

Malware Analysis Report using Rekall

Tigger Trojan

Sality

Silent Banker

Introduction

In this tutorial we are tasked to install Rekall, an advanced forensic and incident response framework, to safely study malicious malware from Virus Share (Where we will get most of our source code to Malware that I will study).

Installing Rekall

First, you'll need to install python 3.6 to help run Rekall. Click the link <https://www.python.org/downloads/release/python-360/> and scroll until you see, “Windows x86-64 executable installer” and follow the installation process along with check marking

Files

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		3f7062ccf8be76491884d0e47ac8b251	22256403	SIG
XZ compressed source tarball	Source release		82b143ebbf4514d7e05876bed7a6b1f5	16805836	SIG
Mac OS X 64-bit/32-bit installer	macOS	for Mac OS X 10.6 and later	72acb0175e7622dec7e1b160a43b8c42	27442222	SIG
Windows help file	Windows		6a842a15ab3b4aa316c91a9779db82ec	7940890	SIG
Windows x86-64 embeddable zip file	Windows	for AMD64/EM64T/x64	0ec0caeaa75bae5d2771cf619917c71f	6925798	SIG
<u>Windows x86-64 executable installer</u>	Windows	for AMD64/EM64T/x64	71c9d30c1110abf7f80a428970ab8ec2	31505640	SIG
Windows x86-64 web-based installer	Windows	for AMD64/EM64T/x64	25b8b6c93a098dfade3b014630f9508e	1312376	SIG
Windows x86 embeddable zip file	Windows		1adf2fb735c5000af32d42c39136727c	6315855	SIG
Windows x86 executable installer	Windows		38d9b036b25725f6acb553d4aece4db4	30566536	SIG
Windows x86 web-based installer	Windows		f71f4590be2cc5cdc43069594d4ea98d	1286984	SIG

11/30/2021

, “ADD TO PATH”.



Then pull command prompt and type, “curl <https://bootstrap.pypa.io/get-pip.py> -o get-pip.py” Results should like as the picture below.

```
C:\> curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py
  % Total    % Received % Xferd  Average Speed   Time     Time      Current
               Dload  Upload Total   Spent    Left Speed
100 2108k  100 2108k    0      0 2108k      0:00:01  0:00:01 --:--:-- 1822k

C:\> python get-pip.py
C:\Python\Python39\lib\site-packages\setuptools\distutils_patch.py:25: UserWarning: Distutils was imported before Setuptools.
This usage is discouraged and may exhibit undesirable behaviors or errors. Please use Setuptools' objects directly or at least
import Setuptools first.
  warnings.warn(
Collecting pip
  Downloading pip-21.3.1-py3-none-any.whl (1.7 MB)
    |████████| 1.7 MB 2.2 MB/s
Collecting wheel
  Downloading wheel-0.37.0-py2.py3-none-any.whl (35 kB)
Installing collected packages: wheel, pip
  Attempting uninstall: pip
    Found existing installation: pip 20.2.3
    Uninstalling pip-20.2.3:
      Successfully uninstalled pip-20.2.3
Successfully installed pip-21.3.1 wheel-0.37.0

C:\>
```

Then, go to this Github page <https://github.com/google/rekall/releases> and download the file, “Rekall_1.7.2.p1_Hurricane.Ridge_x64.exe” and follow it’s directions. For simplicity if prompt on where to put folder put it under C:\\Program Files and make a folder called Rekall and install there.



Then pull up the command prompt on that C:\\Program File\\ and type in, “cd \\program files\\rekall” and type in another line, “rekal --live API” Then your Rekall set and ready to analyze malware.

```
Administrator: Command Prompt - rekal --live API
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd \program files\rekall
C:\Program Files\Rekall>rekal --live API

-----
The Rekall Digital Forensic/Incident Response framework 1.7.2.rc1 (Hurricane Ridge).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

[1] Live (API) 13:26:37>
```

Note: When you have your downloaded malware, be sure to place them under the same Rekall folder that you made in your C drive.

11/30/2021

Name	Date modified	Type	Size
IPython	12/10/2021 1:23 PM	File folder	
certifi	12/10/2021 1:23 PM	File folder	
base_library	12/14/2017 9:52 PM	WinRAR ZIP archive	
zeus.vmem	8/15/2010 3:18 PM	VMEM File	131
tigger.vmem	8/15/2010 3:27 PM	VMEM File	131
silentbanker.vmem	8/15/2010 3:02 PM	VMEM File	131
sality.vmem	8/15/2010 1:44 PM	VMEM File	131
laqma.vmem	8/15/2010 3:14 PM	VMEM File	131
coreflood.vmem	8/15/2010 2:24 PM	VMEM File	131
adware.vmem	1/29/2018 5:59 AM	VMEM File	131
yara	11/2/2017 5:52 PM	Python Extension ...	
yara.cp36-win_amd64	12/14/2017 9:55 PM	Python Extension ...	
win32wnet	11/2/2017 5:52 PM	Python Extension ...	
win32ui	11/2/2017 5:52 PM	Python Extension ...	

Key Commands:

These will be the key commands that we will be using to observe and analyze our Malware.

- Pslist
- Psxview
- Pstree
- Memdump
- Connscan
- Sockets
- Cmdscan
- Malfind
- Hooks_inline #####
- Netstat
- Netscan
- Procinfo
- Moddump

Malware Analyst 1: Tigger Trojan

Background: Is a Trojan that installs a rootkit to gain access to a computer for their admin privileges. It can disable windows security and steal crucial and valuable

11/30/2021

information that is stored on the computer like web cookies, log keystrokes, and could install spy code to stalk a user's browser activity.

```
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Rekall>rekal --filename tigger.vmem

-----
The Rekall Digital Forensic/Incident Response framework 1.7.2.rc1 (Hurricane Ridge).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

-----
```

```
1 tigger.vmem 17:38:38 pslist
2021-12-10 17:38:40,974:WARNING:rekal:1:Inventory for repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget to create an inventory? You must use the tools/profiles/build_profile_repo.py tool with the --inventory flag.
2021-12-10 17:38:40,975:WARNING:rekal:1:Repository http://profiles.rekall-forensic.com will be disabled.
-----> pslist()
 _EPROCESS      name    pid   ppid  thread_count handle_count session_id wow64    process_create_time    process_exit_time
-----
```

_EPROCESS	name	pid	ppid	thread_count	handle_count	session_id	wow64	process_create_time	process_exit_time
0x810b1600	System	4	0	61	179	-	False	-	-
0xf2f5a7e0	alg.exe	216	676	7	108	0	False	2010-08-11 06:06:392	-
0xf3667e8	VmwareTray.exe	432	1724	1	49	0	False	2010-08-11 06:09:312	-
0xf374988	VmwareUser.exe	452	1724	8	204	0	False	2010-08-11 06:09:322	-
0x80f1a4588	wuauctl.exe	888	1028	4	131	0	False	2010-08-11 06:09:377	-
0xf2f5a7e0	smss.exe	544	0	3	21	0	False	2010-08-11 06:06:212	-
0xf1fcd00	svrsvcs.exe	600	544	10	405	0	False	2010-08-11 06:06:232	-
0xf1fcd00	winlogon.exe	632	544	22	519	0	False	2010-08-11 06:06:237	-
0xf2d7020	services.exe	676	632	16	269	0	False	2010-08-11 06:06:242	-
0xf2f5a7e0	lsass.exe	688	632	21	348	0	False	2010-08-11 06:06:242	-
0xf2f2dd0	wmiprvse.exe	828	856	9	214	0	False	2010-08-15 19:26:082	-
0xf2f28230	vmacthlp.exe	844	676	1	24	0	False	2010-08-11 06:06:242	-
0x80ff88d8	svchost.exe	856	676	18	202	0	False	2010-08-11 06:06:242	-
0xf364310	wscntfy.exe	888	1028	1	27	0	False	2010-08-11 06:06:492	-
0xf2f17500	svchost.exe	936	676	9	270	0	False	2010-08-11 06:06:242	-
0x80ffbf910	svchost.exe	1028	676	88	1395	0	False	2010-08-11 06:06:242	-
0xf3b5f8	TPAutoConnect.e	1084	1968	1	61	0	False	2010-08-11 06:06:522	-
0xf1f2a558	svchost.exe	1088	676	7	88	0	False	2010-08-11 06:06:579	-
0xf1f2a558	svchost.exe	1140	676	15	210	0	False	2010-08-11 06:06:579	-
0xf1f17600	poolsv.exe	1432	676	14	137	0	False	2010-08-11 06:06:267	-
0xf1f18828	vttoolsd.exe	1668	676	5	218	0	False	2010-08-11 06:06:357	-
0xf3b65c0	explorer.exe	1724	1708	13	314	0	False	2010-08-11 06:09:392	-
0x80f60da0	wuauctl.exe	1732	1028	7	178	0	False	2010-08-11 06:07:447	-
0xf1f1fd88	VMUpgradeHelper	1788	676	5	100	0	False	2010-08-11 06:06:382	-
0xf1f43b28	TPAutoConnSvc.e	1968	676	5	100	0	False	2010-08-11 06:06:392	-

```
Out: 17:38:46 Plugin: pslist (WinPsList)
```

11/30/2021

```
[1] tigger.vmem 17:44:06> connscan
-----> connscan()
tcpip/GUID/9546A8399BAC4717BC41758594EF0D9C2 matched offset 0x4562+0xf3ba9000=0 offset_p      local_net_address      remote_net_address      pid
0x2214988 172.16.176.143:1034      131.107.115.254:80      1260
0x6015ab0 172.16.176.143:1037      131.107.115.254:443      1260
Out<17:44:09> Plugin: connscan (ConnScan)

[1] tigger.vmem 18:02:55> pstree
-----> pstree()
_EPROCESS          ppid  thd_count hnd_count      create_time
-----
0x810b1660 System (4)          0      61      179 - 
. 0xff2ab020 smss.exe (544)      4      3      21 2010-08-11 06:06:21Z
.. 0xff1ecda0 csrss.exe (608)      544     10      405 2010-08-11 06:06:23Z
... 0xff1ec978 winlogon.exe (632)      544     22      519 2010-08-11 06:06:23Z
.... 0xff247020 services.exe (676)      632     16      269 2010-08-11 06:06:24Z
..... 0xff25a7e0 alg.exe (216)      676      7      108 2010-08-11 06:06:39Z
..... 0xff218230 vmacthlp.exe (844)      676      1      24 2010-08-11 06:06:24Z
.... 0x80ff88d8 svchost.exe (856)      676     18      202 2010-08-11 06:06:24Z
.... 0xff27d4d0 wmprvse.exe (828)      856      9      214 2010-08-15 19:26:08Z
.... 0xff217560 svchost.exe (936)      676      9      270 2010-08-11 06:06:24Z
.... 0x80fbf910 svchost.exe (1028)      676     88      1395 2010-08-11 06:06:24Z
..... 0x80f94588 wuauctl.exe (468)      1028      4      131 2010-08-11 06:09:37Z
..... 0xff364310 wscntfy.exe (888)      1028      1      27 2010-08-11 06:06:49Z
..... 0x80f60da0 wuauctl.exe (1732)      1028      7      178 2010-08-11 06:07:44Z
.... 0xff22d558 svchost.exe (1088)      676      7      80 2010-08-11 06:06:25Z
.... 0xff203b80 svchost.exe (1148)      676     15      210 2010-08-11 06:06:26Z
.... 0xff1d7da0 spoolsv.exe (1432)      676     14      137 2010-08-11 06:06:26Z
.... 0xff1b8b28 vmtoolsd.exe (1668)      676      5      218 2010-08-11 06:06:35Z
.... 0xff1fdc88 VMUpgradeHelper (1788)      676      5      100 2010-08-11 06:06:38Z
.... 0xff143b28 TPAutoConnSvc.e (1968)      676      5      100 2010-08-11 06:06:39Z
.... 0xff38b5f8 TPAutoConnect.e (1084)      1968      1      61 2010-08-11 06:06:52Z
... 0xff255020 lsass.exe (688)      632     21      348 2010-08-11 06:06:24Z
. 0xff3865d0 explorer.exe (1724)      1708     13      314 2010-08-11 06:09:29Z
. 0xff3667e8 VMwareTray.exe (432)      1724      1      49 2010-08-11 06:09:31Z
. 0xff374980 VMwareUser.exe (452)      1724      8      204 2010-08-11 06:09:32Z
Out<18:02:56> Plugin: pstree (PSTree)

[1] tigger.vmem 18:02:56>

[1] tigger.vmem 17:47:28> sockets
-----> sockets()
offset_v  pid   port  proto  protocol      address      create_time
-----
0x80fd1008    4     0    47  GRE      0.0.0.0      2010-08-11 06:08:00Z
0xff258008   688    500   17  UDP      0.0.0.0      2010-08-11 06:06:35Z
0xff367008    4    445    6  TCP      0.0.0.0      2010-08-11 06:06:17Z
0x80fffc128   936    135    6  TCP      0.0.0.0      2010-08-11 06:06:24Z
0x80f62e98   1028   1053   17  UDP      127.0.0.1      2010-08-15 19:26:50Z
0xff225b70   688     0  255  Reserved  0.0.0.0      2010-08-11 06:06:35Z
0xff254008   1028    123   17  UDP      127.0.0.1      2010-08-15 19:26:50Z
0x80fce930   1088   1025   17  UDP      0.0.0.0      2010-08-11 06:06:38Z
0xff127d28   216    1026    6  TCP      127.0.0.1      2010-08-11 06:06:39Z
0xff12b580   1148   1900   17  UDP      127.0.0.1      2010-08-15 19:26:50Z
0xff1b8250   688    4500   17  UDP      0.0.0.0      2010-08-11 06:06:35Z
0xff382e98     4    1033    6  TCP      0.0.0.0      2010-08-11 06:08:00Z
0x80fbdc40     4    445   17  UDP      0.0.0.0      2010-08-11 06:06:17Z
Out<17:47:29> Plugin: sockets (Sockets)
```

11/30/2021

```
[1] tigger.vmem 18:05:53> psxview
-----> psxview()
_EPROCESS      name      pid PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
-----
0x810b1660 System        4 True      False  True  False  True  True
0xff25a7e0 alg.exe     216 True      True  True  True  True  True
0xff3667e8 VMwareTray.exe 432 True      True  True  True  True  True
0xff374980 VMwareUser.exe 452 True      True  True  True  True  True
0x80f94588 wuauctl.exe 468 True      True  True  True  True  True
0xff3802c8 cmd.exe     532 False     False False  False  True  False
0xff2ab020 smss.exe    544 True      False True  False  True  True
0xff1ecda0 csrss.exe   608 True      False True  True  True  True
0xff1ec978 winlogon.exe 632 True      True  True  True  True  True
0xff247020 services.exe 676 True      True  True  True  True  True
0xff255020 lsass.exe   688 True      True  True  True  True  True
0xff27d4d0 wmpirvse.exe 828 True      True  True  True  True  True
0xff218230 vmauthlp.exe 844 True      True  True  True  True  True
0x80ff88d8 svchost.exe 856 True      True  True  True  True  True
0xff364310 wscntfy.exe 888 True      True  True  True  True  True
0xff217560 svchost.exe 936 True      True  True  True  True  True
0x80fbf910 svchost.exe 1028 True     True  True  True  True  True
0xff38b5f8 TPAutoConnect.e 1084 True     True  True  True  True  True
0xff22d558 svchost.exe 1088 True     True  True  True  True  True
0xff203b80 svchost.exe 1148 True     True  True  True  True  True
0xff1ebc08 logonui.exe 1168 False     False False  False  True  False
0xff1d7da0 spoolsv.exe 1432 True     True  True  True  True  True
0xff1b8b28 vmtoolsd.exe 1668 True     True  True  True  True  True
0xff3865d0 explorer.exe 1724 True     True  True  True  True  True
0x80f60da0 wuauctl.exe 1732 True     True  True  True  True  True
0xff1fdc88 VMUpgradeHelper 1788 True     True  True  True  True  True
0xff143b28 TPAutoConnSv.c.e 1968 True     True  True  True  True  True
Out<18:05:58> Plugin: psxview (WindowsPsxView)
[1] tigger.vmem 18:05:58>
```

```
[1] tigger.vmem 19:40:45> hooks_iat 1028
-----> hooks_iat(1028)
      source          target       target_func
-----
Process svchost.exe (1028)
-----
Out<19:40:46> Plugin: hooks_iat (IATHooks)
[1] tigger.vmem 19:40:46>
```

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal -filename tigger.vmem
1 tigger.vmem 19:30:46: malfind
2021-10-10 19:30:48,101:WARNING:rekal:1:Inventory for repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget to create an inventory? You must use the tools/profiling/build_profile_repo.py tool with the --inventory flag.
2021-10-10 19:30:48,104:WARNING:rekal:1:Repository http://profiles.rekall-forensic.com will be disabled.
malfind()
*****
Process: csrss.exe Pid: 608 Address: 0x7ff00000
Vad Tag: Vad Protection: EXECUTE_READWRITE
Protection: 6

0x7ff6f00000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x7ff6f00000
0x7ff6f0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
0x7ff6f0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
0x7ff6f0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
***** vad_0x7ff6f00000 : 0x7ff6f00000
0x7ff6f0000 0x00 0000 add byte ptr [eax], al
0x7ff6f0002 0x2 0000 add byte ptr [eax], al
0x7ff6f0004 0x4 0000 add byte ptr [eax], al
0x7ff6f0006 0x5 0000 add byte ptr [eax], al
0x7ff6f0008 0x6 0000 add byte ptr [eax], al
0x7ff6f000a 0xa 0000 add byte ptr [eax], al
0x7ff6f000c 0xc 0000 add byte ptr [eax], al
0x7ff6f000e 0xe 0000 add byte ptr [eax], al
0x7ff6f0010 0x10 0000 add byte ptr [eax], al
0x7ff6f0012 0x12 0000 add byte ptr [eax], al
0x7ff6f0014 0x14 0000 add byte ptr [eax], al
0x7ff6f0016 0x15 0000 add byte ptr [eax], al
0x7ff6f0018 0x18 0000 add byte ptr [eax], al
0x7ff6f001a 0x1a 0000 add byte ptr [eax], al
0x7ff6f001c 0x1c 0000 add byte ptr [eax], al
0x7ff6f001e 0x1e 0000 add byte ptr [eax], al
0x7ff6f0020 0x1f 0000 add byte ptr [eax], al
0x7ff6f0022 0x2 0000 add byte ptr [eax], al
0x7ff6f0024 0x24 0000 add byte ptr [eax], al
0x7ff6f0026 0x26 0000 add byte ptr [eax], al
0x7ff6f0028 0x28 0000 add byte ptr [eax], al
0x7ff6f002a 0x2a 0000 add byte ptr [eax], al
0x7ff6f002c 0x2c 0000 add byte ptr [eax], al
0x7ff6f002e 0x2e 0000 add byte ptr [eax], al
0x7ff6f0030 0x30 0000 add byte ptr [eax], al
0x7ff6f0032 0x32 0000 add byte ptr [eax], al
0x7ff6f0034 0x34 0000 add byte ptr [eax], al
0x7ff6f0036 0x35 0000 add byte ptr [eax], al
0x7ff6f0038 0x37 0000 add byte ptr [eax], al
0x7ff6f003a 0x3a 0000 add byte ptr [eax], al
0x7ff6f003c 0x3c 0000 add byte ptr [eax], al
0x7ff6f003e 0x3e 0000 add byte ptr [eax], al
0x7ff6f0040 0x40 0000 add byte ptr [eax], al
0x7ff6f0042 0x42 0000 add byte ptr [eax], al
0x7ff6f0044 0x44 0000 add byte ptr [eax], al
0x7ff6f0046 0x46 0000 add byte ptr [eax], al
0x7ff6f0048 0x48 0000 add byte ptr [eax], al
0x7ff6f004a 0x4a 0000 add byte ptr [eax], al
0x7ff6f004c 0x4c 0000 add byte ptr [eax], al
***** vad_0x7ff6f00000 : 0x7ff6f00000
0x7ff6f004e 0x4e 0000 add byte ptr [eax], al
0x7ff6f004f 0x4f 0000 add byte ptr [eax], al
0x7ff6f0050 0x50 0000 add byte ptr [eax], al
0x7ff6f0052 0x52 0000 add byte ptr [eax], al
0x7ff6f0054 0x54 0000 add byte ptr [eax], al
0x7ff6f0056 0x56 0000 add byte ptr [eax], al
0x7ff6f0058 0x58 0000 add byte ptr [eax], al
0x7ff6f005a 0x5a 0000 add byte ptr [eax], al
0x7ff6f005c 0x5c 0000 add byte ptr [eax], al
0x7ff6f005e 0x5e 0000 add byte ptr [eax], al
0x7ff6f0060 0x5f 0000 add byte ptr [eax], al
0x7ff6f0062 0x62 0000 add byte ptr [eax], al
0x7ff6f0064 0x64 0000 add byte ptr [eax], al
0x7ff6f0066 0x66 0000 add byte ptr [eax], al
0x7ff6f0068 0x68 0000 add byte ptr [eax], al
0x7ff6f006a 0x6a 0000 add byte ptr [eax], al
0x7ff6f006c 0x6c 0000 add byte ptr [eax], al
0x7ff6f006e 0x6e 0000 add byte ptr [eax], al
0x7ff6f0070 0x70 0000 add byte ptr [eax], al
0x7ff6f0072 0x72 0000 add byte ptr [eax], al
0x7ff6f0074 0x74 0000 add byte ptr [eax], al
0x7ff6f0076 0x76 0000 add byte ptr [eax], al
0x7ff6f0078 0x78 0000 add byte ptr [eax], al
0x7ff6f007a 0x7a 0000 add byte ptr [eax], al
0x7ff6f007c 0x7c 0000 add byte ptr [eax], al
0x7ff6f007e 0x7e 0000 add byte ptr [eax], al
0x7ff6f0080 0x80 0000 add byte ptr [eax], al
***** vad_0x2c930000 : 0x2c930000
Process: winlogon.exe Pid: 632 Address: 0x2c930000
Vad Tag: VadS Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x2c930000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x2c930000
0x2c930010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
0x2c930020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
0x2c930030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:
***** vad_0x2c930000 : 0x2c930000
0x2c930000 0x00 0000 add byte ptr [eax], al
0x2c930002 0x2 0000 add byte ptr [eax], al
0x2c930004 0x4 0000 add byte ptr [eax], al
0x2c930006 0x5 0000 add byte ptr [eax], al
0x2c930008 0x6 0000 add byte ptr [eax], al
0x2c93000a 0xa 0000 add byte ptr [eax], al
0x2c93000c 0xc 0000 add byte ptr [eax], al
0x2c93000e 0xe 0000 add byte ptr [eax], al
0x2c930010 0x10 0000 add byte ptr [eax], al
0x2c930012 0x12 0000 add byte ptr [eax], al
0x2c930014 0x14 0000 add byte ptr [eax], al
0x2c930016 0x15 0000 add byte ptr [eax], al
0x2c930018 0x18 0000 add byte ptr [eax], al
0x2c93001a 0x1a 0000 add byte ptr [eax], al
0x2c93001c 0x1c 0000 add byte ptr [eax], al
0x2c93001e 0x1e 0000 add byte ptr [eax], al
```

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x2c23001e 0x1e 0000 add byte ptr [eax], al
0x2c230020 0x20 0000 add byte ptr [eax], al
0x2c230022 0x22 0000 add byte ptr [eax], al
0x2c230024 0x24 0000 add byte ptr [eax], al
0x2c230026 0x26 0000 add byte ptr [eax], al
0x2c230028 0x28 0000 add byte ptr [eax], al
0x2c23002a 0x2a 0000 add byte ptr [eax], al
0x2c23002c 0x2c 0000 add byte ptr [eax], al
0x2c23002e 0x2e 0000 add byte ptr [eax], al
0x2c230030 0x30 0000 add byte ptr [eax], al
0x2c230032 0x32 0000 add byte ptr [eax], al
0x2c230034 0x34 0000 add byte ptr [eax], al
0x2c230036 0x36 0000 add byte ptr [eax], al
0x2c230038 0x38 0000 add byte ptr [eax], al
0x2c23003a 0x3a 0000 add byte ptr [eax], al
0x2c23003c 0x3c 0000 add byte ptr [eax], al
0x2c23003e 0x3e 0000 add byte ptr [eax], al
0x2c230040 0x40 0000 add byte ptr [eax], al
0x2c230042 0x42 0000 add byte ptr [eax], al
0x2c230044 0x44 0000 add byte ptr [eax], al
0x2c230046 0x46 0000 add byte ptr [eax], al
0x2c230048 0x48 0000 add byte ptr [eax], al
0x2c23004a 0x4a 0000 add byte ptr [eax], al
0x2c23004c 0x4c 0000 add byte ptr [eax], al
0x2c23004e 0x4e 0000 add byte ptr [eax], al
0x2c230050 0x50 0000 add byte ptr [eax], al
0x2c230052 0x52 0000 add byte ptr [eax], al
0x2c230054 0x54 0000 add byte ptr [eax], al
0x2c230056 0x56 0000 add byte ptr [eax], al
0x2c230058 0x58 0000 add byte ptr [eax], al
0x2c23005a 0x5a 0000 add byte ptr [eax], al
0x2c23005c 0x5c 0000 add byte ptr [eax], al
0x2c23005e 0x5e 0000 add byte ptr [eax], al
0x2c230060 0x60 0000 add byte ptr [eax], al
0x2c230062 0x62 0000 add byte ptr [eax], al
0x2c230064 0x64 0000 add byte ptr [eax], al
0x2c230066 0x66 0000 add byte ptr [eax], al
0x2c230068 0x68 0000 add byte ptr [eax], al
0x2c23006a 0x6a 0000 add byte ptr [eax], al
0x2c23006c 0x6c 0000 add byte ptr [eax], al
0x2c23006e 0x6e 0000 add byte ptr [eax], al
0x2c230070 0x70 0000 add byte ptr [eax], al
0x2c230072 0x72 0000 add byte ptr [eax], al
0x2c230074 0x74 0000 add byte ptr [eax], al
0x2c230076 0x76 0000 add byte ptr [eax], al
0x2c230078 0x78 0000 add byte ptr [eax], al
0x2c23007a 0x7a 0000 add byte ptr [eax], al
0x2c23007c 0x7c 0000 add byte ptr [eax], al
0x2c23007e 0x7e 0000 add byte ptr [eax], al
0x2c230080 0x80 0000 add byte ptr [eax], al
*****
Process: winlogon.exe Pid: 632 Address: 0x37ec0000
Vad Tag: Vad5 Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
Process: winlogon.exe Pid: 632 Address: 0x37ec0000
Vad Tag: Vad5 Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x37ec0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x37ec0000
0x37ec0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x37ec0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x37ec0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .

..... vol 0x37ec0000
0x37ec0000 0x00 0000 add byte ptr [eax], al
0x37ec0002 0x02 0000 add byte ptr [eax], al
0x37ec0004 0x04 0000 add byte ptr [eax], al
0x37ec0006 0x06 0000 add byte ptr [eax], al
0x37ec0008 0x08 0000 add byte ptr [eax], al
0x37ec000a 0x0a 0000 add byte ptr [eax], al
0x37ec000c 0x0c 0000 add byte ptr [eax], al
0x37ec000e 0x0e 0000 add byte ptr [eax], al
0x37ec0010 0x10 0000 add byte ptr [eax], al
0x37ec0012 0x12 0000 add byte ptr [eax], al
0x37ec0014 0x14 0000 add byte ptr [eax], al
0x37ec0016 0x16 0000 add byte ptr [eax], al
0x37ec0018 0x18 0000 add byte ptr [eax], al
0x37ec001a 0x1a 0000 add byte ptr [eax], al
0x37ec001c 0x1c 0000 add byte ptr [eax], al
0x37ec001e 0x1e 0000 add byte ptr [eax], al
0x37ec0020 0x20 0000 add byte ptr [eax], al
0x37ec0022 0x22 0000 add byte ptr [eax], al
0x37ec0024 0x24 0000 add byte ptr [eax], al
0x37ec0026 0x26 0000 add byte ptr [eax], al
0x37ec0028 0x28 0000 add byte ptr [eax], al
0x37ec002a 0x2a 0000 add byte ptr [eax], al
0x37ec002c 0x2c 0000 add byte ptr [eax], al
0x37ec002e 0x2e 0000 add byte ptr [eax], al
0x37ec0030 0x30 0000 add byte ptr [eax], al
0x37ec0032 0x32 0000 add byte ptr [eax], al
0x37ec0034 0x34 0000 add byte ptr [eax], al
0x37ec0036 0x36 0000 add byte ptr [eax], al
0x37ec0038 0x38 0000 add byte ptr [eax], al
0x37ec003a 0x3a 0000 add byte ptr [eax], al
0x37ec003c 0x3c 0000 add byte ptr [eax], al
0x37ec003e 0x3e 0000 add byte ptr [eax], al
0x37ec0040 0x40 0000 add byte ptr [eax], al
0x37ec0042 0x42 0000 add byte ptr [eax], al
0x37ec0044 0x44 0000 add byte ptr [eax], al
0x37ec0046 0x46 0000 add byte ptr [eax], al
0x37ec0048 0x48 0000 add byte ptr [eax], al
0x37ec004a 0x4a 0000 add byte ptr [eax], al
0x37ec004c 0x4c 0000 add byte ptr [eax], al
0x37ec004e 0x4e 0000 add byte ptr [eax], al
0x37ec0050 0x50 0000 add byte ptr [eax], al
0x37ec0052 0x52 0000 add byte ptr [eax], al
0x37ec0054 0x54 0000 add byte ptr [eax], al
0x37ec0056 0x56 0000 add byte ptr [eax], al
0x37ec0058 0x58 0000 add byte ptr [eax], al
```

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal --filename tiggermm

0x3347082c 0x2c 0000 add byte ptr [eax], al
0x33470830 0x2c 0000 add byte ptr [eax], al
0x33470838 0x2c 0000 add byte ptr [eax], al
0x33470832 0x32 0000 add byte ptr [eax], al
0x33470834 0x34 0000 add byte ptr [eax], al
0x33470836 0x36 0000 add byte ptr [eax], al
0x33470838 0x38 0000 add byte ptr [eax], al
0x3347083a 0x3a 0000 add byte ptr [eax], al
0x3347083c 0x3c 0000 add byte ptr [eax], al
0x3347083e 0x3e 0000 add byte ptr [eax], al
0x33470840 0x40 0000 add byte ptr [eax], al
0x33470842 0x42 0000 add byte ptr [eax], al
0x33470844 0x44 0000 add byte ptr [eax], al
0x33470846 0x46 0000 add byte ptr [eax], al
0x33470848 0x48 0000 add byte ptr [eax], al
0x3347084a 0x4a 0000 add byte ptr [eax], al
0x3347084c 0x4c 0000 add byte ptr [eax], al
0x3347084e 0x4e 0000 add byte ptr [eax], al
0x33470850 0x50 0000 add byte ptr [eax], al
0x33470852 0x52 0000 add byte ptr [eax], al
0x33470854 0x54 0000 add byte ptr [eax], al
0x33470856 0x56 0000 add byte ptr [eax], al
0x33470858 0x58 0000 add byte ptr [eax], al
0x3347085a 0x5a 0000 add byte ptr [eax], al
0x3347085c 0x5c 0000 add byte ptr [eax], al
0x3347085e 0x5e 0000 add byte ptr [eax], al
0x33470860 0x5f 0000 add byte ptr [eax], al
0x33470862 0x62 0000 add byte ptr [eax], al
0x33470864 0x64 0000 add byte ptr [eax], al
0x33470866 0x66 0000 add byte ptr [eax], al
0x33470868 0x68 0000 add byte ptr [eax], al
0x3347086a 0x6a 0000 add byte ptr [eax], al
0x3347086c 0x6c 0000 add byte ptr [eax], al
0x3347086e 0x70 0000 add byte ptr [eax], al
0x33470872 0x72 0000 add byte ptr [eax], al
0x33470874 0x74 0000 add byte ptr [eax], al
0x33470876 0x76 0000 add byte ptr [eax], al
0x33470878 0x78 0000 add byte ptr [eax], al
0x3347087a 0x7a 0000 add byte ptr [eax], al
0x3347087c 0x7c 0000 add byte ptr [eax], al
0x3347087e 0x7e 0000 add byte ptr [eax], al
0x33470880 0x80 0000 add byte ptr [eax], al
*****
***** exec P1M: G32 Address: 0x71ee0000
VadSize: Vad5 Protection: EXECUTE,READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x71ee0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x71ee0000
0x71ee0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
***** vad_0x71ee0000 *****: 0x71ee0000
0x71ee0000 0x00 0000 add byte ptr [eax], al
```

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x33470088 0x80 0000 add byte ptr [eax], al
.....
Process: winlogon.exe Pid: 632 Address: 0x71ee0000
Vad Tag: Vad5 Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x71ee0000 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x71ee0000
0x71ee0010 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0020 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x71ee0030 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
..... vad_0x71ee0000 ..... 0x71ee0000
0x71ee0000 0x0 0000 add byte ptr [eax], al
0x71ee0002 0x2 0000 add byte ptr [eax], al
0x71ee0004 0x4 0000 add byte ptr [eax], al
0x71ee0006 0x6 0000 add byte ptr [eax], al
0x71ee0008 0x8 0000 add byte ptr [eax], al
0x71ee000a 0xa 0000 add byte ptr [eax], al
0x71ee000c 0xc 0000 add byte ptr [eax], al
0x71ee000e 0xe 0000 add byte ptr [eax], al
0x71ee0010 0x10 0000 add byte ptr [eax], al
0x71ee0012 0x12 0000 add byte ptr [eax], al
0x71ee0014 0x14 0000 add byte ptr [eax], al
0x71ee0016 0x16 0000 add byte ptr [eax], al
0x71ee0018 0x18 0000 add byte ptr [eax], al
0x71ee001a 0x1a 0000 add byte ptr [eax], al
0x71ee001c 0x1c 0000 add byte ptr [eax], al
0x71ee001e 0x1e 0000 add byte ptr [eax], al
0x71ee0020 0x20 0000 add byte ptr [eax], al
0x71ee0022 0x22 0000 add byte ptr [eax], al
0x71ee0024 0x24 0000 add byte ptr [eax], al
0x71ee0026 0x26 0000 add byte ptr [eax], al
0x71ee0028 0x28 0000 add byte ptr [eax], al
0x71ee002a 0x2a 0000 add byte ptr [eax], al
0x71ee002c 0x2c 0000 add byte ptr [eax], al
0x71ee002e 0x2e 0000 add byte ptr [eax], al
0x71ee0030 0x30 0000 add byte ptr [eax], al
0x71ee0032 0x32 0000 add byte ptr [eax], al
0x71ee0034 0x34 0000 add byte ptr [eax], al
0x71ee0036 0x36 0000 add byte ptr [eax], al
0x71ee0038 0x38 0000 add byte ptr [eax], al
0x71ee003a 0x3a 0000 add byte ptr [eax], al
0x71ee003c 0x3c 0000 add byte ptr [eax], al
0x71ee003e 0x3e 0000 add byte ptr [eax], al
0x71ee0040 0x3f 0000 add byte ptr [eax], al
0x71ee0042 0x42 0000 add byte ptr [eax], al
0x71ee0044 0x44 0000 add byte ptr [eax], al
0x71ee0046 0x46 0000 add byte ptr [eax], al
0x71ee0048 0x48 0000 add byte ptr [eax], al
0x71ee004a 0x4a 0000 add byte ptr [eax], al
0x71ee004c 0x4c 0000 add byte ptr [eax], al
0x71ee004e 0x4e 0000 add byte ptr [eax], al
0x71ee0050 0x50 0000 add byte ptr [eax], al
0x71ee0052 0x52 0000 add byte ptr [eax], al
0x71ee0054 0x54 0000 add byte ptr [eax], al
.....
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0x71ee0054 0x54 0000 add byte ptr [eax], al
0x71ee0056 0x56 0000 add byte ptr [eax], al
0x71ee0058 0x58 0000 add byte ptr [eax], al
0x71ee005a 0x5a 0000 add byte ptr [eax], al
0x71ee005c 0x5c 0000 add byte ptr [eax], al
0x71ee005e 0x5e 0000 add byte ptr [eax], al
0x71ee0060 0x60 0000 add byte ptr [eax], al
0x71ee0062 0x62 0000 add byte ptr [eax], al
0x71ee0064 0x64 0000 add byte ptr [eax], al
0x71ee0066 0x66 0000 add byte ptr [eax], al
0x71ee0068 0x68 0000 add byte ptr [eax], al
0x71ee006a 0x6a 0000 add byte ptr [eax], al
0x71ee006c 0x6c 0000 add byte ptr [eax], al
0x71ee006e 0x6e 0000 add byte ptr [eax], al
0x71ee0070 0x70 0000 add byte ptr [eax], al
0x71ee0072 0x72 0000 add byte ptr [eax], al
0x71ee0074 0x74 0000 add byte ptr [eax], al
0x71ee0076 0x76 0000 add byte ptr [eax], al
0x71ee0078 0x78 0000 add byte ptr [eax], al
0x71ee007a 0x7a 0000 add byte ptr [eax], al
0x71ee007c 0x7c 0000 add byte ptr [eax], al
0x71ee007e 0x7e 0000 add byte ptr [eax], al
0x71ee0080 0x80 0000 add byte ptr [eax], al
.....
Process: winlogon.exe Pid: 632 Address: 0x78850000
Vad Tag: Vad5 Protection: EXECUTE_READWRITE
CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x78850000 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... vad_0x78850000
0x78850010 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x78850020 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x78850030 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
..... vad_0x78850000 ..... 0x78850000
0x78850000 0x0 0000 add byte ptr [eax], al
0x78850002 0x2 0000 add byte ptr [eax], al
0x78850004 0x4 0000 add byte ptr [eax], al
0x78850006 0x6 0000 add byte ptr [eax], al
0x78850008 0x8 0000 add byte ptr [eax], al
0x7885000a 0xa 0000 add byte ptr [eax], al
0x7885000c 0xc 0000 add byte ptr [eax], al
0x7885000e 0xe 0000 add byte ptr [eax], al
0x78850010 0x10 0000 add byte ptr [eax], al
0x78850012 0x12 0000 add byte ptr [eax], al
0x78850014 0x14 0000 add byte ptr [eax], al
0x78850016 0x16 0000 add byte ptr [eax], al
0x78850018 0x18 0000 add byte ptr [eax], al
0x7885001a 0x1a 0000 add byte ptr [eax], al
0x7885001c 0x1c 0000 add byte ptr [eax], al
0x7885001e 0x1e 0000 add byte ptr [eax], al
0x78850020 0x20 0000 add byte ptr [eax], al
0x78850022 0x22 0000 add byte ptr [eax], al
0x78850024 0x24 0000 add byte ptr [eax], al
0x78850026 0x26 0000 add byte ptr [eax], al
0x78850028 0x28 0000 add byte ptr [eax], al
```

11/30/2021

11/30/2021

[1] tigger.vmem 20:08:38 > threads							
_ETHREAD	pid	tid	start	start_symbol	Process	win32_start	win32_start_symb
0x810b13e8	4	8	0x80683528	nt!Phase1Initialization	System	0x0	0x0
0x810b0020	4	12	0x804edb6c	nt!InbvRotateGuiBootDisplay	System	0x0	0x0
0x810b0d20	4	16	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810b0aa8	4	20	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810b0830	4	24	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810b05b8	4	28	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810b0340	4	32	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810af020	4	36	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810afda8	4	40	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810afb30	4	44	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810af8b8	4	48	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810af640	4	52	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810af3c8	4	56	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810ae020	4	60	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810aeda8	4	64	0x80533cd0	nt!ExpWorkerThread	System	0x0	0x0
0x810aeb30	4	68	0x806091a8	nt!ExpWorkerThreadBalanceManager	System	0x0	0x0
0x810ad2c8	4	72	0x80508898	nt!MiDereferenceSegmentThread	System	0x0	0x0
0x810aa020	4	76	0x8064226e	nt!MiModifiedPageWriter	System	0x0	0x0
0x810aad8	4	80	0x8053b3e8	nt!KeBalanceSetManager	System	0x0	0x0
0x810aab30	4	84	0x8053b6de	nt!KeSwapProcessOnStack	System	0x0	0x0
0x810d5020	4	88	0x804ec6e8	nt!FsRtlWorkerThread	System	0x0	0x0
0x810d5da8	4	92	0x804ec6e8	nt!FsRtlWorkerThread	System	0x0	0x0
0x810d0870	4	96	0xfc37cb10	acpi+0x10b10	System	0x0	0x0
0x8102f020	4	100	0x8050ac2a	nt!MiMappedPageWriter	System	0x0	0x0
0x80fc6890	4	104	0xfc32091e	dmio+0xa91e	System	0x0	0x0
0x8102db98	4	108	0xfc1eab85	ndis+0xb85	System	0x0	0x0
0x80fa51a8	4	116	0xfc580f90	redbook+0x5f90	System	0x0	0x0
0xff3c8020	4	136	0xfbfa881a	rdpdr+0x2681a	System	0x0	0x0
0xff3c7748	4	140	0xfbfa881a	rdpdr+0x2681a	System	0x0	0x0
0x80f4b020	4	144	0xfbfa881a	rdpdr+0x2681a	System	0x0	0x0
0x80feeda8	4	148	0xfb9f91cf	rdpdr+0xfcfa	System	0x0	0x0
0xff35d620	4	172	0xfc5eb92d	raspptp+0x92d	System	0x0	0x0
0xff35d3a8	4	176	0xfc5ec103	raspptp+0x1103	System	0x0	0x0
0x80fa8b10	4	280	0xfc0cce96	usbport+0x5e96	System	0x0	0x0
0xff351b38	4	284	0xfc58eefe	vmci+0x3efe	System	0x0	0x0
0xff353da8	4	288	0xfc58ef6c	vmci+0x3f6c	System	0x0	0x0
0x80f4db48	4	292	0xfc0cce96	usbport+0x5e96	System	0x0	0x0
0xff3bfda8	4	336	0xfc1256d0	parport+0x46d0	System	0x0	0x0
0xff36dda8	4	352	0xfc175038	rasacd+0x1038	System	0x0	0x0
0x80fae390	4	356	0xf3b2da99	rdbss+0x18a99	System	0x0	0x0
0x80fae118	4	360	0xf3b2da99	rdbss+0x18a99	System	0x0	0x0
0xff39b738	4	364	0xf3b2da99	rdbss+0x18a99	System	0x0	0x0
0xff39b4c0	4	368	0xf3b158af	rdbss+0x8af	System	0x0	0x0
0x80fc0d020	4	540	0x805ee5b8	nt!SepRmCommandServerThread	System	0x0	0x0
0xff257230	4	1516	0xf35f97d8	mrx dav+0x217d8	System	0x0	0x0
0xff257658	4	1520	0xf35f97d8	mrx dav+0x217d8	System	0x0	0x0
0xff3682d0	4	1524	0xf35f97d8	mrx dav+0x217d8	System	0x0	0x0
0xff251658	4	1528	0xf35db82c	mrx dav+0x382c	System	0x0	0x0
0xff24a560	4	1536	0xf35d8d18	mrx dav+0xd18	System	0x0	0x0

11/30/2021

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem							
0xff257658	4	1520	0xf35f97d8	mrx dav+0x217d8	System	0x0	0x0
0xff3682d0	4	1524	0xf35f97d8	mrx dav+0x217d8	System	0x0	0x0
0xff251658	4	1528	0xf35db82c	mrx dav+0x382c	System	0x0	0x0
0xff24a560	4	1536	0xf35d8d18	mrx dav+0xd18	System	0x0	0x0
0xff242c28	4	1552	0xfc9f7cd4	vmmemctl+0xcda	System	0x0	0x0
0xff24fc10	4	1612	0xf356eb32	srv+0x11b32	System	0x0	0x0
0xff24a998	4	1636	0xf356eb32	srv+0x11b32	System	0x0	0x0
0xff12e5d0	4	276	0xf32ce7b6	http+0x327b6	System	0x0	0x0
0xff12e310	4	296	0xf32ce7b6	http+0x327b6	System	0x0	0x0
0xff12d020	4	300	0xf32ce7b6	http+0x327b6	System	0x0	0x0
0xff12dda8	4	304	0xf32ce7b6	http+0x327b6	System	0x0	0x0
0xff12db30	4	312	0xf32cbdda	http+0x2fd4	System	0x0	0x0
0xff1f92b0	4	1648	0xf2edd150	0xf2edd150	System	0x0	0x0
0xff2674a0	4	1720	0xf2edc54e	0xf2edc54e	System	0x0	0x0
0x80f334a8	4	1992	0xf2edba46	0xf2edba46	System	0x0	0x0
0x80f1b020	4	1916	0xfc7ae0ae	flypydisk+0x30ae	System	0x0	0x0
0xffffbd370	4	1696	0xfc1eab85	ndis+0x6b85	System	0x0	0x0
0xff134da8	216	236	0x7c810867	kernel32+0x10867	alg.exe	0x1005bc6	alg+0x5bc6
0xffff131580	216	256	0x7c810856	kernel32+0x10856	alg.exe	0x77deb479	advapi32+0x1b479
0xffff130da8	216	260	0x7c810856	kernel32+0x10856	alg.exe	0x0	0x0
0xffff128718	216	436	0x7c810856	kernel32+0x10856	alg.exe	0x0	0x0
0xffff1283e8	216	440	0x7c810856	kernel32+0x10856	alg.exe	0x7c92798d	ntdll!RtlQueueWorkItem+0x2b5
0xffff127020	216	444	0x7c810856	kernel32+0x10856	alg.exe	0x7c910760	ntdll!RtlAllocateHeap+0x18c
0xffff37d490	216	1948	0x7c810856	kernel32+0x10856	alg.exe	0x9068	0x9068
0xffff3623c8	432	448	0x7c810867	kernel32+0x10867	VMwareTray.exe	0x40246a	vmwaretray+0x246a
0xffff3762b0	452	456	0x7c810867	kernel32+0x10867	VMwareUser.exe	0x49fcbb	vmwareuser+0x9fcbb
0xffff36cda8	452	1868	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x407130	vmwareuser+0x7130
0xffff384530	452	568	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x412ea0	vmwareuser+0x12ea0
0xffff3a5718	452	1264	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x781329e1	msvcr80+0x29e1
0xffff1e3648	452	1356	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x781329e1	msvcr80+0x29e1
0x81025318	452	1368	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x0	0x0
0x80f95da8	452	1360	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x774f319a	ole32+0x1319a
0xffff392da8	452	1372	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x905b	0x905b
0xffff214248	452	1884	0x7c810856	kernel32+0x10856	VMwareUser.exe	0x9067	0x9067
0x80f18408	468	988	0x7c810867	kernel32+0x10867	wuaclt.exe	0x40bad5	wuaclt+0xbad5
0x80f0d9da8	468	992	0x7c810856	kernel32+0x10856	wuaclt.exe	0x9057	0x9057
0x80f94a68	468	1784	0x7c810856	kernel32+0x10856	wuaclt.exe	0x8771	0x8771
0x80f0da518	468	1000	0x7c810856	kernel32+0x10856	wuaclt.exe	0x4077e2	wuaclt+0x77e2
0xffff29b020	544	548	0x4858a4c8	smss+0xa4c8	smss.exe	0x0	vad_0x0
0xffff27c980	544	556	0x485893b2	smss+0x93b2	smss.exe	0x0	vad_0x0
0xffff1fbda8	544	560	0x485893b2	smss+0x93b2	smss.exe	0x66ae	vad_0x0+0x66ae
0xffff1e0650	608	616	0x75b6b329	winsrv+0xb329	csrss.exe	0x0	vad_0x0
0xffff1f1da8	608	620	0x75b654a4	winsrv+0x54a4	csrss.exe	0x0	vad_0x0
0xffff1ec558	608	624	0x75b44616	csrssrv+0x4616	csrss.exe	0x0	vad_0x0
0xffff1f1980	608	628	0x75b43b3a	csrssrv+0x3b3a	csrss.exe	0x0	vad_0x0
0xffff20f7e8	608	640	0x75b44616	csrssrv+0x4616	csrss.exe	0x0	vad_0x0
0xffff1d6228	608	644	0x75b6b0f7	winsrv+0xb0f7	csrss.exe	0x0	vad_0x0
0x80f02410	608	648	0x75b6b0f7	winsrv+0xb0f7	csrss.exe	0x0	vad_0x0
0xffff24f130	608	696	0x75b6b0f7	winsrv+0xb0f7	csrss.exe	0x0	vad_0x0
0xffff1587e0	608	1824	0x75b62272	winsrv+0x2272	csrss.exe	0x0	vad_0x0
0xffff395298	608	812	0x75b6b59c	winsrv+0xb59c	csrss.exe	0x0	vad_0x0
0xffff20fc10	632	636	0x103d353	winlogon+0x3d353	winlogon.exe	0x0	0x0
0xffff230130	632	656	0x7c810856	kernel32+0x10856	winlogon.exe	0x0	0x0
0xffff224020	632	660	0x7c810856	kernel32+0x10856	winlogon.exe	0x77e76bf0	rpcrt4+0x6bf0
0xffff23b130	632	664	0x7c810856	kernel32+0x10856	winlogon.exe	0x7c92798d	ntdll!RtlQueueWorkItem+0x2b5

11/30/2021

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem						
0xffff217da8	632	920	0x7c810856	kernel32+0x10856	winlogon.exe	0x6db1
0xffff213da8	632	924	0x7c810856	kernel32+0x10856	winlogon.exe	0x76c6c86b
0x80f529f0	632	928	0x7c810856	kernel32+0x10856	winlogon.exe	sfc_os+0xc86b
0xffff299620	632	932	0x7c810856	kernel32+0x10856	winlogon.exe	sfc_os+0xc5ae
0xffff2a5b08	632	1220	0x7c810856	kernel32+0x10856	winlogon.exe	sfc_os+0xc5ae
0xffff200760	632	1252	0x7c810856	kernel32+0x10856	winlogon.exe	0x1039156
0xffff1e33c8	632	1684	0x7c810856	kernel32+0x10856	winlogon.exe	winlogon+0x39156
0xffff1dbd8a	632	1688	0x7c810856	kernel32+0x10856	winlogon.exe	0x76d3cf1
0xffff22e330	632	480	0x7c810856	kernel32+0x10856	winlogon.exe	userenv+0x13cf1
0xffff3b7880	632	112	0x7c810856	kernel32+0x10856	winlogon.exe	userenv+0x13cf1
0xffff1359c0	632	652	0x7c810856	kernel32+0x10856	winlogon.exe	wlnotify+0x14de
0xffff3b5610	632	1008	0x7c810856	kernel32+0x10856	winlogon.exe	0x72d230e8
0xffff37b188	632	1012	0x7c810856	kernel32+0x10856	winlogon.exe	wdmaud+0x30e8
0xffff3608e0	632	1856	0x7c810856	kernel32+0x10856	winlogon.exe	0x76b44dd6
0xffff37ada8	632	1480	0x7c810856	kernel32+0x10856	winlogon.exe	winmm+0x4dd6
0xffff134020	632	1660	0x7c810856	kernel32+0x10856	winlogon.exe	rpcrt4+0x13cf1
0xffff22a468	632	1216	0x7c810856	kernel32+0x10856	winlogon.exe	0x77e76bf0
0xffff136688	632	1072	0x7c810856	kernel32+0x10856	winlogon.exe	0x77e76bf0
0xffff277020	676	700	0x7c810856	kernel32+0x10856	services.exe	0x7c92798d
0x80f03558	676	752	0x7c810856	kernel32+0x10856	services.exe	ntdll!RtlQueueWorkItem+0x2b5
0x80f5f020	676	756	0x7c810856	kernel32+0x10856	services.exe	0x7c910aca
0xffff25c020	676	816	0x7c810856	kernel32+0x10856	services.exe	ntdll!RtlReleaseActivationContext+0x73
0xffff243568	676	820	0x7c810856	kernel32+0x10856	services.exe	0x7c929fae
0xffff244660	676	824	0x7c810856	kernel32+0x10856	services.exe	ntdll!RtlAdjustPrivilege+0x122
0xffff244a88	676	832	0x7c810856	kernel32+0x10856	services.exe	0x7c910760
0xffff244240	676	840	0x7c810856	kernel32+0x10856	services.exe	ntdll!RtlAllocateHeap+0x18c
0xffff219da8	676	872	0x7c810856	kernel32+0x10856	services.exe	0x77e76bf0
0xffff214660	676	916	0x7c810856	kernel32+0x10856	services.exe	0x77e76bf0
0xffff207b88	676	1112	0x7c810856	kernel32+0x10856	services.exe	0x758c349f
0xffff2a4620	676	1116	0x7c810856	kernel32+0x10856	services.exe	umpnpmgr+0x349f
0xffff1ef700	676	1280	0x7c810856	kernel32+0x10856	services.exe	0x758c5df7
0xffff1dfda8	676	1576	0x7c810856	kernel32+0x10856	services.exe	umpnpmgr+0x5df7
0xffff13a020	676	2020	0x7c810856	kernel32+0x10856	services.exe	0x0
0xffff25a558	676	224	0x7c810856	kernel32+0x10856	services.exe	0x0
0xffff240478	676	228	0x7c810856	kernel32+0x10856	services.exe	0x5f771c49
0x80f2ed8a	676	980	0x7c810856	kernel32+0x10856	services.exe	ncobjapi+0x3e24
0xffff281020	688	704	0x7c810856	kernel32+0x10856	services.exe	0x5f773e24
0xffff250020	688	708	0x7c810856	kernel32+0x10856	services.exe	0x5f771d97
0xffff27f1d0	688	712	0x7c810856	kernel32+0x10856	services.exe	0x77e76bf0
0xffff369230	688	716	0x7c810856	kernel32+0x10856	lsass.exe	rpcrt4+0x6bf0
0x80fba218	688	720	0x7c810856	kernel32+0x10856	lsass.exe	lsasrv+0x8e06
0x80feef248	688	736	0x7c810856	kernel32+0x10856	lsass.exe	0x7c92798d
0xffff2a6930	688	760	0x7c810856	kernel32+0x10856	lsass.exe	ntdll!RtlAllocateHeap+0x18c
0xffff1fac90	688	764	0x7c810856	kernel32+0x10856	lsass.exe	0x7c910760
0xffff1fa868	688	768	0x7c810856	kernel32+0x10856	lsass.exe	ntdll!RtlReleaseActivationContext+0x73
0xffff1f96d0	688	780	0x7c810856	kernel32+0x10856	lsass.exe	0x75738e06
0x80faada8	688	784	0x7c810856	kernel32+0x10856	lsass.exe	lsasrv+0x13381
0xffff243990	688	804	0x7c810856	kernel32+0x10856	lsass.exe	0x7c910aca
0xffff252c20	688	836	0x7c810856	kernel32+0x10856	lsass.exe	0x77e76bf0
0xffff1efda8	688	1296	0x7c810856	kernel32+0x10856	lsass.exe	rpcrt4+0x6bf0
0xffff1df3c8	688	1596	0x7c810856	kernel32+0x10856	lsass.exe	advapi32+0xb479
0xffff2594c0	688	1740	0x7c810856	kernel32+0x10856	lsass.exe	0x662e085b
0xffff2587f0	688	1744	0x7c810856	kernel32+0x10856	lsass.exe	hnetcfg+0x3085b
0xffff26a568	688	1748	0x7c810856	kernel32+0x10856	lsass.exe	msvcrt+0x2a341
0xffff225660	688	1752	0x7c810856	kernel32+0x10856	lsass.exe	msvcrt+0x2a341

11/30/2021

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem						
0xff225660	688	1752	0x7c810856	kernel32+0x10856	lsass.exe	0x77c3a341 msvcr7+0x2a341
0xff142bf0	688	1232	0x7c810856	kernel32+0x10856	lsass.exe	0x769c8831 userenv+0x8831
0xff36c1f0	688	1604	0x7c810856	kernel32+0x10856	lsass.exe	0x75738e06 lsasrv+0x8e06
0xff20c428	688	392	0x7c810856	kernel32+0x10856	lsass.exe	0x77e76bf0 rpcrt4+0x6bf0
0x80f32da8	828	1336	0x7c810867	kernel32+0x10867	wmiprvse.exe	0x1024636 wmicore+0x24636
0x80f5c3b8	828	1592	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x5f771c49 ncobjapi+0x1c49
0xff298bc0	828	1708	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x906b 0x906b
0xff2683d0	828	496	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x774f319a ole32+0x1319a
0xff3751d0	828	1016	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x100ce42 wmicore+0xce42
0x80f16da8	828	1464	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x9075 0x9075
0xff3a7368	828	2044	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x0 0x0
0xff237470	828	1176	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x716df2be cimwin32+0xcf2be
0x80f17478	828	1608	0x7c810856	kernel32+0x10856	wmiprvse.exe	0x77e3e70d advapi32+0x6e70d
0xff213578	844	848	0x7c810867	kernel32+0x10867	vmacthlp.exe	0x42aad1 vmacthlp+0x2aad1
0xff1e9da8	856	860	0x7c810867	kernel32+0x10867	svchost.exe	0x1002509 svchost+0x2509
0xff231020	856	896	0x7c810856	kernel32+0x10856	svchost.exe	0x7c92798d ntdll!RtlQueueWorkItem+0x2b5
0xff287c10	856	904	0x7c810856	kernel32+0x10856	svchost.exe	0x7c929f9ae ntdll!RtlAdjustPrivilege+0x122
0xff1fb9b98	856	908	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff1f2da8	856	1036	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff3792d0	856	528	0x7c810856	kernel32+0x10856	svchost.exe	0x7610fe60 termsrv+0x1fe60
0xff3b8978	856	1928	0x7c810856	kernel32+0x10856	svchost.exe	0x7d12 0x7d12
0xff3bada8	856	572	0x7c810856	kernel32+0x10856	svchost.exe	0x77d1 0x77d1
0xff3ba358	856	580	0x7c810856	kernel32+0x10856	svchost.exe	0x760fe99c termsrv+0xe99c
0xff3b8450	856	576	0x7c810856	kernel32+0x10856	svchost.exe	0x760fe894 termsrv+0xe894
0xff3b93d0	856	584	0x7c810856	kernel32+0x10856	svchost.exe	0x760fa72e termsrv+0xa72e
0xff364838	856	604	0x7c810856	kernel32+0x10856	svchost.exe	0x769c8831 userenv+0x8831
0xff36da48	856	588	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff3bb2f8	856	596	0x7c810856	kernel32+0x10856	svchost.exe	0x77e76bf0 rpcrt4+0x6bf0
0xff37fd48	856	592	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff235da8	856	808	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff3ae9a0	856	1488	0x7c810856	kernel32+0x10856	svchost.exe	0x77e76bf0 rpcrt4+0x6bf0
0x80feab0	856	728	0x7c810856	kernel32+0x10856	svchost.exe	0x7c910760 ntdll!RtlAllocateHeap+0x18c
0xff3ba880	888	912	0x7c810867	kernel32+0x10867	wscntfy.exe	0x10027f2 wscntfy+0x27f2
0xff2167f8	936	940	0x7c810867	kernel32+0x10867	svchost.exe	0x1002509 svchost+0x2509
0x80fb6020	936	944	0x7c810856	kernel32+0x10856	svchost.exe	0x77deb479 advapi32+0x1b479
0xff200228	936	948	0x7c810856	kernel32+0x10856	svchost.exe	0x7c92798d ntdll!RtlQueueWorkItem+0x2b5
0x80fc2b0	936	952	0x7c810856	kernel32+0x10856	svchost.exe	0x7c910760 ntdll!RtlAllocateHeap+0x18c
0xff2843c0	936	956	0x7c810856	kernel32+0x10856	svchost.exe	0x7c929f9ae ntdll!RtlAdjustPrivilege+0x122
0xff22f3c0	936	960	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff1f1558	936	968	0x7c810856	kernel32+0x10856	svchost.exe	0x0 0x0
0xff14b210	936	1860	0x7c810856	kernel32+0x10856	svchost.exe	0x9070 0x9070
0xff13d330	936	512	0x7c810856	kernel32+0x10856	svchost.exe	0x77e76bf0 rpcrt4+0x6bf0
0x80fbf698	1028	1032	0x7c810867	kernel32+0x10867	svchost.exe	0x1002509 svchost+0x2509
0xff291da8	1028	1040	0x7c810856	kernel32+0x10856	svchost.exe	0x8b96 0x8b96
0xff291b30	1028	1044	0x7c810856	kernel32+0x10856	svchost.exe	0x7c92798d ntdll!RtlQueueWorkItem+0x2b5
0x80f524e8	1028	1048	0x7c810856	kernel32+0x10856	svchost.exe	0x7c910760 ntdll!RtlAllocateHeap+0x18c
0xff1f7320	1028	1076	0x7c810856	kernel32+0x10856	svchost.exe	0x77deb479 advapi32+0x1b479
0x80f0d4b8	1028	1104	0x7c810856	kernel32+0x10856	svchost.exe	0x9093 0x9093
0xff1f2020	1028	1128	0x7c810856	kernel32+0x10856	svchost.exe	0x76d8ae19 dhcpsvc+0xae19
0xff203818	1028	1140	0x7c810856	kernel32+0x10856	svchost.exe	0x9084 0x9084
0xff1e8448	1028	1364	0x7c810856	kernel32+0x10856	svchost.exe	0x7c910760 ntdll!RtlAllocateHeap+0x18c
0xff205da8	1028	1384	0x7c810856	kernel32+0x10856	svchost.exe	0x77df9981 advapi32+0x29981
0xff1ff7f0	1028	1388	0x7c810856	kernel32+0x10856	svchost.exe	0x77e76bf0 rpcrt4+0x6bf0
0xff1ff3d0	1028	1392	0x7c810856	kernel32+0x10856	svchost.exe	0x77666bb2 wzcsvc+0x46bb2
0xff29b8c8	1028	1396	0x7c810856	kernel32+0x10856	svchost.exe	0x77deb479 advapi32+0x1b479

11/30/2021

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem			
0xff205da8	1028	1384	0x7c810856 kernel32+0x10856
0xff1ff7f0	1028	1388	0x7c810856 kernel32+0x10856
0xff1ff3d0	1028	1392	0x7c810856 kernel32+0x10856
0xff29b8c8	1028	1396	0x7c810856 kernel32+0x10856
0xff227c20	1028	1404	0x7c810856 kernel32+0x10856
0xff205570	1028	1408	0x7c810856 kernel32+0x10856
0xff2277f8	1028	1412	0x7c810856 kernel32+0x10856
0xff2283d8	1028	1416	0x7c810856 kernel32+0x10856
0xff202830	1028	1420	0x7c810856 kernel32+0x10856
0xff22c818	1028	1424	0x7c810856 kernel32+0x10856
0xff22c5a0	1028	1428	0x7c810856 kernel32+0x10856
0xff1e7428	1028	1440	0x7c810856 kernel32+0x10856
0xff1fe4a0	1028	1468	0x7c810856 kernel32+0x10856
0xff1fe4a0	1028	1472	0x7c810856 kernel32+0x10856
0x80fce020	1028	1476	0x7c810856 kernel32+0x10856
0xff24c468	1028	1512	0x7c810856 kernel32+0x10856
0xff242800	1028	1564	0x7c810856 kernel32+0x10856
0xff24b230	1028	1568	0x7c810856 kernel32+0x10856
0xff1dfb30	1028	1580	0x7c810856 kernel32+0x10856
0xff2f88b0	1028	1584	0x7c810856 kernel32+0x10856
0xff257a80	1028	1640	0x7c810856 kernel32+0x10856
0xff160020	1028	1728	0x7c810856 kernel32+0x10856
0xff1fd6f0	1028	1756	0x7c810856 kernel32+0x10856
0xff1fc658	1028	1764	0x7c810856 kernel32+0x10856
0xff1fca88	1028	1772	0x7c810856 kernel32+0x10856
0xff2083d0	1028	1776	0x7c810856 kernel32+0x10856
0xff24f7f8	1028	1780	0x7c810856 kernel32+0x10856
0xff15a668	1028	1796	0x7c810856 kernel32+0x10856
0xff154888	1028	1800	0x7c810856 kernel32+0x10856
0xff159020	1028	1808	0x7c810856 kernel32+0x10856
0xff1490c0	1028	1888	0x7c810856 kernel32+0x10856
0xff148020	1028	1896	0x7c810856 kernel32+0x10856
0xff147da8	1028	1900	0x7c810856 kernel32+0x10856
0xff144360	1028	1924	0x7c810856 kernel32+0x10856
0xff143da8	1028	1932	0x7c810856 kernel32+0x10856
0xff154b20	1028	2016	0x7c810856 kernel32+0x10856
0xff13ada8	1028	2024	0x7c810856 kernel32+0x10856
0xff13ab30	1028	2028	0x7c810856 kernel32+0x10856
0xff139b48	1028	2036	0x7c810856 kernel32+0x10856
0xff2406f0	1028	2040	0x7c810856 kernel32+0x10856
0xff134600	1028	244	0x7c810856 kernel32+0x10856
0xff1301e8	1028	272	0x7c810856 kernel32+0x10856
0xff12a408	1028	416	0x7c810856 kernel32+0x10856
0xff125020	1028	472	0x7c810856 kernel32+0x10856
0xff122810	1028	484	0x7c810856 kernel32+0x10856
0xff121020	1028	488	0x7c810856 kernel32+0x10856
0xff122020	1028	492	0x7c810856 kernel32+0x10856
0xff122360	1028	504	0x7c810856 kernel32+0x10856
0xff25cda8	1028	500	0x7c810856 kernel32+0x10856
0xff376980	1028	520	0x7c810856 kernel32+0x10856
0xff3b7da8	1028	692	0x7c810856 kernel32+0x10856
0xff3ae480	1028	1304	0x7c810856 kernel32+0x10856
0xff3ae710	1028	1308	0x7c810856 kernel32+0x10856
0xff360d58	1028	1312	0x7c810856 kernel32+0x10856
0xff3655b0	1028	1316	0x7c810856 kernel32+0x10856
			svhost.exe 0x77df9981 advapi32+0x29981
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x77666bb2 wcsvc+0x46bb2
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x774f319a ole32+0x1319a
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x0 0x0
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x7730b153 schedsvc+0xb153
			svhost.exe 0x7730a89a schedsvc+0xa89a
			svhost.exe 0x7731709d schedsvc+0x1709d
			svhost.exe 0x0 0x0
			svhost.exe 0x7730a597 schedsvc+0xa597
			svhost.exe 0x8b63 0x8b63
			svhost.exe 0x7c910aca ntdll!RtlReleaseActivationContext+0x73
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x492 0x492
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0
			svhost.exe 0x84b8 0x84b8
			svhost.exe 0x0 0x0
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x769c8831 userenv+0x8831
			svhost.exe 0x767c28de w32time+0x28de
			svhost.exe 0x662e085b hnetcfg+0x3085b
			svhost.exe 0x77738ff5 es+0x28ff5
			svhost.exe 0x75219a1e repdrvfs+0x19a1e
			svhost.exe 0x5f773fbf ncobjapi+0x3fbf
			svhost.exe 0x5f773fbf ncobjapi+0x3fbf
			svhost.exe 0x8e3a 0x8e3a
			svhost.exe 0x776c39c0 authz+0x39c0
			svhost.exe 0x5f743c44 ncprov+0x3c44
			svhost.exe 0x5f771c49 ncobjapi+0x1c49
			svhost.exe 0x5f771c49 ncobjapi+0x1c49
			svhost.exe 0x4c0a82cf wscsvc+0x82cf
			svhost.exe 0x4c0a4c28 wscsvc+0x4c28
			svhost.exe 0x0 0x0
			svhost.exe 0x774f319a ole32+0x1319a
			svhost.exe 0x0 0x0
			svhost.exe 0x0 0x0
			svhost.exe 0x0 0x0
			svhost.exe 0x7c929fae ntdll!RtlAdjustPrivilege+0x122
			svhost.exe 0x7c910760 ntdll!RtlAllocateHeap+0x18c
			svhost.exe 0x0 0x0
			svhost.exe 0x74f02555 ssdpapi+0x2555
			svhost.exe 0x77deb479 advapi32+0x1b479
			svhost.exe 0x776f6207 shsvcs+0x16207
			svhost.exe 0x73405033 tapisrv+0x25033
			svhost.exe 0x0 0x0
			svhost.exe 0x0 0x0
			svhost.exe 0x77e76bf0 rpcrt4+0x6bf0

11/30/2021

C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem						
0xff3655b0	1028	1316	0x7c810856	kernel132+0x10856	svchost.exe	0x77e76bf0
0xff374ab8	1028	1320	0x7c810856	kernel132+0x10856	svchost.exe	0x77e76bf0
0xff37dd80	1028	1324	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff380bc0	1028	1248	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff3b2710	1028	1504	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff3b1d80	1028	1292	0x7c810856	kernel132+0x10856	svchost.exe	0x905a
0xff38da8	1028	208	0x7c810856	kernel132+0x10856	svchost.exe	0x77deb479
0xff38e1d8	1028	220	0x7c810856	kernel132+0x10856	svchost.exe	0x75887b5e
0xff39fda8	1028	1964	0x7c810856	kernel132+0x10856	svchost.exe	0x77e76bf0
0xff3f3c48	1028	1940	0x7c810856	kernel132+0x10856	svchost.exe	0x57cde2a8
0xff3fb7358	1028	232	0x7c810856	kernel132+0x10856	svchost.exe	0x72001a18
0xff381da8	1028	864	0x7c810856	kernel132+0x10856	svchost.exe	0x57d46dd4
0xff39ada8	1028	340	0x7c810856	kernel132+0x10856	svchost.exe	0x57d29bc0
0xff3fb1330	1028	344	0x7c810856	kernel132+0x10856	svchost.exe	0x57d91f91
0xff3fb0da8	1028	348	0x7c810856	kernel132+0x10856	svchost.exe	0x57d63f47
0xff390da8	1028	376	0x7c810856	kernel132+0x10856	svchost.exe	0x76be104
0xff3bc3d0	1028	464	0x7c810856	kernel132+0x10856	svchost.exe	0x7225bb4d
0x80fb610	1028	268	0x7c810856	kernel132+0x10856	svchost.exe	0x77e76bf0
0xff13c360	1028	792	0x7c810856	kernel132+0x10856	svchost.exe	0x7c910760
0x80f2e2a0	1028	1912	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff148970	1028	1692	0x7c810856	kernel132+0x10856	svchost.exe	0x7773802f
0xff154da8	1028	536	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff282b70	1028	1712	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0x80f65020	1028	384	0x7c810856	kernel132+0x10856	svchost.exe	0x762cf010
0xff1eb4c0	1028	1268	0x7c810856	kernel132+0x10856	svchost.exe	0x762cf0a3
0x80ff3020	1028	1452	0x7c810856	kernel132+0x10856	svchost.exe	0x7589b647
0x80fdc378	1028	1820	0x7c810856	kernel132+0x10856	svchost.exe	0x7509b647
0xff1f6da8	1028	200	0x7c810856	kernel132+0x10856	svchost.exe	0x774f319a
0xff388da8	1028	1508	0x7c810856	kernel132+0x10856	svchost.exe	0x74f0742e
0xff36f5f8	1028	124	0x7c810856	kernel132+0x10856	svchost.exe	0x74f0742e
0xff397248	1084	1096	0x7c810867	kernel132+0x10867	TPAutoConnect.e	0x42462c
0xff21a868	1088	1092	0x7c810867	kernel132+0x10867	svchost.exe	0x1002509
0xff1e5c8	1088	1184	0x7c810856	kernel132+0x10856	svchost.exe	0x767756a3
0xff1e55a8	1088	1188	0x7c810856	kernel132+0x10856	svchost.exe	0x7677464b
0xff212c18	1088	1192	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff14f720	1088	1828	0x7c810856	kernel132+0x10856	svchost.exe	0x8bab
0xff14ebf8	1088	1936	0x7c810856	kernel132+0x10856	svchost.exe	0x662e085b
0xff3af4b8	1088	1904	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff38a890	1088	1204	0x7c810856	kernel132+0x10856	svchost.exe	0x77df9981
0xff1eab18	1148	1152	0x7c810867	kernel132+0x10867	svchost.exe	0x1002509
0xff1fa020	1148	1224	0x7c810856	kernel132+0x10856	svchost.exe	0x77deb479
0xff1ef2d0	1148	1276	0x7c810856	kernel132+0x10856	svchost.exe	0x74c41b04
0xff251a80	1148	1540	0x7c810856	kernel132+0x10856	svchost.exe	0x5a6e57c5
0xff24b658	1148	1544	0x7c810856	kernel132+0x10856	svchost.exe	0x5a6e57c5
0xff253658	1148	1548	0x7c810856	kernel132+0x10856	svchost.exe	0x77e76bf0
0xff12d428	1148	316	0x7c810856	kernel132+0x10856	svchost.exe	0x77deb479
0xff12f020	1148	320	0x7c810856	kernel132+0x10856	svchost.exe	0x7c92798d
0xff12fd40	1148	328	0x7c810856	kernel132+0x10856	svchost.exe	0x7c910760
0xff12f998	1148	332	0x7c810856	kernel132+0x10856	svchost.exe	0x7c929fae
0xff12b318	1148	396	0x7c810856	kernel132+0x10856	svchost.exe	0x662e085b
0xff12a8b8	1148	408	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0xff12ace0	1148	412	0x7c810856	kernel132+0x10856	svchost.exe	0x765e721f
0xff1212b0	1148	564	0x7c810856	kernel132+0x10856	svchost.exe	0x668e
0xff37d908	1148	1500	0x7c810856	kernel132+0x10856	svchost.exe	0x0
0x80fd8da8	1148	1056	0x7c810856	kernel132+0x10856	svchost.exe	0x7c910760

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal --filename tigger.vmem
0xff12ace0 1148 412 0x7c810856 kernel32+0x10856 svchost.exe 0x765e721f ssdpsrv+0x721f
0xff1212b0 1148 564 0x7c810856 kernel32+0x10856 svchost.exe 0x668e 0x668e
0xff37d908 1148 1500 0x7c810856 kernel32+0x10856 svchost.exe 0x0 0x0
0x80fd8da8 1148 1056 0x7c810856 kernel32+0x10856 svchost.exe 0x7c910760 nt!RtlAllocateHeap+0x18c
0xff1d7ae8 1432 1436 0x7c810867 kernel32+0x10867 spools.exe 0x100637a spools+0x637a
0xff20d4e0 1432 1444 0x7c810856 kernel32+0x10856 spools.exe 0x77deb479 advapi32+0x1b479
0xff201c30 1432 1448 0x7c810856 kernel32+0x10856 spools.exe 0x77e76bf0 rpcrt4+0x6bf0
0xff201450 1432 1460 0x7c810856 kernel32+0x10856 spools.exe 0x10051dc spools+0x51dc
0xff3891d0 1432 1100 0x7c810856 kernel32+0x10856 spools.exe 0x8e1b 0x8e1b
0xff3814b8 1432 1064 0x7c810856 kernel32+0x10856 spools.exe 0x100569c spools+0x569c
0xff37a930 1432 1120 0x7c810856 kernel32+0x10856 spools.exe 0x723f17d7 usbmon+0x17d7
0xff389980 1432 1196 0x7c810856 kernel32+0x10856 spools.exe 0x75bb2c4f localspl+0x2c4f
0xff397be8 1432 1200 0x7c810856 kernel32+0x10856 spools.exe 0x75bb885c localspl+0x885c
0xff3b21e8 1432 1068 0x7c810856 kernel32+0x10856 spools.exe 0x77e76bf0 rpcrt4+0x6bf0
0xff38a418 1432 1244 0x7c810856 kernel32+0x10856 spools.exe 0x0 0x0
0xff37c418 1432 1852 0x7c810856 kernel32+0x10856 spools.exe 0x77e76bf0 rpcrt4+0x6bf0
0xff360468 1432 1816 0x7c810856 kernel32+0x10856 spools.exe 0x77e76bf0 rpcrt4+0x6bf0
0xff381930 1432 1812 0x7c810856 kernel32+0x10856 spools.exe 0x0 0x0
0xff1b88b0 1668 1672 0x7c810867 kernel32+0x10867 vmtoolsd.exe 0x404597 vmtoolsd+0x4597
0xff1fc230 1668 1760 0x7c810856 kernel32+0x10856 vmtoolsd.exe 0x77deb479 advapi32+0x1b479
0xff14bbf8 1668 1844 0x7c810856 kernel32+0x10856 vmtoolsd.exe 0x8bb6f 0x8bb6f
0xff14ada8 1668 1872 0x7c810856 kernel32+0x10856 vmtoolsd.exe 0x9058 0x9058
0xff379bc0 1668 1380 0x7c810856 kernel32+0x10856 vmtoolsd.exe 0x77e3e70d advapi32+0x6e70d
0xff247da8 1724 1836 0x7c810867 kernel32+0x10867 explorer.exe 0x101e24e explorer+0x1e24e
0xff233788 1724 1840 0x7c810856 kernel32+0x10856 explorer.exe 0x8fd6 0x8fd6
0xff2716f0 1724 1848 0x7c810856 kernel32+0x10856 explorer.exe 0x774f319a ole32+0x1319a
0xff379748 1724 1864 0x7c810856 kernel32+0x10856 explorer.exe 0x77f7422b shlwapi+0x1422b
0xff1423f0 1724 164 0x7c810856 kernel32+0x10856 explorer.exe 0x7c92798d nt!RtlQueueWorkItem+0x2b5
0xff37b600 1724 184 0x7c810856 kernel32+0x10856 explorer.exe 0x7c929fae nt!RtlAdjustPrivilege+0x122
0xff372da8 1724 1496 0x7c810856 kernel32+0x10856 explorer.exe 0x77f7422b shlwapi+0x1422b
0xff144020 1724 204 0x7c810856 kernel32+0x10856 explorer.exe 0x7c910760 nt!RtlAllocateHeap+0x18c
0xff36b980 1724 388 0x7c810856 kernel32+0x10856 explorer.exe 0x0 0x0
0x80f97c10 1724 724 0x7c810856 kernel32+0x10856 explorer.exe 0x72d230e8 wdmaud+0x30e8
0x80f99780 1724 516 0x7c810856 kernel32+0x10856 explorer.exe 0x76b44dd6 winmm+0x4dd6
0x80f1a2e8 1724 612 0x7c810856 kernel32+0x10856 explorer.exe 0x762836f7 stobject+0x36f7
0xff1f9b10 1724 964 0x7c810856 kernel32+0x10856 explorer.exe 0x9069 0x9069
0xff382188 1732 1652 0x7c810867 kernel32+0x10867 wuaclt.exe 0x40bad5 wuaclt+0xbad5
0xff3b5b38 1732 1876 0x7c810856 kernel32+0x10856 wuaclt.exe 0x906a 0x906a
0xff37c890 1732 1588 0x7c810856 kernel32+0x10856 wuaclt.exe 0x606b73ae esent+0x73ae
0xff398638 1732 680 0x7c810856 kernel32+0x10856 wuaclt.exe 0x606b73ae esent+0x73ae
0xff382600 1732 1768 0x7c810856 kernel32+0x10856 wuaclt.exe 0x606b73ae esent+0x73ae
0xff3976c0 1732 2012 0x7c810856 kernel32+0x10856 wuaclt.exe 0x606b73ae esent+0x73ae
0xff37e370 1732 152 0x7c810856 kernel32+0x10856 wuaclt.exe 0x8778 0x8778
0xff1fd1a0 1788 1792 0x7c810867 kernel32+0x10867 VMUpgradeHelper 0x41705d vmupgradehelper+0x1705d
0xff153290 1788 1804 0x7c810856 kernel32+0x10856 VMUpgradeHelper 0x77deb479 advapi32+0x1b479
0xff149be0 1788 1880 0x7c810856 kernel32+0x10856 VMUpgradeHelper 0x86a8 0x86a8
0xff1475d0 1788 1908 0x7c810856 kernel32+0x10856 VMUpgradeHelper 0x8773 0x8773
0xff121da8 1788 800 0x7c810856 kernel32+0x10856 VMUpgradeHelper 0x9059 0x9059
0xff141340 1968 1972 0x7c810867 kernel32+0x10867 TPAutoConnSvc.e 0x40a26e tpautoconnsvc+0xa26e
0xff22a6f8 1968 1996 0x7c810856 kernel32+0x10856 TPAutoConnSvc.e 0x77deb479 advapi32+0x1b479
0xff11fda8 1968 892 0x7c810856 kernel32+0x10856 TPAutoConnSvc.e 0x40b65f tpautoconnsvc+0xb65f
0xff11fb30 1968 868 0x7c810856 kernel32+0x10856 TPAutoConnSvc.e 0x769c8831 userenv+0x8831
0xff3b64c8 1968 984 0x7c810856 kernel32+0x10856 TPAutoConnSvc.e 0x40b65f tpautoconnsvc+0xb65f
Out<20:08:48> Plugin: threads (Threads)
[1] tigger.vmem 20:08:48
```

Malware Analyst 2: Sality

Background: A malware that aims to lower your security and delete important files related to Windows system while also replacing and spreading itself to other files. This virus can not only affect computer's files, but it can also possibly delete antivirus security to further spread itself.

11/30/2021

```
C:\Windows\System32\cmd.exe - rekal --filename sality.vmem
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Rekall>rekal --filename sality.vmem

The Rekall Digital Forensic/Incident Response framework 1.7.2.rc1 (Hurricane Ridge).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

[1] sality.vmem 19:02:07 pslist
2021-12-10 19:02:08,946:WARNING:rekal:1:Inventory for repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget to create an inventory? You must use the tools/profiles/build_profile_repo.py tool with the --inventory flag.
2021-12-10 19:02:08,947:WARNING:rekal:1:repository http://profiles.rekall-forensic.com will be disabled.

pslist()
LPROCCESS          name      pid   ppid  thread_count handle_count session_id wow64  process_create_time    process_exit_time
0x810h1660 System       4      0      58        190     0 False 2010-08-11 06:06:392 -
0xf25a7e0 alg.exe     216     676     7      108     0 False 2010-08-11 06:06:392 -
0xf367e8 VMwareTray.exe 432     1724    4      53      0 False 2010-08-11 06:06:312 -
0xf374980 VMwareUser.exe 452     1724    11     208     0 False 2010-08-11 06:06:322 -
0x80f4588 wuauctl.exe 468     1028    7      139     0 False 2010-08-11 06:06:372 -
0xf2ab20 smss.exe    544     4      3      21      0 False 2010-08-11 06:06:212 -
0xfledca0 csrss.exe   608     544    11      434     0 False 2010-08-11 06:06:232 -
0xf1c978 winlogon.exe 632     544    19      513     0 False 2010-08-11 06:06:232 -
0xf2d7020 services.exe 676     632    16      269     0 False 2010-08-11 06:06:242 -
0xf2d7130 lsass.exe    680     632    21      349     0 False 2010-08-11 06:06:245 -
0xf2d8230 svchost.exe 944     676     1      24      0 False 2010-08-11 06:06:242 -
0x80ff88d8 svchost.exe 956     676    18      203     0 False 2010-08-11 06:06:242 -
0xf3a4310 wscnfy.exe 889     1028    4      32      0 False 2010-08-11 06:06:492 -
0xf27560 svchost.exe 936     676    11      268     0 False 2010-08-11 06:06:242 -
0x80ff9f10 svchost.exe 1028    676    88      1426    0 False 2010-08-11 06:06:242 -
0xf3b5f8 TPAutoConnect.e 1084    1968    4      66      0 False 2010-08-11 06:06:522 -
0xf2d558 svchost.exe 1088     676    6      80      0 False 2010-08-11 06:06:252 -
0xf2b3b00 svchost.exe 1148     676    15      212     0 False 2010-08-11 06:06:262 -
0x80f167b8 cmd.exe    1368    1668    0      -      0 False 2010-08-15 17:43:452 2010-08-15 17:43:452
0xf1d7a0 spoolsv.exe 1432     676    13      135     0 False 2010-08-11 06:06:262 -
0xf1b828 vmtoolsd.exe 1668     676    5      221     0 False 2010-08-11 06:06:352 -
0xf3b65d0 explorer.exe 1724    1708    18      414     0 False 2010-08-11 06:06:392 -
0x80fd17e1 exif.dll.exe 1724    1028    7      178     0 False 2010-08-11 06:07:472 -
0xf1fd88 VMpilotHelper 1788     676    5      102     0 False 2010-08-11 06:06:382 -
0xf1d3b28 TPAutocommSvc.e 1968     676    5      100     0 False 2010-08-11 06:06:392 -
0xf22f3d0 aelas.exe   1984    1724    19      139     0 False 2010-08-15 17:43:262 -
Out:19:02:10: Plugin: pslist (WinPnPList)
[1] sality.vmem 19:02:49 connscan
[1] sality.vmem 19:02:49 connscan()
tcpip/GUID/9546A8399BAC4717BC41758594EF0D9C2 matched offset 0x4562+0xf3ba9000=0 offset_p      local_net_address      remote_net_address      pid
0x214988 172.16.176.143:1034      131.107.115.254:80      1260
0x6015ab0 172.16.176.143:1037      131.107.115.254:443      1260
Out:19:02:51: Plugin: connscan (ConnScan)
[1] sality.vmem 19:03:13 > sockets
[1] sality.vmem 19:03:13 > sockets()
offset_v  pid  port  proto  protocol  address  create_time
-----+
0x80fd1008  4      0      47  GRE      0.0.0.0  2010-08-11 06:08:002
0xff258008  688    500    17  UDP      0.0.0.0  2010-08-11 06:06:352
0xfff367008  4      445    6   TCP      0.0.0.0  2010-08-11 06:06:172
0x80ffc128  936    135    6   TCP      0.0.0.0  2010-08-11 06:06:242
0xffff225b70 688    0      255  Reserved 0.0.0.0  2010-08-11 06:06:352
0xffff227340 1028   123    17  UDP      127.0.0.1 2010-08-15 17:43:452
0x80fce930  1088   1025   17  UDP      0.0.0.0  2010-08-11 06:06:382
0xffff36b250 1028   1055   6   TCP      0.0.0.0  2010-08-15 17:43:452
0xffff396c68 1984   5565   17  UDP      0.0.0.0  2010-08-15 17:43:322
0xffff127d28 216    1026   6   TCP      127.0.0.1 2010-08-11 06:06:392
0xffff153a20 1148   1900   17  UDP      127.0.0.1 2010-08-15 17:43:452
0xffff1b8250 688    4500   17  UDP      0.0.0.0  2010-08-11 06:06:352
0xffff382e98  4      1033   6   TCP      0.0.0.0  2010-08-11 06:08:002
0x80fbdc40  4      445    17  UDP      0.0.0.0  2010-08-11 06:06:172
Out:19:03:13: Plugin: sockets (Sockets)
```

11/30/2021

EPROCESS	ppid	thd_count	hnd_count	create_time
0x810b1660 System (4)	0	58	190	-
. 0xff2ab020 smss.exe (544)	4	3	21	2010-08-11 06:06:21Z
.. 0xff1ecda0 csrss.exe (608)	544	11	434	2010-08-11 06:06:23Z
.. 0xff1ec978 winlogon.exe (632)	544	19	513	2010-08-11 06:06:23Z
... 0xff247020 services.exe (676)	632	16	269	2010-08-11 06:06:24Z
... 0xff25a7e0 alg.exe (216)	676	7	108	2010-08-11 06:06:39Z
... 0xff218230 vmacthlp.exe (844)	676	1	24	2010-08-11 06:06:24Z
... 0x80ff88d8 svchost.exe (856)	676	18	203	2010-08-11 06:06:24Z
.... 0xff217560 svchost.exe (936)	676	11	268	2010-08-11 06:06:24Z
.... 0x80fbf910 svchost.exe (1028)	676	88	1426	2010-08-11 06:06:24Z
.... 0x80f94588 wuauctl.exe (468)	1028	7	139	2010-08-11 06:09:37Z
.... 0xff364310 wsctfy.exe (888)	1028	4	32	2010-08-11 06:06:49Z
.... 0x80f60da0 wuauctl.exe (1732)	1028	7	178	2010-08-11 06:07:44Z
.... 0xff22d558 svchost.exe (1088)	676	6	80	2010-08-11 06:06:25Z
.... 0xff203b80 svchost.exe (1148)	676	15	212	2010-08-11 06:06:26Z
.... 0xff1d7da0 spoolsv.exe (1432)	676	13	135	2010-08-11 06:06:26Z
.... 0xff1b8b28 vmtoolsd.exe (1668)	676	5	221	2010-08-11 06:06:35Z
.... 0x80f167b8 cmd.exe (1368)	1668	0	-	2010-08-15 17:43:45Z
.... 0xff1fdc88 VMUpgradeHelper (1788)	676	5	102	2010-08-11 06:06:38Z
.... 0xff143b28 TPAutoConnSvc.e (1968)	676	5	100	2010-08-11 06:06:39Z
.... 0xff38b5f8 TPAutoConnect.e (1084)	1968	4	66	2010-08-11 06:06:52Z
... 0xff255020 lsass.exe (688)	632	21	349	2010-08-11 06:06:24Z
0xff3865d0 explorer.exe (1724)	1708	18	414	2010-08-11 06:09:29Z
. 0xff3667e8 VMwareTray.exe (432)	1724	4	53	2010-08-11 06:09:31Z
. 0xff374980 VMwareUser.exe (452)	1724	11	208	2010-08-11 06:09:32Z
. 0xff22f3d0 aelas.exe (1984)	1724	19	139	2010-08-15 17:43:26Z

11/30/2021

```
[1] sality.vmem 19:03:55> psxview
-----> psxview()
 _EPROCESS      name      pid PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
-----
0x810b1660 System          4 True    False  True  False  True  True  True
0xff25a7e0 alg.exe        216 True   True  True  True  True  True  True
0xff3667e8 VMWareTray.exe 432 True   True  True  True  True  True  True
0xff374980 VMWareUser.exe 452 True   True  True  True  True  True  True
0x80f94588 wuauctl.exe   468 True   True  True  True  True  True  True
0xff2ab020 smss.exe       544 True   False  True  False  True  True  True
0xff1ecd00 csrss.exe     608 True   False  True  True  True  True  True
0xff1ec978 winlogon.exe   632 True   True  True  True  True  True  True
0xff247020 services.exe  676 True   True  True  True  True  True  True
0xff255020 lsass.exe     688 True   True  True  True  True  True  True
0xff218230 vmauthlp.exe  844 True   True  True  True  True  True  True
0x80ff88d8 svchost.exe   856 True   True  True  True  True  True  True
0xff364310 wscntfy.exe   888 True   True  True  True  True  True  True
0xff217560 svchost.exe   936 True   True  True  True  True  True  True
0x80fbf910 svchost.exe   1028 True  True  True  True  True  True  True
0xf38b5f8 TPAutoConnect.e 1084 True  True  True  True  True  True  True
0xff22d558 svchost.exe   1088 True  True  True  True  True  True  True
0xff203b80 svchost.exe   1148 True  True  True  True  True  True  True
0x80f167b8 cmd.exe       1368 True  False  True  False  True  True  False
0xff1d7da0 spoolsv.exe   1432 True  True  True  True  True  True  True
0xff1b8b28 vmtoolsd.exe  1668 True  True  True  True  True  True  True
0xff3865d0 explorer.exe   1724 True  True  True  True  True  True  True
0x80f60da0 wuauctl.exe   1732 True  True  True  True  True  True  True
0xff1fdc88 VMUpgradeHelper 1788 True  True  True  True  True  True  True
0xff143b28 TPAutoConnSvc.e 1968 True  True  True  True  True  True  True
0xff22f3d0 aelas.exe      1984 True  True  True  True  True  True  True
Out<19:03:59> Plugin: psxview (WindowsPsxView)
[1] sality.vmem 19:03:59>
```

```
[1] sality.vmem 21:25:11> hooks_iat 1368
-----> hooks_iat(1368)
      source           target           target_func
-----
-----
Process cmd.exe (1368)
-----
Out<21:25:11> Plugin: hooks_iat (IATHooks)
[1] sality.vmem 21:25:11>
```

```
[1] sality.vmem 21:28:17> cmdscan
-----> cmdscan()
*****
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0xf786f8 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x448
Cmd Address Text
-----
Out<21:28:17> Plugin: cmdscan (CmdScan)
```

Procinfo

11/30/2021

```
*****
Pid: 1724 explorer.exe

Process Environment
=::=:\\
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=BILLY-DB5B96DD3
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Administrator
LOGONSERVER=\BILLY-DB5B96DD3
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramFiles=C:\Program Files
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=BILLY-DB5B96DD3
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

DE Information

```
*****
Pid: 1984 aelas.exe

Process Environment
=::=:\\
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=BILLY-DB5B96DD3
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Administrator
LOGONSERVER=\BILLY-DB5B96DD3
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramFiles=C:\Program Files
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=BILLY-DB5B96DD3
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

Malware Analyst 3: Silent Banker

Background: Is a Trojan Banker that is known to steal your information like keystrokes, screenshots, etc. Except is most notably know to steal information that includes your finances. Mostly this can be done with using a misleading spoof website to scam you (thinking that it's the real official website) for any of your important finical information, and it can backdoor by installing virus with access to your email.

```
C:\Windows\System32\cmd.exe -rekal --filename silentbanker.vmem
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Rekall\rekal --filename silentbanker.vmem

The Rekall Digital Forensic/Incident Response framework 1.7.2.rc1 (Hurricane Ridge).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

[1] silentbanker.vmem 20:51:10 pslist
2021-12-10 20:51:13,146:WARNING:rekal:1:Inventory For repository "http://profiles.rekall-forensic.com" seems malformed. Are you behind a captive portal or proxy? If this is a custom repository, did you forget to create an inventory? You must use the tools/profiles/build_profile_repo.py tool with the --inventory flag.
2021-12-10 20:51:13,145:WARNING:rekal:1:Repository: http://profiles.rekall-forensic.com will be disabled.

pslist()
-----
```

l_EPROCESS	name	pid	ppid	thread_count	handle_count	session_id	wow64	process_create_time	process_exit_time
0x810b1660	System	4	0	59	183	-	False	-	-
0xff25a7e0	alg.exe	216	676	6	105	0	False	2010-08-11 06:06:39z	-
0xf3d67e8	VWareTray.exe	432	1724	1	49	0	False	2010-08-11 06:09:31z	-
0xf3f74980	VWareUser.exe	452	1724	7	192	0	False	2010-08-11 06:09:32z	-
0x80f45888	wuauctl.exe	468	1028	4	135	0	False	2010-08-11 06:09:37z	-
0xf2ab20	smss.exe	544	4	3	21	-	False	2010-08-11 06:06:21z	-
0xf1c1d0d0	csrss.exe	688	544	11	369	0	False	2010-08-11 06:06:22z	-
0xf1d07000	cryptsp.dll.exe	632	544	18	511	0	False	2010-08-11 06:06:23z	-
0xf2d7020	servicemsc.exe	676	632	16	269	0	False	2010-08-11 06:06:24z	-
0xf255020	lcass.exe	688	622	19	345	0	False	2010-08-11 06:06:24z	-
0xf2f8230	vmatchip.exe	944	676	1	24	0	False	2010-08-11 06:06:24z	-
0x80ff88d8	svchost.exe	856	676	17	199	0	False	2010-08-11 06:06:24z	-
0xf3f4310	wscnfy.exe	888	1028	1	27	0	False	2010-08-11 06:06:49z	-
0xf2f7560	svchost.exe	936	676	10	270	0	False	2010-08-11 06:06:24z	-
0x80fbff10	svchost.exe	1028	676	71	1355	0	False	2010-08-11 06:06:24z	-
0xf3b5f8	TPAutoConnect.e	1084	1968	1	61	0	False	2010-08-11 06:06:52z	-
0xf2d558	svchost.exe	1088	676	4	79	0	False	2010-08-11 06:06:25z	-
0xf385c0	cmd.exe	1136	1668	0	-	0	False	2010-08-15 19:01:51z	2010-08-15 19:01:51z
0xf263b88	svchost.exe	1148	676	14	208	0	False	2010-08-11 06:06:26z	-
0xf1f07d0	spools.exe	1432	676	13	135	0	False	2010-08-11 06:06:27z	-
0xf1f0550	vmtools.exe	1660	676	5	222	0	False	2010-08-11 06:06:35z	-
0xf3f0550	vmplayer.exe	1724	1724	12	317	0	False	2010-08-11 06:09:29z	-
0xf1f1dc88	VMMpupgradeWorker	1788	676	4	109	0	False	2010-08-11 06:06:38z	-
0x80f1b020	TEXPLORE.EXE	1884	1724	9	351	0	False	2010-08-15 18:54:05z	-
0xf1f43b28	TPAutoConnSvc.e	1968	676	5	100	0	False	2010-08-11 06:06:39z	-

```
Out:20:51:14 Plugin: pslist (WinPsList)
```

```
[1] silentbanker.vmem 21:21:25 connscan
-----> connscan()
tcpip/GUID/9546A8399BAC4717BC41758594EF0D9C2 matched offset 0x4562+0xf3ba9000=0 offset_p      local_net_address      remote_net_address      pid
-----
```

0x10732d8	172.16.176.143:1086	65.55.149.121:80	1884
0x1073e0	172.16.176.143:1098	65.54.81.155:80	1884
0x1073778	172.16.176.143:1077	65.55.15.243:80	1884
0x1073d00	172.16.176.143:1096	65.54.81.155:80	1884
0x107ae70	172.16.176.143:1063	202.89.231.60:80	1884
0x107ed68	172.16.176.143:1073	65.54.81.223:80	1884
0x107ed58	172.16.176.143:1088	65.55.239.161:80	1884
0x10c5e70	172.16.176.143:1074	65.55.15.241:80	1884
0x10f1d00	172.16.176.143:1079	209.234.225.242:80	1884
0x10fb4b8	172.16.176.143:1089	65.54.81.155:80	1884
0x111d900	172.16.176.143:1070	72.246.94.11:80	1884
0x1134e70	172.16.176.143:1068	65.55.253.21:80	1884
0x113b638	172.16.176.143:1076	65.55.15.123:80	1884
0x224988	172.16.176.143:1052	65.55.12.249:80	1884
0x2db12e0	172.16.176.143:1091	65.54.81.155:80	1884
0x2db1480	172.16.176.143:1080	65.54.81.174:80	1884
0x485dd58	172.16.176.143:1061	65.54.81.47:80	1884
0x4862b60	172.16.176.143:1069	96.6.124.43:80	1884
0x4863810	172.16.176.143:1078	65.54.81.206:80	1884
0x5ce6e70	172.16.176.143:1059	65.54.81.185:80	1884
0x5e354b8	172.16.176.143:1090	65.54.81.155:80	1884
0x5e3cb48	172.16.176.143:1062	4.23.40.126:80	1884
0x6015ab0	172.16.176.143:1056	69.43.160.4:80	1884
0x6232e70	172.16.176.143:1064	64.4.18.73:80	1884
0x6384e70	172.16.176.143:1055	207.46.140.21:80	1884

```
Out:21:21:26 Plugin: connscan (ConnScan)
```

11/30/2021

EPROCESS	ppid	thd_count	hnd_count	create_time
0x810b1660 System (4)	0	59	183	-
0xff2ab020 smss.exe (544)	4	3	21	2010-08-11 06:06:21Z
0xff1ecda0 csrss.exe (608)	544	11	365	2010-08-11 06:06:23Z
0xff1ec978 winlogon.exe (632)	544	18	511	2010-08-11 06:06:23Z
0xff247020 services.exe (676)	632	16	269	2010-08-11 06:06:24Z
0xff25a7e0 alg.exe (216)	676	6	105	2010-08-11 06:06:39Z
0xff218230 vmauthlsp.exe (844)	676	1	24	2010-08-11 06:06:24Z
0x80ff88d8 svchost.exe (856)	676	17	199	2010-08-11 06:06:24Z
0xff217560 svchost.exe (936)	676	10	270	2010-08-11 06:06:24Z
0x80fbf910 svchost.exe (1028)	676	71	1355	2010-08-11 06:06:24Z
0x80f94588 wuaucnt.exe (468)	1028	4	135	2010-08-11 06:09:37Z
0xff364310 wscntfy.exe (888)	1028	1	27	2010-08-11 06:06:49Z
0xff22d558 svchost.exe (1088)	676	4	79	2010-08-11 06:06:25Z
0xff203b80 svchost.exe (1148)	676	14	208	2010-08-11 06:06:26Z
0xff1d7da0 spoolsv.exe (1432)	676	13	135	2010-08-11 06:06:26Z
0xff1b8b28 vmtoolsd.exe (1668)	676	5	222	2010-08-11 06:06:35Z
0xff3856c0 cmd.exe (1136)	1668	0	-	2010-08-15 19:01:51Z
0xff1fdc88 VMUpgradeHelper (1788)	676	4	100	2010-08-11 06:06:38Z
0xff143b28 TPAutoConnSvc.e (1968)	676	5	100	2010-08-11 06:06:39Z
0xff38b5f8 TPAutoConnect.e (1084)	1968	1	61	2010-08-11 06:06:52Z
0xff255020 lsass.exe (688)	632	19	345	2010-08-11 06:06:24Z
0xff3865d0 explorer.exe (1724)	1708	12	317	2010-08-11 06:09:29Z
0xff3667e8 VMwareTray.exe (432)	1724	1	49	2010-08-11 06:09:31Z
0xff374980 VMwareUser.exe (452)	1724	7	192	2010-08-11 06:09:32Z
0x80f1b020 IEXPLORE.EXE (1884)	1724	9	351	2010-08-15 18:54:05Z

11/30/2021

```
[1] silentbanker.vmem 21:21:43> psxview
-----> psxview()
_EPROCESS      name      pid PsActiveProcessHead CSRSS PspCidTable Sessions Handles PSScan Thrdproc
-----
0x810b1660 System        4 True      False True  False  True  True
0xff25a7e0 alg.exe     216 True     True  True  True  True  True
0xff3667e8 VMWareTray.exe 432 True     True  True  True  True  True
0xff374980 VMWareUser.exe 452 True     True  True  True  True  True
0x80f94588 wuauctl.exe  468 True     True  True  True  True  True
0xf2ab020 smss.exe    544 True     False True  False  True  True
0xf1ecd0 csrss.exe   608 True     False True  True  True  True
0xf1ec978 winlogon.exe 632 True     True  True  True  True  True
0xff247020 services.exe 676 True     True  True  True  True  True
0xf255020 lsass.exe   688 True     True  True  True  True  True
0xf218230 vmauthlp.exe 844 True     True  True  True  True  True
0x80ff88d8 svchost.exe 856 True     True  True  True  True  True
0x364310 wscntfy.exe  888 True     True  True  True  True  True
0xf217560 svchost.exe  936 True     True  True  True  True  True
0x80fbf910 svchost.exe 1028 True    True  True  True  True  True
0xf38b5f8 TPAutoConnect.e 1084 True    True  True  True  True  True
0xf22d558 svchost.exe  1088 True    True  True  True  True  True
0xf3856c0 cmd.exe     1136 True    False True  False  True  False
0xf203b80 svchost.exe  1148 True    True  True  True  True  True
0xf1d7da0 spoolsv.exe 1432 True    True  True  True  True  True
0xf1b8b28 vmtoolsd.exe 1668 True    True  True  True  True  True
0xf3865d0 explorer.exe 1724 True    True  True  True  True  True
0x80f60da0 wuauctl.exe 1732 False   False False  False  True  False
0xf1fdc88 VMUpgradeHelper 1788 True    True  True  True  True  True
0x80f1b020 IEXPLORE.EXE 1884 True    True  True  True  True  True
0xf143b28 TPAutoConnSv.e 1968 True    True  True  True  True  True
Out<21:21:46> Plugin: psxview (WindowsPsxView)
[1] silentbanker.vmem 21:21:46>
```

```
[1] silentbanker.vmem 21:26:05> hooks_iat 1136
-----> hooks_iat(1136)
      source          target          target_func
-----
Process cmd.exe (1136)
-----
Out<21:26:05> Plugin: hooks_iat (IATHooks)
```

```
[1] silentbanker.vmem 21:29:07> cmdscan
-----> cmdscan()
*****
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0xf786f8 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x448
Cmd Address Text
-----
Out<21:29:07> Plugin: cmdscan (CmdScan)
```

11/30/2021

```
*****
Pid: 432 VMwareTray.exe

Process Environment
=::=-:\_
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=BILLY-DB5B96DD3
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOME PATH=\Documents and Settings\Administrator
LOGONSERVER=\BILLY-DB5B96DD3
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Program Files\VMware\VMware Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramFiles=C:\Program Files
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=BILLY-DB5B96DD3
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS

PE Infomation
Attribute Value
-----
*****
```

```
*****
Pid: 452 VMwareUser.exe

Process Environment
=::=-:\_
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=BILLY-DB5B96DD3
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOME PATH=\Documents and Settings\Administrator
LOGONSERVER=\BILLY-DB5B96DD3
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Program Files\VMware\VMware Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramFiles=C:\Program Files
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=BILLY-DB5B96DD3
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

References:

Tutorial Links

<https://www.youtube.com/watch?v=verKqNVshS4>

<http://www.rekall-forensic.com/documentation-1/rekall-documentation/tutorial>

<https://stariix.blogspot.com/2018/05/zeus-trojan-memory-forensics-with.html>

<https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1>

Source Codes Links

<https://virusshare.com/file?364040375650bf968b7503de130ecf17b8194f47825847e98149446acd741e50>

<https://github.com/google/rekall>

<https://github.com/google/rekall/releases>

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

<https://github.com/InQuest/malware-samples>

<https://www.python.org/downloads/release/python-360/>

Note Information Links about the Analyzed Malware

11/30/2021

<https://www.darkreading.com/attacks-breaches/-tigger-trojan-keeps-security-researchers-hopping>

<https://en.wikipedia.org/wiki/Sality>

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/sality>

<https://www.eclipseaviation.com/is-silent-banker-a-trojan-horse-2/>

Malware Database Links

<https://virusshare.com/>

<https://bazaar.abuse.ch/browse/>

<https://reverseengineering.stackexchange.com/questions/206/where-can-i-as-an-individual-get-malware-samples-to-analyze>

<https://zeltser.com/malware-sample-sources/>

Miscellaneous Links to Helpful information

<https://evild3ad.com/1136/volatility-memory-forensics-federal-trojan-aka-r2d2/>

<https://sensorstechforum.com/popular-windows-file-types-used-malware-2018/>

<https://rioasmara.com/2019/09/28/basic-extracting-malware-from-memory/>

<https://github.com/InQuest/malware-samples>

<https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>

<https://github.com/ganboing/malwarecookbook>