Malware ☣ Archaeology

This Is the Fastest Way to Hunt Windows Endpoints

Michael Gough

MalwareArchaeology.com

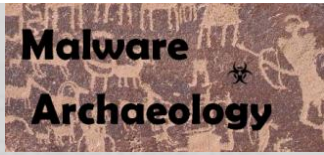
Who am I

- Blue Team Defender Ninja, Malware Archaeologist, Logoholic
- I love "properly" configured logs – they tell us Who, What, Where, When and hopefully How

Creator of

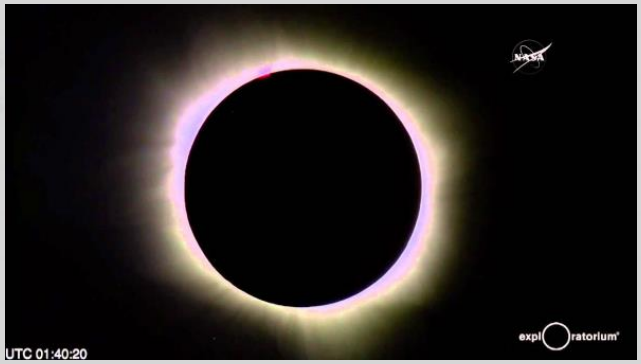
"Windows Logging Cheat Sheet", "Windows File Auditing Cheat Sheet"
"Windows Registry Auditing Cheat Sheet", "Windows Splunk Logging Cheat Sheet"
"Windows PowerShell Logging Cheat Sheet", "Malware Management Framework"
NEW **- "Windows HUMIO Logging Cheat Sheet"**

- Co-Creator of "**Log-MD" – Log Malicious Discovery Tool** LOG-MD
  - **With @Boettcherpwned – Brakeing Down Security PodCast**
- Co-host of "***Brakeing Down Incident Response***" podcast
- **@HackerHurricane** also my Blog



Hunting requires some ‘Back to Basics’ to achieve “Totality”

Achieve Totality



Coverage - Asset Management

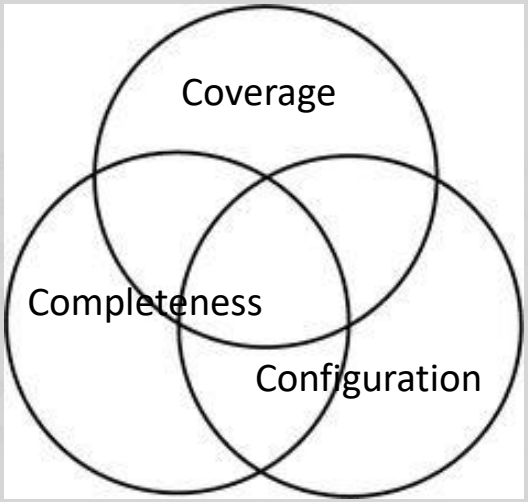
- Can you see every host?
- Do you have ghost assets?
- Remote systems (Road Warriors)
- Powered down VM's/Systems
- IP Scan all devices and identify the OS

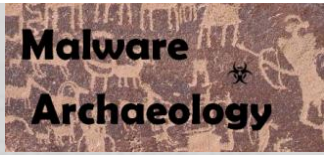
Completeness - Deployment

- Are your agent(s) installed and running properly

Configuration – System Settings

- Are the systems configured correctly
- Enable all that you want and expect





We need a Hunting method

What to base a Hunt on?

- So what do we look for ?
- What do we base our hunts on?

- Where do we start?

- What is the most extensive list of tactics on the adversaries?

IR Reports

- IR Firms publish their findings
  - Many published on MalwareArchaeology.com
  - I call this Malware Management
    - MalwareManagementFramework.org
- Presentations by those of us that have fought and won/lost against advanced adversaries

- These are the best way to get the latest TTP's
- Use these TTP's to hunt for
- And create a framework to map everything you do with the tool(s) you use

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

Malware Archaeology

Mitre Att@ck

Adversarial Tactics, Techniques & Common Knowledge

- This is a good place to start and map all your detection, prevention, and hunt activities to
- Not enough details as to how
  - You will need to map them
  - Or find someone that has, maybe a product(s)
- But most can be mapped to logging for example
- Add Log Management
- Add some Sysmon or WLS to the logs for more details
- Add LOG-MD-Pro, and other tool or script(s)
- Add a solution to query the OS (I love BigFix)
- Add Network tools
- Fill other gaps

LOG-MD

Malware Archaeology

Map them to ATT&CK

- Map the tools you have to the ATT&CK Matrix
- This will give you a place to start and a way to track and rate your activities

Tactic	Technique TechniqueName	ID	Data Source 1	Data Source 2	Data Source 3	Data Source 4	Data Source 5	Data Source 6
Persistence,Privilege Escalation	AppCert DLLs	T1182	4688 Process Execution	4657 Windows Registry	Loaded DLLs			
Persistence,Privilege Escalation	AppInit DLLs	T1103	4688 Process Execution	4657 Windows Registry	Loaded DLLs			
Persistence,Privilege Escalation	Application Shimming	T1138	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	Loaded DLLs	System calls	
Persistence,Privilege Escalation	File System Permissions Weakness	T1044	4663 File monitoring	4688 Process CMD Line	7040, 7045 Services			
Persistence,Privilege Escalation	New Service	T1050	4657 Windows Registry	4688 Process Execution	4688 Process CMD Line			
Persistence,Privilege Escalation	Path Interception	T1034	4688 Process Execution	4663 File monitoring	8000-8027, 866 Whitelist Failures			
Persistence,Privilege Escalation	Port Monitors	T1013	4688 Process Execution	4657 Windows Registry	4663 File monitoring	AutoRuns	DLL monitoring	API monitoring
Persistence,Privilege Escalation	Service Registry Permissions Weakness	T1058	4688 Process CMD Line	7040, 7045 Services	4657 Windows Registry			
Persistence,Privilege Escalation	Web Shell	T1100	4688 Process Execution	4663 File monitoring	4624, 4625 Authentication logs	Netflow/Enclave netflow	Anti-virus	
Privilege Escalation	Exploitation for Privilege Escalation	T1068	1000, 1001 Windows Error Reporting	4688 Process Execution	Application Logs			
Privilege Escalation	SID-History Injection	T1178	4624, 4625	Windows event logs	API monitoring			

Malware Archaeology

Introducing

- The **Windows ATT&CK Logging Cheat Sheet**
- 11 Tactics and 187 Techniques mapped to Windows Event IDs

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

TACTIC: COLLECTION

Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

Tactic	TechniqueName	Technique ID	Data Source 1	Data Source 2	Data Source 3	Data Source 4	Data Source 5	Data Source 6	Data Source 7	Data Source 8	Data Source 9	Data Source 10	Data Source 11
Collection	Audio Capture	T1123	4688 Process Execution	4663 File monitoring	API monitoring								
Collection	Automated Collection	T1119	4688 Process CMD Line	4663 File monitoring	Data loss prevention								
Collection	Clipboard Data	T1115	API monitoring										
Collection	Data from Information Repositories	T1213	Application Logs	Authentication logs	Data loss prevention	Third-party application logs							
Collection	Data from Local System	T1005	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell logs	4663 File monitoring	5861 WMI						
Collection	Data from Network Shared Drive	T1039	4688 Process CMD Line	4688 Process Execution	5140/5145 Share connection	4663 File monitoring							
Collection	Data from Removable Media	T1025	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry	4663 File monitoring	5140/5145 Net Shares						
Collection	Data Staged	T1074	4688 Process CMD Line	4688 Process Execution	4663 File monitoring								

Malware Archaeology

Introducing

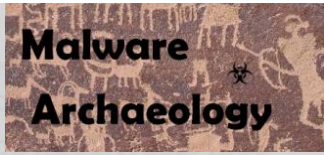
LOG–MD
Discover it

- The **Windows LOG-MD ATT&CK Cheat Sheet**
- 11 Tactics and 187 Techniques mapped to Windows Event IDs, LOG-MD, and Sysmon

Defense Evasion	Software Packing	T1045	LOG-MD - B9 Binary file metadata					
Defense Evasion	Timestomp	T1099	4688 Process CMD Line	4688 Process Execution	4663 File monitoring			
Defense Evasion,Execution	CMSTP	T1191	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Control Panel Items	T1196	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	Windows event logs	LOG-MD - B9 Binary file metadata	Sysmon ID 7 DLL monitoring
Defense Evasion,Execution	InstallUtil	T1118	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Mshta	T1170	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Regsvcs/Regasm	T1121	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Regsvr32	T1117	4688 Process CMD Line	4688 Process Execution	Sysmon - ID 7 Loaded DLLs	4657 Windows Registry		
Defense Evasion,Execution	Rundll32	T1085	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	LOG-MD - B9 Binary file metadata		
Defense Evasion,Execution	Scripting	T1064	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	LOG-MD - Hash Compare		
Defense Evasion,Execution	Signed Binary Proxy Execution	T1218	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Signed Script Proxy Execution	T1216	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Execution	Trusted Developer Utilities	T1127	4688 Process Execution	4688 Process CMD Line				
Defense Evasion,Persistence	BITS Jobs	T1197	BITS Logs Windows event logs	4688 Process CMD Line	API monitoring	Packet capture		
Defense Evasion,Persistence	Component Firmware	T1109	4688 Process CMD Line	4663 File Monitoring				
Defense Evasion,Persistence	Component Object Model Hijacl	T1122	LOG-MD Windows Registry Compare	4688 Process CMD Line	Sysmon - ID 7 DLL monitoring	Sysmon - ID 7 Loaded DLLs		
Defense Evasion,Persistence	Hidden Files and Directories	T1158	4663	4688	4688	LOG-MD		

80/20 rule

- Another VERY important point is we need to ignore or not worry about the 20% that you don't, or can't cover.
- Don't get hung up on the 20% or you will continue to flounder
- Worry about the 80% you CAN or COULD do
- You have to learn to walk before you worry about trying to be, or cover 100% (run)
- Being good at 80% should be a goal
- You will improve over time as you get better



What to Hunt for

So what to hunt for… quickly

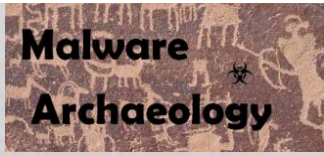
- You basically have two options
- Three, if you include network traffic, but that is not as fast IMHO and you can add this method as you get better and faster and can integrate it into your hunting methodology
  - Part of that 20% I just mentioned
- That leaves two methods you can do quickly

Quick Methods of Hunting

These are two faster methods you can hunt on Windows

1. What is in the logs
2. What is not in the logs

- These items are faster and easier to hunt for and you probably have a tool(s) that can do a lot of it already (e.g. SCCM, BigFix, Humio, Splunk, LOG-MD, Cb, Endgame, scripts, etc.)



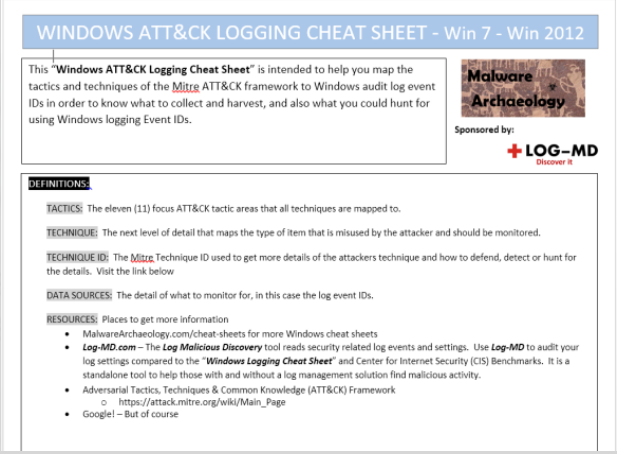
The Logs

What is in the Logs

- Event ID's
  - Map them to YOUR ATT&CK Matrix

- But you MUST enable the "Right Stuff" first
  - This is ***Configuration*** of the 3 C's
  - 1GB Security Log gets you roughly 1 week of data
  - Some logs will get you a longer period

- Windows Logging Cheat Sheet
- Windows Advanced Logging Cheat Sheet
- Windows PowerShell Logging Cheat Sheet
- And other cheat sheets…



WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

This "**Windows ATT&CK Logging Cheat Sheet**" is intended to help you map the tactics and techniques of the Mitre ATT&CK framework to Windows audit log event IDs in order to know what to collect and harvest, and also what you could hunt for using Windows logging Event IDs.

Malware Archaeology

Sponsored by: LOG-MD

DEFINITIONS:

TACTICS: The eleven (11) focus ATT&CK tactic areas that all techniques are mapped to.

TECHNIQUE: The next level of detail that maps the type of item that is misused by the attacker and should be monitored.

TECHNIQUE ID: The Mitre Technique ID used to get more details of the attackers technique and how to defend, detect or hunt for the details. Visit the link below

DATA SOURCES: The detail of what to monitor for, in this case the log event IDs.

RESOURCES: Places to get more information

- MalwareArchaeology.com/cheat-sheets for more Windows cheat sheets
- ***Log-MD.com*** – The ***Log Malicious Discovery*** tool reads security related log events and settings. Use ***Log-MD*** to audit your log settings compared to the "***Windows Logging Cheat Sheet***" and Center for Internet Security (CIS) Benchmarks. It is a standalone tool to help those with and without a log management solution find malicious activity.
- Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework
  - https://attack.mitre.org/wiki/Main_Page
- Google! – But of course

What is in the Logs

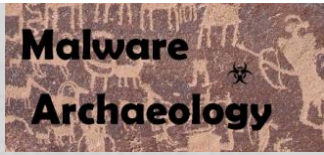
- You can hunt them locally if you follow the Cheat Sheet(s)
  - Enabling Process command Line is key
  - Write a script or use a tool like LOG-MD to collect log data
- Log Management/SIEM is optimal and you will get longer than a week worth of data

What is in the Logs

- Push and run LOG-MD-Pro, PowerShell, or any script or tool can think of to query the logs
- Process Command Line (4688) is a key indicator, New Service (7045), etc.
- There are a lot of Event ID's you can hunt for to indicate things that have happened
- Data in IR Reports and the Cheat Sheets are a place to start for Event IDs and commands

What is in the Logs

- Obvious Log Events such as
  - Suspicious PowerShell events (200-500, 4100-4104)
    - obfuscation, web calls, size of block, Base64, etc.
  - Logins (one account to multiple systems) (4624)
  - Process CMD Line – e.g. Rundll32 malware.dll (4688)
  - Quantity of Admin commands run in a short period
  - New Task (106)
  - New Service (7045)
  - What process called SeTcbPrivilege (Mimikatz) 4703



Not in the Logs

Non-Logs

- Map them to YOUR ATT&CK Matrix
- Run LOG-MD-Pro or other tool/script to collect things like
  - AutoRuns
  - WMI Persistence
  - Large Registry Keys (Data in a value that is large)
  - Null Byte in the registry (Interesting Artifacts)
  - Sticky Keys exploit (Interesting Artifacts)
  - Locked Files
- Other artifacts from IR reports/Preso's, etc.

LOG-MD

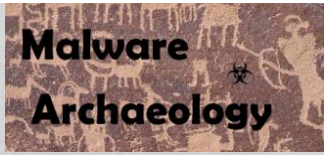
Non-Logs

- Use a tool that can query the OS to look for
  - Registry Keys, Values, Data
  - Files and Directories
  - Yes, hashes if you must
- Dates can be stomped, but dates of keys and folders often are not
- And you can look for ‘created in the last X hours or days’ if you compare to prior hunts

Your Goal(s)

- Elimination !!!
- Eliminate that you do NOT have some known bad things, these will get you started, expand from there
  - Malicious AutoRuns
  - Malicious PowerShell
  - WMI Persistence
  - Large Registry Keys
- These four items account for 90+% of all malware we have seen in the past 6+ years

LOG-MD



Tools

My Top 10 Hunting Tools

1. Log Management (Splunk, Humio, ELK, Graylog)
2. Query the OS type tool (BigFix ROCKS!)
3. LOG-MD-Pro (details)
4. n/a
5. n/a
6. n/a
7. n/a
8. n/a
9. n/a
10. n/a

Tools to Query the OS

- BigFix
- Tanium
- SCCM
- OS Query
- InvestiGator
- Grr
- PowerShell
- Kansa
- Old Fashioned scripts
- EDR-IR tools (Cb, CrowdStrike, Endgame, Red Cloak, etc.)
- LOG-MD-Pro (My personal favorite)

LOG-MD

Malware Archaeology

How do I hunt for PS?

- Without Log Management?

LOG-MD

- Or with it, we consume LOG-MD-Pro logs into Log Management too

	B	C	D	E
	Event_ID	Time		
8	4688	46:27.8	Suspisious Artifact |	| '-enc' Detected |
6	600	46:28.3	Suspisious Artifact |	| '-enc' Detected |
2	400	46:28.3	Suspisious Artifact |	| '-enc' Detected |
8	4688	46:57.8	Suspisious Artifact |	| 'bypass' Detected |
8	4688	47:16.5	Obfuscation | Exceeded-Block-Size |	| (138) ' | (264) + | (2660) BLOCK_SIZE |
8	600	47:17.5	Obfuscation | Exceeded-Block-Size |	| (138) ' | (264) + | (2658) BLOCK_SIZE |
6	400	47:17.7	Obfuscation | Exceeded-Block-Size |	| (138) ' | (264) + | (2658) BLOCK_SIZE |
1	4688	47:28.5	[illegible] |	| 'bypass' Detected |
7	4688	01:33.4	| Obfuscation | Exceeded-Block-Size | Suspisious Artifact |	| (20) ' | (558) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http'
4	4688	01:33.5	| Obfuscation | Exceeded-Block-Size | Suspisious Artifact |	| (20) ' | (527) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http'
6	600	01:33.7	| Obfuscation | Exceeded-Block-Size | Suspisious Artifact |	| (20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http'
2	400	01:33.7	| Obfuscation | Exceeded-Block-Size | Suspisious Artifact |	| (20) ' | (522) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http'
8	4104	01:33.9	| Obfuscation | Exceeded-Block-Size | Suspisious Artifact |	| (20) ' | (575) BLOCK_SIZE | '-enc' Detected | 'webclient' Detected | 'http'
8	4688	01:34.0	Obfuscation | Suspisious Artifact |	| (8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected |
8	600	01:34.2	Obfuscation | Suspisious Artifact |	| (8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected |
2	400	01:34.4	Obfuscation | Suspisious Artifact |	| (8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected |
0	4104	01:34.2	Obfuscation | Suspisious Artifact |	| (8) ' | 'webclient' Detected | 'http' Detected | 'download' Detected |

https://www.linkedin.com/company/threathunting

https://www.twitter.com/threathunting_

Resources

- Mitre - ATT&CK Framework
  - attack.mitre.org/wiki/Main_Page
- Endgame – The Endgame Guide to Threat Hunting
  - https://pages.endgame.com/rs/627-YBU-612/images/The%20Endgame%20Guide%20to%20Threat%20Hunting%20-%20ebook.pdf
- Sqrrl - Hunt Evil Your Practical Guide to Threat Hunting
  - https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf
- SANS Poster – Find Evil
  - Digital-forensics.sans.org/media/poster_2014_find_evil.pdf

Resources

- Cyb3rWard0g/ThreatHunter-Playbook
  - https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
- beahunt3r/Windows-Hunting
  - https://github.com/beahunt3r/Windows-Hunting
- ThreatHunting.net
- ThreatHunting.org
- Findingbad.blogspot.com

Questions?

You can find us at:

- **Log-MD.com**

- **@HackerHurricane**
- **HackerHurricane.com (blog)**
- **MalwareArchaeology.com – Cheat Sheets**
- **Listen to the "Brakeing Down Incident Response" Podcast**
  - **BDIRPodcast.com**