Malware Root Cause Analysis

Don’t Be a Bone Head

Corey Harrell
NY Office of the State Comptroller

The Situation

Every day computers are used to conduct business and then ….

BONES

Agenda

- Finding Malware Like Iron Man Recap
- Why Root Cause Analysis
- Don’t Be A Bone Head
- Compromise Root Cause Analysis Model
- Malware Root Cause Analysis in Action
- Conclusion

C:\>whoami.exe /priv

- Author “Journey Into Incident Response” Blog
- Developed & Teach Malware Analysis Curriculum, Champlain College
- Masters of Science in Information Assurance (MSIA)
- Bachelors of Science in Telecommunications
- Certified Ethical Hacker (CEH)

- DFIR 6 yrs >> InfoSec 8 yrs >> IT 10+ yrs
  - **Current Work: Incident Response (Response) & SIEM (Detection)**
  - Previous Work: Forensics Support for Incident Response
  - Previous Work: Network Penetration Testing Against NYS Agencies

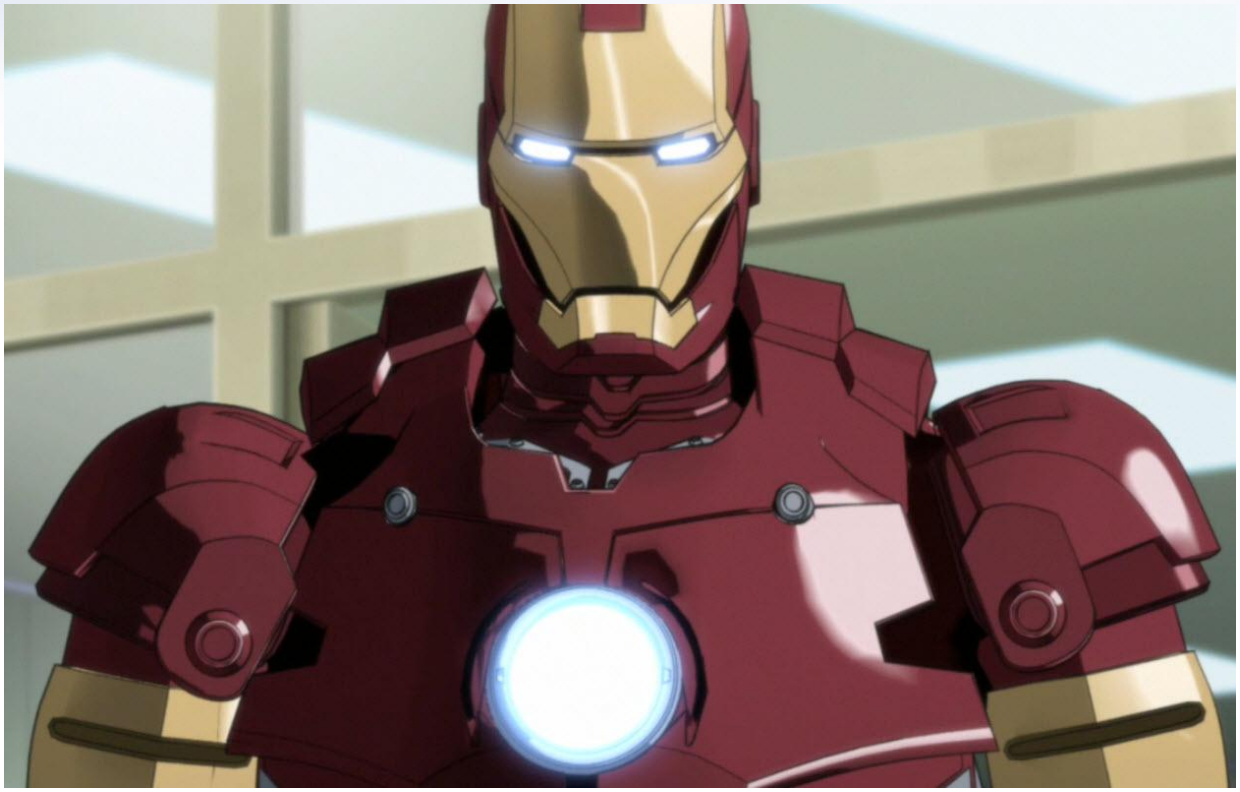
FINDING MALWARE LIKE IRON MAN RECAP

Finding Malware Like Iron Man

Last Year - Malware Is a Tool in a Threat's Hands

Finding Malware Like Iron Man

- Malware Forensics Triage Technique



Finding Malware Like Iron Man Slide Decks

http://journeyintoir.blogspot.com/2013/07/finding-malware-like-iron-man-slide.html

Finding Malware Like Iron Man

Malware Indicators 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

Focus for Root Cause Analysis

Finding Malware Like Iron Man

Triage Examination Steps

- 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)

Focus for Root Cause Analysis

Finding Malware Like Iron Man

- Proven Technique To Locate Malware Fast
  - All malware dropped onto a system
  - **Even Hollywood uses the technique!!!!**

- Let's see how it worked for the Bones "Geeks"

WHY ROOT CAUSE ANALYSIS

What is Root Cause Analysis

- Defined

A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks

("Managing Information," 2011)

Why Root Cause Analysis

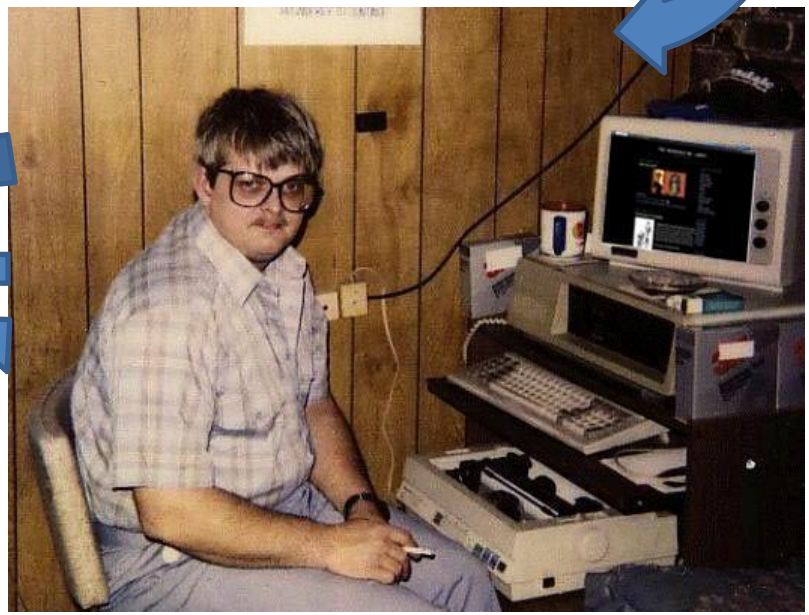
- Common Approach #1

symantec.

McAfee®

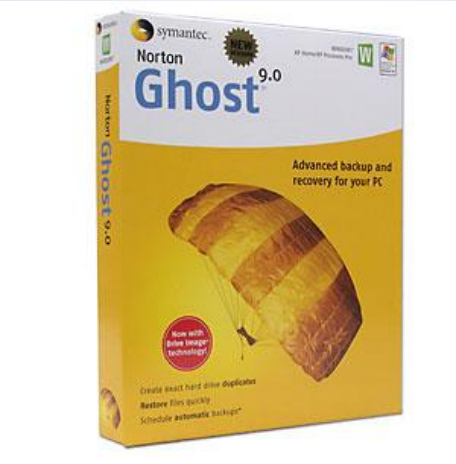
avast!®

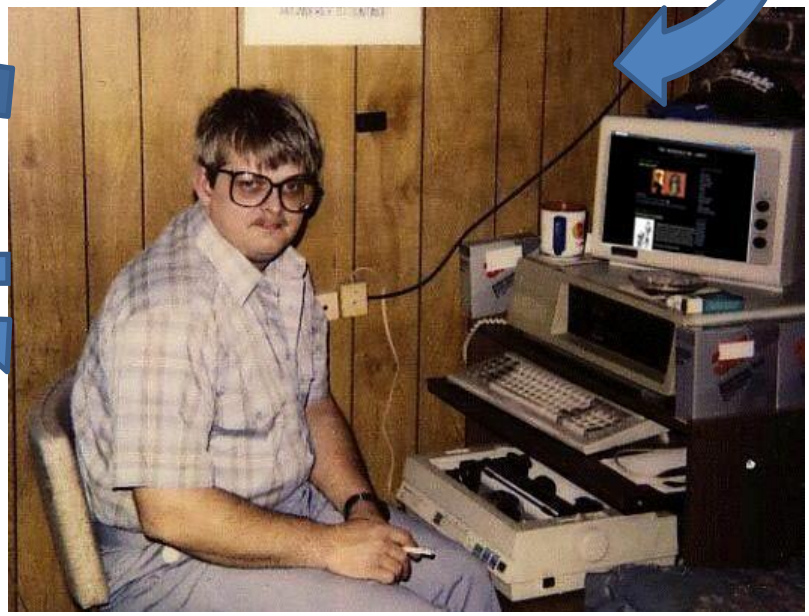
Malwarebytes



Why Root Cause Analysis

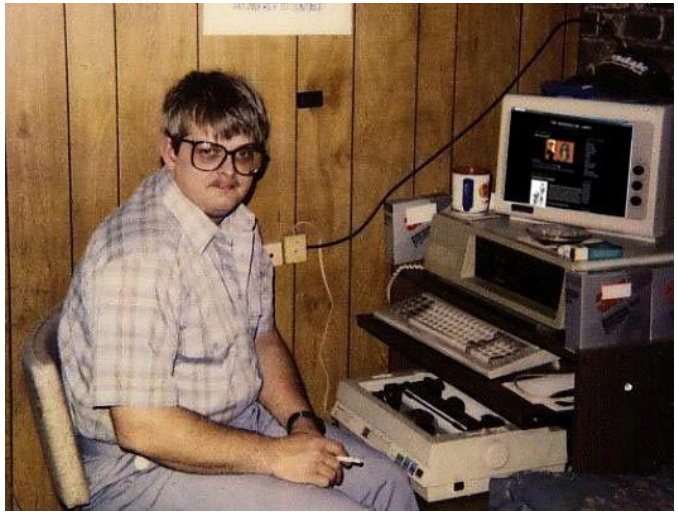
- Common Approach #2





Why Root Cause Analysis

- Didn't Solve the Problem
  - **Only Solved the Symptom**



Why Root Cause Analysis

"First, **prevention and preventative security controls** will fail"

"look at antivirus tools and contrast their 99%-plus deployment rates with widespread ongoing malware infection rates"

(Chuvakin, 2013)

Why Root Cause Analysis

Reason

To determine “HOW” threats are compromising us

Knowing the “how” lets us address the <u>underlying causes</u>

DON’T BE A BONE HEAD

Don’t Be A Bone Head

- How Not To Do Root Cause Analysis

Don’t Be A Bone Head

One day I was using my computer when

While I was drinking

Didn’t Guess

Analyzed the Data and Not the Coffee Cup

Don’t Be A Bone Head

Listen to Those Who Analyze the Data!!!!

US agency baffled by modern technology, destroys mice to get rid of viruses

$170,000 of PCs, printers, keyboards, cameras, and mice destroyed in gross overreaction.

by **Peter Bright** - July 8 2013, 7:00pm EDT

CYBERWAR | HARDENING | 269

Don’t Be A Bone Head

Listen to Those Who Analyze the Data!!!!

EDA's CIO, fearing that the agency was under attack from a nation-state, insisted instead on a policy of physical destruction. The EDA destroyed not only (uninfected) desktop computers but also printers, cameras, keyboards, and even *mice*. The destruction only stopped—sparing $3 million of equipment—because the agency had run out of money to pay for destroying the hardware.

The total cost to the taxpayer of this incident was $2.7 million: $823,000 went to the security contractor for its investigation and advice, $1,061,000 for the acquisition of temporary infrastructure (requisitioned from the Census Bureau), $4,300 to destroy $170,500 in IT equipment, and $688,000 paid to contractors to assist in development of a long-term response. Full recovery took close to a year.

Don't Be A Bone Head

Stop, Preserve, and Then Analyze The Data!!!

17 FEB 10

'Time Bomb' May Have Destroyed 800 Norfolk City PCs

The City of Norfolk, Virginia is reeling from a massive computer meltdown in which an unidentified family of malicious code destroyed data on nearly 800 computers citywide. The incident is still under investigation, but city officials say the attack may have been the result of a computer time bomb planted in advance by an insider or employee and designed to trigger at a specific date.

Don’t Be A Bone Head

Stop, Preserve, and Then Analyze The Data!!!

IT specialists for the city found that the system serving as the distribution point for the malware within the city’s network was a print server that handles printing jobs for Norfolk City Hall. However, an exact copy of the malware on that server may never be recovered, as city computer technicians quickly isolated and rebuilt the offending print server.

“Obviously, our first reaction was to shut it down and restore services, and at least initially we weren’t concerned about capturing [the malware] or setting it aside,” Cluff said.

COMPROMISE ROOT CAUSE ANALYSIS MODEL

Compromise Root Cause Analysis Model

- Attack Vector Definition

"a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome"

(Attack, 2010)

- Has three parts
  - The path or means is the exploit used
  - The payload is the outcome of the exploit
  - The delivery mechanism is how the exploit/payload is sent to target

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

Source

- Is where the attack originated from
  - From your company's perspective
  - Attacks can originate from outside/inside company
  - External source is anything outside your company

- Examples for Malware
  - Malicious websites
  - Malicious advertisements on websites
  - Email phishing attack
  - Employee planting backdoor

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

1st Delivery Mechanism

- Sends the exploit to the network or system

- Methods for Malware
  - Internet
  - Email
  - Network services
  - Removable media
  - Physical access

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

Exploit

- Something that takes advantage of a vulnerability
  - Vulnerability is a weakness or flaw
  - Present in operating systems, applications or human

- Methods for Malware
  - Client side software
  - Removable media
  - Network shares
  - Social engineering

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

2nd Delivery Mechanism

- Sends the payload to the network or system
  - Exploit may result in a payload being sent the system
  - Not always present
- Methods for Malware
  - Internet
  - Network services
  - Removable media

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

Payload

- Payload or malicious outcome to network/system
  - Actions ranging from:
    - unauthorized access
    - denial of service
    - remote code execution
    - Privileges
- Examples for Malware
  - Data stealing Trojans
  - Remote Access Trojans

Compromise Root Cause Analysis Model

Compromise Root Cause Analysis Model

Indicators

- Everything that occurs after the initial compromise
  - All post compromise activity
  - Activity for detection and response

- Examples for Malware
  - Downloading files
  - Malware executing
  - Network traversal
  - Data exfiltration

MALWARE ROOT CAUSE ANALYSIS IN ACTION

Malware Root Cause Analysis in Action

How to use the Compromise RCA Model

- During analysis you organize information/artifacts
  - Artifacts are discovered through analyzing the data!!!
  - Objective is to identify: exploit, payload, delivery mechanisms
    - Key: look for when malware activity first started
    - Key: look for exploit artifacts to identify payload and source

- Documented Example
  - Harrell, C. (2012). Malware Root Cause Analysis. Retrieved from http://journeyintoir.blogspot.com/2012/07/malware-root-cause-analysis.html

Malware Root Cause Analysis in Action

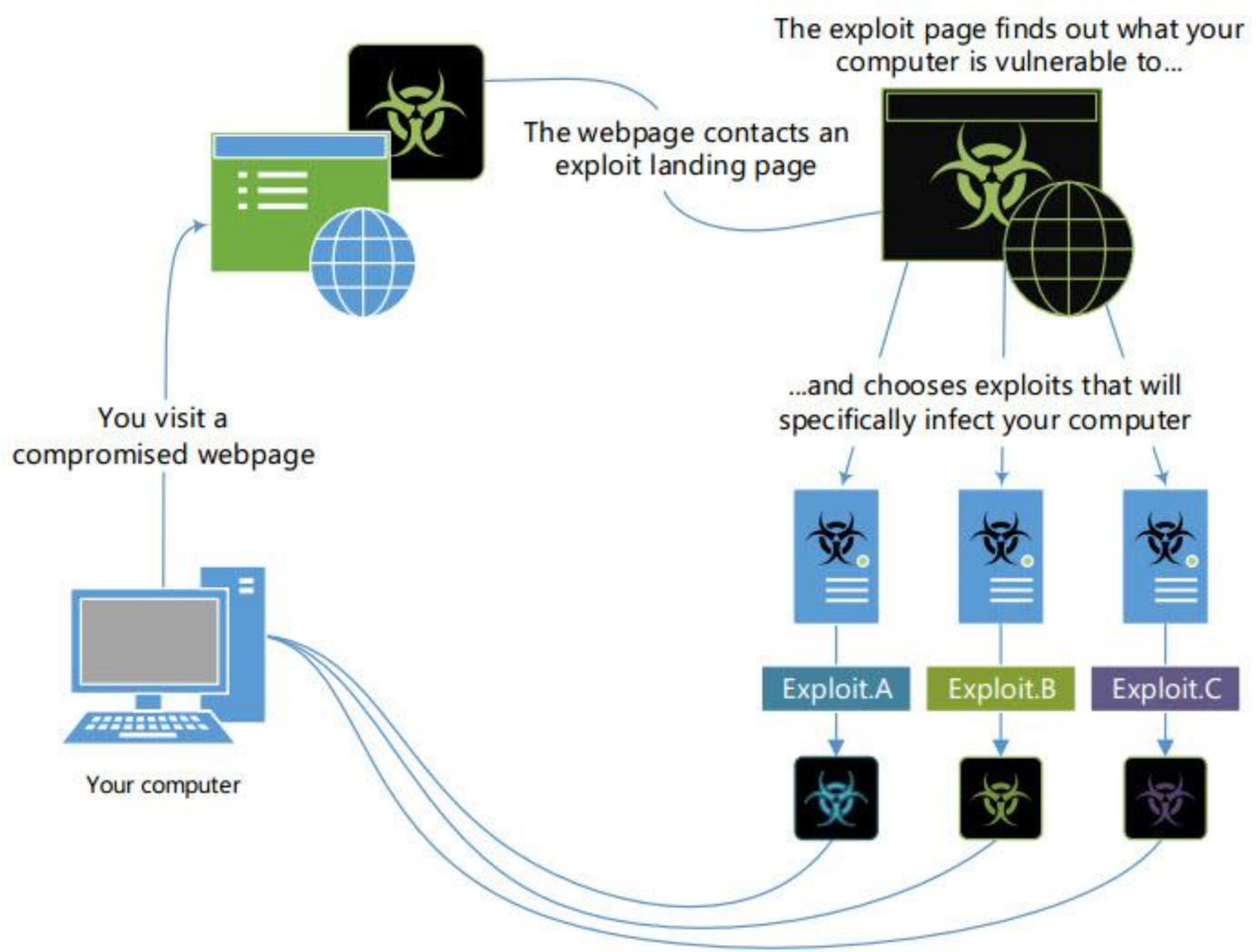
Compromise RCA Model for Common Attack

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	

(ENISA, 2013)

Malware Root Cause Analysis in Action

Attack Vector Artifacts for Drive-by



Malware Root Cause Analysis in Action

Indicators

- IDS alert for system with data stealing Trojan
- Prefetch files identify malware

Filename	Last Run Time	Process Path
SILVERLIGHT.CONFIG...	5/11/2014 1:45:59 AM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT SILVERLIGHT\5.0.61118.0\SILVERLIGHT
AGCP.EXE-4FC06263.pf	5/11/2014 1:46:00 AM	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT SILVERLIGHT\5.0.61118.0\AGCP.EXE
0320.DLL-FF63DE02.pf	5/11/2014 1:46:02 AM	\DEVICE\HARDDISKVOLUME1\USERS\LAB\APPDATA\LOCAL\TEMP\0320.DLL

Filename	Full Path	Device Path
SATTECH.DLL		\DEVICE\HARDDISKVOLUME1\USERS\LAB\APPDATA\LOCAL\SATTECH.DLL
0320.DLL		\DEVICE\HARDDISKVOLUME1\USERS\LAB\APPDATA\LOCAL\TEMP\0320.DLL

Malware Root Cause Analysis in Action

Indicators

- $MFT Timeline show

date	time	MACB	sourcetype	desc
5/11/2014	1:46:02	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\0320.dll
5/11/2014	1:46:04	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local
5/11/2014	1:46:04	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\sattech.dll
5/11/2014	1:46:11	MACB	NTFS$MFT	[root]\Windows\Prefetch\SILVERLIGHT.CONFIGURATION.EXE-CB2726E3.pf
5/11/2014	1:46:11	MACB	NTFS$MFT	[root]\Windows\Prefetch\AGCP.EXE-4FC06263.pf
5/11/2014	1:46:12	MACB	NTFS$MFT	[root]\Windows\Prefetch\0320.DLL-FF63DE02.pf
5/11/2014	1:46:13	M.C.	NTFS$MFT	[root]\Windows\Prefetch\SPPSVC.EXE-CBE91656.pf
5/11/2014	1:46:13	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\WuRedir\7971F918-A847-4430-9279
5/11/2014	1:46:13	.A..	NTFS$MFT	[root]\Windows\SoftwareDistribution\Download\c3248eb572cb5f82e63ce
5/11/2014	1:46:14	M.C.	NTFS$MFT	[root]\Windows\SoftwareDistribution\Download\c3248eb572cb5f82e63ce
5/11/2014	1:46:15	M.C.	NTFS$MFT	[root]\Users\lab\AppData\LocalLow\Microsoft\Silverlight\mssl.lck

Timezone is UTC

Malware Root Cause Analysis in Action

Payload

- Payload is the Trojans

date	time	MACB	sourcetype	desc
5/11/2014	1:46:02	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\0320.dll
5/11/2014	1:46:04	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local
5/11/2014	1:46:04	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\sattech.dll

Timezone is UTC

Malware Root Cause Analysis in Action

2nd Delivery Mechanism

- Unknown
  - To confirm need to reverse the exploit

date	time	MACB	sourcetype	desc
5/11/2014	1:46:00	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W
5/11/2014	1:46:00	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\f
5/11/2014	1:46:00	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\f
5/11/2014	1:46:01	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\AuthCabs
5/11/2014	1:46:01	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\WuRedir\9482F4B4-E343-43B6-B170-9A65BC822C77
5/11/2014	1:46:01	..C.	NTFS$MFT	[root]\Windows\SoftwareDistribution\AuthCabs\authcab.cab
5/11/2014	1:46:02	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\0320.dll
5/11/2014	1:46:04	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local
5/11/2014	1:46:04	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\sattech.dll

Timezone is UTC

Malware Root Cause Analysis in Action

Exploit

- Exploits leave the same artifacts on systems
  - Artifacts can confirm or eliminate attack methods
- Silverlight was identified
  - Areas to look for possible artifacts
    - Temporary File Creation
    - Indications of the Vulnerable Application Executing
    - Internet Activity

Malware Root Cause Analysis in Action

Temporary File Creation

- **Webpage created in a temporary Internet files storage location**
  - contains the code to load the Silverlight application exploit
  - C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<randon folder>

Malware Root Cause Analysis in Action

Indications of the Vulnerable Application Executing

- **Folder activity involving the Silverlight application**
  - C:\Users\<username>\AppData\LocalLow\Microsoft\Silverlight
- **File creation inside the Silverlight application folder**
  - C:\Users\<username>\AppData\LocalLow\Microsoft\Silverlight\filename.tmp
  - C:\Users\<username>\AppData\LocalLow\Microsoft\Silverlight\mssl.lck
- **References to Silverlight programs in prefetch files**
  - including CONHOST.EXE's prefetch file handles

Malware Root Cause Analysis in Action

Internet Activity

- **Web browser history of user accessing websites within the timeframe of interest**
- **Files located in the browser cache folder**
  - C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

Malware Root Cause Analysis in Action

Exploit

- Re-examining program execution artifacts
  - Vulnerable application executing in prefetch files

Filename	Last Run Time
SILVERLIGHT.CONFIGURATION.EXE-CB2726E3.pf	5/11/2014 1:45:59 AM
AGCP.EXE-4FC06263.pf	5/11/2014 1:46:00 AM
0320.DLL-FF63DE02.pf	5/11/2014 1:46:02 AM
SPPSVC.EXE-CBE91656.pf	5/11/2014 1:46:02 AM
VSSVC.EXE-04D079CC.pf	5/11/2014 1:46:31 AM
SVCHOST.EXE-8FD92526.pf	5/11/2014 1:46:32 AM
WUAUCLT.EXE-830BCC14.pf	5/11/2014 1:46:35 AM
SILVERLIGHT_DEVELOPER.EXE-49608895.pf	5/11/2014 1:46:36 AM
INSTALL.EXE-0C3D3F29.pf	5/11/2014 1:46:38 AM
MSIEXEC.EXE-B5AFA339.pf	5/11/2014 1:46:38 AM
MSI9594.TMP-5CBF123E.pf	5/11/2014 1:46:39 AM
MSI99CC.TMP-793BA93F.pf	5/11/2014 1:46:40 AM
COREGEN.EXE-EB498EB3.pf	5/11/2014 1:46:40 AM
CONHOST.EXE-3218E401.pf	5/11/2014 1:46:40 AM

Malware Root Cause Analysis in Action

Exploit

- Re-examining program execution artifacts
  - Vulnerable application executing in prefetch files

CONHOST.EXE-3218E401.pf	5/11/2014 1:46:40 AM	12/6/2012 5:18:28 PM	5/11/2014 1:46:40 AM

Filename	Device Path
COREGEN.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT SILVERLIGHT\5.0.61118.0\COREGEN.EXE
DEFRAG.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DEFRAG.EXE
DWMAPI.DLL	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DWMAPI.DLL

Malware Root Cause Analysis in Action

Exploit

- Re-examining system activity in timeline
  - Vulnerable application executing (file creation)

date	time	MACB	sourcetype	desc
5/11/2014	1:46:02	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\0320.dll
5/11/2014	1:46:04	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local
5/11/2014	1:46:04	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\sattech.dll
5/11/2014	1:46:11	MACB	NTFS$MFT	[root]\Windows\Prefetch\SILVERLIGHT.CONFIGURATION.EXE-CB2726E3.pf
5/11/2014	1:46:11	MACB	NTFS$MFT	[root]\Windows\Prefetch\AGCP.EXE-4FC06263.pf
5/11/2014	1:46:12	MACB	NTFS$MFT	[root]\Windows\Prefetch\0320.DLL-FF63DE02.pf
5/11/2014	1:46:13	M.C.	NTFS$MFT	[root]\Windows\Prefetch\SPPSVC.EXE-CBE91656.pf
5/11/2014	1:46:13	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\WuRedir\7971F918-A847-4430-9279
5/11/2014	1:46:13	.A..	NTFS$MFT	[root]\Windows\SoftwareDistribution\Download\c3248eb572cb5f82e63ce
5/11/2014	1:46:14	M.C.	NTFS$MFT	[root]\Windows\SoftwareDistribution\Download\c3248eb572cb5f82e63ce
5/11/2014	1:46:15	M.C.	NTFS$MFT	[root]\Users\lab\AppData\LocalLow\Microsoft\Silverlight\mssl.lck

Timezone is UTC

Malware Root Cause Analysis in Action

Exploit

- Examining system activity in timeline
  - Vulnerable application executing (folder activity)

date	time	MACB	sourcetype	desc
5/11/2014	1:46:44	.AC.	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\uk\Microsoft.V
5/11/2014	1:46:44	.AC.	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\vi\Microsoft.V
5/11/2014	1:46:48	.A.B	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\mscorlib.ni.dll
5/11/2014	1:46:48	M.C.	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\mscorlib.ni.dll
5/11/2014	1:46:48	MACB	NTFS$MFT	[root]\Windows\Prefetch\WUAUCLT.EXE-830BCC14.pf
5/11/2014	1:46:48	MACB	NTFS$MFT	[root]\Windows\Prefetch\SILVERLIGHT_DEVELOPER.EXE-49608895.pf
5/11/2014	1:46:48	.A.B	NTFS$MFT	[root]\Windows\Prefetch\COREGEN.EXE-6AFEB42D.pf
5/11/2014	1:46:48	.A.B	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\System.ni.dll
5/11/2014	1:46:48	M.C.	NTFS$MFT	[root]\Program Files\Microsoft Silverlight\5.1.30214.0\System.ni.dll

Timezone is UTC

Malware Root Cause Analysis in Action

1st Delivery Mechanism

- Delivery methods leave the same artifacts on systems
  - Artifacts can confirm or eliminate attack methods
- Internet Explorer was identified
  - Area to look for possible artifacts
    - Internet Activity

Malware Root Cause Analysis in Action

Internet Activity

- **Web browser history of user accessing websites within the timeframe of interest**
- **Files located in the browser cache folder**
  - C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\
  - C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low

Malware Root Cause Analysis in Action

Internet Activity

- **Files located in the cookie folder**
  - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies
  - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies\Low

Malware Root Cause Analysis in Action

1st Delivery Mechanism

- Examining system activity in timeline
  - Internet activity (file and folder activity for browser)

date	time	MACB	sourcetype	desc
5/11/2014	1:46:00	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W
5/11/2014	1:46:00	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\fa
5/11/2014	1:46:00	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\fa
5/11/2014	1:46:01	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\AuthCabs
5/11/2014	1:46:01	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\WuRedir\9482F4B4-E343-43B6-B170-9A65BC822C77
5/11/2014	1:46:01	..C.	NTFS$MFT	[root]\Windows\SoftwareDistribution\AuthCabs\authcab.cab
5/11/2014	1:46:02	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\0320.dll
5/11/2014	1:46:04	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local
5/11/2014	1:46:04	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\sattech.dll

Timezone is UTC

Malware Root Cause Analysis in Action

1st Delivery Mechanism

- Examining system activity in timeline
  - Internet activity (file and folder activity for browser)

date	time	MACB	sourcetype	desc
5/11/2014	1:45:59	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\AIAI0AXH\v[3].gif
5/11/2014	1:45:59	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\8fdhe54wg1[1].htm
5/11/2014	1:45:59	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\KV3GY8BO\300x600[1].jpg
5/11/2014	1:45:59	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\AIAI0AXH\stripe[1].png
5/11/2014	1:46:00	..C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012014051020140511
5/11/2014	1:46:00	..C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012014051020140511\index.dat
5/11/2014	1:46:00	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\8fdhe54wg1[1].htm

Timezone is UTC

Malware Root Cause Analysis in Action

1st Delivery Mechanism

- Examining system activity in timeline
  - Internet activity (file and folder activity for browser)

date	time	MACB	sourcetype	desc
5/11/2014	1:45:55	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\freshdekor_com[1]
5/11/2014	1:45:55	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\style[5].css
5/11/2014	1:45:55	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\freshdekor_com[1]
5/11/2014	1:45:55	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\I87XK24W\style[5].css
5/11/2014	1:45:56	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CIJUICXX\css[1].css
5/11/2014	1:45:56	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\KV3GY8BO\ie9[1].css
5/11/2014	1:45:56	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\AIAI0AXH\shortcodes[1].css
5/11/2014	1:45:56	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\AIAI0AXH\shortcodes[1].css

Timezone is UTC

Malware Root Cause Analysis in Action

Source

- Internet

Artifacts

- Cached compromised or malicious webpage
  - Internet Explorer
    - C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 \random_folder

Malware Root Cause Analysis in Action

Source

8fdhe54wg1[1].htm 105

Menu Search

Pass cluster some

- Teem tishnailo.net
- Search the Web

- Products

-

Malware Root Cause Analysis in Action

Source

8fdhe54wg1[1].htm 105 Regular File 5/11/2014 1:45

```
<script>
var nHsYwVOyi; function oJoVJW($gc1m){ var ho2=
     {
}  ,ZqP,IbptOD=          [],FBIX5=
 ""+'mCha'+'rCo',XnZvi,MEv= "",D6=
    $gc1m.length,Kam2tI=
   0,sRybz,qqtEXQ,rx=
0,s4m=
43,Cr9Nm=
 [s4m,s4m+1],s4m=
s4m+4,KUjvS=

'rCod',ch=
'cha',SK=       [s4m, ++s4m],Qi$3=
[s4m,s4m+10],s4m=
s4m+17,GhThT=           [s4m,s4m+26],s4m=     s4m+32,CE=
[s4m,s4m+26],OvgsV=
String['fro'+FBIX5+'de'],UZNGE=
```

Malware Root Cause Analysis in Action

Source

freshdekor_com[1] 38 Regular File 5/11/2014 1:45:...

Möbel | Architecture | Dekorationsideen | Landschaftsdesign | Moderne Innendekoration | Wohnaccessoires | Dekoration | Search...

FRESH DEKOR.COM

Küchenarbeitsplatten – Pflegetipps und Materialkunde

April 28, 2014 Comments Off

Küchenarbeitsplatten – Pflegetipps und Materialkunde Die Arbeitsplatte in der Küche wird täglich stark

Malware Root Cause Analysis in Action

Source

```
<script type="text/javascript">
<!--
d=document;d.write('<a href="http://www.tyxo.bg/?143555" title="Tyxo.bg counter"><img
width="1" height="1" border="0" alt="Tyxo.bg counter"
src="'+location.protocol+'//cnt.tyxo.bg/143555?rnd='+Math.round(Math.random()*2147483647));
d.write('&sp='+screen.width+'x'+screen.height+'&r='+escape(d.referrer)+'"></a>');
//-->
</script><noscript><a href="http://www.tyxo.bg/?143555" title="Tyxo.bg counter"><img src="
http://cnt.tyxo.bg/143555" width="1" height="1" border="0" alt="Tyxo.bg counter"
/></a></noscript>
<!-- KRAI NA TYXO.BG BROYACH -->
</html>
<!-- Dynamic page generated in 12.422 seconds. -->
<!-- Cached page generated by WP-Super-Cache on 2014-05-11 01:44:07 -->
```

Indicators

- IDS alert

Payload

- 0320.dll created in temp folder
- sattech.dl created in temp folder

2nd Delivery Mechanism

- Unknown

Exploit

- SILVERLIGHT.CONFIGURATION.EXE executed
- mssl.lck created in the Silverlight folder
- Activity for "Program Files\Microsoft Silverlight" folder

1st Delivery Mechanism

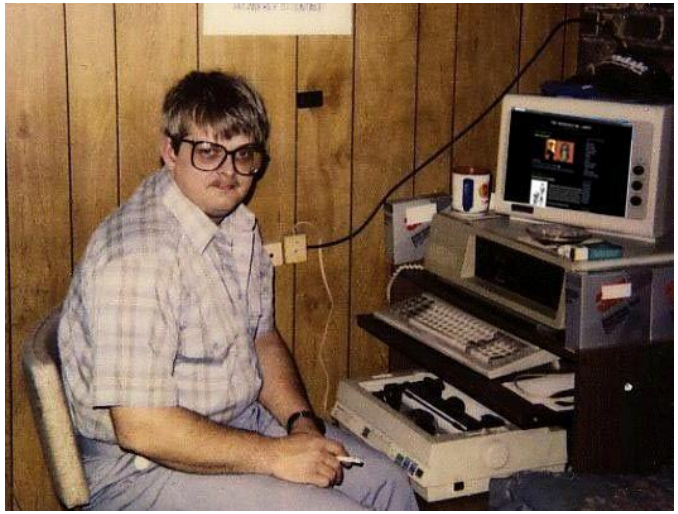
- Files created in the Temporary Internet Files

Source

- Suspicious webpage 8fdhe54wg1[1].htm
- Suspicious webpage freshdekor_com[1]

Malware Root Cause Analysis in Action

- Didn't Solve the Problem
  - **Only Solved the Symptom**



Malware Root Cause Analysis in Action

- This is What Needs to Be Solved

5/21/2014
09:30 AM

Mathew J. Schwartz
News

Microsoft Silverlight Exploit Kit Attacks Spike

While crimeware authors continue gunning for outdated plug-ins, researchers report that businesses are finding and stopping related intrusions more quickly.

Beware a surge in attacks that target outdated versions of the Microsoft Silverlight plug-in.

TIME TO WIN SOME CANDY

Spot the Root Cause #1

- Program execution (prefetch files) revealed

Filename	Last Run Time	Process Path
INVOICE.83842.EXE-25880C7B.pf	1/16/2014 12:32:14 AM	\DEVICE\HARDDISKVOLUME1\USERS\LAB\APPDATA\LOCAL\TEMP\TEMP1_INVOICE.83842[1].ZIP\INVOICE.83842.EXE

Spot the Root Cause #1

date	time	MACB	sourcetype	desc
1/16/2014	0:31:42	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Roaming\Microsoft\Windows\Cookies\Low\lab@mail.yahoo[1].txt
1/16/2014	0:31:42	.A.B	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YX44XJ5H\invoice.83842[1].zip
1/16/2014	0:31:43	MACB	NTFS$MFT	[root]\ProgramData\Microsoft\Windows Defender\IMpService925A3ACA-C353-458A-AC8D-A7E5EB378092.lock
1/16/2014	0:31:43	M.C.	NTFS$MFT	[root]\ProgramData\Microsoft\Windows Defender\Support\MPLog-07132009-215552.log
1/16/2014	0:31:44	MAC.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\WER\ERC
1/16/2014	0:31:45	MAC.	NTFS$MFT	[root]\Windows\SoftwareDistribution\DataStore\Logs
1/16/2014	0:31:45	MACB	NTFS$MFT	[root]\Windows\SoftwareDistribution\DataStore\Logs\tmp.edb
1/16/2014	0:31:47	M.C.	NTFS$MFT	[root]\Users\lab\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YX44XJ5H\invoice.83842[1].zip
1/16/2014	0:31:49	M...	NTFS$MFT	[root]\Windows\Prefetch\SPPSVC.EXE-CBE91656.pf
1/16/2014	0:31:50	M...	NTFS$MFT	[root]\Windows\Prefetch\SVCHOST.EXE-18D06B2E.pf
1/16/2014	0:32:13	MACB	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\Temp1_invoice.83842[1].zip
1/16/2014	0:32:13	M...	NTFS$MFT	[root]\Users\lab\AppData\Local\Temp\Temp1_invoice.83842[1].zip\invoice.83842.exe

Timezone is UTC

Spot the Root Cause #2

- Program execution (shim cache) revealed

```
C:\Users\anon\AppData\Local\Temp\N0Hz98kc64ZOzj.exe
  LastModTime: Fri Apr 20 20:44:29 2012 Z

C:\Windows\system32\wbem\wmiprvse.exe
  LastModTime: Sat Nov 20 12:17:55 2010 Z

C:\ProgramData\VHuvoNRQPlUqRK.exe
  LastModTime: Fri Apr 20 20:41:10 2012 Z

C:\Windows\system32\regsvr32.exe
  LastModTime: Tue Jul 14 01:14:30 2009 Z

C:\Users\anon\AppData\Local\Temp\0.11512169499856473h7i.exe
  LastModTime: Fri Apr 20 20:41:10 2012 Z
```

Spot the Root Cause #2

date	time	MACB	sourcetype	desc
4/20/2012	20:41:08	M...	NTFS$MFT	[root]\Users\anon\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\P5WPQWPX\hqdefault[1].jpg
4/20/2012	20:41:08	.A.B	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5\10874ac5-7334b734.idx
4/20/2012	20:41:08	.A.B	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39\36158da7-67c256c0.idx
4/20/2012	20:41:08	.A.B	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39\36158da7-67c256c0
4/20/2012	20:41:08	.A.B	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5\10874ac5-7334b734
4/20/2012	20:41:08	M...	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5\10874ac5-7334b734
4/20/2012	20:41:08	MA..	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5
4/20/2012	20:41:08	M...	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39\36158da7-67c256c0
4/20/2012	20:41:08	MA..	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39
4/20/2012	20:41:08	M...	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\39\36158da7-67c256c0.idx
4/20/2012	20:41:08	M...	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\5\10874ac5-7334b734.idx
4/20/2012	20:41:09	M...	NTFS$MFT	[root]\Users\anon\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\lastAccessed
4/20/2012	20:41:10	M.C.	NTFS$MFT	[root]\ProgramData\VHuvoNRQPlUqRK.exe
4/20/2012	20:41:11	M...	NTFS$MFT	[root]\Windows\Prefetch\JAVA.EXE-E27B75C2.pf
4/20/2012	20:41:14	.A.B	NTFS$MFT	[root]\Users\anon\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XTC12EJN\products[1].htm

Timezone is UTC

CONCLUSION

Remember the two benefits of failure.

First, if you do fail, you learn what doesn't work; and

second, the failure gives you the **opportunity to try a new approach**.

~ Roger Von Oech

References

- Harrell, C. (2013). *Journey into IR Methodology*. Retrieved from http://journeyintoir.blogspot.com/p/journey-into-ir-methodology.html
- Chuvakin, A. (2013). *Security Incident Response in the Age of APT*. Retrieved from https://www.gartner.com/doc/2596322/security-incident-response-age-apt
- *Attack Vector*. (2010). Retrieved from http://searchsecurity.techtarget.com/definition/attack-vector
- Enisa. (2013). *ENISA Threat Landscape*. Retrieved from http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISAThreatLandscape

References

- *Microsoft Security Intelligence Report: Featured Intelligence*. (2014). Retrieved from http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_Exploitation_Trends_English.pdf
- Harrell, C. (2014). *CVE 2013-0074 & 3896 Silverlight Exploit Artifacts*. Retrieved from http://journeyintoir.blogspot.com/2014/05/cve-2013-0074-3896-silverlight-exploit.html
- Schwartz, M. (2014). *Microsoft Silverlight Exploit Kit Attacks Spike*. Retrieved from http://www.darkreading.com/attacks-breaches/microsoft-silverlight-exploit-kit-attacks-spike/d/d-id/1269073

References

- Harrell, C. (2012). *Compromise Root Cause Analysis Model*. Retrieved from http://journeyintoir.blogspot.com/2012/06/compromise-root-cause-analysis-model.html
- Harrell, C. (2010). *Attack Vector Artifacts*. Retrieved from http://journeyintoir.blogspot.com/2010/11/attack-vector-artifacts.html
- *Managing Information Security Risk*. (2011). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

C:\>dsquery user -name "corey"| dsget user -samid -email -display

@corey_harrell

http://journeyintoir.blogspot.com

charrell[at]osc.state.ny.us

QUESTIONS?