Ransomware

Hunting and Scoping an Attack

Windows attack patterns you can use RIGHT NOW for detection!

Andrew Skatoff

GCFA, GDAT, GREM, GNFA

whoami

- Andrew Skatoff
  - Senior Cyber Security Manager
    - Threat Hunting
    - Malware Analysis
    - Incident Response / Forensics
  - 18 years in Cyber Security
  - My views/comments != Employer's
  - 4 kids + 1 wife @ Richmond, VA
  - Approx 2-3 cats

What's Special About Ransomware?

- Many TTPs are the same as any other attack
- Some TTPs are unique to ransomware
- This will be our focus

Right of Boom?

- Isn't it already too late to detect at this stage?

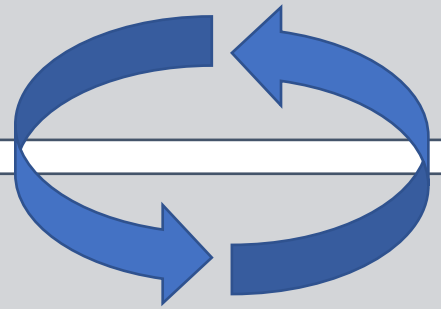
- Some ransomware waits for a user to login before encryption. Other devices may be sitting idle waiting for a login. You can stop them before they get encrypted! If you can find them!
  - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

- Use telemetry to quickly scope/contain the damage (rather than counting help desk calls).

Ransomware Attack Stages

Gain Access
- Phishing Attacks / Web drive by
- Deploy Tools (e.g. Cobalt Strike, AgentTesla, Qakbot)

Privilege Escalation
- Recon for credentials (e.g. Bloodhound -> Kerberoasting)
- Gain Domain Admin



Recon the Enterprise
- Identify HVAs for maximum impact
- Enumerate defenses

Exfil Data

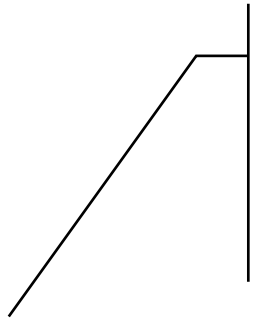
Disable Defenses / Recovery
- Stop Security Agents and Diagnostics
- Relax ACLs
- Unlock files
- Destroy Backups and Evidence

Deploy Ransomware
- Endpoints | File Servers | Domain Controllers

Our Focus

Detection Fundamentals

- Command Line Auditing is a MUST!
  - Security log EventCode 4688 – requires GPO settings to capture
    - https://www.malwarearchaeology.com/cheat-sheets
  - EDR | Sysmon



These apply to all commandline detection opportunities. The rest of the slides will show other opportunities in this format

- EventLogs
  - Security
  - System
  - PowerShell
  - Sysmon
  - Defender
  - WMI

Category	Source	Comments
Command Line	Sysmon.evtx	EventCode=1
Command Line of Process Execution	Security.evtx	EventCode=4688
EDR	*	*

The commands in this deck assume two things:
1. You are monitoring **process execution** and associated **command lines**,
2. The commands are **in plain text** and not encoded via PowerShell or otherwise obscured (e.g. passed via API).

- Centralized Logs are a MUST!

Enumerate Defenses

- PowerShell/WMI to list AV/Firewall tools
  - `Select * FROM (AntivirusProduct | FirewallProduct | AntiSpywareProduct)`
  - `(WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiSpywareProduct Get displayname /format:csv)`
  - `(WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntivirusProduct Get displayname /format:csv)`
  - `(WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path FirewallProduct Get displayname /format:csv)`
  - `wmic process list`
- SC.exe to list services
  - `sc query`

Category	Source	Comments
PowerShell	Microsoft-Windows-PowerShell%4Operational.evtx	4103, 4104 – Script Block logging Logs suspicious scripts by default in PS v5 Logs all scripts if configured

https://isc.sans.edu/forums/diary/Keep+an+Eye+on+Your+WMI+Logs/25012/

https://www.hexacorn.com/blog/2020/08/20/sc-and-its-quirky-cmd-line-args/

Disable Defenses: Security Tools

- Stop services
  - `net stop SharedAccess`
  - `sc stop wuauserv`
  - `Sc pause MpsSvc`
- Delete services
  - `sc delete MpsSvc`

Category	Source	Comments
Services	System.evtx	EventCode=7036 – Service started or stopped EventCode=7040 – Start type changed (Boot | On Request | Disabled)
Process Exit	Security.evtx	EventCode=4689 YMMV
Process Exit	Sysmon	EventCode=5 (Look for spikes in volume)
Service Delete	Sysmon	EvenCode=13 – Registry set value

- Kill processes (security tools and productivity tools for file locks)
  - CMD/PSH: `wmic process "where name like '%WinDefend%'" delete`
  - `Taskkill /IM ccSvcHst.exe`

Disable Defenses: Security Tools

Disable/Misconfigure Microsoft Defender

Sc.exe

```
sc config WinDefend
start= disabled
```

PowerShell

```
PowerShell Set-MpPreference -DisableRealtimeMonitoring $true
PowerShell Set-MpPreference -DisableBehaviorMonitoring $true
PowerShell Add-MpPreference -ExclusionPath C:
PowerShell Add-MpPreference -ExclusionExtension ".exe"
```

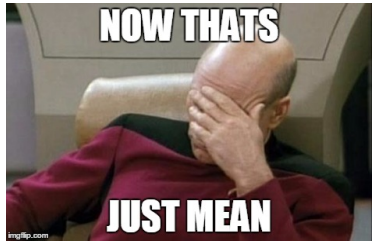
Category	Source	Comments
Services	System.evtx	EventCode=7040 – Start type changed (Boot | On Request | Disabled)
Registry	Microsoft-Windows-Sysmon/Operational	EventCode=12 EventCode=13 Monitoring this registry key will also help with detection: \HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions
Registry	Microsoft-Windows-Windows Defender/Operational	Event ID 5001 will detect Defender AV Real-Time being disabled. Event ID 5007 may be monitored to detect Defender configuration changes.

Disable Defenses: Security Tools

- Disable/Misconfigure Windows Firewall
  - `netsh ipsec static set policy name=Bastards assign=y`
  - `netsh firewall set opmode mode=disable`
  - `netsh Advfirewall set allprofiles state off`
  - `net stop SharedAccess`

Category	Source	Comments
Services	System.evtx	EventCode=7036 – Service started or stopped EventCode=7040 – Start type changed (Boot | On Request | Disabled)
Task Manager	Microsoft-Windows-Sysmon/Operational	EventCode=12-14 for registry changes

- Disable Task Manager
  - `reg.exe add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f`



Disable Defenses: Relax ACLs

- Take Ownership of Files
  - `takeown.exe /S system /U user /P password /F Myshare*`
- Relax ACLs
  - `icacls.exe C:\Windows\system32\evil.exe /reset`
  - `icacls ""C:*"" /grant Everyone:F /T /C /Q`
  - `icacls ""D:*"" /grant Everyone:F /T /C /Q`

Relaxing filesystem ACLs allows the malware to access/encrypt all files.

https://redcanary.com/blog/ryuk-ransomware-attack/

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
WastedLocker_Threat Advisory-August 7 2020.pdf (mcafee.com)

Disable Defenses: AntiForensics

Category	Source	Comments
Clear Event Logs	Security.evtx	EventCode=1102 | Security event logs cleared
Clear Event Logs	System.evtx	EventCode=104 | Any event log was cleared

- Clear Event Logs
  - `wevtutil.exe cl Application`
  - `wevtutil.exe cl Security`
  - `wevtutil.exe cl System`
  - `FOR /F "delims=" %%I IN ('WEVTUTIL EL') DO (WEVTUTIL CL "%%I")`
- Delete USN Journal
  - `wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:`
  - `fsutil usn deletejournal /D C:"`

Disable Recovery

- Disable Windows Automatic Startup Repair
  - `bcdedit /set bootstatuspolicy ignoreallfailures`
  - `bcdedit /set recoveryenabled no`
  - `shutdown /r /f /t 00`
- Enforce reboot in safemode
  - `reg add HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal\evilservicename`
  - `bcdedit.exe /set safeboot minimal`
  - `shutdown /r /f /t 00`

Category	Source	Comments
Registry	Microsoft-Windows-Sysmon/Operational	EventCode=12-14
Services	System.evtx	EventCode=7036 – Service started or stopped EventCode=7040 – Start type changed (Boot | On Request | Disabled) EventCode=7045 – Service was installed

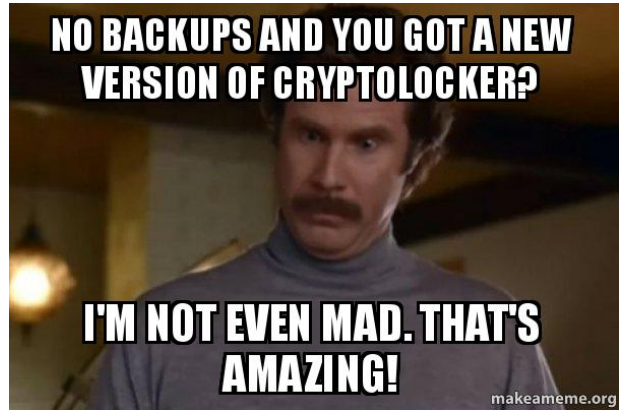
Destroy Backups

- Delete backup files with “del”
  - `del /s /f /q c:*.VHD c:*.bac c:*.bak c:*.wbcat c:*.bkf c:Backup*.* c:ackup*.* c:*.set c:*.win c:*.dsk`
- Delete backups via “wbadmin”
  - `wbadmin delete catalog -quiet`
    `wbadmin DELETE SYSTEMSTATEBACKUP`
    `wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest`
- PowerShell - Delete computer restore point
  - Psh: `Get-ComputerRestorePoint | delete-ComputerRestorePoint`

Category	Source	Comments
PowerShell	Microsoft-Windows-PowerShell%4Operational.evtx	4103, 4104 – Script Block logging Logs suspicious scripts by default in PS v5 Logs all scripts if configured

Destroy Backups

- Vssadmin.exe
  - `vssadmin.exe delete shadows /All /Quiet`
  - `vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB`

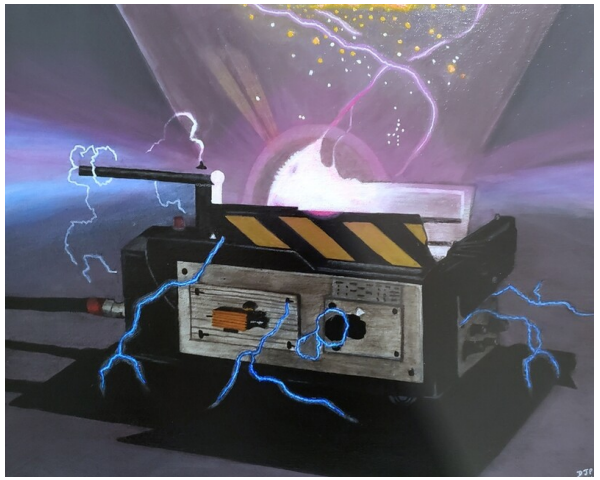


- PowerShell
  - `Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}`
  - `PowerShell Get-WmiObject Win32_ShadowCopy | % { $_.Delete() }`
  - `PowerShell Get-WmiObject Win32_ShadowCopy | Remove-WmiObject`

Category	Source	Comments
PowerShell	Microsoft-Windows-PowerShell%4Operational.evtx	4103, 4104 – Script Block logging Logs suspicious scripts by default in PS v5 Logs all scripts if configured

Key Takeaways

- Many Ransomware TTPs are unique
- It may not be too late!
- You can use them to prevent/detect late stages of a ransomware attacks.
- Quickly scope a successful attack to assess and limit the impact.
- Isolate impacted assets.



Q & A

References

- https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
- https://www.gdatasoftware.com/blog/2020/11/36459-babax-stealer-rebrands-to-osno-installs-rootkit
- https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
- https://redcanary.com/blog/ryuk-ransomware-attack/
- https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
- https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/
- https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf
- https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/
- https://medium.com/cert-advisory/what-you-should-absolutely-know-about-petya-and-misha-ransomware-attack-goldeneye-ransomware-8c3f8883fb8
- https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
- https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3/
- https://malware.news/t/threat-analysis-unit-tau-threat-intelligence-notification-snatch-ransomware/36365
- https://labs.sentinelone.com/the-fonix-raas-new-low-key-threat-with-unnecessary-complexities/
- https://redcanary.com/blog/its-all-fun-and-games-until-ransomware-deletes-the-shadow-copies/
- https://resources.infosecinstitute.com/topic/ransomware-deletion-methods-and-the-canary-in-the-coal-mine/
- https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
- https://thedfirreport.com/wp-content/uploads/2020/11/fullpysa.png
- https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-find-ransomware?view=o365-worldwide