Dll injection

DFIRCON APT Malware Analysis(PART2)

დღეს განახებთ თუ როგორ იყენებენ კრმინალები dll injection-ის ტექნიკას

გამოყენებული ხელსაწყოები: Strings/Volatility

ეს ტექნიკა გამოიყენება ანტივირუსების გვერდის ავლისთვის, დღეს-დღეობით ყველაზე გავრცელებული ტექნიკა არის, რასაც ვირუსის ავტორები იყენებენ

რა არის DLL ინჟექშენი?

ძირითადათ ამ ტექნიკას შეუძლია ორი რამ: შეუძლია გაეშვას მემორიში ძალიან მარტივად ან გამოიძახოს სხვა პროცესი,
ინექციისთვის იყენებს ყველასთვის კარგად ნაცნობ აპებს, ჩვენს შემთხვევაში ვირუსმა გამოიძახა პროცესი და ამის შემდეგ მოხდა Dll Injection-ი.Dll-ის ჩაინჯექტება ხდება ორნაირად ინჟექშენი Windows API-ის გამოყენებით, რომელიც იყენებს განსხვავებულ ფუნქციებს, როგორიცაა: VirtualAllocEx(), ReadProcessMemory(),WriteProcessMemory(), რაც შეეხება VirtualAllocEx() ფუნქციას მხოლოდ NT-ზე დაფუძნებულ პლატფორმებზე მუშაობს. ამის გარდა არის კიდე სხვა გზაც რისი გამოყენებით შესაძლებელია ინჟექშენის გაკეთებას Debugging API-ის გამოყენებით. მაშ ასე გადავიდეთ ტექნიკურ ანალიზზე.

```
ch3k1 ~ # python /usr/local/bin/vol.py -f /home/ch3k1/Desktop/sans/APT.img --profile=WinXPSP2x86 pslist | grep iexplore
Volatility Foundation Volatility Framework 2.3.1
0x81dbdda0 iexplore.exe           796    884      8      152      0      0 2009-05-05 19:28:28 UTC+0000
ch3k1 ~ #
```

მოკლედ რა მოხდა ჩვენს მანქანაზე, მომხმარებელი, რომელიც ინტერნეტ ექსპლორერით შედიოდა ინტერნეტში მისი დახმარებით მოხდა მანქანის დაინფიცირება, პირველ რიგში გავიგოთ ქონექშენები რა იპ_ებზე დაფიქსირდა.

```
---------- ------------------------ ------------------------ ---
0x0205ece0 192.168.157.10:1050      222.128.1.2:443          1672
0x020611f8 192.168.157.10:1053      218.85.133.23:89         796
0x032c01f8 192.168.157.10:1053      218.85.133.23:89         796
0x0337dce0 192.168.157.10:1050      222.128.1.2:443          1672
0x08a4ace0 192.168.157.10:1050      222.128.1.2:443          1672
0x18200ce0 192.168.157.10:1050      222.128.1.2:443          1672
ch3k1 ~ #
```

თუ დავაკვირდებით პროცესის პიდ-ის ნომერს და ერთ-ერთი ქონექშენის პიდ-ს დავინახავთ რომ იპ მისამართს
იპ:218.85.133.23
პიდ: 796
მივანდოთ ეს იპ მისამართი გუგლს იქნება რამე იცოდეს: მოკლედ ამ იპ მისამართს კარგი რეპუტაცია ნამდვილად არ აქვს

Recent reports on same IP/ASN/Domain

Last 6 reports on IP: 218.85.133.23

Date	Alerts / IDS	URL	IP
2013-12-12 20:19:57	0 / 0	http://218.85.133.23:89/index.asp?503000010000	218.85.133.23
2013-12-12 15:20:27	0 / 0	http://218.85.133.23	218.85.133.23
2013-12-09 22:27:08	0 / 0	http://218.85.133.23:89	218.85.133.23
2013-12-06 03:41:54	0 / 0	http://218.85.133.23	218.85.133.23
2013-12-05 02:01:17	0 / 0	http://218.85.133.23	218.85.133.23
2013-09-24 20:34:33	0 / 0	http://xorone.3322.org	218.85.133.23

Last 6 reports on ASN: AS4134 Chinanet

Date	Alerts / IDS	URL	IP
2012-10-16 19:29:10	0 / 1	http://www.cz89.com/read_707756.htm	183.60.136.56
2012-10-17 06:23:45	0 / 2	http://ppg.gdl.netease.com/ppg_full.exe	122.226.169.181
2012-10-17 06:24:59	0 / 1	http://zhy520.f3322.org:8081/ie.html	218.95.29.3
2012-10-17 06:48:12	0 / 2	http://www.aohaha.com/7capp/images/tips.gif	59.57.15.215
2012-10-17 12:52:25	0 / 1	http://zz.xlkj518.com/download/hosts.txt	218.64.254.36
2012-10-17 13:38:20	0 / 1	http://www.cz89.com/read_698153.htm	183.60.136.45

საიტზე შესვლისას ჩვენი მანქანა დაინფიცირდა ვირუსულმა კოდმა DLL ინჟექშენი გააკეთა explorer.exe მაშ ასე დაახლოებით 1 საათი ვდამპავდი ყველა DLL-ს რასაც ეს პროცესი იყენებდა და როგორც იქნა ვნახე ცუდი DLL-ი

```
0x75f70000     0xa000         0x1 C:\WINDOWS\System32\davclnt.dll
0x7e720000    0xb0000         0x1 C:\WINDOWS\system32\SXS.DLL
0x75cf0000    0x91000         0x1 C:\WINDOWS\system32\MLANG.dll
0x00970000     0xc000         0x1 C:\WINDOWS\system32\irykmmww.dll
```

DLL-ის სახელია irykmmww.dll, ამის შემდეგ გადავწყვიტე ფაილი ამეტვირთა ვირუსტოტალზე:

virustotal

SHA256: fe9fbcc2cf6c6666d2cdd17b7665ce66fd3ba2ceec381cf4ea09f2a7a3387749
File name: module.1672.1fa71a8.970000.dll
Detection ratio: 29 / 47
Analysis date: 2013-12-15 14:25:32 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Graftor.37219	20131211
Agnitum		20131214
AhnLab-V3	Backdoor/Win32.PcClient	20131215
AntiVir	TR/Spy.Gen	20131215
Antiy-AVL		20131210
Avast	Win32:PcClient-GC [Trj]	20131215
AVG	BackDoor.Generic17.CCRL	20131215

47-დი ანტივირუსიდან 29-ა ანტივირუსმა შეძლო მისი დაჭერა

შევამოწმოთ პროცესები ქონექშენები და დავაკვირდეთ პიდ-ის ნომერს:

```
ch3k1 ~ # python /usr/local/bin/vol.py -f /home/ch3k1/Desktop/sans/APT.img --profile=WinXPSP2x86 pstree | grep explorer.exe
Volatility Foundation Volatility Framework 2.3.1
 0x81da71a8:explorer.exe                      1672   1624     15    586 2009-04-16 16:10:10 UTC+0000
ch3k1 ~ # python /usr/local/bin/vol.py -f /home/ch3k1/Desktop/sans/APT.img --profile=WinXPSP2x86 connscan | grep 1672
Volatility Foundation Volatility Framework 2.3.1
0x0205ece0 192.168.157.10:1050       222.128.1.2:443          1672
0x0337dce0 192.168.157.10:1050       222.128.1.2:443          1672
0x08a4ace0 192.168.157.10:1050       222.128.1.2:443          1672
0x18200ce0 192.168.157.10:1050       222.128.1.2:443          1672
ch3k1 ~ #
```

explorer.exe პროცესი ქონექშენს აკეთებდა Remote ჰოსტთან 222.128.1.2 კომუნიკაციის პორტი 443 ანუ ქონექშენი დაშიფრული იყო

```
AppData
V%X_
B~k!C~
|!WE~&
exploder.exe
admin
222.128.1.2
pork_bun
StubPath
SOFTWARE\Classes\http\shell\open\command
explorer.exe
Software\Microsoft\Active Setup\Installed Components\
C:\WINDOWS\system32\exploder.exe
C:\WINDOWS\system32\exploder.exe
```

ფუნქციები რომელსაც DLL-ი იყენებდა:

```
KERNEL32.dll
GetDesktopWindow
GetWindowTextA
wsprintfA
GetActiveWindow
CallNextHookEx
GetFocus
ToAscii
GetKeyboardState
SetWindowsHookExA
SetThreadDesktop
OpenDesktopA
SetProcessWindowStation
OpenWindowStationA
GetThreadDesktop
GetProcessWindowStation
IsCharAlphaNumericA
EnumWindows
SendMessageA
GetWindowLongA
GetClassNameA
EnumChildWindows
GetWindowThreadProcessId
```

ფაილი ასევე კეილოგერის ფუნქციის გამოყენებით იპარავდა პაროლებს სხვადასხვა მეილ კლიენტებიდან ასევე icq-დან

```
msmsgs.exe
icqlite.exe
icq.exe
QQ.exe
Foxmail.exe
msimn.exe
OutLook.exe
IExplore.exe
Name:
Time :
PassWD: [
PASSWORD
TEXT
POP3 User Name
\Software\Microsoft\Internet Account Manager\Accounts\00000001
Identities
POP3 Password2
POP3 Server
pop3 User's Name
HTTPMail Password2
Hotmail
HTTPMail User Name
Software\Microsoft\Internet Account Manager\Accounts\
Software\Microsoft\Internet Account Manager\Accounts
AutoComplete Passwords
```

მოკლედ იმედია მოგეწონებათ, კეთილი სურვილებით და დაცული კომპიუტერებით

მადლობას მოვახსენებ სანს, ასევე Volatility-ის შემქნელებს, ასევე explot-db.com-ს

Blog: *http://securitylabge.blogspot.com/*