

CIRCL - Digital Forensics 1.0.3

Introduction: Windows-, Memory- and File Forensics



CIRCL *TLP:CLEAR*

info@circl.lu

December, 2024

Overview

1. Windows Registry
2. Event Logs
3. Other Sources of Information
4. Malware Analysis
5. Analysing files
6. Live Response
7. Memory Forensics
8. Bibliography and Outlook

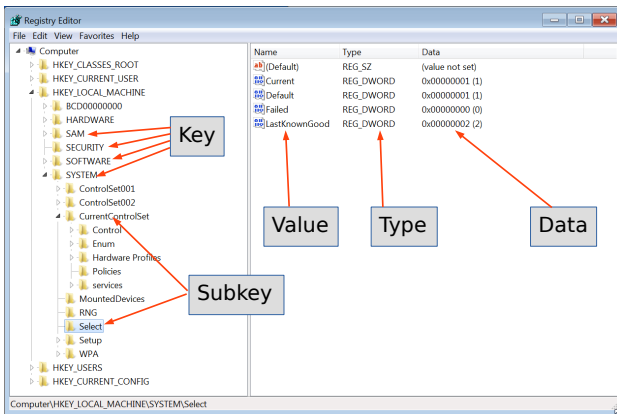


1. Windows Registry

1.1 About: Windows Registry

- MS DOS and old Windows
 - On system boot: What programs to load
 - How the system interact with the user
 - `autoexec.bat`
 - `config.sys`
 - `system.ini`
 - `win.ini`
 - <https://support.microsoft.com/en-us/help/256986/>
 - A central hierarchical database
 - Replace text based config files
 - Contains information for operating
 - Hardware system wide
 - OS all aspects
 - Applications installed
 - User preferences / behavior
- A gold mine for forensics

1.1 About: Windows Registry



Key data structures contains a last write time stamp

1.1 About: Windows Registry

- Hive files: Location

`%SystemRoot%\system32\config`

→ SAM, SECURITY, SYSTEM, SOFTWARE

`%UserProfile%\NTUSER.DAT`

`%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat`

→ Created during system boot

- How often do you manually edit the Registry?

- `regedit.exe`

- Black Magic for many admins

- Every user interacts with the Registry

- Timestamps → Timeline

1.2 Under the hood: Key Cell

```
0000:  a0ff ffff  6e6b 2000  6f0f 0e3b b78d d101  ....nk .o...;....
0010:  0200 0000 085e 0500  0000 0000 0000 0000  ....^.....
0020:  ffff ffff ffff ffff  0200 0000 0021 0500  ....!.....
0030:  102e 0000 ffff ffff  0000 0000 0000 0000  ....
0040:  1400 0000 1000 0000  0000 0000 0a00 0000  ....
0050:  496e 7465 7266 6163  6573 0080 0200 0000  Interfaces.....
```

Offsets :	0x00	0	4	Size
	0x04	4	2	Node ID
	0x06	6	2	Node type
	0x08	8	8	Last write time
		
	0x4c	76	2	Lenght of key name
	0x50	80	<76>	key name + padding

- Exercise: Calculate the size of the key cell
a0 ff ff ff
- Exercise: Calculate the size of the key name
0a 00

1.2 Under the hood: Value Cell

```
0000:                                d8ff ffff 766b 0d00          ....vk...
0010: 0400 0080 0200 0000 0400 0000 0100 0000  ....
0020: 4c61 7374 4b6e 6f77 6e47 6f6f 6400 0000  LastKnownGood...
```

Offset :	0x00	0	4	Size
	0x04	4	2	Node ID
	0x06	6	2	Value name length
	0x08	8	4	Data length
	0x0c	12	4	Data offset
	0x10	16	4	value typw

- Exercise: Calculate the size of the value cell

d8 ff ff ff

- Exercise: Calculate the size of the value name length

0d 00

1.3 Hive files

- SAM
 - Security Accounts Manager: Local users
- Security
 - Audit settings
 - Machine, domain SID
- System
 - Hardware configuration
 - System configuration
- Software
 - Windows settings
 - Application information
- NTUser.dat
 - User behavior and settings
- UsrClass.dat
 - Graphical User Interface information

1.3 Hive files

- Windows XP:

`C:\Documents and Settings\<username>\NTUSER.DAT`

`C:\Documents and Settings\<username>\Local Settings\
Application Data\Microsoft\Windows\UsrClass.dat`

- Windows Vista and above:

`C:\Users\<user>\NTUSER.DAT`

`C:\Users\<user>\AppData\Local\Microsoft\Windows\
UsrClass.dat`

- `C:\Windows\inf\setupapi.log`
(Plug and Play Log)

1.3 Hive files - Exercise: Get hive files

Extract registry hive files from forensic image

```
- mkdir registry/out
```

1.3 Hive files - Exercise: Get hive files

Extract registry hive files from forensic image

1. Investigate Meta-Information

```
ewfinfo image.E01  
ewfexport image.E01
```

```
mkdir registry/out
```

1.3 Hive files - Exercise: Get hive files

Extract registry hive files from forensic image

1. Investigate Meta-Information

```
ewfinfo image.E01  
ewfexport image.E01
```

2. Mount evidences

```
sudo mkdir /media/case1  
mmls image.raw  
sudo mount -o ro,offset=$((512*63)) image.raw /media/case1/
```

1.3 Hive files - Exercise: Get hive files

Extract registry hive files from forensic image

1. Investigate Meta-Information

```
ewfinfo image.E01
ewfexport image.E01
```

2. Mount evidences

```
sudo mkdir /media/case1
mmls image.raw
sudo mount -o ro,offset=$((512*63)) image.raw /media/case1/
```

3. Copy files

```
mkdir registry
cp /media/case1/WINDOWS/system32/config/SAM registry
cp /media/case1/WINDOWS/system32/config/software registry
cp /media/case1/WINDOWS/system32/config/system registry
cp /media/case1/WINDOWS/system32/config/SECURITY registry
cp /media/case1/Documents\ and\ Settings/Jean/NTUSER.DAT registry
cp /media/case1//Documents\ and\ Settings/Jean/Local\ Settings/
  Application\ Data/Microsoft/Windows/UsrClass.dat registry/
ls registry/
mkdir registry/out
```

1.4 RegRipper

- <https://github.com/keydet89/RegRipper4.0>
- Plugins: 385

```
regripper -h
Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.
```

```
ls /usr/lib/regripper/plugins | grep pl$ | wc -l
249
```

```
ls /usr/lib/regripper/plugins | grep -v pl$
all
amcache
ntuser
sam
security
software
syscache
system
usrclass
```

1.4 RegRipper - Examples

```
regripper -p compname -r software
Select not found.
```

```
regripper -p compname -r system
  ComputerName    = JEAN-13FBF038A3
  TCP/IP Hostname = jean-13fbf038a3
```

```
regripper -p run -r NTUSER.DAT
```

```
Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2008-07-18 04:36:52Z
  MSMSGs - "C:\Program Files\Messenger\msmsgs.exe" /background
  Aim6 - "C:\Program Files\AIM6\aim6.exe" /d locale=en-US ee://aol/imApp
```

```
regripper -p run -r software
```

```
Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2008-07-06 07:21:46Z
  VMware User Process - C:\Program Files\VMware\VMware Tools\VMwareUser.exe
  VMware Tools - C:\Program Files\VMware\VMware Tools\VMwareTray.exe
```

```
Microsoft\Windows\CurrentVersion\Run\OptionalComponents
LastWrite Time 2008-07-06 07:21:46Z
```


1.4 RegRipper - Examples

```
mkdir registry/out
```

```
regripper -f sam -r SAM > out/sam.txt  
regripper -a      -r SAM > out/sam2.txt  
less registry/out/sam.txt
```

User Information

```
Username      : Administrator [500]  
Full Name     :  
User Comment  : Built-in account for administering the computer/domain  
Account Type  : Default Admin User  
Account Created : 2008-05-13 22:20:14Z  
Name          :  
Last Login Date : 2008-07-21 01:22:18Z  
Pwd Reset Date : 2008-05-13 22:23:39Z  
Pwd Fail Date  : Never  
Login Count   : 24  
Embedded RID   : 500  
    —> Password does not expire  
    —> Normal user account  
  
Username      : Guest [501]  
Full Name     :  
User Comment  : Built-in account for guest access to the computer/domain  
Account Type  : Default Guest Acct  
Account Created : 2008-05-13 22:20:14Z
```

1.5 RegRipper: Exercise

1. Extract Hive files from infected PC
2. Rip them with RegRipper profiles
3. Collect important general information
4. Try to find incident related artefacts
5. Add the information to report

1.5 RegRipper: Exercise

1. Extract Hive files from infected PC
2. Rip them with RegRipper profiles
3. Collect important general information
4. Try to find incident related artefacts
5. Add the information to report

```
mkdir registry/out
```

```
regripper -a -r SAM > out/sam.txt
regripper -a -r SECURITY > out/security.txt
regripper -a -r software > out/software.txt
regripper -a -r system > out/system.txt
regripper -a -r NTUSER.DAT > out/NTUser.txt
regripper -a -r UserClass.dat > out/UserClass.txt
```

```
ls -lh out/
 24K Nov 11 07:46 NTUser.txt
 7.1K Nov 11 07:47 sam.txt
 603 Nov 11 07:46 security.txt
658K Nov 11 07:46 software.txt
157K Nov 11 07:46 system.txt
 1.5K Nov 11 07:47 UserClass.txt
```

1.6 General information: sam, security

```
less out/SAM.txt
```

```
Username      : Administrator [500]
Last Login Date : 2008-07-21 01:22:18Z
Pwd Fail Date  : Never
Login Count    : 24
```

```
Username      : Jean [1004]
Last Login Date : 2008-07-20 00:00:41Z
Pwd Fail Date  : Never
Login Count    : 80
```

```
Group Name    : Administrators [7]
LastWrite     : 2008-05-14 05:35:35Z
S-1-5-21-484763869-796845957-839522115-1006
S-1-5-21-484763869-796845957-839522115-1008
S-1-5-21-484763869-796845957-839522115-1007
S-1-5-21-484763869-796845957-839522115-1005
S-1-5-21-484763869-796845957-839522115-1003
S-1-5-21-484763869-796845957-839522115-500
S-1-5-21-484763869-796845957-839522115-1004
```

```
less out/security.txt
```

1.6 General information: system, software

```
regripper -p winver -r software
```

ProductName	Microsoft Windows XP
CSDVersion	Service Pack 3
BuildLab	2600.xpsp.080413-2111
RegisteredOrganization	
RegisteredOwner	Jean User
InstallDate	2008-05-13 21:29:32Z

```
regripper -p networkcards -r software
```

Description	Key	LastWrite time
VMware Accelerated AMD PCNet Adapter		2008-05-14 05:31:26Z

```
regripper -p uninstall -r software
```

```
2008-07-19 23:32:23Z
  VMware Tools v.3.2.0.1288
  ....
```

```
regripper -p ips -r system
```

IPAddress	Domain
192.168.117.129	localdomain

1.6 General information: system, software

```
regripper -p profilelist -r software
```

```
Path       : %SystemDrive%\Documents and Settings\Jean  
SID        : S-1-5-21-484763869-796845957-839522115-1004  
LastWrite  : 2008-07-21 01:18:00Z
```

```
Path       : %SystemDrive%\Documents and Settings\Devon  
SID        : S-1-5-21-484763869-796845957-839522115-1007  
LastWrite  : 2008-07-12 06:04:40Z
```

```
Path       : %SystemDrive%\Documents and Settings\Administrator  
SID        : S-1-5-21-484763869-796845957-839522115-500  
LastWrite  : 2008-07-21 01:31:01Z
```

```
regripper -p shutdown -r system
```

```
ControlSet001\Control\Windows key, ShutdownTime value  
LastWrite time: 2008-07-21 01:31:32Z  
ShutdownTime  : 2008-07-21 01:31:32Z
```

```
regripper -p timezone -r system
```

```
ControlSet001\Control\TimeZoneInformation  
LastWrite Time 2008-05-14 06:55:57Z  
DaylightName   -> GMT Daylight Time
```

1.7 Tracing user activity

MRU - Most Recently Used

Open/Save As dialog box

```
regripper -p comdlg32 -r NTUSER.DAT
```

Recent Docs opened via Win. Explorer

```
regripper -p recentdocs -r NTUSER.DAT
```

ShellBags (Win7+)

Properties of folders

```
regripper -p shellbags -r UserClass.dat
```

Program execution

UserAssist: GUI based launched

```
regripper -p userassist -r NTUSER.DAT
```

ShimCache: Track compatibility issues

```
regripper -p shimcache -r system
```

1.7 Tracing user activity

USB attached devices

USBStor: Attached devices

```
less /media/case1/WINDOWS/setupapi.log  
regripper -p usbstor -r system
```

USBStor: Vendor & Product ID

```
regripper -p usb -r system
```

MountedDevices

```
regripper -p mountdev -r system
```

MountPoints

```
regripper -p mp2 -r NTUSER.DAT
```

SANS Posters:

<https://www.sans.org/posters/windows-forensic-analysis/>
<https://www.sans.org/posters/hunt-evil/>



2. Windows Event Logs

2.1 Introduction

- Up to Windows XP
 - Mainly 3 .evt files:
 - Security: `secevent.evt`
 - System: `sysevent.evt`
 - Application: `appevent.evt`
 - ... maybe some server service specific
 - Location: `/Windows/System32/config/`
 - Binary Event Log file format
- Beginning with Vista
 - Many .evtx files:
 - Security.evtx
 - System.evtx
 - Application.evtx
 - 120 files ++
 - Location: `/Windows/System32/winevt/Logs/`
 - New binary XML format

2.1 Introduction

- Advantage
 - Full fledged logging
 - Logging important events: E.g. Logon Success, ...
 - Detailed information
- Disadvantage
 - Limited period of time
 - Important events not logged by default: E.g. Logon Fail
 - Many events, hard to find related information
- Always interesting
 - Logon / Logoff
 - System boot
 - Services started
 - Hardware (dis)connected

2.2 Example: Event Viewer

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Event Viewer (Local)' tree with 'Security' selected under 'Windows Logs'. The right pane shows a list of security events. The event '4624 Logon' is selected, and its details are displayed in the bottom pane.

Security Number of events: 814 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	16/04/2020 18:17:28	Microsoft...	4672	Special Lo...
Audit S...	16/04/2020 18:17:28	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:17:28	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:17:28	Microsoft...	4648	Logon
Audit S...	16/04/2020 18:16:57	Microsoft...	4624	Logon
Audit S...	16/04/2020 18:16:55	Microsoft...	5024	Other Surt...

Event 4624, Microsoft Windows security auditing.

General **Details**

An account was successfully logged on.

Subject:

- Security ID: SYSTEM
- Account Name: WIN7WS\$
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

Logon Type: 2

New Logon:

- Security ID: Win7WS\John
- Account Name: John
- Account Domain: Win7WS
- Logon ID: 0x18333
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x18c

2.3 Get support

- Review logging policies

```
$ rip.pl -r SECURITY -p auditpol
```

```
.....
system:Other System Events          S/F
Logon/Logoff:Logon                  S
Logon/Logoff:Logoff                 S
Logon/Logoff:Account Lockout        S
Logon/Logoff:IPsec Main Mode         N
Logon/Logoff:IPsec Quick Mode        S
Logon/Logoff:IPsec Extended Mode     N
Logon/Logoff:Special Logon           N
Logon/Logoff:Other Logon/Logoff Events N
Logon/Logoff:Network Policy Server   S/F
Object Access:File System            N
.....
```

- Online:

- Microsoft TechNet
- <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- <http://eventid.net/>

2.4 Extracting and exploring event logs: Exercise

Extracting event logs

-

2.4 Extracting and exploring event logs

Extracting event logs

```
mkdir evtX
mkdir evtX/out

mmls nps-2008-jean.raw
sudo mount -o ro,offset=$((512*63)) nps-2008-jean.raw /media/sansforensics/casenps/

cp /media/sansforensics/casenps/WINDOWS/system32/config/AppEvent.Evt evtX/
cp /media/sansforensics/casenps/WINDOWS/system32/config/SecEvent.Evt evtX/
cp /media/sansforensics/casenps/WINDOWS/system32/config/SysEvent.Evt evtX/
ls -lh evtX/
```

Exploring event logs

2.4 Extracting and exploring event logs: Exercise

Extracting event logs

```
mkdir evtX
mkdir evtX/out

mmls image.raw
sudo mount=0 ro,offset=$((512*63)) image.raw/media/case1/

cp /media/case1/WINDOWS/system32/config/AppEvent.Evt evtX/
cp /media/case1/WINDOWS/system32/config/SecEvent.Evt evtX/
cp /media/case1/WINDOWS/system32/config/SysEvent.Evt evtX/
ls -lh evtX/
```

Exploring event logs

```
sudo apt install libevt-utils

evtinfo evtX/AppEvent.Evt
evtinfo evtX/SecEvent.Evt
evtinfo evtX/SysEvent.Evt

evtexport AppEvent.Evt | less
evtexport SysEvent.Evt | less
```


2.4 Extracting and exploring event logs

<https://eventlogxp.com/>

Untitled.elx - Event Log Explorer

File View Event Advanced Window Help

<Load filter>

Security on WIN8-SIFT

Showing 28541 event(s)

Type	Date	Time	Event	Source	Category	User	Comp
Audit Success	4/17/2020	6:18:17 AM	4624	Microsoft-Windows-Se-Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:18:17 AM	4648	Microsoft-Windows-Se-Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:18:04 AM	4672	Microsoft-Windows-Se-Special Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:18:04 AM	4624	Microsoft-Windows-Se-Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:06:49 AM	4672	Microsoft-Windows-Se-Special Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:06:49 AM	4624	Microsoft-Windows-Se-Legon	N/A	Win8	Win8
Audit Success	4/17/2020	6:06:20 AM	4672	Microsoft-Windows-Se-Special Legon	N/A	Win8	Win8

Description

Account Domain: DFIR
Logon ID: 000003E7

Logon Type: 5

Impersonation Level: Impersonation

New Logon:
Security ID: S-1-5-18
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 000003E7
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 00000234
Process Name: C:\Windows\System32\services.exe

Network Information:
Workstation Name: -
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: Advapi
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

2.5 Example .evtx

- Logon Success

```
$ evtxexport Security.evtx | less
.....
Event number           : 668
Written time           : Apr 15, 2019 12:58:33.650031000 UTC
Event level             : Information (0)
Computer name           : Win7WS
Source name             : Microsoft-Windows-Security-Auditing
Event identifier        : 0x00001210 (4624)
Number of strings       : 20
String: 1               : S-1-5-18
String: 2               : WIN7WS$
String: 3               : WORKGROUP
String: 4               : 0x0000000000000003e7
String: 5               : S-1-5-21-3408732720-2018246097-660081352-1000
String: 6               : John
String: 7               : Win7WS
String: 9               : 2
.....
String: 17              : 0x0000018c
String: 18              : C:\Windows\System32\winlogon.exe
String: 19              : 127.0.0.1
```

- Logon Fail

```
$ evtxexport Security.evtx | grep 4625
```

2.5 Example .evtx

Monterey Technology Group, ... (US) | https://www.ultimatewindowssecurity.com/se | ...

This is a valuable piece of information as it tells you HOW the user just logged on:

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648 . MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

Impersonation Level: (Win2012 and later)

From MSDN

Anonymous	Anonymous COM impersonation level that hides the identity of the caller. Calls to WMI may fail with this impersonation level.
-----------	---

2.6 Other log files

- /Windows/setuplog.txt
 - Untill WinXP, when Windows is installed
- /Windows//Debug/netsetup.log
 - Untill WinXP, when Windows is installed
- /Windows/setupact.log
 - Graphical part of setup process

```
2019-04-05 11:39:56, Info CBS Starting the TrustedInstaller main loop.  
2019-04-05 11:39:56, Info CBS TrustedInstaller service starts successfully.  
2019-04-05 11:39:56, Info CBS Setup in progress, aborting startup processing check  
2019-04-05 11:39:56, Info CBS Startup processing thread terminated normally
```

- /Windows/setupapi.log

```
/Windows/inf/setupapi.dev.log  
/Windows/inf/setupapi.app.log  
/Windows/inf/setupapi.offline.log
```

- /Windows/Tasks/SCHEDLGU.TXT
 - Task Scheduler Log

2.7 Exercise: Automated tools

Example: Chainsaw

```
wget https://github.com/WithSecureLabs/chainsaw/releases/
      download/v2.10.1/chainsaw_all_platforms+rules.zip

7z x chainsaw_all_platforms+rules.zip
cd chainsaw
chmod +x ./chainsaw.x86_64-unknown-linux-gnu
git clone https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.git

./chainsaw.x86_64-unknown-linux-gnu hunt EVTX-ATTACK-SAMPLES/ -s sigma/
  --mapping mappings/sigma-event-logs-all.yml | less

[+] Loading detection rules from: sigma/
[!] Loaded 3336 detection rules (490 not loaded)
[+] Loading forensic artefacts from: EVTX-ATTACK-SAMPLES/Command
    and Control, 2 (extensions: .evt, .evtx)
```

Challenge: Hayabusa

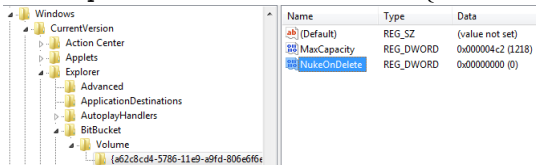
```
https://github.com/Yamato-Security/hayabusa
```



3. Other Windows Artifacts

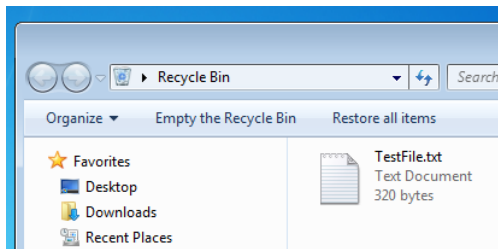
3.1 Recycle Bin - User support to undelete

- Files move to Recycle Bin:
 - Moved by mouse
 - Right click: Delete
- Not move to Recycle Bin:
 - Right click: Delete + SHIFT
 - Command line: del
 - Files on network shares
- NukeOnDelete
 - HKEY_USERS/_UUID_/Software/Microsoft/Windows/CurrentVersion/Explorer/BitBucket/Volume/{_Volume ID_}/NukeOnDelete



3.1 Recycle Bin - Life-Investigate

- Play script: `TextFile.txt`
 - 2019-04-30 17:31:57 UTC+2: Born
 - 2019-04-30 17:34:44 UTC+2: Content Modified
 - 2019-04-30 17:35:32 UTC+2: Deleted
- Analyze Recycle.Bin:



3.1 Recycle Bin - Forensics

- Play script: `TextFile.txt`
 - 2019-04-30 17:31:57 UTC+2: Born
 - 2019-04-30 17:34:44 UTC+2: Content Modified
 - 2019-04-30 17:35:32 UTC+2: Deleted
- Analyze `Recycle.Bin` directory:

```
/ $Recycle.Bin/S-1-5-21-3408732720-2018246097-660081352-1000/  
129 Apr  5 11:46  desktop.ini  
544 Apr 30 17:35  '$IOMHI9A.txt '  
320 Apr 30 17:34  '$ROMHI9A.txt '
```

```
strings -el \ $IOMHI9A.txt  
C:\Users\John\Documents\recycleTest\TestFile.txt
```

```
strings \ $ROMHI9A.txt  
      Test File  
      =====  
      This is a test file. It is just created to test Forensic  
      Artifacts for the 'Recycle Bin'.  
      .....
```

3.1 Recycle Bin - Forensics

- Play script: `TextFile.txt`
 - 2019-04-30 17:31:57 UTC+2: Born
 - 2019-04-30 17:34:44 UTC+2: Content Modified
 - 2019-04-30 17:35:32 UTC+2: Deleted
- File system timeline `Recycle.Bin` directory:

```
Tue Apr 30 2019 17:31:57
    320 ...b 47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt
```

```
Tue Apr 30 2019 17:34:44
    320 ma.. 47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt
```

```
Tue Apr 30 2019 17:35:32
    544 macb 44155-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$IOMHI9A.txt
    48 mac. 47022-144-1 /Users/John/Documents/recycleTest
    320 ..c. 47164-128-1 /$Recycle.Bin/S-1-5-21- ..... -1000/$ROMHI9A.txt
    376 mac. 9632-144-1 /$Recycle.Bin/S-1-5-21- ..... -1000
```



3.2 LNK Files

- Link or shortcut to files, applications, resources
- User activity: Files access
 - Local
 - Network shares
 - Appached devices
- LNK file remain after target file is deleted

Thu May 02 2019 14:54:02

280 ...b 43701—144—1 /Users/John/Documents/LNK

Thu May 02 2019 14:54:28

66 macb 43702—128—1 /Users/John/Documents/LNK/Test.txt

1573 macb 43922—128—4 /Users/John/AppData/Roaming/Microsoft/
Windows/Recent/LNK.lnk

2779 macb 43716—128—4 /Users/John/AppData/Roaming/Microsoft/
Windows/Recent/Test.txt.lnk

3.2 LNK Files

- Information inside LNK files
 - Target file MAC times
 - Target file size
 - Target file path
 - Volume information

```
exiftool Test.txt.lnk
```

```
...
Create Date       : 2019:05:02 14:54:28+02:00
Access Date      : 2019:05:02 14:54:28+02:00
Modify Date      : 2019:05:02 14:54:28+02:00
Target File Size  : 66
Icon Index       : (none)
Run Window       : Normal
Hot Key          : (none)
Drive Type       : Fixed Disk
Volume Label     :
Local Base Path   : C:\Users\
Net Name         : 8
Net Provider Type : Unknown (0x20000)
Relative Path     : ..\..\..\..\Documents\Test\Test.txt
Working Directory : C:\Users\John\Documents\Test
Machine ID       : john-pc
```

3.2 LNK Files: Exercise

Extract and investigate LNK file for document: 'm57biz.xls'

Preparation work:

3.2 LNK Files: Exercise

Extract and investigate LNK file for document: 'm57biz.xls'

Preparation work:

```
sudo mount -o ro,offset=$((512*63)) image.raw /media/case1  
mkdir lnk
```

Copy LNK file :

3.2 LNK Files: Exercise

Extract and investigate LNK file for document: 'm57biz.xls'

Preparation work:

```
sudo mount -o ro,offset=$((512*63)) image.raw /media/case1  
mkdir lnk
```

Copy LNK file:

```
cp /media/case1/Documents\ and\ Settings/Jean/Recent/m57biz.lnk lnk/
```

Investigate with exiftool:

3.2 LNK Files: Exercise

Extract and investigate LNK file for document: 'm57biz.xls'

Preparation work:

```
sudo mount -o ro,offset=$((512*63)) image.raw /media/case1
mkdir lnk
```

Copy LNK file:

```
cp /media/case1/Documents\ and\ Settings/Jean/Recent/m57biz.lnk lnk/
```

Investigate with exiftool:

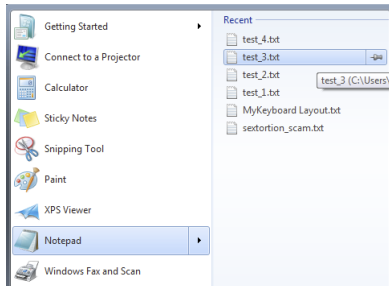
```
exiftool lnk/m57biz.lnk
```

```
.....
```

File Attributes	: Archive
Create Date	: 2008:07:20 01:28:03+00:00
Access Date	: 2008:07:20 01:28:03+00:00
Modify Date	: 2008:07:20 01:28:03+00:00
Target File Size	: 291840
Drive Type	: Fixed Disk
Local Base Path	: C:\Documents and Settings\Jean\Desktop\m57biz.xls
Machine ID	: jean-13fbf038a3

3.3 Jump Lists

- Introduced with Windows 7
- Similar Recent folder
- Recently opened documents / application
- Makes them accessible at Windows main menu



AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations

AppData/Roaming/Microsoft/Windows/Recent/CustomDestinations

3.3 Jump Lists

- File names start with 16 hex characters → JumpList ID
- File names end with .xxxDestinations-ms

```
C:> dir \Users\John\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

04/05/2020	12:50	33	792	1b4dd67f29cb1962	.automaticDestinations-ms
14/06/2019	16:43	4	608	28c8b86deab549a1	.automaticDestinations-ms
10/04/2019	14:32	29	696	6824f4a902c78fbd	.automaticDestinations-ms
10/04/2020	14:12	9	216	7e4dca80246863e3	.automaticDestinations-ms
04/05/2020	12:50	8	704	918e0ecb43d17e23	.automaticDestinations-ms
10/04/2019	14:30	3	072	b74736c2bd8cc8a5	.automaticDestinations-ms
09/04/2019	14:43	6	144	de48a32edcbe79e4	.automaticDestinations-ms

- Each Hex value correspond to an fixed application
- 918e0ecb43d17e23 = Notepad.exe

→ <https://github.com/EricZimmerman/JumpList/blob/master/JumpList/Resources/AppIDs.txt>

3.3 Jump Lists

- Exercise: Identify applications

```
cd JumpLists/AutomaticDestinations/  
ls -l
```

```
1b4dd67f29cb1962.automaticDestinations-ms ->  
28c8b86deab549a1.automaticDestinations-ms ->  
6824f4a902c78fbd.automaticDestinations-ms ->  
7e4dca80246863e3.automaticDestinations-ms ->  
918e0ecb43d17e23.automaticDestinations-ms ->  
b74736c2bd8cc8a5.automaticDestinations-ms ->  
de48a32edcbe79e4.automaticDestinations-ms ->
```

- Exercise: Analyze the Notepad Jump List file

3.3 Jump Lists

- Exercise: Identify applications

```
cd JumpLists/AutomaticDestinations/  
ll
```

```
1b4dd67f29cb1962.automaticDestinations-ms -> Windows Explorer  
28c8b86deab549a1.automaticDestinations-ms -> Internet Explorer 8  
6824f4a902c78fbd.automaticDestinations-ms -> Firefox 64.x  
7e4dca80246863e3.automaticDestinations-ms -> Control Panel  
918e0ecb43d17e23.automaticDestinations-ms -> Notepad (32-bit)  
b74736c2bd8cc8a5.automaticDestinations-ms -> WinZip  
de48a32edcbe79e4.automaticDestinations-ms -> Acrobat Reader 15.x
```

- Exercise: Analyze the Notepad Jump List file

3.3 Jump Lists

- Exercise: Identify applications

```
cd JumpLists/AutomaticDestinations/  
ll
```

```
1b4dd67f29cb1962.automaticDestinations-ms -> Windows Explorer  
28c8b86deab549a1.automaticDestinations-ms -> Internet Explorer 8  
6824f4a902c78fbd.automaticDestinations-ms -> Firefox 64.x  
7e4dca80246863e3.automaticDestinations-ms -> Control Panel  
918e0ecb43d17e23.automaticDestinations-ms -> Notepad (32-bit)  
b74736c2bd8cc8a5.automaticDestinations-ms -> WinZip  
de48a32edcbe79e4.automaticDestinations-ms -> Acrobat Reader 15.x
```

- Exercise: Analyze the Notepad Jump List file

```
7z l 918e0ecb43d17e23.automaticDestinations-ms
```

Date	Time	Attr	Size	Compressed	Name
		1398	1408	2
		1368	1408	1
		436	448	4
		392	448	3

```
-> file
```

```
-> exiftool
```

```
-> strings
```

```
7z x 918e0ecb43d17e23.automaticDestinations-ms  
strings -el DestList
```

3.4 Prefetch Files

- Application prefetching since XP
 - Monitor an application when it starts
 - Collect information about resources needed
 - Wait 10sec after application started
 - Know where to find the resources
 - Better performance: App launch faster
 - Better user experience
- Forensics value:
 - Proof an application was started
 - Secondary artifact
 - Created by the OS
 - Not deleted by the attacker
 - Even if the application don't exists anymore
 - And more

3.4 Prefetch Files

- Example: From file system time line

```
Thu May 02 2019 14:52:40
179712 .a.. 10940-128-3 /Windows/notepad.exe
```

```
Thu May 02 2019 14:52:50
56 mac. 42729-144-6 /Windows/Prefetch
16280 macb 43700-128-4 /Windows/Prefetch/NOTEPAD.EXE-D8414F97.pf
```

- Elements of the file name at /Windows/Prefetch
 - Application name
 - One way hash of path to the application
 - File extension: .pf
- Information found inside a Prefetch file:
 - Run count: How often application run
 - Last time executed
 - Application name incl. parameter
 - Path to application and resources

3.4 Prefetch Files

- Parsing a Prefetch file

```
prefetch.py -f NOTEPAD.EXE-D8414F97.pf
```

```
Executable Name: NOTEPAD.EXE
```

```
Run count: 1
```

```
Last Executed: 2019-05-02 12:52:40.339584
```

```
Resources loaded:
```

```
1:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\NTDLL.DLL
```

```
2:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNEL32.DLL
```

```
3:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
```

```
4:      \DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\KERNELBASE.DLL
```

```
.....
```

```
.....
```

- Additional benefits like:
 - User folder where the malware got executed
 - Compare Run count of different VSS could
→ Behavior of user

3.4 Prefetch Files: Exercise

Extract and investigate the Excel prefetch file

Copy prefetch file :

```
mkdir prefetch  
cp /media/sansforensics/casenps/WINDOWS/Prefetch/EXCEL.EXE-1C75F8D6.pf prefetch/
```

Investigate LNK file :

```
strings -el prefetch/EXCEL.EXE-1C75F8D6.pf | less
```

```
pref.pl -f prefetch/EXCEL.EXE-1C75F8D6.pf
```

```
File       : prefetch/EXCEL.EXE-1C75F8D6.pf  
Exe Path   : \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE  
Last Run   : Sun Jul 20 01:27:40 2008  
Run Count  : 2
```

3.5 XP Restore Points

- Backup of:
 - Critical system files
 - Registry partially
 - Local user profiles
 - But NO user data!
- Created automatically:
 - Every 24 hours
 - Windows Update
 - Installation of applications incl. driver
 - Manually
- For user: Useful to recover a broken system
- For analyst:
 - `rp.log`
 - Description of the cause
 - Time stamp
 - State of the system at different times

3.6 VSS - Volume Shadow Copy Service

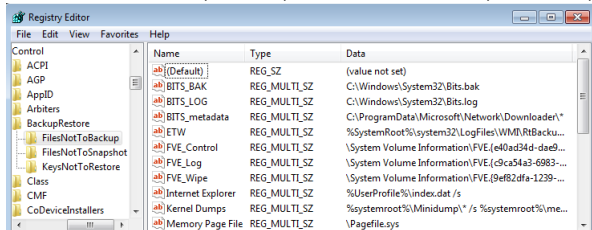
- Backup Service
 - System files
 - User data files
 - Operates on block level
- On live system
 - Run CMD as administrator

```
>vssadmin list shadows /for=c:/  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2005 Microsoft Corp.
```

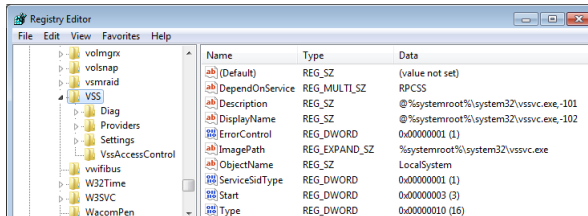
```
Contents of shadow copy set ID: {33eb3a7b-6d03-4045-aa70-37b714d49c72}  
  Contained 1 shadow copies at creation time: 10/04/2019 16:06:30  
    Shadow Copy ID: {34d9910b-ac1d-4b10-b282-89dde217d0fb}  
      Original Volume: (C:)\?\Volume{a62c8cd4-5786-11e9-a9fd-806e6f6e6963}\  
      Shadow Copy Volume: \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1  
      Originating Machine: Win7WS  
      Service Machine: Win7WS  
      Provider: 'Microsoft Software Shadow Copy provider 1.0'  
      Type: ClientAccessibleWriters  
      Attributes: Persistent, Client-accessible, No auto release, Differential,  
      Auto recovered
```

3.6 VSS - Configuration

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/VSS



HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/BackupRestore



3.5 VSS - Analysis

Analyze disk image

```
vshadowinfo -o $((512*206848)) 8d34ce.raw
```

Volume Shadow Snapshot information:

Number of stores: 1

Store: 1

Identifier	: 237c8de3-5b99-11e9-9925-080027062798
Shadow copy set ID	: 33eb3a7b-6d03-4045-aa70-37b714d49c72
Creation time	: Apr 10, 2019 14:06:30.365699200 UTC
Shadow copy ID	: 34d9910b-ac1d-4b10-b282-89dde217d0fb
Volume size	: 11 GiB (12777947136 bytes)
Attribute flags	: 0x0042000d

Mounting VSC: A 2 step approach

```
sudo vshadowmount -o $((512*206848)) 8d34ce.raw /mount/vss/
```

```
sudo ls -l /mount/vss/  
-r--r--r-- 1 root root 12777947136 Jan  1  1970 vss1
```

```
sudo file /mount/vss/vss1  
/mount/vss/vss1: DOS/MBR boot sector, code offset 0x52+2, OEM-ID "NTFS
```

```
sudo mount -o ro /mount/vss/vss1 /mnt/
```



4. Basic Malware Analysis

4.1 Introduction

Take care: Self-Infection:

- Keep away from production
- Isolated machines (VMs)
- Network considerations

Exchange of malware via email:

- Password protected archive
- Password: `infected`

5 Phases of analysis

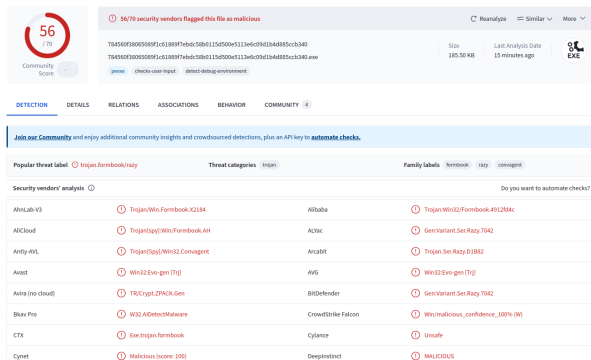
1. OSINT - Open Source Intelligence
2. Automatic Analysis (Sandbox)
3. Static Analysis
4. Dynamic Analysis (Behavioral Analysis)
5. Reverse Engineering

4.2 OSINT - IoCs

- Is the file Form.exe malicious?
- What it is doing?

```
ls -l Form.exe
md5sum Form.exe
sha1sum Form.exe
sha256sum Form.exe
```

189952 Form.exe
a8371cb187d99711691ccbecf8f35657
8dec32121d2f9f876c2b157451968796608d3dd5
784560f38065089f1c61869f7ebdc58b0115d500e5113e6c09d1b4d885ccb340



The screenshot shows the VirusShare analysis page for the file Form.exe. The file's SHA-256 hash is 784560f38065089f1c61869f7ebdc58b0115d500e5113e6c09d1b4d885ccb340. The file size is 185.50 KB, and it was last analyzed 15 minutes ago. The file is flagged as malicious by 56/70 security vendors. The file is identified as a Trojan (Trojan/Formbook.Razy). The file is also identified as a formbook, razy, and convagent. The file is also identified as a Trojan (Trojan/Formbook.Razy).

56/70 security vendors flagged this file as malicious

Reanalyze Similar More

784560f38065089f1c61869f7ebdc58b0115d500e5113e6c09d1b4d885ccb340

Size: 185.50 KB Last Analysis Date: 15 minutes ago

EXE

DESCRIPTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY

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

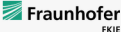

Popular threat label: Trojan/Formbook.Razy Threat categories: Trojan Family labels: formbook, razy, convagent

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win/Formbook.X2134	Alibaba	Trojan/Win32/Formbook.4512544c
AICloud	Trojan(Spy)/Win/Formbook.AH	ALYac	GenVariant.Ser.Razy.7042
Antiy-AVL	Trojan(Spy)/Win32.Convagent	Avira	Trojan.Ser.Razy.D1B82
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	TR/Crypt.ZPACK.Gen	BKDefender	GenVariant.Ser.Razy.7042
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTE	Exe.trojan.formbook	Cyline	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS


4.2 OSINT - Malpedia



Inventory Statistics Usage ApiVector Login

Quicksearch...

win. formbook [\(Back to overview\)](#)

 **Formbook**


aka: win.xloader


Actor(s): [SWEED](#), [Cobalt](#)


[VTCollection](#) [URLhaus](#) [GFI](#) [GFI](#)


FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.

References

2024-11-13 · [TEHTRIS](#) · [TEHTRIS](#)
 **Cracking Formbook malware: Blind deobfuscation and quick response techniques**
[Formbook](#)

2024-06-15 · [Medium](#) [b.magnezi](#) · [0xMrMagnezi](#)
 **Malware Analysis FormBook**
[Formbook](#)

2024-04-15 · [Positive Technologies](#) · [Aleksandr Badaev](#), [Kseniya Naumova](#)
 **SteganoAmor campaign: TA558 mass-attacking companies and public institutions all around the world**
[LokiBot](#) [404 Keylogger](#) [Agent Tesla](#) [CloudEye](#) [Formbook](#) [Remcos](#) [XWorm](#)

2024-02-28 · [Security Intelligence](#) · [Golo Muhr](#), [Ole Villadsen](#)
 **X-Force data reveals top spam trends, campaigns and senior superlatives in 2023**
[404 Keylogger](#) [Agent Tesla](#) [Black Basta](#) [DarkGate](#) [Formbook](#) [IcedID](#) [Loki Password Stealer \(PWS\)](#) [Pikabot](#) [QakBot](#) [Remcos](#)

2024-01-24 · [Medium](#) [shaddy43](#) · [Shayan Ahmed Khan](#)

4.2 OSINT - VirusTotal Details

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

Behavior Tags ⓘ

checks-user-input detect-debug-environment obfuscated

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox VMRay flags this file as: MALWARE

⚠ The sandbox C2AE flags this file as: STEALER

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN

MITRE ATT&CK Tactics and Techniques ⓘ

+ Execution TA0002

- Persistence TA0003

- 🔗 Hijack Execution Flow T1574
- 🔗 DLL Side-Loading T1574.002
 - Tries to load missing DLLs

+ Privilege Escalation TA0004

+ Defense Evasion TA0005

- Credential Access TA0006

- 🔗 Input Capture T1056
 - Creates a DirectInput object (often for capturing keystrokes)

+ Discovery TA0007

+ Collection TA0009

+ Command and Control TA0011

Malware Behavior Catalog Tree

⬆

4.2 OSINT - abuse.ch - MalwareBazaar

MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the [web upload](#) or the [API](#).



504

Submissions (past 24 hours)



Mirai

Most seen malware family (past 24 hours)



843'371

Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

Browse Database

Search

Search Syntax ?

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2023-03-29 13:07	784560f38065089f1c61...	exe	Formbook	EXE FormBook	Anonymous	

Showing 1 to 1 of 1 entries

Previous 1 Next

4.2 OSINT - MISPPriv

Tags	type:OSINT lip:white MALWARE
Date	2023-03-29
Threat Level	Medium
Analysis	Ongoing
Distribution	All communities
Published	Yes 2023-03-30 03:34:10
#Attributes	4006 (417 Objects)
First recorded change	2023-03-29 00:05:26
Last change	2023-03-30 00:03:02
Modification map	
Sightings	506 (0)
Activity	
Correlation	Enabled (disable)

—Photos —Galaxy +Event graph +Event timeline +Correlation graph +Galaxy matrix +Event reports —Attributes —Discussion

X 154060: MalwareBa...

Galaxies

< previous next > [view all](#)

+/-	[] [x]	[] [x]	Scope toggle ▾	Deleted	Decay score	Context	Related Tags	Filtering tool (1)	Expand all Objects	Collapse all Attributes	a8371cb187d99711691tcbeef8f35657				
	Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Action
	2023-03-29	ae9...06e		Object name: file :: References: 0	mids - mids <div>a8371cb187d99711691tcbeef8f35657</div> <div>A Hide the Attribute</div>			Malware payload (Formbook)		Inherit					
<input type="checkbox"/>	2023-03-29	700...2fc	Payload delivery	mids:	a8371cb187d99711691tcbeef8f35657 mids			Malware payload (Formbook)		119	Inherit			(0/0)	

4.3 Sandbox - Joe

JOESandboxCloud **BASIC**

Search (Hash, ID, Tag) ...

Analyze

Results

Deep Malware Analysis

1 Choose Analysis Architecture

Windows

macOS

Android

Linux

Advanced

2 Define Sample Source and Choose Analysis System

Upload Sample

Add more files

Clear files

Form.exe selected

Make sure to use the original sample name.
Do not rename samples!

Browse URL

More Options

Download & Execute File

Command Line

Choose Analysis System

Select up to 3 of 3 available systems.

w10x64

10x w10x64

Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01

3 Live Interaction & Results

4.3 Sandbox - Joe

JOESandboxCloud

BASIC

Overview

Signatures

Process Tree

Domains / IPs

Dropped

Static

Network

Stats

Behavior

Disassembly

Windows Analysis Report

Create Interactive Tour

Form.exe

Overview

General Information

Detection

Signatures

Classification

Process Tree

Sample name:

Form.exe

Analysis ID:

1569184

MD5:

a8371cb187d9971...

SHA1:

8dec32121d29987...

SHA256:

784560f38065089f...

Info:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

FormBook

Score:

80

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus / Scanner detection for submitted sa...

Malicious sample detected (through commun...

Multi AV Scanner detection for submitted file

Yara detected FormBook

AI detected suspicious sample

Machine Learning detection for sample

AV process strings found (often used to termin...

Checks if the current process is being debugged

Contains functionality for execution timing, ofte...

Contains functionality to access loader functio...

Detected potential crypto function

One or more processes crash

PE file does not import any functions

Classification

Process Tree

System is w10x64

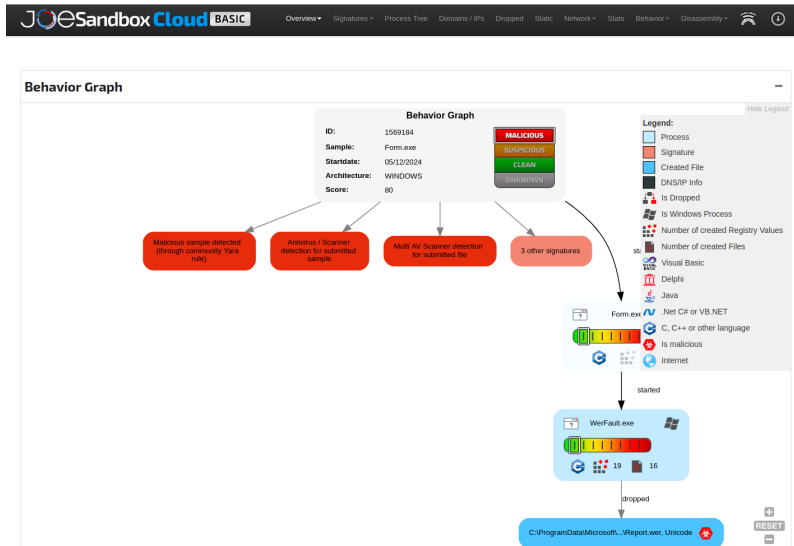
Form.exe (PID: 3680 cmdline: "C:\Users\user\Desktop\Form.exe" MD5: A8371CB187D99711691CCBEFC8F3657)

WerFault.exe (PID: 6776 cmdline: "C:\Windows\SysWOW64\WerFault.exe -u -p 3680 -s 228 MD5: C31336C1EFC2CCB44B4326EA793040F2)

cleanup

71 of 120

4.3 Sandbox - Joe



4.3 Sandbox - Cuckoo3

cert-ee / cuckoo3

Q Type to search

+ -

> Code

Issues 73

Pull requests 1

Discussions

Actions

Projects 1

Security

Insights

cuckoo3 Public

Watch 26

Fork 84

Star 647

main

1 Branch

1 Tag

Q Go to file

Add file

<> Code

cert-ee-raider Merge pull request #170 from cert-ee/feat/template_fix 6409a8b · 3 months ago 891 Commits

.github	fix: Fixed template location	3 months ago
INSTALL	docs: Quickstart	3 months ago
common	Add ids_flag and timestamp to Misp processing, search usi...	10 months ago
core	chore: Changed default configuration values to match new ...	3 months ago
devtools	Add devtool to generate and update cwd migration txt files	3 years ago
docs	docs: Fixed errors and phrasing in web-ui configuration	3 months ago
docsrc/rlrc	Merge branch 'mkdocs' into delivery	3 years ago
machineries	Support Python 3.10	last year
node	Support Python 3.10	last year
processing	Add ids_flag and timestamp to Misp processing, search usi...	10 months ago
web	Bump braces from 3.0.2 to 3.0.3 in /web/cuckoo/web/clientsrc	6 months ago
.gitignore	update for release	3 years ago
CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md	3 months ago
CONTRIBUTING.md	Create CONTRIBUTING.md	3 months ago
LICENSE	update for release	3 years ago
README.md	docs: Quickstart	3 months ago

Install sh

Not marked remove because remove removed from main

last user

About

Cuckoo3 is a Python 3 open source automated malware analysis system.

[cuckoo-hatch.cert.ee](#)

- Readme
- EUPL-1.2 license
- Code of conduct
- Activity
- Custom properties
- 647 stars
- 26 watching
- 84 forks
- Report repository

Releases

1 tags

Packages

No packages published

Contributors 8

Languages

4.4 Static Analysis

- Malware delivery: Email
 - Office documents
 - PDF
 - .EXE
 - Analyze:
 - Hash values
 - Strings
 - Resources
 - Imported functions
 - Exported functions
 - Certificate
 -
- Capabilities of the malware

4.4 Static Analysis - Strings

```
pestr -n 7 Form.exe | less
```

```
!This program cannot be run in DOS mode.  
<Ar5<zw1<Zv  
EThis program cannot be run in DOS mode.  
:Yf/yZjP  
[]sk/Jo  
X|e^BZ8  
Rh%';,V
```

```
pescan Form.exe
```

file entropy:	7.322160 (probably packed)
fpu anti-disassembly:	no
imagebase:	normal
entrypoint:	normal
DOS stub:	normal
TLS directory:	not found
timestamp:	normal
section count:	1 (low)

```
pesec Form.exe
```

ASLR:	yes
DEP/NX:	yes
SEH:	yes
Stack cookies (EXPERIMENTAL):	yes

4.4 Static Analysis - PE - Portable Execution format

- Describe program files
- Contain:
 - Meta data
 - Instructions
 - Text data
 - Resources: Pictures and alike
- Tell Windows how to load a program
- Provide resources to running program
- Provide resources like code signature

- | |
|---|
| 1. DOS Header |
| 2. PE Header |
| 3. OPTional Header |
| 4. Section Headers |
| 5. .text Section (Program Code) |
| 6. .idata Section (Importd Libs) |
| 7. .rsrc Section (Strings, Images, ...) |
| 8. .reloc Section (Memory Translation) |

4.4 Static Analysis - PE - Basic Analysis

file Form.exe

Form.exe: PE32 executable (GUI) Intel 80386, for MS Windows

exiftool Form.exe

File Name	: Form.exe
File Size	: 186 KiB
.....	
File Type	: Win32 EXE
File Type Extension	: exe
MIME Type	: application/octet-stream
Machine Type	: Intel 386 or later, and compatibles
Time Stamp	: 2000:07:31 02:00:25+02:00
Image File Characteristics	: Executable, 32-bit
PE Type	: PE32
Linker Version	: 11.0
Code Size	: 185856
Initialized Data Size	: 0
Uninitialized Data Size	: 0
Entry Point	: 0x12e0
OS Version	: 6.0
Image Version	: 0.0
Subsystem Version	: 6.0
Subsystem	: Windows GUI
Warning	: Error processing PE data dictionary

4.4 Static Analysis - PE - Basic Analysis

file Quotation.exe

Quotation.exe: PE32 executable (GUI) Intel 80386, for MS Windows

exiftool Quotation.exe

```
...
Machine Type           : Intel 386 or later, and compatibles
Time Stamp             : 2005:08:14 14:47:46+02:00
PE Type               : PE32
Linker Version         : 6.0
Code Size              : 647168
Initialized Data Size  : 32768
Uninitialized Data Size : 0
Entry Point            : 0x15f4
OS Version             : 4.0
Character Set          : Unicode
Comments              : Natcher
Company Name           : Glucosazone
Legal Copyright        : CRUSTER3
Legal Trademarks       : Forearming
Product Name           : UNKLE
File Version           : 1.02.0009
Product Version        : 1.02.0009
Internal Name          : Aurous
Original File Name     : Aurous.exe
```

4.4 Static Analysis - PE - Header

readpe -H Form.exe

DOS Header

Magic number:	0x5a4d (MZ)
Bytes in last page:	144
Pages in file:	3
.....	

Optional/Image header

Magic number:	0x10b (PE32)
Linker major version:	11
Linker minor version:	0
Size of .text section:	0x2d600
Size of .data section:	0
Size of .bss section:	0
Entrypoint:	0x12e0
Address of .text section:	0x1000
Address of .data section:	0x2f000
ImageBase:	0x400000
Alignment of sections:	0x1000
Alignment factor:	0x200
.....	
Size of image:	0x2f000
Size of headers:	0x200
Checksum:	0
Subsystem required:	0x2 (IMAGE_SUBSYSTEM_WINDOWS_GUI)
DLL characteristics:	0x8140
.....	

4.4 Static Analysis - PE - Imported Functions

```
readpe -i ../1.exe
```

Library

Name:

COMCTL32.dll

Functions

Name:

ImageList_GetDragImage

Name:

ImageList_Merge

Name:

ImageList_SetOverlayImage

Name:

UninitializeFlatSB

Name:

ImageList_DragEnter

Library

Name:

OLEAUT32.dll

Functions

Function

Ordinal:

294

Library

Name:

ADVAPI32.dll

Functions

Name:

RegOpenKeyExA

Name:

MapGenericMask

Name:

AdjustTokenGroups

Name:

SetSecurityDescriptorDacl

Name:

GetSecurityDescriptorLength

Name:

StartServiceA

Name:

OpenServiceA

Library

Name:

MSVCRT.dll

Functions

Name:

_mbssnpn

4.4 Static Analysis - PE - Resources

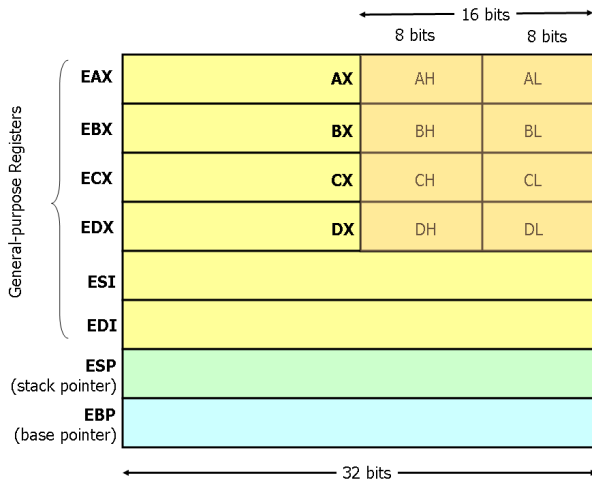
wrestool -l ../1.exe

```
—type=3 —name=23166 —language=2064 [type=icon offset=0x398cd8 size=455]
—type=3 —name=23167 —language=2064 [type=icon offset=0x398e78 size=648]
—type=3 —name=23168 —language=2064 [type=icon offset=0x398f78 size=642]
—type=3 —name=23169 —language=2064 [type=icon offset=0x399118 size=671]
—type=3 —name=23170 —language=2064 [type=icon offset=0x399358 size=1152]
—type=3 —name=23171 —language=2064 [type=icon offset=0x3995d8 size=1401]
—type=3 —name=23172 —language=2064 [type=icon offset=0x399a18 size=739]
—type=5 —name=34145 —language=2064 [type=dialog offset=0x398740 size=426]
—type=5 —name=34146 —language=2064 [type=dialog offset=0x3988f0 size=382]
—type=5 —name=34147 —language=2064 [type=dialog offset=0x398a70 size=562]
—type=9 —name=44061 —language=2064 [type=accelerator offset=0x3986e8 size=88]
—type=0 —name=5676 —language=2064 [offset=0x398ca8 size=11]
—type=0 —name=5677 —language=2064 [offset=0x398cb8 size=30]
—type=0 —name=5678 —language=2064 [offset=0x399c58 size=219344]
—type=0 —name=5679 —language=2064 [offset=0x3cf528 size=3852]
—type=14 —name=63607 —language=2064 [type=group_icon offset=0x398e60 size=20]
—type=14 —name=63608 —language=2064 [type=group_icon offset=0x398f60 size=20]
—type=14 —name=63609 —language=2064 [type=group_icon offset=0x399100 size=20]
—type=14 —name=63610 —language=2064 [type=group_icon offset=0x399340 size=20]
—type=14 —name=63611 —language=2064 [type=group_icon offset=0x3995c0 size=20]
—type=14 —name=63612 —language=2064 [type=group_icon offset=0x399a00 size=20]
—type=14 —name=63613 —language=2064 [type=group_icon offset=0x399c40 size=20]
```

4.4 Static Analysis - Considerations

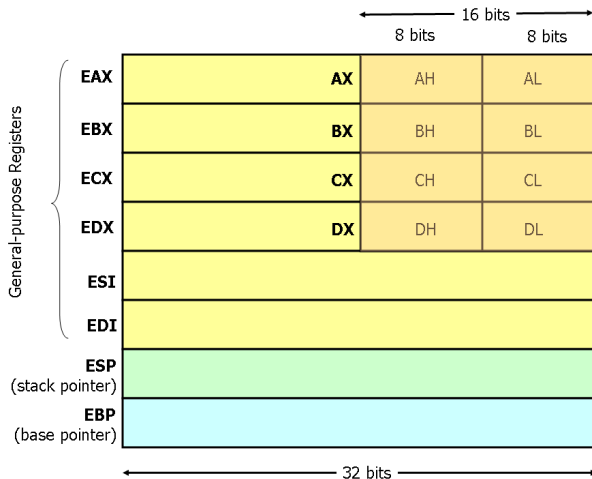
- Perfect disassembly → Unsolved problem
- Linear disassembly
 - Identify the program code
 - Decode the bytes
- Linear disassembly limitations
 - Don't know how instructions get decoded by CPU
 - Could not counter fight obfuscation
- Obfuscation techniques
 - Packing
 - Resource Obfuscation
 - Anti-Disassembly
 - Dynamic Data Download
- Counter fight obfuscation
 - Dynamic Analysis
 - Run malware in isolated environment

4.5 x86 Assembly: General-Purpose Registers



<https://www.cs.virginia.edu/~evans/cs216/guides/x86.html>

4.5 x86 Assembly: Stack and Control Flow Registers



<https://www.cs.virginia.edu/~evans/cs216/guides/x86.html>

4.5 x86 Assembly: Instructions

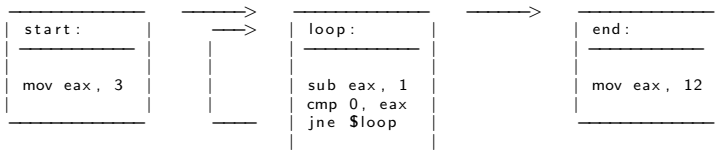
Arithmetic:	add ebx, 100	Adds 100 to the value in EBX
	sub ecx, 123	Subtract 123 from the value in ECX
	inc ah	Increments value in AH by 1
	dec al	Decrements value in AL by 1
Data Movement:	mov eax, ebx	Move value in EBX into register EAX
	mov eax, [0x4711]	Move value at memory 0x4711 into EAX
	mov eax, 1	Move the value 1 into register EAX
	mov [0x4711], eax	Move value of EAX into memory 0x4711
Stack:	push 1	Increment ESP; Store 1 on top of stack
	pop eax	Store highest value in EAX; Decrement ESP
Control Flow:	call [address]	1. Put EIP on top of the stack 2. Put [address] into EIP
	ret	1. Popped top of the stack into EIP 2. Resume execution
	jmp 0x1234	Start executing program code at 0x1234
	cmp eax, 100	1. Compares value in EAX with 100 2. Based on result set EFLAGS register
	jge 0x1234	1. Interpret EFLAGS register 2. If 'greater' or 'equal' flag then jump

4.5 x86 Assembly: Control Flow Graphs

<code>start:</code>	Symbol for address of next instruction
<code>mov eax, 3</code>	Initialize a counter of 3 into EAX
<code>loop:</code>	Symbol for address of next instruction
<code>sub eax, 1</code>	Subtract 1 from value in EAX
<code>cmp 0, eax</code>	Compare value in EAX with 0; Set EFLAGS
<code>jne \$loop</code>	IF EFLAGS 'not equal' jump to 'loop'
<code>end:</code>	Symbol for address of next instruction
<code>mov eax, 12</code>	

4.5 x86 Assembly: Control Flow Graphs

start:	Symbol for address of next instruction
mov eax, 3	Initialize a counter of 3 into EAX
loop:	Symbol for address of next instruction
sub eax, 1	Subtract 1 from value in EAX
cmp 0, eax	Compare value in EAX with 0; Set EFLAGS
jne \$loop	IF EFLAGS 'not equal' jump to 'loop'
end:	Symbol for address of next instruction
mov eax, 12	





5. Analysing files

5.1 Analysing files

- Standard Linux commands

- `file`
 - `strings`
 - `exiftool`
 - `md5sum`, `sha1sum`
 - `7z`
 -

- Dedicated tools

- `oledump.py`
 - `pdfid.py`, `pdf-parser.py`
 - VirusTotal tools
 -

- Exercise: Run `exiftool` on carving recovered documents

5.2 Analysing files

- Online resources
 - NSRL - National Software Reference Library
 - VirusTotal
 - CIRCL: DMA
 - CIRCL: MISP Threat Sharing Platform
- Demo: Search MD5
 - A479C4E7ED87AEDAFAD7D9936DC80115
 - 81e9036aed5502446654c8e5a1770935
- Analysing files could become a training on it's own

5.2 Analysing files: Outlook PST

1. Preparation :

```
sudo mount -o ro,offset=$((512*63)) nps-2008-jean.raw /media/sansforensics/casenps/  
mkdir outlook  
mkdir outlook/out
```

2. Copy .pst file

```
cp /media/sansforensics/casenps/Documents\ and\ Settings/Jean/Local\ Settings/  
Application\ Data/Microsoft/Outlook/outlook.pst outlook/.
```

3. Extract Emails

```
file outlook/outlook.pst  
outlook/outlook.pst: Microsoft Outlook email folder (<=2002)
```

```
readpst outlook/outlook.pst -o outlook/out/
```

```
cd outlook/out/  
ls  
Inbox.mbox Outbox.mbox 'Sent Items.mbox'
```

5.2 Analysing files: Outlook PST

4. Analyze Emails

```
less Sent\ Items.mbox
```

```
I've attached the information that you have requested to this email message.
```

```
.....
```

```
.....
```

```
-----Original Message-----
```

```
From: alison@m57.biz [mailto:tuckgorge@gmail.com]
```

```
Sent: Sunday, July 20, 2008 2:23 AM
```

```
To: jean@m57.biz
```

```
Subject: Please send me the information now
```

```
.....
```

```
Hi, Jean.
```

```
I'm sorry to bother you, but I really need that information now -----
```

```
.....
```

```
-----boundary-LibPST-iamunique-1836211713_-_-
```

```
filename="m57biz.xls"
```

```
less Inbox.mbox
```

```
From "tuckgorge@gmail.com" Sun Jul 20 01:22:45 2008
```

```
X-Original-To: jean@m57.biz
```

```
To: jean@m57.biz
```

```
From: tuckgorge@gmail.com (alison@m57.biz)
```



6. Live Response

6.1 Volatile Data

- Memory dump
- Live analysis:
 - System time
 - Logged-on users
 - Open files
 - Network -connections -status
 - Process information -memory
 - Process / port mapping
 - Clipboard content
 - Services
 - Command history
 - Mapped drives / shares
 - !!! Do not store information on the subject system !!!
- Image of live system (Possible issues)
- Shutdown and image if possible

6.1 Collecting Volatile Data

<https://docs.microsoft.com/en-us/sysinternals/>

- System Time

```
> date /t & time /t           # Don't forget to note wall-clock-time
Tue 03/26/2019                # Note timezone of PC
01:31 PM
```

- Loggedon Users

```
> net session

> .\PsLoggedon.exe
Users logged on locally:
      3/26/2019 1:30:23 PM      John-PC\John
No one is logged on via resource shares.

> .\logonsessions.exe
[5] Logon session 00000000:0001ad9d:
    User name:      John-PC\John
    Auth package:   NTLM
    Logon type:     Interactive
    Session:        1
    Sid:             S-1-5-21-3031575581-801213887-4188682232-1001
    Logon time:      3/26/2019 1:30:23 PM
    Logon server:    JOHN-PC
```

6.1 Collecting Volatile Data

- Open Files

```
> net file  
  
> .\psfile.exe
```

- Network Connections and Status

```
> netstat -anob
```

Proto	Local Address	Foreign Address	State	PID	RpcSs
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	696	[svchost.exe]
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING	2504	[wmpnetwk.exe]
TCP	0.0.0.0:10243	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	364	[wininit.exe]


```
> netstat -rn
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.0.2.2	10.0.2.15	10
	10.0.2.0	255.255.255.0	On-link	10.0.2.15	266
	10.0.2.15	255.255.255.255	On-link	10.0.2.15	266


```
> ipconfig /all
```


6.1 Collecting Volatile Data

- Running Processes

> tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System	4	Services	0	600 K
smss.exe	252	Services	0	792 K
csrss.exe	328	Services	0	3,224 K
wininit.exe	364	Services	0	3,316 K
csrss.exe	372	Console	1	4,196 K
winlogon.exe	400	Console	1	6,272 K
services.exe	460	Services	0	6,628 K
lsass.exe	468	Services	0	8,428 K
lsim.exe	476	Services	0	3,040 K
svchost.exe	584	Services	0	6,596 K
cmd.exe	3100	Console	1	2,480 K

> tasklist /svc

Image Name	PID	Services
svchost.exe	584	DcomLaunch, PlugPlay, Power
svchost.exe	696	RpcEptMapper, RpcSs
svchost.exe	792	Audiosrv, Dhcp, eventlog, HomeGroupProvider, lmhosts, wscsv
svchost.exe	844	AudioEndpointBuilder, CscService, HomeGroupListener, Netman, TrkWks, UxSms,
svchost.exe	876	EventSystem, fdPHost, FontCache, netprofm, nsi, WdiServiceHost

6.1 Collecting Volatile Data

- Running Processes

```
> .\pslist.exe -x
```

```
> .\pslist.exe -t
```

Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
explorer	1252	8	26	912	212044	47672	36304
VBoxTray	360	8	12	153	61384	5624	1476
cmd	548	8	1	24	29256	2564	2628
pslist	3452	13	1	123	45908	3640	1652
WzPreloader	1244	8	6	119	109748	9064	11224
cmd	3100	8	1	20	27464	2480	1804

```
> .\Listdlls.exe
```

```
> .\handle.exe
```

- Processes/Port Mapping

```
> .\tcpvcon -n -c -a
```

```
TCP,svchost.exe,692,LISTENING,0.0.0.0,0.0.0.0
TCP,System,4,LISTENING,10.0.2.15,0.0.0.0
TCP,wmpnetwk.exe,2428,LISTENING,0.0.0.0,0.0.0.0
TCP,wininit.exe,364,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,776,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,896,LISTENING,0.0.0.0,0.0.0.0
TCP,services.exe,460,LISTENING,0.0.0.0,0.0.0.0
```

6.1 Collecting Volatile Data

- Command History

```
> doskey /history
netstat -anob
.\Listdlls.exe
.\handle.exe
.\tcpvcon -n -c -a
cls
doskey /history
```

- Processes/Port Mapping

6.2 Non Volatile Data

- Clear Pagefile at shutdown

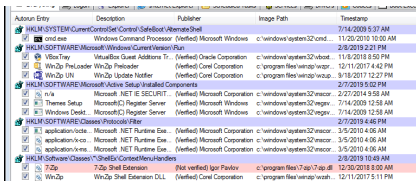
```
> reg QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management"
.....
ClearPageFileAtShutdown    REG_DWORD    0x0
.....
```

- Update Last Access disabled

```
> reg QUERY "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem"
.....
NtfsDisableLastAccessUpdate    REG_DWORD    0x0
.....
```

- Autostart locations

```
> .\Autoruns.exe
```



Autoboot Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 9:37 AM
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd...	11/20/2010 10:00 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/8/2019 2:21 PM
VBoxTray	VirtualBox Guest Addition Tr...	(Verified) Oracle Corporation	c:\windows\system32\vboad...	11/8/2018 8:50 PM
WinZip PreLoader	WinZip Preloader	(Verified) Corel Corporation	c:\program files\winzip\wzpr...	12/11/2017 4:42 PM
WinZip UN	WinZip Update Notifier	(Verified) Corel Corporation	c:\program files\winzip\wzup...	3/18/2017 12:27 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2/7/2019 5:02 PM
n/a	Microsoft .NET IE SECURIT...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	2/27/2014 9:58 AM
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr...	7/14/2009 12:58 AM
Windows Desk...	Microsoft(C) Register Server	(Verified) Microsoft Windows	c:\windows\system32\regsvr...	7/14/2009 12:58 AM
HKLM\SOFTWARE\Classes\Protocol\Filer				2/7/2019 4:46 PM
application\icm...	Microsoft .NET Runtime Exe...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
application\icm...	Microsoft .NET Runtime Exe...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
application\icm...	Microsoft .NET Runtime Exe...	(Verified) Microsoft Corporation	c:\windows\system32\mscor...	3/5/2010 4:06 AM
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2/8/2019 10:49 AM
7Zip	7Zip Shell Extension	(Not verified) Igor Pavlov	c:\program files\7zip\7zip.dl	12/30/2018 8:00 AM
WinZip	WinZip Shell Extension DLL	(Verified) Corel Corporation	c:\program files\winzip\wzsh...	12/11/2017 5:11 PM

6.3 Across the network

- Get Nmap command-line zipfile

<https://nmap.org/download.html>

- On Linux set up a netcat listener

```
nc -k -l 9999 >> logfile.txt
```

- Sending from subject system

```
ncat aaa.bbb.ccc.ddd 9999
```

```
echo "Date and Time" | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
date /t | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
time /t | ncat.exe aaa.bbb.ccc.ddd 9999
```

```
echo "_____" | ncat.exe aaa.bbb.ccc.ddd 9999
```



7. Memory Forensics

7.1 About Memory Forensics

- History
 - 2005: String search
 - → EProcess structures
- Finding EProcess structures
 - Find the doubly linked list (ntoskrnl.exe)
 - Brute Force searching
- Information expected
 - Processes (hidden)
 - Services (listening)
 - Malware
 - Network connections
 - Registry content
 - Passwords
 - Cleartext data

7.2 Capturing memory

- Prepare USB device
 - File system: ExFAT; NTFS
 - Executable capturing tool
 - No installation - Little impact as possible
 - Write capture on device
 - Administrator privileges required
- Capture memory from running system
 - Dumplt.exe
 - DumpIt.exe part of Comae-Toolkit
 - <https://www.comae.com/>
 - <https://github.com/Crypt2Shell/Comae-Toolkit/>

```
cd Z:\comae\x86\  
DumpIt.exe /OUTPUT memory_20201215_1138.bin  
-- Press y to write the memory dump into the working directory
```


7.2 Capturing memory

Service Pack: Service Pack 3
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

and are therefore time

et in order to activate

File Edit View Tools Help

Search Folders

Go

Name

- Bin2Dmp
- Comae.ps1
- ComaeRespond.ps
- dbgeng.dll
- dbghelp.dll
- Dmp2Bin
- Dmp23son
- Dumplt
- Hibr2Bin
- Hibr2Dmp
- memXPvnc202206
- memXPvnc202206.
- SwishDbgExt.dll
- symsrv.dll
- Z2Dmp

Command Prompt - .\Dumplt.exe /OUTPUT memoryXPvnc202206.bin

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\IEUser>e:

E:\>cd memory\x86\

E:\memory\x86>.\Dumplt.exe /OUTPUT memoryXPvnc202206.bin

Dumplt 3.0.20201127.1 (X86) (Nov 27 2020)
Copyright (C) 2007 - 2020, Matt Suiche (msuiche)
Copyright (C) 2016 - 2020, Comae Technologies DMCC <https://www.comae.com>
All rights reserved.

Dumplt is the best for acquisition but... our platform Stardust is also the best for analysis!
Access it on https://my.comae.com - info@comae.com if you have any questions.

Destination path:          ???E:\memory\x86\memoryXPvnc202206.bin
Computer name:             IE6WINXP

--> Proceed with the acquisition ? [y/n]
```

7.2 Capturing memory

- Hibernation file: `hiberfil.sys`
 - Created when going into hibernation mode
 - Fully fledged memory content
 - Compressed and slightly modified
 - Can be converted into raw memory dump
 - Force hibernation:

```
powercfg /h[ibernate] [on|off]  
psshutdown -h
```
- Pagefile: `pagefile.sys`
- Swapfile: `swapfile.sys` (Windows 8)
- Crash dump: `memory.dmp` (Blue Screen)

7.3 BulkExtractor Exercise

1. Preparation

```
sudo mount -o ro,offset=$((512*2048)) circl-dfir.dd /media/case1

mkdir memory
mkdir memory/out

cp /media/case1/memory/* memory
cd memory
```

2. BulkExtractor

```
bulk_extractor -o out/ DEMO-PC-20180315-160249.raw
```

3. Investigate results

```
ls -lh out/

less out/url_histogram.txt
less out/email_histogram.txt
less out/aes_keys.txt
```

7.4 Volatility Overview

Volatility 2 or Volatility 3

```
python vol.py -h | less
python vol.py -info | less
```

...	
imagecopy	Copies a physical address space out as a raw DD image
imageinfo	Identify information for the image
...	
pslist	Print all running processes by following the EPROCESS lists
psscan	Scan Physical memory for _EPROCESS pool allocations
pstree	Print process list as a tree
psxview	Find hidden processes with various process listings
...	
sockets	Print list of open sockets
sockscan	Scan Physical memory for _ADDRESS_OBJECT objects (tcp sockets)
...	

```
vol.py -f <filename> <plugin [options]> --profile=<profile>
vol.py -f memdump.raw imageinfo
```

```
sudo apt install python3-pefile
git clone https://github.com/volatilityfoundation/volatility3.git
```

7.4 Volatility Overview: Exercise

Identify profile:

```
vol.py -f DEMO-PC-20180315-160249.raw imageinfo
```

```
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (memory/DEMO-PC-20180315-160249.raw)
PAE type : No PAE
DTB : 0x185000L
KDBG : 0x82954c70L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0x82955d00L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2018-03-15 16:02:54 UTC+0000
Image local date and time : 2018-03-15 17:02:54 +0100
```

```
—> vol.py -f <filename> <plugin [options]> —profile=Win7SP1x86_23418
```

```
export VOLATILITY_PROFILE=Win7SP1x86_23418
```

```
—> vol.py -f <filename> <plugin [options]>
```

7.5 Volatility: Process Analysis

`pslist`

- Running processes
- Process IP - PID
- Parent PIP - PPID
- Start time

`pstree`

- Like `pslist`
- Visual child-parent relation

`psscan`

- Brute Force
- Find inactive and/or hidden processes

`psxview`

- Run and compare some tests
- Correlate `psscan` and `pslist`

7.5 Volatility: Process Analysis

```
volatility —profile=Win7SP1x86 -f Win-Enc-20190415.raw pslist > pslist.txt
```

Offset (V)	Name	PID	PPID	Thds	Hnds	Ses	Wow64	Start
0x84233af0	System	4	0	70	505	—	0	2019-04-15 15:02:52 UTC+0000
0x848d8288	smss.exe	248	4	2	29	—	0	2019-04-15 15:02:52 UTC+0000
0x8487a700	csrss.exe	324	308	9	384	0	0	2019-04-15 15:02:54 UTC+0000
0x84fbb530	csrss.exe	360	352	7	274	1	0	2019-04-15 15:02:54 UTC+0000
0x84fc3530	wininit.exe	368	308	3	77	0	0	2019-04-15 15:02:54 UTC+0000
0x84fd0530	winlogon.exe	396	352	4	112	1	0	2019-04-15 15:02:54 UTC+0000
0x85048a18	services.exe	456	368	8	203	0	0	2019-04-15 15:02:55 UTC+0000
0x8505ac00	lsass.exe	464	368	7	580	0	0	2019-04-15 15:02:55 UTC+0000
0x8505caa0	lsmd.exe	472	368	10	145	0	0	2019-04-15 15:02:55 UTC+0000
...								
...								
...								
0x85050b60	WmiPrvSE.exe	3268	564	9	175	0	0	2019-04-15 15:06:52 UTC+0000
0x8438bd40	owxxb-a.exe	3432	3368	15	471	1	0	2019-04-15 15:07:13 UTC+0000
0x84394030	VSSVC.exe	3676	456	6	123	0	0	2019-04-15 15:07:22 UTC+0000
0x84394488	svchost.exe	3728	456	6	70	0	0	2019-04-15 15:07:23 UTC+0000
0x84a243c8	notepad.exe	3820	3432	1	64	1	0	2019-04-15 15:08:05 UTC+0000
0x846d8030	iexplore.exe	3832	3432	19	427	1	0	2019-04-15 15:08:06 UTC+0000
0x846d2d40	iexplore.exe	3908	3832	11	293	1	0	2019-04-15 15:08:07 UTC+0000
0x846e5a58	dllhost.exe	3928	564	6	94	1	0	2019-04-15 15:08:07 UTC+0000
0x84684d40	dllhost.exe	4012	564	10	212	1	0	2019-04-15 15:08:08 UTC+0000

7.5 Volatility: Process Analysis

volatility —profile=Win7SP1x86 -f Win-Enc-20190415.raw psxview > psxview

Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd
.....									
0x3f60f030	taskhost.exe	352	True	True	True	True	True	True	True
0x3fa84d40	dllhost.exe	4012	True	True	True	True	True	True	True
0x3ec23148	spoolsv.exe	1296	True	True	True	True	True	True	True
0x3f63f470	explorer.exe	920	True	True	True	True	True	True	True
0x3ff0bd40	owxxb-a.exe	3432	True	True	True	True	True	True	True
0x3f3d0530	winlogon.exe	396	True	True	True	True	True	True	True
0x3f3c3530	wininit.exe	368	True	True	True	True	True	True	True
0x3ec9f030	svchost.exe	688	True	True	True	True	True	True	True
0x3ef3d758	VBoxTray.exe	1832	True	True	True	True	True	True	True
0x3fae5a58	dllhost.exe	3928	True	True	True	True	True	True	True
0x3ec50b60	WmiPrivSE.exe	3268	True	True	True	True	True	True	True
0x3ec88b90	svchost.exe	564	True	True	True	True	True	True	True
0x3ecd3768	svchost.exe	820	True	True	True	True	True	True	True
0x3ef4f030	SearchIndexer.	2008	True	True	True	True	True	True	True
0x3ec08d40	svchost.exe	1444	True	True	True	True	True	True	True
0x3ed10d40	svchost.exe	1008	True	True	True	True	True	True	True
0x3f6243c8	notepad.exe	3820	True	True	True	True	True	True	True
0x3ecd95f8	svchost.exe	852	True	True	True	True	True	True	True
0x3fad2d40	ieexplore.exe	3908	True	True	True	True	True	True	True
.....									
.....									

7.6 Volatility: Network Analysis

- Windows XP and 2003 Server
 - connections
 - connscan
 - sockets
- Windows 7
 - netscan

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw netscan > netscan.txt
```

Proto	Local Address	Foreign Address	State	Pid	Owner
.....					
UDPv4	0.0.0.0:0	:::		2748	powershell.exe
UDPv6	:::0	:::		2748	powershell.exe
TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	456	services.exe
TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	464	lsass.exe
TCPv6	:::49156	:::0	LISTENING	464	lsass.exe
TCPv4	10.0.2.15:49167	2.17.201.11:80	ESTABLISHED	1128	svchost.exe
TCPv4	10.0.2.15:49166	93.184.220.29:80	ESTABLISHED	1128	svchost.exe
TCPv4	10.0.2.15:49165	50.62.124.1:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49160	216.239.32.21:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49162	2.17.201.8:80	ESTABLISHED	3432	owxxb-a.exe
TCPv4	10.0.2.15:49168	13.107.21.200:80	ESTABLISHED	3832	ieexplore.exe
TCPv4	10.0.2.15:49159	94.23.7.52:80	CLOSE_WAIT	2748	powershell.exe
.....					

7.7 Volatility: Other plugins

- Other useful plugins

```
volatility -f memdump.raw sessions
volatility -f memdump.raw privs
volatility -f memdump.raw hivelist
volatility -f memdump.raw filescan
volatility -f memdump.raw timeline
volatility -f memdump.raw hashdump
```

- Get SIDs

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw getsids
```

```
powershell.exe (2748): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
owxxb-a.exe (3432): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
notepad.exe (3820): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
iexplore.exe (3832): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
iexplore.exe (3908): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
dllhost.exe (3928): S-1-5-21-3408732720-2018246097-660081352-1000 (John)
```

7.7 Volatility: Other plugins

- Command line history

```
vol.py --profile=Win7SP1x86 -f memdump.raw cmdline
vol.py --profile=Win7SP1x86 -f memdump.raw cmdscan
vol.py --profile=Win7SP1x86 -f memdump.raw consoles
```

- Find suspicious processes

```
volatility --profile=Win7SP1x86 -f Win-Enc-20190415.raw malfind
```

```
Process: owxxb-a.exe Pid: 3432 Address: 0x400000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 134, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
0x00400000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x00400010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x00400020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00400030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00  .....
```

```
0x00400000  4d          DEC EBP
0x00400001  5a          POP EDX
0x00400002  90          NOP
```

7.8 Volatility Exercise

```
python volatility3/vol.py -q --help | less
mkdir out2
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.pslist >out2/pslist
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.pstree >out2/pstree
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.psscan >out2/psscan
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.psxview >out2/psxvie
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.netscan.NetScan >out2/netscan
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.dumpfiles.DumpFiles >out2/dumpfiles
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.filescan.FileScan >out2/filescan
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw timeliner > out2/timeliner
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.registry.hivelist >out2/hivelist
```

```
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.consoles.Consoles >out2/consoles
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.cmdline.CmdLine >out2/cmdline
python volatility3/vol.py -q -f ./DEMO-PC-20180315-160249.raw windows.cmdline.CmdScan >out2/cmdscan
```



8. Bibliography and Outlook

8.1 Bibliography

- Windows Forensic Analysis 2E
Harlan Carvey
Syngress 2nd edition
ISBN-13: 978-1-59-749422-9
- Windows Forensics
Dr. Philip Polstra
CreateSpace Independent Publishing
ASIN: B01K3RPWIY
- Windows Forensic Analysis for Windows 7 3E
Harlan Carvey
Syngress
ISBN-13: 978-1-59-749727-5

8.2 Outlook

- Scheduled Tasks
- Windows 8 analyzis
- Windows 10 analyzis
- Internet artifacts
- Mobile Forensics

Overview

1. Windows Registry
2. Event Logs
3. Other Sources of Information
4. Malware Analysis
5. Analysing files
6. Live Response
7. Memory Forensics
8. Bibliography and Outlook