پزشکی قانونی تروجان حافظه

Malware Memory Forensics

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 اموخت چگونگی استفاده از مزایای پزشکی قانونی مانند Volatility تجزیه و تحیل از حافظه و استفاده قاونی 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 قاونوی را بیان می کنیم.

1- اکتساب حافظه (Memory Acquistion)

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

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

Volatility – بررسی اجمالی سریع

Volatilityیک 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– یاhelp – می توان استفاده کرد که یکسری امکانات به همراه پلاگین ها را به ما نشان می دهد.

```
Python vol.py  -h
```

از سوئیچ f– یاprofile – 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

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 Acquistion برای نسخه نمایشی ، از حافظه فایلی بنام infected.dmp می گیریم.

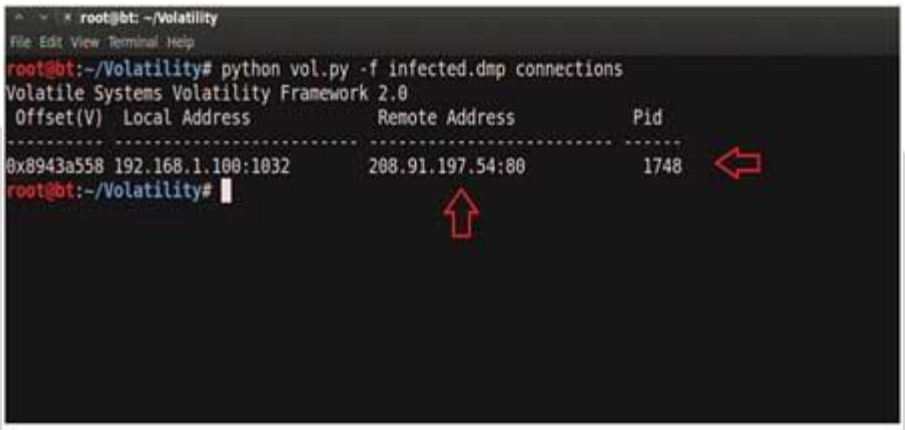
ازدحام – تجزیه و تحلیل حافظه

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

مرحله 1 – شروع با آنچه که می دانیم

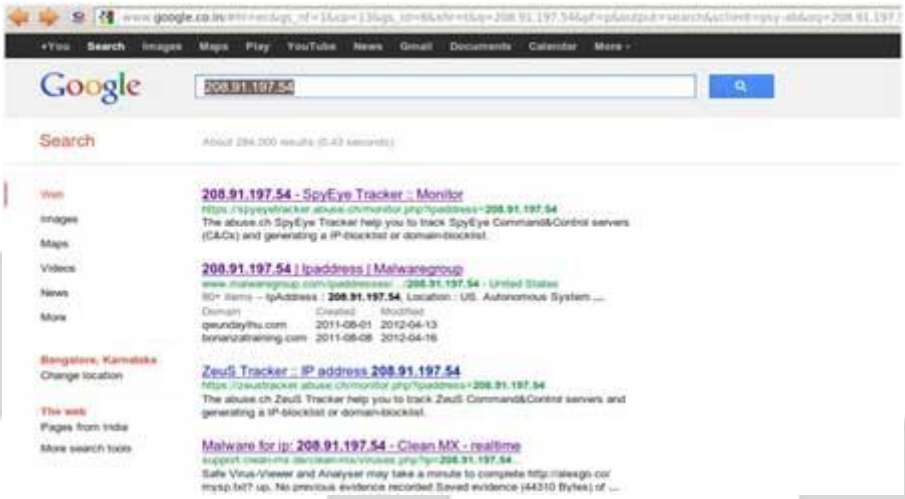
ما از اخطار دستگاه هشدار دهنده مبنی بر ساخته شدن یک اتصال HTTP به 208.91.197.54 آگاه شدیم. بنابراین اجازه داریم که به اتصالات شبکه نگاهی بیاندازیم.

Volatilityماژول های اتصال یافته به ما نشان می دهد که اتصال به ip های مخرب ساخته شده توسط PID 1748 صورت گرفته است.



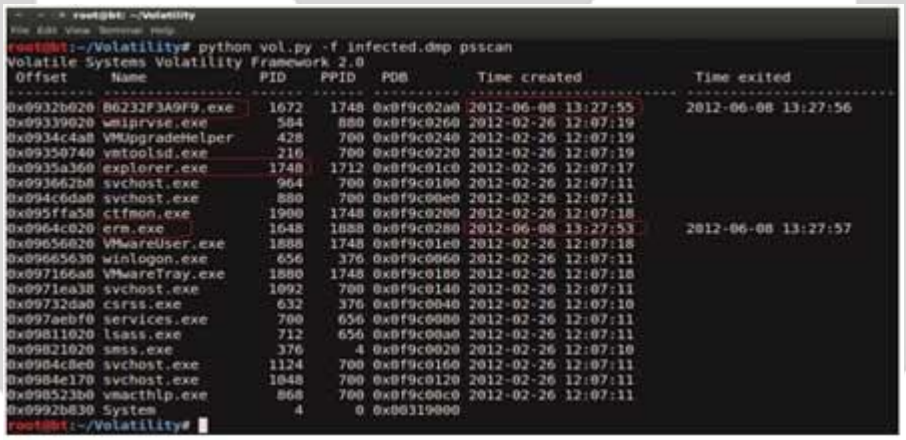
مرحله 2 – اطلاعاتی در خصوص 208.91.197.54

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 تائید این موضوع داریم.



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 زوئن 2012 گزارش داده است.

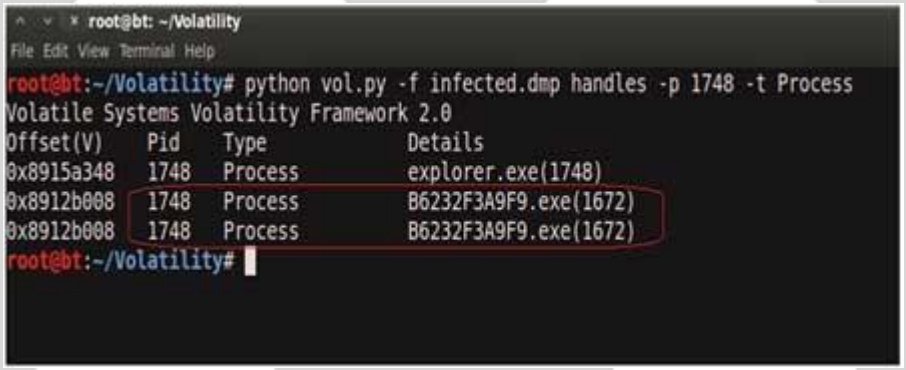


```
root@bt:~/Volatility# python vol.py -f infected.dmp psscan
Volatile Systems Volatility Framework 2.0
 Offset     Name             PID    PPID   PDB        Time created            Time exited
------------------------------------------------------------------------------------------
0x0932b020 B6232F3A9F9.exe   1672   1748 0x0f9c02a0 2012-06-08 13:27:55      2012-06-08 13:27:56
0x09339020 wmiprvse.exe       584    880 0x0f9c0260 2012-02-26 12:07:19
0x0934c4a8 VMUpgradeHelper    428    700 0x0f9c0240 2012-02-26 12:07:19
0x09350740 vmtoolsd.exe       216    700 0x0f9c0220 2012-02-26 12:07:19
0x0935a360 explorer.exe      1748   1712 0x0f9c01c0 2012-02-26 12:07:17
0x093662b8 svchost.exe        964    700 0x0f9c0180 2012-02-26 12:07:11
0x094c6da0 svchost.exe        880    700 0x0f9c00e0 2012-02-26 12:07:11
0x095ffa58 ctfmon.exe        1900   1748 0x0f9c0200 2012-02-26 12:07:18
0x0964c020 erm.exe           1648   1888 0x0f9c0280 2012-06-08 13:27:53      2012-06-08 13:27:57
0x09656020 VMwareUser.exe    1888   1748 0x0f9c01e0 2012-02-26 12:07:18
0x09665630 winlogon.exe       656    376 0x0f9c0060 2012-02-26 12:07:11
0x097166a8 VMwareTray.exe    1880   1748 0x0f9c0180 2012-02-26 12:07:18
0x0971ea38 svchost.exe       1092    700 0x0f9c0140 2012-02-26 12:07:11
0x09732da0 csrss.exe          632    376 0x0f9c0040 2012-02-26 12:07:10
0x097aebf0 services.exe       700    656 0x0f9c0080 2012-02-26 12:07:11
0x09811020 lsass.exe          712    656 0x0f9c00a0 2012-02-26 12:07:11
0x09821020 smss.exe           376      4 0x0f9c0020 2012-02-26 12:07:10
0x0984c8e0 svchost.exe       1124    700 0x0f9c0160 2012-02-26 12:07:11
0x0984e170 svchost.exe       1048    700 0x0f9c0120 2012-02-26 12:07:11
0x098523b0 vmacthlp.exe       868    700 0x0f9c00c0 2012-02-26 12:07:11
0x0992b830 System               4      0 0x00319000
root@bt:~/Volatility#
```


مرحله 4 – فرآیند دسته ای از explorer.exe

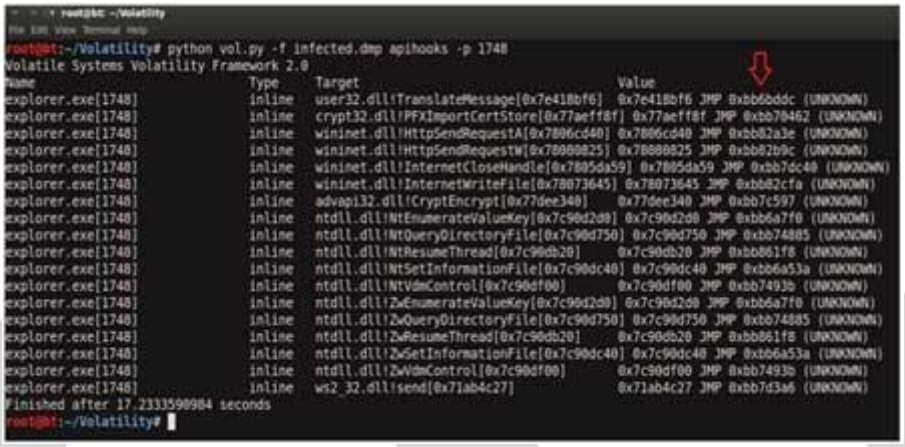
حالا که می دانیم explorer.exe را (که یک فرآیند سیستم عامل است) در ساختن این اتصال آلوده نقش دارد پس احتمال وجود دارد که خود explorer.exe نیز آلوده باشد.

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.



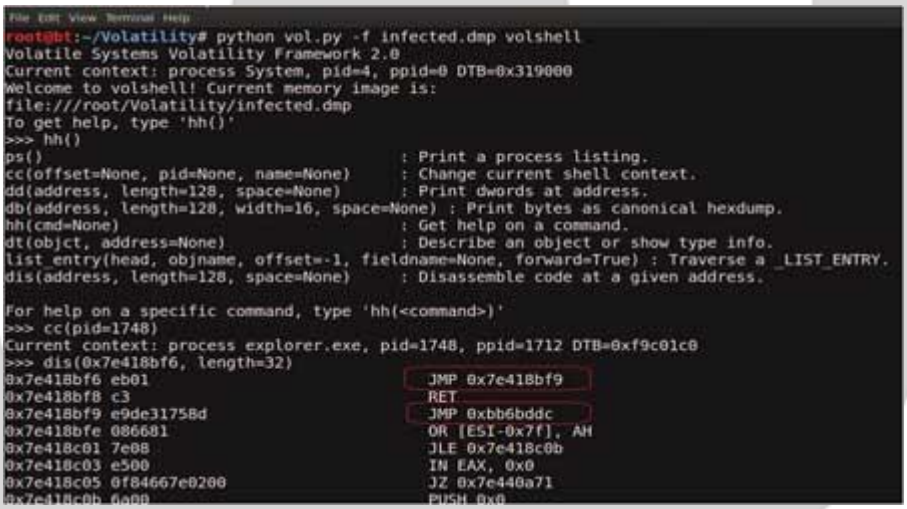
مرحله 5- قلاب API در explorer.exe

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



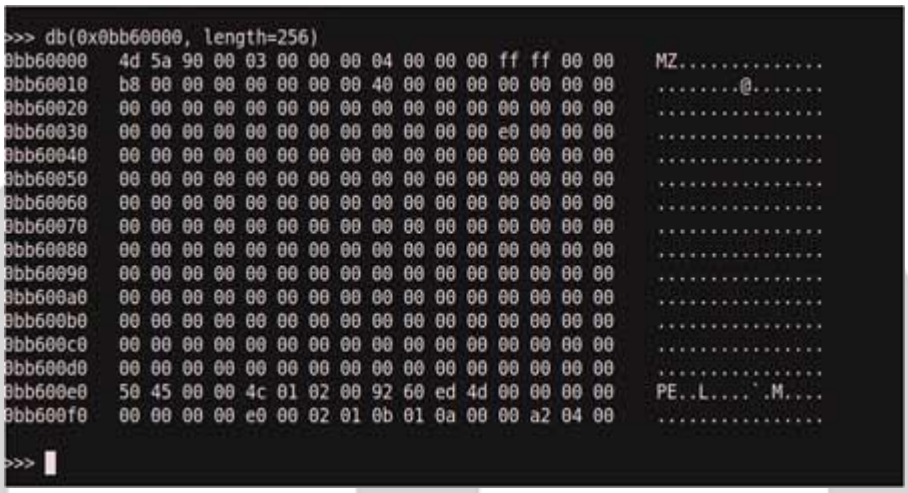
مرحله 6 – بررسی قلاب

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



مرحله 7 – EXE های جاسازی شده در explorer.exe

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

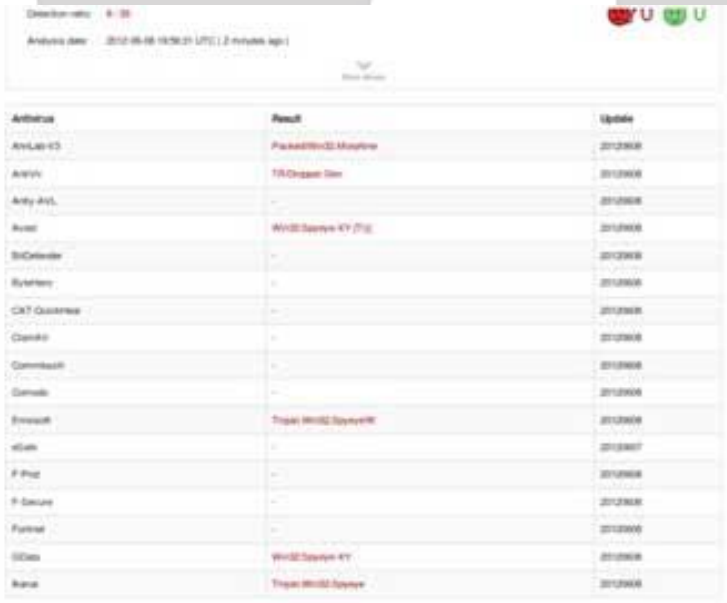


مرحله 8 – آزاد سازی EXE جاسازی شده

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

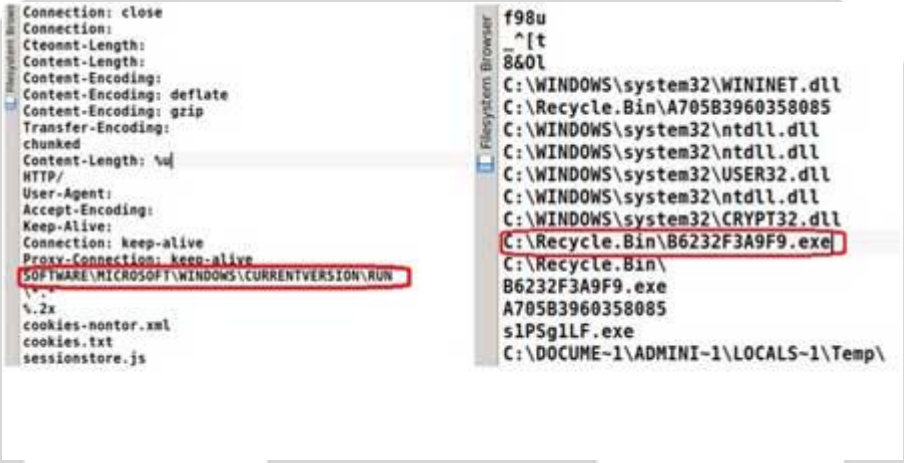
مرحله 9– ارسال فایل برای چک کردن توسط virus total

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



مرحله 10- چگونه اطلاعات بیشتر بدست بیاوریم

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



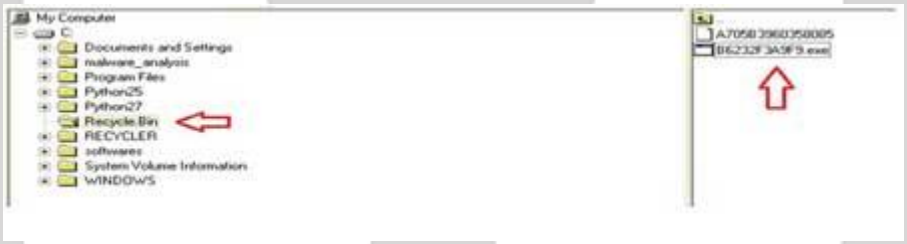
مرحله 11 – چاپ کردن کلید ریجستری

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

```
root@bt:~/Volatility# python vol.py -f infected.dmp printkey -K "SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"
Volatile 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        4Y3Y0C3A1F7XZHZWACQCUD : (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 ساز . برای پیدا کردن و استخراج مصنوعات قانونی از حافظه و مهندسی معکوس و تجزیه و تحلی این روش به ما کمک می کند.