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,

ინექცისთვის 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.

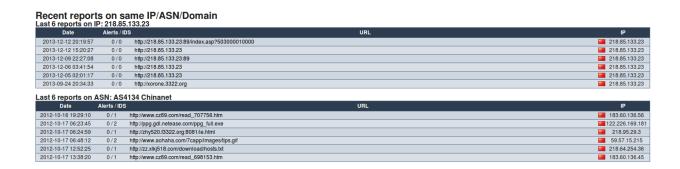
```
0x0205ece0 192.168.157.10:1050
                                      222.128.1.2:443
                                                                  1672
0x020611f8 192.168.157.10:1053
                                      218.85.133.23:89
                                                                  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
```

თუ დავაკვირდებით პროცესის პიდ-ის ნომერს და ერთ-ერთი ქონექშენის პიდ-ს დავინახავთ რომ იპ მისამართს

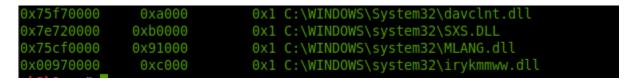
o3:218.85.133.23

პიდ: 796

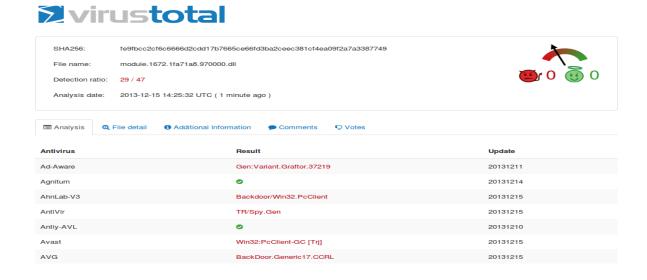
მივანდოთ ეს იპ მისამართი გუგლს იქნება რამე იცოდეს: მოკლედ ამ იპ მისამართს კარგი რეპუტაცია ნამდვილად არ აქვს



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



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



47-დი ანტივირუსიდან 29-ა ანტივირუსმა შეძლო მისი დაჭერა

შევამოწმოთ პროცესები ქონექშენები და დავაკვირდეთ პიდ-ის ნომერს:

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 გამოყენეზით 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
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/