Birdirbir

written by Mert SARICA | 4 Ağustos, 2012

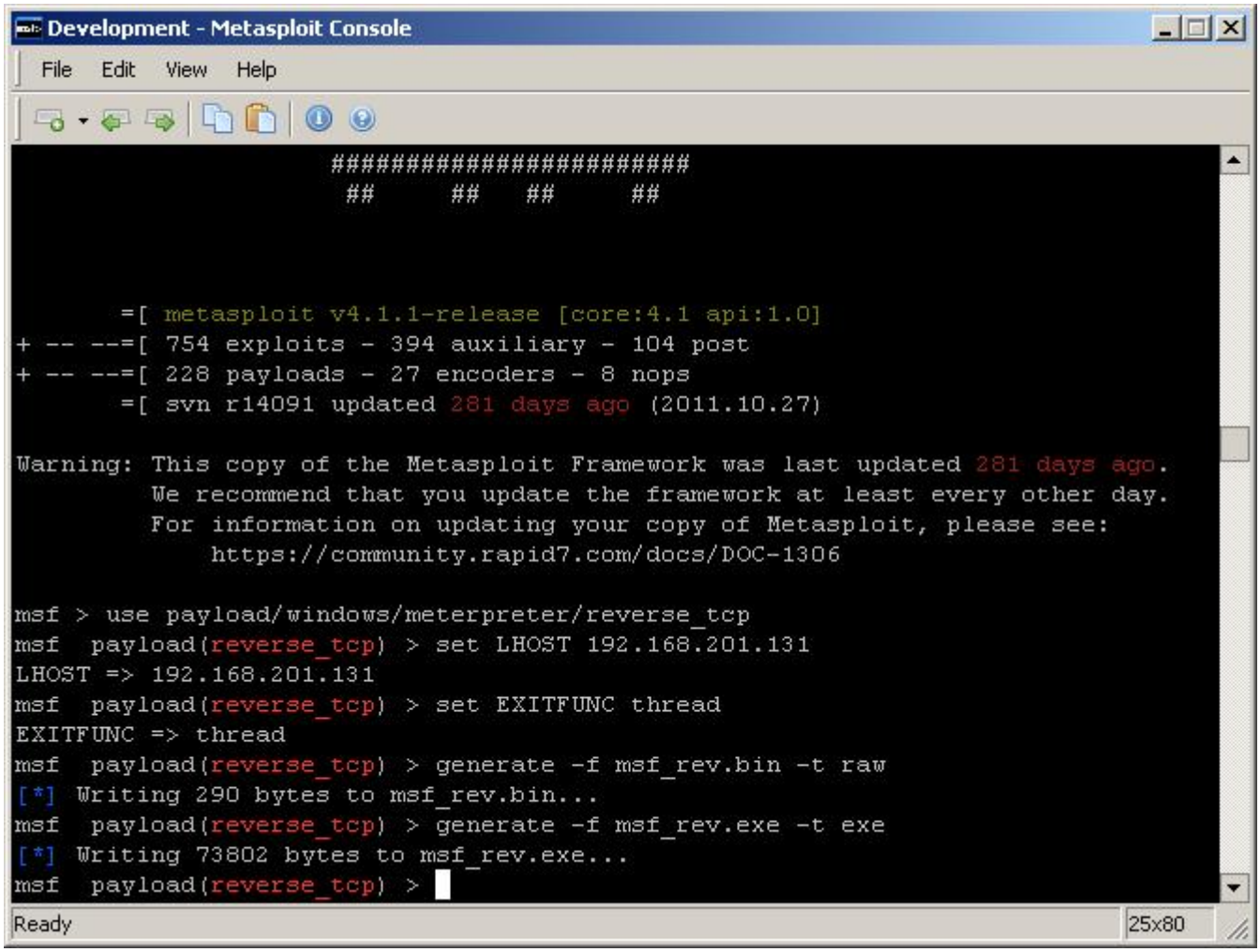
Penetrasyon (sızma) testi gerçekleştirenlerin çoğu hem sunduğu sayısız imkanlar, hem açık kaynak kodlu olması ve hem de ücetsiz olması nedeniyle Metasploit istismar aracını kullanmayı tercih etmektedirler. Metasploit'in en beğenilen özelliklerinden biri şüphesiz barındırmış olduğu Meterpreter aracıdır. 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'ın bu denli güçlü, sinsi olması, Antivirüs üreticilerinin de gözünden kaçmamış ve çoğu üretici Meterpreter'ın 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'ın Antivirüs yazılımları tarafından tespit edilmemesi büyük önem arz etmiştir ve penetrasyon testlerinde çeşitli kodlama (encode) yöntemleri ile oluşturulan Meterpreter'ın 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 ettiğin için alarm üretebilmektedir.

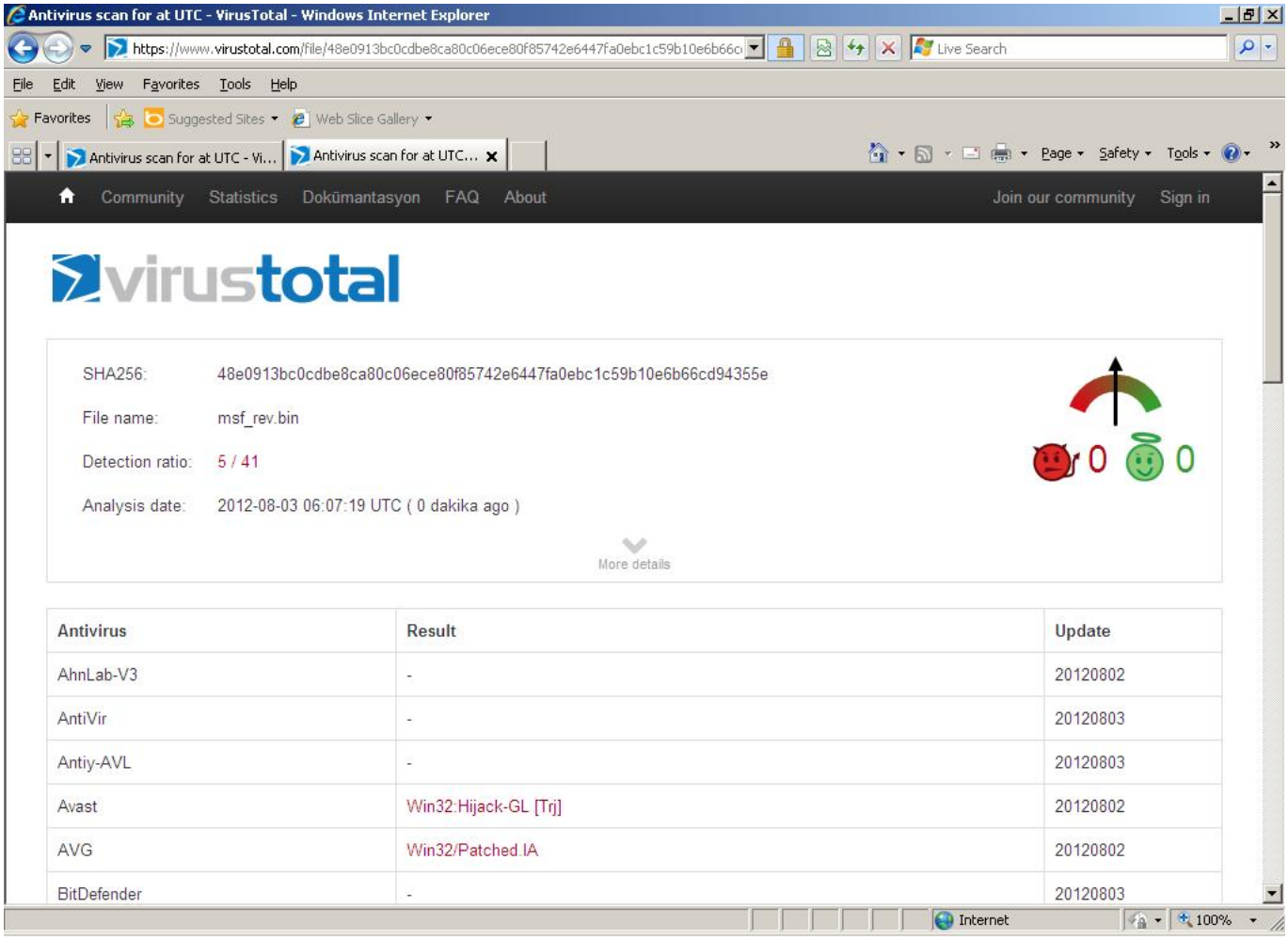
Meterpreter, hem kabuk kodunu (shellcode) içeren yürütülebilir program (executable) olarak hem de istismar aracının (exploit) ham (raw) kabuk kodu olarak üretilebilmekte ve kullanabilmektedir. Tek fark, ham olarak üretilmesi (generate -t raw) durumunda bunu çalıştıracak ilave bir programa ihtiyaç duymaktadır. 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 internetten indirdiği ham kodu (örnek: meterpreter reverse tcp kodu) indirip hedef işleme (process) enjekte (code injection) eden Code Injection gibi bir araç, Meterpreter'ın Metasploit ile haberleşmesini herhangi bir kodlama (encode) yöntemi kullanmadan sağlayabilmektedir.

Teoride güzel de pratikte nasıl oluyor diye soracak olursanız;

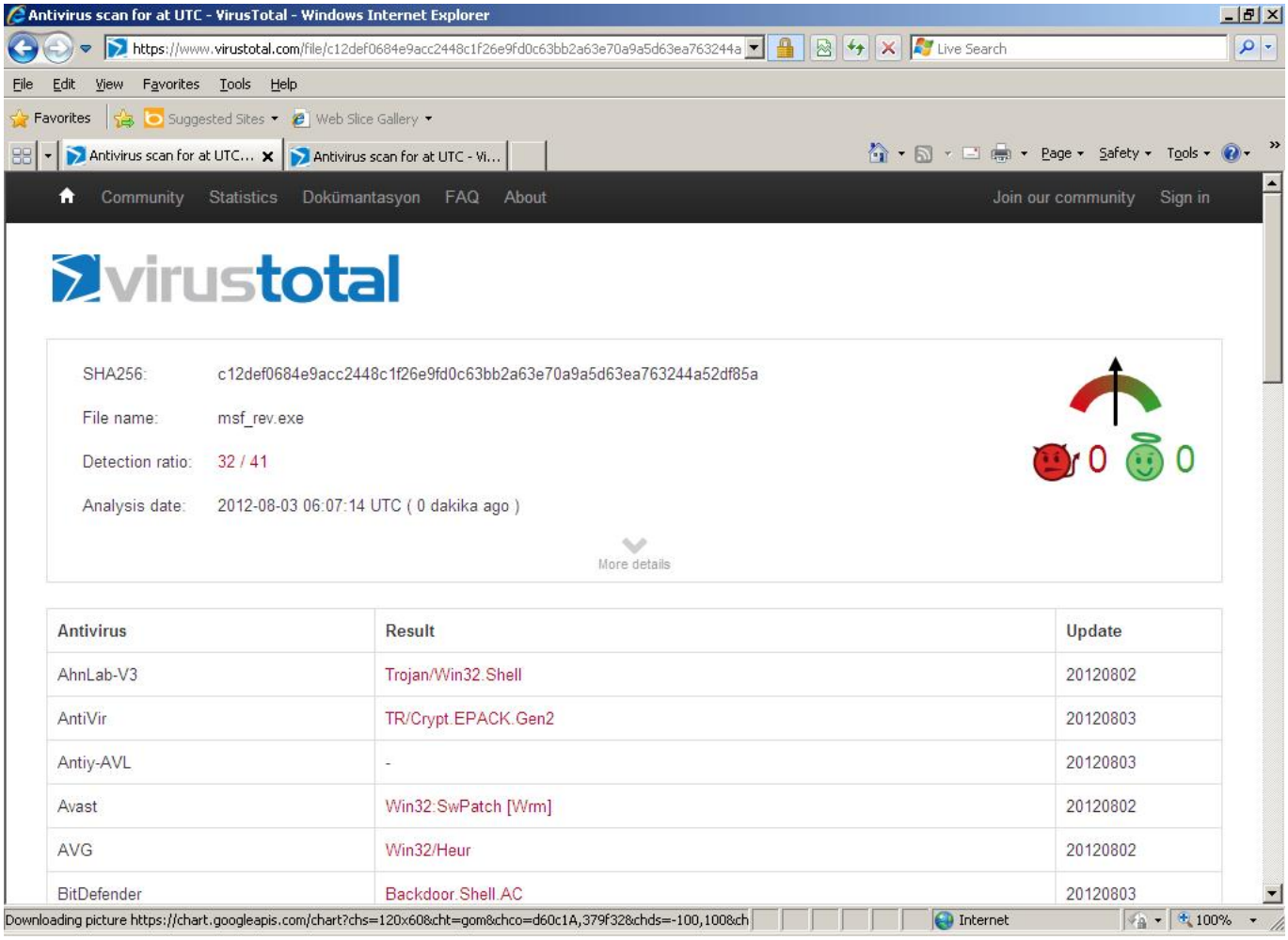
Öncelikle Metasploit ile hem ham hem de yürütülebilir program olarak Meterpreter oluşturalım.



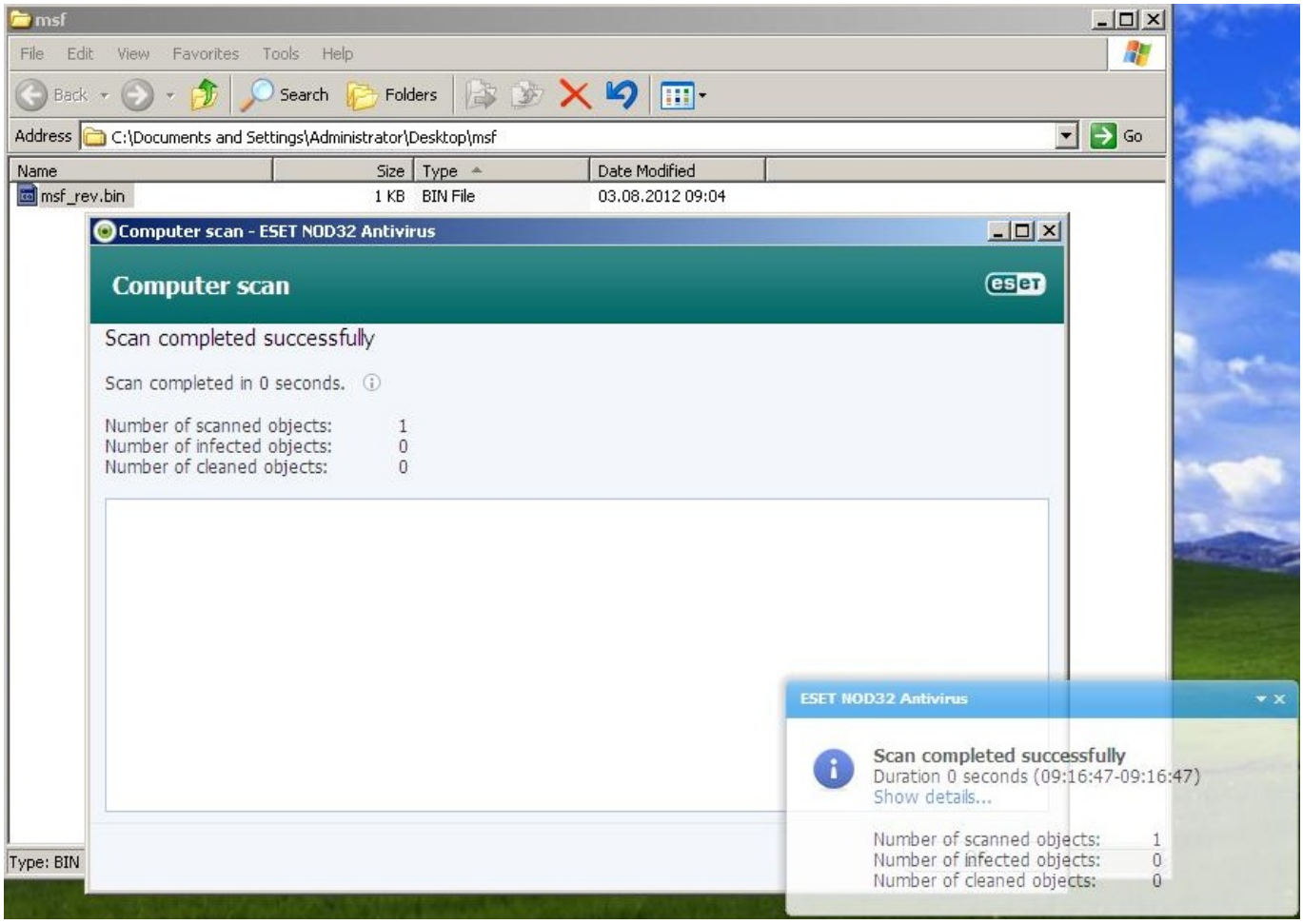
Ardından ham halini VirusTotal sitesine yükleyelim. (Rapora buradan ulaşabilirsiniz.) 41 Antivirüs yazılımından sadece 5 tanesi (AVG, Avast, Symantec, Mcafee GW Edition, GData) kodlanmamış (encode) Meterpreter'ı tespit edebilmektedir.

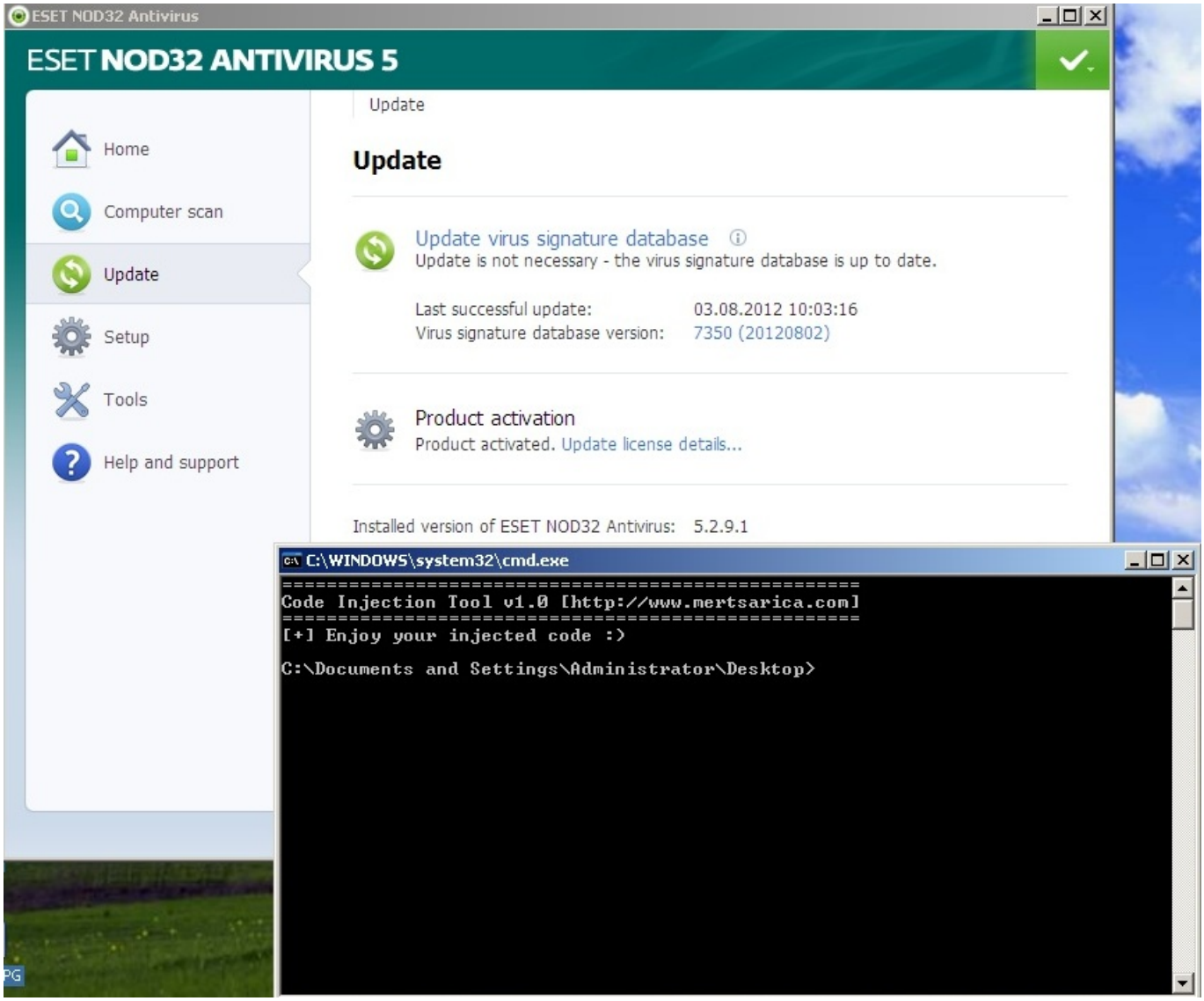


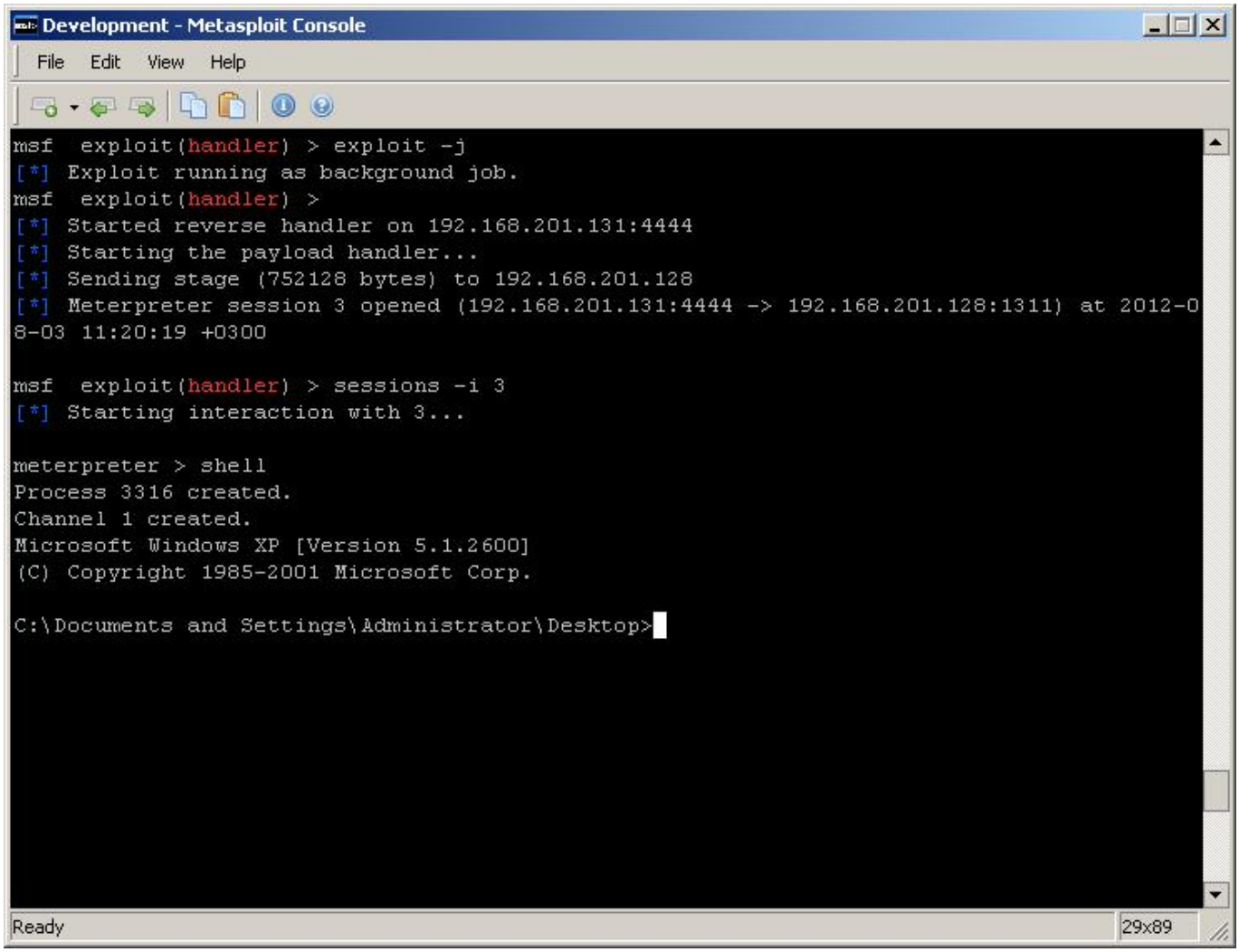
Ardından yürütülebilir program (executable) halini VirusTotal sitesine yükleyelim. (Rapora buradan ulaşabilirsiniz. 41 Antivirüs yazılımından sadece 32 tanesi kodlanmamış (encode) Meterpreter'ı tespit edebilmektedir.



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
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\msf
Go
Name Size Type Date Modified
msf_rev.bin 1 KB BIN File 03.08.2012 09:04
Computer scan - ESET NOD32 Antivirus
Computer scan
eset
Scan completed successfully
Scan completed in 0 seconds.
Number of scanned objects: 1
Number of infected objects: 0
Number of cleaned objects: 0
Type: BIN
ESET NOD32 Antivirus
Scan completed successfully
Duration 0 seconds (09:16:47-09:16:47)
Show details...
Number of scanned objects: 1
Number of infected objects: 0
Number of cleaned objects: 0


ESET NOD32 Antivirus
ESET NOD32 ANTIVIRUS 5
Home
Computer scan
Update
Setup
Tools
Help and support
Update
Update
Update virus signature database
Update is not necessary - the virus signature database is up to date.
Last successful update: 03.08.2012 10:03:16
Virus signature database version: 7350 (20120802)
Product activation
Product activated. Update license details...
Installed version of ESET NOD32 Antivirus: 5.2.9.1
C:\WINDOWS\system32\cmd.exe
Code Injection Tool v1.0 [http://www.mertsarica.com]
[+] Enjoy your injected code :)
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…