



پزشکی قانونی تروجان حافظه

Malware Memory Forensics

HACKFANS

Unknown Digital Security Team

JANUARY 1, 2013

HACKFANS.ORG

F4RY4R_RED & X3NON

بسمه تعالی

پزشکی قانونی تروجان حافظه

مقدمه

پزشکی قانونی حافظه تجزیه و تحلیلی از تصویر حافظه در حال اجرای کامپیوتر است. در این مقاله خواهید آموخت چگونه استفاده از مزایای پزشکی قانونی مانند Volatility تجزیه و تحیل از حافظه و استفاده قانونی از آن در زندگی واقعی خودمان.

این مقاله بخشی از مهندسی معکوس و درس تجزیه و تحلیل تروجان می باشد.

چرا پزشکی قانونی حافظه ؟

پزشکی قانونی در خارج کردن آثار کشف شده از حافظه یک کامپیوتر مانند فرآیند در حال اجرا ، اتصال به شبکه ، لود شدن مازول ها و غیره و همچنین در تشخیص rootkit ها و مهندسی معکوس به ما کمک می کند. در لیست زیر مراحل وارد شدن در حافظه توسط پزشکی قانونی را بیان می کنیم.

1- اکتساب حافظه (Memory Acquisition)

این مرحله شامل آزاد سازی حافظه دستگاه هدف بر روی ماشین فیزیکی است . شما می توانید برای این کار از ابزارهایی مانند dumpit , memoryze , win32dd/win64dd , fast dump در ماشین های مجازی برای دستیابی آسان به قسمتی از حافظه استفاده کنید. همچنین می توانید آنرا به حالت تعلیق در VM و گرفتن فایل "vmem" انجام دهید.

2- آنالیز حافظه

HACKFANS
Unknown Digital Security Team



قسمتی از حافظه را انتخاب می کنیم . در گام بعدی از تجزیه و تحلیل حافظه می توان یک شی قانونی از آن را گرفت. برای تجزیه و تحلیل حافظه می توان از ابزارهایی مانند Volatility و memorize استفاده نمود.

Volatility – بررسی اجمالی سریع

Volatility یک چهارچوب قانونی پیشرفته نوشته به زبان python در حافظه می باشد. که می توان آنرا بر روی سیستم عامل های مختلف مانند (ویندوز ، لینوکس و...) با جزئیات کامل نصب و راه اندازی نمود.

طریقه استفاده از Volatility

از سوئیچ هایی مانند h- یا help- می توان استفاده کرد که یکسری امکانات به همراه پلاگین ها را به ما نشان می دهد.

Python vol.py -h

از سوئیچ f- یا profile- به منظور نشان دادن حالتی از حافظه ی در حال تجزیه و تحلیل می توان استفاده نمود

Python vol.py -f mem.dmp – profile =winxpsp3x86

برای دانستن اطلاعات پروفایل از دستور زیر استفاده می کنیم

Python vol.py -f mem.dmp imageinfo

ازدحام در پزشکی قانونی حافظه
HACKFANS
Unknown Digital Security Team

به منظور درک پزشکی قانونی حافظه و مراحل آن ما یک سناریو به شرح زیر ایجاد کرده ایم.



سناریوی نسخه ی نمایش

دستگاه امنیتی بر روی سیستم شما هشدار از ساخته شدن یک اتصال از طریق HTTP با IP 208.91.197.54 از یک منبع IP 192.168.1.100 را به تاریخ 8 ژوئن 2012 در حدود ساعت 13:30 را می دهد. تحقیقی در خصوص ارتباط حافظه دستگاه با IP 192.168.1.100 صورت می گیرد.

مراحل آماده سازی

برای شروع و بدست آوردن قسمتی از حافظه IP 192.168.1.100 با استفاده از ابزار Memory Acquisition برای نسخه نمایشی، از حافظه فایلی بنام infected.dmp می گیریم.

ازدحام - تجزیه و تحلیل حافظه

حالا که ما فایل infected.dmp را بدست آوردیم باید شروع به تجزیه و تحلیل ان کنیم.

مرحله 1 - شروع با آنچه که می دانیم

ما از اخطار دستگاه هشدار دهنده مبنی بر ساخته شدن یک اتصال HTTP به 208.91.197.54 آگاه شدیم. بنابراین اجازه داریم که به اتصالات شبکه نگاهی بیاندازیم.

HACKFANS
Unknown Digital Security Team



Volatility ماژول های اتصال یافته به ما نشان می دهد که اتصال به ip های مخرب ساخته شده توسط PID

1748 صورت گرفته است.

```
root@bt: ~/Volatility
File Edit View Terminal Help
root@bt:~/Volatility# python vol.py -f infected.dmp connections
Volatile Systems Volatility Framework 2.0
Offset(V) Local Address Remote Address Pid
-----
0x8943a558 192.168.1.100:1032 208.91.197.54:80 1748
root@bt:~/Volatility#
```

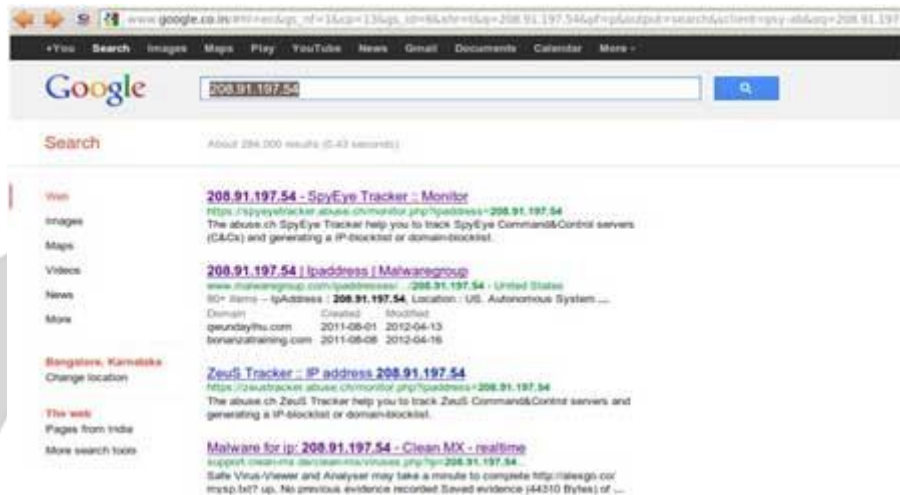
مرحله 2 - اطلاعاتی در خصوص 208.91.197.54

با وارد کردن این IP در جستجوی گوگل خواهیم دید که این IP احتمالاً با نرم افزارهای مخربی مانند

spyeye همراه است که ما نیاز به تایید این موضوع داریم.

HACKFANS
Unknown Digital Security Team





مرحله 3- PID 1748 چیست؟

از آنجائیکه از اتصال شبکه به IP 208.91.197.54 با PID 1748 فایل ساخته شده است. ما باید برای تعیین این PID از ابزار psscan استفاده کنیم. این ابزار به ما نشان می دهد که PID 1748 متعلق به explorer.exe می باشد. همچنین از دو روند ایجاد شده توسط دستگاههای امنیتی در همان زمان یعنی 8 ژوئن 2012 گزارش داده است.

```

root@kali:~/Volatility# python vol.py -f infected.dmp psscan
Volatility Systems Volatility Framework 2.0
Offset Name PID PPID PDB Time created Time exited
-----
0x0932b020 86232f3a9f9.exe 1672 1748 0xbff9c02a0 2012-06-08 13:27:55 2012-06-08 13:27:56
0x09339620 wmiprvse.exe 584 880 0xbff9c0260 2012-02-26 12:07:19
0x0934c4a8 VMopgradehelper 428 700 0xbff9c0240 2012-02-26 12:07:19
0x09359740 vmtoolsd.exe 216 700 0xbff9c0220 2012-02-26 12:07:19
0x0935a360 explorer.exe 3748 1712 0xbff9c01c0 2012-02-26 12:07:17
0x093662b8 svchost.exe 964 700 0xbff9c0180 2012-02-26 12:07:11
0x094c6da8 svchost.exe 880 700 0xbff9c00e0 2012-02-26 12:07:11
0x095ffa58 cfmon.exe 1908 1748 0xbff9c0200 2012-02-26 12:07:18
0x0964c020 err.exe 1648 1888 0xbff9c0280 2012-06-08 13:27:53 2012-06-08 13:27:57
0x09656620 VMwareUser.exe 1888 1748 0xbff9c01e0 2012-02-26 12:07:18
0x09665630 winlogon.exe 656 376 0xbff9c0060 2012-02-26 12:07:11
0x097166a8 VMwareTray.exe 1880 1748 0xbff9c0180 2012-02-26 12:07:18
0x0971ea38 svchost.exe 1092 700 0xbff9c0140 2012-02-26 12:07:11
0x09732da8 csrss.exe 632 376 0xbff9c0040 2012-02-26 12:07:10
0x097aebf0 services.exe 700 656 0xbff9c0080 2012-02-26 12:07:11
0x09811020 lsass.exe 712 656 0xbff9c00a0 2012-02-26 12:07:11
0x09821020 smss.exe 376 4 0xbff9c0020 2012-02-26 12:07:10
0x0984c8e0 svchost.exe 1124 700 0xbff9c0160 2012-02-26 12:07:11
0x0984e170 svchost.exe 1048 700 0xbff9c0120 2012-02-26 12:07:11
0x098523b0 vmacthlp.exe 868 700 0xbff9c00c0 2012-02-26 12:07:11
0x0992b030 System 4 0 0xb0319000
root@kali:~/Volatility#

```

مرحله 4- فرآیند دسته ای از explorer.exe



حالا که می دانیم explorer.exe را (که یک فرآیند سیستم عامل است) در ساختن این اتصال آلوده نقش دارد پس احتمال وجود دارد که خود explorer.exe نیز آلوده باشد.

در فرآیند دسته explorer.exe این اجازه داده می شود تا فایل آلوده ساخته شود . در تصویر زیر نشان داده شده است که explorer.exe از دسته B6232F3A9F9.exe است ولی با وجود اینها باز اجازه اتصال را می دهد.

```

root@bt: ~/Volatility
File Edit View Terminal Help
root@bt:~/Volatility# python vol.py -f infected.dmp handles -p 1748 -t Process
Volatile Systems Volatility Framework 2.0
Offset(V)  Pid  Type      Details
0x8915a348 1748 Process   explorer.exe(1748)
0x8912b008 1748 Process   B6232F3A9F9.exe(1672)
0x8912b008 1748 Process   B6232F3A9F9.exe(1672)
root@bt:~/Volatility#

```

مرحله 5- قلاب API در explorer.exe

ماژول قلاب API نشان می دهد که یک پرش در explorer.exe به محل نامعلومی صورت گرفته است.

HACKFANS
Unknown Digital Security Team



```

root@bt:~/Volatility# python vol.py -f infected.dmp apihooks -p 1748
Volatility Systems Volatility Framework 2.0
Name                Type      Target                                Value
explorer.exe[1748]  inline   user32.dll!TranslateMessage[0x7e418bf6] 0x7e418bf6 JMP 0xbb6bddd (UNKNOWN)
explorer.exe[1748]  inline   crypt32.dll!PFXImportCertStore[0x77aeff8f] 0x77aeff8f JMP 0xbb79462 (UNKNOWN)
explorer.exe[1748]  inline   wininet.dll!HttpSendRequestA[0x7806c4d0] 0x7806c4d0 JMP 0xbb82a3e (UNKNOWN)
explorer.exe[1748]  inline   wininet.dll!HttpSendRequestA[0x78080825] 0x78080825 JMP 0xbb82b9c (UNKNOWN)
explorer.exe[1748]  inline   wininet.dll!InternetCloseHandle[0x7805da59] 0x7805da59 JMP 0xbb7dc48 (UNKNOWN)
explorer.exe[1748]  inline   wininet.dll!InternetWriteFile[0x78073645] 0x78073645 JMP 0xbb82cfa (UNKNOWN)
explorer.exe[1748]  inline   advapi32.dll!CryptEncrypt[0x77dee340] 0x77dee340 JMP 0xbb7c597 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!NTEnumerateValueKey[0x7c90d209] 0x7c90d209 JMP 0xbb6a7f0 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!NTQueryDirectoryFile[0x7c90d750] 0x7c90d750 JMP 0xbb74885 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!NTResumeThread[0x7c90db20] 0x7c90db20 JMP 0xbb861f8 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!NTSetInformationFile[0x7c90dc40] 0x7c90dc40 JMP 0xbb6a53a (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!NTVdmControl[0x7c90df00] 0x7c90df00 JMP 0xbb7493b (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!ZwEnumerateValueKey[0x7c90d209] 0x7c90d209 JMP 0xbb6a7f0 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!ZwQueryDirectoryFile[0x7c90d750] 0x7c90d750 JMP 0xbb74885 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!ZwResumeThread[0x7c90db20] 0x7c90db20 JMP 0xbb861f8 (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!ZwSetInformationFile[0x7c90dc40] 0x7c90dc40 JMP 0xbb6a53a (UNKNOWN)
explorer.exe[1748]  inline   ntdll.dll!ZwVdmControl[0x7c90df00] 0x7c90df00 JMP 0xbb7493b (UNKNOWN)
explorer.exe[1748]  inline   ws2_32.dll!send[0x71ab4c27] 0x71ab4c27 JMP 0xbb763b6 (UNKNOWN)
Finished after 17.2333590984 seconds
root@bt:~/Volatility#

```

مرحله 6 - بررسی قلاب

این قلاب نشان می دهد که ابتدا یک پرش کوتاه و سپس یک پرش بلند به محل تروجان صورت گرفته است.

```

root@bt:~/Volatility# python vol.py -f infected.dmp volshell
Volatility Systems Volatility Framework 2.0
Current context: process System, pid=4, ppid=0 DTB=0x319000
Welcome to volshell! Current memory image is:
file:///root/Volatility/infected.dmp
To get help, type 'hh()'
>>> hh()
ps()                : Print a process listing.
cc(offset=None, pid=None, name=None) : Change current shell context.
dd(address, length=128, space=None)  : Print dwords at address.
db(address, length=128, width=16, space=None) : Print bytes as canonical hexdump.
hh(cmd=None)        : Get help on a command.
dt(object, address=None) : Describe an object or show type info.
list entry(head, objname, offset=-1, fieldname=None, forward=True) : Traverse a _LIST_ENTRY.
dis(address, length=128, space=None)  : Disassemble code at a given address.

For help on a specific command, type 'hh(<command>)'
>>> cc(pid=1748)
Current context: process explorer.exe, pid=1748, ppid=1712 DTB=0xf9c01c8
>>> dis(0x7e418bf6, length=32)
0x7e418bf6 eb01          JMP 0x7e418bf9
0x7e418bf8 c3                RET
0x7e418bf9 e9de31758d       JMP 0xbb6bddd
0x7e418bfe 086681          OR [ESI-0x7f], AH
0x7e418c01 7e08          JLE 0x7e418c0b
0x7e418c03 e500          IN EAX, 0x0
0x7e418c05 0f84667e0200   JZ 0x7e440a71
0x7e418c0b 6a00          PUSH 0x0

```

مرحله 7 - EXE های جاسازی شده در explorer.exe

HACKFANS
Unknown Digital Security Team



با چاپ بایتها در محل قلاب ، حضور یک فایل اجرایی جاسازی شده در explorer.exe مشاهده میشود.

```
>>> db(0xbb60000, length=256)
0bb60000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0bb60010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0bb60020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00  .....
0bb60040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb60090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb600a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb600b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb600c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb600d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0bb600e0  50 45 00 00 4c 01 02 00 92 60 ed 4d 00 00 00 00  PE..L....M...
0bb600f0  00 00 00 00 e0 00 02 01 0b 01 0a 00 00 a2 04 00  .....
>>> |
```

مرحله 8 – آزاد سازی EXE جاسازی شده

ابزار Vadump از ابزارهای EXE جاسازی شده در explorer.exe است.

```
root@bt: ~/Volatility
File Edit View Terminal Help
root@bt:~/Volatility# python vol.py -f infected.dmp vaddump -p 1748 -D dump/
Volatile Systems Volatility Framework 2.0
Pid: 1748
.....
root@bt:~/Volatility# |
```

HACKFANS
Unknown Digital Security Team





مرحله 9- ارسال فایل برای چک کردن توسط virus total

با ارسال این فایل به virus total نشان میدهد که این فایل بخشهای از SpyEye میباشد.

Antivirus	Result	Update
AvLab-CS	Passed/No2:Malware	20120608
AVP	TR/Orgen-Spy	20120608
Avy-AVL	-	20120608
Avast	Win32/SpyEye-KY (7)	20120608
BitDefender	-	20120608
Cyren	-	20120608
CAT-Quarantine	-	20120608
DavKd	-	20120608
Comodo	-	20120608
DrWeb	-	20120608
Emsisoft	Traps Win32/SpyEye	20120608
Forti	-	20120607
F-Secure	-	20120608
Fortinet	-	20120608
GData	-	20120608
King	Traps Win32/SpyEye	20120608

U n k



مرحله 10- چگونه اطلاعات بیشتر بدست بیاوریم

رشته استخراج شده از فایل اجرایی نشان می دهد منابعی را در (کلید رجستری و اجرایی) و همچنین فایلی مشکوک در مسیر اجرایی B6232F3A9F9.exe نشان می دهد.

```

Filesystem Browser
Connection: close
Connection:
Content-Length:
Content-Length:
Content-Encoding:
Content-Encoding: deflate
Content-Encoding: gzip
Transfer-Encoding:
Transfer-Encoding: chunked
Content-Length: %u\
HTTP/
User-Agent:
Accept-Encoding:
Keep-Alive:
Connection: keep-alive
Proxy-Connection: keep-alive
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
%.2x
cookies-nontor.xml
cookies.txt
sessionstore.js

Filesystem Browser
f98u
^[\t
860\
C:\WINDOWS\system32\WININET.dll
C:\Recycle.Bin\A705B3960358085
C:\WINDOWS\system32\ntdll.dll
C:\WINDOWS\system32\ntdll.dll
C:\WINDOWS\system32\USER32.dll
C:\WINDOWS\system32\ntdll.dll
C:\WINDOWS\system32\CRYPT32.dll
C:\Recycle.Bin\B6232F3A9F9.exe
C:\Recycle.Bin\
B6232F3A9F9.exe
A705B3960358085
s1PSg1LF.exe
C:\DOCUME-1\ADMINI-1\LOCALS-1\Temp\
  
```

مرحله 11- چاپ کردن کلید رجستری

با چاپ کلید رجستری مشخص می شو که نرم افزارهای مخرب برای زنده ماندن و راه اندازی مجدد سیستم نیاز به ایجاد یک کلید رجستری دارند.

HACKFANS

Unknown Digital Security Team



```

root@kali:~/Volatility# python vol.py -f infected.dmp printkey -K "SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"
Volatility Systems Volatility Framework 2.0
Legend: (S) = Stable (V) = Volatile
-----
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2011-10-31 15:07:20
Subkeys:
Values:
-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2011-10-31 20:28:57
Subkeys:
Values:
-----
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-06-08 13:27:56
Subkeys:
Values:
REG_SZ ctfmon.exe : (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ 4Y3Y6C3A1F7AZN2WAC0C0D : (S) C:\Recycle.Bin\B6232F3A9F9.exe
    
```

مرحله 12 - پیدا کردن EXE مخرب در دستگاه آلوده

اکنون که ما مسیر اجرایی مشکوک را می دانیم این مسیر در پیدا کردن فایل EXE مخرب کمک می کند.



نتیجه

پزشکی قانونی حافظه یک روش قدرتمند است و با یک ابزاری مانند Volatility آنرا ممکن می سازد. برای پیدا کردن و استخراج مصنوعات قانونی از حافظه و مهندسی معکوس و تجزیه و تحلی این روش به ما کمک می کند.

HACKFANS
Unknown Digital Security Team

