Case Study – Rootkit Analysis

Monnappa (m0nna)

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

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
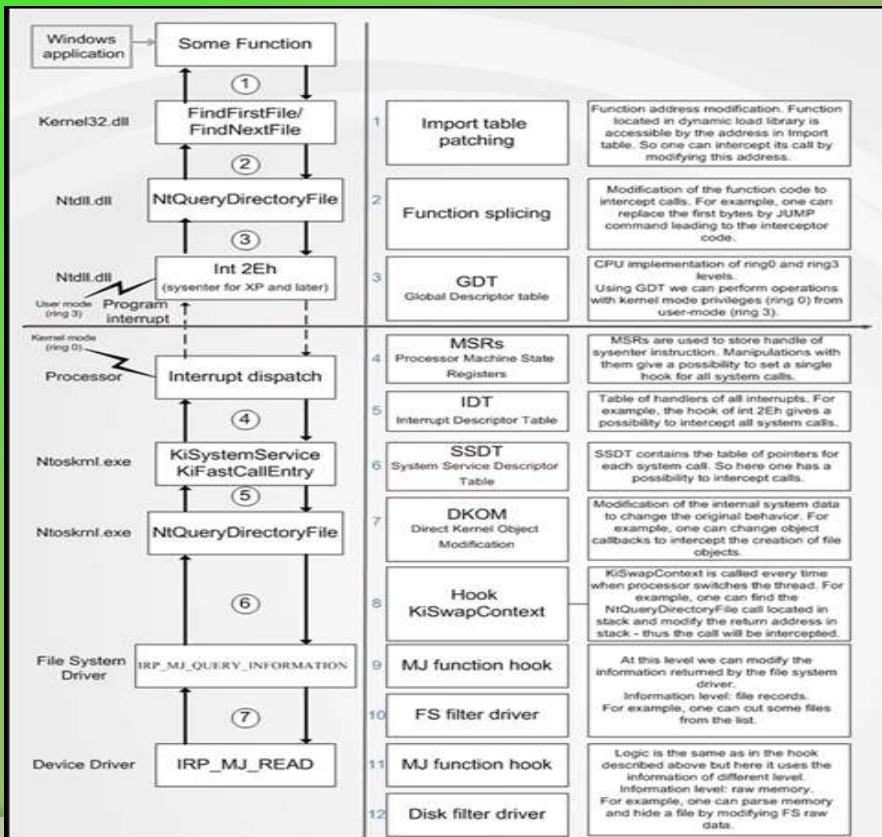
NOTE

➤ **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

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
```

Rootkit Submission to VirusTotal

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

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"
```

```
.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"
.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

Sends Spam

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

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
```
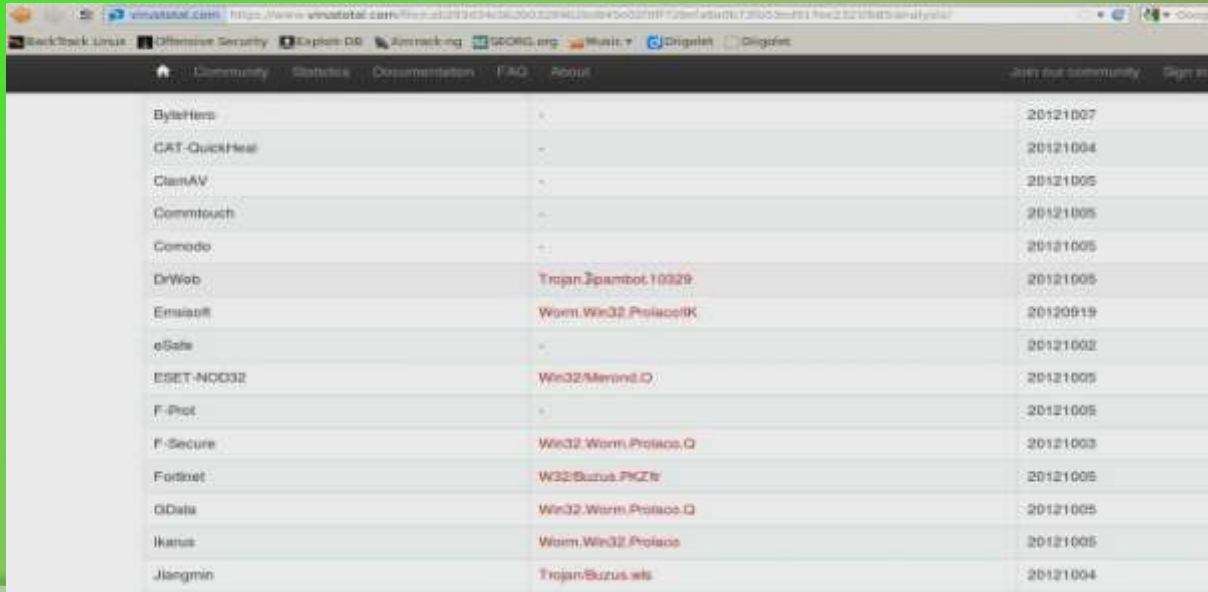
Hides Process from security tool

Hides the process from process explorer

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 09:22:58
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	0x0f5c02a0	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

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

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"

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

VT results for dumped DLL

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

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

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

Reference

➢ [Complete Reference Guide for Reversing & Malware Analysis Training](#)

Thank You !

www.SecurityXploded.com