

# Hunting Malware with Timelines



Mari DeGrazia

@maridegrazia

[az4n6.blogspot.com](http://az4n6.blogspot.com)

[Github.com/mdegrazia](https://github.com/mdegrazia)

# Hunting for Malware

- Suspect Files Created
- File Execution
- Persistence Mechanisms
- User Activity
- IIV

# Why Timelines

- Combine artifacts
- Normalize timestamps
- Reporting

Filesystem

Registry

Eventlogs

# Approach



# Roadmap

- How to create a timeline
- How to look through the timeline
- Ways to scale

# Timeline Format














- TLN

Time | Source | Host | User | Description

# Sniper Steps

- Create Bodyfile of filesystem
  - MD5|name|inode|mode\_as\_string|UID|GID|size|  
atime|mtime|ctime|ctime
- Convert to TLN format
- Add Artifacts in TLN format
- Finalize Timeline

# Filesystem

Name	Date modified	Date created	Size
 TC DFA62.tmp	4/12/2016 7:14 AM	4/12/2016 7:14 AM	
 TC DFAC3.tmp	4/12/2016 7:14 AM	4/12/2016 7:14 AM	
 TC DFAD4.tmp	4/12/2016 7:14 AM	4/12/2016 7:14 AM	
 TC DFAF8.tmp	4/12/2016 9:02 AM	4/12/2016 9:02 AM	
 TC DFB05.tmp	4/12/2016 7:14 AM	4/12/2016 7:14 AM	
 TC DFC10.tmp	4/12/2016 7:14 AM	4/12/2016 7:14 AM	
 WebInstaller	4/16/2016 9:36 AM	4/16/2016 9:36 AM	
 {1D3FC843-7426-4CB4-9316-001F1E227E1F}.png	4/11/2016 10:41 PM	4/11/2016 10:41 PM	6 KB
 {2CFC656B-2618-4817-89A9-588347DA520C} - OProcSessld.dat	5/6/2016 6:25 PM	5/6/2016 6:25 PM	0 KB
 {25FD8C31-8867-4F1D-BF8E-8B2DD42279F0}.png	4/11/2016 10:41 PM	4/11/2016 10:41 PM	6 KB
 {49E295E2-4665-437B-B2C2-3CB3CE1600A3}.png	4/11/2016 10:41 PM	4/11/2016 10:41 PM	6 KB
 {726CAC5D-BF22-4F4F-A11C-80449C4E10E6} - OProcSessld....	4/12/2016 8:51 PM	4/12/2016 8:51 PM	0 KB
 {731649E9-27D7-4DB5-A5AA-34D9F603BF4E} - OProcSessld.d...	5/6/2016 4:26 PM	5/6/2016 4:26 PM	0 KB





## mshwinhost.exe Properties



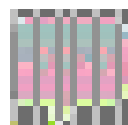
General

Compatibility

Security

Details

Previous Versions



mshwinhost.exe

Type of file: Application (.exe)

Description: mshwinhost.exe

Location: E:\Users\ITSupport\AppData\Roaming\AdobeFlash

Size: 104 KB (106,496 bytes)

Size on disk: 108 KB (110,592 bytes)

Created: Friday, April 9, 2010, 10:20:23 PM

Modified: Friday, April 9, 2010, 10:20:23 PM

Accessed: Friday, April 9, 2010, 10:20:23 PM

# Timestomping

SIA

.\mswinhost.exe

M: Sat Apr 10 05:20:23 **2010 Z**

A: Sat Apr 10 05:20:23 **2010 Z**

C: Thu Sep 10 05:20:23 2015 Z

B: Sat Apr 10 05:20:23 **2010 Z**

File Name

FN: mswinhost.exe Parent Ref: 43035 Parent Seq: 1

M: Thu Sep 10 05:20:23 **2015 Z**

A: Thu Sep 10 05:20:23 **2015 Z**

C: Thu Sep 10 05:20:23 2015 Z

B: Thu Sep 10 05:20:23 **2015 Z**

# Filesystem

- Mount Image
- Run FLS from Sleuthkit
  - `Fls.exe -m C: -f ntfs -r \\. \E: > C:\bodyfile`
- Convert to TLN Format
  - `bodyfile.exe -f bodyfile -s MDEGRAZIA-PC  
>>tmp_tln.txt`

# Filesystem

- Parse \$MFT only
- AnalyzeMFT
- MFTDump

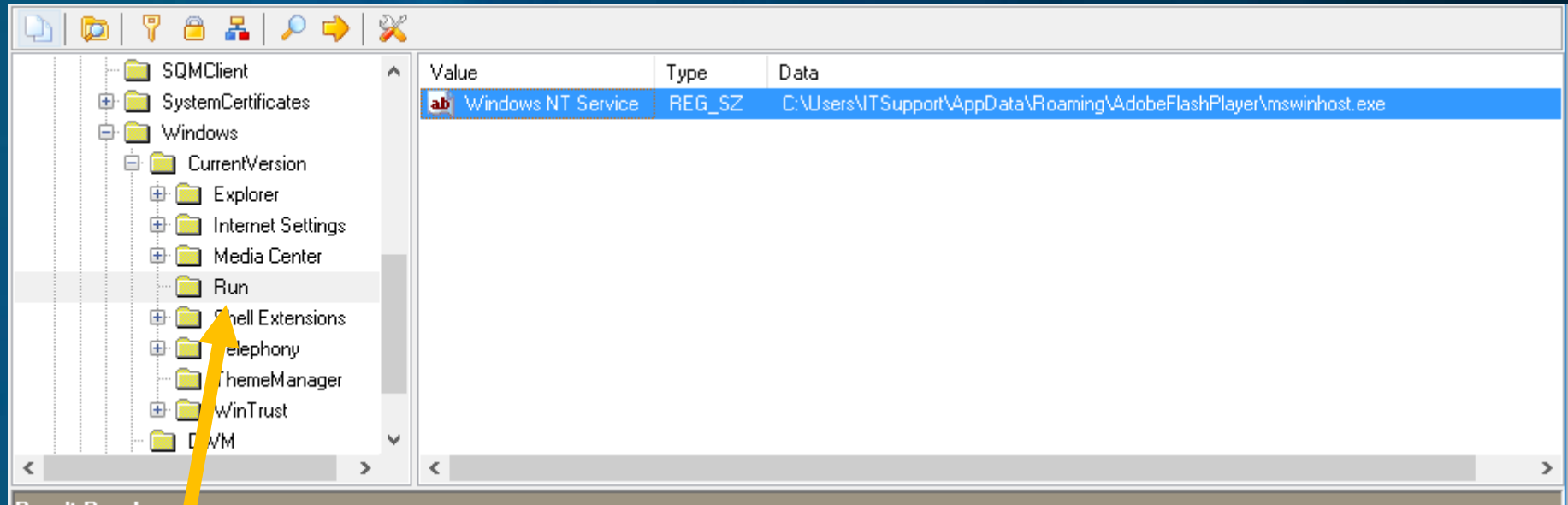
# Output

```
1441679379|FILE|DeGraziaMD-PC|MACB [90] C:/Windows/Fonts/cga80866.fon ($FILE_NAME)
1441679379|FILE|DeGraziaMD-PC|..C. [5168] C:/Windows/Fonts/cga80866.fon
1247517059|FILE|DeGraziaMD-PC|.A.B [5168] C:/Windows/Fonts/cga80866.fon
1244669150|FILE|DeGraziaMD-PC|M... [5168] C:/Windows/Fonts/cga80866.fon
1441679379|FILE|DeGraziaMD-PC|MACB [90] C:/Windows/Fonts/cga80869.fon ($FILE_NAME)
1441679379|FILE|DeGraziaMD-PC|..C. [5168] C:/Windows/Fonts/cga80869.fon
1247517059|FILE|DeGraziaMD-PC|.A.B [5168] C:/Windows/Fonts/cga80869.fon
1244669150|FILE|DeGraziaMD-PC|M... [5168] C:/Windows/Fonts/cga80869.fon
1441679379|FILE|DeGraziaMD-PC|MACB [90] C:/Windows/Fonts/cga80woa.fon ($FILE_NAME)
1441679379|FILE|DeGraziaMD-PC|..C. [4304] C:/Windows/Fonts/cga80woa.fon
1247517059|FILE|DeGraziaMD-PC|.A.B [4304] C:/Windows/Fonts/cga80woa.fon
1244669150|FILE|DeGraziaMD-PC|M... [4304] C:/Windows/Fonts/cga80woa.fon
1441679379|FILE|DeGraziaMD-PC|MACB [84] C:/Windows/Fonts/comic.ttf ($FILE_NAME)
1441679379|FILE|DeGraziaMD-PC|..C. [132832] C:/Windows/Fonts/comic.ttf
```

# Registry

- SAM
- SYSTEM
- SECURITY
- NTUSER
- USRClass

# Registry



## Keys

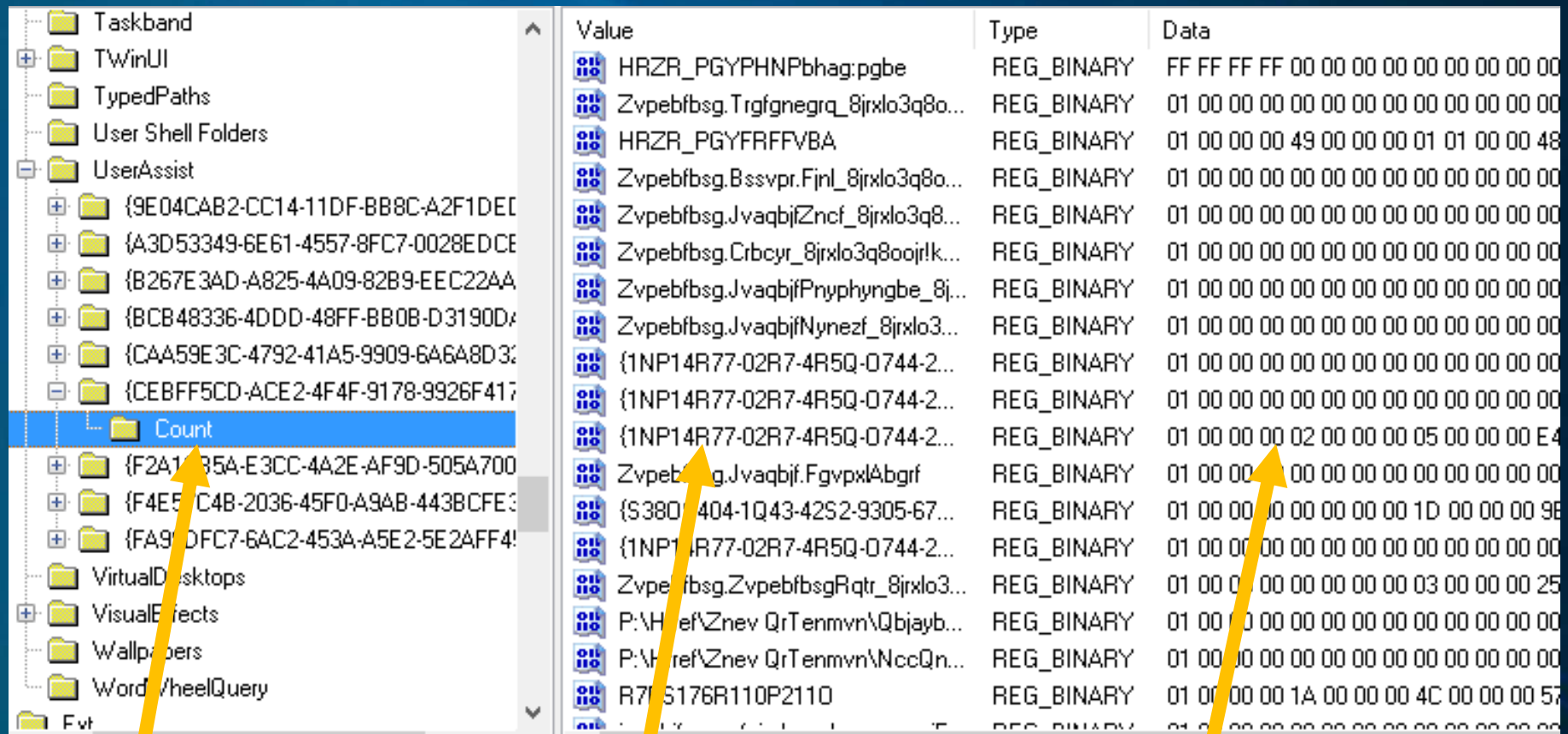
```
regtime.exe -r System -m HKLM/System -s Comp1 >>  
tmp_tln.txt
```

# Output

```
1441860078|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet002/services/SharedAccess/Epoch2
1441860077|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet001/Control/Network
1441860077|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet002/Control/Network
1441860077|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet002/services/SharedAccess/Epoch
1441860076|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet001/Enum/Root/LEGACY_SRV/0000
1441860076|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet001/services/FDResPub/ServiceData
1441860076|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet001/services/LanmanServer/Parameters
1441860076|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet002/Enum/Root/LEGACY_SRV/0000
1441860076|REG|DeGraziaMD-PC|M... HKLM/System/ControlSet002/services/FDResPub/ServiceData
```



# Registry



	Value	Type	Data
	HRZR_PGYPHNPbhag:pgbe	REG_BINARY	FF FF FF FF 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.Trqfgnegrq_8jrxlo3q8o...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	HRZR_PGYFRFFVBA	REG_BINARY	01 00 00 00 49 00 00 00 01 01 00 00 48
	Zvpebfbsg.Bssvpr.Fjnl_8jrxlo3q8o...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.JvaqbifZncf_8jrxlo3q8...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.Crbcyr_8jrxlo3q8oojrlk...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.JvaqbifPnyphyngbe_8j...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.JvaqbifNynezf_8jrxlo3...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	{1NP14R77-02R7-4R5Q-0744-2...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	{1NP14R77-02R7-4R5Q-0744-2...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	{1NP14R77-02R7-4R5Q-0744-2...	REG_BINARY	01 00 00 00 02 00 00 00 05 00 00 00 E4
	Zvpebfbsg.Jvaqbif.FgvpxlAbgrf	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	{S380-404-1Q43-42S2-9305-67...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 1D 00 00 00 9E
	{1NP14R77-02R7-4R5Q-0744-2...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	Zvpebfbsg.ZvpebfbsgRqtr_8jrxlo3...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 03 00 00 00 25
	P:\Href\Znev QrTenmvn\Qbjayb...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	P:\Href\Znev QrTenmvn\NccQn...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 00 00
	R77S176R110P2110	REG_BINARY	01 00 00 00 1A 00 00 00 4C 00 00 00 57

Keys

Values

Data

# User Assist



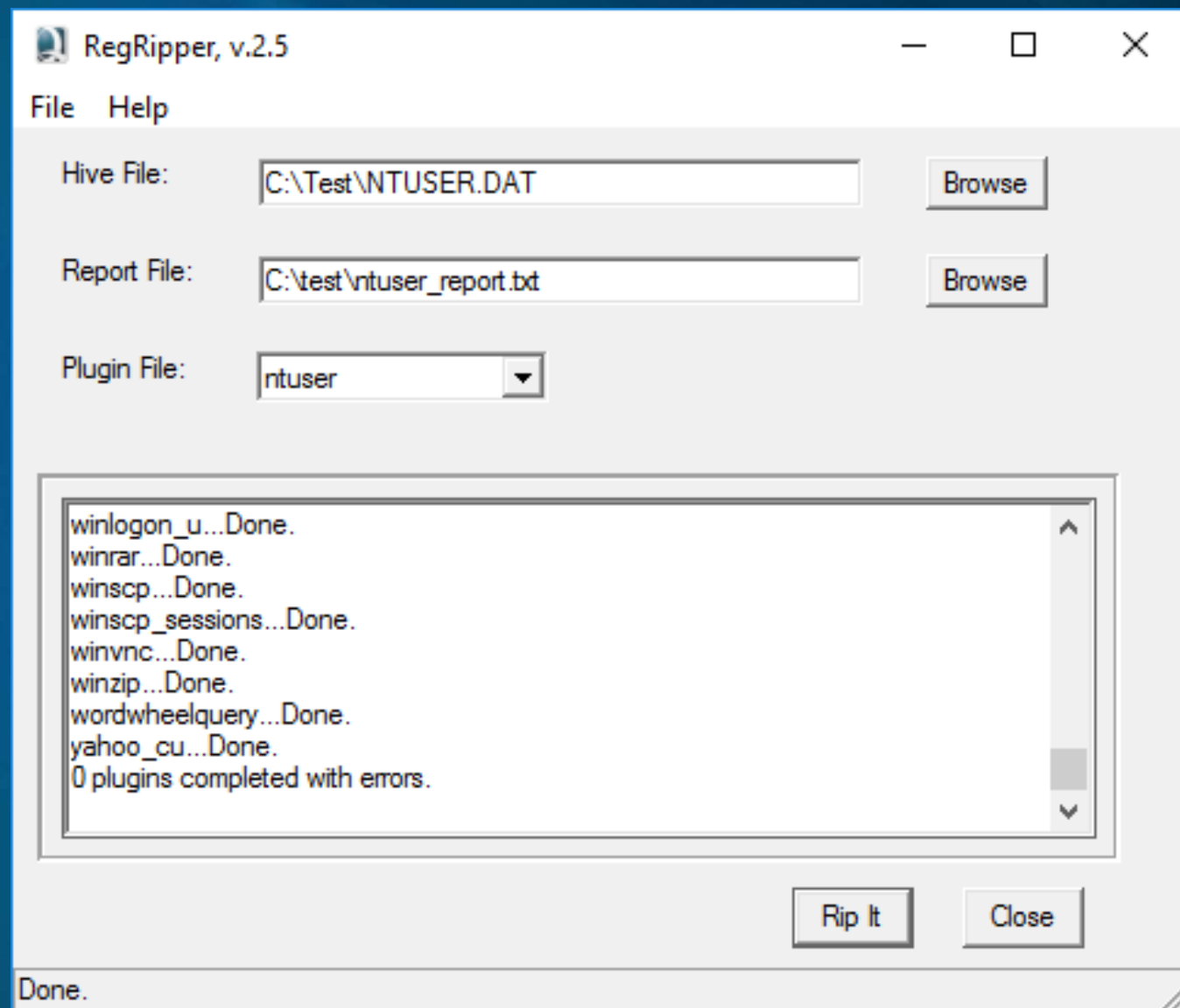
The screenshot shows the Windows Registry Editor with the path 'UserAssist' expanded. A red circle highlights the 'Count' folder. The right pane displays a list of registry values, all of type 'REG\_BINARY'. The values are organized into a table with four columns: Name, Data Type, and Data. The 'Data' column contains hexadecimal values representing the count of uses for each application.

Name	Data Type	Data
{7P5N40RS-N0S0-40SP-874N-P0S2R0...}	REG_BINARY	01 00 00 00 01 00 00 00 07 00 00 00 EC
P:\Hfref\Znev QrT enmvn\Qbjaybnqf\Nin...	REG_BINARY	01 00 00 00 01 00 00 00 01 00 00 00 BC
Puebzt	REG_BINARY	01 00 00 00 00 00 00 00 01 00 00 00 16
{7P5N40RS-N0S0-40SP-874N-P0S2R0...}	REG_BINARY	01 00 00 00 00 00 00 00 05 00 00 00 5E
P:\Hfref\Znev QrT enmvn\Qbjaybnqf\Ce...	REG_BINARY	01 00 00 00 02 00 00 00 00 00 00 00 00
P:\Hfref\Znev QrT enmvn\NccQngn\Yb...	REG_BINARY	01 00 00 00 00 00 00 00 08 00 00 00 44
P:\Hfref\Znev QrT enmvn\NccQngn\Yb...	REG_BINARY	01 00 00 00 00 00 00 00 00 00 00 00 62
P:\Hfref\Znev QrT enmvn\NccQngn\Yb...	REG_BINARY	01 00 00 00 00 00 00 00 02 00 00 00 82
{1NP14R77-02R7-4R5Q-0744-2R01NR...}	REG_BINARY	01 00 00 00 01 00 00 00 00 00 00 00 00
ninfg! nagvivehf	REG_BINARY	01 00 00 00 00 00 00 00 02 00 00 00 E4
Q:\rapnfr_rknzware_(k64)_71001.rkr	REG_BINARY	01 00 00 00 01 00 00 00 01 00 00 00 E9

5/5/2016 14:25:06 2016 Z

3

# RegRipper



# RegRipper

- `rip.exe -r NTUSER.DAT -p userassist_tln -s DeGraziaMD-PC >> tmp_tln.txt`

# Output

```
1290288590|REG|DeGraziaMD-PC||M... AppCompatCache - C:\Windows\System32\mssvp.dll
1290288559|REG|DeGraziaMD-PC||M... [Program Execution] AppCompatCache - C:\Windows\WinSxS\x86_netfx-clrg
1247534058|REG|DeGraziaMD-PC||M... [Program Execution] AppCompatCache - C:\Windows\system32\DrvInst.exe
1441862411|REG|DeGraziaMD-PC||M... [Program Execution] AppCompatCache - C:\Windows\PSEXESVC.exe
1290288548|REG|DeGraziaMD-PC||M... AppCompatCache - C:\Windows\System32\DeviceCenter.dll
```

# Event Logs

- SECURITY
- SYSTEM
- APPLICATION

# EVTX Logs

- LogParser -i:EVT -o:CSV "Select RecordNumber,TO\_UTCTIME(TimeGenerated),EventID,SourceName,ComputerName,SID,Strings FROM application.evtx" >> application.csv
- Evtxparse.exe application.csv >> tmp\_tln.txt



# Output

```
1441862695|EVTX|Server||Winlogon/4101;DegraziaMD-PC,,0x00000000,0x00000001
1441862695|EVTX|Server||Wlclntfy/6000;DegraziaMD-PC,,SessionEnv
1441862695|EVTX|Server||Software Protection Platform Service/1003;DegraziaMD-PC,,
1441862695|EVTX|Server||Desktop Window Manager/9007;DegraziaMD-PC,,
1441862725|EVTX|Server||Desktop Window Manager/9009;DegraziaMD-PC,,0x40010004
1441862725|EVTX|Server||Wlclntfy/6000;DegraziaMD-PC,,SessionEnv
```



# Finalize Timeline

- `parse.exe -f tmp_tln.txt -c >> timeline.csv`

# Batch file



- Timeline\_win7.bat H: C:\cactuscon\timeline\  
DeGraziaMD-PC

# Find Badness

- Installed Services
  - Service Control Manager/7045
- Suspect File Execution
- Recently created EXE and DLL files
- CurrentVersion/Run
- Remote Login
  - Microsoft-Windows-Security-Auditing/4624, type 3
  - Microsoft-Windows-Security-Auditing/4634, type 3
  - RDPCLIP.EXE-9067FA0E.pf

# Shotgun Approach

- `log2timeline.py /cases/timeline/myhost.plaso image.e01`
- `psort.py -o l2tcsv myhost.plaso >> myhost.csv`



# Try both – No Filename Attribute

	A	B	D	E	J
	date	time	MACE	source	short
6	4/10/2010	5:20:29	.A..	FILE	/Users/ITSupport/AppData/Roaming/AdobeFlashPlayer/mswinhost.exe
7	4/10/2010	5:20:29	...B	FILE	/Users/ITSupport/AppData/Roaming/AdobeFlashPlayer/mswinhost.exe
8	4/10/2010	5:20:29	M...	FILE	/Users/ITSupport/AppData/Roaming/AdobeFlashPlayer/mswinhost.exe
1	9/10/2015	5:20:29	..C.	FILE	/Users/ITSupport/AppData/Roaming/AdobeFlashPlayer/mswinhost.exe
6					
7					
8					

# Try both – Run Key Entry

date	time	source	type	desc
9/10/2015	5:20:34	REG	Last Written	[\\Software\\Microsoft\\Windows\\CurrentVersion\\Run] Windows NT Service: C:\\Users\\ITSupport\\AppData\\Roaming\\AdobeFlashPlayer\\mswinhost.exe

M
filename
Win7_Malware.E01:/Windows/System32/config/DEFAULT

# Resources

- Harlan's Git Hub
  - <https://github.com/keydet89>
- Autopsy
  - <http://www.sleuthkit.org/>
- FTK Imager
  - <http://accessdata.com>



# Questions?

@maridegrazia

az4n6.blogspot.com

Github.com/mdegrazia