TUGAS COMPUTER FORENSIC

EVOLUTION OF MEMORY VOLATILITY

DATA DIRI ANGGOTA

2540120603
Nicolas Saputra Gunawan

2540124620
Jeffrey Jingga

2540119633
Mikael Wiryamanta Wijaya

2540124740
Satya Kusuma

2540115181
Pitra Winarianto

DAFTAR ISI

Introduction

Banyaknya serangan yang berupa fileless malware membuatnya susah untuk bisa dideteksi oleh antivirus software. Dengan begitu, pengaplikasian volatile memory forensic sangat berguna dalam melakukan analisis malware tersebut

Volatile memory biasanya berisi:

1. Fragmented Encrypted Files
2. Running Processes
3. Network Connection
4. Cache

Memory Acquisition Technique

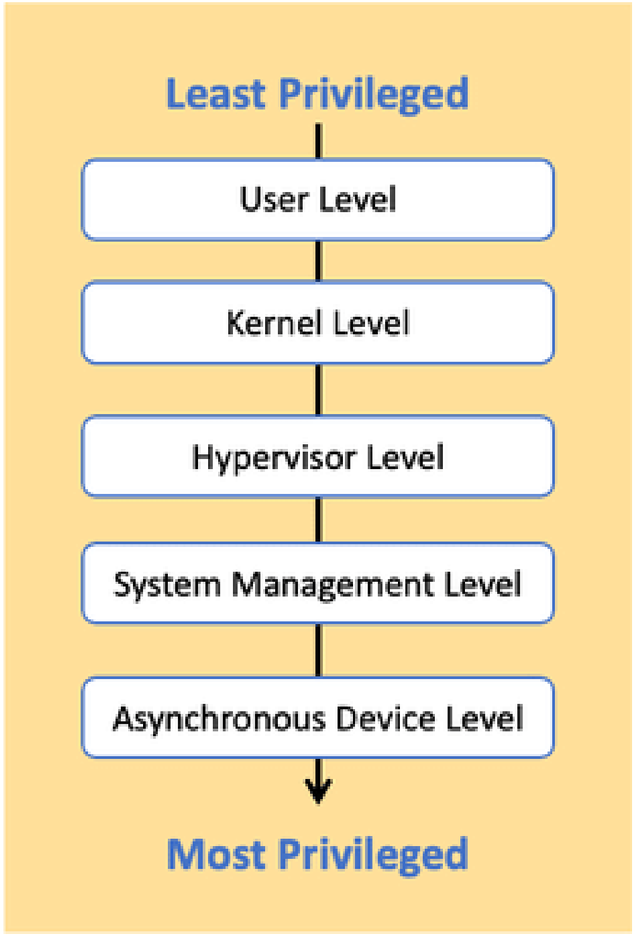
Kualitas dari volatile memory analysis sangat bergantung pada memory dump yang diambil dari sistem.

Hal yang membuat Forensic Image yang baik:

1. Correctness
2. Atomicity
3. Integrity

Berdasarkan Latzo’s taxonomy alat akuisisi dibedakan berdasarkan 3 dimensi seperti berikut:

Latzo Taxonomy



Dimension 1:
Access Level Hierarchy

Pre-Incident
- Higher atomicity dump
- Requires foresight before incident occurs

Post-Incident
- Can be used if incident has already occurred
- Lower atomicity dump

Dimension 2:
Time of Deployment

Non-Terminating
- Doesn't interfere with system operations
- Preserves forensic evidence more cleanly

Terminating
- Usually built into the operating system
- No additional configuration required

Dimension 3:
Need for Termination

Acquisition Technique

1. User Level

- Pada tingkat ini akuisisi memori dilakukan melalui software emulator.
- Alat akuisisi harus di deploy atau di install pre-incident.
- Pada tingkat ini biasanya alat akuisi bersifat non-terminating.

Tools-tools pada user level biasanya digunakan pada kernel debugger ataupun virtual machine karena memiliki performa yang lebih tinggi dan isolasi malware yang lebih baik.

Acquisition Technique

2. Kernel Level

- Pada tingkat ini biasanya dapat menggunakan Driver Kernel, Dump Crash, dan Debugger yang berjalan di atas executable.

- Driver kernel biasanya di deploy post-incident, sedangkan Dump Crash merupakan built in sehingga dikategorikan sebgai pre-incident, dan untuk Debugger sendiri dapat melakukan keduanya.

- Driver kernel dan debugger dapat dikategorikan sebagai non-terminating, sedangkan Dump Crash dikategorikan sebagai terminating , dan untuk Debugger sendiri dapat melakukan keduanya.

Acquisition Technique

3. Hypervisor Level

- Pada tingkat ini biasanya menggunakan virtualization tools seperti VMware dan LibVMI.

- Kebanyakan tools pada tingkat ini biasanya di deploy pre-incident, tetapi terdapat beberapa pengecualian seperti HyperSleuth, Vis, and a tool by Cheng.

- VM dapat dipause lalu memorynya dapat diambil dari tools yang disediakan vendor seperti VMware (vmss2core.exe) dan LibVMI yang memiliki fungsi dump-memory.

Acquisition Technique

4. Synchronous Management Level (SML)

- SML ini merupakan operating mode dari system architecture yang independent pada OS pada umumnya yang menghandle basic input output dan Unified Extensible Firmware Interface (BIOS/UEFI).

- Tidak banyak yang mengimplementasikan tingkat ini dalam toolsnya

Acquisition Technique

5. Asynchronous Device Level (ADL).

- Pada tingkat ini akuisisi memory menggunakan bantuan perangkat keras eksternal, seperti PCILeech dan Inception.

- Pada tingkat ini terutama 2 device diatas dapat di deploy post-incident dan dikategorikan sebagai non-terminating.

- Tools ini mengakses memory melalui system buses dengan memanfaatkan direct memory access (DMA).

- Dikarenakan sistem akan terus berjalan maka tidak memungkinkan untuk mendapatkan atomic snapshot.

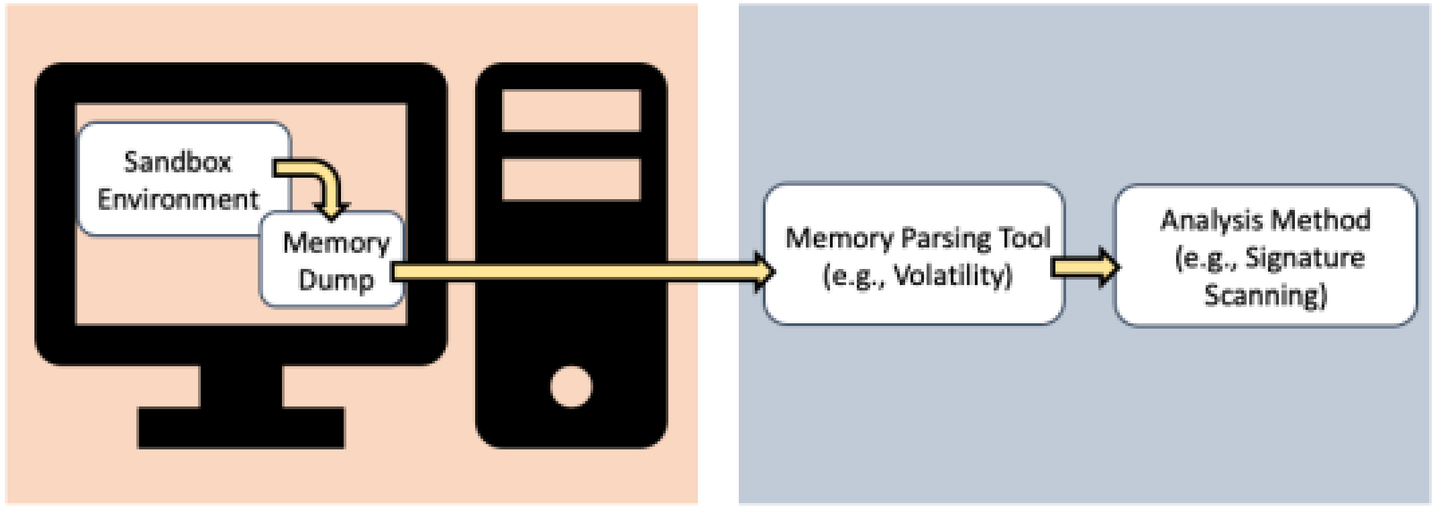
Discussion

- Tidak ada alat akuisisi yang sempurna. Apabila alat tersebut dapat menciptakan image yang atomic, benar, dan berintegritas biasanya memiliki kekurangan pada performance dan biasanya membutuhkan terminating program. Sedangkan apabila alat tersebut memiliki performance yang bagus maka hasilnya tidak akan begitu bagus.

- Selain itu terdapat beberapa masalah dengan teknik anti-forensic dan juga pendeteksi dari malware tersebut.

Memory Analysis

Proses umum untuk memperoleh memory dump dan menganalisisnya untuk mengidentifikasi malware melibatkan eksekusi malware (biasanya di sandbox environtment) dan pengambilan memory dump dari sistem yang terpengaruh. Setelah itu, memory dump tersebut diparse menggunakan alat seperti Volatility, dan analisis tambahan dapat dilakukan pada hasil output dari Volatility.



Memory Analysis

- Sudah ada beberapa memory analysis tools yang dibuat dan memungkinkan user untuk parse memory dumps.
- Open source tools seperti Volatility dan Rekall
- Commercial tools seperti Cellebrite Inspector, FireEye Redline, Magnet AXIOM, dan WindowsSCOPE. Commercial tools menggunakan atau memanfaatkan volatility, namun ada fitur tambahan seperti enterprise-level remote endpoint management with additional analysis.

Volatility

- Open source
- Python-based framework untuk memory dump analysis.
- Supports Windows, Linux, and Macintosh machines.
- Menangani berbagai format dump file dan memiliki extensible API.
- Implementasi yang efisien dengan feature-creating functionality.

Performance

- Developers mengklaim bahwa efisiensinya yang lebih tinggi dibandingkan dengan memory forensic software lainnya.
- Kemampuan untuk membuat list kernel modules dari sistem 80 GB dalam hitungan detik.
- Volatility3 beta mengklaim peningkatan performa yang besar dibandingkan dengan Volatility2 dan Rekall.

Volatility

Basic Capabilities

- Mengekstrak proses saat ini dan sebelumnya, memuat DLLs, dan console shell commands.
- Mengambil memory resident pages, process executables, dan informasi tentang VAD nodes.
- Memperoleh data tentang kernel drivers yang dimuat pada sistem maupun yang disembunyikan di memori fisik atau di disk.
- Mengidentifikasi objek process thread melalui pool tag scanning.
- Mengekstrak informasi tentang koneksi sistem, termasuk TCP endpoints, TCP listeners, UDP endpoints, dan UDP listeners.

Rekall

- Rekall berasal dari cabang dari Volatility pada tahun 2011.
- Berkembang menjadi advanced forensic and incident response framework.

- Rekall dapat meng-parse dumps dari Windows, Linux, and Mac OS.
- Memberikan informasi tentang system processes, memory structures, dan network connections.

- Dilengkapi dengan memory dump functionality.
- Supports live memory analysis, mirip seperti forensic mode Volatility.

- Ada fitur graphical user interface (GUI) yang sangat berguna.
- Menggabungkan metode yang dirancang untuk lebih mendukung versi OS yang lain.

- Rekall tidak lagi dikelola secara aktif oleh developernya, sehingga membatasi kegunaannya bagi peneliti forensik memori di masa depan.

Rekall

- Volatility dan Rekall merupakan tools untuk pemeriksaan manual memory dump files yang dapat memberikan informasi tentang computer systems, process memory, kernel memory and objects, and network connections.
- Tools ini tidak berdiri sendiri, namun merupakan sebuah platform end-to-end yang secara otomatis dapat mendeteksi keberadaan malicious code dalam sistem komputer.
- Diperlukan operator berpengalaman untuk mengekstrak dan menafsirkan isi dari volatile memory.
- Karena tingkat pembuatan malware jauh melebihi kemampuan para ahli untuk melakukan reverse engineering, tools ini akan menjadi sangat bagus bila digunakan dengan software lain yang memberikan otomatisasi dalam proses pendeteksian malware.

Scanning Methods

- Dalam forensik, pendekatan scanning fokus pada pencarian data forensik pada sistem terinfeksi, terutama pada memory dump file. Meskipun scanning physical memory memberikan gambaran yang tidak lengkap, teknik ini cepat dan efektif sebagai respons pertama terhadap infeksi.
- Signature-based scanning, mencari string atau urutan byte tertentu, sementara heuristic based scanning mencari perintah, logika, atau instruksi khusus

Signature Scanning

- Mencocokkan malware signatures yang diketahui dengan konten dari memory dump files.
- YARA signatures telah muncul sebagai metode scanning industry de facto, dan didukung langsung dalam Volatility.
- Dapat meng-scan virtual address space atau memory image secara langsung.
- Context-aware scanning yang menggunakan database Windows Page Frame Number (PFN) dapat meningkatkan matching speed and accuracy, karena virtual address space tidak perlu direkonstruksi pada setiap proses.
- Challenge: Requirements storage yang besar untuk banyak memory dump files.
- Upaya untuk membuat public repositories untuk memory dump files.
- Compression utilities and signature creation berdasarkan compressed memory files yang telah dipertimbangkan.
- MemScrimper methodology mengatasi storage issues dengan hanya mengkompres secara selektif bagian antara system memory snapshots yang bersih dan terinfeksi.

Heuristic Scanning

- Mendeteksi ancaman menggunakan aturan dan algoritme untuk mengidentifikasi perintah atau instruksi yang menunjukkan niat jahat.
- Lebih dapat digeneralisasikan dibandingkan dengan signatures, memungkinkan identifikasi malware yang sebelumnya tidak terlihat.
- Sering kali digunakan bersamaan dengan signature scanning.

- USIM toolkit yang dibuat oleh Pendergrass merupakan kumpulan alat pengumpulan pengukuran integritas untuk memeriksa abstraksi OS.
- Berfokuskan pada namespaces, filesystems, networking, communication channels, environment variables, runtime linkers/loaders, and virtual memory management.
- Menyediakan graph-based structure yang dinilai berdasarkan administrator-defined rules.
- Dirancang untuk analisis lebih mendalam pada data memory dan non-memory forensic menggunakan rule-based heuristics, bukan automated malware detection.

Dynamic Analysis within a Sandbox

- Malware dapat dieksekusi dalam lingkungan terkendali yang disebut sandbox, dan perilaku serta karakteristiknya, termasuk informasi tentang volatile memory dapat direkam.
- Sandbox merupakan aspek penting dari teknik forensik dinamis, karena melindungi sistem user dari infeksi yang tidak diinginkan.
- Proses bare-metal, yaitu malware dijalankan di luar sandbox, hampir tidak dapat diskalakan karena perlu reinstall semua sistem setelah setiap kali malware dijalankan untuk memulihkan sistem user ke kondisi awal yang bersih dan aman.
- Ada dua pendekatan utama yang digunakan untuk menyiapkan sandbox, virtualization dan emulation.

Virtualized Environments

- Virtualized environment, yang dikenal sebagai virtual machine, dikendalikan oleh hypervisor yang mengisolasinya satu sama lain dan hardware yang mendasarinya.
- Kehadiran hypervisor sulit untuk disembunyikan dari malware, dan evasive coding techniques dapat digunakan untuk mendeteksi dan mengubah perilakunya.
- Mengumpulkan data detail tentang eksekusi program sulit dilakukan karena ketidakmampuan menjalankan hypervisor dan mesin virtual machine bersamaan.

Software Emulators

- Emulator mensimulasikan fungsionalitas software atau hardware, memberikan fleksibilitas dalam menjalankan guest program pada arsitektur CPU yang berbeda.
- Ketika guest program dijalankan, analyst dapat memperoleh tampilan instruksi demi instruksi tentang perilaku malware.
- Emulator mungkin dikenakan performance penalty yang signifikan, dan seperti hypervisor, emulator dapat dideteksi dan di-bypassed oleh malware menggunakan evasive techniques.

Sandbox Tools

- Sistem commercial sandbox meliputi AnyRun, Crowdstrike Falcon Sandbox, FireEye, JoeSecurity, Palo Alto WildFire, dan VirusTotal.
- Free and open-source sandbox tools termasuk Cuckoo, DRAKVUF, Sandboxie, dan SpeakEasy.
- Tools-tools ini biasanya digunakan untuk behavior-based malware detection, dengan user berinteraksi melalui berbagai interfaces seperti command line utilities, web GUIs, or local GUIs.
- Meskipun ada di mana-mana, sistem sandbox tetap memiliki keterbatasan. Sistem Sandbox mungkin sulit untuk dikonfigurasikan dengan benar untuk dapat melawan teknik anti-analisis secara efektif.
- Penelitian ini membahas evasive techniques yang digunakan oleh pembuat malware dan tindakan pencegahan untuk memerangi sandbox evasion.
- Peningkatan performance and compatibility telah dieksplorasi, dengan beberapa mengusulkan sistem baru untuk mengurangi ketergantungan hypervisor dan meningkatkan skalabilitas.

Sandbox Tools

- Sandbox system baru yang memanfaatkan VM introspection dan memory forensic techniques.
- Sistem ini menggunakan Xen hypervisor, LibVMI untuk mengakses memori virtual machine, dan framework Volatility untuk menganalisis perilaku sistem.
- Pendekatan ini bertujuan untuk mengurangi ketergantungan hypervisor dan meningkatkan kompatibilitas dan skalabilitas.

Machine Learning Approaches

- Penggunaan pendekatan berbasis machine learning (ML) dalam deteksi malware telah meluas dalam beberapa tahun terakhir.
- Pendekatan ML ini dapat diklasifikasikan menjadi dua kelompok, Feature Engineering Approaches dan Computer Vision Approaches.

Feature Engineering Approaches

Aghaeikheirabady:

- Membandingkan berbagai pengklasifikasi untuk deteksi malware pada volatile memory.
- Fitur yang digunakan dari VAD tree, file in memory, registry keys, and changes.
- Menekankan pentingnya mendiskusikan fitur yang dipilih untuk replikasi hasil.

Murthaja:

- Pengklasifikasi yang dibuat menggunakan fitur yang terkait dengan API calls, DLL injections, registry, and network connections.
- Mencapai akurasi >93% dengan jaringan neural berulang.

Arfeen:

- Menggunakan 15 fitur (9 after selection) dari 900 memory dumps.
- Menggunakan algoritma XGBoost classification untuk mendeteksi ransomware.
- Mencapai akurasi 89%, berfokus pada lima keluarga ransomware dan tiga proses jinak.

Lashkari:

- Mengekstraksi 36 fitur dari memory dumps, yang mencakup berbagai aspek sistem.
- Mencapai 93% true positive rate dan 6,6% false positive rate menggunakan randomized decision trees.
- Limited dataset (1900 samples) to 7 malware families and a few benign samples.
- Kumpulan limited dataset (1900 sampel) untuk 7 keluarga malware dan beberapa sampel jinak.

Computer Vision Approaches

Xu et al. dan Bozkir et al. mengadaptasi metode yang digunakan dalam computer vision ke dalam memory forensic.

	Xu et al.	Bozkir et al.
Data Representation	• Membagi eksekusi program menjadi epoch. • Merangkum pola akses data dengan empat histogram dari akses memori acak. • Histogram mempertimbangkan berbagai jenis akses memori: far calls, near calls, branch instructions, dan load/store instructions.	Merender dump memori dari proses sebagai gambar dengan berbagai skema render.
Feature Set	• Menggunakan histogram sebagai set fitur. • Empat jenis histogram akses memori berfungsi sebagai fitur untuk klasifikasi.	Mengaplikasikan deskriptor fitur visual seperti GIST dan HOG untuk menghitung fitur visual dari gambar yang dirender.

Classifiers	• Membangun klasifikasi menggunakan regresi logistik, support vector machine (SVM), dan random forest. • Mengaplikasikan klasifikasi untuk mendeteksi eksekusi kernel rootkit dan malware korupsi memori tingkat pengguna.	Menggunakan klasifikasi random forest, XGBoost, linear SVM, sequential minimal optimization (SMO), dan J48.
Results	• Mencapai akurasi hampir 100% dalam mendeteksi kernel rootkit dengan tingkat positif palsu kurang dari 1%. • Untuk malware tingkat pengguna, mencapai prediksi positif sejati yang tinggi (88%) dengan tingkat positif palsu yang kecil (1%).	• Memperlakukan masalah sebagai klasifikasi multikelas. • Model terbaik mencapai akurasi tinggi (hingga 96%) dalam memprediksi keluarga malware dari sampel baru.
Unique Contribution	• Memungkinkan sistem deteksi langsung. • Memberikan representasi unik dari data melalui teknik computer vision yang diadaptasi.	Dataset hanya berisi 10 keluarga malware yang berbeda, yang mungkin membatasi generalisabilitas hasil.

Discussion

- Setiap tools yang ada memiliki kekuatan dan kelemahanya tersendiri, dan setiap toolsnya juga memiliki teknik pendekatan yang berbeda-beda.

- Dynamic analysis dan machine learning memiliki pendekatan yang lebih baik dalam malware detection akan tetapi signature scanning adalah teknik yang lebih umum digunakan dikarenakan keakuratan dan performanya, namun rentan terhadap malware yang baru muncul.

- Pendekatan menggunakan machine learning dalam penelitian ini masih menggunakan datset berukuran kecil, ketika menggunakan dataset berukuran besar maka peneliti akan menghadapi time complexity dari machine learning tersebut.

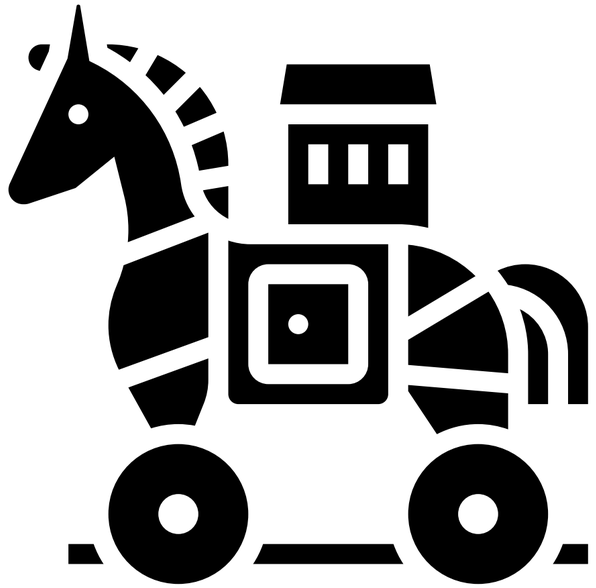
Future Work

- Dalam metode akuisisi dan analisis volatile memory masih harus dikembangkan lagi. Terutama pada pengembangan tools pada system management level yang efisien, atomic, dan aman.
- Penelitan pada machine learning harus dikonfirmasi tingkat efektifitas dari metode ini.
- Volatile memory analysis pada android dan juga IoT.

Conclusion

- Dengan berkembangnya jaman, memory acquisition tools yang diciptakan menjadi beragam untuk OS pada umumnya, akan tetepi tools ini memiliki perbedaan dari berbagai aspek seperti akurasi, kecepatan, dan penggunaanya.
- Volatility sendiri merupakan salah satu acquisition tools yang cukup terkenal dan banyak digunakan.
- Memory forensik termasuk kedalam dynamic analysis baik melalui sandboxing, scanning, ataupun machine learning.
- Sandbox lebih baik dalam menganalisis behavior malware tetapi tidak efektif ketika malware memiliki sandbox evasion code.
- scanning lebih cepat dan mudah dalam pemakaiannya, tetapi tidak dapat mendeteksi malware yang belum pernah muncul dan hanya menganalisis sedikit behaviornya
- Penggunaan machine learning memberikan hasil yang menjanjikan namun harus dicoba kembali dengan dataset yang lebih besar

CRIDEX Memory Analysis.



Step by step

1. Listing all processes and check process tree.
2. Execute malfind plugin.
3. Checks for dll used.
4. Check cmd history.
5. Check network information [Failed in Vola 3].
6. Check network information [Using Vola 2].
7. Dump the malware process (using vola 2 and 3)
8. Upload to Virus Total.

1. Listing all processes and check process tree.

python3 vol.py -f <path_to_file> windows.pslist

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem windows.pslist
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly pr
ocess a VMEM file. These should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A     Disabled
```

1. Listing all processes and check process tree.

python3 vol.py -f <path_to_file> windows.pstree

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem windows.pstree
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly pr
ocess a VMEM file. These should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A
* 368   4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A
** 584  368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A
** 608  368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A
*** 664 608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A
*** 652 608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A
**** 1056       652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A
**** 1220       652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A
**** 1512       652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A
**** 908        652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A
**** 1004       652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A
***** 1136      1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A
***** 1588      1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A
**** 788        652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A
**** 824        652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A
* 1640  1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A
sansforensics@siftworkstation: ~/volatility3
```

2. Execute malfind plugin

python3 vol.py -f <path_to_file> windows.malfind

```
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 e0 00 00 00 ........
0x1460000:      dec     ebp
0x1460001:      pop     edx
0x1460002:      nop
0x1460003:      add     byte ptr [ebx], al
0x1460005:      add     byte ptr [eax], al
0x1460007:      add     byte ptr [eax + eax], al
0x146000a:      add     byte ptr [eax], al
1640    reader_sl.exe   0x3d0000        0x3f0fff        VadS    PAGE_EXECUTE_READWRITE  33      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 e0 00 00 00 ........
0x3d0000:       dec     ebp
0x3d0001:       pop     edx
0x3d0002:       nop
0x3d0003:       add     byte ptr [ebx], al
0x3d0005:       add     byte ptr [eax], al
0x3d0007:       add     byte ptr [eax + eax], al
0x3d000a:       add     byte ptr [eax], al
```

3. Checks for dll used.

python3 vol.py -f <path_to_file> windows.dlllist --pid 1640

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem windows.dlllist --pid 1640
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly pr
ocess a VMEM file. These should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

1640    reader_sl.exe   0x400000        0xa000  Reader_sl.exe   C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe  N/A     Disabled
1640    reader_sl.exe   0x7c900000      0xaf000 ntdll.dll       C:\WINDOWS\system32\ntdll.dll   N/A     Disabled
1640    reader_sl.exe   0x7c800000      0xf6000 kernel32.dll    C:\WINDOWS\system32\kernel32.dll        N/A     Disabled
1640    reader_sl.exe   0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  N/A     Disabled
1640    reader_sl.exe   0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   N/A     Disabled
1640    reader_sl.exe   0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
1640    reader_sl.exe   0x77e70000      0x92000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
1640    reader_sl.exe   0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
1640    reader_sl.exe   0x7c9c0000      0x817000        SHELL32.dll     C:\WINDOWS\system32\SHELL32.dll N/A     Disabled
1640    reader_sl.exe   0x77c10000      0x58000 msvcrt.dll      C:\WINDOWS\system32\msvcrt.dll  N/A     Disabled
1640    reader_sl.exe   0x77f60000      0x76000 SHLWAPI.dll     C:\WINDOWS\system32\SHLWAPI.dll N/A     Disabled
1640    reader_sl.exe   0x7c420000      0x87000 MSVCP80.dll     C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_
6b128700\MSVCP80.dll    N/A     Disabled
1640    reader_sl.exe   0x78130000      0x9b000 MSVCR80.dll     C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_
6b128700\MSVCR80.dll    N/A     Disabled
1640    reader_sl.exe   0x773d0000      0x103000        comctl32.dll    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf
1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll    N/A     Disabled
1640    reader_sl.exe   0x5d090000      0x9a000 comctl32.dll    C:\WINDOWS\system32\comctl32.dll        N/A     Disabled
1640    reader_sl.exe   0x5ad70000      0x38000 uxtheme.dll     C:\WINDOWS\system32\uxtheme.dll N/A     Disabled
1640    reader_sl.exe   0x71ab0000      0x17000 WS2_32.dll      C:\WINDOWS\system32\WS2_32.dll  N/A     Disabled
1640    reader_sl.exe   0x71aa0000      0x8000  WS2HELP.dll     C:\WINDOWS\system32\WS2HELP.dll N/A     Disabled
sansforensics@siftworkstation: ~/volatility3
```

4. Check CMD history.

python3 vol.py -f <path_to_file> windows.cmdline

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem windows.cmdline
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly pr
ocess a VMEM file. These should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x10 is not valid (process exited?)
368     smss.exe        \SystemRoot\System32\smss.exe
584     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows S
erverDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequest
Threads=16
608     winlogon.exe    winlogon.exe
652     services.exe    C:\WINDOWS\system32\services.exe
664     lsass.exe       C:\WINDOWS\system32\lsass.exe
824     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
908     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1004    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1056    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1220    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1484    explorer.exe    C:\WINDOWS\Explorer.EXE
1512    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1640    reader_sl.exe   "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
788     alg.exe C:\WINDOWS\System32\alg.exe
1136    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1
1588    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe"
sansforensics@siftworkstation: ~/volatility3
```

5. Check network information [Failed in Volatility 3].

python3 vol.py -f <path_to_file> windows.netscan

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem windows.netscan
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly pr
ocess a VMEM file. These should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created
Traceback (most recent call last):
  File "vol.py", line 10, in <module>
    volatility3.cli.main()
  File "/home/sansforensics/volatility3/volatility3/cli/__init__.py", line 790, in main
    CommandLine().run()
  File "/home/sansforensics/volatility3/volatility3/cli/__init__.py", line 447, in run
    renderers[args.renderer]().render(constructed.run())
  File "/home/sansforensics/volatility3/volatility3/cli/text_renderer.py", line 193, in render
    grid.populate(visitor, outfd)
  File "/home/sansforensics/volatility3/volatility3/framework/renderers/__init__.py", line 245, in populate
    for level, item in self._generator:
  File "/home/sansforensics/volatility3/volatility3/framework/plugins/windows/netscan.py", line 386, in _generator
    netscan_symbol_table = self.create_netscan_symbol_table(
  File "/home/sansforensics/volatility3/volatility3/framework/plugins/windows/netscan.py", line 338, in create_netscan_symbol_table
    symbol_filename, class_types = cls.determine_tcpip_version(
  File "/home/sansforensics/volatility3/volatility3/framework/plugins/windows/netscan.py", line 304, in determine_tcpip_version
    raise NotImplementedError(
NotImplementedError: This version of Windows is not supported: 5.1 15.2600!
sansforensics@siftworkstation: ~/volatility3
```

6. Check network information in Volatility 2

volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
volatility -f cridex.vmem --profile=WinXPSP2x86 connections

```
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$ volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x02087620 172.16.112.128:1038      41.168.5.140:8080         1484
0x023a8008 172.16.112.128:1037      125.19.103.198:8080       1484
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$ volatility -f cridex.vmem --profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x81e87620 172.16.112.128:1038      41.168.5.140:8080         1484
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$
```

6. Check network information in Volatility 2

volatility -f cridex.vmem --profile=WinXPSP2x86 sockets

```
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$ volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ -------------- --------------- -----------
0x81ddb780      664    500     17 UDP            0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x82240d08     1484   1038      6 TCP            0.0.0.0         2012-07-22 02:44:45 UTC+0000
0x81dd7618     1220   1900     17 UDP            172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x82125610      788   1028      6 TCP            127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x8219cc08        4    445      6 TCP            0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x81ec23b0      908    135      6 TCP            0.0.0.0         2012-07-22 02:42:33 UTC+0000
0x82276878        4    139      6 TCP            172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x82277460        4    137     17 UDP            172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x81e76620     1004    123     17 UDP            127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x82172808      664      0    255 Reserved       0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x81e3f460        4    138     17 UDP            172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x821f0630     1004    123     17 UDP            172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x822cd2b0     1220   1900     17 UDP            127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x82172c50      664   4500     17 UDP            0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x821f0d00        4    445     17 UDP            0.0.0.0         2012-07-22 02:42:31 UTC+0000
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$
```

7. Dump the malware process in Volatility 3.

python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem -o ../Downloads/compforen/cridex_memdump/ windows.dumpfiles --pid 1640

```
sansforensics@siftworkstation: ~/volatility3
$ python3 vol.py -f ../Downloads/compforen/cridex_memdump/cridex.vmem -o ../Downloads/compforen/cridex_memdump/ windows.dumpfiles --pid 1640
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These
should be placed in the same directory with the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x821ccf90      reader_sl.exe   file.0x821ccf90.0x822116f0.DataSectionObject.reader_sl.exe.dat
ImageSectionObject      0x821ccf90      reader_sl.exe   file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe.img
ImageSectionObject      0x81e38f90      kernel32.dll    file.0x81e38f90.0x82233008.ImageSectionObject.kernel32.dll.img
ImageSectionObject      0x82239890      advapi32.dll    file.0x82239890.0x82201250.ImageSectionObject.advapi32.dll.img
ImageSectionObject      0x81eb4768      msvcrt.dll      file.0x81eb4768.0x820d0008.ImageSectionObject.msvcrt.dll.img
ImageSectionObject      0x81eb4908      comctl32.dll    file.0x81eb4908.0x82308818.ImageSectionObject.comctl32.dll.img
ImageSectionObject      0x81e31800      uxtheme.dll     file.0x81e31800.0x822213b0.ImageSectionObject.uxtheme.dll.img
ImageSectionObject      0x82076110      comctl32.dll    file.0x82076110.0x82076008.ImageSectionObject.comctl32.dll.img
ImageSectionObject      0x8214be50      ws2_32.dll      file.0x8214be50.0x820d2d60.ImageSectionObject.ws2_32.dll.img
ImageSectionObject      0x8214bdb8      ws2help.dll     file.0x8214bdb8.0x81ec0c78.ImageSectionObject.ws2help.dll.img
ImageSectionObject      0x81eb9808      gdi32.dll       file.0x81eb9808.0x82239990.ImageSectionObject.gdi32.dll.img
ImageSectionObject      0x820d09c0      rpcrt4.dll      file.0x820d09c0.0x82307688.ImageSectionObject.rpcrt4.dll.img
ImageSectionObject      0x81eb43b8      secur32.dll     file.0x81eb43b8.0x822502f8.ImageSectionObject.secur32.dll.img
ImageSectionObject      0x81eb4838      shlwapi.dll     file.0x81eb4838.0x81e84008.ImageSectionObject.shlwapi.dll.img
DataSectionObject       0x8226d8d8      msvcp80.dll     file.0x8226d8d8.0x820d2c70.DataSectionObject.msvcp80.dll.dat
ImageSectionObject      0x8226d8d8      msvcp80.dll     file.0x8226d8d8.0x8226d7c0.ImageSectionObject.msvcp80.dll.img
DataSectionObject       0x821cfb68      msvcr80.dll     file.0x821cfb68.0x820d2910.DataSectionObject.msvcr80.dll.dat
ImageSectionObject      0x821cfb68      msvcr80.dll     file.0x821cfb68.0x821cfa50.ImageSectionObject.msvcr80.dll.img
ImageSectionObject      0x8233f5e0      ntdll.dll       file.0x8233f5e0.0x823c72d8.ImageSectionObject.ntdll.dll.img
ImageSectionObject      0x82225de0      user32.dll      file.0x82225de0.0x82261cc0.ImageSectionObject.user32.dll.img
DataSectionObject       0x820d08b0      shell32.dll     file.0x820d08b0.0x8232dbc0.DataSectionObject.shell32.dll.dat
ImageSectionObject      0x820d08b0      shell32.dll     file.0x820d08b0.0x82261e90.ImageSectionObject.shell32.dll.img
DataSectionObject       0x82210a48      shell32.dll     file.0x82210a48.0x8232dbc0.DataSectionObject.shell32.dll.dat
ImageSectionObject      0x82210a48      shell32.dll     file.0x82210a48.0x82261e90.ImageSectionObject.shell32.dll.img
sansforensics@siftworkstation: ~/volatility3
```

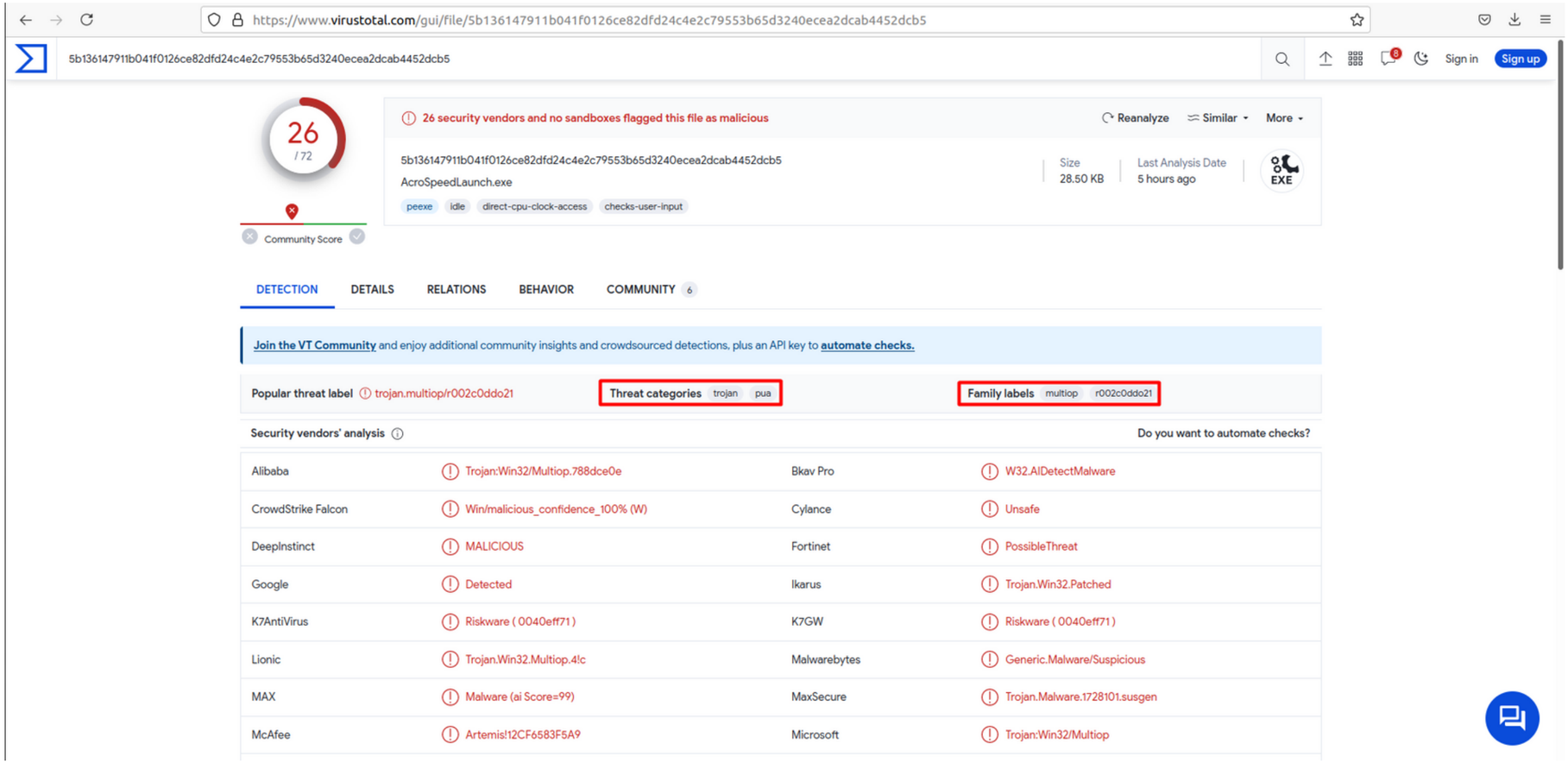
7. Dump the malware process in Volatility 2.

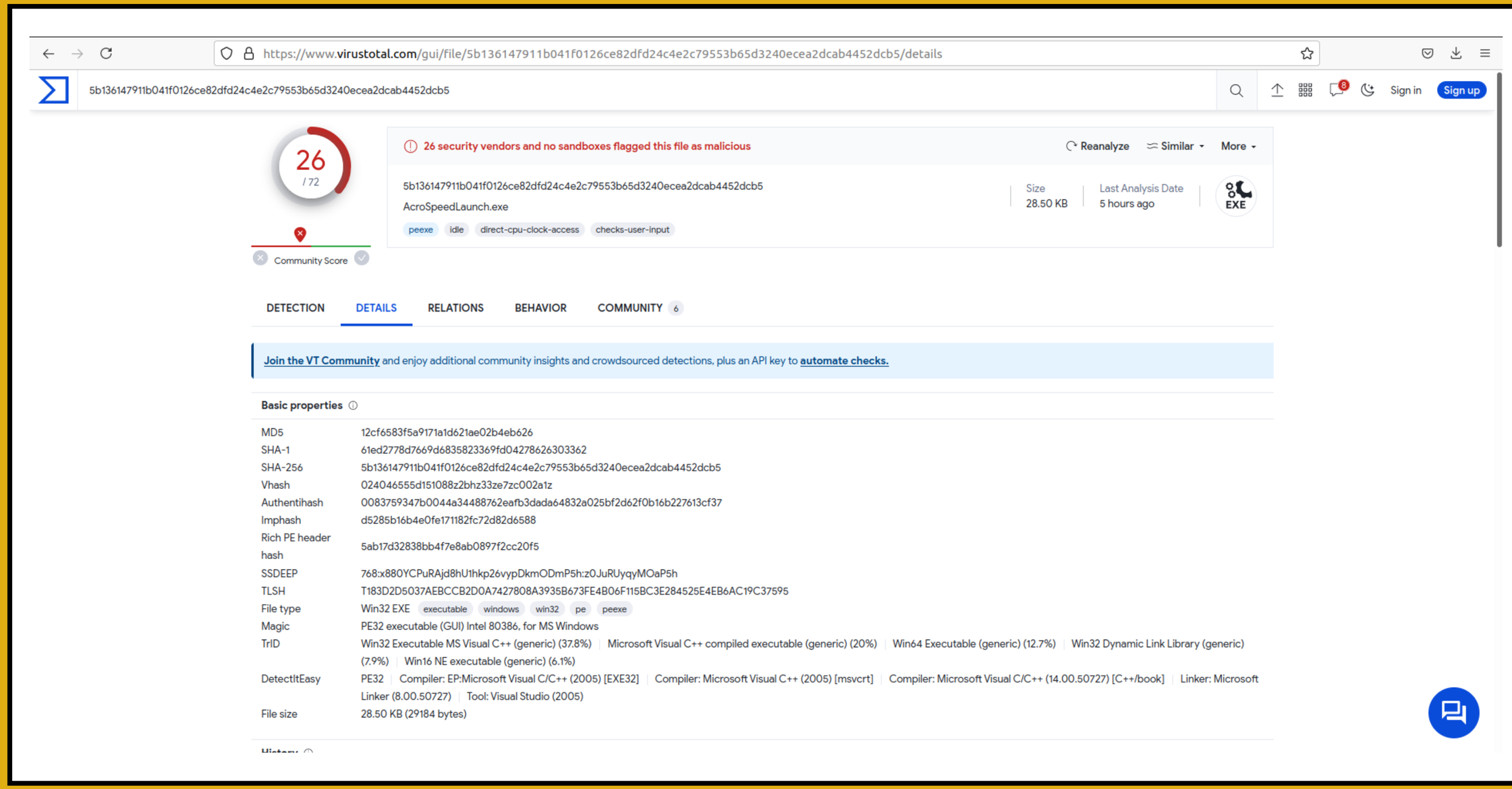
volatility -f cridex.vmem --profile=WinXPSP2x86 procdump -p 1640 --dump-dir=.

```
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
$ volatility -f cridex.vmem --profile=WinXPSP2x86 procdump -p 1640 --dump-dir=.
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81e7bda0 0x00400000 reader_sl.exe        OK: executable.1640.exe
sansforensics@siftworkstation: ~/Downloads/compforen/cridex_memdump
```

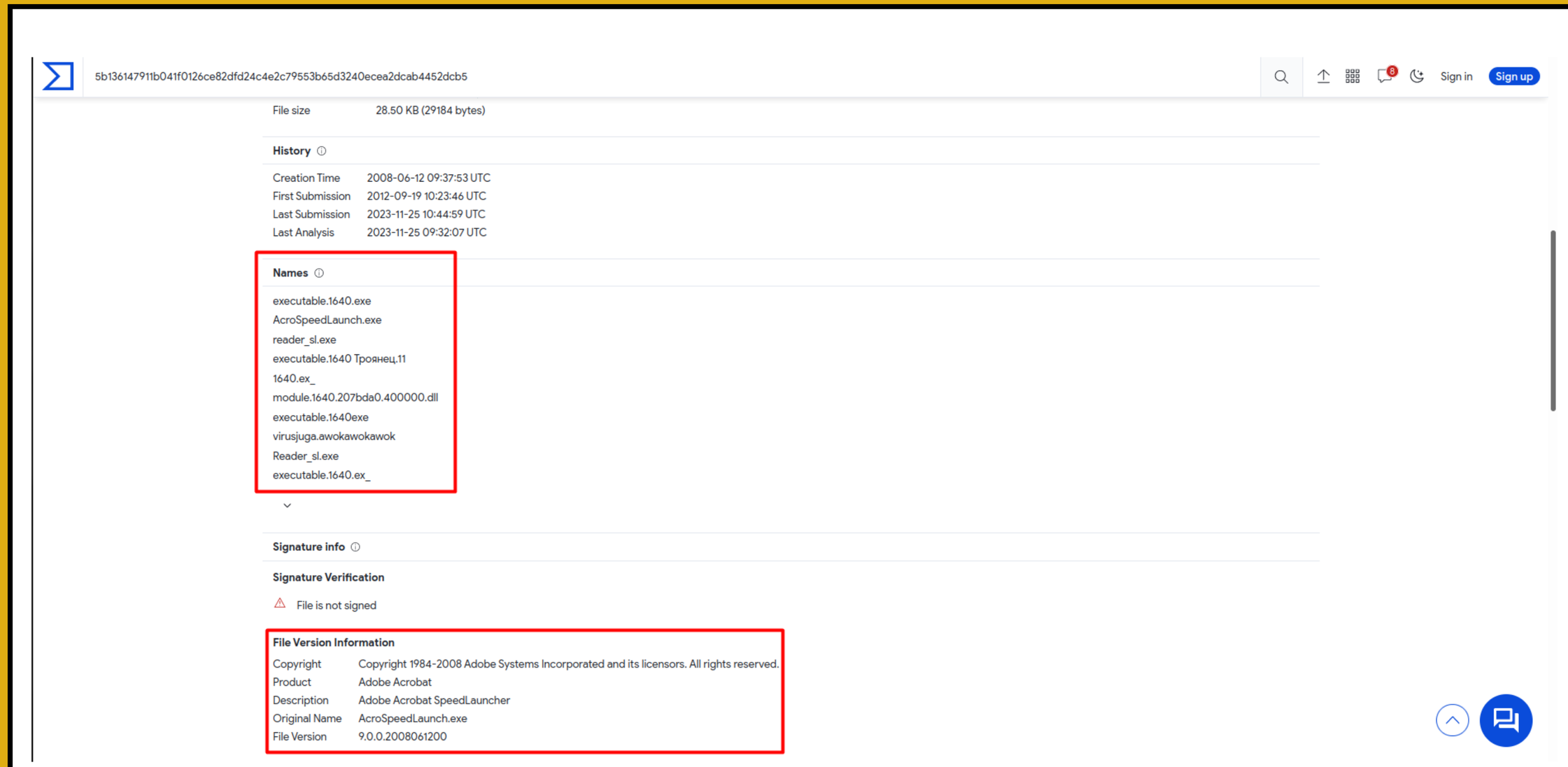
8. Upload to virus total.

https://www.virustotal.com/gui/file/5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5



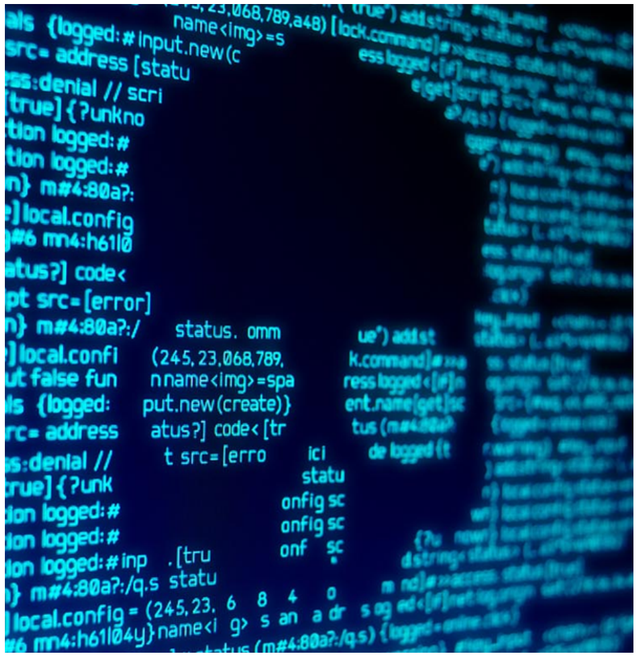


Cridex Memory Analysis



Cridex Memory Analysis

SHYLock Memory Analysis.



Step by step

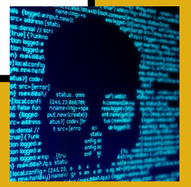
1. Listing all processes and check process tree.
2. Execute malfind plugin.
3. Checks for dll used.
4. Check cmd history.
5. Dump the malware process
6. Upload to Virus Total.

1. List All tree and processes

python3 vol.py -f [file] windows.pslist

```
arkoov@Ark:~/Desktop/volatility3$ python3 vol.py -f ../Binus/Forensics/shylock.vmem windows.pslist
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required
ylock.vmem and shylock.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime    File outpu

4       0       System  0x819cc830      60      209     N/A     False   N/A     N/A     Disabled
384     4       smss.exe        0x818efda0      3       19      N/A     False   2011-09-26 01:33:32.000000      N/A Disabled
612     384     csrss.exe       0x81616ab8      12      473     0       False   2011-09-26 01:33:35.000000      N/A Disabled
636     384     winlogon.exe    0x814c9b40      16      498     0       False   2011-09-26 01:33:35.000000      N/A Disabled
680     636     services.exe    0x81794d08      15      271     0       False   2011-09-26 01:33:35.000000      N/A Disabled
692     636     lsass.exe       0x814a2cd0      24      356     0       False   2011-09-26 01:33:35.000000      N/A Disabled
852     680     vmacthlp.exe    0x815c2630      1       25      0       False   2011-09-26 01:33:35.000000      N/A Disabled
868     680     svchost.exe     0x81470020      17      199     0       False   2011-09-26 01:33:35.000000      N/A Disabled
944     680     svchost.exe     0x818b5248      11      274     0       False   2011-09-26 01:33:36.000000      N/A Disabled
1040    680     MsMpEng.exe     0x813a0458      16      322     0       False   2011-09-26 01:33:36.000000      N/A Disabled
1076    680     svchost.exe     0x816b7020      87      1477    0       False   2011-09-26 01:33:36.000000      N/A Disabled
1200    680     svchost.exe     0x817f7548      6       81      0       False   2011-09-26 01:33:37.000000      N/A Disabled
1336    680     svchost.exe     0x8169a1d0      14      172     0       False   2011-09-26 01:33:37.000000      N/A Disabled
1516    680     spoolsv.exe     0x813685e0      14      159     0       False   2011-09-26 01:33:39.000000      N/A Disabled
1752    1696    explorer.exe    0x818f5cd0      32      680     0       False   2011-09-26 01:33:45.000000      N/A Disabled
1812    680     svchost.exe     0x815c9638      4       102     0       False   2011-09-26 01:33:46.000000      N/A Disabled
1876    1752    VMwareTray.exe  0x8192d7f0      3       84      0       False   2011-09-26 01:33:46.000000      N/A Disabled
1888    1752    VMwareUser.exe  0x818f6458      9       245     0       False   2011-09-26 01:33:47.000000      N/A Disabled
1900    1752    msseces.exe     0x8164a020      11      205     0       False   2011-09-26 01:33:47.000000      N/A Disabled
1912    1752    ctfmon.exe      0x81717370      3       93      0       False   2011-09-26 01:33:47.000000      N/A Disabled
2000    680     svchost.exe     0x813a5b28      6       119     0       False   2011-09-26 01:33:47.000000      N/A Disabled
200     680     vmtoolsd.exe    0x81336638      5       234     0       False   2011-09-26 01:33:47.000000      N/A Disabled
424     680     VMUpgradeHelper 0x81329b28      5       100     0       False   2011-09-26 01:33:48.000000      N/A Disabled
2028    1076    wscntfy.exe     0x812d6020      3       63      0       False   2011-09-26 01:33:55.000000      N/A Disabled
2068    680     TPAutoConnSvc.e 0x812c1718      5       99      0       False   2011-09-26 01:33:55.000000      N/A Disabled
2272    680     alg.exe 0x812b03e0      7       112     0       False   2011-09-26 01:33:55.000000      N/A     Disabled
3372    2068    TPAutoConnect.e 0x81324020      3       90      0       False   2011-09-26 01:33:59.000000      N/A Disabled
2396    680     msiexec.exe     0x814e7b38      5       127     0       False   2011-09-26 01:34:45.000000      N/A Disabled
3756    1752    cmd.exe 0x814db608      3       56      0       False   2011-09-30 00:20:44.000000      N/A     Disabled
3128    200     cmd.exe 0x812f59a8      0       -       0       False   2011-09-30 00:26:30.000000      2011-09-30 00:26:30.00
```

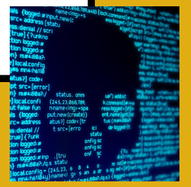


1. List All tree and processes

python3 vol.py -f [file] windows.pstree

```
arkoov@Ark:~/Desktop/volatility3$ python3 vol.py -f ../Binus/Forensics/shylock.vmem windows.pstree
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be re
ylock.vmem and shylock.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x819cc830      60      209     N/A     False   N/A     N/A
* 384   4       smss.exe        0x818efda0      3       19      N/A     False   2011-09-26 01:33:32.000000      N/A
** 636  384     winlogon.exe    0x814c9b40      16      498     0       False   2011-09-26 01:33:35.000000      N/A
*** 680 636     services.exe    0x81794d08      15      271     0       False   2011-09-26 01:33:35.000000      N/A
**** 2272       680     alg.exe 0x812b03e0      7       112     0       False   2011-09-26 01:33:55.000000      N/A
**** 868        680     svchost.exe     0x81470020      17      199     0       False   2011-09-26 01:33:35.000000
**** 200        680     vmtoolsd.exe    0x81336638      5       234     0       False   2011-09-26 01:33:47.000000
***** 3128      200     cmd.exe 0x812f59a8      0       -       0       False   2011-09-30 00:26:30.000000      2011-09
**** 424        680     VMUpgradeHelper 0x81329b28      5       100     0       False   2011-09-26 01:33:48.000000
**** 1516       680     spoolsv.exe     0x813685e0      14      159     0       False   2011-09-26 01:33:39.000000
**** 1040       680     MsMpEng.exe     0x813a0458      16      322     0       False   2011-09-26 01:33:36.000000
**** 944        680     svchost.exe     0x818b5248      11      274     0       False   2011-09-26 01:33:36.000000
**** 1200       680     svchost.exe     0x817f7548      6       81      0       False   2011-09-26 01:33:37.000000
**** 2000       680     svchost.exe     0x813a5b28      6       119     0       False   2011-09-26 01:33:47.000000
**** 852        680     vmacthlp.exe    0x815c2630      1       25      0       False   2011-09-26 01:33:35.000000
**** 1076       680     svchost.exe     0x816b7020      87      1477    0       False   2011-09-26 01:33:36.000000
***** 2028      1076    wscntfy.exe     0x812d6020      3       63      0       False   2011-09-26 01:33:55.000000
**** 1812       680     svchost.exe     0x815c9638      4       102     0       False   2011-09-26 01:33:46.000000
**** 2068       680     TPAutoConnSvc.e 0x812c1718      5       99      0       False   2011-09-26 01:33:55.000000
***** 3372      2068    TPAutoConnect.e 0x81324020      3       90      0       False   2011-09-26 01:33:59.000000
**** 1336       680     svchost.exe     0x8169a1d0      14      172     0       False   2011-09-26 01:33:37.000000
**** 2396       680     msiexec.exe     0x814e7b38      5       127     0       False   2011-09-26 01:34:45.000000
*** 692 636     lsass.exe       0x814a2cd0      24      356     0       False   2011-09-26 01:33:35.000000      N/A
** 612  384     csrss.exe       0x81616ab8      12      473     0       False   2011-09-26 01:33:35.000000      N/A
1752    1696    explorer.exe    0x818f5cd0      32      680     0       False   2011-09-26 01:33:45.000000      N/A
* 1888  1752    VMwareUser.exe  0x818f6458      9       245     0       False   2011-09-26 01:33:47.000000      N/A
* 1900  1752    msseces.exe     0x8164a020      11      205     0       False   2011-09-26 01:33:47.000000      N/A
* 3756  1752    cmd.exe 0x814db608      3       56      0       False   2011-09-30 00:20:44.000000      N/A
* 1876  1752    VMwareTray.exe  0x8192d7f0      3       84      0       False   2011-09-26 01:33:46.000000      N/A
* 1912  1752    ctfmon.exe      0x81717370      3       93      0       False   2011-09-26 01:33:47.000000      N/A
```



2. Execute Malfind Plugin

python3 vol.py -f [file] windows.malfind

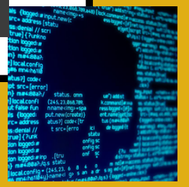
```
1752    explorer.exe    0x36e0000       0x3776fff       VadS    PAGE_EXECUTE_READWRITE  151     1
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 56 03 00 20 09 00 ..V.....
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 01 00 00 ........
0x36e0000:      dec     ebp
0x36e0001:      pop     edx
0x36e0002:      nop
0x36e0003:      add     byte ptr [ebx], al
0x36e0005:      add     byte ptr [eax], al
0x36e0007:      add     byte ptr [eax + eax], al
0x36e000a:      add     byte ptr [eax], al
```

3. Checks for dll used.

python3 vol.py -f [file] windows.dlllist

```
arkoov@Ark:~/Desktop/volatility3$ python3 vol.py -f ../Binus/Forensics/shylock.vmem windows.dlllist --pid 1752
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to c
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

1752    explorer.exe    0x1000000       0xff000 Explorer.EXE    C:\WINDOWS\Explorer.EXE N/A     Disabled
1752    explorer.exe    0x7c900000      0xb2000 ntdll.dll       C:\WINDOWS\system32\ntdll.dll   N/A     Disabled
1752    explorer.exe    0x7c800000      0xf6000 kernel32.dll    C:\WINDOWS\system32\kernel32.dll        N/A     Disabled
1752    explorer.exe    0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
1752    explorer.exe    0x77e70000      0x93000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
1752    explorer.exe    0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
1752    explorer.exe    0x75f80000      0xfd000 BROWSEUI.dll    C:\WINDOWS\system32\BROWSEUI.dll        N/A     Disabled
1752    explorer.exe    0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   N/A     Disabled
1752    explorer.exe    0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  N/A     Disabled
1752    explorer.exe    0x77c10000      0x58000 msvcrt.dll      C:\WINDOWS\system32\msvcrt.dll  N/A     Disabled
1752    explorer.exe    0x774e0000      0x13e000        ole32.dll       C:\WINDOWS\system32\ole32.dll   N/A     Disabled
1752    explorer.exe    0x77f60000      0x76000 SHLWAPI.dll     C:\WINDOWS\system32\SHLWAPI.dll N/A     Disabled
1752    explorer.exe    0x77120000      0x8b000 OLEAUT32.dll    C:\WINDOWS\system32\OLEAUT32.dll        N/A     Disabled
1752    explorer.exe    0x7e290000      0x173000        SHDOCVW.dll     C:\WINDOWS\system32\SHDOCVW.dll N/A     Disabled
1752    explorer.exe    0x77a80000      0x95000 CRYPT32.dll     C:\WINDOWS\system32\CRYPT32.dll N/A     Disabled
1752    explorer.exe    0x77b20000      0x12000 MSASN1.dll      C:\WINDOWS\system32\MSASN1.dll  N/A     Disabled
1752    explorer.exe    0x754d0000      0x80000 CRYPTUI.dll     C:\WINDOWS\system32\CRYPTUI.dll N/A     Disabled
1752    explorer.exe    0x5b860000      0x55000 NETAPI32.dll    C:\WINDOWS\system32\NETAPI32.dll        N/A     Disabled
1752    explorer.exe    0x77c00000      0x8000  VERSION.dll     C:\WINDOWS\system32\VERSION.dll N/A     Disabled
1752    explorer.exe    0x3d930000      0xd1000 WININET.dll     C:\WINDOWS\system32\WININET.dll N/A     Disabled
```

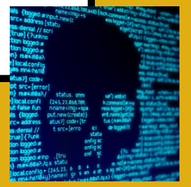


4. Check cmd history.

python3 vol.py -f [file] windows.cmdline

```
arkoov@Ark:~/Desktop/volatility3$ python3 vol.py -f ../Binus/Forensics/shylock.vmem windows.cmdline
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or V
. These should be placed in the same directory with the same file name, e.g. shylock.vmem and shylock
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x10 is not valid (process exited?)
384     smss.exe        \SystemRoot\System32\smss.exe
612     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,307
1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 Profil
636     winlogon.exe    winlogon.exe
680     services.exe    C:\WINDOWS\system32\services.exe
692     lsass.exe       C:\WINDOWS\system32\lsass.exe
852     vmacthlp.exe    "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
868     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
944     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1040    MsMpEng.exe     "c:\Program Files\Microsoft Security Essentials\MsMpEng.exe"
1076    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1200    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1336    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1516    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1752    explorer.exe    C:\WINDOWS\Explorer.EXE
1812    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1876    VMwareTray.exe  "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
1888    VMwareUser.exe  "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
1900    msseces.exe     "C:\Program Files\Microsoft Security Essentials\msseces.exe" -hide -runkey
1912    ctfmon.exe      "C:\WINDOWS\system32\ctfmon.exe"
2000    svchost.exe     C:\WINDOWS\system32\svchost.exe -k imgsvc
200     vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
424     VMUpgradeHelper "C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe" /service
2028    wscntfy.exe     C:\WINDOWS\system32\wscntfy.exe
2068    TPAutoConnSvc.e "C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe"
2272    alg.exe C:\WINDOWS\System32\alg.exe
3372    TPAutoConnect.e TPAutoConnect.exe -q -i vmware -a COM1 -F 30
2396    msiexec.exe     C:\WINDOWS\system32\msiexec.exe /V
3756    cmd.exe "C:\WINDOWS\system32\cmd.exe"
3128    cmd.exe Required memory at 0x7ffd5010 is not valid (process exited?)
```



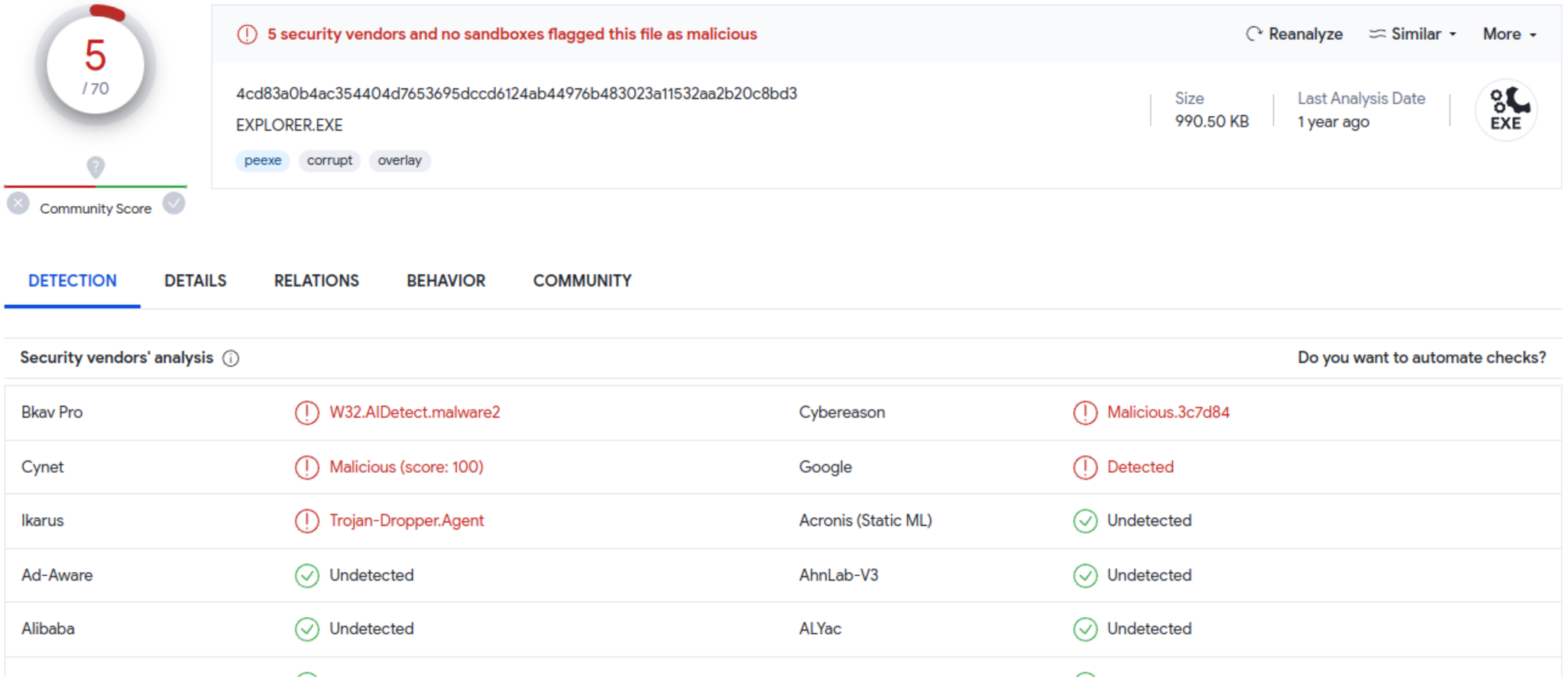
5. Dump Malicious Process

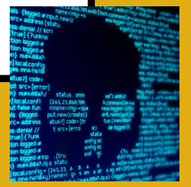
python3 vol.py -f <file> windows.dumpfiles --pid <pid>

```
arkoov@Ark:~/Desktop/volatility3$ python3 vol.py -f ../Binus/Forensics/shylock.vmem windows.dumpfiles --pid 1752
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be require
. These should be placed in the same directory with the same file name, e.g. shylock.vmem and shylock.vmss.
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x8170deb8      4e7fd67a        Error dumping file
SharedCacheMap  0x8170deb8      4e7fd67a        file.0x8170deb8.0x81809360.SharedCacheMap.4e7fd67a.vacb
DataSectionObject       0x815b01f0      index.dat       file.0x815b01f0.0x81713958.DataSectionObject.index.dat.dat
DataSectionObject       0x81620540      index.dat       Error dumping file
DataSectionObject       0x815c1f00      index.dat       file.0x815c1f00.0x814a5008.DataSectionObject.index.dat.dat
ImageSectionObject      0x817aa628      DropboxExt.13.dll       file.0x817aa628.0x81714b90.ImageSectionObject.DropboxExt.13.
ImageSectionObject      0x8149af30      normaliz.dll    file.0x8149af30.0x81808550.ImageSectionObject.normaliz.dll.img
ImageSectionObject      0x817255d8      explorer.exe    file.0x817255d8.0x818ee930.ImageSectionObject.explorer.exe.img
ImageSectionObject      0x815b1eb8      xpsp2res.dll    file.0x815b1eb8.0x8170aef0.ImageSectionObject.xpsp2res.dll.img
ImageSectionObject      0x81922e20      vmhgfs.dll      file.0x81922e20.0x81922e98.ImageSectionObject.vmhgfs.dll.img
DataSectionObject       0x81884350      index.dat       Error dumping file
DataSectionObject       0x817aa798      index.dat       file.0x817aa798.0x81713958.DataSectionObject.index.dat.dat
DataSectionObject       0x817977a8      index.dat       file.0x817977a8.0x814a5008.DataSectionObject.index.dat.dat
DataSectionObject       0x812d5cf0      urlmon.dll.mui  Error dumping file
DataSectionObject       0x8131ef90      hgfs.dat        Error dumping file
ImageSectionObject      0x81674028      kernel32.dll    file.0x81674028.0x8192f6a0.ImageSectionObject.kernel32.dll.img
ImageSectionObject      0x816149c0      netapi32.dll    file.0x816149c0.0x815c8f08.ImageSectionObject.netapi32.dll.img
ImageSectionObject      0x816523f8      wininet.dll     file.0x816523f8.0x81945a68.ImageSectionObject.wininet.dll.img
ImageSectionObject      0x8149ad60      iertutil.dll    file.0x8149ad60.0x8161f638.ImageSectionObject.iertutil.dll.img
ImageSectionObject      0x8187f5e8      uxtheme.dll     file.0x8187f5e8.0x8161c7a8.ImageSectionObject.uxtheme.dll.img
```

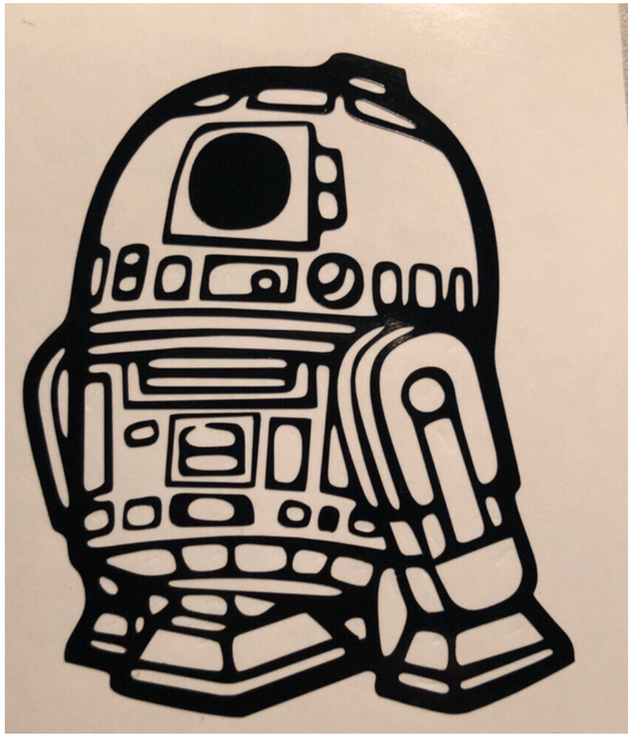
6. Test to Virus Total





ShyLock Memory Analysis

R2D2 memory analysis



Step by step

1. Check using volatility3 **[Failed]**
2. Check **profile**
3. Check **process list** & **process tree**
4. Check **cmdscan**
5. Check **connscan**
6. **Dump** the malware
7. Upload to **Virus Total**

1. Check using volatility3 [Failed]

python3 vol.py -f [file] windows.pslist

```
┌──(plasma㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f /home/plasma/Desktop/0zapftis.vmem windows.pslist
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file m
ay be required to correctly process a VMEM file. These should be placed in the same directory with the same fil
e name, e.g. 0zapftis.vmem and 0zapftis.vmss.
WARNING  volatility3.framework.plugins: Automagic exception occurred: ValueError: Symbol type not in symbol_tab
le_name1 SymbolTable: _ETHREAD

Unsatisfied requirement plugins.PsList.kernel.symbol_table_name:

A symbol table requirement was not fulfilled.  Please verify that:
        The associated translation layer requirement was fulfilled
        You have the correct symbol file for the requirement
        The symbol file is under the correct directory or zip file
        The symbol file is named appropriately or contains the correct banner

Unable to validate the plugin requirements: ['plugins.PsList.kernel.symbol_table_name']
```

2. Check profile

python2 vol.py -f [file] imageinfo

```
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/plasma/Desktop/0zapftis.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-10-10 17:06:54 UTC+0000
     Image local date and time : 2011-10-10 13:06:54 -0400
```


3. Check process list

python2 vol.py -f [file] --profile=WinXPSPS2x86 pslist

python2 vol.py -f [file] --profile=WinXPSPS2x86 pstree

```
┌──(plasma㉿kali)-[~/Desktop/volatility]
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x819cc830 System                    4      0     55      162 ------      0
0x81945020 smss.exe                536      4      3       21 ------      0 2011-10-10 17:03:56 UTC+0000
0x816c6020 csrss.exe               608    536     11      355      0      0 2011-10-10 17:03:58 UTC+0000
0x813a9020 winlogon.exe            632    536     24      533      0      0 2011-10-10 17:03:58 UTC+0000
0x816da020 services.exe            676    632     16      261      0      0 2011-10-10 17:03:58 UTC+0000
0x813c4020 lsass.exe               688    632     23      336      0      0 2011-10-10 17:03:58 UTC+0000
0x81772ca8 vmacthlp.exe            832    676      1       24      0      0 2011-10-10 17:03:59 UTC+0000
0x8167e9d0 svchost.exe             848    676     20      194      0      0 2011-10-10 17:03:59 UTC+0000
0x817757f0 svchost.exe             916    676      9      217      0      0 2011-10-10 17:03:59 UTC+0000
0x816c6da0 svchost.exe             964    676     63     1058      0      0 2011-10-10 17:03:59 UTC+0000
0x815daca8 svchost.exe            1020    676      5       58      0      0 2011-10-10 17:03:59 UTC+0000
0x813aeda0 svchost.exe            1148    676     12      187      0      0 2011-10-10 17:04:00 UTC+0000
0x817937e0 spoolsv.exe            1260    676     13      140      0      0 2011-10-10 17:04:00 UTC+0000
0x81754990 VMwareService.e        1444    676      3      145      0      0 2011-10-10 17:04:00 UTC+0000
0x8136c5a0 alg.exe                1616    676      7       99      0      0 2011-10-10 17:04:01 UTC+0000
0x815c4da0 wscntfy.exe            1920    964      1       27      0      0 2011-10-10 17:04:39 UTC+0000
0x813bcda0 explorer.exe           1956   1884     18      322      0      0 2011-10-10 17:04:39 UTC+0000
0x816d63d0 VMwareTray.exe          184   1956      1       28      0      0 2011-10-10 17:04:41 UTC+0000
0x8180b478 VMwareUser.exe          192   1956      6       83      0      0 2011-10-10 17:04:41 UTC+0000
0x818233c8 reader_sl.exe           228   1956      2       26      0      0 2011-10-10 17:04:41 UTC+0000
0x815e7be0 wuauclt.exe             400    964      8      173      0      0 2011-10-10 17:04:46 UTC+0000
0x817a34b0 cmd.exe                 544   1956      1       30      0      0 2011-10-10 17:06:42 UTC+0000
```

```
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x819cc830:System                                     4      0     55    162 1970-01-01 00:00:00 UTC+0000
. 0x81945020:smss.exe                                536      4      3     21 2011-10-10 17:03:56 UTC+0000
.. 0x816c6020:csrss.exe                              608    536     11    355 2011-10-10 17:03:58 UTC+0000
.. 0x813a9020:winlogon.exe                           632    536     24    533 2011-10-10 17:03:58 UTC+0000
... 0x816da020:services.exe                          676    632     16    261 2011-10-10 17:03:58 UTC+0000
.... 0x817757f0:svchost.exe                          916    676      9    217 2011-10-10 17:03:59 UTC+0000
.... 0x81772ca8:vmacthlp.exe                         832    676      1     24 2011-10-10 17:03:59 UTC+0000
.... 0x816c6da0:svchost.exe                          964    676     63   1058 2011-10-10 17:03:59 UTC+0000
..... 0x815c4da0:wscntfy.exe                        1920    964      1     27 2011-10-10 17:04:39 UTC+0000
..... 0x815e7be0:wuauclt.exe                         400    964      8    173 2011-10-10 17:04:46 UTC+0000
.... 0x8167e9d0:svchost.exe                          848    676     20    194 2011-10-10 17:03:59 UTC+0000
.... 0x81754990:VMwareService.e                     1444    676      3    145 2011-10-10 17:04:00 UTC+0000
.... 0x8136c5a0:alg.exe                             1616    676      7     99 2011-10-10 17:04:01 UTC+0000
.... 0x813aeda0:svchost.exe                         1148    676     12    187 2011-10-10 17:04:00 UTC+0000
.... 0x817937e0:spoolsv.exe                         1260    676     13    140 2011-10-10 17:04:00 UTC+0000
.... 0x815daca8:svchost.exe                         1020    676      5     58 2011-10-10 17:03:59 UTC+0000
... 0x813c4020:lsass.exe                             688    632     23    336 2011-10-10 17:03:58 UTC+0000
 0x813bcda0:explorer.exe                            1956   1884     18    322 2011-10-10 17:04:39 UTC+0000
. 0x8180b478:VMwareUser.exe                          192   1956      6     83 2011-10-10 17:04:41 UTC+0000
. 0x817a34b0:cmd.exe                                 544   1956      1     30 2011-10-10 17:06:42 UTC+0000
. 0x816d63d0:VMwareTray.exe                          184   1956      1     28 2011-10-10 17:04:41 UTC+0000
. 0x818233c8:reader_sl.exe                           228   1956      2     26 2011-10-10 17:04:41 UTC+0000
```

4. Check cmdscan

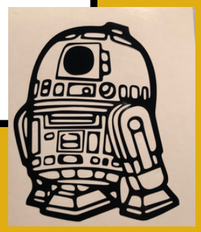
python2 vol.py -f [file] --profile=WinXPSPS2x86 cmdscan

```
┌──(plasma㉿kali)-[~/Desktop/volatility]
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem --profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0x11132d8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x4c4
Cmd #0 @ 0x4e1eb8: sc query malwar
Cmd #1 @ 0x11135e8: sc query malware
```

5. Check connscan

python2 vol.py -f [file] --profile=WinXPSPS2x86 connscan

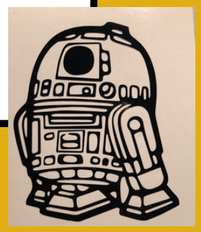
```
┌──(plasma㉿kali)-[~/Desktop/volatility]
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01a25a50 0.0.0.0:1026              172.16.98.1:6666          1956
```

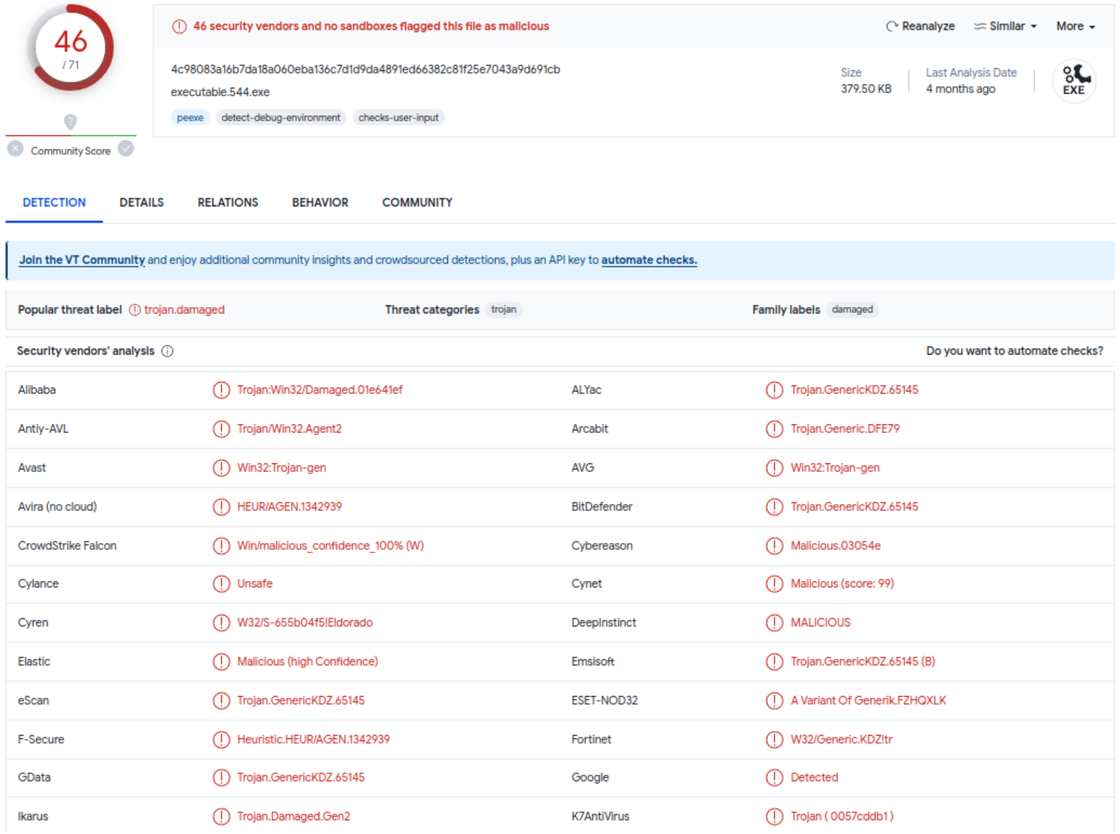
6. Dump the malware

python2 vol.py -f [file] --profile=WinXPSPS2x86 procdump -p 544 --dump-dir .

```
└─$ python2 vol.py -f /home/plasma/Desktop/0zapftis.vmem --profile=WinXPSP2x86 procdump -p 544 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
────────── ────────── ──────────────────── ──────
0x817a34b0 0x4ad00000 cmd.exe              OK: executable.544.exe
```



7. Upload to Virus Total



46 / 71

Community Score

46 security vendors and no sandboxes flagged this file as malicious

Reanalyze · Similar · More

4c98083a16b7da18a060eba136c7d1d9da4891ed66382c81f25e7043a9d691cb

executable.544.exe

peexe · detect-debug-environment · checks-user-input

Size 379.50 KB | Last Analysis Date 4 months ago | EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.damaged | Threat categories: trojan | Family labels: damaged

Security vendors' analysis — Do you want to automate checks?

Alibaba	Trojan:Win32/Damaged.01e641ef	ALYac	Trojan.GenericKDZ.65145
Antiy-AVL	Trojan/Win32.Agent2	Arcabit	Trojan.Generic.DFE79
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	HEUR/AGEN.1342939	BitDefender	Trojan.GenericKDZ.65145
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.03054e
Cylance	Unsafe	Cynet	Malicious (score: 99)
Cyren	W32/S-655b04f5!Eldorado	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKDZ.65145 (B)
eScan	Trojan.GenericKDZ.65145	ESET-NOD32	A Variant Of Generik.FZHQXLK
F-Secure	Heuristic.HEUR/AGEN.1342939	Fortinet	W32/Generic.KDZ!tr
GData	Trojan.GenericKDZ.65145	Google	Detected
Ikarus	Trojan.Damaged.Gen2	K7AntiVirus	Trojan (0057cddb1)

Basic properties

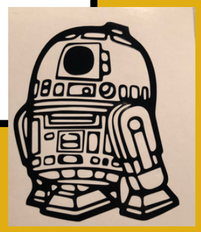
MD5	6cee14703054e226e87a963372f767aa
SHA-1	4f1608147a171da8934ff0731aea53acee1e820b
SHA-256	4c98083a16b7da18a060eba136c7d1d9da4891ed66382c81f25e7043a9d691cb
Vhash	0350361d151az7049lz4fz
Authentihash	c144fe906c542ed211e7e4253bacbcaa307f54aee2fb72b21f949eb63d57961a
Imphash	a6e4db6d0301308509a7f5737a79f454
Rich PE header hash	5cc43b360694cd46cac03c4e1fca30b6
SSDEEP	1536:arcS2L72fsoex7hwXG1blazEfo2KMMrK78l3s4E:l2voeN4G17Ef5KlrK78l3s4E
TLSH	T1B5844A11B3A1A473D6E2257019A933718A7DFC75852E96CBF950CA2CE874D80DB28F1E
File type	Win32 EXE · executable · windows · win32 · pe · peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) · Microsoft Visual C++ compiled executable (generic) (20%) · Win64 Executable (generic) (12.7%) · Win32 Dynamic Link Library (generic) (7.9%) · Win16 NE executable (generic) (6.1%)
DetectItEasy	PE32 · Compiler: Microsoft Visual C/C++ (2003) · Linker: Microsoft Linker (7.10*) [Console32,console]
File size	379.50 KB (388608 bytes)
PEiD packer	Microsoft Visual C++ v7.1 EXE

History

Creation Time	2004-08-04 06:14:22 UTC
First Seen In The Wild	2018-07-04 10:25:36 UTC
First Submission	2017-09-25 12:59:33 UTC
Last Submission	2023-11-25 10:11:45 UTC
Last Analysis	2023-07-21 10:42:05 UTC

Names

executable.544.exe
module.544.19a34b0.4ad00000.dll
cmd.544.exe
-executable.544.exe
544.cmd.exe
executable.544.exe.bin



THANK YOU!