Case Study – Rootkit Analysis

Monnappa (m0nna)

www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer’s only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **null** & **Garage4Hackers** community for their extended support and cooperation.
- Special thanks to **ThoughtWorks** for the beautiful and bigger venue.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Reversing & Malware Analysis Training

This presentation is part of our **Reverse Engineering & Malware Analysis** Training program. Currently it is delivered only during our local meet for FREE of cost.

For complete details of this course, visit our Security Training page.

Who am I

Monnappa

- m0nna
- Member of SecurityXploded (SX)
- Info Security Investigator @ Cisco
- Reverse Engineering, Malware Analysis, Memory Forensics
- GREM
- Email: monnappa22@gmail.com,
- Twitter: @monnappa22
- Linkedin: http://www.linkedin.com/pub/monnappa-ka-grem-ceh/42/45a/1b8

Course Q&A

- Keep yourself up to date with latest security news
  - http://www.securityphresh.com

- For Q&A, join our mailing list.
  - http://groups.google.com/group/securityxploded

Contents

- What is a Rootkit?
- User Mode Rootkits
- Kernel Mode Rootkits
- Function Call cycle on Windows
- Levels of hooking/modification on Windows
- Demo 1 (mader– SSDT hook)
- Demo 2 (prolaco – DKOM)
- Demo 3 (darkmegi /waltrodock– installs device driver)
- Demo 4 (carberp– syscall patch and inline API hook)

What is a Rootkit?

- Program that perform system hooking or modifies functionality of OS
- Hide files, processes, other objects to conceal its presence
- Intercepts and alters the normal execution flow
- Can contain both user mode and kernel mode components
- Some rootkits can install as device drivers
- Types: User Mode and Kernel Mode Rootkits

User Mode Rootkits

- Runs in Ring 3

- Hooking in user space or application space

- Some common user mode Rootkit technqiues:
  - IAT (Import Address Table) hooking
  - Inline API hooking

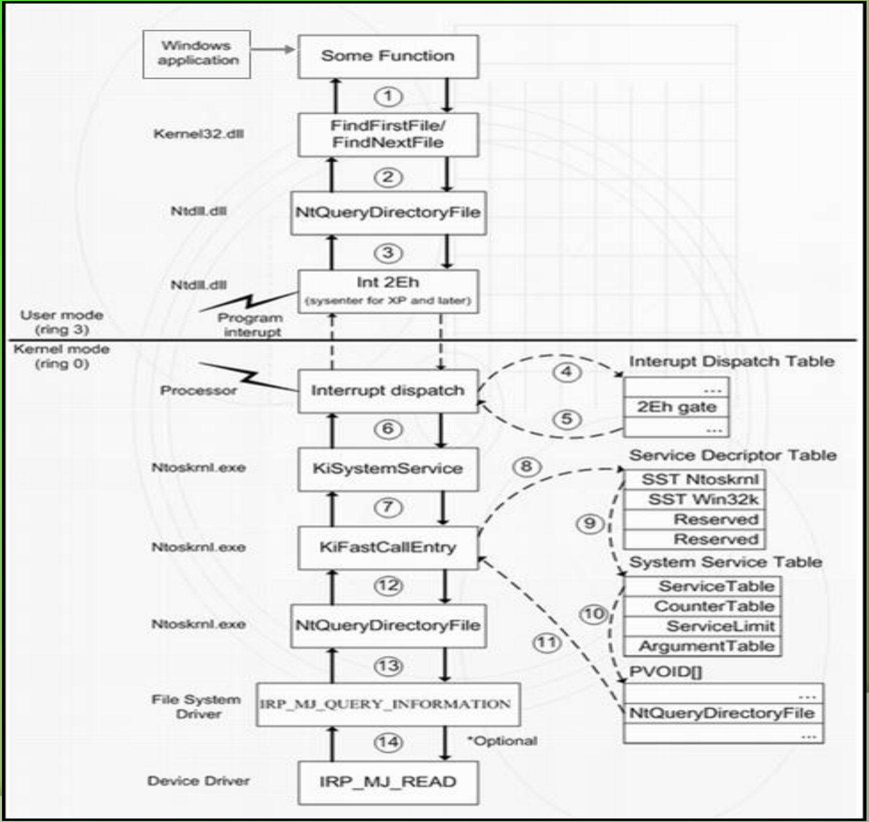
- Rootkit need to perform patching in the memory space of every running application

Kernel Mode Rootkits

- **Runs in Ring 0**
- **System hooking or modification in kernel space**
- **Some Kernel mode Rootkit techniques:**
  - SSDT (System Service Descriptor Table) hooking
  - DKOM (Direct Kernel Object Manipulation)
  - IDT (Interrupt Descriptor Table) hooking
  - Installing as Device Drivers
  - Driver IRP hooking

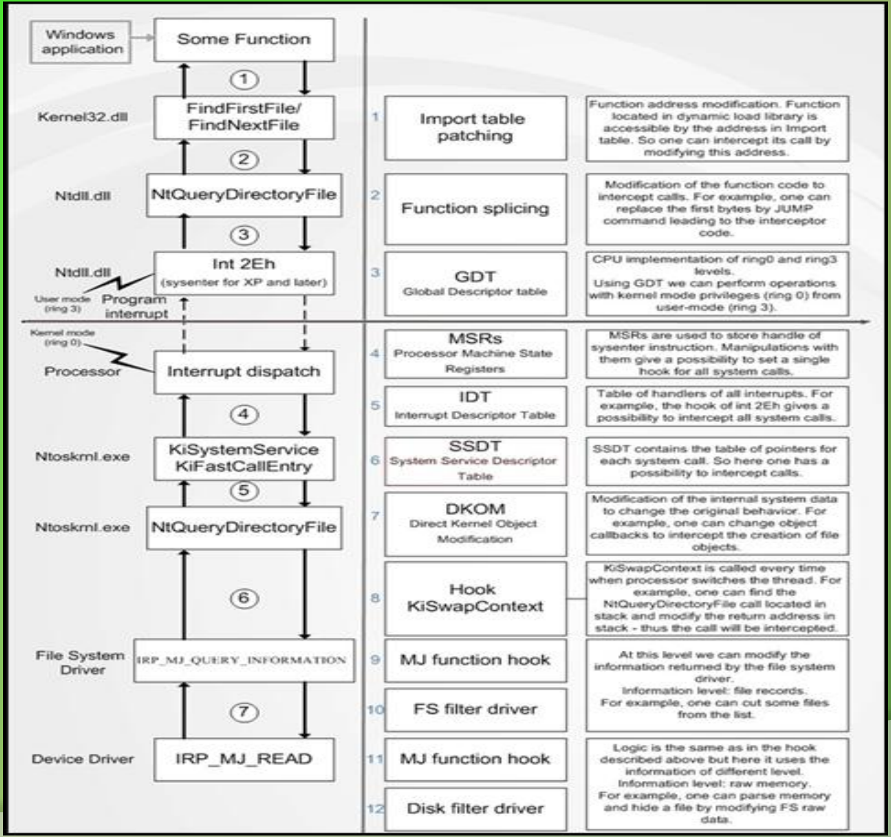
Function Call cycle on Windows

Below screenshot shows the API lifecycle on Windows system



Levels of hooking/modification on Windows

The below screenshot shows tables and objects that Rootkit can hook/modify to hide its presence



1	Import table patching	Function address modification. Function located in dynamic load library is accessible by the address in Import table. So one can intercept its call by modifying this address.
2	Function splicing	Modification of the function code to intercept calls. For example, one can replace the first bytes by JUMP command leading to the interceptor code.
3	GDT Global Descriptor table	CPU implementation of ring0 and ring3 levels. Using GDT we can perform operations with kernel mode privileges (ring 0) from user-mode (ring 3).
4	MSRs Processor Machine State Registers	MSRs are used to store handle of sysenter instruction. Manipulations with them give a possibility to set a single hook for all system calls.
5	IDT Interrupt Descriptor Table	Table of handlers of all interrupts. For example, the hook of int 2Eh gives a possibility to intercept all system calls.
6	SSDT System Service Descriptor Table	SSDT contains the table of pointers for each system call. So here one has a possibility to intercept calls.
7	DKOM Direct Kernel Object Modification	Modification of the internal system data to change the original behavior. For example, one can change object callbacks to intercept the creation of file objects.
8	Hook KiSwapContext	KiSwapContext is called every time when processor switches the thread. For example, one can find the NtQueryDirectoryFile call located in stack and modify the return address in stack - thus the call will be intercepted.
9	MJ function hook	At this level we can modify the information returned by the file system driver. Information level: file records. For example, one can cut some files from the list.
10	FS filter driver	
11	MJ function hook	Logic is the same as in the hook described above but here it uses the information of different level. Information level: raw memory. For example, one can parse memory and hide a file by modifying FS raw data.
12	Disk filter driver	

NOTE

- **Rootkit Theory and Techniques will be covered in depth in our Advanced Training Series. This session focuses on the Rootkit Analysis.**

- **Because of the time constraint, the demo uses a script "sandbox.py" which automates the behavioural analysis and memory analysis discussed in the Part 8 (Malware Memory Fornesics) and Part 9 (Advanced Malware Analysis) of the training session.**

http://nagareshwar.securityxploded.com/2012/06/16/training-session-part-8-%E2%80%93-practical-reversing-iii-memory-forensics/

http://nagareshwar.securityxploded.com/2012/07/15/training-session-part-9-%E2%80%93-practical-reversing-iv-advanced-malware-analysis/

- **"sandbox.py" uses the tools CaptureBat (file, processs, registry activity), tshark (network activity), InetSim (simulating the services like dns, http, smtp) and Volatility (Memory Forensics) to produce the results. All these tools were discussed in Part 9 (Advanced Malware Analysis) of the training session.**

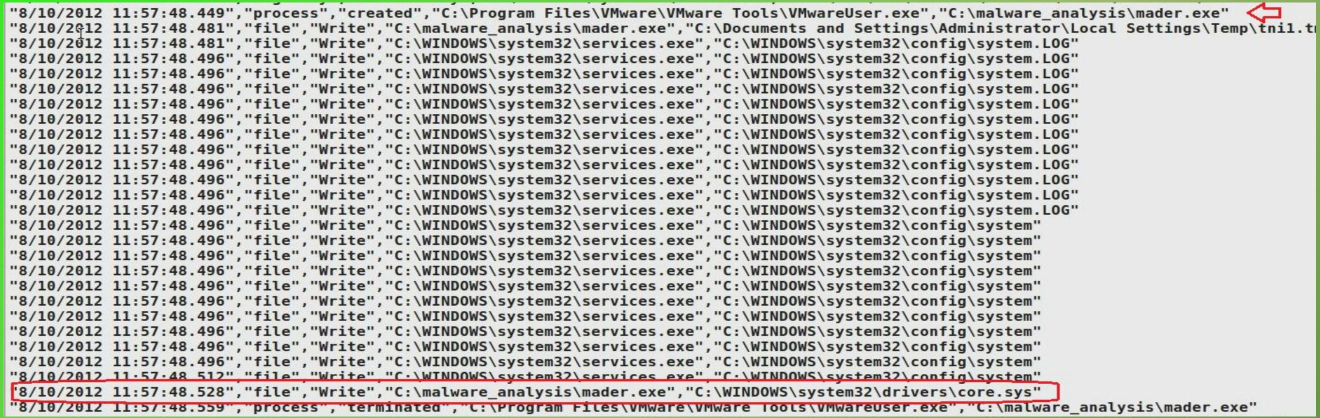
DEMO 1

(MADER – SSDT HOOKING)

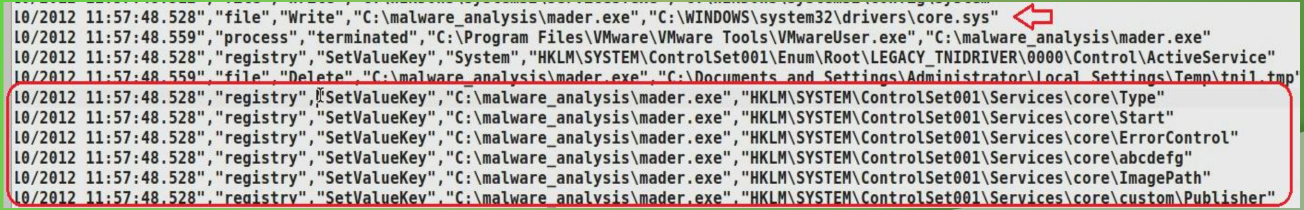
http://youtu.Be/5cld2hukfbu

Executing the sample mader.exe

Executing the sample drops a driver and loads it as kernel service



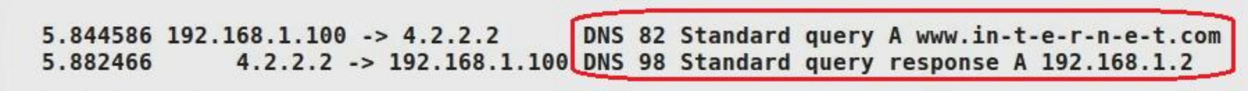
```
"8/10/2012 11:57:48.449","process","created","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\mader.exe"
"8/10/2012 11:57:48.481","file","Write","C:\malware_analysis\mader.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\tni1.tı
"8/10/2012 11:57:48.481","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system.LOG"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.496","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.512","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 11:57:48.528","file","Write","C:\malware_analysis\mader.exe","C:\WINDOWS\system32\drivers\core.sys"
"8/10/2012 11:57:48.559","process","terminated","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\mader.exe"
```



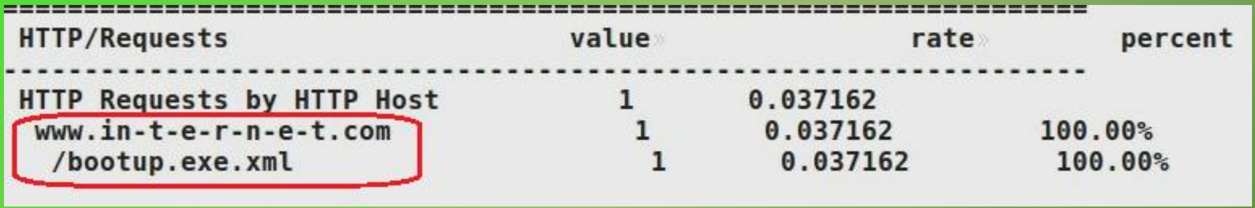
```
l0/2012 11:57:48.528","file","Write","C:\malware_analysis\mader.exe","C:\WINDOWS\system32\drivers\core.sys"
l0/2012 11:57:48.559","process","terminated","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\mader.exe"
l0/2012 11:57:48.528","registry","SetValueKey","System","HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TNIDRIVER\0000\Control\ActiveService"
l0/2012 11:57:48.559","file","Delete","C:\malware_analysis\mader.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\tni1.tmp'
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\Type"
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\Start"
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\ErrorControl"
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\abcdefg"
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\ImagePath"
l0/2012 11:57:48.528","registry","SetValueKey","C:\malware_analysis\mader.exe","HKLM\SYSTEM\ControlSet001\Services\core\custom\Publisher"
```

Network Activity

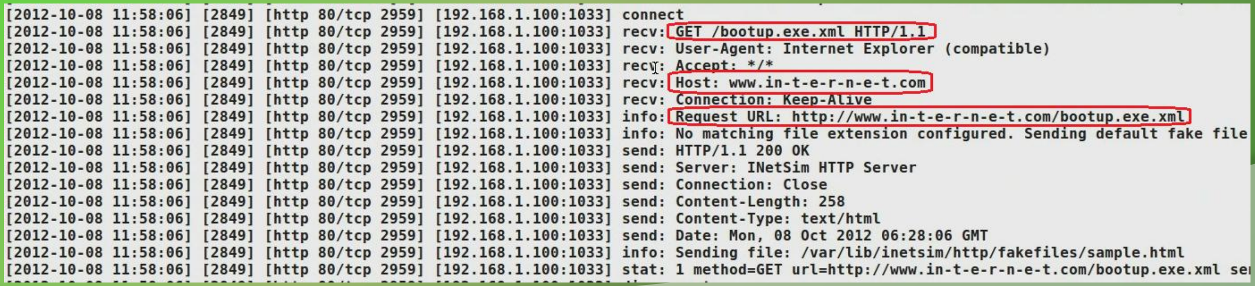
The malware makes dns query and downloads additional files



```
5.844586 192.168.1.100 -> 4.2.2.2       DNS 82 Standard query A www.in-t-e-r-n-e-t.com
5.882466       4.2.2.2 -> 192.168.1.100 DNS 98 Standard query response A 192.168.1.2
```



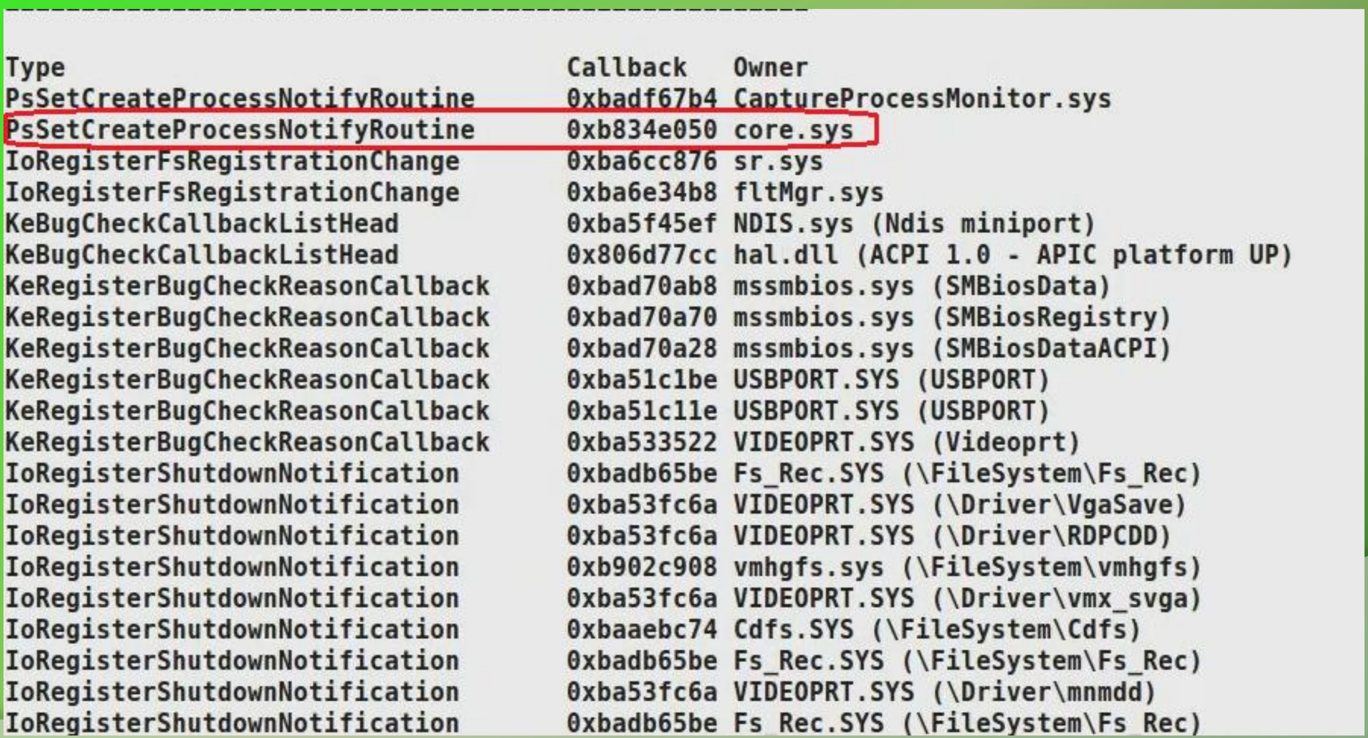
```
=================================================================================
HTTP/Requests                          value                     rate        percent
---------------------------------------------------------------------------------
HTTP Requests by HTTP Host               1        0.037162
 www.in-t-e-r-n-e-t.com                   1        0.037162          100.00%
  /bootup.exe.xml                          1        0.037162          100.00%
```



```
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] connect
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] recv: GET /bootup.exe.xml HTTP/1.1
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] recv: User-Agent: Internet Explorer (compatible)
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] recv: Accept: */*
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] recv: Host: www.in-t-e-r-n-e-t.com
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] recv: Connection: Keep-Alive
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] info: Request URL: http://www.in-t-e-r-n-e-t.com/bootup.exe.xml
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] info: No matching file extension configured. Sending default fake file
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: HTTP/1.1 200 OK
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: Server: INetSim HTTP Server
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: Connection: Close
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: Content-Length: 258
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: Content-Type: text/html
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] send: Date: Mon, 08 Oct 2012 06:28:06 GMT
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html
[2012-10-08 11:58:06] [2849] [http 80/tcp 2959] [192.168.1.100:1033] stat: 1 method=GET url=http://www.in-t-e-r-n-e-t.com/bootup.exe.xml se
```

Kernel Callbacks

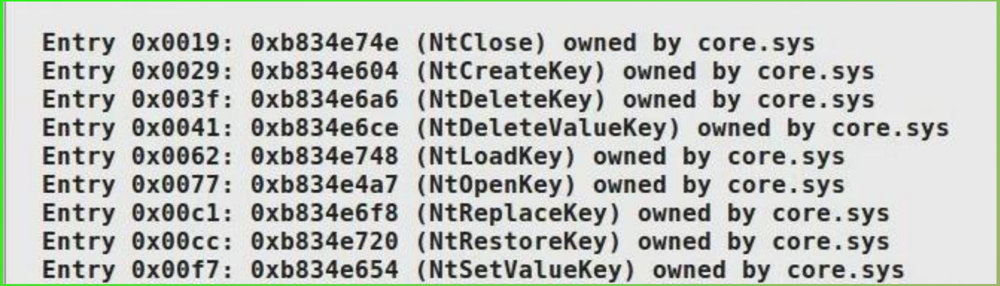
Rootkit uses callbacks to monitor for process creation activity



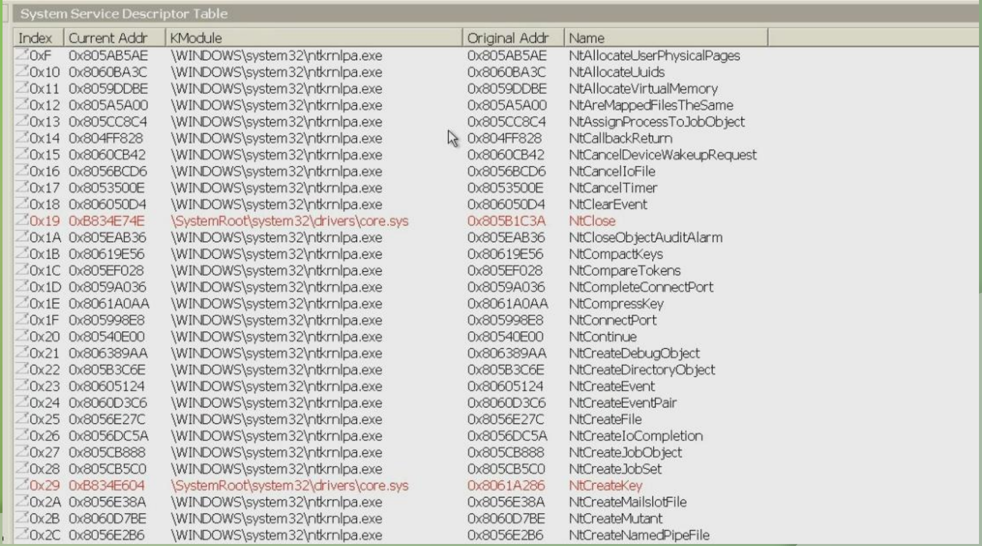
```
----------------------------------------------------

Type                                 Callback   Owner
PsSetCreateProcessNotifyRoutine      0xbadf67b4 CaptureProcessMonitor.sys
PsSetCreateProcessNotifyRoutine      0xb834e050 core.sys
IoRegisterFsRegistrationChange       0xba6cc876 sr.sys
IoRegisterFsRegistrationChange       0xba6e34b8 fltMgr.sys
KeBugCheckCallbackListHead           0xba5f45ef NDIS.sys (Ndis miniport)
KeBugCheckCallbackListHead           0x806d77cc hal.dll (ACPI 1.0 - APIC platform UP)
KeRegisterBugCheckReasonCallback     0xbad70ab8 mssmbios.sys (SMBiosData)
KeRegisterBugCheckReasonCallback     0xbad70a70 mssmbios.sys (SMBiosRegistry)
KeRegisterBugCheckReasonCallback     0xbad70a28 mssmbios.sys (SMBiosDataACPI)
KeRegisterBugCheckReasonCallback     0xba51c1be USBPORT.SYS (USBPORT)
KeRegisterBugCheckReasonCallback     0xba51c11e USBPORT.SYS (USBPORT)
KeRegisterBugCheckReasonCallback     0xba533522 VIDEOPRT.SYS (Videoprt)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\VgaSave)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\RDPCDD)
IoRegisterShutdownNotification       0xb902c908 vmhgfs.sys (\FileSystem\vmhgfs)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\vmx_svga)
IoRegisterShutdownNotification       0xbaaebc74 Cdfs.SYS (\FileSystem\Cdfs)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\mnmdd)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
```

SSDT Hooking

Rootkit modifies the pointers in the SSDT to protect itself from deletion or removal



```
Entry 0x0019: 0xb834e74e (NtClose) owned by core.sys
Entry 0x0029: 0xb834e604 (NtCreateKey) owned by core.sys
Entry 0x003f: 0xb834e6a6 (NtDeleteKey) owned by core.sys
Entry 0x0041: 0xb834e6ce (NtDeleteValueKey) owned by core.sys
Entry 0x0062: 0xb834e748 (NtLoadKey) owned by core.sys
Entry 0x0077: 0xb834e4a7 (NtOpenKey) owned by core.sys
Entry 0x00c1: 0xb834e6f8 (NtReplaceKey) owned by core.sys
Entry 0x00cc: 0xb834e720 (NtRestoreKey) owned by core.sys
Entry 0x00f7: 0xb834e654 (NtSetValueKey) owned by core.sys
```

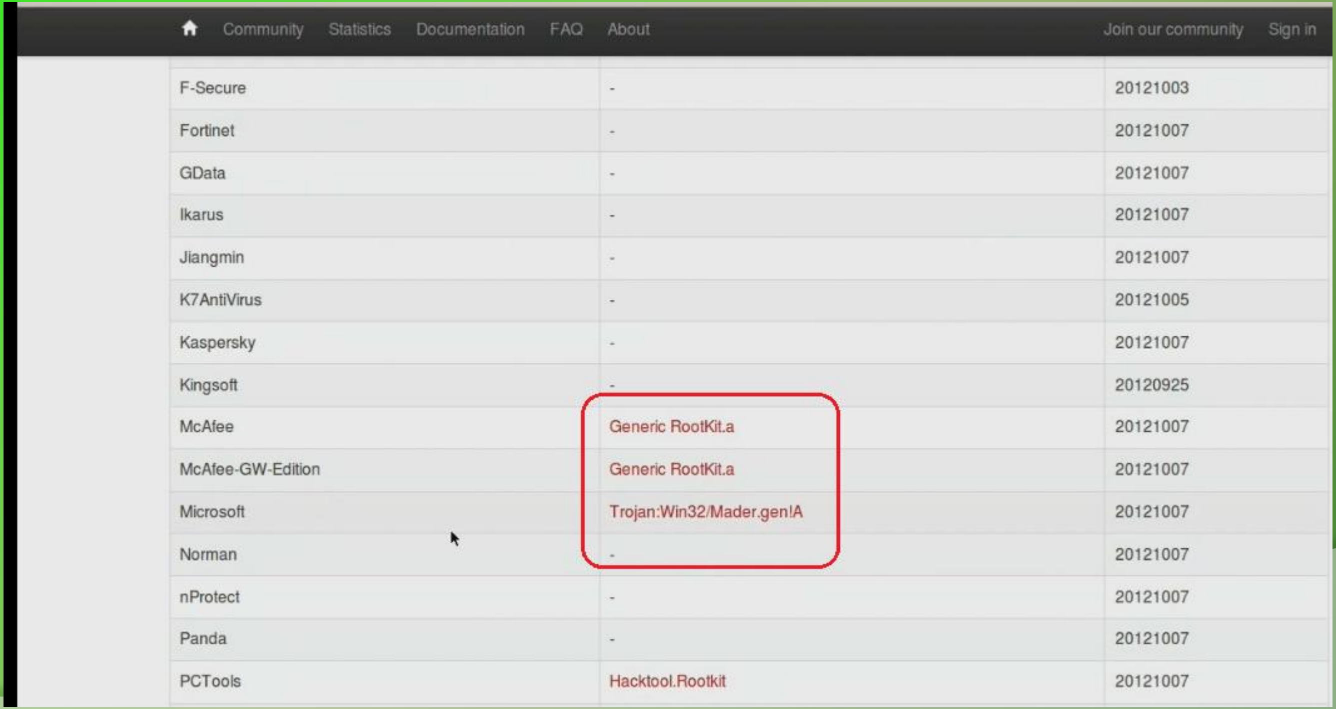


System Service Descriptor Table

Index	Current Addr	KModule	Original Addr	Name
0xF	0x805AB5AE	\WINDOWS\system32\ntkrnlpa.exe	0x805AB5AE	NtAllocateUserPhysicalPages
0x10	0x8060BA3C	\WINDOWS\system32\ntkrnlpa.exe	0x8060BA3C	NtAllocateUuids
0x11	0x8059DDBE	\WINDOWS\system32\ntkrnlpa.exe	0x8059DDBE	NtAllocateVirtualMemory
0x12	0x805A5A00	\WINDOWS\system32\ntkrnlpa.exe	0x805A5A00	NtAreMappedFilesTheSame
0x13	0x805CC8C4	\WINDOWS\system32\ntkrnlpa.exe	0x805CC8C4	NtAssignProcessToJobObject
0x14	0x804FF828	\WINDOWS\system32\ntkrnlpa.exe	0x804FF828	NtCallbackReturn
0x15	0x8060CB42	\WINDOWS\system32\ntkrnlpa.exe	0x8060CB42	NtCancelDeviceWakeupRequest
0x16	0x8056BCD6	\WINDOWS\system32\ntkrnlpa.exe	0x8056BCD6	NtCancelIoFile
0x17	0x8053500E	\WINDOWS\system32\ntkrnlpa.exe	0x8053500E	NtCancelTimer
0x18	0x806050D4	\WINDOWS\system32\ntkrnlpa.exe	0x806050D4	NtClearEvent
0x19	0xB834E74E	\SystemRoot\system32\drivers\core.sys	0x805B1C3A	NtClose
0x1A	0x805EAB36	\WINDOWS\system32\ntkrnlpa.exe	0x805EAB36	NtCloseObjectAuditAlarm
0x1B	0x80619E56	\WINDOWS\system32\ntkrnlpa.exe	0x80619E56	NtCompactKeys
0x1C	0x805EF028	\WINDOWS\system32\ntkrnlpa.exe	0x805EF028	NtCompareTokens
0x1D	0x8059A036	\WINDOWS\system32\ntkrnlpa.exe	0x8059A036	NtCompleteConnectPort
0x1E	0x8061A0AA	\WINDOWS\system32\ntkrnlpa.exe	0x8061A0AA	NtCompressKey
0x1F	0x805998E8	\WINDOWS\system32\ntkrnlpa.exe	0x805998E8	NtConnectPort
0x20	0x80540E00	\WINDOWS\system32\ntkrnlpa.exe	0x80540E00	NtContinue
0x21	0x806389AA	\WINDOWS\system32\ntkrnlpa.exe	0x806389AA	NtCreateDebugObject
0x22	0x805B3C6E	\WINDOWS\system32\ntkrnlpa.exe	0x805B3C6E	NtCreateDirectoryObject
0x23	0x80605124	\WINDOWS\system32\ntkrnlpa.exe	0x80605124	NtCreateEvent
0x24	0x8060D3C6	\WINDOWS\system32\ntkrnlpa.exe	0x8060D3C6	NtCreateEventPair
0x25	0x8056E27C	\WINDOWS\system32\ntkrnlpa.exe	0x8056E27C	NtCreateFile
0x26	0x8056DC5A	\WINDOWS\system32\ntkrnlpa.exe	0x8056DC5A	NtCreateIoCompletion
0x27	0x805CB888	\WINDOWS\system32\ntkrnlpa.exe	0x805CB888	NtCreateJobObject
0x28	0x805CB5C0	\WINDOWS\system32\ntkrnlpa.exe	0x805CB5C0	NtCreateJobSet
0x29	0xB834E604	\SystemRoot\system32\drivers\core.sys	0x8061A286	NtCreateKey
0x2A	0x8056E38A	\WINDOWS\system32\ntkrnlpa.exe	0x8056E38A	NtCreateMailslotFile
0x2B	0x8060D7BE	\WINDOWS\system32\ntkrnlpa.exe	0x8060D7BE	NtCreateMutant
0x2C	0x8056E2B6	\WINDOWS\system32\ntkrnlpa.exe	0x8056E2B6	NtCreateNamedPipeFile

Rootkit Submission to VirusTotal

VirusTotal confirms the Rootkit after dumping and submitting the driver from memory



F-Secure	-	20121003
Fortinet	-	20121007
GData	-	20121007
Ikarus	-	20121007
Jiangmin	-	20121007
K7AntiVirus	-	20121005
Kaspersky	-	20121007
Kingsoft	-	20120925
McAfee	Generic RootKit.a	20121007
McAfee-GW-Edition	Generic RootKit.a	20121007
Microsoft	Trojan:Win32/Mader.gen!A	20121007
Norman	-	20121007
nProtect	-	20121007
Panda	-	20121007
PCTools	Hacktool.Rootkit	20121007

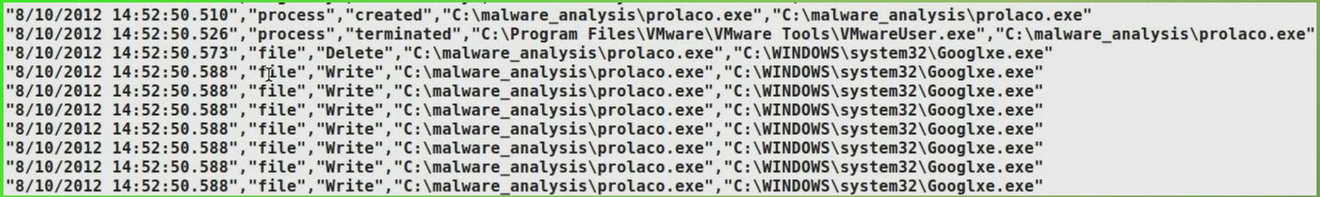
DEMO 2

(PROLACO – PROCESS HIDING USING DKOM)

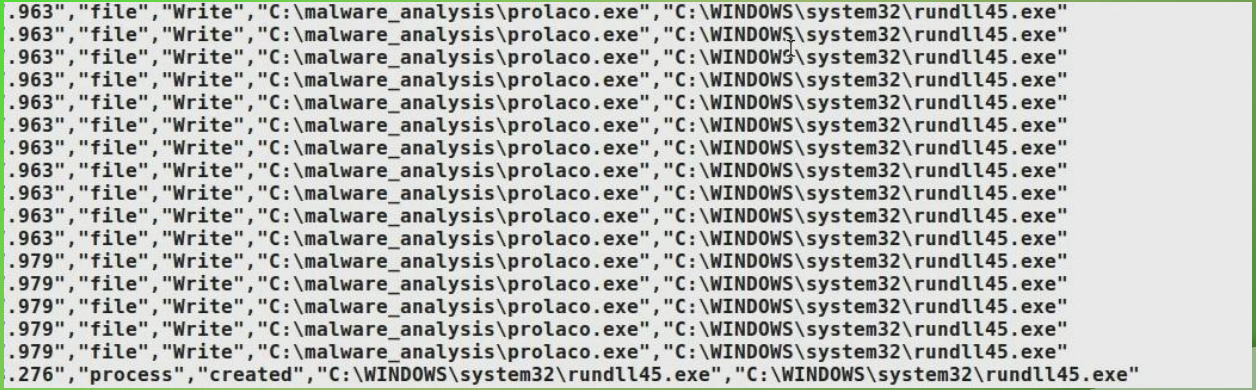
http://youtu.be/J7odu8OkBYs

Executing the sample prolaco.exe

Prolaco.exe drops two files on “Googlxe.exe” and “Rundll45.exe” on the filesystem



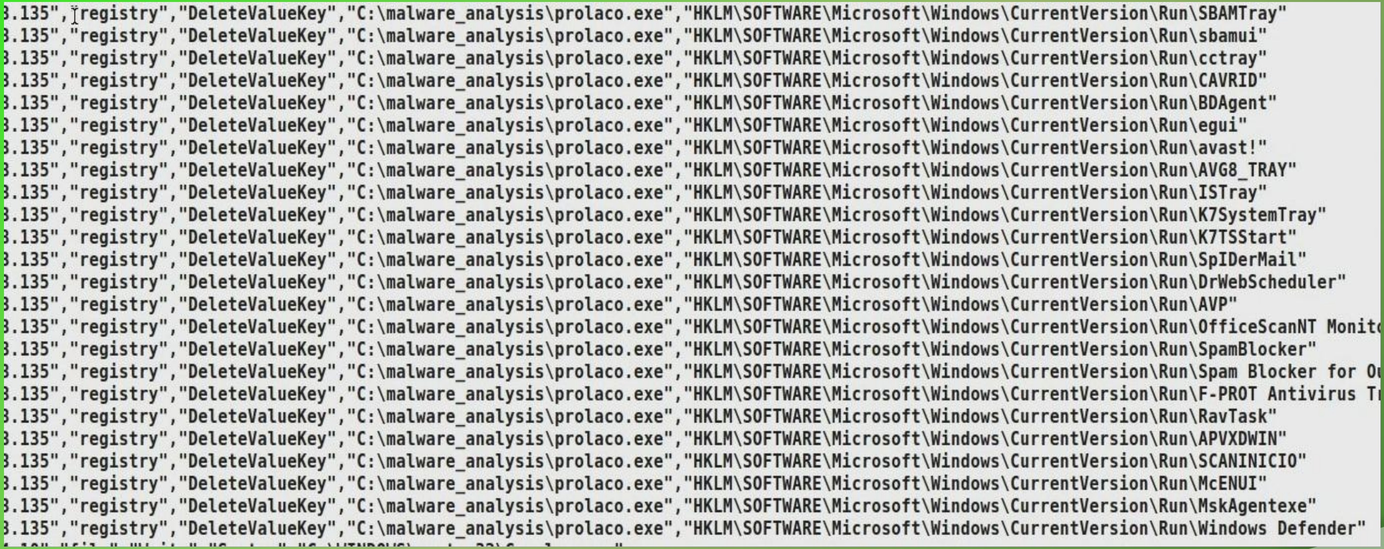
```
"8/10/2012 14:52:50.510","process","created","C:\malware_analysis\prolaco.exe","C:\malware_analysis\prolaco.exe"
"8/10/2012 14:52:50.526","process","terminated","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\prolaco.exe"
"8/10/2012 14:52:50.573","file","Delete","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
"8/10/2012 14:52:50.588","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\Googlxe.exe"
```



```
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.963","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.979","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.979","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.979","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.979","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.979","file","Write","C:\malware_analysis\prolaco.exe","C:\WINDOWS\system32\rundll45.exe"
.276","process","created","C:\WINDOWS\system32\rundll45.exe","C:\WINDOWS\system32\rundll45.exe"
```

Disables Security Products

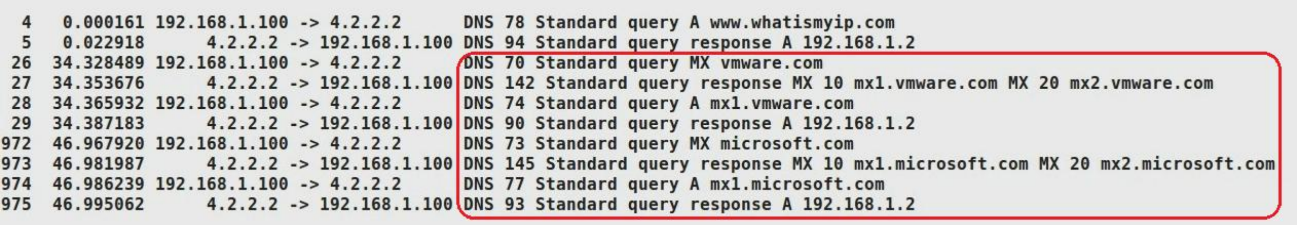
Prevents the security products from running by looking for the security products and deleting its registry key value



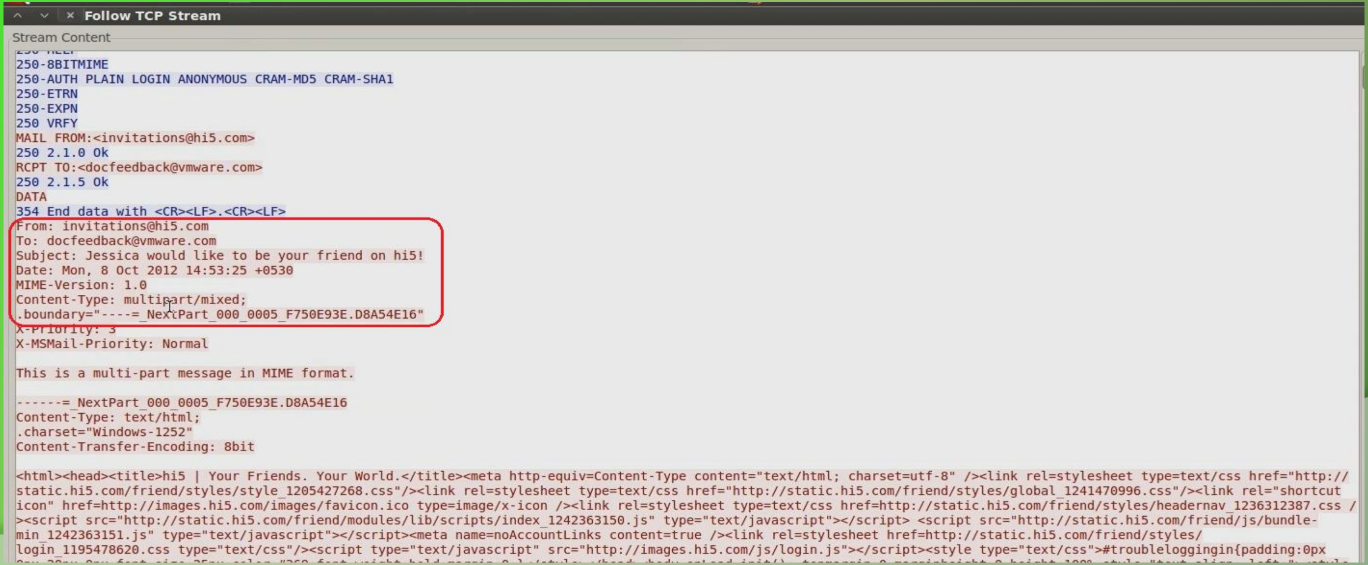
```
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SBAMTray"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sbamui"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\cctray"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CAVRID"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BDAgent"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\egui"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avast!"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AVG8_TRAY"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ISTray"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\K7SystemTray"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\K7TSStart"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SpIDerMail"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\DrWebScheduler"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AVP"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OfficeScanNT Monit
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SpamBlocker"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Spam Blocker for O
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\F-PROT Antivirus T
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RavTask"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\APVXDWIN"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SCANINICIO"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\McENUI"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MskAgentexe"
3.135","registry","DeleteValueKey","C:\malware_analysis\prolaco.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Defender"
```

Sends Spam

The malware sends spam invitation mails to the some of the organizations



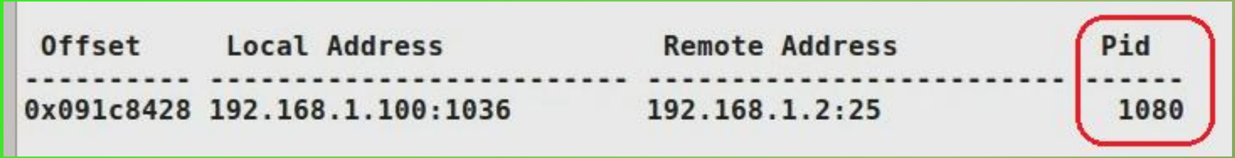
```
  4   0.000161 192.168.1.100 -> 4.2.2.2      DNS 78 Standard query A www.whatismyip.com
  5   0.022918       4.2.2.2 -> 192.168.1.100 DNS 94 Standard query response A 192.168.1.2
 26  34.328489 192.168.1.100 -> 4.2.2.2      DNS 70 Standard query MX vmware.com
 27  34.353676       4.2.2.2 -> 192.168.1.100 DNS 142 Standard query response MX 10 mx1.vmware.com MX 20 mx2.vmware.com
 28  34.365932 192.168.1.100 -> 4.2.2.2      DNS 74 Standard query A mx1.vmware.com
 29  34.387183       4.2.2.2 -> 192.168.1.100 DNS 90 Standard query response A 192.168.1.2
972  46.967920 192.168.1.100 -> 4.2.2.2      DNS 73 Standard query MX microsoft.com
973  46.981987       4.2.2.2 -> 192.168.1.100 DNS 145 Standard query response MX 10 mx1.microsoft.com MX 20 mx2.microsoft.com
974  46.986239 192.168.1.100 -> 4.2.2.2      DNS 77 Standard query A mx1.microsoft.com
975  46.995062       4.2.2.2 -> 192.168.1.100 DNS 93 Standard query response A 192.168.1.2
```



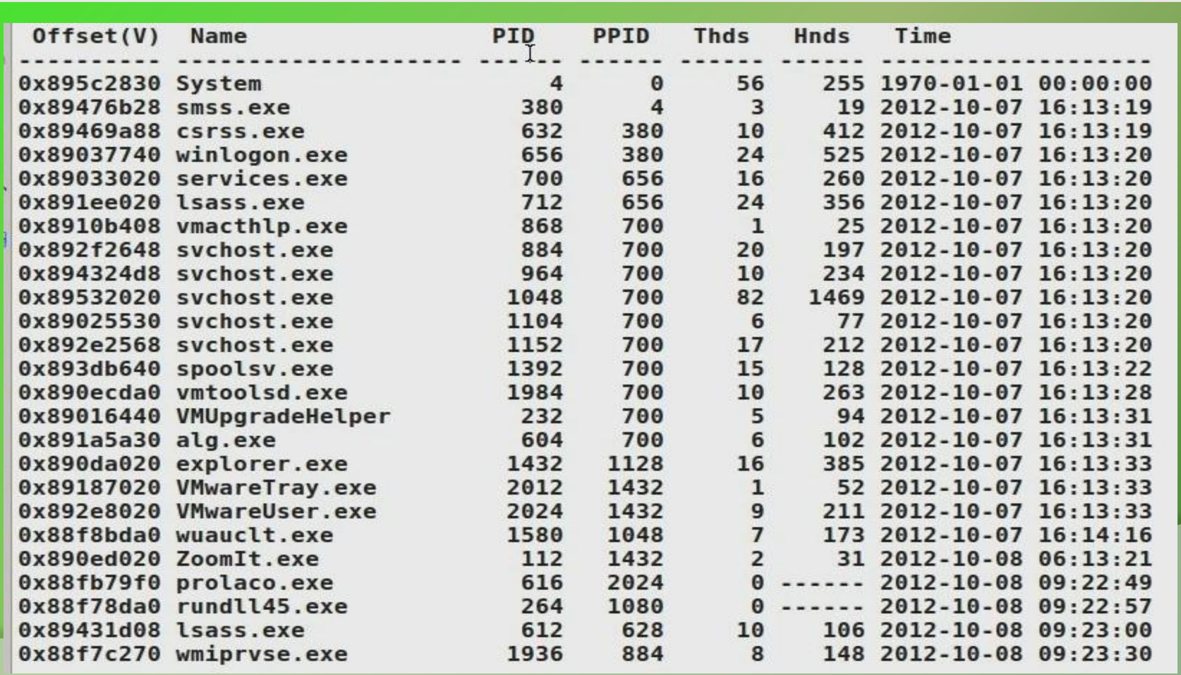
```
250-8BITMIME
250-AUTH PLAIN LOGIN ANONYMOUS CRAM-MD5 CRAM-SHA1
250-ETRN
250-EXPN
250 VRFY
MAIL FROM:<invitations@hi5.com>
250 2.1.0 Ok
RCPT TO:<docfeedback@vmware.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: invitations@hi5.com
To: docfeedback@vmware.com
Subject: Jessica would like to be your friend on hi5!
Date: Mon, 8 Oct 2012 14:53:25 +0530
MIME-Version: 1.0
Content-Type: multipart/mixed;
.boundary="----=_NextPart_000_0005_F750E93E.D8A54E16"
X-Priority: 3
X-MSMail-Priority: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_0005_F750E93E.D8A54E16
Content-Type: text/html;
.charset="Windows-1252"
Content-Transfer-Encoding: 8bit

<html><head><title>hi5 | Your Friends. Your World.</title><meta http-equiv=Content-Type content="text/html; charset=utf-8" /><link rel=stylesheet type=text/css href="http://
static.hi5.com/friend/styles/style_1205427268.css"/><link rel=stylesheet type=text/css href="http://static.hi5.com/friend/styles/global_1241470996.css"/><link rel="shortcut
icon" href=http://images.hi5.com/images/favicon.ico type=image/x-icon /><link rel=stylesheet type=text/css href=http://static.hi5.com/friend/styles/headernav_1236312387.css /
><script src="http://static.hi5.com/friend/modules/lib/scripts/index_1242363150.js" type="text/javascript"></script> <script src="http://static.hi5.com/friend/js/bundle-
min_1242363151.js" type="text/javascript"></script><meta name=noAccountLinks content=true /><link rel=stylesheet href=http://static.hi5.com/friend/styles/
login_1195478620.css type="text/css"/><script type="text/javascript" src="http://images.hi5.com/js/login.js"></script><style type="text/css">#troubleloggingin{padding:0px
```

Hides the process

Process id 1080 sends the spam, but the rootkits hides that process from the process listing using DKOM technique



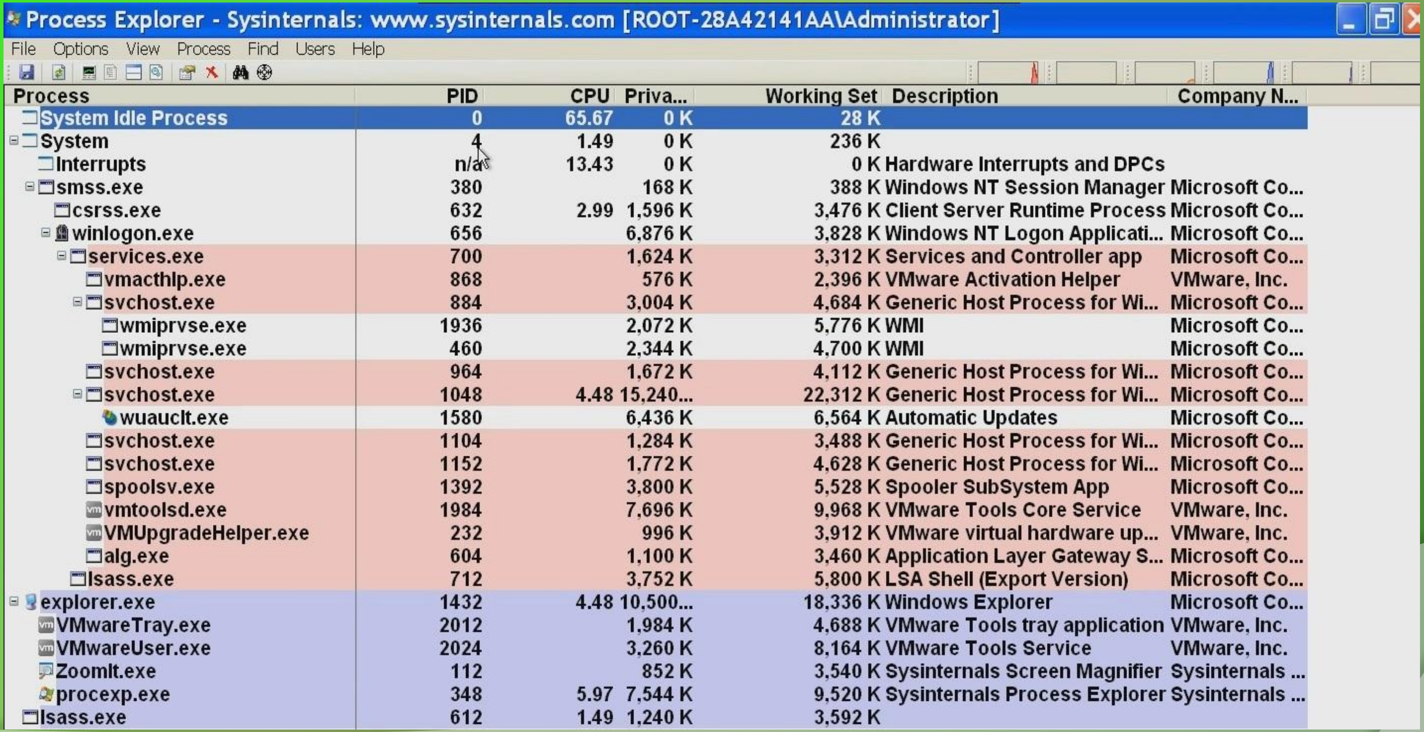
```
 Offset     Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x091c8428 192.168.1.100:1036        192.168.1.2:25              1080
```



```
 Offset(V)  Name                 PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ -------------------
0x895c2830 System                    4      0     56    255 1970-01-01 00:00:00
0x89476b28 smss.exe                380      4      3     19 2012-10-07 16:13:19
0x89469a88 csrss.exe               632    380     10    412 2012-10-07 16:13:19
0x89037740 winlogon.exe            656    380     24    525 2012-10-07 16:13:20
0x89033020 services.exe            700    656     16    260 2012-10-07 16:13:20
0x891ee020 lsass.exe               712    656     24    356 2012-10-07 16:13:20
0x8910b408 vmacthlp.exe            868    700      1     25 2012-10-07 16:13:20
0x892f2648 svchost.exe             884    700     20    197 2012-10-07 16:13:20
0x894324d8 svchost.exe             964    700     10    234 2012-10-07 16:13:20
0x89532020 svchost.exe            1048    700     82   1469 2012-10-07 16:13:20
0x89025530 svchost.exe            1104    700      6     77 2012-10-07 16:13:20
0x892e2568 svchost.exe            1152    700     17    212 2012-10-07 16:13:20
0x893db640 spoolsv.exe            1392    700     15    128 2012-10-07 16:13:22
0x890ecda0 vmtoolsd.exe           1984    700     10    263 2012-10-07 16:13:28
0x89016440 VMUpgradeHelper         232    700      5     94 2012-10-07 16:13:31
0x891a5a30 alg.exe                 604    700      6    102 2012-10-07 16:13:31
0x890da020 explorer.exe           1432   1128     16    385 2012-10-07 16:13:33
0x89187020 VMwareTray.exe         2012   1432      1     52 2012-10-07 16:13:33
0x892e8020 VMwareUser.exe         2024   1432      9    211 2012-10-07 16:13:33
0x88f8bda0 wuauclt.exe            1580   1048      7    173 2012-10-07 16:14:16
0x890ed020 ZoomIt.exe              112   1432      2     31 2012-10-08 06:13:21
0x88fb79f0 prolaco.exe             616   2024      0 ------ 2012-10-08 09:22:49
0x88f78da0 rundll45.exe            264   1080      0 ------ 2012-10-08 09:22:57
0x89431d08 lsass.exe               612    628     10    106 2012-10-08 09:23:00
0x88f7c270 wmiprvse.exe           1936    884      8    148 2012-10-08 09:23:30
```

Hides Process from security tool

Hides the process from process explorer



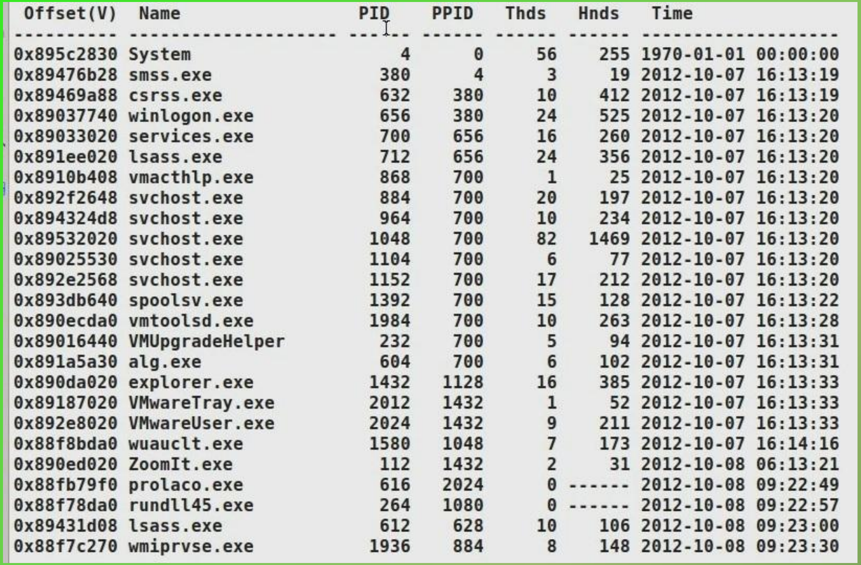
Process Explorer - Sysinternals: www.sysinternals.com [ROOT-28A42141AA\Administrator]

Process	PID	CPU	Priva...	Working Set	Description	Company N...
System Idle Process	0	65.67	0 K	28 K		
System	4	1.49	0 K	236 K		
Interrupts	n/a	13.43	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	380		168 K	388 K	Windows NT Session Manager	Microsoft Co...
csrss.exe	632	2.99	1,596 K	3,476 K	Client Server Runtime Process	Microsoft Co...
winlogon.exe	656		6,876 K	3,828 K	Windows NT Logon Applicati...	Microsoft Co...
services.exe	700		1,624 K	3,312 K	Services and Controller app	Microsoft Co...
vmacthlp.exe	868		576 K	2,396 K	VMware Activation Helper	VMware, Inc.
svchost.exe	884		3,004 K	4,684 K	Generic Host Process for Wi...	Microsoft Co...
wmiprvse.exe	1936		2,072 K	5,776 K	WMI	Microsoft Co...
wmiprvse.exe	460		2,344 K	4,700 K	WMI	Microsoft Co...
svchost.exe	964		1,672 K	4,112 K	Generic Host Process for Wi...	Microsoft Co...
svchost.exe	1048	4.48	15,240...	22,312 K	Generic Host Process for Wi...	Microsoft Co...
wuauclt.exe	1580		6,436 K	6,564 K	Automatic Updates	Microsoft Co...
svchost.exe	1104		1,284 K	3,488 K	Generic Host Process for Wi...	Microsoft Co...
svchost.exe	1152		1,772 K	4,628 K	Generic Host Process for Wi...	Microsoft Co...
spoolsv.exe	1392		3,800 K	5,528 K	Spooler SubSystem App	Microsoft Co...
vmtoolsd.exe	1984		7,696 K	9,968 K	VMware Tools Core Service	VMware, Inc.
VMUpgradeHelper.exe	232		996 K	3,912 K	VMware virtual hardware up...	VMware, Inc.
alg.exe	604		1,100 K	3,460 K	Application Layer Gateway S...	Microsoft Co...
lsass.exe	712		3,752 K	5,800 K	LSA Shell (Export Version)	Microsoft Co...
explorer.exe	1432	4.48	10,500...	18,336 K	Windows Explorer	Microsoft Co...
VMwareTray.exe	2012		1,984 K	4,688 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	2024		3,260 K	8,164 K	VMware Tools Service	VMware, Inc.
ZoomIt.exe	112		852 K	3,540 K	Sysinternals Screen Magnifier	Sysinternals ...
procexp.exe	348	5.97	7,544 K	9,520 K	Sysinternals Process Explorer	Sysinternals ...
lsass.exe	612	1.49	1,240 K	3,592 K		

Detecting the hidden process

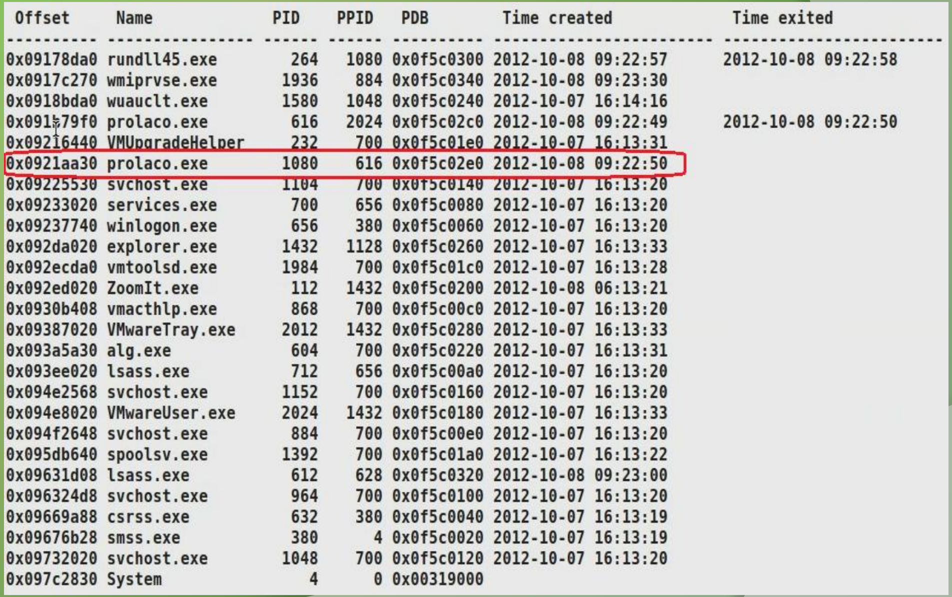
Comparing the process listing using Volatility's "pslist" and "psscan" plugin, shows the hidden process prolaco.exe (pid 1080)

pslist



```
 Offset(V)  Name                    PID   PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ -------------------
0x895c2830 System                    4      0     56    255 1970-01-01 00:00:00
0x89476b28 smss.exe                380      4      3     19 2012-10-07 16:13:19
0x89469a88 csrss.exe               632    380     10    412 2012-10-07 16:13:19
0x89037740 winlogon.exe            656    380     24    525 2012-10-07 16:13:20
0x89033020 services.exe            700    656     16    260 2012-10-07 16:13:20
0x891ee020 lsass.exe               712    656     24    356 2012-10-07 16:13:20
0x8910b408 vmacthlp.exe            868    700      1     25 2012-10-07 16:13:20
0x892f2648 svchost.exe             884    700     20    197 2012-10-07 16:13:20
0x894324d8 svchost.exe             964    700     10    234 2012-10-07 16:13:20
0x89532020 svchost.exe            1048    700     82   1469 2012-10-07 16:13:20
0x89025530 svchost.exe            1104    700      6     77 2012-10-07 16:13:20
0x892e2568 svchost.exe            1152    700     17    212 2012-10-07 16:13:20
0x893db640 spoolsv.exe            1392    700     15    128 2012-10-07 16:13:22
0x890ecda0 vmtoolsd.exe           1984    700     10    263 2012-10-07 16:13:28
0x89016440 VMUpgradeHelper         232    700      5     94 2012-10-07 16:13:31
0x891a5a30 alg.exe                 604    700      6    102 2012-10-07 16:13:31
0x890da020 explorer.exe           1432   1128     16    385 2012-10-07 16:13:33
0x89187020 VMwareTray.exe         2012   1432      1     52 2012-10-07 16:13:33
0x892e8020 VMwareUser.exe         2024   1432      9    211 2012-10-07 16:13:33
0x88f8bda0 wuauclt.exe            1580   1048      7    173 2012-10-07 16:14:16
0x890ed020 ZoomIt.exe              112   1432      2     31 2012-10-08 06:13:21
0x88fb79f0 prolaco.exe             616   2024      0 ------ 2012-10-08 09:22:49
0x88f78da0 rundll45.exe            264   1080      0 ------ 2012-10-08 09:22:57
0x89431d08 lsass.exe               612    628     10    106 2012-10-08 09:23:00
0x88f7c270 wmiprvse.exe           1936    884      8    148 2012-10-08 09:23:30
```

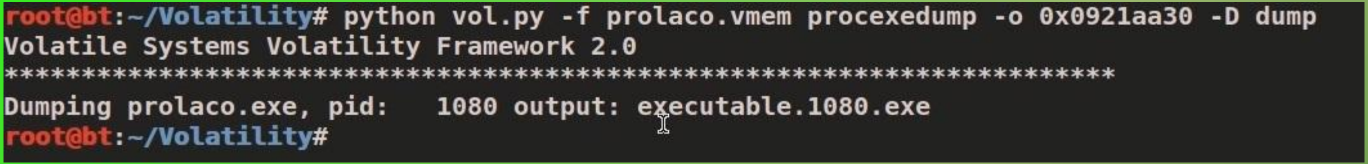
psscan



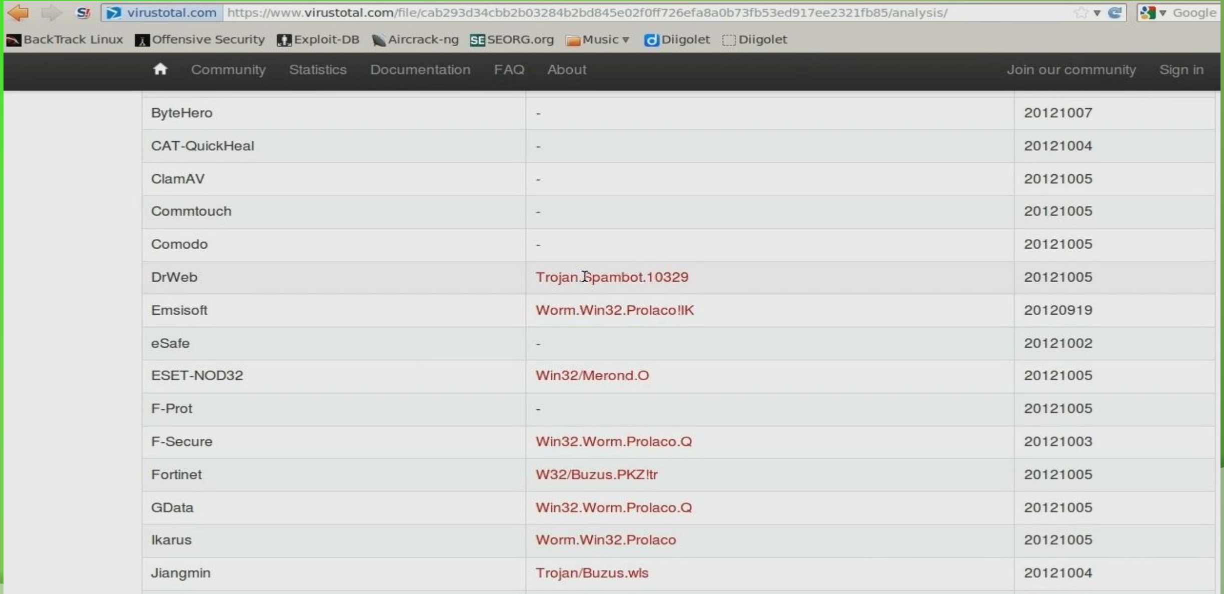
```
Offset     Name                PID   PPID  PDB        Time created             Time exited
---------- ---------------- ------ ------ ---------- ------------------------ ------------------------
0x09178da0 rundll45.exe        264   1080 0x0f5c0300 2012-10-08 09:22:57      2012-10-08 09:22:58
0x0917c270 wmiprvse.exe       1936    884 0x0f5c0340 2012-10-08 09:23:30
0x0918bda0 wuauclt.exe        1580   1048 0x0f5c0240 2012-10-07 16:14:16
0x091b79f0 prolaco.exe         616   2024 0x0f5c02c0 2012-10-08 09:22:49      2012-10-08 09:22:50
0x09216440 VMUpgradeHelper     232    700 0x0f5c01e0 2012-10-07 16:13:31
0x0921aa30 prolaco.exe        1080    616 0x0f5c02e0 2012-10-08 09:22:50
0x09225530 svchost.exe        1104    700 0x0f5c0140 2012-10-07 16:13:20
0x09233020 services.exe        700    656 0x0f5c0080 2012-10-07 16:13:20
0x09237740 winlogon.exe        656    380 0x0f5c0060 2012-10-07 16:13:20
0x092da020 explorer.exe       1432   1128 0x0f5c0260 2012-10-07 16:13:33
0x092ecda0 vmtoolsd.exe       1984    700 0x0f5c01c0 2012-10-07 16:13:28
0x092ed020 ZoomIt.exe          112   1432 0x0f5c0200 2012-10-08 06:13:21
0x0930b408 vmacthlp.exe        868    700 0x0f5c00c0 2012-10-07 16:13:20
0x09387020 VMwareTray.exe     2012   1432 0x0f5c0280 2012-10-07 16:13:33
0x093a5a30 alg.exe             604    700 0x0f5c0220 2012-10-07 16:13:31
0x093ee020 lsass.exe           712    656 0x0f5c00a0 2012-10-07 16:13:20
0x094e2568 svchost.exe        1152    700 0x0f5c0160 2012-10-07 16:13:20
0x094e8020 VMwareUser.exe     2024   1432 0x0f5c0180 2012-10-07 16:13:33
0x094f2648 svchost.exe         884    700 0x0f5c00e0 2012-10-07 16:13:20
0x095db640 spoolsv.exe        1392    700 0x0f5c01a0 2012-10-07 16:13:22
0x09631d08 lsass.exe           612    628 0x0f5c0320 2012-10-08 09:23:00
0x096324d8 svchost.exe         964    700 0x0f5c0100 2012-10-07 16:13:20
0x09669a88 csrss.exe           632    380 0x0f5c0040 2012-10-07 16:13:19
0x09676b28 smss.exe            380      4 0x0f5c0020 2012-10-07 16:13:19
0x09732020 svchost.exe        1048    700 0x0f5c0120 2012-10-07 16:13:20
0x097c2830 System                4      0 0x00319000
```

Dumping the hidden process

Dumping the hidden process from memory and submitting to VirusTotal confirms the presence of malicious hidden process



```
root@bt:~/Volatility# python vol.py -f prolaco.vmem procexedump -o 0x0921aa30 -D dump
Volatile Systems Volatility Framework 2.0
************************************************************************
Dumping prolaco.exe, pid:   1080 output: executable.1080.exe
root@bt:~/Volatility#
```



ByteHero	-	20121007
CAT-QuickHeal	-	20121004
ClamAV	-	20121005
Commtouch	-	20121005
Comodo	-	20121005
DrWeb	Trojan.Spambot.10329	20121005
Emsisoft	Worm.Win32.Prolaco!IK	20120919
eSafe	-	20121002
ESET-NOD32	Win32/Merond.O	20121005
F-Prot	-	20121005
F-Secure	Win32.Worm.Prolaco.Q	20121003
Fortinet	W32/Buzus.PKZ!tr	20121005
GData	Win32.Worm.Prolaco.Q	20121005
Ikarus	Worm.Win32.Prolaco	20121005
Jiangmin	Trojan/Buzus.wls	20121004

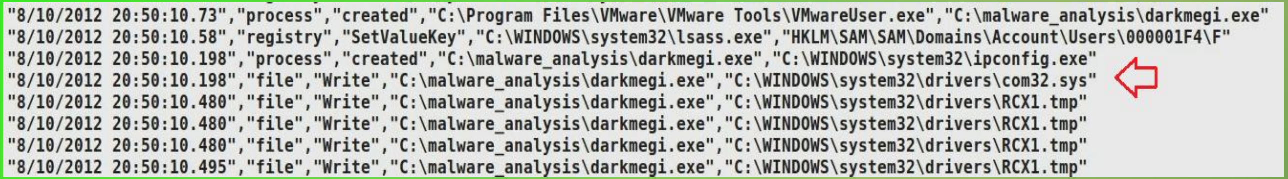
DEMO 3

(DARKMEGI/WALTRODOCK – INSTALLS DEVICE DRIVER)

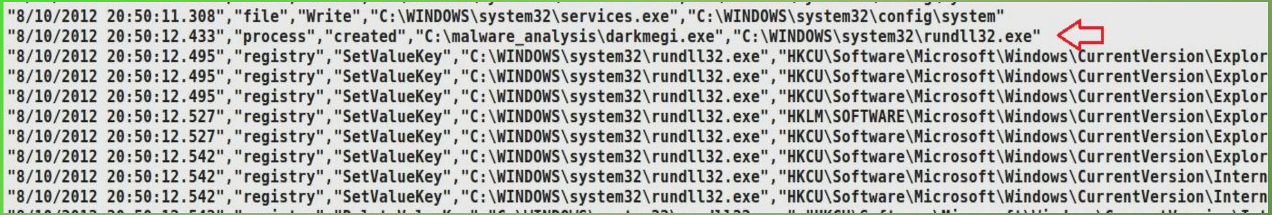
http://youtu.be/ZAWfu-tRzrc

Executing the sample darkmegi.exe

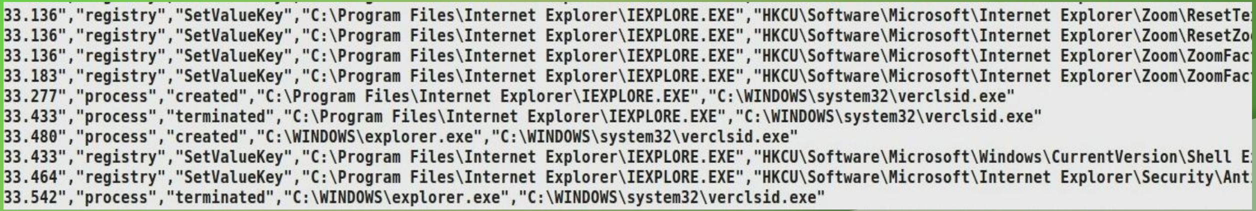
The sample drops a driver and also invokes rundll32 and iexplore proces.



```
"8/10/2012 20:50:10.73","process","created","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\darkmegi.exe"
"8/10/2012 20:50:10.58","registry","SetValueKey","C:\WINDOWS\system32\lsass.exe","HKLM\SAM\SAM\Domains\Account\Users\000001F4\F"
"8/10/2012 20:50:10.198","process","created","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\ipconfig.exe"
"8/10/2012 20:50:10.198","file","Write","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\drivers\com32.sys"
"8/10/2012 20:50:10.480","file","Write","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\drivers\RCX1.tmp"
"8/10/2012 20:50:10.480","file","Write","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\drivers\RCX1.tmp"
"8/10/2012 20:50:10.480","file","Write","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\drivers\RCX1.tmp"
"8/10/2012 20:50:10.495","file","Write","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\drivers\RCX1.tmp"
```



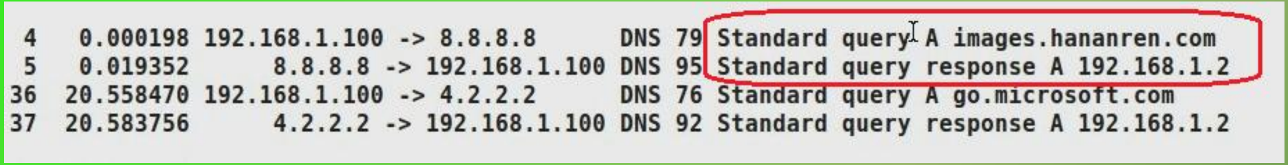
```
"8/10/2012 20:50:11.308","file","Write","C:\WINDOWS\system32\services.exe","C:\WINDOWS\system32\config\system"
"8/10/2012 20:50:12.433","process","created","C:\malware_analysis\darkmegi.exe","C:\WINDOWS\system32\rundll32.exe"
"8/10/2012 20:50:12.495","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.495","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.495","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.527","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.527","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.542","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explor
"8/10/2012 20:50:12.542","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Intern
"8/10/2012 20:50:12.542","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Intern
```



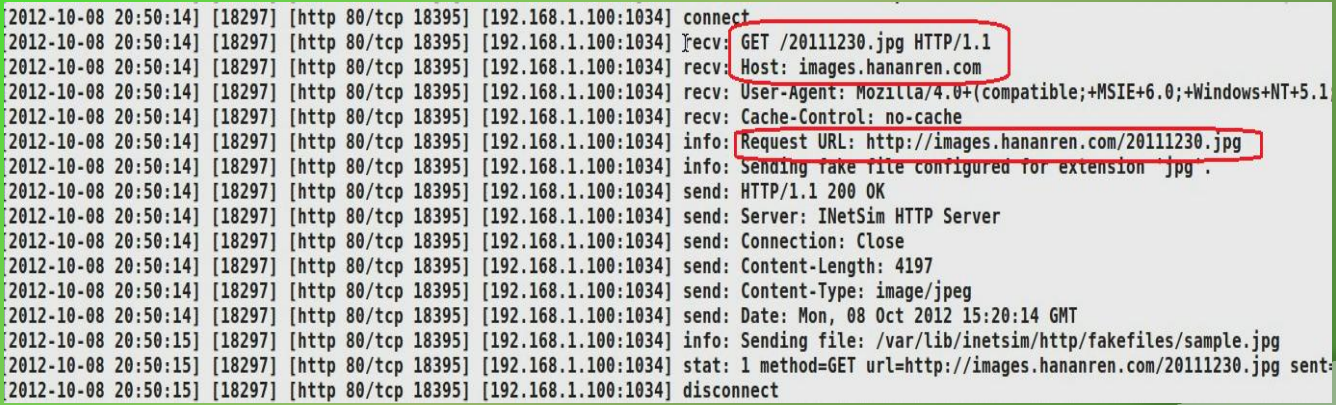
```
33.136","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Internet Explorer\Zoom\ResetTe
33.136","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Internet Explorer\Zoom\ResetZo
33.136","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Internet Explorer\Zoom\ZoomFac
33.183","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Internet Explorer\Zoom\ZoomFac
33.277","process","created","C:\Program Files\Internet Explorer\IEXPLORE.EXE","C:\WINDOWS\system32\verclsid.exe"
33.433","process","terminated","C:\Program Files\Internet Explorer\IEXPLORE.EXE","C:\WINDOWS\system32\verclsid.exe"
33.480","process","created","C:\WINDOWS\explorer.exe","C:\WINDOWS\system32\verclsid.exe"
33.433","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Windows\CurrentVersion\Shell E
33.464","registry","SetValueKey","C:\Program Files\Internet Explorer\IEXPLORE.EXE","HKCU\Software\Microsoft\Internet Explorer\Security\Ant
33.542","process","terminated","C:\WINDOWS\explorer.exe","C:\WINDOWS\system32\verclsid.exe"
```

Network Activity

Makes dns query and download additional files



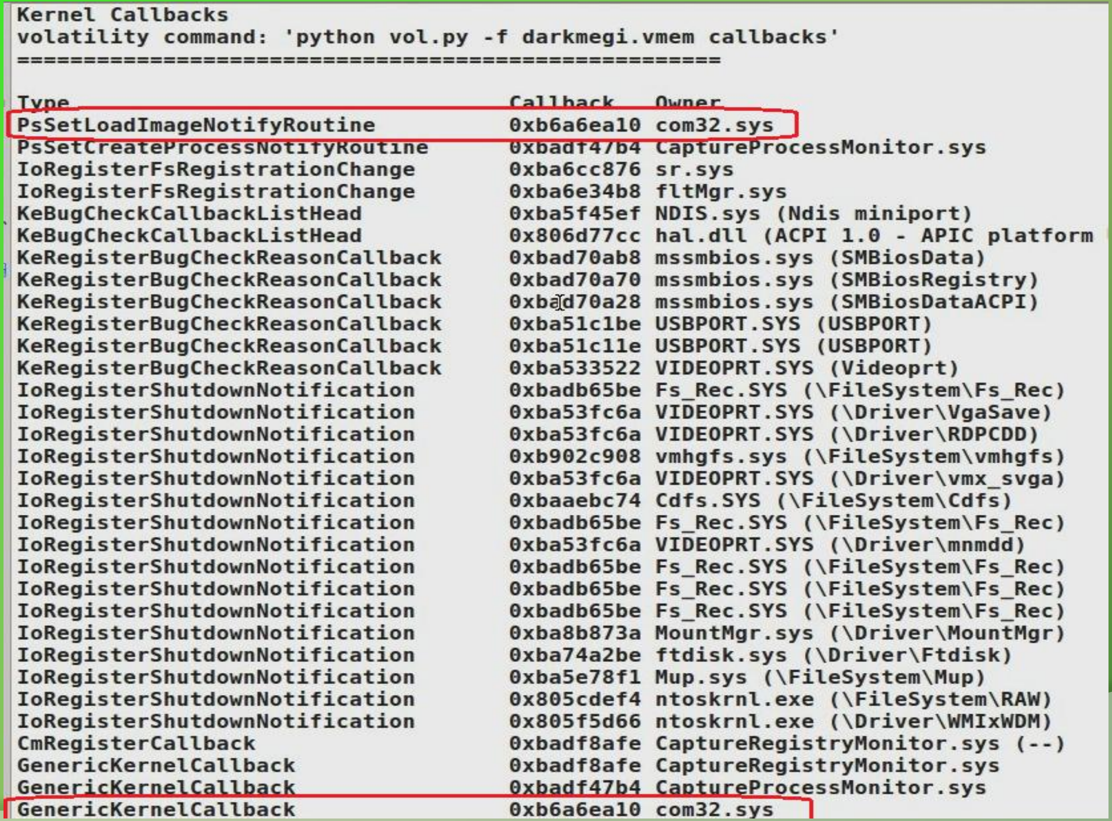
```
 4   0.000198 192.168.1.100 -> 8.8.8.8       DNS 79 Standard query A images.hananren.com
 5   0.019352       8.8.8.8 -> 192.168.1.100 DNS 95 Standard query response A 192.168.1.2
36  20.558470 192.168.1.100 -> 4.2.2.2       DNS 76 Standard query A go.microsoft.com
37  20.583756       4.2.2.2 -> 192.168.1.100 DNS 92 Standard query response A 192.168.1.2
```



```
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] connect
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] recv: GET /20111230.jpg HTTP/1.1
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] recv: Host: images.hananren.com
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] recv: User-Agent: Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] recv: Cache-Control: no-cache
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] info: Request URL: http://images.hananren.com/20111230.jpg
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] info: Sending fake file configured for extension 'jpg'.
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: HTTP/1.1 200 OK
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: Server: INetSim HTTP Server
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: Connection: Close
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: Content-Length: 4197
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: Content-Type: image/jpeg
[2012-10-08 20:50:14] [18297] [http 80/tcp 18395] [192.168.1.100:1034] send: Date: Mon, 08 Oct 2012 15:20:14 GMT
[2012-10-08 20:50:15] [18297] [http 80/tcp 18395] [192.168.1.100:1034] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.jpg
[2012-10-08 20:50:15] [18297] [http 80/tcp 18395] [192.168.1.100:1034] stat: 1 method=GET url=http://images.hananren.com/20111230.jpg sent=
[2012-10-08 20:50:15] [18297] [http 80/tcp 18395] [192.168.1.100:1034] disconnect
```

Sets Callbacks

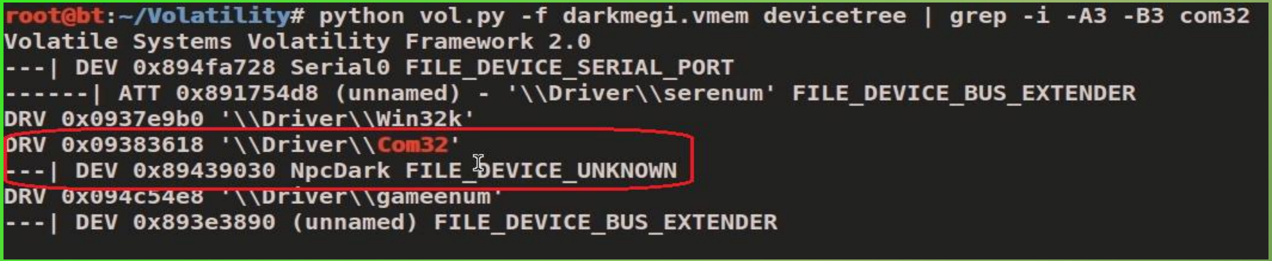
Sets kernel callbacks to montior for an Image/DLL loading



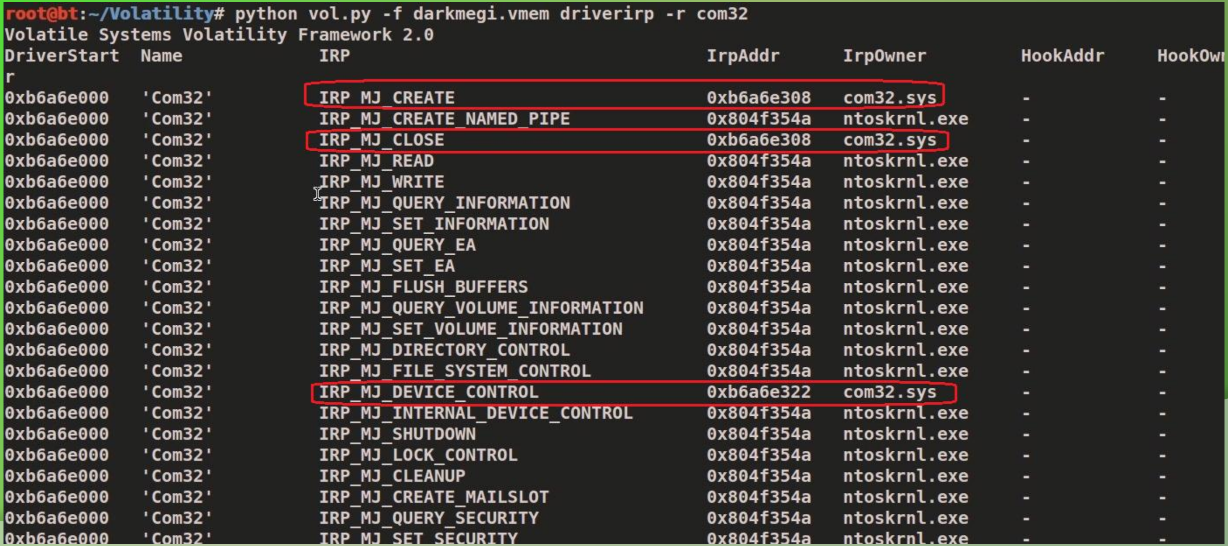
```
Kernel Callbacks
volatility command: 'python vol.py -f darkmegi.vmem callbacks'
=====================================================

Type                                 Callback   Owner
PsSetLoadImageNotifyRoutine          0xb6a6ea10 com32.sys
PsSetCreateProcessNotifyRoutine      0xbadf47b4 CaptureProcessMonitor.sys
IoRegisterFsRegistrationChange       0xba6cc876 sr.sys
IoRegisterFsRegistrationChange       0xba6e34b8 fltMgr.sys
KeBugCheckCallbackListHead           0xba5f45ef NDIS.sys (Ndis miniport)
KeBugCheckCallbackListHead           0x806d77cc hal.dll (ACPI 1.0 - APIC platform
KeRegisterBugCheckReasonCallback     0xbad70ab8 mssmbios.sys (SMBiosData)
KeRegisterBugCheckReasonCallback     0xbad70a70 mssmbios.sys (SMBiosRegistry)
KeRegisterBugCheckReasonCallback     0xbad70a28 mssmbios.sys (SMBiosDataACPI)
KeRegisterBugCheckReasonCallback     0xba51c1be USBPORT.SYS (USBPORT)
KeRegisterBugCheckReasonCallback     0xba51c11e USBPORT.SYS (USBPORT)
KeRegisterBugCheckReasonCallback     0xba533522 VIDEOPRT.SYS (Videoprt)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\VgaSave)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\RDPCDD)
IoRegisterShutdownNotification       0xb902c908 vmhgfs.sys (\FileSystem\vmhgfs)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\vmx_svga)
IoRegisterShutdownNotification       0xbaaebc74 Cdfs.SYS (\FileSystem\Cdfs)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xba53fc6a VIDEOPRT.SYS (\Driver\mnmdd)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xbadb65be Fs_Rec.SYS (\FileSystem\Fs_Rec)
IoRegisterShutdownNotification       0xba8b873a MountMgr.sys (\Driver\MountMgr)
IoRegisterShutdownNotification       0xba74a2be ftdisk.sys (\Driver\Ftdisk)
IoRegisterShutdownNotification       0xba5e78f1 Mup.sys (\FileSystem\Mup)
IoRegisterShutdownNotification       0x805cdef4 ntoskrnl.exe (\FileSystem\RAW)
IoRegisterShutdownNotification       0x805f5d66 ntoskrnl.exe (\Driver\WMIxWDM)
CmRegisterCallback                   0xbadf8afe CaptureRegistryMonitor.sys (--)
GenericKernelCallback                0xbadf8afe CaptureRegistryMonitor.sys
GenericKernelCallback                0xbadf47b4 CaptureProcessMonitor.sys
GenericKernelCallback                0xb6a6ea10 com32.sys
```

Examining the driver

The driver creates a device and accepts control codes from usermode programs



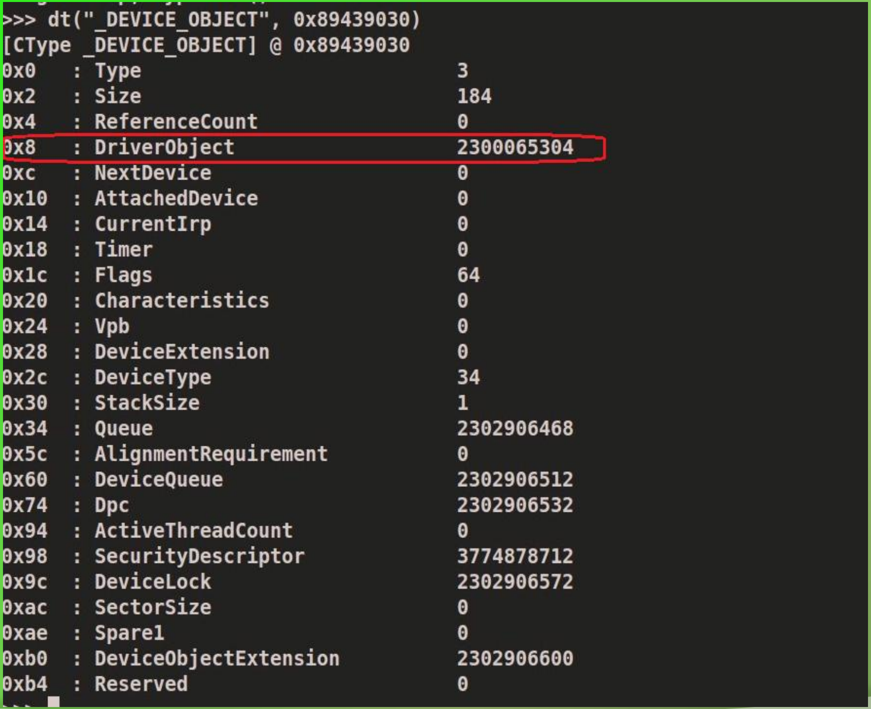
```
root@bt:~/Volatility# python vol.py -f darkmegi.vmem devicetree | grep -i -A3 -B3 com32
Volatile Systems Volatility Framework 2.0
---| DEV 0x894fa728 Serial0 FILE_DEVICE_SERIAL_PORT
------| ATT 0x891754d8 (unnamed) - '\\Driver\\serenum' FILE_DEVICE_BUS_EXTENDER
DRV 0x0937e9b0 '\\Driver\\Win32k'
DRV 0x09383618 '\\Driver\\Com32'
---| DEV 0x89439030 NpcDark FILE_DEVICE_UNKNOWN
DRV 0x094c54e8 '\\Driver\\gameenum'
---| DEV 0x893e3890 (unnamed) FILE_DEVICE_BUS_EXTENDER
```



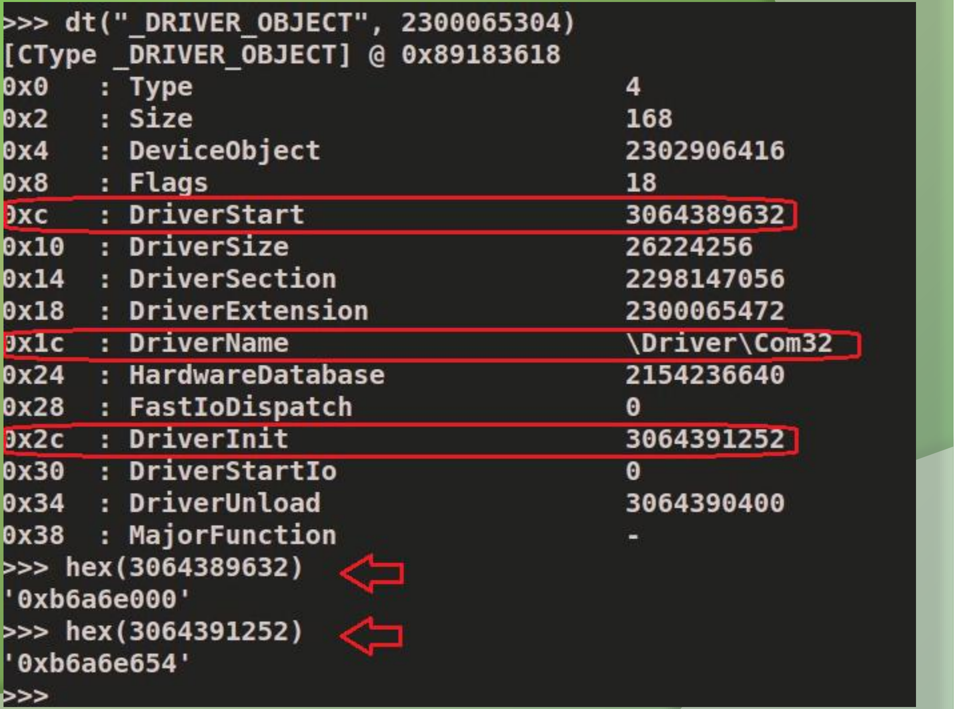
```
root@bt:~/Volatility# python vol.py -f darkmegi.vmem driverirp -r com32
Volatile Systems Volatility Framework 2.0
DriverStart  Name             IRP                                  IrpAddr      IrpOwner         HookAddr     HookOwn
r
0xb6a6e000   'Com32'          IRP_MJ_CREATE                        0xb6a6e308   com32.sys         -            -
0xb6a6e000   'Com32'          IRP_MJ_CREATE_NAMED_PIPE             0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_CLOSE                         0xb6a6e308   com32.sys         -            -
0xb6a6e000   'Com32'          IRP_MJ_READ                          0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_WRITE                         0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_QUERY_INFORMATION             0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_SET_INFORMATION               0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_QUERY_EA                      0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_SET_EA                        0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_FLUSH_BUFFERS                 0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_QUERY_VOLUME_INFORMATION      0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_SET_VOLUME_INFORMATION        0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_DIRECTORY_CONTROL             0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_FILE_SYSTEM_CONTROL           0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_DEVICE_CONTROL                0xb6a6e322   com32.sys         -            -
0xb6a6e000   'Com32'          IRP_MJ_INTERNAL_DEVICE_CONTROL       0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_SHUTDOWN                      0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_LOCK_CONTROL                  0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_CLEANUP                       0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_CREATE_MAILSLOT               0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_QUERY_SECURITY                0x804f354a   ntoskrnl.exe      -            -
0xb6a6e000   'Com32'          IRP_MJ_SET_SECURITY                  0x804f354a   ntoskrnl.exe      -            -
```

Device and Driver object

Examining the device and driver objects shows the base address and address of DriverEntry routine



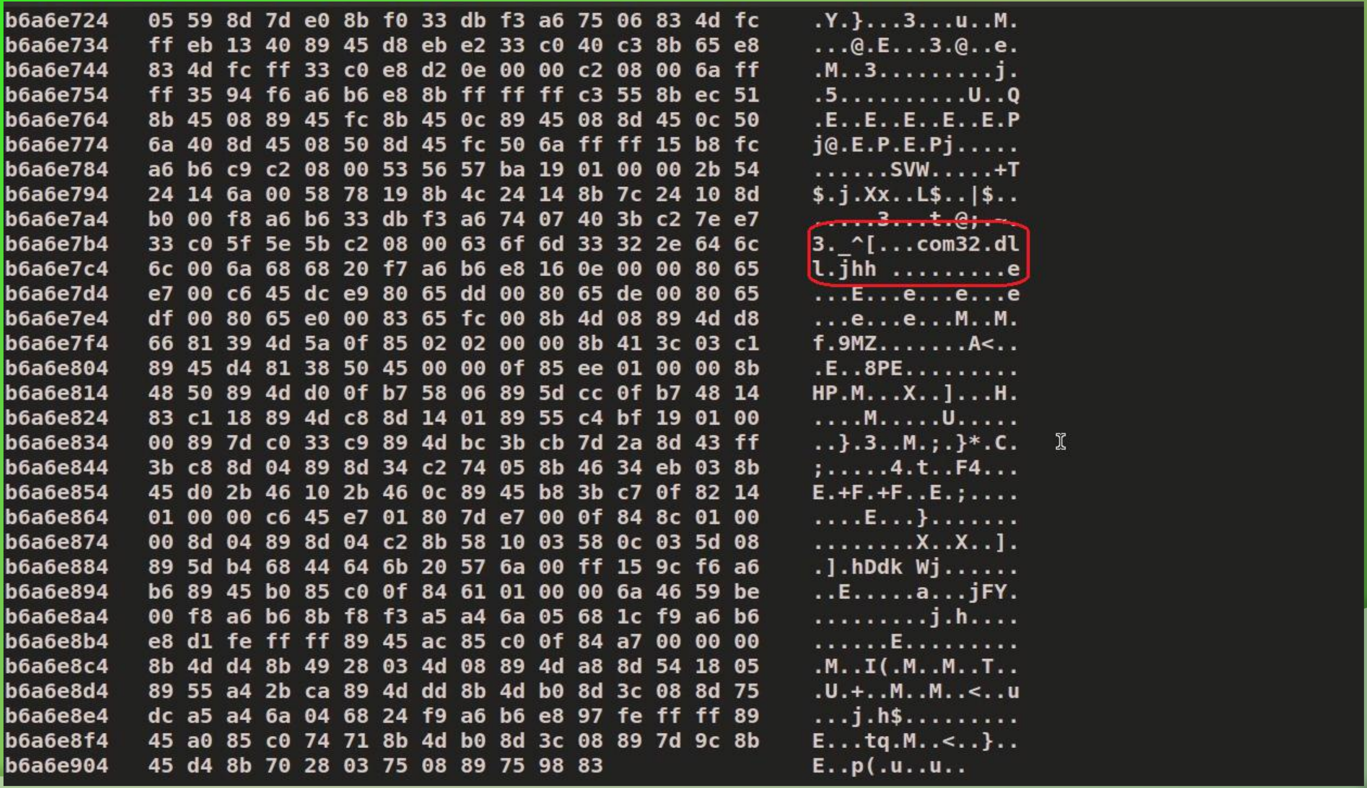
```
>>> dt("_DEVICE_OBJECT", 0x89439030)
[CType _DEVICE_OBJECT] @ 0x89439030
0x0    : Type                          3
0x2    : Size                          184
0x4    : ReferenceCount                0
0x8    : DriverObject                  2300065304
0xc    : NextDevice                    0
0x10   : AttachedDevice                0
0x14   : CurrentIrp                    0
0x18   : Timer                         0
0x1c   : Flags                         64
0x20   : Characteristics               0
0x24   : Vpb                           0
0x28   : DeviceExtension               0
0x2c   : DeviceType                    34
0x30   : StackSize                     1
0x34   : Queue                         2302906468
0x5c   : AlignmentRequirement          0
0x60   : DeviceQueue                   2302906512
0x74   : Dpc                           2302906532
0x94   : ActiveThreadCount             0
0x98   : SecurityDescriptor            3774878712
0x9c   : DeviceLock                    2302906572
0xac   : SectorSize                    0
0xae   : Spare1                        0
0xb0   : DeviceObjectExtension         2302906600
0xb4   : Reserved                      0
```



```
>>> dt("_DRIVER_OBJECT", 2300065304)
[CType _DRIVER_OBJECT] @ 0x89183618
0x0    : Type                          4
0x2    : Size                          168
0x4    : DeviceObject                  2302906416
0x8    : Flags                         18
0xc    : DriverStart                   3064389632
0x10   : DriverSize                    26224256
0x14   : DriverSection                 2298147056
0x18   : DriverExtension               2300065472
0x1c   : DriverName                    \Driver\Com32
0x24   : HardwareDatabase              2154236640
0x28   : FastIoDispatch                0
0x2c   : DriverInit                    3064391252
0x30   : DriverStartIo                 0
0x34   : DriverUnload                  3064390400
0x38   : MajorFunction                 -
>>> hex(3064389632)
'0xb6a6e000'
>>> hex(3064391252)
'0xb6a6e654'
>>>
```

DriverEntry routine

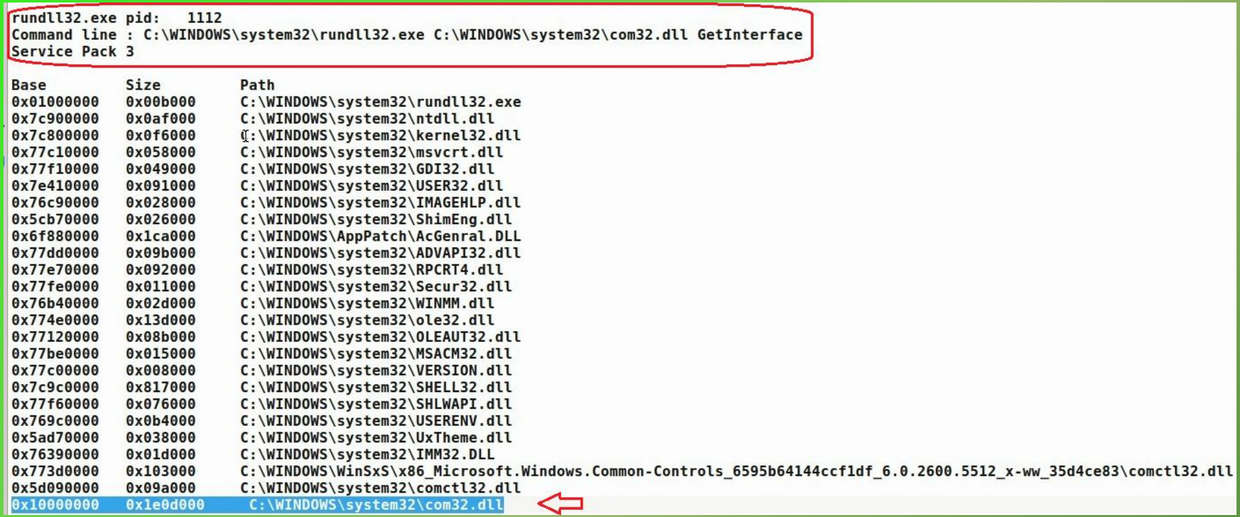
Examining the DriverEntry routine shows the presence of a DLL “com32.dll”



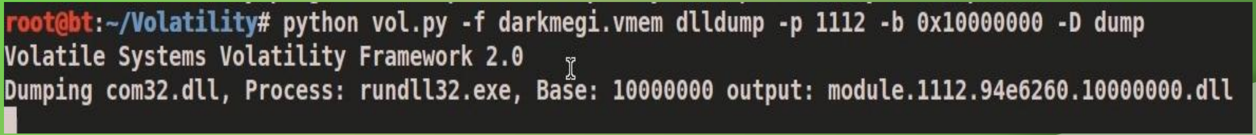
```
b6a6e724   05 59 8d 7d e0 8b f0 33 db f3 a6 75 06 83 4d fc    .Y.}...3...u..M.
b6a6e734   ff eb 13 40 89 45 d8 eb e2 33 c0 40 c3 8b 65 e8    ...@.E...3.@..e.
b6a6e744   83 4d fc ff 33 c0 e8 d2 0e 00 00 c2 08 00 6a ff    .M..3.........j.
b6a6e754   ff 35 94 f6 a6 b6 e8 8b ff ff ff c3 55 8b ec 51    .5..........U..Q
b6a6e764   8b 45 08 89 45 fc 8b 45 0c 89 45 08 8d 45 0c 50    .E..E..E..E..E.P
b6a6e774   6a 40 8d 45 08 50 8d 45 fc 50 6a ff ff 15 b8 fc    j@.E.P.E.Pj.....
b6a6e784   a6 b6 c9 c2 08 00 53 56 57 ba 19 01 00 00 2b 54    ......SVW.....+T
b6a6e794   24 14 6a 00 58 78 19 8b 4c 24 14 8b 7c 24 10 8d    $.j.Xx..L$..|$..
b6a6e7a4   b0 00 f8 a6 b6 33 db f3 a6 74 07 40 3b c2 7e e7    .....3...t.@;.~.
b6a6e7b4   33 c0 5f 5e 5b c2 08 00 63 6f 6d 33 32 2e 64 6c    3._^[...com32.dl
b6a6e7c4   6c 00 6a 68 68 20 f7 a6 b6 e8 16 0e 00 00 80 65    l.jhh .........e
b6a6e7d4   e7 00 c6 45 dc e9 80 65 dd 00 80 65 de 00 80 65    ...E...e...e...e
b6a6e7e4   df 00 80 65 e0 00 83 65 fc 00 8b 4d 08 89 4d d8    ...e...e...M..M.
b6a6e7f4   66 81 39 4d 5a 0f 85 02 02 00 00 8b 41 3c 03 c1    f.9MZ.......A<..
b6a6e804   89 45 d4 81 38 50 45 00 00 0f 85 ee 01 00 00 8b    .E..8PE.........
b6a6e814   48 50 89 4d d0 0f b7 58 06 89 5d cc 0f b7 48 14    HP.M...X..]...H.
b6a6e824   83 c1 18 89 4d c8 8d 14 01 89 55 c4 bf 19 01 00    ....M.....U.....
b6a6e834   00 89 7d c0 33 c9 89 4d bc 3b cb 7d 2a 8d 43 ff    ..}.3..M.;.}*.C.
b6a6e844   3b c8 8d 04 89 8d 34 c2 74 05 8b 46 34 eb 03 8b    ;.....4.t..F4...
b6a6e854   45 d0 2b 46 10 2b 46 0c 89 45 b8 3b c7 0f 82 14    E.+F.+F..E.;....
b6a6e864   01 00 00 c6 45 e7 01 80 7d e7 00 0f 84 8c 01 00    ....E...}.......
b6a6e874   00 8d 04 89 8d 04 c2 8b 58 10 03 58 0c 03 5d 08    ........X..X..].
b6a6e884   89 5d b4 68 44 64 6b 20 57 6a 00 ff 15 9c f6 a6    .].hDdk Wj......
b6a6e894   b6 89 45 b0 85 c0 0f 84 61 01 00 00 6a 46 59 be    ..E.....a...jFY.
b6a6e8a4   00 f8 a6 b6 8b f8 f3 a5 a4 6a 05 68 1c f9 a6 b6    .........j.h....
b6a6e8b4   e8 d1 fe ff ff 89 45 ac 85 c0 0f 84 a7 00 00 00    ......E.........
b6a6e8c4   8b 4d d4 8b 49 28 03 4d 08 89 4d a8 8d 54 18 05    .M..I(.M..M..T..
b6a6e8d4   89 55 a4 2b ca 89 4d dd 8b 4d b0 8d 3c 08 8d 75    .U.+..M..M..<..u
b6a6e8e4   dc a5 a4 6a 04 68 24 f9 a6 b6 e8 97 fe ff ff 89    ...j.h$.........
b6a6e8f4   45 a0 85 c0 74 71 8b 4d b0 8d 3c 08 89 7d 9c 8b    E...tq.M..<..}..
b6a6e904   45 d4 8b 70 28 03 75 08 89 75 98 83                E..p(.u..u..
```

Dumping the DLL from memory

The DLL dumped from the memory, which was loaded by rundll32.exe



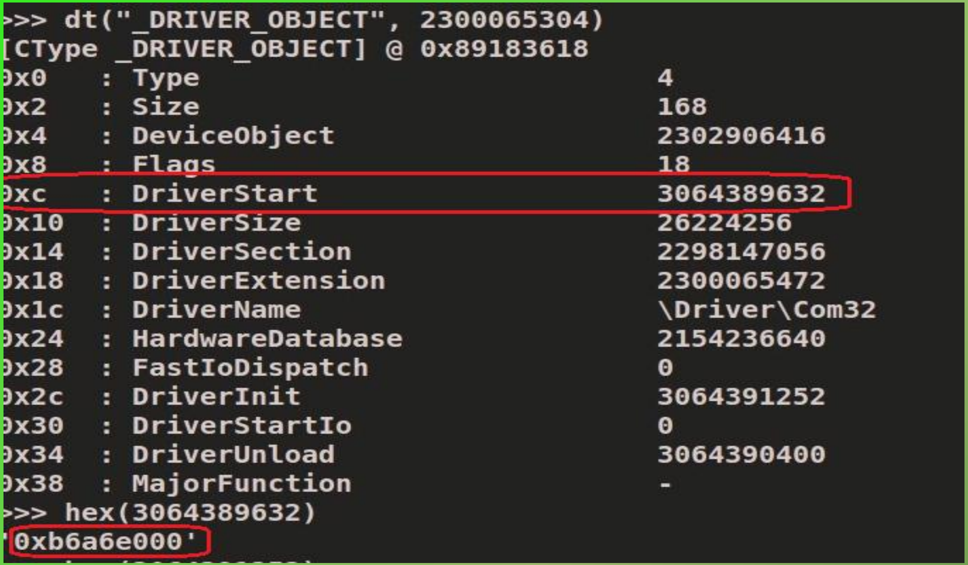
```
rundll32.exe pid:   1112
Command line : C:\WINDOWS\system32\rundll32.exe C:\WINDOWS\system32\com32.dll GetInterface
Service Pack 3

Base         Size         Path
0x01000000   0x00b000     C:\WINDOWS\system32\rundll32.exe
0x7c900000   0x0af000     C:\WINDOWS\system32\ntdll.dll
0x7c800000   0x0f6000     C:\WINDOWS\system32\kernel32.dll
0x77c10000   0x058000     C:\WINDOWS\system32\msvcrt.dll
0x77f10000   0x049000     C:\WINDOWS\system32\GDI32.dll
0x7e410000   0x091000     C:\WINDOWS\system32\USER32.dll
0x76c90000   0x028000     C:\WINDOWS\system32\IMAGEHLP.dll
0x5cb70000   0x026000     C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000     C:\WINDOWS\AppPatch\AcGenral.DLL
0x77dd0000   0x09b000     C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000   0x092000     C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000   0x011000     C:\WINDOWS\system32\Secur32.dll
0x76b40000   0x02d000     C:\WINDOWS\system32\WINMM.dll
0x774e0000   0x13d000     C:\WINDOWS\system32\ole32.dll
0x77120000   0x08b000     C:\WINDOWS\system32\OLEAUT32.dll
0x77be0000   0x015000     C:\WINDOWS\system32\MSACM32.dll
0x77c00000   0x008000     C:\WINDOWS\system32\VERSION.dll
0x7c9c0000   0x817000     C:\WINDOWS\system32\SHELL32.dll
0x77f60000   0x076000     C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000   0x0b4000     C:\WINDOWS\system32\USERENV.dll
0x5ad70000   0x038000     C:\WINDOWS\system32\UxTheme.dll
0x76390000   0x01d000     C:\WINDOWS\system32\IMM32.DLL
0x773d0000   0x103000     C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000   0x09a000     C:\WINDOWS\system32\comctl32.dll
0x10000000   0x1e0d000     C:\WINDOWS\system32\com32.dll
```



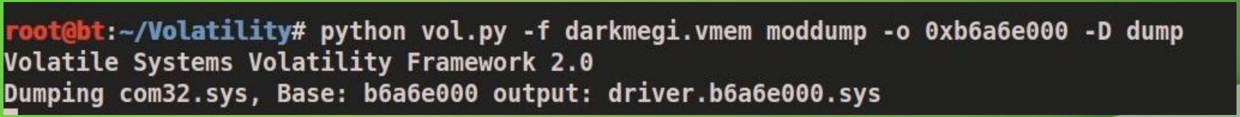
```
root@bt:~/Volatility# python vol.py -f darkmegi.vmem dlldump -p 1112 -b 0x10000000 -D dump
Volatile Systems Volatility Framework 2.0
Dumping com32.dll, Process: rundll32.exe, Base: 10000000 output: module.1112.94e6260.10000000.dll
```

Dumping the Device Driver

Dumping the driver after determining the Driver's base address



```
>>> dt("_DRIVER_OBJECT", 2300065304)
[CType _DRIVER_OBJECT] @ 0x89183618
0x0   : Type                          4
0x2   : Size                          168
0x4   : DeviceObject                  2302906416
0x8   : Flags                         18
0xc   : DriverStart                   3064389632
0x10  : DriverSize                    26224256
0x14  : DriverSection                 2298147056
0x18  : DriverExtension               2300065472
0x1c  : DriverName                    \Driver\Com32
0x24  : HardwareDatabase              2154236640
0x28  : FastIoDispatch                0
0x2c  : DriverInit                    3064391252
0x30  : DriverStartIo                 0
0x34  : DriverUnload                  3064390400
0x38  : MajorFunction                 -
>>> hex(3064389632)
'0xb6a6e000'
```

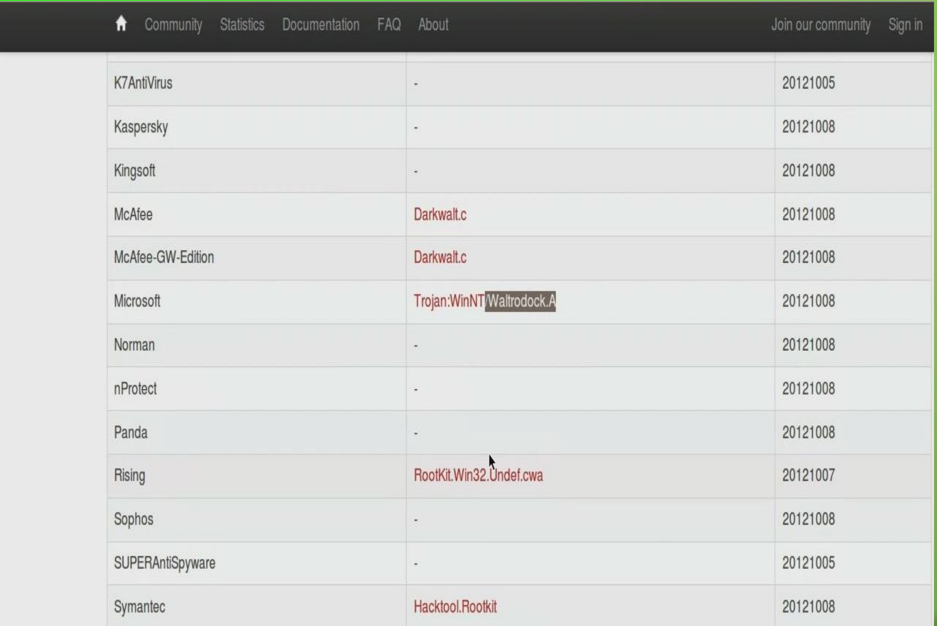


```
root@bt:~/Volatility# python vol.py -f darkmegi.vmem moddump -o 0xb6a6e000 -D dump
Volatile Systems Volatility Framework 2.0
Dumping com32.sys, Base: b6a6e000 output: driver.b6a6e000.sys
```

DLL and Driver Submission

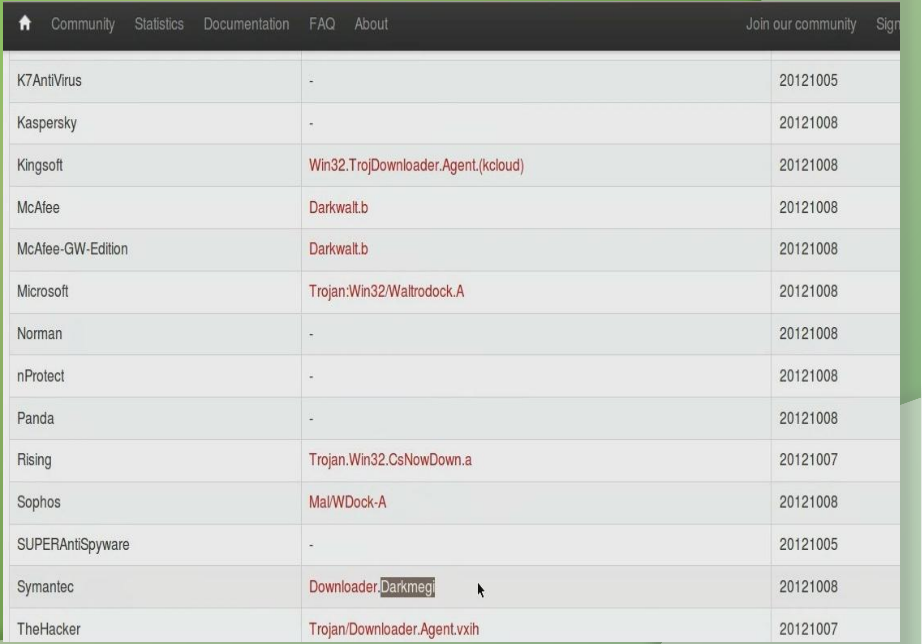
VT confirms the Rootkit component after submitting the samples

VT results for dumped Driver



K7AntiVirus	-	20121005
Kaspersky	-	20121008
Kingsoft	-	20121008
McAfee	Darkwalt.c	20121008
McAfee-GW-Edition	Darkwalt.c	20121008
Microsoft	Trojan:WinNT/Waltrodock.A	20121008
Norman	-	20121008
nProtect	-	20121008
Panda	-	20121008
Rising	RootKit.Win32.Undef.cwa	20121007
Sophos	-	20121008
SUPERAntiSpyware	-	20121005
Symantec	Hacktool.Rootkit	20121008

VT results for dumped DLL



K7AntiVirus	-	20121005
Kaspersky	-	20121008
Kingsoft	Win32.TrojDownloader.Agent.(kcloud)	20121008
McAfee	Darkwalt.b	20121008
McAfee-GW-Edition	Darkwalt.b	20121008
Microsoft	Trojan:Win32/Waltrodock.A	20121008
Norman	-	20121008
nProtect	-	20121008
Panda	-	20121008
Rising	Trojan.Win32.CsNowDown.a	20121007
Sophos	Mal/WDock-A	20121008
SUPERAntiSpyware	-	20121005
Symantec	Downloader.Darkmegi	20121008
TheHacker	Trojan/Downloader.Agent.vxih	20121007

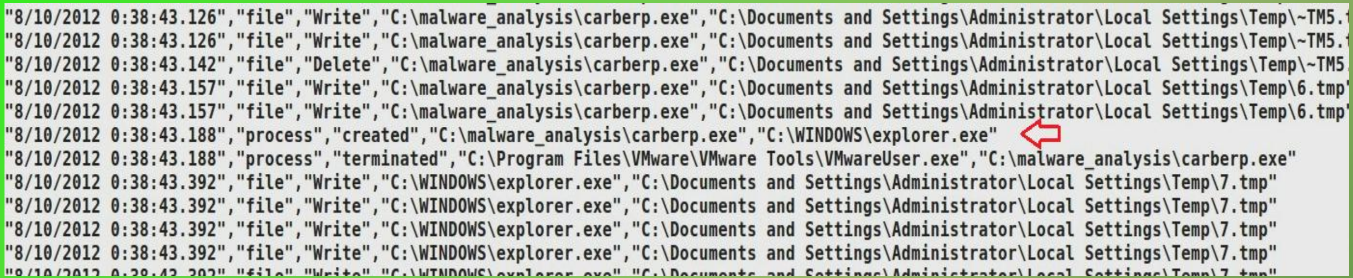
DEMO 4

(CARBERP – SYSCALL PATCH AND INLINE HOOKS)

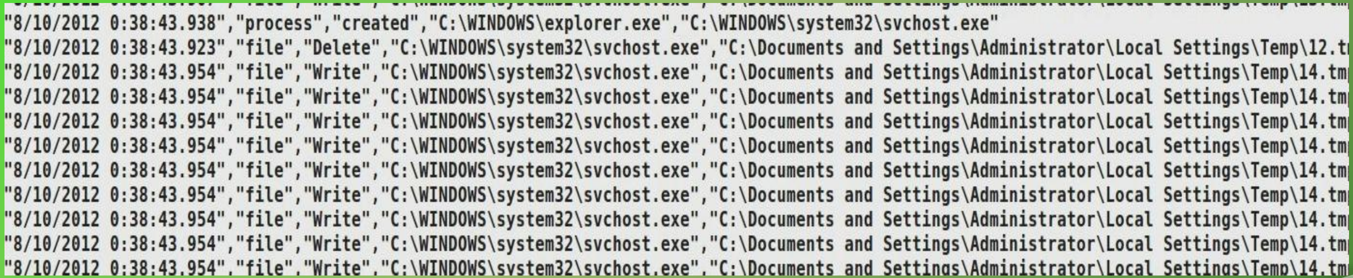
http://youtu.be/ui_qLL3_w7A

Executing the sample carberp.exe

The sample creates .tmp files and invokes explorer.exe and svchost.exe



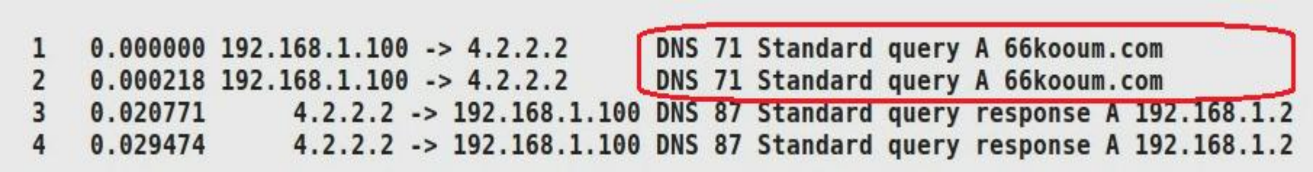
```
"8/10/2012 0:38:43.126","file","Write","C:\malware_analysis\carberp.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\~TM5.t
"8/10/2012 0:38:43.126","file","Write","C:\malware_analysis\carberp.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\~TM5.t
"8/10/2012 0:38:43.142","file","Delete","C:\malware_analysis\carberp.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\~TM5
"8/10/2012 0:38:43.157","file","Write","C:\malware_analysis\carberp.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\6.tmp'
"8/10/2012 0:38:43.157","file","Write","C:\malware_analysis\carberp.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\6.tmp'
"8/10/2012 0:38:43.188","process","created","C:\malware_analysis\carberp.exe","C:\WINDOWS\explorer.exe"
"8/10/2012 0:38:43.188","process","terminated","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\carberp.exe"
"8/10/2012 0:38:43.392","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\7.tmp"
"8/10/2012 0:38:43.392","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\7.tmp"
"8/10/2012 0:38:43.392","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\7.tmp"
"8/10/2012 0:38:43.392","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\7.tmp"
"8/10/2012 0:38:43.392","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\7.tmp"
```



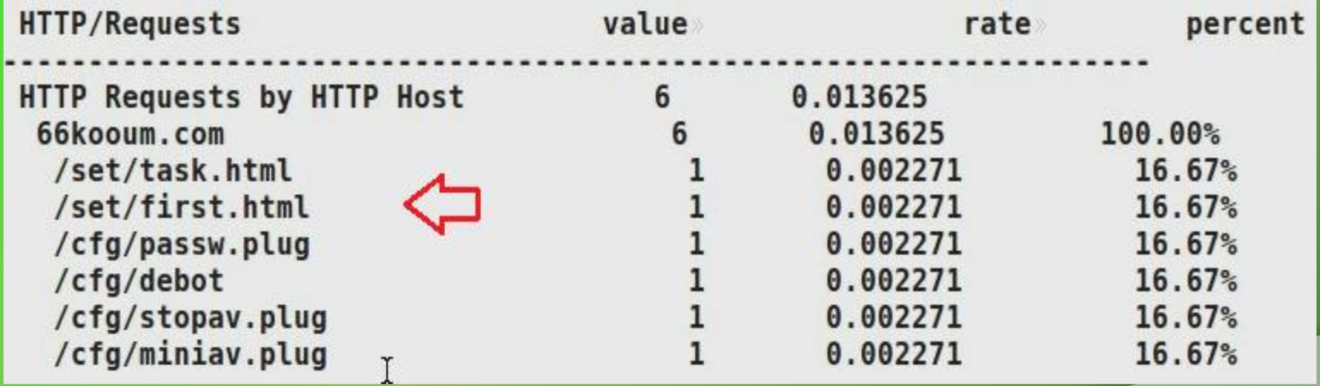
```
"8/10/2012 0:38:43.938","process","created","C:\WINDOWS\explorer.exe","C:\WINDOWS\system32\svchost.exe"
"8/10/2012 0:38:43.923","file","Delete","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\12.t
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
"8/10/2012 0:38:43.954","file","Write","C:\WINDOWS\system32\svchost.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\14.tm
```

Network Activity

Malware performs dns and http activity



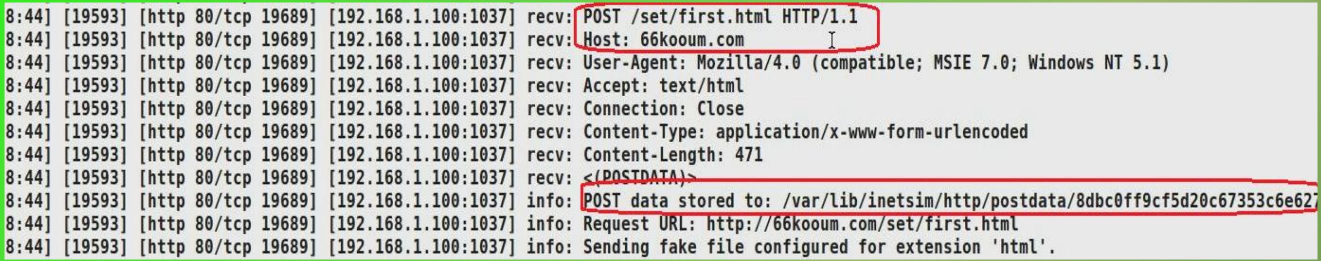
```
1   0.000000 192.168.1.100 -> 4.2.2.2       DNS 71 Standard query A 66kooum.com
2   0.000218 192.168.1.100 -> 4.2.2.2       DNS 71 Standard query A 66kooum.com
3   0.020771       4.2.2.2 -> 192.168.1.100 DNS 87 Standard query response A 192.168.1.2
4   0.029474       4.2.2.2 -> 192.168.1.100 DNS 87 Standard query response A 192.168.1.2
```



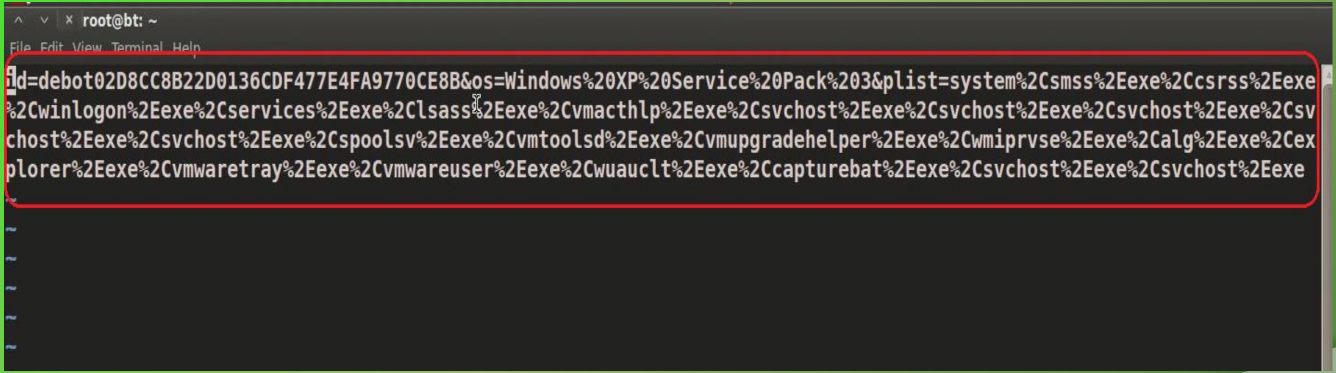
```
HTTP/Requests                         value                  rate       percent
-------------------------------------------------------------------------------
HTTP Requests by HTTP Host               6       0.013625
 66kooum.com                              6       0.013625         100.00%
  /set/task.html                           1       0.002271          16.67%
  /set/first.html                          1       0.002271          16.67%
  /cfg/passw.plug                          1       0.002271          16.67%
  /cfg/debot                               1       0.002271          16.67%
  /cfg/stopav.plug                         1       0.002271          16.67%
  /cfg/miniav.plug                         1       0.002271          16.67%
```

Submits process information

Submits process information on the system to the command and control server



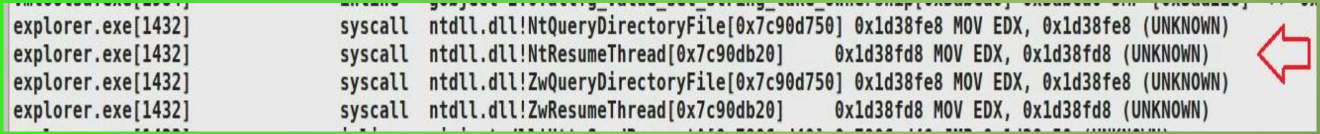
```
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: POST /set/first.html HTTP/1.1
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: Host: 66kooum.com
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: Accept: text/html
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: Connection: Close
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: Content-Type: application/x-www-form-urlencoded
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: Content-Length: 471
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] recv: <(POSTDATA)>
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] info: POST data stored to: /var/lib/inetsim/http/postdata/8dbc0ff9cf5d20c67353c6e627
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] info: Request URL: http://66kooum.com/set/first.html
8:44] [19593] [http 80/tcp 19689] [192.168.1.100:1037] info: Sending fake file configured for extension 'html'.
```



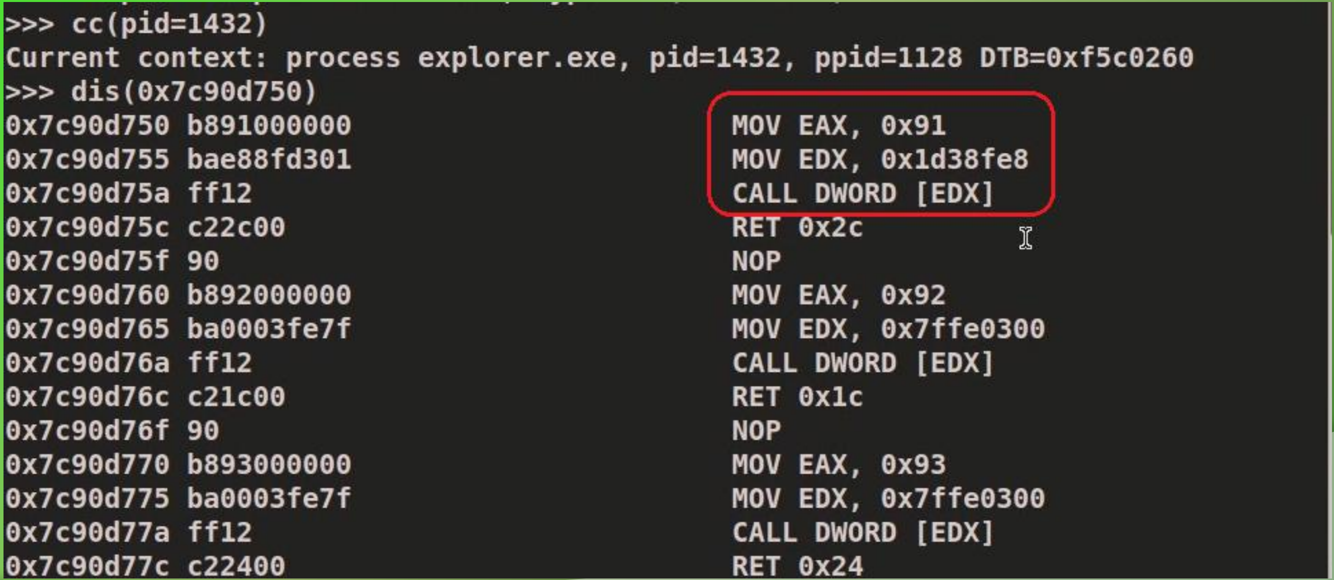
```
id=debot02D8CC8B22D0136CDF477E4FA9770CE8B&os=Windows%20XP%20Service%20Pack%203&plist=system%2Csmss%2Eexe%2Ccsrss%2Eexe
%2Cwinlogon%2Eexe%2Cservices%2Eexe%2Clsass%2Eexe%2Cvmacthlp%2Eexe%2Csvchost%2Eexe%2Csvchost%2Eexe%2Csvchost%2Eexe%2Csv
chost%2Eexe%2Csvchost%2Eexe%2Cspoolsv%2Eexe%2Cvmtoolsd%2Eexe%2Cvmupgradehelper%2Eexe%2Cwmiprvse%2Eexe%2Calg%2Eexe%2Cex
plorer%2Eexe%2Cvmwaretray%2Eexe%2Cvmwareuser%2Eexe%2Cwuauclt%2Eexe%2Ccapturebat%2Eexe%2Csvchost%2Eexe%2Csvchost%2Eexe
~
~
~
~
~
~
```

SYSCALL Patch

Patches SYSCALL in ntdll.dll to hide its presence



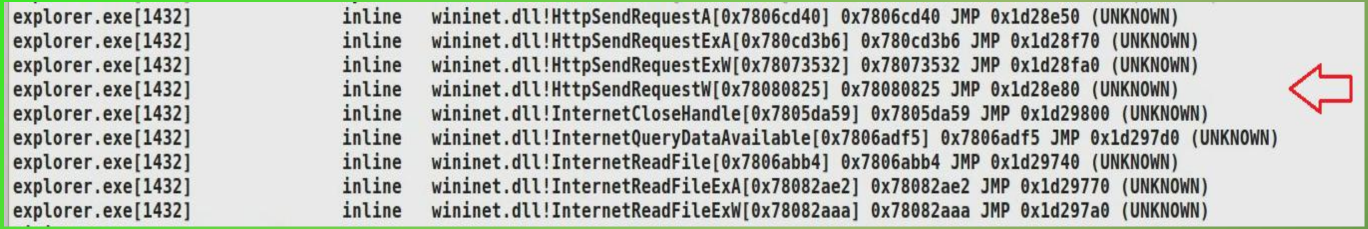
```
explorer.exe[1432]            syscall  ntdll.dll!NtQueryDirectoryFile[0x7c90d750] 0x1d38fe8 MOV EDX, 0x1d38fe8 (UNKNOWN)
explorer.exe[1432]            syscall  ntdll.dll!NtResumeThread[0x7c90db20]     0x1d38fd8 MOV EDX, 0x1d38fd8 (UNKNOWN)
explorer.exe[1432]            syscall  ntdll.dll!ZwQueryDirectoryFile[0x7c90d750] 0x1d38fe8 MOV EDX, 0x1d38fe8 (UNKNOWN)
explorer.exe[1432]            syscall  ntdll.dll!ZwResumeThread[0x7c90db20]     0x1d38fd8 MOV EDX, 0x1d38fd8 (UNKNOWN)
```



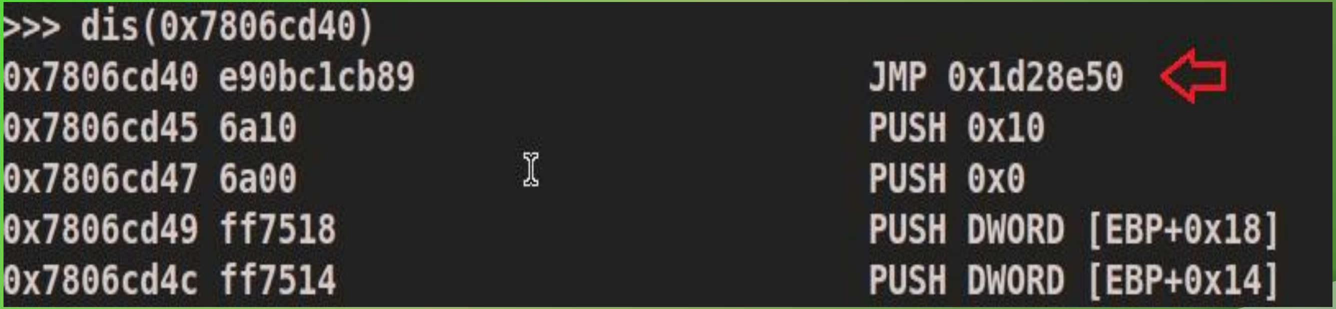
```
>>> cc(pid=1432)
Current context: process explorer.exe, pid=1432, ppid=1128 DTB=0xf5c0260
>>> dis(0x7c90d750)
0x7c90d750 b891000000                      MOV EAX, 0x91
0x7c90d755 bae88fd301                      MOV EDX, 0x1d38fe8
0x7c90d75a ff12                            CALL DWORD [EDX]
0x7c90d75c c22c00                          RET 0x2c
0x7c90d75f 90                              NOP
0x7c90d760 b892000000                      MOV EAX, 0x92
0x7c90d765 ba0003fe7f                      MOV EDX, 0x7ffe0300
0x7c90d76a ff12                            CALL DWORD [EDX]
0x7c90d76c c21c00                          RET 0x1c
0x7c90d76f 90                              NOP
0x7c90d770 b893000000                      MOV EAX, 0x93
0x7c90d775 ba0003fe7f                      MOV EDX, 0x7ffe0300
0x7c90d77a ff12                            CALL DWORD [EDX]
0x7c90d77c c22400                          RET 0x24
```

Inline API Hooks

Hooks API calls to steal http data, the hooking functions points to unknown location



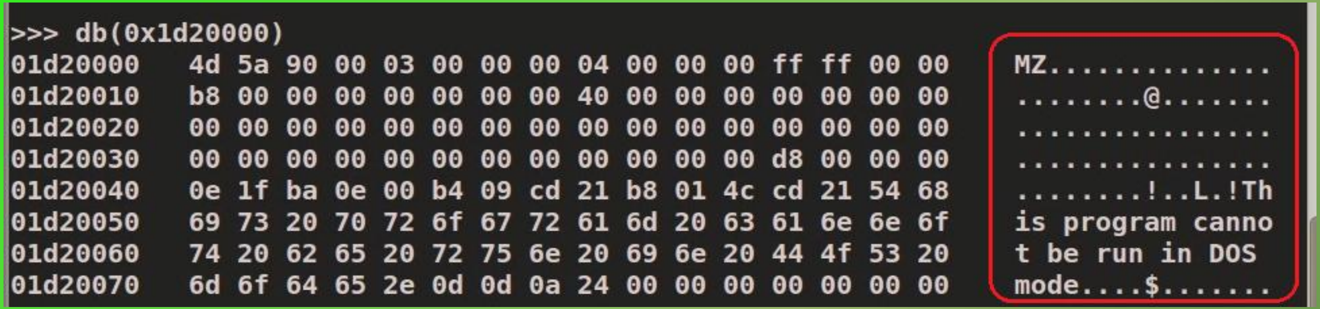
```
explorer.exe[1432]              inline   wininet.dll!HttpSendRequestA[0x7806cd40] 0x7806cd40 JMP 0x1d28e50 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!HttpSendRequestExA[0x780cd3b6] 0x780cd3b6 JMP 0x1d28f70 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!HttpSendRequestExW[0x78073532] 0x78073532 JMP 0x1d28fa0 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!HttpSendRequestW[0x78080825] 0x78080825 JMP 0x1d28e80 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!InternetCloseHandle[0x7805da59] 0x7805da59 JMP 0x1d29800 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!InternetQueryDataAvailable[0x7806adf5] 0x7806adf5 JMP 0x1d297d0 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!InternetReadFile[0x7806abb4] 0x7806abb4 JMP 0x1d29740 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!InternetReadFileExA[0x78082ae2] 0x78082ae2 JMP 0x1d29770 (UNKNOWN)
explorer.exe[1432]              inline   wininet.dll!InternetReadFileExW[0x78082aaa] 0x78082aaa JMP 0x1d297a0 (UNKNOWN)
```



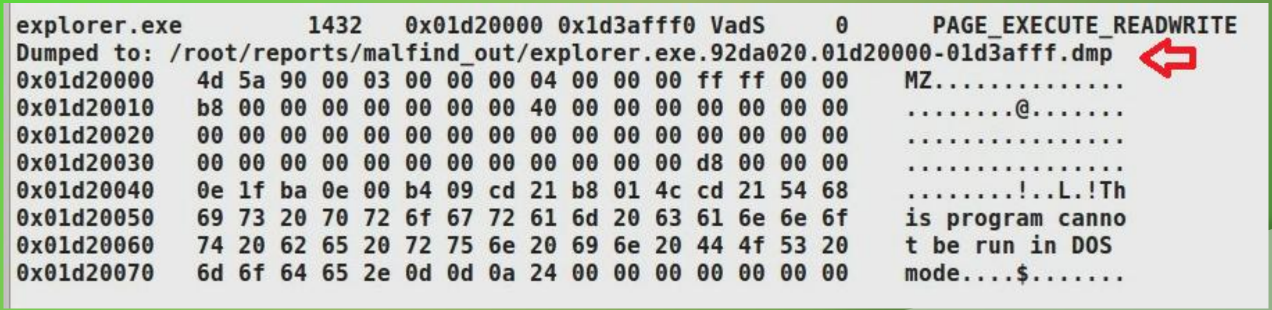
```
>>> dis(0x7806cd40)
0x7806cd40 e90bc1cb89                         JMP 0x1d28e50
0x7806cd45 6a10                               PUSH 0x10
0x7806cd47 6a00                               PUSH 0x0
0x7806cd49 ff7518                             PUSH DWORD [EBP+0x18]
0x7806cd4c ff7514                             PUSH DWORD [EBP+0x14]
```

Embedded Executable

Dumping the embedded executable which was determined by examining the hooking function.



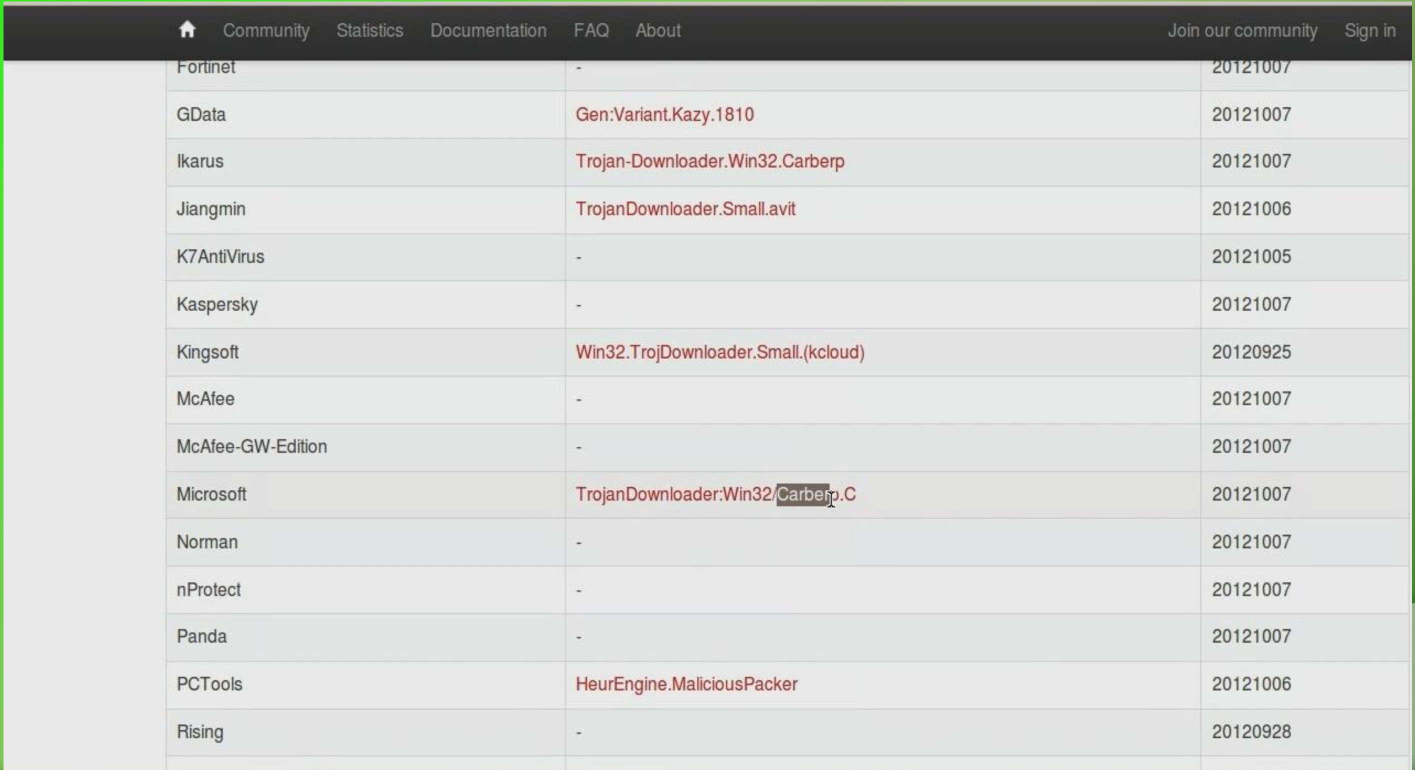
```
>>> db(0x1d20000)
01d20000   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ..............
01d20010   b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    ........@.......
01d20020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
01d20030   00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00    ................
01d20040   0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68    ........!..L.!Th
01d20050   69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    is program canno
01d20060   74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    t be run in DOS 
01d20070   6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    mode....$.......
```



```
explorer.exe         1432   0x01d20000 0x1d3afff0 VadS     0       PAGE_EXECUTE_READWRITE
Dumped to: /root/reports/malfind_out/explorer.exe.92da020.01d20000-01d3afff.dmp
0x01d20000   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ..............
0x01d20010   b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    ........@.......
0x01d20020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x01d20030   00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00    ................
0x01d20040   0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68    ........!..L.!Th
0x01d20050   69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    is program canno
0x01d20060   74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    t be run in DOS 
0x01d20070   6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    mode....$.......
```

Embedded EXE Submission

VirusTotal confirms the executable as component of Carberp



Fortinet	-	20121007
GData	Gen:Variant.Kazy.1810	20121007
Ikarus	Trojan-Downloader.Win32.Carberp	20121007
Jiangmin	TrojanDownloader.Small.avit	20121006
K7AntiVirus	-	20121005
Kaspersky	-	20121007
Kingsoft	Win32.TrojDownloader.Small.(kcloud)	20120925
McAfee	-	20121007
McAfee-GW-Edition	-	20121007
Microsoft	TrojanDownloader:Win32/Carberp.C	20121007
Norman	-	20121007
nProtect	-	20121007
Panda	-	20121007
PCTools	HeurEngine.MaliciousPacker	20121006
Rising	-	20120928

Reference

- Complete Reference Guide for Reversing & Malware Analysis Training

Thank You !

www.SecurityXploded.com