DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Harvesting Logs for Enhanced Investigations

I <3 Logs

David Gainey
DISA Incident Response Team
9 JAN 2019

Who Am I?

- Computer Scientist
- Herald of Hunting
- Incident Responder for 10+ years with DISA

Collect

- What is the most valuable resource for incident response?
  - Historical data; typically in the form of logs
- What should be centralized?
  - Host logs, IDS logs, Flow data, Bro/Zeek logs, syslog
  - Everything you can!
- It doesn't have to cost a fortune
  - Free/low cost options exist
- But, why?
  - Compromise detection (hunting)
  - Incident investigation
    - Enrichment
- Protect it.

Logs

- **Collect what you have**
  - **Windows Event Forwarding (Jessica Payne)**
  - **Intrusion Detection Systems, Flow/Bro data, Syslog, etc.**

Logs

- **Collect what you have**
  - **Windows Event Forwarding (Jessica Payne)**
  - **Intrusion Detection Systems, Flow/Bro data, Syslog, etc.**

- **Log the right things**
  - **DISA STIGs – event log modifications**
  - **https://docs.google.com/spreadsheets/d/1ow7YRDEDJs67kcKMZZ66_5z1ipJry9QrsDQkjQvizJM/edit#gid=0**

- **Go further**
  - **Sysmon**
    - Filter full path; otherwise you might miss badness

Learn

- Microsoft Windows
  - Process Hierarchy - What is normal?
  - Software installation norms
  - Persistence mechanisms
- Your Environment
  - What software is unique to your environment?
  - How do your user's operate?
  - How do your administrators operate?
- What are adversarial TTPs?

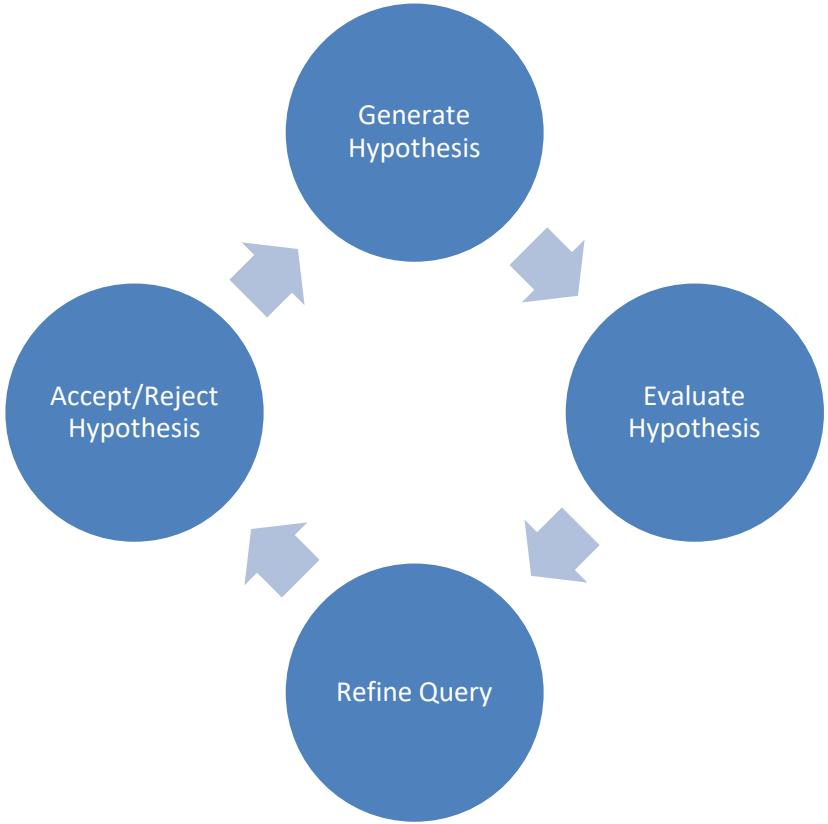
Learn

- Microsoft Windows
  - Process Hierarchy - What is normal?
  - Software installation norms
  - Persistence mechanisms
- Your Environment
  - What software is unique to your environment?
  - How do your user's operate?
  - How do your administrators operate?
- What are adversarial TTPs?
- How does malware work?
  - Process injection
  - Credential Harvesting
  - Techniques for hiding

Hunting Concepts

- Indicator-driven
  - Indicators of compromise
  - High fidelity; easily modified; rapid identification
- Intelligence-driven
  - Learn how specific groups operate
  - Look for specific TTPs related to those groups
- Hypothesis-driven
  - Develop a hypothesis, test, refine
  - All hypotheses will fail at first; most hypotheses will fail in the end

Hypothesis-Driven



Hunting Concepts

- Indicator-driven
  - Indicators of compromise
  - High fidelity; easily modified; rapid identification
- Intelligence-driven
  - Learn how specific groups operate
  - Look for specific TTPs related to those groups
- Hypothesis-driven
  - Develop a hypothesis, test, refine
  - All hypotheses will fail at first; most hypotheses will fail in the end
- Warning: Dive deep enough and you will surely find “weird” stuff that is completely normal.
  - https://isc.sans.edu/diary/Google+Chrome+and+%28weird%29+DNS+requests/10312

Analyze

- Investigate IDS Alerts
  - Alert for Flash exploit; did flash run on the system? Any additional activity?
  - Malicious IP identified; what process made the connection? Passive DNS?
- "Stacking"/Least Frequency of Occurrence
  - Processes with network traffic
  - Parent/Child relationships
  - Full process path

Stacking – Explorer

process_parent_path.keyword: "c:\windows\explorer.exe" Add a filter + Actions

process_parent_path.keyword: Descending	process_path.keyword: Descending	Count
c:\windows\explorer.exe	c:\program files (x86)\lego company\lego digital designer\ldd.exe	3
c:\windows\explorer.exe	c:\program files (x86)\lego software\lego mindstorms ev3 home edition\mindstormsev3.exe	3
c:\windows\explorer.exe	c:\program files\realtek\audio\hda\ravbg64.exe	3
c:\windows\explorer.exe	c:\program files\realtek\audio\hda\rtkngui64.exe	3
c:\windows\explorer.exe	c:\program files\waves\maxxaudio\wavessvc64.exe	3
c:\windows\explorer.exe	c:\program files\windows defender\msascuil.exe	3
c:\windows\explorer.exe	c:\users\fll\appdata\local\microsoft\onedrive\onedrive.exe	3
c:\windows\explorer.exe	c:\windows\syswow64\runonce.exe	3

Stacking - svchost

process_parent_path.keyword: "c:\windows\system32\svchost.exe" Add a filter + Actions

process_parent_path.keyword: Descending	process_path.keyword: Descending	Count
c:\windows\system32\svchost.exe	c:\windows\system32\sc.exe	1
c:\windows\system32\svchost.exe	c:\windows\system32\usoclient.exe	1
c:\windows\system32\svchost.exe	c:\windows\system32\wbem\wmiadap.exe	1
c:\windows\system32\svchost.exe	c:\program files\realtek\audio\hda\ravbg64.exe	2
c:\windows\system32\svchost.exe	c:\program files\windowsapps\microsoft.skypeapp_14.35.76.0_x64__kzf8qxf38zg5c\skypeapp.exe	2
c:\windows\system32\svchost.exe	c:\program files\windowsapps\microsoft.skypeapp_14.35.76.0_x64__kzf8qxf38zg5c\skypebackgroundhost.exe	2
c:\windows\system32\svchost.exe	c:\program files\windowsapps\microsoft.windowscommunicationsapps_16005.11001.20106.0_x64__8wekyb3d8bbwe\hxtsr.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\applicationframehost.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\audiodg.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\browser_broker.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\cliprenew.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\dxgiadaptercache.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\mobsync.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\sihost.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\smartscreen.exe	2
c:\windows\system32\svchost.exe	c:\windows\system32\wbem\unsecapp.exe	2

Stacking – Services

process_parent_path.keyword: "c:\windows\system32\services.exe" Add a filter + Actions

process_parent_path.keyword: Descending	process_path.keyword: Descending	Count
c:\windows\system32\services.exe	c:\program files\rempl\sedsvc.exe	2
c:\windows\system32\services.exe	c:\windows\system32\sgrmbroker.exe	2
c:\windows\system32\services.exe	c:\windows\system32\sppsvc.exe	2
c:\windows\system32\services.exe	c:\program files\realtek\audio\hda\rtkaudioservice64.exe	3
c:\windows\system32\services.exe	c:\program files\waves\maxxaudio\wavessyssvc64.exe	3
c:\windows\system32\services.exe	c:\programdata\microsoft\windows defender\platform\4.18.1810.5-0\msmpeng.exe	3
c:\windows\system32\services.exe	c:\programdata\microsoft\windows defender\platform\4.18.1810.5-0\nissrv.exe	3
c:\windows\system32\services.exe	c:\windows\system32\dellrctlservice.exe	3
c:\windows\system32\services.exe	c:\windows\system32\driverstore\filerepository\ki126974.inf_amd64_9168fc04b8275db9\igfxcuiservice.exe	3
c:\windows\system32\services.exe	c:\windows\system32\driverstore\filerepository\ki126974.inf_amd64_9168fc04b8275db9\intelcphdcpsvc.exe	3
c:\windows\system32\services.exe	c:\windows\system32\driverstore\filerepository\ki126974.inf_amd64_9168fc04b8275db9\intelcphecisvc.exe	3
c:\windows\system32\services.exe	c:\windows\system32\searchindexer.exe	3
c:\windows\system32\services.exe	c:\windows\system32\securityhealthservice.exe	3
c:\windows\system32\services.exe	c:\windows\system32\spoolsv.exe	3
c:\windows\system32\services.exe	c:\windows\system32\upfc.exe	3
c:\windows\system32\services.exe	c:\winlogbeat-6.5.2-windows-x86_64\winlogbeat.exe	3
c:\windows\system32\services.exe	c:\windows\system32\svchost.exe	236

Suspicious Powershell

event_data.CommandLine: Descending	Count
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -executionpolicy Bypass -nologo -noninteractive -NoProfile -WindowStyle Hidden -file [redacted]	309
"C:\Windows\SysWOW64\rundll32.exe" [redacted]	63
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & [redacted]	11
"C:\WINDOWS\system32\netsh.exe" wlan add profile \ [redacted] \Policies\ [redacted] \Machine\Scripts\Startup [redacted] user=all	10
"C:\WINDOWS\system32\netsh.exe" wlan delete profile name= [redacted]	10
C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe -File [redacted] \Policies\ [redacted] \Machine\Scripts\Startup\ [redacted] -ExecutionPolicy Bypass	10
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & [redacted]	7
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy ByPass -WindowStyle Hidden -file [redacted]	7
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy ByPass -WindowStyle Hidden -file [redacted]	7
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & [redacted]	4

Sysmon – Network Activity

event_data.Image: Descending	Count
System	4,393,734
C:\Windows\System32\lsass.exe	796,447
C:\Windows\System32\svchost.exe	566,827
C:\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE	369,034
C:\Windows\System32\spoolsv.exe	44,929
C:\Program Files[redacted]	24,038
C:\Windows\SysWOW64[redacted]	20,573
C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	14,482
C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE	13,429
C:\Windows\explorer.exe	8,341
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	7,276
C:\Windows\System32\dasHost.exe	7,207
C:\Windows\System32\vmms.exe	6,495
C:\Program Files\[redacted]	5,646
C:\Program Files (x86)\Microsoft Office\Office15\SPDESIGN.EXE	4,598

Sysmon – Network Activity Ascending

event_data.Image: Descending	Count
C:\Program Files\[redacted]	92
C:\Program Files (x86)\[redacted]	96
C:\Program Files (x86)\Microsoft Office\Office14\SPDESIGN.EXE	116
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	118
C:\Windows\SysWOW64\Macromed\Flash\[redacted]	124
C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe	128
C:\Program Files (x86)\Microsoft Office\Office15\MSACCESS.EXE	132
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	134
C:\Program Files (x86)\[redacted]	138
C:\Windows\SysWOW64\[redacted]	161
C:\Program Files\[redacted]	191
C:\Windows\[redacted]	194
C:\PROGRA~2\MICROS~1\Office15\EXCEL.EXE	213
C:\Windows\dwrcs\DWRCST.EXE	226
C:\Windows\System32\mmc.exe	240

Acrobat – Network Connectivity

- **Sysmon – No Domain Name (uses reverse lookups)**

C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\Acrobat.exe	69.58.181.160	pki-crl.symauth.net
C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\Acrobat.exe	23.15.8.120	-

- **Bro – Use dns.log to identify the domain**

dns	a122.g2.akamai.net	23.15.8.120, 23.15.8.137
dns	acroipm2.adobe.com	acroipm2.adobe.com.edgesuite.net, a122.g2.akamai.net, 23.15.8.120, 23.15.8.137

Enrichment

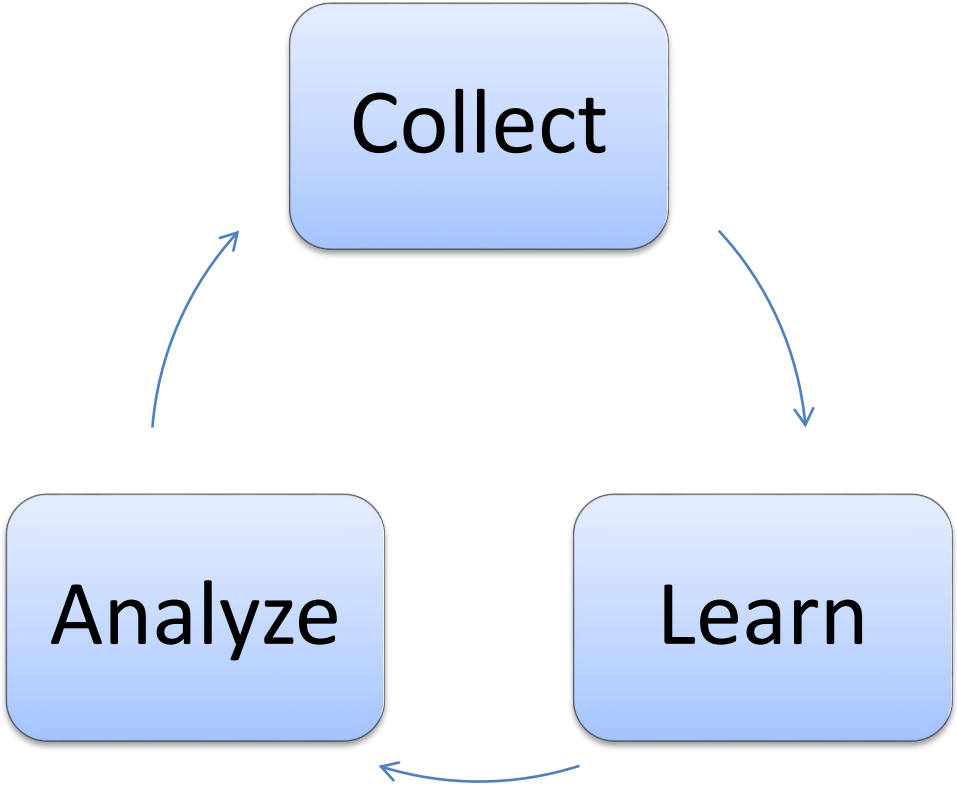
type	dest_hostname	dest_ip	src_ip	src_hostname
conn	cse.google.com	172.217.0.142	[redacted]	
conn	www.googletagmanager.com	173.194.175.97		
conn	r1---sn-q4flrnee.googlevideo.com	209.85.165.198		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	googleads.g.doubleclick.net	209.85.144.157		
conn	apis.google.com	172.217.0.142		
conn	www.google-analytics.com	173.194.204.138		
conn	googleads.g.doubleclick.net	172.217.21.226		

One More Thing…

One More Thing…

- **Machine Learning**

Summary



Resources - Tools

- https://github.com/Cyb3rWard0g/HELK
  - https://cyberwardog.blogspot.com/
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- https://securityonion.net/
- https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events
- https://uncoder.io/

Resources – Videos

- https://channel9.msdn.com/Events/Ignite/Australia-2015/INF327
- https://www.irongeek.com/i.php?page=videos/bsidescolumbus2018/p05-the-quieter-you-become-the-more-youre-able-to-helk-nate-guagenti-roberto-rodriquez

Resources - Knowledge

- https://www.andreafortuna.org/dfir/forensics/standard-windows-processes-a-brief-reference/
- https://github.com/Cyb3rWard0g/OSSEM
- https://attack.mitre.org/matrices/enterprise/
- https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf
- http://www.hexacorn.com/blog/category/autostart-persistence/
- http://blogs.sans.org/cyber-defense/files/2014/07/Process_Hacker_SANS_Jason_Fossen.pdf
- https://github.com/keydet89/Tools/blob/master/exe/eventmap.txt
- https://youtu.be/7q7GGg-Ws9s
- https://www.threathunting.net/reading-list
- https://jpcertcc.github.io/ToolAnalysisResultSheet/

Resources - Validation

- https://atomicredteam.io/
- https://github.com/endgameinc/RTA
- https://github.com/uber-common/metta
- https://github.com/mitre/caldera

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**