiğim kullanıcı adı ve şifre ile giriş yaptıktan sonra sonra çerezin (cookie) bir türlü bir sonraki istekte gönderilmediğini farkettim ve üzerine bir yandan kafa yorar bir yandan araştırma yaparken Mechanize adındaki o müthiş modülü keşfettim.

Mechanize modülü, bir web sitesi üzerinde urllib modülü ile kolay olmayan fakat internet tarayıcısı (web browser) ile oldukça kolay olan işlemleri (örneğin form doldurma, bağlantıları (links) ayrıştırmaya) gerçekleştirmenizi sağlayan oldukça ama oldukça faydalı bir modül.

Hazırlamış olduğum programı sil baştan mechanize desteği ile tekrar hazırladıktan sonra ortaya vad (vbulletin attachment downloader) programı çıkıverdi. VAD'ın kullanımı hazırlamış olduğum diğer tüm programlarımda olduğu gibi oldukça basit.

Eğer hedef forum, eklenti indirebilmeniz için kullanıcı adı ve şifre ile kimlik doğrulama gerçekleştirmenizi istiyorsa yapmanız gereken programa -u ile kullanıcı adını, -p ile şifreyi belirtmek olacaktır. Eğer diske kayıt edilen her eklentinin ayrıca Novirusthanks sitesinde taratılmasını istiyorsanız bu durumda programa -s parametresini belirtmeniz yeterli olacaktır.

Örnek olarak eğer site kimlik doğrulamaya ihtiyaç duymuyorsa ve diske kayıt edilen tüm eklentileri taratmak istiyorsanız çalıştırmanız gereken komut:
vad.py -h http://www.forum.com -s

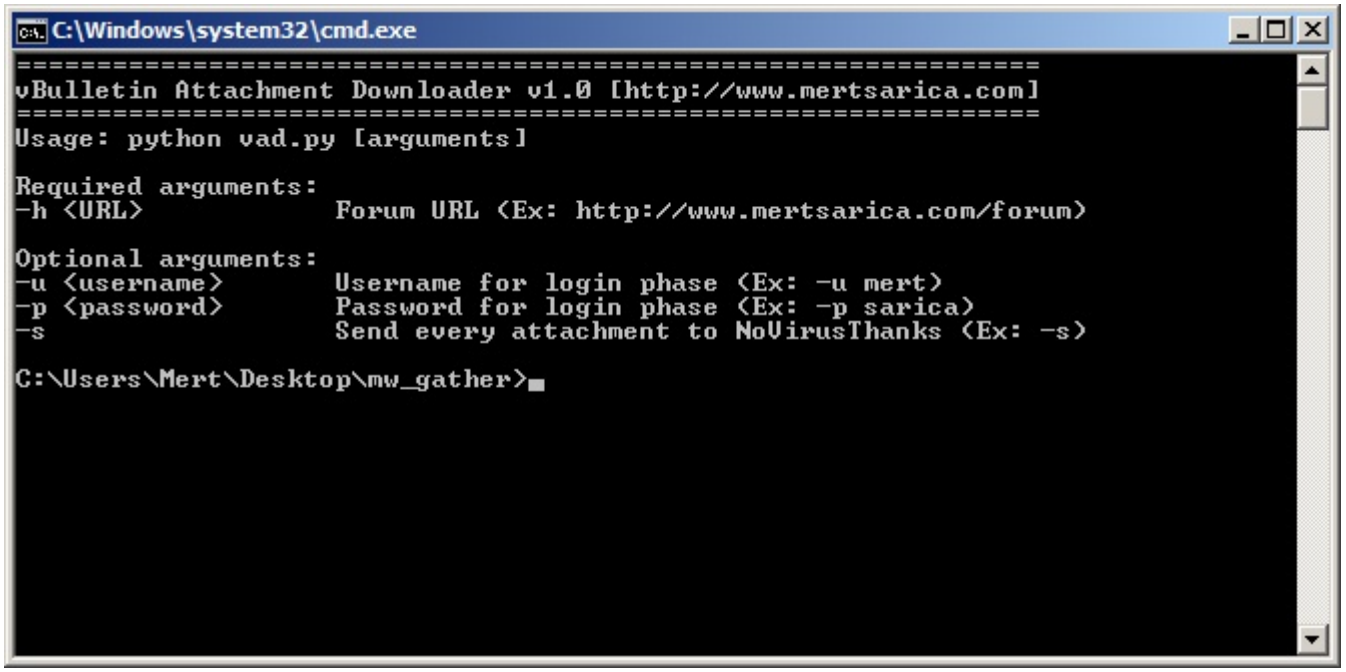
Eğer site kimlik doğrulamaya ihtiyaç duyuyorsa çalıştırmanız gereken komut ise:
vad.py -h http://www.forum.com -u kullanici -p şifre -s

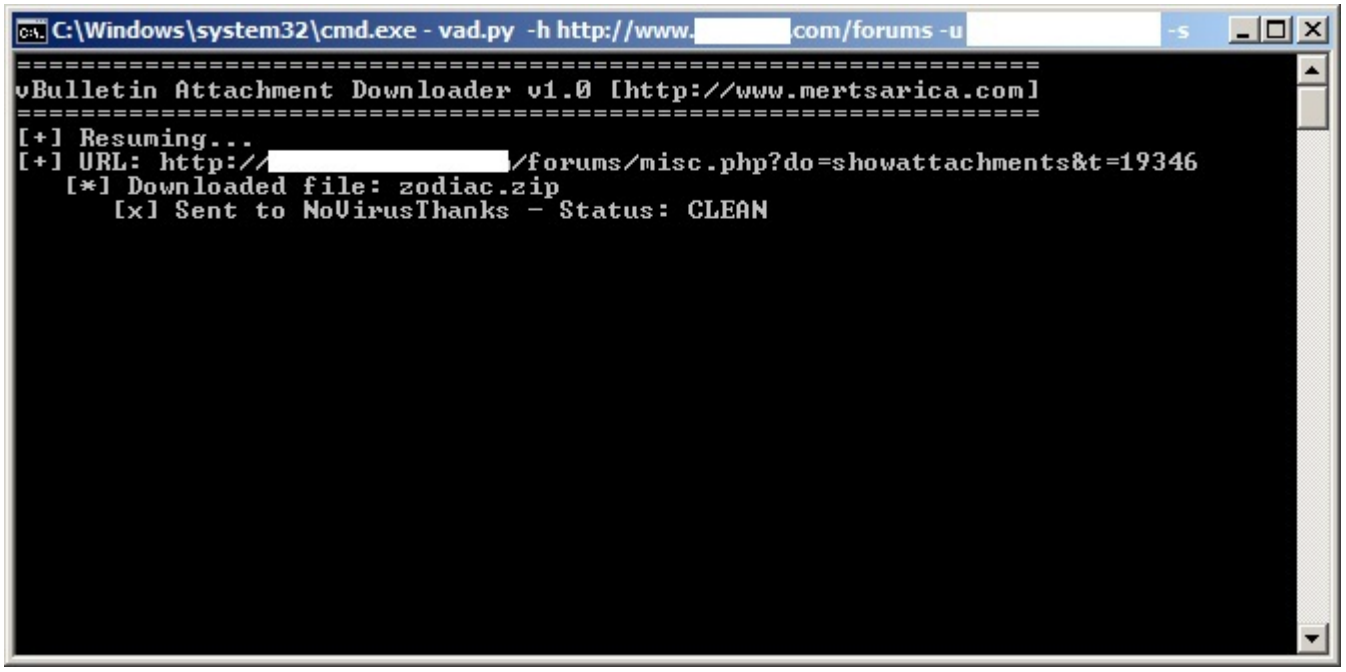
Programda ayrıca kaldığı yerden devam etme özelliğide bulunmaktadır bu sayede sadece yeni eklenen eklentileri indirmek için tüm eklentilerin en baştan yüklenmesine gerek kalmayacaktır. Virüs tarama sonuçları scan.txt adı altında disk üzerine kayıt edilmektedir.

Programı hazırlamamdaki amaç hem kendi işimi görmesi hemde bu siteler üzerinden yayılan ve insanları mağdur edebilecek potansiyel zararlı yazılımların antivirüs üreticileri tarafından kolayca tanınmasını sağlamaktı, umarım hem güvenlik uzmanları hem de Python severler için faydalı bir program olmuştur.

Programın kaynak koduna buradan ulaşabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim.


C:\Windows\system32\cmd.exe
vBulletin Attachment Downloader v1.0 [http://www.mertsarica.com]
Usage: python vad.py [arguments]
Required arguments:
-h <URL> Forum URL (Ex: http://www.mertsarica.com/forum)
Optional arguments:
-u <username> Username for login phase (Ex: -u mert)
-p <password> Password for login phase (Ex: -p sarica)
-s Send every attachment to NoVirusThanks (Ex: -s)
C:\Users\Mert\Desktop\mw_gather>


C:\Windows\system32\cmd.exe - vad.py -h http://www. com/forums -u -s
vBulletin Attachment Downloader v1.0 [http://www.mertsarica.com]
[+] Resuming...
[+] URL: http:// /forums/misc.php?do=showattachments&t=19346
[*] Downloaded file: zodiac.zip
[x] Sent to NoVirusThanks - Status: CLEAN