Forging Forensic Fortifications

Andrew Hay, Co-Founder and CTO, LEO Cyber Security
+1.415.940.9660
andrew.hay@leocybersecurity.com
www.leocybersecurity.com
@andrewsmhay
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Why Forge Fortifications For Forensics?</td>
<td>2</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>3</td>
</tr>
<tr>
<td>Tools That Add Value</td>
<td>4</td>
</tr>
<tr>
<td>Summary</td>
<td>5</td>
</tr>
</tbody>
</table>
About Me

- Chief Technology Officer (CTO) @ LEO Cyber Security
- Former:
  - CISO @ DataGravity
  - Director of Research @ OpenDNS
  - Chief Evangelist & Director of Research @ CloudPassage
  - Senior Security Analyst @ 451 Research
  - Sr. Security Analyst in higher education and a bank in Bermuda
- Blogger, author, and rugby coach
Why Forge Fortifications For Forensics?

Introduction

Configuration Settings

Tools That Add Value

Summary
MTTR is King

• Mean Time To Resolution (MTTR) is a great starting point when you’re looking to cut incident resolution times from hours to minutes

• How much dwell time is there between STEP 3 and STEP 5?
• What’s the typical hold up?
On average, how much time elapsed between the initial compromise and detection (i.e., the dwell time)? How long from detection to remediation?
SANS 2017 IR Survey

On average, how much time elapsed between containment and remediation?

- 82% reported that remediation activities take place within one month of containment
- 33% performing these activities within 24 hours
- But we can help DFIR teams do better!

Digital forensics and incident response (DFIR) is a delicate and intricate process.

There are a number of things that you can do to your systems to make it easier for your responders.

This includes configuration settings and free third-party tools to install on all of your systems.
UPDATE LOGGING SETTINGS
Log Information

• “No logs, no crime” - Anonymous
• Log files are used to maintain a record of activities
  – e.g. activities of the operating system, certain applications, etc.
• VERY important to ensure all systems ship logs off the host to a central and immutable location
Log Information

• When rolling out new systems, make sure to perform the following tasks for both operating system and application logs

  – Ship logs to a central and immutable location using a well documented protocol - e.g. syslog, REST API, etc.
  – Increase default log size - treat the host log as a backup
  – Log denies as well as successes - helps add to the narrative

• If a system isn’t logging, it shouldn’t be allowed to run
Log Information

• Simple Ansible role to setup system to send syslog to remote system
  – https://github.com/juju4/ansible-syslogclient

• Manage rsyslog client and server
  – https://forge.puppet.com/saz/rsyslog

• Elastic
  – Filebeat: Lightweight shipper for logs
    • https://www.elastic.co/products/beats/filebeat
  – Winlogbeat: Lightweight shipper for Windows event logs
    • https://www.elastic.co/products/beats/winlogbeat
Configuration Setting

ENABLE POWERSHELL LOGGING
• Attackers and developers of penetration-testing frameworks are increasingly leveraging Windows PowerShell to conduct their operations

• PowerShell supports three types of logging
  – module logging
  – script block logging
  – transcription

• PowerShell events are written to the PowerShell operational log Microsoft-Windows-PowerShell%4Operational.evtx

ref: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
Module Logging

- Records pipeline execution details as PowerShell executes, including variable initialization and command invocations

   - `EnableModuleLogging` and `ModuleNames`

HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging
PowerShell Logging

Script Block Logging

- Records blocks of code as they are executed by the PowerShell engine, thereby capturing the full contents of code executed by an attacker, including scripts and commands

  - `EnableScriptBlockLogging`

  HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
Transcription

- Creates a unique record of every PowerShell session, including all input and output, exactly as it appears in the session
  - `EnableTranscripting`, `EnableInvocationHeader`, and `OutputDirectory`

```
HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\Transcription
```
Configuration Setting

ENABLE NTFS LAST ACCESS TIMES
NTFS Last Access Times

- NTFS keeps track of lots of time stamps.
- Each file has a time stamp for 'Create', 'Modify', 'Access', and 'Entry Modified'.
- The latter refers to the time when the MFT entry itself was modified.
- These four values are commonly abbreviated as the 'MACE' values.
NTFS Last Access Times

• Enable last access times for NTFS partitions

• `NtfsDisableLastAccessUpdate` Registry key
  
  HKLM\SYSTEM\CurrentControlSet\Control\FileSystem
Configuration Setting

ENABLE PREFETCH AND SUPERFETCH
Enable Prefetch/Superfetch

• Enable *Prefetch* on servers plus user computers running SSDs
• Windows Prefetch files, introduced in Windows XP, are designed to speed up the application startup process
• Prefetch files contain:
  – The name of the executable
  – A Unicode list of DLLs used by that executable
  – A count of how many times the executable has been run
  – A timestamp indicating the last time the program was run
• The feature is also found in Windows Vista, where it has been augmented with SuperFetch, ReadyBoot, and ReadyBoost.
  – *Note*: For SSD drives Prefetch is disabled by default
Enable Prefetch/Superfetch

- SuperFetch - analyzes per-machine usage patterns over time and optimizes the data that is kept in memory
- The Prefetch files are stored in `%SystemRoot%\Prefetch`

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
```

- Set the `EnablePrefetcher` and `EnableSuperfetch` values to 0
Configuration Setting

WEB BROWSER HISTORY SETTINGS
Web Browsers

- Increase web browser history beyond the default
- Prevent users from clearing their Internet history
Web Browsers: IE

• Increase web browser history beyond the default
  – *DaysToKeep* Registry key

  HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Internet Settings\Url History

• Enter a number between 0 to 999 days (default is 20)
Prevent users from clearing their Internet history

- If this setting is disabled, browsing and download history cannot be deleted
  - Users may be able to edit or delete the history database files directly, and the browser itself may expire or archive any or all history items at any time

- Registry location:
  `Software\Policies\Google\Chrome\AllowDeletingBrowserHistory`

- Mac/Linux preference name:
  `AllowDeletingBrowserHistory`
Configuration Setting

ENABLE SHADOW VOLUME COPIES
Shadow Copy

- Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service, or VSS)
- Allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use
- Should be enabled on all workstations and servers to help recover from ransomware
Registry Keys and Values for Backup and Restore


Special consideration: MaxShadowCopies

- The default data for this value is 64
- The minimum is 1
- The maximum is 512
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Why Forge Fortifications For Forensics?</td>
<td>2</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>3</td>
</tr>
<tr>
<td>Tools That Add Value</td>
<td>4</td>
</tr>
<tr>
<td>Summary</td>
<td>5</td>
</tr>
</tbody>
</table>
Third-Party Tools

MICROSOFT SYSINTERNALS SYSMON
Microsoft Sysmon

- System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

- Provides detailed information about process creations, network connections, and changes to file creation time.

- By collecting the events it generates you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.
Microsoft Sysmon

- **Sysmon download and information**

- **Sysmon configuration file template with default high-quality event tracing**

- **Sysmon Chef cookbook**
  - [https://supermarket.chef.io/cookbooks/sysmon](https://supermarket.chef.io/cookbooks/sysmon)
Third-Party Tools

ON-DEMAND SYSTEM QUERYING
osquery

- **osquery** is an operating system instrumentation framework for OS X/macOS, Windows, and Linux.

- The tools, created by Facebook, make low-level operating system analytics and monitoring both performant and intuitive.

- With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.
osquery

• e.g. check the processes that have a deleted executable:
  – SELECT * FROM processes WHERE on_disk = 0;

• osquery Puppet module
  – https://forge.puppet.com/bryana/osquery

• osquery Chef cookbook
  – https://supermarket.chef.io/cookbooks/osquery

• Ansible osquery role
  – https://github.com/juju4/ansible-osquery
Third-Party Tools

RAPID RESPONSE TOOLS
• GRR Rapid Response
• Remote live forensics for incident response
• Features
  – Cross-platform support for Linux, OS X and Windows clients
  – Live remote memory analysis using open source memory drivers for Linux, OS X and Windows via the Rekall memory analysis framework
  – Powerful search and download capabilities for files and the Windows registry
  – Secure communication infrastructure designed for Internet deployment
  – Client automatic update support
  – Detailed monitoring of client CPU, memory, IO usage and self-imposed limits
**GRR**

- Ansible role to setup GRR
  - [https://github.com/juju4/ansible-grr](https://github.com/juju4/ansible-grr)

- Github download
  - [https://github.com/google/grr](https://github.com/google/grr)
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Why Forge Fortifications For Forensics?</td>
<td>2</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>3</td>
</tr>
<tr>
<td>Tools That Add Value</td>
<td>4</td>
</tr>
<tr>
<td>Summary</td>
<td>5</td>
</tr>
</tbody>
</table>
Digital forensics and incident response activities are complex and often very involved
  – Why not help your teammates do their jobs faster and easier?

Simple configuration settings can help add context to the incident response narrative
  – Little to no impact on operational state of systems

Additional free tools also aid in information capture and analysis for DFIR activities
  – Easier than being reactive during an incident and disrupting what you’re working on
I reached out to a few folks prior to this session to gather their input:
- Nick Klein, @kleinco
- Julien Touche, @julientouche
- Andrew Case, @attrc
- Andre Gironda, @AndreGironda
- Jerod Alexander, @jerod
- Todd Mesick, @tmesick1
- Darren Windham
Forging Forensic Fortifications

Andrew Hay, Co-Founder and CTO, LEO Cyber Security
+1.415.940.9660
andrew.hay@leocybersecurity.com
www.leocybersecurity.com
@andrewsmhay