

Finding Malware

LIKE IRON MAN

NYS SECURITY CONVERSION



Author: Corey Harrell, Office of the State Comptroller



Who Am I?

- Author "Journey Into Incident Response" blog
- Developing Malware Analysis course curriculum, Champlain College
- Masters of Science in Information Assurance (MSIA)
- Certified Ethical Hacker (CEH)
- Encase Certified Forensic Examiner (EnCE)

- DFIR 5 yrs >> InfoSec 7 yrs >> IT 10+ yrs
 - Current Work: Defender and Incident Response
 - Current Work (off hours): Exclusively Malware Infections
 - Previous Work: DFIR Support Fraud and Security Incidents
 - Previous Work: Vulnerability Assessments Against other NYS Agencies

Disclaimers

- Disclaimer #1

All opinions and rants expressed are solely my own and do not express the views or opinions of my employer

- Disclaimer #2

All content and data is my own and does not represent work I have done for my employer

- Disclaimer #3

I sell nothing; I just believe in sharing information

Finding Malware Outline

- What Is Malware
- Why Perform Malware Forensics
- Malware Forensics
 - Program Execution
 - Auto-start Locations
 - File System (NTFS) Artifacts
- Mock Case – Iron Man Style

What Is Malware?

What Is Malware?

- Different Malware Definitions
 - National Institute of Standards and Technology Definition (Mell, Kent, & Nusbaum, 2005)

“Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim”

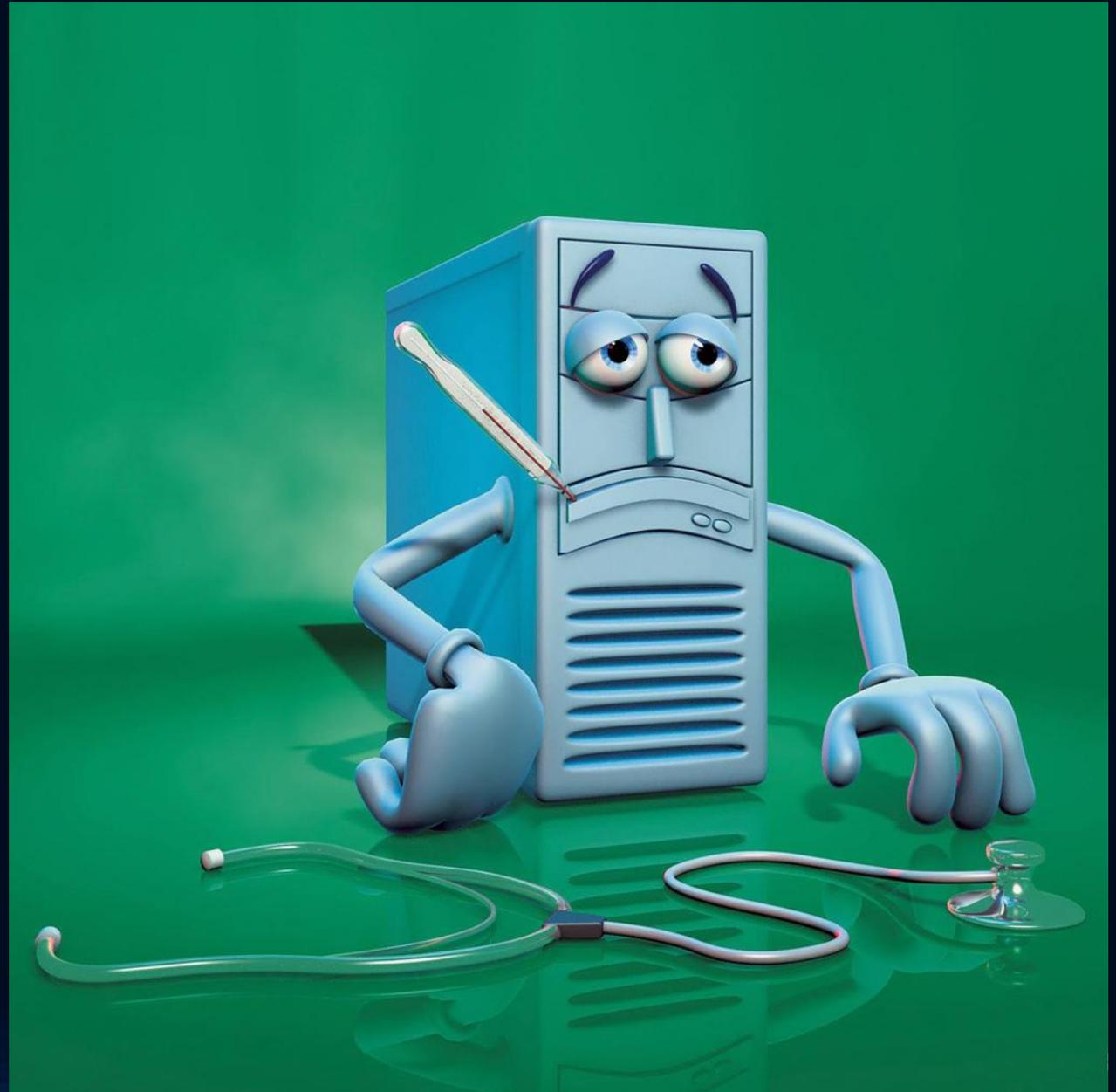
What Is Malware?

- People Don't Remember Definitions
 - They Remember Images & Words – The Wrong Images & Words
- Case in Point – Tony Stark



What Is Malware?

- It's a Sickness



What Is Malware?

- They Are Germs



What Is Malware?

- They Are Bugs



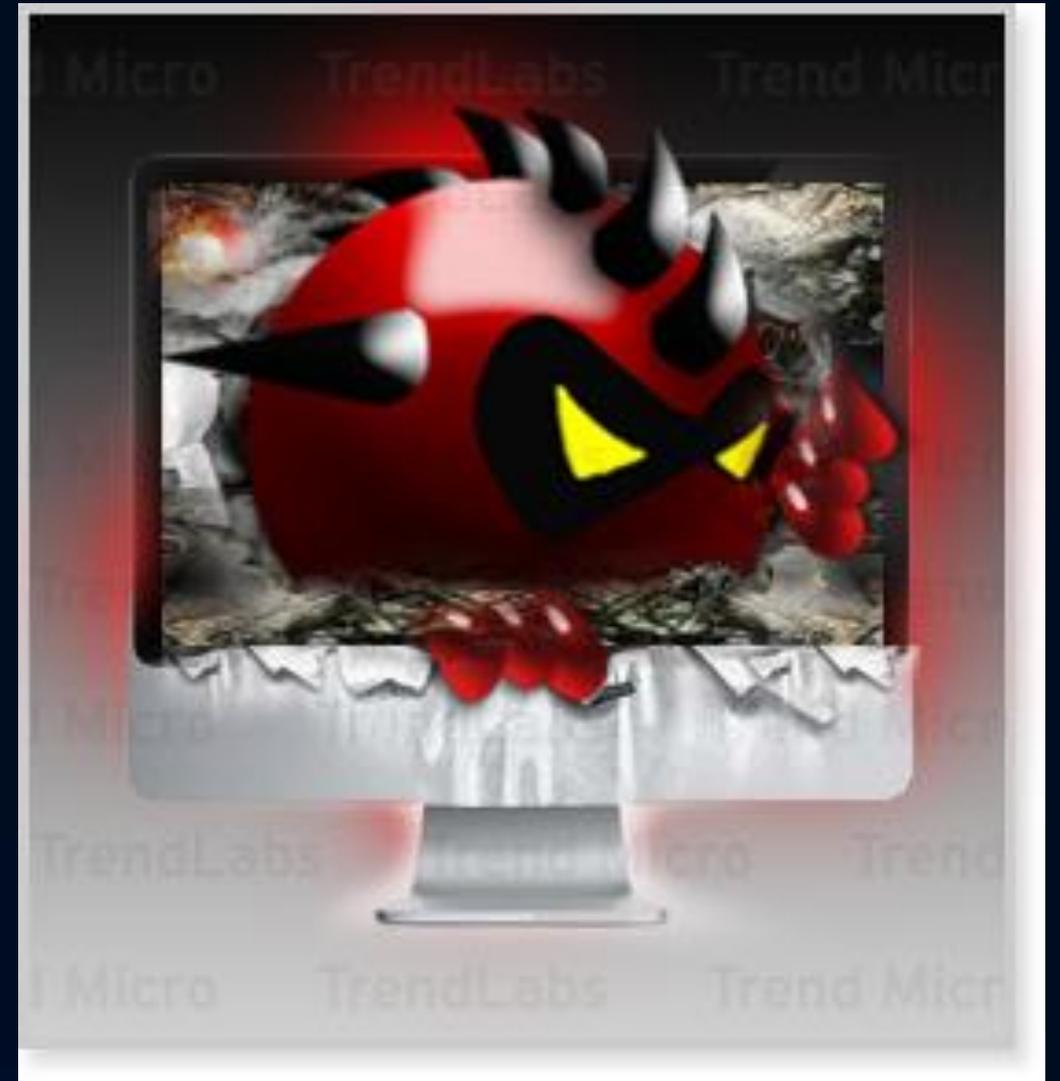
What Is Malware?

- They Are Critters



What Is Malware?

- They Are Straight Up Evil



What Is Malware?

- The old view sees malware as a:
 - Sickness
 - Nuisance
 - Disruption
 - Inconvenience
 - Critters
 - Bugs
 - Germs
 - Script kiddies
 - Straight Up Evilness

This View Directly Impacts the Response to Malware

What Is Malware?

- As Malware Wreaks Havoc Who Do People Want to Call?

Seriously, this guy?



What Is Malware?

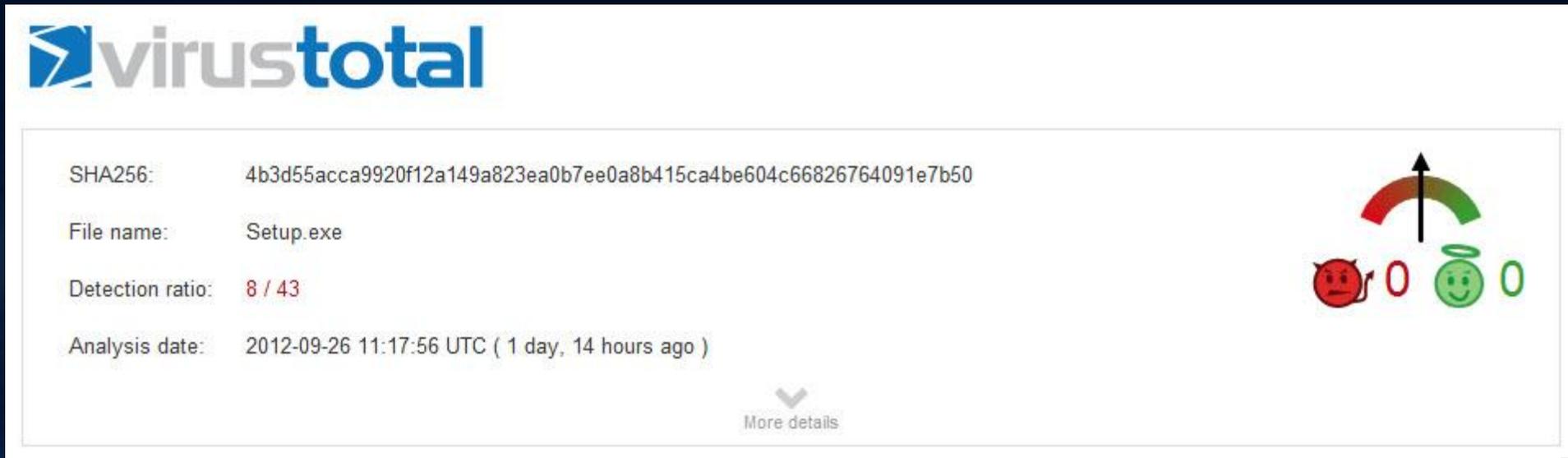
Tony Stark (aka Computer Doctor) Treatment



What Is Malware?

Tony Stark (aka Computer Doctor) Treatment

- Didn't Work Just Like in the Real World



The screenshot shows the VirusTotal interface for a file named 'Setup.exe'. The SHA256 hash is 4b3d55acca9920f12a149a823ea0b7ee0a8b415ca4be604c66826764091e7b50. The detection ratio is 8 / 43. The analysis date is 2012-09-26 11:17:56 UTC (1 day, 14 hours ago). A 'More details' link is visible at the bottom. On the right side, there is a gauge with a red-to-green gradient and an upward-pointing arrow, and two circular icons: a red devil face with horns and a green angel face with wings, each with a '0' next to it.

virustotal

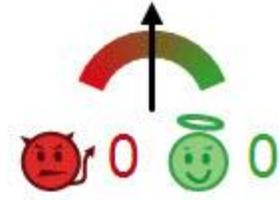
SHA256: 4b3d55acca9920f12a149a823ea0b7ee0a8b415ca4be604c66826764091e7b50

File name: Setup.exe

Detection ratio: 8 / 43

Analysis date: 2012-09-26 11:17:56 UTC (1 day, 14 hours ago)

[More details](#)



What Is Malware?

Computer Doctors' Treatment

- Treatment #1
 - Scan with one to three anti-virus programs
- Treatment #2
 - Scan with anti-virus programs <- it fails
 - Wipe computer
 - Re-image computer
 - Redeploy computer back into production

What Is Malware?

- Houston, we've had a problem?
 - The old view about malware is not accurate
- Malware is no longer a:
 - Sickness
 - Nuisance
 - Disruption
 - Product of script kiddies
 - Geeks showing their skills off to the world

Malware has evolved into something different

What Is Malware?

- Malware are now common place tools
 - Tools that serve specific purposes to accomplish certain goals



What Is Malware

- Malware serves specific purposes to accomplish certain goals
- Common malware functionality
 - Downloader / Dropper <- installs additional malware
 - Data Stealer <- steals data
 - Backdoor (Remote Access) <- provides remote access capabilities
 - Rogue Security Software <- tricks users into purchasing malware to infect themselves
 - Computer Usage <- uses computer i.e. proxies, email relays, VPNs, DDOS, etc
 - Destructive <- prevents access or destroys data i.e. encryption

Why Perform Malware Forensics

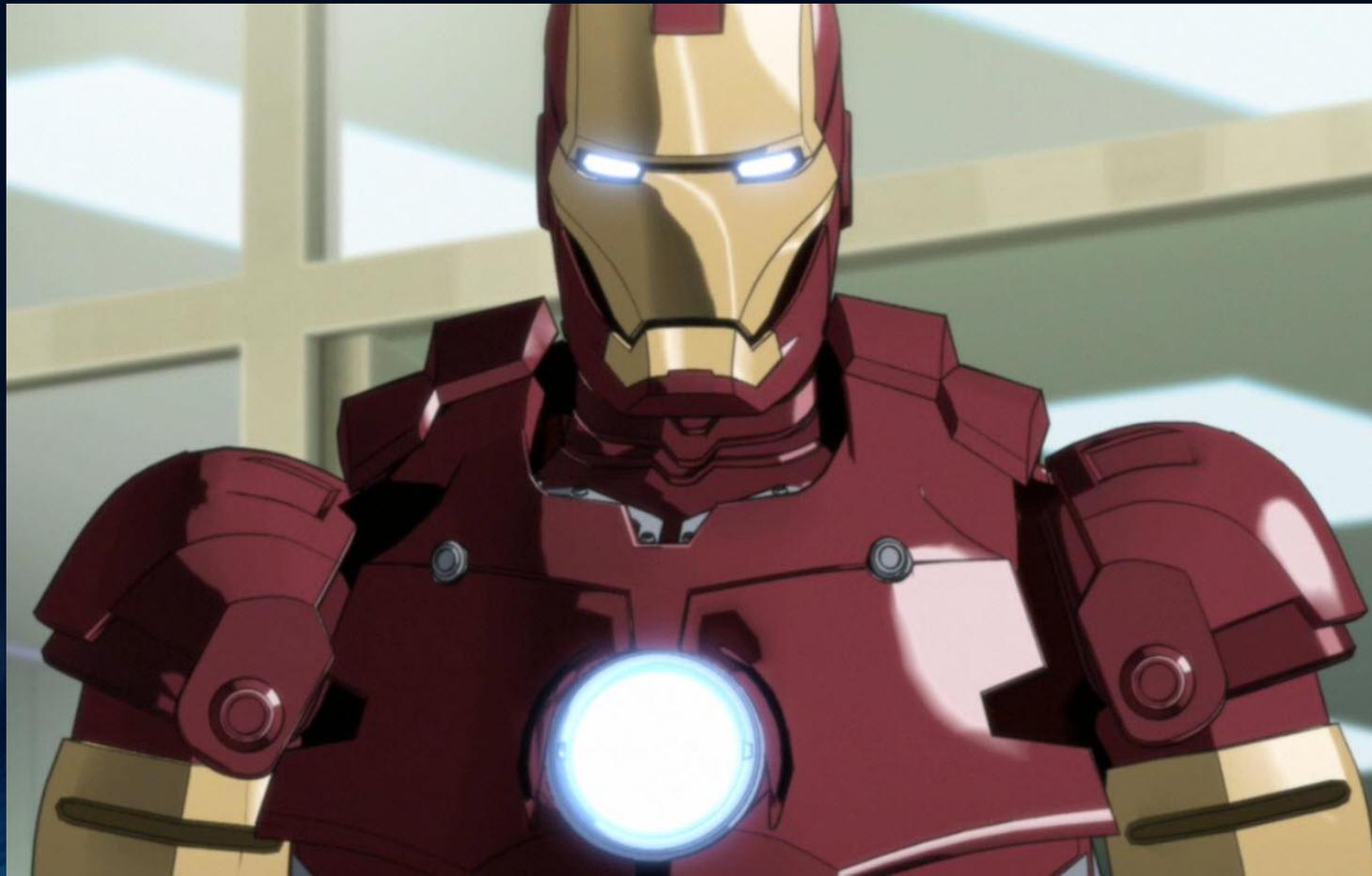
Why Perform Malware Forensics

- Malware Response Based on Old View
 - Scan with anti-virus programs
 - Wipe computer
 - Re-image computer
 - Redeploy computer back into production
- What's Missing From the Response
 - Root Cause Analysis
 - How is malware bypassing security controls?
 - Risk Mitigation (What needs to be done to reduce future infections?)
 - Risk Exposure (What was the attacker trying to do?)



Why Perform Malware Forensics

- A new Approach to Malware Response Is Needed



Why Perform Malware Forensics

- Malware has evolved so must our response
- What we need is
 - You, Me, and analysts
- What we need to do is
 - Be like Iron Man and go after the malware on our systems and networks
 - Perform root cause analysis
 - Determine how the malware bypassed our security controls
 - Reduce risks by strengthening controls to reduce future infections

Malware Forensics

Malware Forensics Examination Process

- Profile the System
- Examine the System's Volatile Data
- Examine on Disk Any Identified Files
- Conduct Scans for Known Malicious Code
- Examine the Programs Ran on the System
- Examine the Auto-start Locations
- Examine Host Based Logs for Activity of Interest
- Examine File System Artifacts

Malware Detection Steps

- Perform System Timeline Analysis

Applies to both

- Examine Web Browsing
- Examine User Profiles of Interest
- Perform Keyword Search
- Examine Suspected Malicious Files (Harrell, 2013)

Root Cause Analysis Steps

Malware Forensics Examination Process

- Profile the System
- Examine the System's Volatile Data
- Examine on Disk Any Identified Files
- Conduct Scans for Known Malicious Code
- **Examine the Programs Ran on the System**
- **Examine the Auto-start Locations**
- Examine Host Based Logs for Activity of Interest
- **Examine File System Artifacts**
- Perform System Timeline Analysis
- Examine Web Browsing
- Examine User Profiles of Interest
- Perform Keyword Search
- Examine Suspected Malicious Files (Harrell, 2013)

Malware Detection Steps

Malware Forensics Tools

Windows Prefetch Files

- WinPrefetchView
 - http://www.nirsoft.net/utils/win_prefetch_view.html

Windows Registry Hives

- RegRipper
 - <http://code.google.com/p/regripper/downloads/list>
- auto_rip
 - <http://code.google.com/p/regripper/downloads/list>

NTFS Artifacts

- AnalyzeMFT
 - <https://github.com/dkovar/analyzeMFT>
- Windows Journal Parser
 - http://tzworks.net/prototype_page.php?proto_id=5

Malware Forensics

Malware Indicators

- What to look for:
 - Programs executing from temporary or cache folders
 - Programs executing from user profiles (AppData, Roaming, Local, etc)
 - Programs executing from C:\ProgramData or All Users profile
 - Programs executing from C:\RECYLER
 - Programs stored as Alternate Data Streams (i.e. C:\Windows\System32:svchost.exe)
 - Programs with random and unusual file names
 - Windows programs located in wrong folders (i.e. C:\Windows\svchost.exe)
 - Other activity on the system around suspicious files

Malware Forensics Examination Step

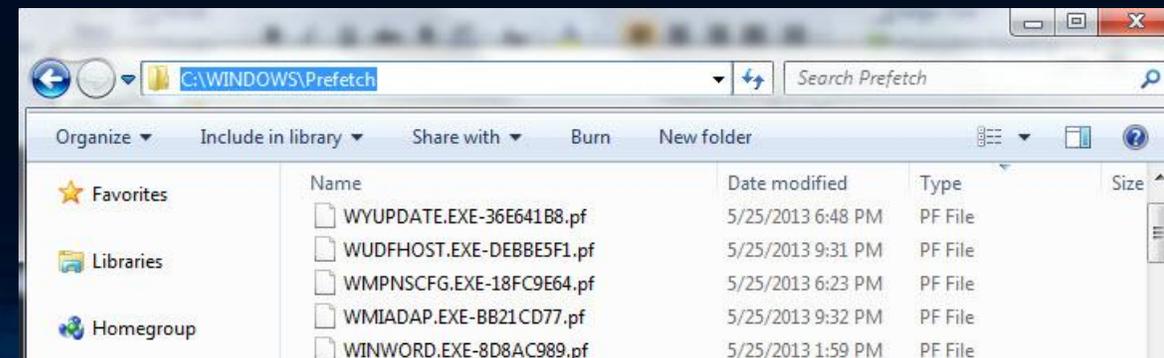
Examine the Programs Ran on the System

- Program Execution Artifacts
 - Prefetch files
 - AppCompatCache registry key
 - Legacy registry keys
 - UserAssist registry key
 - MUICache registry key

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review prefetch files
 - Windows enables prefetching to make system boots or applications startups faster
 - Prefetch files (*.pf) store data and files accessed during boot or application start-up
 - Location
 - C:\Windows\Prefetch
 - Information Provided
 - .pf file creation date generally shows when program first executed
 - .pf file last modified date shows when program last executed
 - Process's file path
 - Process's last run time
 - Process's run count
 - Files accessed during start-ups



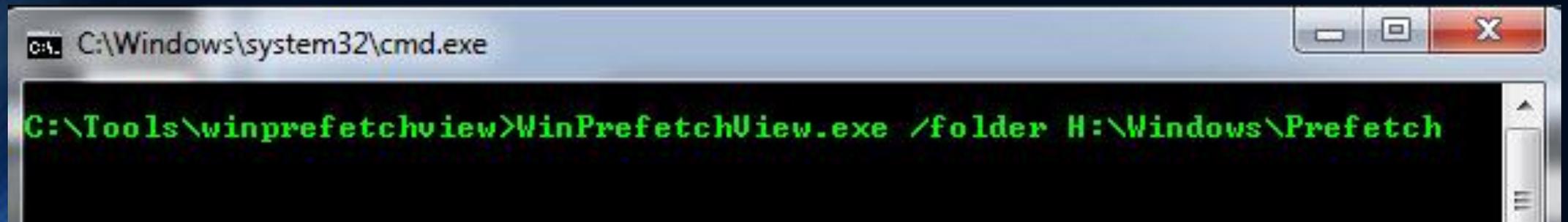
Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review prefetch files
 - Winprefetchview.exe
 - Command:

```
C:\Tools\winprefetchview>winprefetchview.exe /folder F:\Windows\Prefetch
```

- /folder switch: to parse Prefetch folder from another system

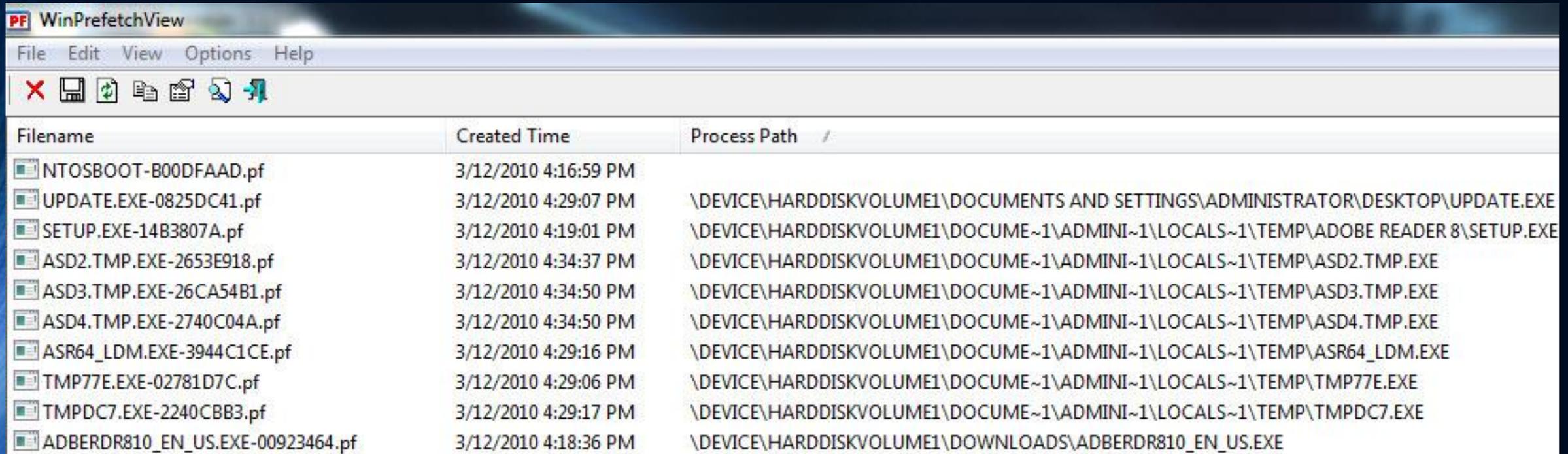


```
C:\Windows\system32\cmd.exe  
C:\Tools\winprefetchview>WinPrefetchView.exe /folder H:\Windows\Prefetch
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review prefetch files
 - Winprefetchview.exe



The screenshot shows the WinPrefetchView application window. The title bar reads 'WinPrefetchView'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. The toolbar contains icons for file operations. The main area displays a table with three columns: 'Filename', 'Created Time', and 'Process Path'.

Filename	Created Time	Process Path
NTOSBOOT-B00DFAAD.pf	3/12/2010 4:16:59 PM	
UPDATE.EXE-0825DC41.pf	3/12/2010 4:29:07 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\DESKTOP\\UPDATE.EXE
SETUP.EXE-14B3807A.pf	3/12/2010 4:19:01 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ADOBE READER 8\\SETUP.EXE
ASD2.TMP.EXE-2653E918.pf	3/12/2010 4:34:37 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ASD2.TMP.EXE
ASD3.TMP.EXE-26CA54B1.pf	3/12/2010 4:34:50 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ASD3.TMP.EXE
ASD4.TMP.EXE-2740C04A.pf	3/12/2010 4:34:50 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ASD4.TMP.EXE
ASR64_LDM.EXE-3944C1CE.pf	3/12/2010 4:29:16 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ASR64_LDM.EXE
TMP77E.EXE-02781D7C.pf	3/12/2010 4:29:06 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\TMP77E.EXE
TMPDC7.EXE-2240CBB3.pf	3/12/2010 4:29:17 PM	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\TMPDC7.EXE
ADBERDR810_EN_US.EXE-00923464.pf	3/12/2010 4:18:36 PM	\\DEVICE\\HARDDISKVOLUME1\\DOWNLOADS\\ADBERDR810_EN_US.EXE

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review AppCompatCache registry key
 - Application Compatibility Database is used by Windows to identify application compatibility issues (Davis, 2012)
 - Location
 - Varies by operating system version
 - Windows 7: HKLM\SYSTEM\CurrentControlSetoo#\Control\Session Manager\AppCompatCache\
 - Information Provided
 - Executable's last modification date
 - Executable's file path

Malware Forensics Examination Steps

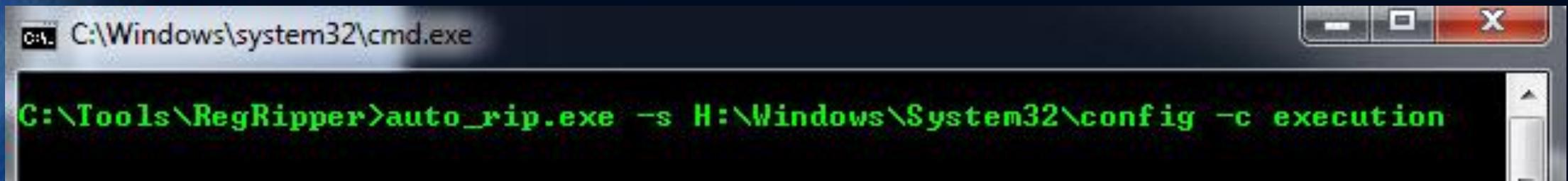
Examine the Programs Ran on the System

- Review AppCompatCache registry key
 - RegRipper (rip.exe or rip.pl)
 - Command:

```
C:\Tools\RegRipper>rip.exe -r H:\Windows\System32\config\SYSTEM -p appcompatcache
```

- r switch: specifies registry hive

-p switch: specifies plug-in

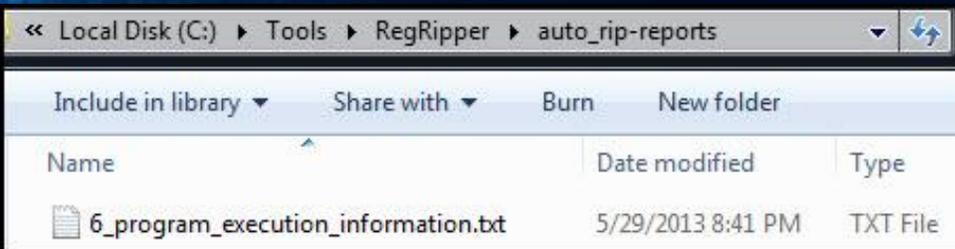
A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt displays the command 'C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -c execution' in green text on a black background. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

```
C:\Windows\system32\cmd.exe  
C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -c execution
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review AppCompatCache registry key
 - auto_rip (auto_rip.exe or auto_rip.pl)



```
appcompatcache v.20130425
(System) Parse files from system hive shim cache

Signature: 0xdeadbeef
winXP, 32-bit

ModTime: Thu Jan  1 00:00:00 1970 Z
UpdTime: Thu Jan  1 00:00:00 1970 Z
Size    : 0 bytes

C:\Documents and Settings\Administrator\Desktop\update.exe
ModTime: Fri Mar 12 16:28:25 2010 Z
UpdTime: Fri Mar 12 16:28:57 2010 Z
Size    : 20480 bytes

C:\WINDOWS\system32\blastcln.exe
ModTime: Mon Apr 14 09:42:14 2008 Z
UpdTime: Fri Mar 12 16:16:19 2010 Z
Size    : 71680 bytes

C:\WINDOWS\system32\spupdwxp.exe
ModTime: Mon Apr 14 09:42:38 2008 Z
UpdTime: Fri Mar 12 16:15:56 2010 Z
Size    : 20992 bytes
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review AppCompatCache registry key
 - auto_rip (auto_rip.exe or auto_rip.pl)

```
C:\Program Files\Java\jre1.6.0_03\bin\client\jvm.dll
ModTime: Thu Jan  1 00:00:00 1970 Z
UpdTime: Fri Mar 12 16:30:17 2010 Z
Size    : 0 bytes

C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\PDFshell.dll
ModTime: Fri May 11 03:54:08 2007 Z
UpdTime: Fri Mar 12 18:41:20 2010 Z
Size    : 372736 bytes

C:\Program Files\Dr. Guard\drguard.exe
ModTime: Fri Mar 12 16:35:10 2010 Z
UpdTime: Fri Mar 12 18:40:30 2010 Z
Size    : 2347008 bytes

C:\Program Files\Java\jre1.6.0_03\bin\javaw.exe
ModTime: Tue Sep 25 03:30:30 2007 Z
UpdTime: Fri Mar 12 16:21:19 2010 Z
Size    : 135168 bytes

C:\downloads\Memoryze\MemoryDD.bat
ModTime: Mon Jul  6 20:29:16 2009 Z
UpdTime: Fri Mar 12 16:33:59 2010 Z
Size    : 2962 bytes
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review Legacy registry keys
 - Correlates to when first time a Windows service was run (Carvey, 2011)
 - Location
 - HKLM\System\CurrentControlSetoo#\Enum\Root
 - Information Provided
 - First time service executed
 - DLL or driver's file path

Malware Forensics Examination Steps

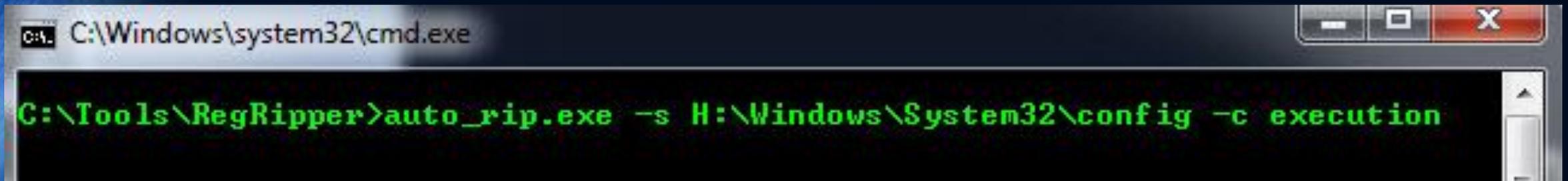
Examine the Programs Ran on the System

- Review Legacy registry keys
 - RegRipper (rip.exe or rip.pl)
 - Command:

```
C:\Tools\RegRipper>rip.exe -r H:\Windows\System32\config\SYSTEM -p legacy
```

- r switch: specifies registry hive

-p switch: specifies plug-in

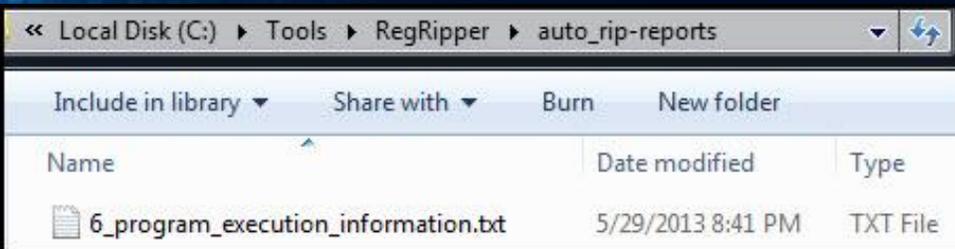
A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt displays the command 'C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -c execution' in green text on a black background. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

```
C:\Windows\system32\cmd.exe  
C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -c execution
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review Legacy registry keys
 - auto_rip (auto_rip.exe or auto_rip.pl)



```
Fri Mar 12 18:39:57 2010 (UTC)
LEGACY_AFD\0000 - AFD
LEGACY_BEEP\0000 - Beep
LEGACY_DMBOOT\0000 - dmboot
LEGACY_DMLOAD\0000 - dmload
LEGACY_FIPS\0000 - Fips
LEGACY_GPC\0000 - Generic Packet Classifier
LEGACY_HTTP\0000 - HTTP
LEGACY_IPNAT\0000 - IP Network Address Translator
LEGACY_IPSEC\0000 - IPSEC driver
LEGACY_KSECDD\0000 - ksecdd
LEGACY_MANDIANT_TOOLS\0000 - Mandiant_Tools
LEGACY_MNMDD\0000 - mnmd
LEGACY_MOUNTMGR\0000 - mountmgr
LEGACY_NDIS\0000 - NDIS System Driver
LEGACY_NDISTAPI\0000 - Remote Access NDIS TAPI Driver
LEGACY_NDISUIO\0000 - NDIS Usermode I/O Protocol
LEGACY_NDPROXY\0000 - NDProxy
LEGACY_NETBT\0000 - NetBios over Tcpip
LEGACY_NULL\0000 - Null
LEGACY_PARTMGR\0000 - PartMgr
LEGACY_PARVDM\0000 - ParVdm
LEGACY_RASACD\0000 - Remote Access Auto Connection Driver
LEGACY_RDPCCD\0000 - RDPCCD
LEGACY_TCPIP\0000 - TCP/IP Protocol Driver
LEGACY_VGASAVE\0000 - VgaSave
LEGACY_VOLSnap\0000 - volSnap
LEGACY_WANARP\0000 - Remote Access IP ARP Driver
LEGACY__VOIDVSIPBCCDXR\0000 - _VOIDvsipbccdxr
Fri Mar 12 16:32:16 2010 (UTC)
LEGACY_MANDIANT_TOOLS
Fri Mar 12 16:29:28 2010 (UTC)
LEGACY__VOIDVSIPBCCDXR
Fri Mar 12 16:25:14 2010 (UTC)
LEGACY_WSCSVC\0000 - Security Center
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review UserAssist registry key
 - Stores information about actions user took through the shell
 - Double-clicking Windows shortcuts
 - Starting applications through the Start Menu
 - Location
 - HKCU\Software\Microsoft\Windows\Currentversion\Explorer\Userassist\{GUID}\Count
 - Information Provided
 - User launched the application or executable through interaction with the shell
 - Application or executable's last run time
 - Application or executable's file path

Malware Forensics Examination Steps

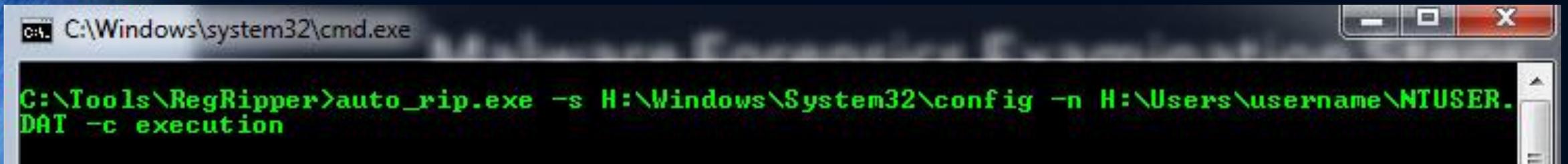
Examine the Programs Ran on the System

- Review UserAssist registry key
 - RegRipper (rip.exe or rip.pl)
 - Command:

```
C:\Tools\RegRipper>rip.exe -r H:\Users\username\NTUSER.DAT -p userassist
```

- r switch: specifies registry hive

-p switch: specifies plug-in

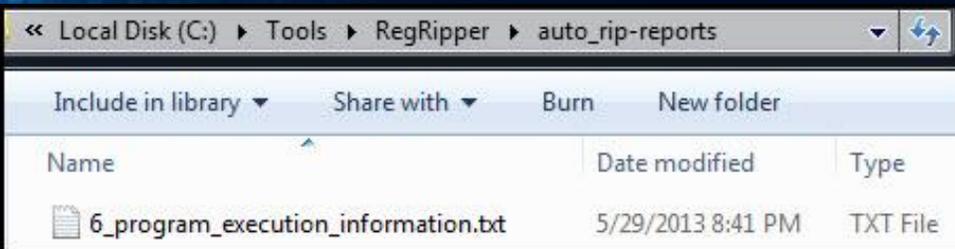
A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt displays the command 'C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -n H:\Users\username\NTUSER.DAT -c execution' in green text on a black background. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

```
C:\Windows\system32\cmd.exe  
C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -n H:\Users\username\NTUSER.DAT -c execution
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review UserAssist registry key
 - auto_rip (auto_rip.exe or auto_rip.pl)



```
UserAssist
Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Nov 2 14:42:56 2007 (UTC)

{5E6AB780-7743-11CF-A12B-00AA004AE837}
Fri Mar 12 18:40:56 2010 Z
  UEME_UITOOLBAR (5)
  UEME_UITOOLBAR:0x1,126 (1)
Fri Mar 12 16:18:55 2010 Z
  UEME_UITOOLBAR:0x1,130 (4)

{75048700-EF1F-11D0-9888-006097DEACF9}
Fri Mar 12 18:41:27 2010 Z
  UEME_RUNPATH (28)
  UEME_RUNPATH:C:\WINDOWS\system32\notepad.exe (2)
Fri Mar 12 18:41:14 2010 Z
  UEME_RUNPATH:C:\WINDOWS\system32\cmd.exe (3)
Fri Mar 12 18:40:34 2010 Z
  UEME_UIQCUT (4)
Fri Mar 12 16:38:37 2010 Z
  UEME_UISCUT (13)
  UEME_RUNPATH::{20D04FE0-3AEA-1069-A2D8-08002B30309D} (8)
Fri Mar 12 16:33:59 2010 Z
  UEME_RUNPATH:Shortcut to MemoryDD.bat.lnk (4)
  UEME_RUNPATH:(null) (4)
Fri Mar 12 16:28:57 2010 Z
  UEME_RUNPATH:C:\Documents and settings\Administrator\Desktop\update.exe (1)
Fri Mar 12 16:23:59 2010 Z
  UEME_RUNPATH:C:\WINDOWS\system32\mmc.exe (3)
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review MUICache registry key
 - Stores information about what programs ran under a user account
 - Location
 - Varies based on OS
 - Windows XP located in NTUSER.DAT
 - Windows 7 located in UsrClass.dat
 - Windows 7: HKCU\ Local Settings\MuiCache
 - Information Provided
 - The user account an executable ran under
 - Executable's file path

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review MUICache registry key
 - RegRipper (rip.exe or rip.pl)
 - Command:

```
C:\Tools\RegRipper>rip.exe -r H:\Users\username\  
AppData\Local\Microsoft\Windows\UsrClasst.dat -p muicache
```

- r switch: specifies registry hive

-p switch: specifies plug-in

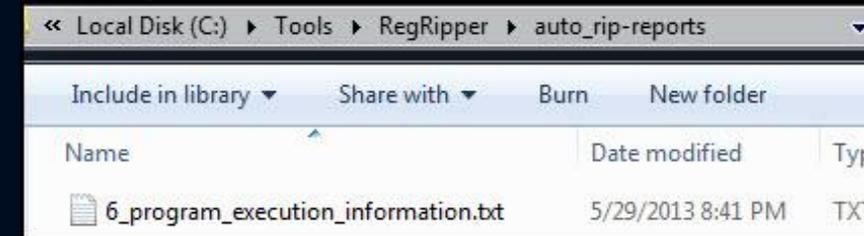
A screenshot of a Windows command prompt window. The title bar shows 'C:\Windows\system32\cmd.exe'. The command prompt displays the following command in green text:

```
C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -n H:\Users\username\NTUSER.DAT -u H:\Users\username\AppData\Local\Microsoft\Windows\UsrClass.dat -c execution
```

Malware Forensics Examination Steps

Examine the Programs Ran on the System

- Review MUICache registry key
 - auto_rip (auto_rip.exe or auto_rip.pl)



```
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\windows\ShellNoRoam\MUICache
Lastwrite Time Fri Mar 12 18:41:16 2010 (UTC)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Adobe Reader 8\setup.exe (Adobe Bootstrapper for single installation)
C:\Program Files\VMware\VMware Tools\VMwareTray.exe (VMwareTray)
C:\Program Files\VMware\VMware Tools\VMwareUser.exe (VMwareUser)
C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe (Adobe Acrobat SpeedLauncher)
C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe (Java(TM) Platform SE binary)
C:\WINDOWS\system32\mmc.exe (Microsoft Management Console)
C:\WINDOWS\Explorer.EXE (windows Explorer)
C:\WINDOWS\system32\notepad.exe (Notepad)
C:\Program Files\windows NT\Accessories\WORDPAD.EXE (wordPad)
C:\Program Files\Internet Explorer\iexplore.exe (Internet Explorer)
C:\WINDOWS\system32\shell32.dll (windows shell Common Dll)
C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe (Adobe Reader 8.1)
C:\WINDOWS\system32\mspaint.exe (Paint)
C:\WINDOWS\system32\shimgvw.dll (windows Picture and Fax Viewer)
C:\Program Files\windows Media Player\wmplayer.exe (windows Media Player)
C:\Documents and Settings\Administrator\Desktop\update.exe (update)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\TMP77E.exe (Logical Disk Manager ASR utility)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\TMPDC7.exe (TMPDC7)
C:\downloads\Memoryze\MemoryDD.bat (MemoryDD)
C:\WINDOWS\system32\cmd.exe (windows Command Processor)
C:\downloads\Memoryze\Memoryze.exe (Mandiant Agent Manager)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\asr64_ldm.exe (Logical Disk Manager ASR utility)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\asd2.tmp.exe (asd2.tmp)
C:\Program Files\Dr. Guard\drguard.exe (drguard)
```



Malware Forensics Examination Steps

Examine the Auto-start Locations

- Review Auto-start Locations
 - Auto-start locations are used to start programs automatically on system start-up or user log in
 - Location
 - Varies by operating system version
 - File system, Registry
 - Most common are Run keys and Windows services
 - Information Provided
 - Executable's file path
 - Timestamps can show when infection occurred

Malware Forensics Examination Step

Examine the Auto-start Locations

- Registry Run keys are common location
- Software Hive Run Keys
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - HKLM\Software\ Microsoft\Windows\CurrentVersion\RunServices
 - HKLM\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - soft_run RegRipper plugin

Malware Forensics Examination Step

Examine the Auto-start Locations

- Registry Run keys are common location
- NTUSER.DAT Hive Run Keys
 - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce
 - HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
 - HKCU\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
 - Run value
 - Load value
 - user_run RegRipper plugin

Malware Forensics Examination Step

Examine the Auto-start Locations

- Windows Services are another common location
- System Hive
 - HKLM\System\CurrentControlSet\services
 - services RegRipper plugin (list services by last write times)
 - svcdll RegRipper plugin (list services with ServiceDLL values)
 - svc RegRipper plugin to (list services and drivers by last write times)

Malware Forensics Examination Step

Examine the Auto-start Locations

- Software Hive Locations
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
 - winlogon RegRipper plugin
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
 - winlogon RegRipper plugin
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
 - winlogon RegRipper plugin
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System
 - winlogon RegRipper plugin
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
 - winlogon RegRipper plugin
 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList
 - winlogon RegRipper plugin
 - HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
 - installedcomp RegRipper plugin
 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
 - installedcomp RegRipper plugin
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
 - shellexec RegRipper plugin
 - HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
 - shellexec RegRipper plugin
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
 - bho RegRipper plugin
 - HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
 - bho RegRipper plugin

Malware Forensics Examination Step

Examine the Auto-start Locations

- Software Hive Locations

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
 - drivers32 RegRipper plugin
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
 - drivers32 RegRipper plugin
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
 - imagefile RegRipper plugin
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
 - imagefile RegRipper plugin
- HKLM\SOFTWARE\Classes\Exefile\Shell\Open\Command\{Default}
 - cmd_shell RegRipper plugin
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
 - appinitdlls and init_dlls RegRipper plugins
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
 - appinitdlls RegRipper plugin
- HKLM\SOFTWARE\Microsoft\SchedulingAgent
 - schedagent RegRipper plugin
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
 - shellext RegRipper plugin
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
 - svchost RegRipper plugin

Malware Forensics Examination Step

Examine the Auto-start Locations

- System Hive Locations
 - HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
 - appcertdlls RegRipper plugin
 - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
 - securityproviders RegRipper plugin
 - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages
 - lsa_packages RegRipper plugin
 - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
 - lsa_packages RegRipper plugin
 - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
 - lsa_packages RegRipper plugin
 - HKLM\SYSTEM\ControlSet\Control\Session Manager\CWDIllegalInDllSearch
 - dllsearch RegRipper plugin
 - HKLM\SYSTEM\ControlSet\Control\SafeBoot
 - safeboot RegRipper plugin

Malware Forensics Examination Step

Examine the Auto-start Locations

- NTUSER.DAT Hive Locations
 - HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
 - winlogon_u RegRipper plugin
 - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
 - load RegRipper plugin
 - HKCU\Software\Microsoft\Command Processor\Autorun
 - cmdproc RegRipper plugin

Malware Forensics Examination Step

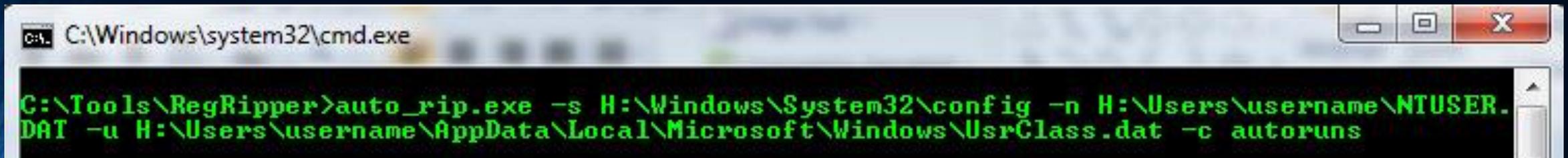
Examine the Auto-start Locations

- UsrClass.dat Hive Location
 - HKCU\Classes\Exefile\Shell\Open\Command\Default
 - cmd_shell_u RegRipper plugin

Malware Forensics Examination Steps

Examine the Auto-start Locations

- auto_rip (auto_rip.exe or auto_rip.pl)

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt is open to the directory 'C:\Tools\RegRipper'. The command entered is 'auto_rip.exe -s H:\Windows\System32\config -n H:\Users\username\NTUSER.DAT -u H:\Users\username\AppData\Local\Microsoft\Windows\UsrClass.dat -c autoruns'. The output of the command is not visible.

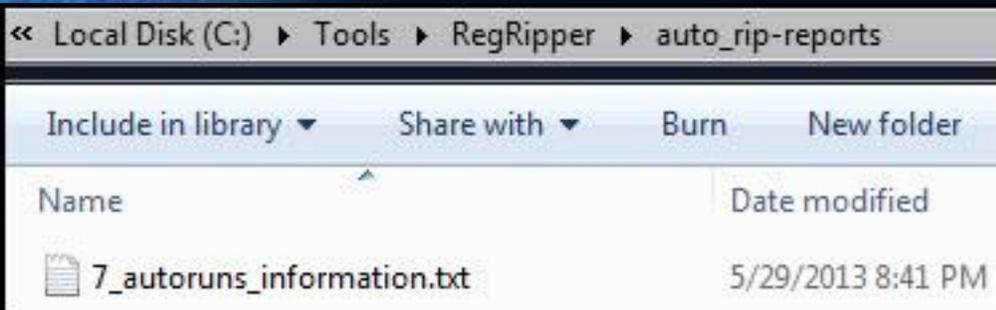
```
C:\Windows\system32\cmd.exe
C:\Tools\RegRipper>auto_rip.exe -s H:\Windows\System32\config -n H:\Users\username\NTUSER.DAT -u H:\Users\username\AppData\Local\Microsoft\Windows\UsrClass.dat -c autoruns
```

Malware Forensics Examination Steps

Examine the Auto-start Locations

- auto_rip (auto_rip.exe or auto_rip.pl)
 - NTUSER.DAT Hive Run Keys

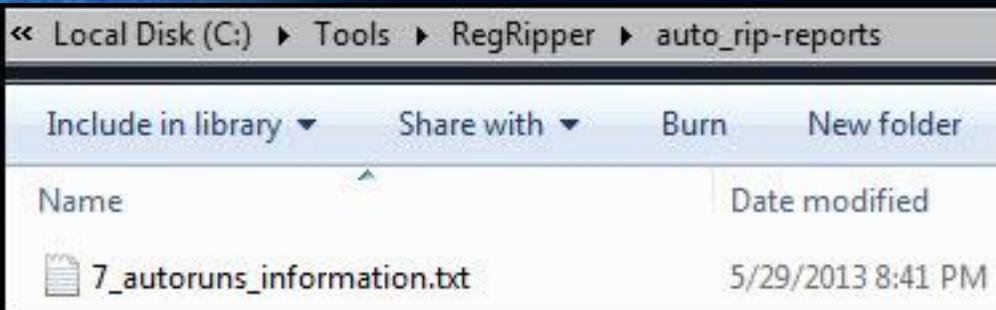
```
user_run v.20130425
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive
Software\Microsoft\windows\CurrentVersion\Run
LastWrite Time Fri Mar 12 16:35:35 2010 (UTC)
  asr64_ldm.exe: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\asr64_ldm.exe
  Dr. Guard: "C:\Program Files\Dr. Guard\drguard.exe" -noscan
Software\wow6432Node\Microsoft\windows\CurrentVersion\Run not found.
Software\Microsoft\windows\CurrentVersion\RunOnce
LastWrite Time Fri Mar 12 16:16:41 2010 (UTC)
Software\Microsoft\windows\CurrentVersion\RunOnce has no values.
```



Malware Forensics Examination Steps

Examine the Auto-start Locations

- auto_rip (auto_rip.exe or auto_rip.pl)
 - Services



```
Name = _VOIDvsipbccdxr
Display =
ImagePath = \systemroot\_VOIDvsipbccdxr\_VOIDd.sys
Type = Kernel driver
Start = System start
Group =

Fri Mar 12 16:29:28 2010Z
Name = _VOIDd.sys
Display =
ImagePath = \systemroot\system32\drivers\_VOIDfjtivkowvn.sys
Type = Kernel driver
Start = system start
Group = file system

Fri Mar 12 16:17:03 2010Z
Name = USBSTOR
Display = USB Mass Storage Driver
ImagePath = system32\DRIVERS\USBSTOR.SYS
Type = Kernel driver
Start = Manual
Group =
```

Malware Forensics Examination Step

Examine File System Artifacts

- New Technologies File System (NTFS) default for Windows NT based systems
- NTFS artifacts of interest
 - Master File Table (\$MFT)
 - Change Journal (\$UsnJrnl)

Malware Forensics Examination Step

Examine File System Artifacts

- Review the Master File Table (\$MFT)
 - Contains the information about all files and folders
 - Every file and folder has at least one entry in the \$MFT
 - \$MFT entry is used to store attributes
 - \$Standard_Information -> timestamps easily changed
 - \$File_Name -> timestamps more difficult to change
 - \$Data -> file's contents
 - Location
 - Beneath the root of volume (i.e. C:\\$MFT)
 - Information Provided
 - Files and folders creation dates, last modified dates, and last access dates
 - Files and folders paths
 - Timeline of file system activity to perform root cause analysis

Malware Forensics Examination Steps

Examine File System Artifacts

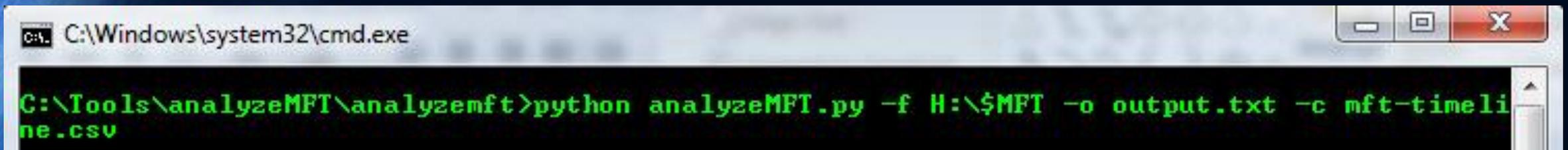
- Review Master File Table (\$MFT)
 - analyzeMFT.py (or analyzeMFT.exe)
 - Command:

```
C:\Tools\analyzeMFT\analyzemft>python analyzeMFT.py -f H:\$MFT -o output.txt -c mft-timeline.csv
```

- f switch: specifies file

-o switch: specifies output file

- c switch: specifies output in timeline (l2t format)



```
C:\Windows\system32\cmd.exe  
C:\Tools\analyzeMFT\analyzemft>python analyzeMFT.py -f H:\$MFT -o output.txt -c mft-timeline.csv
```

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
3/12/2010	16:35:11	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Desktop/Dr. Guard Support.Ink
3/12/2010	16:35:11	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Desktop/Dr. Guard Support.Ink
3/12/2010	16:35:11	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Desktop/Dr. Guard Support.Ink
3/12/2010	16:35:11	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Desktop/Dr. Guard Support.Ink
3/12/2010	16:35:11	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/Microsoft/Internet Explorer/Quick Launch/Dr. Guard.Ink
3/12/2010	16:35:11	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/Microsoft/Internet Explorer/Quick Launch/Dr. Guard.Ink
3/12/2010	16:35:11	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/Microsoft/Internet Explorer/Quick Launch/Dr. Guard.Ink
3/12/2010	16:35:11	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/Microsoft/Internet Explorer/Quick Launch/Dr. Guard.Ink
3/12/2010	16:35:21	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/DRGUARD.EXE-23A7FB3B.pf
3/12/2010	16:35:21	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/DRGUARD.EXE-23A7FB3B.pf
3/12/2010	16:35:21	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/DRGUARD.EXE-23A7FB3B.pf
3/12/2010	16:35:21	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/DRGUARD.EXE-23A7FB3B.pf
3/12/2010	16:35:28	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/splash.mp3
3/12/2010	16:35:28	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/splash.mp3
3/12/2010	16:35:28	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/splash.mp3
3/12/2010	16:35:28	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/splash.mp3
3/12/2010	16:35:28	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/virus.mp3
3/12/2010	16:35:28	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/virus.mp3
3/12/2010	16:35:28	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/virus.mp3
3/12/2010	16:35:28	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/virus.mp3
3/12/2010	16:35:31	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/drg.dat

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	
date	time	macb	source	sourcetype	
3/12/2010	16:34:57	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drgext.dll
3/12/2010	16:34:57	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac854e.tmp
3/12/2010	16:34:57	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac854e.tmp
3/12/2010	16:34:57	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac854e.tmp
3/12/2010	16:34:57	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac854e.tmp
3/12/2010	16:34:57	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drghook.dll
3/12/2010	16:34:57	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drghook.dll
3/12/2010	16:34:57	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drghook.dll
3/12/2010	16:34:57	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drghook.dll
3/12/2010	16:34:57	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac8677.tmp
3/12/2010	16:34:57	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac8677.tmp
3/12/2010	16:34:57	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac8677.tmp
3/12/2010	16:34:57	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac8677.tmp
3/12/2010	16:34:58	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/uninstall.exe
3/12/2010	16:34:58	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/uninstall.exe
3/12/2010	16:34:58	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/uninstall.exe
3/12/2010	16:34:58	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/uninstall.exe
3/12/2010	16:34:58	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac887a.tmp
3/12/2010	16:34:58	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac887a.tmp
3/12/2010	16:34:58	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac887a.tmp
3/12/2010	16:34:58	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac887a.tmp
3/12/2010	16:35:10	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drguard.exe
3/12/2010	16:35:10	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drguard.exe
3/12/2010	16:35:10	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drguard.exe
3/12/2010	16:35:10	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drguard.exe

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
3/12/2010	16:34:50	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD3TM~1.EXE
3/12/2010	16:34:50	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD3TM~1.EXE
3/12/2010	16:34:50	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD3TM~1.EXE
3/12/2010	16:34:50	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asd4.tmp
3/12/2010	16:34:50	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asd4.tmp
3/12/2010	16:34:50	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asd4.tmp
3/12/2010	16:34:50	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asd4.tmp
3/12/2010	16:34:50	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD4TM~1.EXE
3/12/2010	16:34:50	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD4TM~1.EXE
3/12/2010	16:34:50	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD4TM~1.EXE
3/12/2010	16:34:50	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/ASD4TM~1.EXE
3/12/2010	16:34:50	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD4.TMP.EXE-2740C04A.pf
3/12/2010	16:34:50	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD4.TMP.EXE-2740C04A.pf
3/12/2010	16:34:50	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD4.TMP.EXE-2740C04A.pf
3/12/2010	16:34:50	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD4.TMP.EXE-2740C04A.pf
3/12/2010	16:34:50	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD3.TMP.EXE-26CA54B1.pf
3/12/2010	16:34:50	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD3.TMP.EXE-26CA54B1.pf
3/12/2010	16:34:50	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD3.TMP.EXE-26CA54B1.pf
3/12/2010	16:34:50	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASD3.TMP.EXE-26CA54B1.pf
3/12/2010	16:34:56	.A..	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drg.db
3/12/2010	16:34:56	M...	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drg.db
3/12/2010	16:34:56	..C.	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drg.db
3/12/2010	16:34:56	...B	FILE	NTFS \$MFT	/Program Files/DR1A09~1.GUA/drg.db
3/12/2010	16:34:57	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/uac8415.tmp

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	
date	time	macb	source	sourcetype	
3/12/2010	16:32:41	M...	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDmfeklnmal.dll
3/12/2010	16:32:41	..C.	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDmfeklnmal.dll
3/12/2010	16:32:41	...B	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDmfeklnmal.dll

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	
date	time	macb	source	sourcetype	
3/12/2010	16:29:09	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NET.EXE-01A53C2F.pf
3/12/2010	16:29:16	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASR64_LDM.EXE-3944C1CE.pf
3/12/2010	16:29:16	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASR64_LDM.EXE-3944C1CE.pf
3/12/2010	16:29:16	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASR64_LDM.EXE-3944C1CE.pf
3/12/2010	16:29:16	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/ASR64_LDM.EXE-3944C1CE.pf
3/12/2010	16:29:17	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMPDC7.EXE-2240CBB3.pf
3/12/2010	16:29:17	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMPDC7.EXE-2240CBB3.pf
3/12/2010	16:29:17	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMPDC7.EXE-2240CBB3.pf
3/12/2010	16:29:17	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMPDC7.EXE-2240CBB3.pf
3/12/2010	16:29:28	.A..	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr
3/12/2010	16:29:28	M...	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr
3/12/2010	16:29:28	..C.	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr
3/12/2010	16:29:28	...B	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr
3/12/2010	16:29:28	.A..	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr/_VOIDd.sys
3/12/2010	16:29:28	M...	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr/_VOIDd.sys
3/12/2010	16:29:28	..C.	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr/_VOIDd.sys
3/12/2010	16:29:28	...B	FILE	NTFS \$MFT	/WINDOWS/_VOIDvsipbccdxr/_VOIDd.sys
3/12/2010	16:29:29	.A..	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDfwwbrqjhp.dll
3/12/2010	16:29:29	M...	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDfwwbrqjhp.dll
3/12/2010	16:29:29	..C.	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDfwwbrqjhp.dll
3/12/2010	16:29:29	...B	FILE	NTFS \$MFT	/WINDOWS/system32/_VOIDfwwbrqjhp.dll
3/12/2010	16:29:29	...B	FILE	NTFS \$MFT	/WINDOWS/Temp/_VOID53f7.tmp

Malware Forensics Examination Steps

analyzeMFT.py

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
3/12/2010	16:27:22	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/8RY4MW9H/NOV1_1~1.HTM
3/12/2010	16:28:36	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/RUNDLL32.EXE-2E540F2E.pf
3/12/2010	16:28:36	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/RUNDLL32.EXE-2E540F2E.pf
3/12/2010	16:28:36	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/RUNDLL32.EXE-2E540F2E.pf
3/12/2010	16:28:36	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/RUNDLL32.EXE-2E540F2E.pf
3/12/2010	16:28:58	.A..	FILE	NTFS \$MFT	/Documents and Settings/All Users/Favorites/_favdata.dat
3/12/2010	16:28:58	M...	FILE	NTFS \$MFT	/Documents and Settings/All Users/Favorites/_favdata.dat
3/12/2010	16:28:58	..C.	FILE	NTFS \$MFT	/Documents and Settings/All Users/Favorites/_favdata.dat
3/12/2010	16:28:58	...B	FILE	NTFS \$MFT	/Documents and Settings/All Users/Favorites/_favdata.dat
3/12/2010	16:29:06	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asr64_Idm.exe
3/12/2010	16:29:06	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asr64_Idm.exe
3/12/2010	16:29:06	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asr64_Idm.exe
3/12/2010	16:29:06	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/asr64_Idm.exe
3/12/2010	16:29:07	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMP77E.EXE-02781D7C.pf
3/12/2010	16:29:07	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMP77E.EXE-02781D7C.pf
3/12/2010	16:29:07	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMP77E.EXE-02781D7C.pf
3/12/2010	16:29:07	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/TMP77E.EXE-02781D7C.pf
3/12/2010	16:29:07	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SC.EXE-012262AF.pf
3/12/2010	16:29:07	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SC.EXE-012262AF.pf
3/12/2010	16:29:07	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SC.EXE-012262AF.pf
3/12/2010	16:29:07	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SC.EXE-012262AF.pf
3/12/2010	16:29:07	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UPDATE.EXE-0825DC41.pf
3/12/2010	16:29:07	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UPDATE.EXE-0825DC41.pf
3/12/2010	16:29:07	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UPDATE.EXE-0825DC41.pf
3/12/2010	16:29:07	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UPDATE.EXE-0825DC41.pf
3/12/2010	16:29:08	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/_VOID1029.tmp

Malware Forensics Examination Step

Examine File System Artifacts

- Review the Windows Change Journal (\$UsnJrnl:J)
 - Records when changes are made to files and folders (historical information)
 - Provides historical information
 - Location
 - \$Extend\ \$UsnJrnl:J
 - J alternate data stream stored the change journal
 - Information Provided
 - Time of change
 - Reason for change
 - File/Directory name
 - \$MFT record number
 - Timestamp information can be combined into timeline with other NTFS artifacts

Malware Forensics Examination Steps

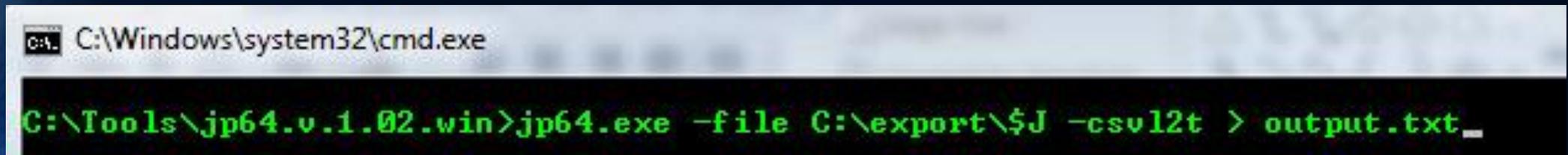
Examine File System Artifacts

- Review Windows Change Journal (\$UsnJrnl:J)
 - jp64.exe (or jp32.exe)
 - Command:

```
C:\Tools\jp64.v.1.02.win>jp64.exe -file C:\export\%J -csvl2t > output.txt
```

- file switch: specifies file (shown is exported \$UsnJrnl:\$J)

- csvl2t switch: specifies output in timeline (l2t format)



```
C:\Windows\system32\cmd.exe  
C:\Tools\jp64.v.1.02.win>jp64.exe -file C:\export\%J -csvl2t > output.txt_
```

Malware Forensics Examination Steps

jp64.exe

note: image below is from different system infected with ZeroAccess Rootkit

date	time	MACB	sourcetype	type	short
12/6/2012	22:18:05	M...	NTFS \$MFT	\$SI [M...] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/L
12/6/2012	22:18:05	..C.	NTFS \$MFT	\$SI [..C.] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/L
12/6/2012	22:18:05	...B	NTFS \$MFT	\$SI [...B] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/L
12/6/2012	22:18:05		NTFS \$LOGFILE	File Rename Event	File Renamed
12/6/2012	22:18:05		NTFS \$LOGFILE	File Creation Event	FILE Created
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_created	n
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_added	n
12/6/2012	22:18:05	..C.	NTFS:\$UsnJrnl:J\$	attrib_changed	n
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_added	n
12/6/2012	22:18:05	..C.	NTFS:\$UsnJrnl:J\$	attrib_changed	n
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_added	n
12/6/2012	22:18:05	..C.	NTFS:\$UsnJrnl:J\$	attrib_changed	{5da39e95-8007-4308-c6cf-bc61795d0d}
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_created	{5da39e95-8007-4308-c6cf-bc61795d0d}
12/6/2012	22:18:05	..C.	NTFS:\$UsnJrnl:J\$	attrib_changed	{5da39e95-8007-4308-c6cf-bc61795d0d}
12/6/2012	22:18:05	...B	NTFS:\$UsnJrnl:J\$	file_created	{5da39e95-8007-4308-c6cf-bc61795d0d}
12/6/2012	22:18:05	.A..	NTFS \$MFT	\$SI [.A..] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/n
12/6/2012	22:18:05	M...	NTFS \$MFT	\$SI [M...] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/n
12/6/2012	22:18:05	..C.	NTFS \$MFT	\$SI [..C.] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/n
12/6/2012	22:18:05	...B	NTFS \$MFT	\$SI [...B] time	/Windows/Installer/{5da39e95-8007-4308-c6cf-bc61795d0d}/n

Mock Case – Iron Man Style

Incident Detected

- User provides a very detailed report

“My computer is acting funny”

Responding to the System

- Gaining access to data on the system
 - Remotely over the wire to the live system
 - Running collection scripts on the system
 - Removing the hard drive
 - Imaging the hard drive and working on the forensic copy

Tip

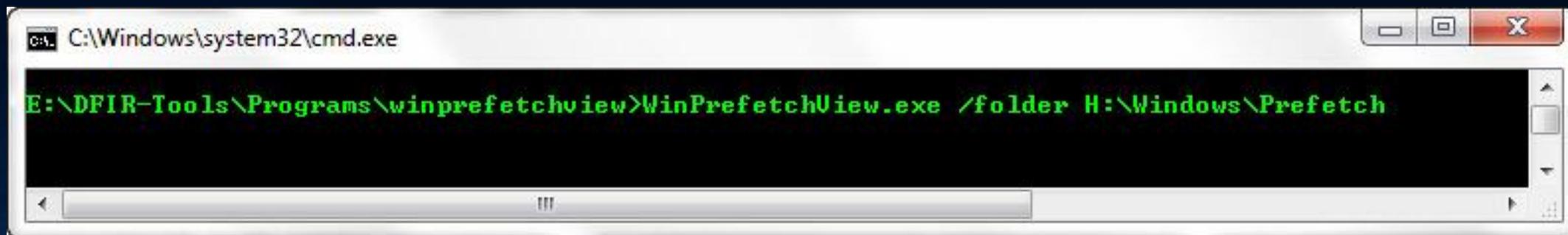
- Responding remotely or using collection scripts is the better alternative

Digital Forensics Blasphemy

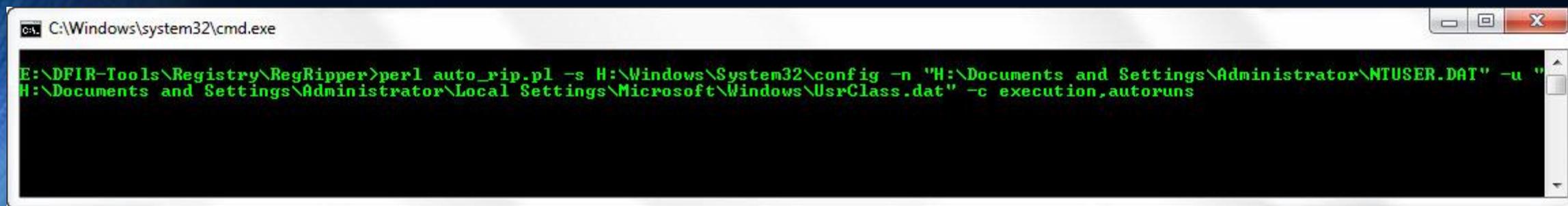
- Skip imaging the drive and work directly on the original copy
 - Imaging takes too much time (but use precautions if imaging becomes necessary)

Hunting for Malware

- Parse program execution and auto-start artifacts



```
C:\Windows\system32\cmd.exe
E:\DFIR-Tools\Programs\winprefetchview>WinPrefetchView.exe /folder H:\Windows\Prefetch
```



```
C:\Windows\system32\cmd.exe
E:\DFIR-Tools\Registry\RegRipper>perl auto_rip.pl -s H:\Windows\System32\config -n "H:\Documents and Settings\Administrator\NTUSER.DAT" -u "H:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat" -c execution,autoruns
```

Hunting for Malware

- Review program execution
 - Prefetch files
 - Look at process paths for malware indicators

Filename	Created Time	Modified Time	Process Path
FTK IMAGER.EXE-25ECB6F3.pf	3/10/2011 1:18:24 PM	3/10/2011 1:18:2...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\DESKTOP\\PROGRAMS\\IMAGER LITE 2.9.0\\FTK IMAGER.EXE
PROCMON.EXE-000B5C95.pf	3/10/2011 1:18:16 PM	3/10/2011 1:18:1...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\DESKTOP\\PROGRAMS\\PROCESSMONITOR\\PROCMON.EXE
REGSHOT.EXE-355EC1DD.pf	3/10/2011 1:18:04 PM	3/10/2011 1:18:0...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\DESKTOP\\PROGRAMS\\REGSHOT_1.8.2_SRC_BIN\\REGSHOT.EXE
FTK IMAGER.EXE-066C1EA6.pf	3/10/2011 2:05:46 PM	3/10/2011 2:05:4...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\TEST\\DESKTOP\\PROGRAMS\\IMAGER LITE 2.9.0\\FTK IMAGER.EXE
PROCMON.EXE-05034A9F.pf	3/10/2011 2:05:40 PM	3/10/2011 2:05:4...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\TEST\\DESKTOP\\PROGRAMS\\PROCESSMONITOR\\PROCMON.EXE
REGSHOT.EXE-2C5D6AE4.pf	3/10/2011 2:05:36 PM	3/10/2011 2:05:3...	\\DEVICE\\HARDDISKVOLUME1\\DOCUMENTS AND SETTINGS\\TEST\\DESKTOP\\PROGRAMS\\REGSHOT_1.8.2_SRC_BIN\\REGSHOT.EXE
000C54AD.TMP-134FDD0A.pf	10/14/2011 10:55:47 PM	10/14/2011 10:55...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\000C54AD.TMP
000C6518.TMP-1B7E315C.pf	10/14/2011 10:56:02 PM	10/14/2011 10:56...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\000C6518.TMP
SETUP.EXE-14B3807A.pf	10/14/2011 10:28:38 PM	10/14/2011 10:32...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\ADOBE READER 8\\SETUP.EXE
QUICKTIMEINSTALLERADMIN.EXE-0111BF55.pf	10/14/2011 10:36:15 PM	10/14/2011 10:36...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\IXP418.TMP\\QUICKTIMEINSTALLERADMIN.EXE
MSI15.TMP-0E2297CB.pf	10/14/2011 10:25:42 PM	10/14/2011 10:25...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\MSI15.TMP
MSI4.TMP-263BF63E.pf	10/14/2011 10:25:23 PM	10/14/2011 10:25...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\MSI4.TMP
NOTMY.EXE-335CAAA7.pf	10/14/2011 10:55:47 PM	10/14/2011 10:55...	\\DEVICE\\HARDDISKVOLUME1\\DOCUME~1\\ADMINI~1\\LOCALS~1\\TEMP\\NOTMY.EXE

Hunting for Malware

- Review program execution
 - Prefetch files
 - Check out the loaded modules inside the prefetch file

Filename	Full Path	Device Path	Index
NOTMY.EXE-335CAAA7.pf	10/14/2011 10:55:47 PM	10/14/2011 10:55:47 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\NOTMY.EXE
PCB_BUILD_23_SMTP.EXE-152B7E8E.pf	10/14/2011 10:55:57 PM	10/14/2011 10:55:57 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\PCB_BUILD_23_SMTP.EXE
SVCHOST.EXE-072D0CB1.pf	10/14/2011 10:56:00 PM	10/14/2011 10:56:00 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\SVCHOST.EXE
000C6518.TMP-1B7E315C.pf	10/14/2011 10:56:02 PM	10/14/2011 10:56:02 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\000C6518.TMP
ADVAPI32.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL	6
APPHELP.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\APPHELP.DLL	10
DLEEQRDJ.BAT		\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\DLEEQRDJ.BAT	9
KERNEL32.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL	1
LOCALE.NLS		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOCALE.NLS	3
NOTMY.EXE		\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\NOTMY.EXE	5
NTDLL.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL	0
RPCRT4.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RPCRT4.DLL	7
SECUR32.DLL		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SECUR32.DLL	8
SORTTBLS.NLS		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SORTTBLS.NLS	4
SYSMMAIN.SDB		\DEVICE\HARDDISKVOLUME1\WINDOWS\APPPATCH\SYSMMAIN.SDB	11
UNICODE.NLS		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\UNICODE.NLS	2

Hunting for Malware

- Review program execution
 - Prefetch files
 - Sort by time (prefetch creation time, modification time, or last run time)

Filename	Created Time	Modified Time	Process Path
IPCONFIG.EXE-2395F30B.pf	10/14/2011 10:29:39 PM	10/14/2011 10:30:22 PM	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\IPCONFIG.EXE
ADBERDR811_EN_US-10 OCTOBER 2-25D687B2.pf	10/14/2011 10:31:26 PM	10/14/2011 10:31:26 PM	\DEVICE\HARDDISK1\DP(1)0-0+3\SOFTWARE\ATTACK-ARTIFACTS\OLD APPS\READER\ADBERDR811_EN_US-10 OCTOBER 2007.EXE
QUICKTIMEPLAYER76-19 JANUARY -32B21A5B.pf	10/14/2011 10:35:42 PM	10/14/2011 10:35:42 PM	\DEVICE\HARDDISK1\DP(1)0-0+3\SOFTWARE\ATTACK-ARTIFACTS\OLD APPS\QUICKTIME\QUICKTIMEPLAYER76-19 JANUARY 2009.EXE
QUICKTIMEINSTALLERADMIN.EXE-0111BF55.pf	10/14/2011 10:36:15 PM	10/14/2011 10:36:15 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\IXP418.TMP\QUICKTIMEINSTALLERADMIN.EXE
SOFTWAREUPDATE.EXE-1415D1B8.pf	10/14/2011 10:36:15 PM	10/14/2011 10:36:15 PM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\APPLE SOFTWARE UPDATE\SOFTWAREUPDATE.EXE
DLLHOST.EXE-205D880D.pf	10/14/2011 10:36:20 PM	10/14/2011 10:36:20 PM	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DLLHOST.EXE
QTTASK.EXE-342507FB.pf	10/14/2011 10:37:25 PM	10/14/2011 10:37:25 PM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\QUICKTIME\QTTASK.EXE
FLASHPLAYER10R45_2_WIN.EXE-32E647B2.pf	10/14/2011 10:38:16 PM	10/14/2011 10:38:16 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\TEMPORARY DIRECTORY 1 FOR FP10_ARCHIVE-30 SEPTEMBER 2008.ZIP\FP10_ARCHIVE\10R45_2\FLASHPLAY...
RUNDLL32.EXE-32FACC6A.pf	10/14/2011 10:38:40 PM	10/14/2011 10:38:40 PM	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RUNDLL32.EXE
JAVA.EXE-0C263507.pf	10/14/2011 10:48:21 PM	10/14/2011 10:48:27 PM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\JAVA\JRE6\BIN\JAVA.EXE
JAUCHECK.EXE-0CBF467B.pf	10/14/2011 10:48:31 PM	10/14/2011 10:48:31 PM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\COMMON FILES\JAVA\JAVA UPDATE\JAUCHECK.EXE
JUCHECK.EXE-1B0E4D0A.pf	10/14/2011 10:48:34 PM	10/14/2011 10:48:34 PM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\COMMON FILES\JAVA\JAVA UPDATE\JUCHECK.EXE
UNIFORM TRAFFIC TICKET.EXE-3A9408AA.pf	10/14/2011 10:55:12 PM	10/14/2011 10:55:12 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\TEMPORARY DIRECTORY 1 FOR UNIFORM%20TRAFFIC%20TICKET[1].ZIP\UNIFORM TRAFFIC TICKET.EXE
SVCHOST.EXE-3530F672.pf	10/14/2011 10:55:22 PM	10/14/2011 10:55:22 PM	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SVCHOST.EXE
000C54AD.TMP-134FDD0A.pf	10/14/2011 10:55:47 PM	10/14/2011 10:55:47 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\000C54AD.TMP
NOTMY.EXE-335CAA7.pf	10/14/2011 10:55:47 PM	10/14/2011 10:55:47 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\NOTMY.EXE
PCB_BUILD_23_SMTMP.EXE-152B7E8E.pf	10/14/2011 10:55:57 PM	10/14/2011 10:55:57 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\PCB_BUILD_23_SMTMP.EXE
SVCHOST.EXE-072D0CB1.pf	10/14/2011 10:56:00 PM	10/14/2011 10:56:00 PM	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SVCHOST.EXE
000C6518.TMP-1B7E315C.pf	10/14/2011 10:56:02 PM	10/14/2011 10:56:02 PM	\DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\000C6518.TMP

Hunting for Malware

- Review program execution
 - AppCompatCache registry key
 - Look at process paths for malware indicators
 - Look for activity around 10/15/2011 02:55:00 UTC (10/14/2011 10:55:00 EDT)

```
C:\WINDOWS\system32\zipfldr.dll
ModTime: Mon Apr 14 09:42:12 2008 Z
UpdTime: Sat Oct 15 02:54:11 2011 Z
Size   : 338432 bytes

C:\WINDOWS\system32\mycomput.dll
ModTime: wed Aug  4 11:59:59 2004 Z
UpdTime: Thu Mar 10 17:15:05 2011 Z
Size   : 90112 bytes

C:\Documents and Settings\Administrator\Application Data\KB961710.exe
ModTime: Sat Oct 15 02:58:50 2011 Z
UpdTime: Sat Oct 15 03:00:17 2011 Z
Size   : 25088 bytes

C:\Program Files\VMware\VMware Tools\vmacthlp.exe
ModTime: Thu Sep 18 22:32:38 2008 Z
UpdTime: Sat Oct 15 02:59:48 2011 Z
Size   : 358960 bytes

C:\WINDOWS\msagent\agentsvr.exe
ModTime: Mon Apr 14 09:42:14 2008 Z
UpdTime: Thu Mar 10 16:04:25 2011 Z
Size   : 256512 bytes
```

Hunting for Malware

- Review program execution
 - AppCompatCache registry key
 - Look at process paths for malware indicators
 - Look for activity around 10/15/2011 02:55:00 UTC (10/14/2011 10:55:00 EDT)

```
C:\WINDOWS\system32\wscntfy.exe
ModTime: Mon Apr 14 09:42:42 2008 Z
UpdTime: Sat Oct 15 03:01:57 2011 Z
Size : 13824 bytes

C:\Documents and Settings\All users\Local Settings\Temp\17f7fff4.com
ModTime: Mon Apr 14 09:42:38 2008 Z
UpdTime: Sat Oct 15 03:00:11 2011 Z
Size : 39936 bytes

C:\WINDOWS\system32\shgina.dll
ModTime: Mon Apr 14 09:42:06 2008 Z
UpdTime: Sat Oct 15 02:44:12 2011 Z
Size : 68096 bytes

C:\WINDOWS\pchealth\uploadLB\Binaries\uploadm.exe
ModTime: Mon Apr 14 09:42:40 2008 Z
UpdTime: Thu Sep 4 14:53:06 2008 Z
Size : 150528 bytes

C:\WINDOWS\system32\oobe\msoobe.exe
ModTime: Mon Apr 14 09:42:30 2008 Z
UpdTime: Thu Mar 10 16:04:09 2011 Z
Size : 29184 bytes

C:\Program Files\Java\jre6\bin\javaws.exe
ModTime: Sat Oct 15 02:25:46 2011 Z
UpdTime: Sat Oct 15 02:48:23 2011 Z
Size : 153376 bytes
```

Hunting for Malware

- Review program execution
 - MUICache registry key
 - Look at process paths for malware indicators

```
muicache v.20130425
(NTUSER.DAT,USRCLASS.DAT) Gets EXES from user's MUICache key

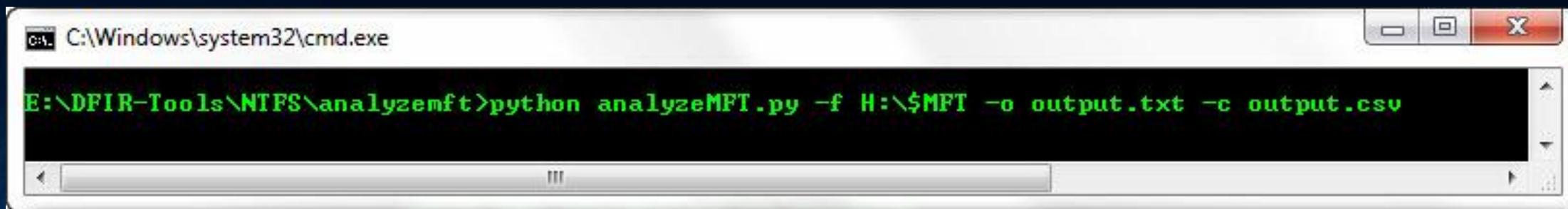
Software\Microsoft\windows\shellNoRoam\MUICache
Lastwrite Time Sat Oct 15 03:01:52 2011 (UTC)
  C:\DOCUME~1\ALLUSE~1\LOCALS~1\Temp\17f7fff4.com (17f7fff4)
  C:\Program Files\VMware\VMware Tools\VMwareTray.exe (VMware Tools tray application)
  C:\Program Files\VMware\VMware Tools\VMwareUser.exe (VMware Tools Service)
  C:\Program Files\Common Files\Java\Java Update\jusched.exe (Java(TM) update scheduler)
  C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe (Adobe Acrobat SpeedLauncher)
  C:\Program Files\QuickTime\QTTask.exe (QuickTime Task)
  C:\Documents and Settings\Administrator\Application Data\KB961710.exe (Hula Tired Spec Nabs Dupe wing)
  C:\WINDOWS\Explorer.EXE (windows Explorer)
Local Settings\Software\Microsoft\windows\shell\MUICache not found.
ALERT: muicache: Software\Microsoft\windows\shellNoRoam\MUICache C:\DOCUME~1\ALLUSE~1\LOCALS~1\Temp\17f7fff4.com has "Temp" in path.
```

Hunting for Malware

- Review auto-start locations
 - Skipping since program execution provided enough leads
 - C:/Documents and Settings/All Users/Local Settings/Temp/NOTMY.EXE
 - C:/Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
 - C:/Documents and Settings/Administrator/Local Settings/Temp/000c6518.tmp
 - C:/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
 - C://Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
 - C:/Documents and Settings/Administrator/Local Settings/Temp/Temporary Directory 2 for Uniform%20traffic%20ticket[1].zip/Uniform traffic ticket.exe
 - C:/Documents and Settings/Administrator/Application Data/KB961710.exe
 - C:/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com

Hunting for Malware

- Parse NTFS artifacts



A screenshot of a Windows command prompt window. The title bar shows the path `C:\Windows\system32\cmd.exe`. The command prompt is open to the directory `E:\DFIR-Tools\NTFS\analyzemft`. The command entered is `python analyzeMFT.py -f H:\$MFT -o output.txt -c output.csv`. The command prompt has a scroll bar at the bottom and standard window controls (minimize, maximize, close) in the top right corner.

```
C:\Windows\system32\cmd.exe
E:\DFIR-Tools\NTFS\analyzemft>python analyzeMFT.py -f H:\$MFT -o output.txt -c output.csv
```

Hunting for Malware

- Review NTFS artifacts
 - Master File Table (\$MFT)
 - Look for activity around 10/15/2011 02:55:00 UTC (10/14/2011 10:55:00 EDT)

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
10/15/2011	2:55:47	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:47	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:48	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NOTMY.EXE-335CAA7.pf
10/15/2011	2:55:48	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NOTMY.EXE-335CAA7.pf
10/15/2011	2:55:48	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NOTMY.EXE-335CAA7.pf
10/15/2011	2:55:48	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NOTMY.EXE-335CAA7.pf
10/15/2011	2:55:48	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/000C54AD.TMP-134FDD0A.pf
10/15/2011	2:55:48	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/000C54AD.TMP-134FDD0A.pf
10/15/2011	2:55:48	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/000C54AD.TMP-134FDD0A.pf
10/15/2011	2:55:48	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/000C54AD.TMP-134FDD0A.pf
10/15/2011	2:55:50	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/KB961710.exe
10/15/2011	2:55:50	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/KB961710.exe
10/15/2011	2:55:50	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/KB961710.exe
10/15/2011	2:55:50	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Application Data/KB961710.exe
10/15/2011	2:55:51	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
10/15/2011	2:55:51	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
10/15/2011	2:55:51	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
10/15/2011	2:55:51	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
10/15/2011	2:55:52	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/P1kAlMiG2Kb7Fz.exe.tmp
10/15/2011	2:55:53	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/P1kAlMiG2Kb7Fz.exe.tmp
10/15/2011	2:55:53	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/P1kAlMiG2Kb7Fz.exe.tmp
10/15/2011	2:55:53	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/P1kAlMiG2Kb7Fz.exe.tmp
10/15/2011	2:55:58	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/PCB_BUILD_23_SMTP.EXE-152B7E8E.pf
10/15/2011	2:55:58	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/PCB_BUILD_23_SMTP.EXE-152B7E8E.pf
10/15/2011	2:55:58	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/PCB_BUILD_23_SMTP.EXE-152B7E8E.pf
10/15/2011	2:55:58	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/PCB_BUILD_23_SMTP.EXE-152B7E8E.pf
10/15/2011	2:56:01	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SVCHOST.EXE-072D0CB1.pf

Hunting for Malware

- Review NTFS artifacts

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
10/15/2011	2:55:15	.A..	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp
10/15/2011	2:55:15	M...	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp
10/15/2011	2:55:15	..C.	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp
10/15/2011	2:55:15	...B	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp
10/15/2011	2:55:15	.A..	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com
10/15/2011	2:55:15	M...	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com
10/15/2011	2:55:15	..C.	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com
10/15/2011	2:55:15	...B	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com
10/15/2011	2:55:23	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SVCHOST.EXE-3530F672.pf
10/15/2011	2:55:23	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SVCHOST.EXE-3530F672.pf
10/15/2011	2:55:23	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SVCHOST.EXE-3530F672.pf
10/15/2011	2:55:23	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/SVCHOST.EXE-3530F672.pf
10/15/2011	2:55:46	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
10/15/2011	2:55:46	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
10/15/2011	2:55:46	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
10/15/2011	2:55:46	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
10/15/2011	2:55:47	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:47	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:47	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:47	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
10/15/2011	2:55:48	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/NOTMY.EXE-335CAA7.pf

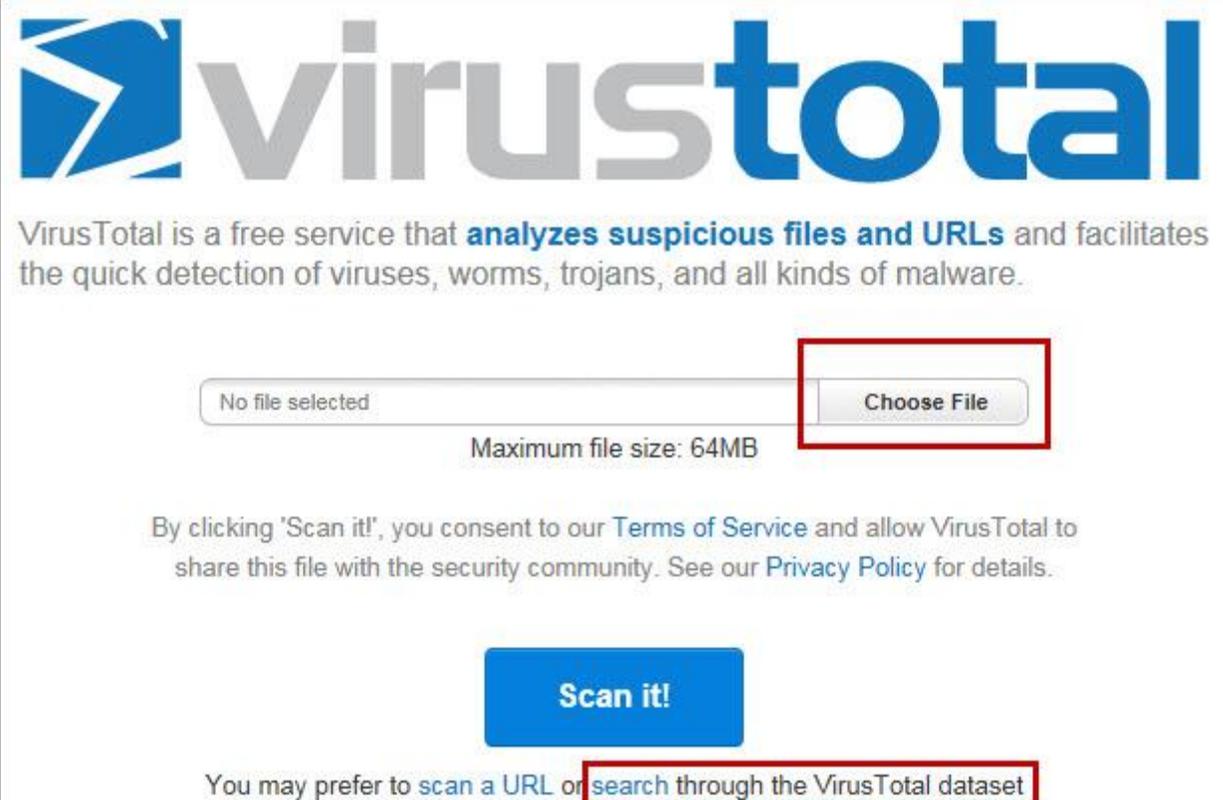
Hunting for Malware

- Review NTFS artifacts

A	B	D	E	F	J
date	time	macb	source	sourcetype	short
10/15/2011	2:52:37	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/8RY4MW9H/hasNewUpdates[1].htm
10/15/2011	2:52:37	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/8RY4MW9H/hasNewUpdates[1].htm
10/15/2011	2:52:37	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/8RY4MW9H/hasNewUpdates[1].htm
10/15/2011	2:52:58	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/4967GLU3/nav_logo_76x32[1].gif
10/15/2011	2:52:58	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/4967GLU3/nav_logo_76x32[1].gif
10/15/2011	2:52:58	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/4967GLU3/nav_logo_76x32[1].gif
10/15/2011	2:52:58	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/4967GLU3/nav_logo_76x32[1].gif
10/15/2011	2:52:59	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/2U4CUDAM/CAO149CL.zip&view=none
10/15/2011	2:52:59	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/2U4CUDAM/CAO149CL.zip&view=none
10/15/2011	2:52:59	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/2U4CUDAM/CAO149CL.zip&view=none
10/15/2011	2:52:59	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/2U4CUDAM/CAO149CL.zip&view=none
10/15/2011	2:53:41	.A..	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/M20M2OXX/Uniform%20traffic%20ticket[1].zip
10/15/2011	2:53:41	M...	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/M20M2OXX/Uniform%20traffic%20ticket[1].zip
10/15/2011	2:53:41	..C.	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/M20M2OXX/Uniform%20traffic%20ticket[1].zip
10/15/2011	2:53:41	...B	FILE	NTFS \$MFT	/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/M20M2OXX/Uniform%20traffic%20ticket[1].zip
10/15/2011	2:55:10	.A..	FILE	NTFS \$MFT	ORPHAN/Uniform traffic ticket.exe
10/15/2011	2:55:10	M...	FILE	NTFS \$MFT	ORPHAN/Uniform traffic ticket.exe
10/15/2011	2:55:10	..C.	FILE	NTFS \$MFT	ORPHAN/Uniform traffic ticket.exe
10/15/2011	2:55:10	...B	FILE	NTFS \$MFT	ORPHAN/Uniform traffic ticket.exe
10/15/2011	2:55:13	.A..	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UNIFORM TRAFFIC TICKET.EXE-3A9408AA.pf
10/15/2011	2:55:13	M...	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UNIFORM TRAFFIC TICKET.EXE-3A9408AA.pf
10/15/2011	2:55:13	..C.	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UNIFORM TRAFFIC TICKET.EXE-3A9408AA.pf
10/15/2011	2:55:13	...B	FILE	NTFS \$MFT	/WINDOWS/Prefetch/UNIFORM TRAFFIC TICKET.EXE-3A9408AA.pf
10/15/2011	2:55:15	.A..	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings
10/15/2011	2:55:15	M...	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings
10/15/2011	2:55:15	..C.	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings
10/15/2011	2:55:15	...B	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings
10/15/2011	2:55:15	.A..	FILE	NTFS \$MFT	/Documents and Settings/All Users/Local Settings/Temp

Hunting for Malware

- Confirm file(s) are malicious
 - One Option: VirusTotal <https://www.virustotal.com/>
 - Search by hash
 - Upload and scan file (use wisely)



The screenshot shows the VirusTotal website interface. At the top is the VirusTotal logo. Below it is a description: "VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware." The main section features a file upload area with a text box containing "No file selected" and a "Choose File" button. Below this is the text "Maximum file size: 64MB". A "Scan it!" button is positioned below the upload area. At the bottom, there is a link to "search through the VirusTotal dataset". Red boxes highlight the "Choose File" button, the "Scan it!" button, and the "search through the VirusTotal dataset" link.

virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected **Choose File**

Maximum file size: 64MB

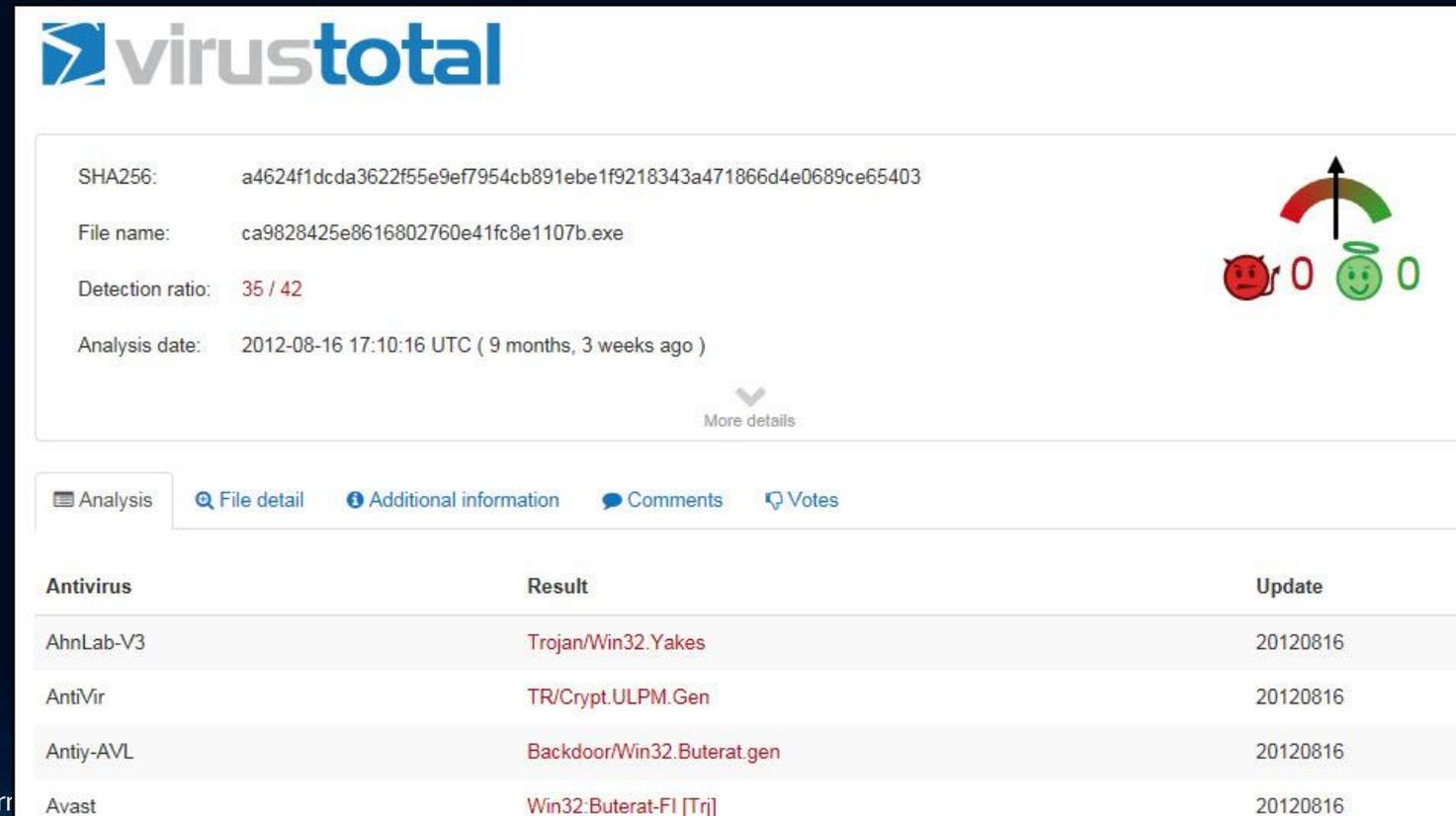
By clicking "Scan it!", you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

You may prefer to scan a URL or **search through the VirusTotal dataset**

Hunting for Malware

- Confirm file(s) are malicious
 - Uniform traffic ticket.exe results



virustotal

SHA256: a4624f1dcda3622f55e9ef7954cb891ebe1f9218343a471866d4e0689ce65403

File name: ca9828425e8616802760e41fc8e1107b.exe

Detection ratio: 35 / 42

Analysis date: 2012-08-16 17:10:16 UTC (9 months, 3 weeks ago)

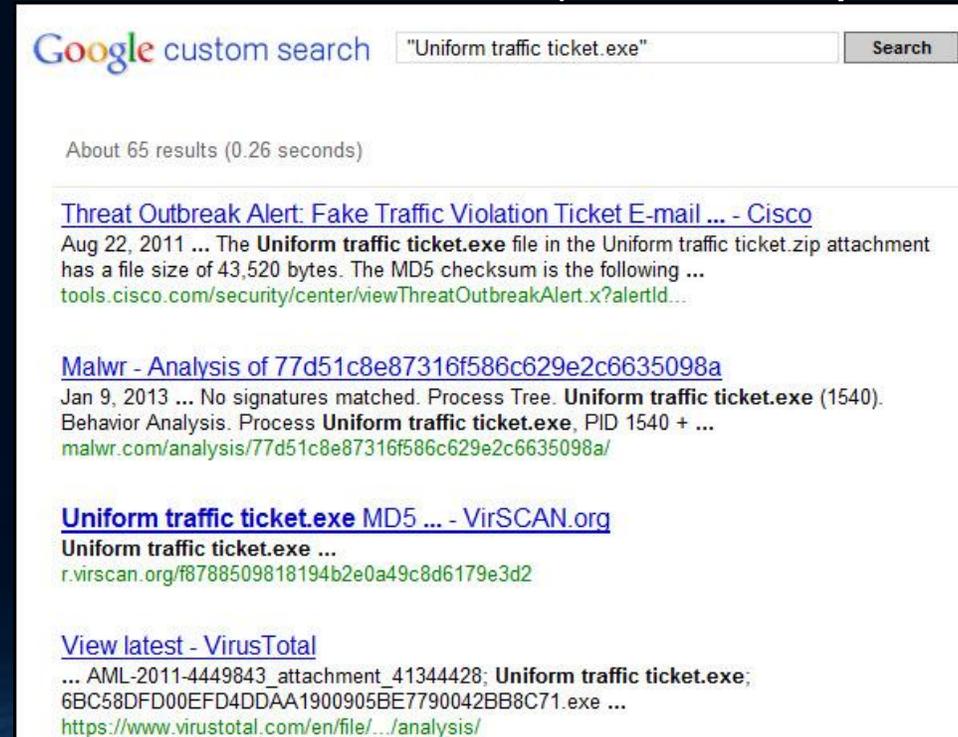
[More details](#)

Analysis | [File detail](#) | [Additional information](#) | [Comments](#) | [Votes](#)

Antivirus	Result	Update
AhnLab-V3	Trojan/Win32.Yakes	20120816
AntiVir	TR/Crypt.ULPM.Gen	20120816
Antiy-AVL	Backdoor/Win32.Buterat.gen	20120816
Avast	Win32:Buterat-FI [Trj]	20120816

Hunting for Malware

- Use Google to get more context about the attack
 - Malware Analysis Search:
<http://www.google.com/cse/home?cx=011750002002865445766:pc6ozx1rliu>
- Keyword search on attack indicators (file names, folder names, etc.)



Google custom search "Uniform traffic ticket.exe" Search

About 65 results (0.26 seconds)

[Threat Outbreak Alert: Fake Traffic Violation Ticket E-mail ... - Cisco](#)
Aug 22, 2011 ... The **Uniform traffic ticket.exe** file in the Uniform traffic ticket.zip attachment has a file size of 43,520 bytes. The MD5 checksum is the following ...
tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId...

[Malwr - Analysis of 77d51c8e87316f586c629e2c6635098a](#)
Jan 9, 2013 ... No signatures matched. Process Tree. **Uniform traffic ticket.exe** (1540). Behavior Analysis. Process **Uniform traffic ticket.exe**, PID 1540 + ...
malwr.com/analysis/77d51c8e87316f586c629e2c6635098a/

[Uniform traffic ticket.exe MD5 ... - VirSCAN.org](#)
Uniform traffic ticket.exe ...
r.virscan.org/f8788509818194b2e0a49c8d6179e3d2

[View latest - VirusTotal](#)
... AML-2011-4449843_attachment_41344428; **Uniform traffic ticket.exe**; 6BC58DFD00EFD4DDAA1900905BE7790042BB8C71.exe ...
<https://www.virustotal.com/en/file/.../analysis/>

Hunting for Malware

- Use Google to get more context about the attack

Description

Cisco Security Intelligence Operations has detected significant activity related to spam e-mail messages that claim to contain a traffic violation ticket for the recipient. The text in the message body instructs the recipient to open an attachment to view further details. However, the .zip attachment contains a malicious .exe file that, when executed, attempts to infect the system with malicious code.

E-mail messages that are related to this threat (RuleID3629, RuleID3735, and RuleID3735KVR) may contain the following files:

- Ticket.zip*
- Ticket.exe*
- Uniform traffic ticket.zip*
- Uniform traffic ticket.exe*
- uniform traffic ticket.exe*

The *Ticket.exe* file has a file size of 29,184 bytes. The MD5 checksum, which is a unique identifier of the executable, is the following string: 0x6361D4A40485345C18473F3C6B4B6609

The *Uniform traffic ticket.exe* file in the *Uniform traffic ticket.zip* attachment has a file size of 43,520 bytes. The MD5 checksum is the following string: 0xA723EE743BD5D7E4CEE9951F8A6D0C09

Hunting for Malware

What Did We Learn in Minutes?

- Is the system infected?
 - C:/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/M2oM2OXX/Uniform%2otraffic%2oticket[1].zip
 - C:/Documents and Settings/All Users/Local Settings/Temp/17f7fff4.com
 - C://Documents and Settings/Administrator/Local Settings/Temp/000c54ad.tmp
 - C://Documents and Settings/Administrator/Local Settings/Temp/pcb_build_23_smtp.exe
 - C:/Documents and Settings/Administrator/Application Data/KB961710.exe
 - C:/Documents and Settings/Administrator/Local Settings/Temp/svchost.exe
 - C:/Documents and Settings/Administrator/Local Settings/Temp/P1kAlMiG2Kb7Fz.exe.tmp
 - C:/Documents and Settings/Administrator/Local Settings/Temp/Temporary Directory 2 for Uniform%2otraffic%2oticket[1].zip/Uniform traffic ticket.exe
 - C:/Documents and Settings/Administrator/Desktop/Uniform traffic ticket.exe
- When did the infection occur?
 - Sat Oct 15 02:55:10 2011 when \DOCUME~1\ADMINI~1\LOCALS~1\TEMP\TEMPORARY DIRECTORY 1 FOR UNIFORM%20TRAFFIC%20TICKET[1].ZIP\UNIFORM TRAFFIC TICKET.EXE executed

Hunting for Malware

What Did We Learn in Minutes?

- How did the infection occur?
 - Zip archive was downloaded from the Internet and a program inside it was executed
- What was taken?
 - Have malware samples to look into and research
- Were we targeted or was it a random attack?
 - Random attack from a SPAM campaign
- What can be done to reduce future occurrences
 - Security awareness refresher to users about SPAM emails
 - Block all zips containing executables for email <- email client wasn't infection vector but could have been

Hunting for Malware

What We Would Have Learned Wiping, Re-imaging, and Redeploying

- **We can't answer any of these questions**
 - Is the system infected?
 - When did the infection occur?
 - How did the infection occur?
 - What was taken?
 - Were we targeted or was it a random attack?
 - What can be done to reduce future occurrences

The Choice Is Yours

You Can Be Like Tony Stark

Or



References

Mell, P. & Kent, K. & Nusbaum, J. (2005). *Guide to Malware Incident Prevention and Handling*. Retrieved April 30, 2013, from <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>

Goncharov, M. (2012). *Russian Underground 101*. Retrieved April 30, 2013, from <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

Ollmann, G. (2011). *Behind Today's Crimeware Installation Lifecycle: How Advanced Malware Morphs to Remain Stealthy and Persistent*. Retrieved May 01, 2013, from https://www.damballa.com/downloads/r_pubs/WP_Advanced_Malware_Install_LifeCycle.pdf

Harrell, C. (2013). *Journey into IR Methodology*. Retrieved May 03, 2013, from <http://journeyintoir.blogspot.com/p/journey-into-ir-methodology.html>

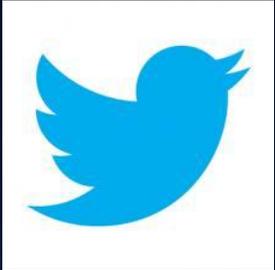
References

Davis, A. (2012). *Leveraging the Application Compatibility Cache in Forensic Investigations*. Retrieved May 01, 2013, from <https://www.mandiant.com/blog/leveraging-application-compatibility-cache-forensic-investigations/>

Carvey, H. (2011). *Windows Registry Forensics*. Elsevier: Burlington.

Iron Man Anime Series Season 1, Ep. 6 "Technical Difficulties". (2013). Retrieved March 2013, from <https://itunes.apple.com/us/tv-season/iron-man-anime-series-season-1/id449452770>

Contact Info



@corey_harrell



<http://journeyintoir.blogspot.com>



charrell[at]osc.state.ny.us

