STOPPING TARGETED RANSOMWARE ATTACKS

TIM GURGANUS

CHRIS RILEY

STOPPING TARGETED RANSOMWARE ATTACKS - AGENDA

- Targeted Ransomware is growing at a rapid pace
- Inside Targeted Ransomware Attacks
- War Stories and Lessons Learned
- Detection
- Mitigation Strategy
- Recommendations
- Conclusion

RANSOMWARE ATTACK GROUPS TARGETING ORGANIZATIONS

WHO'S BEEN TARGETED WITH RANSOMWARE?

- Lake City Florida $480k to Ryuk
- Riviera City Florida $592k to Ryuk
- Jackson County Georgia$ 400k to Ryuk
- LaPort County Indiana $130k to Ryuk
- 23 municipalities in Texas impacted by Sodin (Revil) 08/16 – No Ransom Paid
- Norsk Hydro - Ryuk – No Ransom Paid
- Georgia Court System – No Ransom Paid

INSIDE A RYUK RANSOMWARE ATTACK

- Ryuk – Initial intrusion over email to install Trickbot and Powershell Empire
- Who is Ryuk? Financially motivated, pen-test training, develop ransomware as well as scripts for lateral movement and ransomware distribution
- Multiple cases of an Emotet -> TrickBot -> Ryuk infection chain observed
- Reports of Ryuk distributed by malspam campaigns as well.
- Trickbot's pre-install script disables Windows security features (realtime scanning, Windows Defender..) making further intrusions easier
- Ryuk attackers communicate with victims via email or chat (2 email addresses in the ransom note)
- Ryuk ransomware infections use anti-forensics and anti-recovery tactics by deleting the shadow copies and then creating new ones, that are tiny, to overwrite the deleted shadow files
- Ryuk also seems adepts at locating and destroying system backups
- During recon phase, attackers build a target list in a text file of Windows systems to encrypt. The Ryuk ransomware binary and some scripts and other utilities like PSEXEC and ADFind.exe are put on a staging server
- Ryuk attackers will use the "get_user" command to look for service accounts (those with Service Principle Name (SPN) set, ServicePrincipleName=*) in the target's Active Directory.
- In lateral movement stage, mimikatz (invoke-mimikatz.ps1) is used to facilitate pass-the-hash lateral movement

INSIDE A SODIN RANSOMWARE ATTACK

- Sodin intrusion vector is often compromising 3rd party managed IT or software providers.
- Who is Sodin? former Gandcrab developers, RaaS actors and top 5 Gandcrab distributors
- Sobin is highly evasive, and takes many measures to prevent its detection by antivirus and dynamic malware analysis
- Sodin distributes the Ostap backdoor botnet as a JSE file for persistent access
- Ostap can download other payloads, make WMI calls for recon and lateral movement
- Sodin uses UAC bypass to run with elevated privileges and do more damage
- Sodin uses an exploit of CVE-2018-8453 to elevate privileges to kernel before encryption
- Sodin creates a new service to run with elevated privileges (usually called “wifi internet conection”)
- Sodin functions include the option to delete the contents of blacklisted folders
- Sodin can exfiltrate basic host information (function is enabled with –net parameter)
- Like Gandcrab, Sodin ransomware has an internally stored, encoded configuration

INSIDE A TARGETED RANSOMWARE ATTACK

- Attackers often use utilities like Bloodhound or Powerview for mapping admin access and lateral movement
- Ransomware attackers often have access to a target enterprise for weeks and have plenty of time for data exfil, but it is still not observed that often
- After owning MS Exchange accounts, attackers often send internal phishing attacks to get more account credentials or get more installations of Trickbot malware
- Most attackers use PSEXEC at some point for coordinated distribution of files or launching the next stage
- Attackers often target the same organization a few months later (more phishing, Nigerian threat actors using same accounts)
- Other attacks are carried out using credentials stolen with Trickbot including:
  - Attacking Bank accounts of the business
  - Direct deposit redirects
- Other corporate accounts have been abused as well (Order $1 million in Verizon cell phone equipment using a corporate bill account and send to NJ)

WAR STORIES AND LESSONS LEARNED

Once attackers have local administrator access, they disable EDR before running malware:
- EDR and Antivirus agent should have a password required to remove it
- Monitor logs for EDR or Antivirus service being disabled or removed in bulk

Attackers also use Admin access to disable Windows Defender
Most targeted ransomware victims have no Endpoint security and just use Windows Defender (which detects 25% of malware)

It is really common to see the same local administrator password shared across an enterprise
- That account can disable EDR or Antivirus on every Windows host

Service accounts with interactive login is a common mistake

Attackers also add interactive login privilege to a service account
- This can be logged and detected

Most attackers don't have to be stealthy because no one is keeping up with their authentication logs

WAR STORIES AND LESSONS LEARNED

Attackers delay ransomware encryption phase to:

1) Exfiltrate some of the data
   a. Data exfil is by building RAR or ZIP on a staging host and then transmit using SFTP
   b. Attackers may exfil email contact lists to Trickbot CnC servers for use in subsequent attacks

2) Find backups, encrypt backups first, delete, then overwrite, then encrypt the backup servers

Other than elevation of privilege, Windows exploits are not used that often

Attackers usually use MS Office macros and steal credentials with malware or social engineering

Effective mitigation is PATCH critical servers and workstations and manage passwords and have backups, use least privileges, don't use default security settings, transcription logs from Powershell, not giving network login rights to too many accounts

AFFECTS OF CYBER INSURANCE

What is cyber insurance?

From Nationwide.com
Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records.

Won't my general liability policy cover cyber liability?

General liability insurance covers bodily injuries and property damage resulting from your products, services or operations. Cyber insurance is often excluded from a general liability policy.

What does cyber insurance cover?

- Besides legal fees and expenses, cyber insurance typically helps with:
- Notifying customers about a data breach
- Restoring personal identities of affected customers
- Recovering compromised data
- Repairing damaged computer systems

Most states require companies to notify customers of a data breach involving personally identifiable information[2]– a process that can be very expensive. And even though most states don't require companies to offer free credit monitoring following a breach, such a gesture goes a long way with public relations.

LAKE CITY FLORIDA

June 24th 2019 Lake City Florida – Hit with Ransomware (Ryuk). Mayor and Council had an emergency session to decide best path forward to recover operations from the attack. In order to save time and money it was decided to allow the city's cyber insurer to pay the ransom of 42 bit coin $460,000. Under the city's policy they were only responsible for a $10,000 deductible.

Another point of consideration is coverage limits. Lake City had a one million dollar coverage limit. Recovery time and effort would have exceeded that limit, possibly out pacing the the Ransom demand.

AFFECTS OF CYBER INSURANCE

Law Enforcement and Cyber Security professionals recommend not paying the ransom. By paying the ransom the attackers are emboldened to continue carrying out similar attacks.

Is cyber insurance fueling the recent rash of ransomware attacks?

Attackers have switched from posting a bit coin wallet to providing an email address for Ransom responses. When the attackers receive notification they begin to ask questions about your environment and if you have cyber insurance.

DO NOT REVEAL YOU HAVE INSURANCE – This will encourage the attackers to increase the ransom demand.

Did the problem really get fixed? By paying the Ransom and restoring operations did the vulnerabilities get fixed the caused the issue to begin with?

MITIGATION STRATEGY

One of the problems I'm constantly seeing is security leaders becoming hyper-focused on ransomware. They'll do anything to prevent ransomware when really, they should be protecting themselves from all malware.

Ransomware may hurt the most, but what we're seeing now with this modular malware, the ransomware is not the initial piece of malware.
So, if you're only hyper-focused on the Ryuk ransomware, you are putting your focus and effort on the wrong place.
You need to be focused on what brings in the Ryuk, the TrickBot or the Emotet, or one of these other parts that are part of a botnet.

The ransomware is just the end payload. You need to focus on how the attacker got in.

MITIGATION STRATEGY

When it comes to ransomware mitigation advice for the enterprise, they should prevent the preventable by patching. Enterprises also have to do the basics of cyber hygiene and have the ability to recover and be resilient. Anti fragility is critical, and that's about more than prevention, it's detection, segmentation, back up, it's redundancy and it's recovery.

Preventive measures, such as reviewing vulnerabilities on servers, segmentation and reviewing user access rights, are easy to suggest but evidently harder to implement.

Identify the data and systems that are critical for your organization to continue to function. If they can't be protected, ensure you have a robust non-attached backup solution that's stored securely.

Early response to ransomware should be to protect those identified critical systems and data. When ransomware is detected, act swiftly to protect those systems.

To stop the spread of ransomware, automate the response that focuses on blocking lateral movement. Targeted ransomware attacks often begin the final phase on weekends or off-hours and a manual response may take too long.

MITIGATION STRATEGY

- Email Security
- URL Inspection
- Harden MS Office to prevent macro execution
- If the Trickbot malDoc is opened in an environment where Powershell is restricted to constrained language mode, the Powershell Empire reverse shell connection will not be created even if macros are enabled. Enabling Powershell constrained language mode is recommended.

NETWORK SEGMENTATION

- After initial intrusion, attackers seek out the systems and data that, if encrypted, would shutdown the primary activities of the business.
- Identify critical business assets (data, accounts, services) and put each in a separate segment
- Implement Zero trust micro-segmentation
- Enact Security Zones for different classes of data (yellow, orange, red, red-hot)
- Protect backup systems

AD HARDENING

Most attacks use Bloodhound, ADFind , Powerview, or AD Explorer type tools

These tools can be broken by hardening Active Directory

Remove *enumeration of group membership* privilege by anyone

Remove *enumeration of Admin group membership* by Authenticated Users

To detect AD Recon of certain privileged groups, add auditing of:
- Read all permissions activity
- Read all properties activity

Users in the *Protected Users* group won't use NTLMv2 authentication which means there won't be any hashes for mimikatz to dump and use for pass the hash propagation.

DETECTION

Monitor Windows Service creation using SIEM or Splunk dashboard or Kibana

During lateral movement phase of attack, the PSEXEC service is often created on systems the attackers have been able to access with the credentials they harvest

Hunt for PSEXEC service being CREATED and started – this isn't necessary, but attackers often do it for convenience
Trickbot malware also creates a service !!

- AD Honeypot accounts
- Powershell Logging
- Process creation Logging
- Create account profiles for service accounts – if account runs PSEXEC or something out of the ordinary, it should be investigated

DETECTING ACTIVE DIRECTORY ATTACKS

New targeted ransomware attacks throughout 2019 and noticed a trend during the summer to government targets

Analysis of these attacks has found several things they all have in common:

1. Targets all used MS Active Directory for identity and access management
2. Targets all allowed unrestricted Powershell execution
3. Attackers used mimikatz in some form for privilege escalation and compromising AD

A new detection method for seeing these attacks is to create and then monitor honeypot accounts

Use Active Directory for IAM create these accounts and then work with IM to monitor them

AD Honeypot Accounts are created in two forms:

1. Accounts with hard to crack passwords in a fake department
2. Accounts with easy to guess, but believable, passwords that have NO real access or real privileges

AD Honeypot accounts would allow detection of:

Recon Attack using AD Explorer
Kerber Roasting

Account Enumeration using PowerSQL type tools

Admin group enumeration using BloodHound type tools

Password Spray

DETECTING ACTIVE DIRECTORY ATTACKS – HONEYPOT ACCOUNTS

AD Honeypot accounts should be created with normal naming convention for Admins or Admin groups

AD Honeypot accounts should have believable metadata such as description, logon scripts, last login times, last password change dates

AD Honey groups should be created for the fake departments containing computer accounts with file shares and login scripts

Fake computer accounts should list OS as Windows XP or legacy Server 2003 so as to attract interest by attackers

Fake login scripts and home directories should have password.txt files with fake, but believable, passwords in plain text

Create fake LinkedIn profiles, Azure and MS Exchange accounts to go along with the fake honeypot accounts

Other Recommended Protections:

- LAPS – randomize local admin password on each machine
- CredentialGuard – older OS have NTLM digest enabled, CredentialGuard limits the password info that can be dumped from memory by mimikatz
- EDR – Security software that can stop malicious Powershell
- Restricted Powershell mode – limit Powershell commands to these needed for system administration

POWERSHELL HARDENING RECOMMENDATIONS

1) Enable Powershell logging

2) Use Powershell Constrained Language Mode

3) Disable Powershell 2.0 Engine to prevent down grade attacks in Windows 10

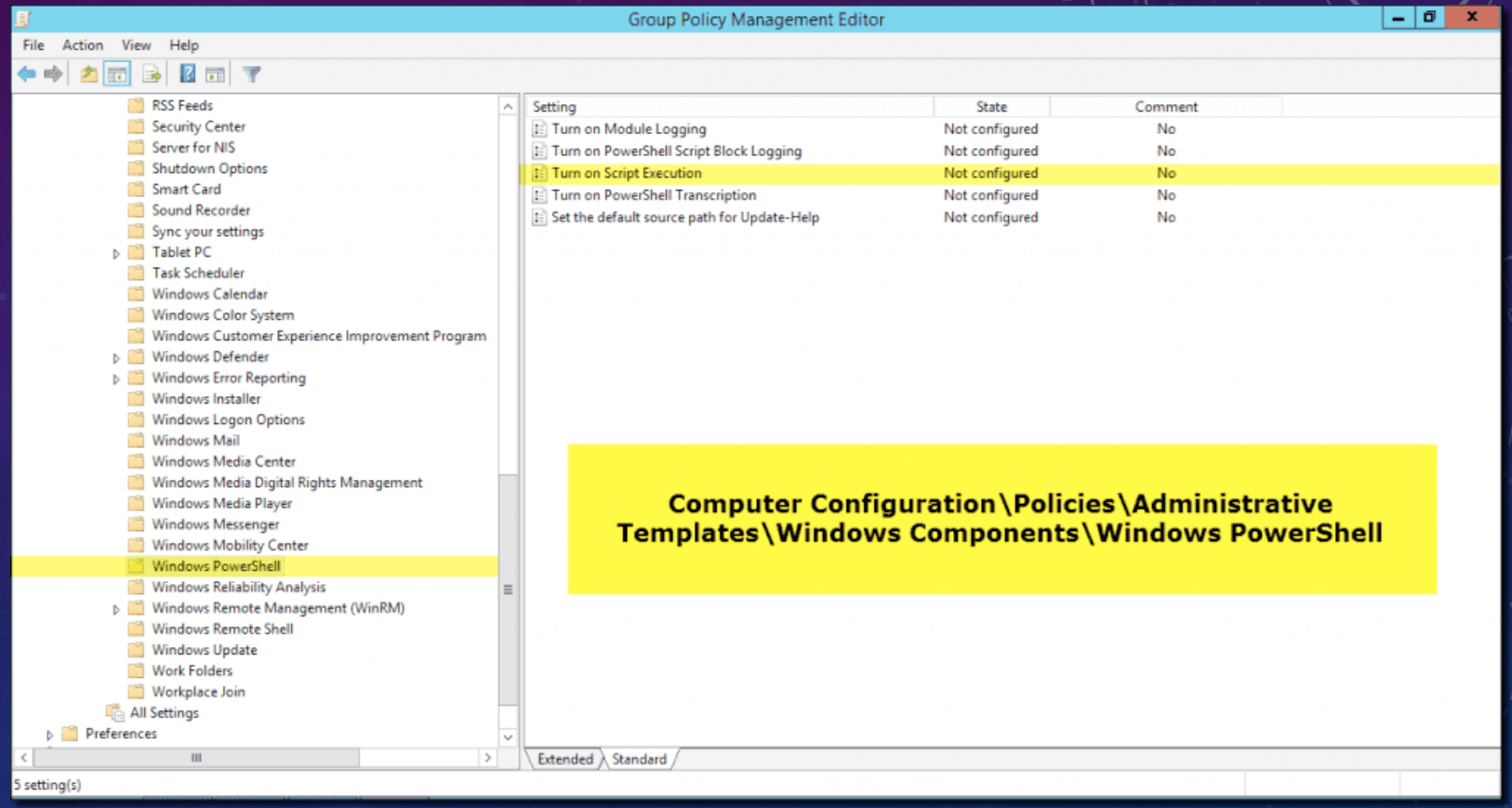
4) Install CVE-2019-0632 important patch to Powershell to fix constrained language mode bypass attack (patched in Feb 2019)

5) Use EDR software that can detect and block powershell abuse

6) Execution Policy Code Signing

POWERSHELL HARDENING

- Require Signed scripts
- Use Constrained Language Mode



POWERSHELL LOGGING

Another critical step for PowerShell and getting visibility is to enable logging. Todays EDR solutions to a good job of identifying when PowerShell is in use, but if you don't have a cutting edge EDR solution it's a good idea to feed PowerShell logs into your SIEM or logging solution.

POWERSHELL LOGGING CHANGES AND OS VERSION

PowerShell Versions and OS: The ability to perform advanced logging of PowerShell is limited to certain operating systems and the versionsof PowerShellused. Basic PowerShell logging is available for all versions of Windows 7, Server 2008 and above, but advanced auditing is limited to PowerShell 4 and 5. The following lists the OS, log(s),andEvent ID's for each operating system and PowerShell version to monitor.

- Windows 7 and Server 2008 and above:
  - PowerShell version 2 thru 4, "Windows PowerShell" log – Event ID's 400, 500, 501and 800
- Windows 8.1and Server 2012 and above:
  - PowerShell version 3 and 4, "Windows PowerShell" log - Event ID's 400, 500, 501 and 800
  - "Microsoft-Windows-PowerShell/Operational" log – Event ID 4104
- Windows 7 and Server 2008 and above:
  - PowerShell version 5, "Windows PowerShell" log - Event ID's 200, 400, 500 and 501
  - "Microsoft-Windows-PowerShell/Operational" log – Event ID 4104

POWERSHELL LOGGING – WINDOWS EVENT FORWARDING (WEF)

What is Windows Event Forwarding? WEF is a way you can get any or al event logs from a Windows computer, and forward/pull them to a Windows Server (collector) acting as the subscription manager.

WinRM must be enabled on all endpoints for this to work.

If you're pushing endpoint events to a WEF collector you will need to create a Group Policy that sets up a subscription manager on all your endpoints.

Log into your collector, run Event Viewer, and click Subscriptions.

You will be prompted to start the service

When you build out your Subscription you pull in events related to PowerShell transcription logging. When building this you will need to log event ID 4104

POWERSHELL CONSTRAINED LANGUAGE MODE

Constrained Language Mode is a very powerful tool for locking down PowerShell.

So what is Constrained Language Mode?

Limits the capability of PowerShell to base functionality, removing advance feature support, such as >NET and Windows API calls and COM access. This lack of advanced functionality stops most PowerShell attack tools, because they rely on these methods. However, in enterprise environments it can negatively affect legitimate scripts; thus it is highly recommended to schedule a testing period before activating this option, to filter out the legitimately used code.

Enable Constrained Language Mode:
[Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine')
Enable via Group Policy:
Computer Configuration\Preferences\Windows Settings\Environment (https://adsecurity.org/?p=2604)

POSSIBLE WAYS TO BYPASS CONSTRAINED LANGUAGE MODE

There are a couple of ways constrained language mode could be bypassed.

- Disable 2.0 Engine to Prevent Downgrade Attacks. If 2.0 is still enabled an attacker can downgrade to use PowerShell V 2.0 allowing the attacker to bypass constrained language mode.
- If an attacker has enough privileges to the targeted system (admin rights) they can remove __PSLockdownPolicy variable (PSLockdown should be used for testing only!) and respawn a new powershell session, thus bypass contrained language mode settings.
- Use GPO to implement enterprise wide and audit changes to the GPO policy for CLM.

DISABLE POWERSHELL 2.0 TO PREVENT DOWNGRADE ATTACKS

With new versions of powershell more security focused features are being put in place. This makes older powershell versions attractive to attackers.

“PowerShell –Version 2 –Command <….>”

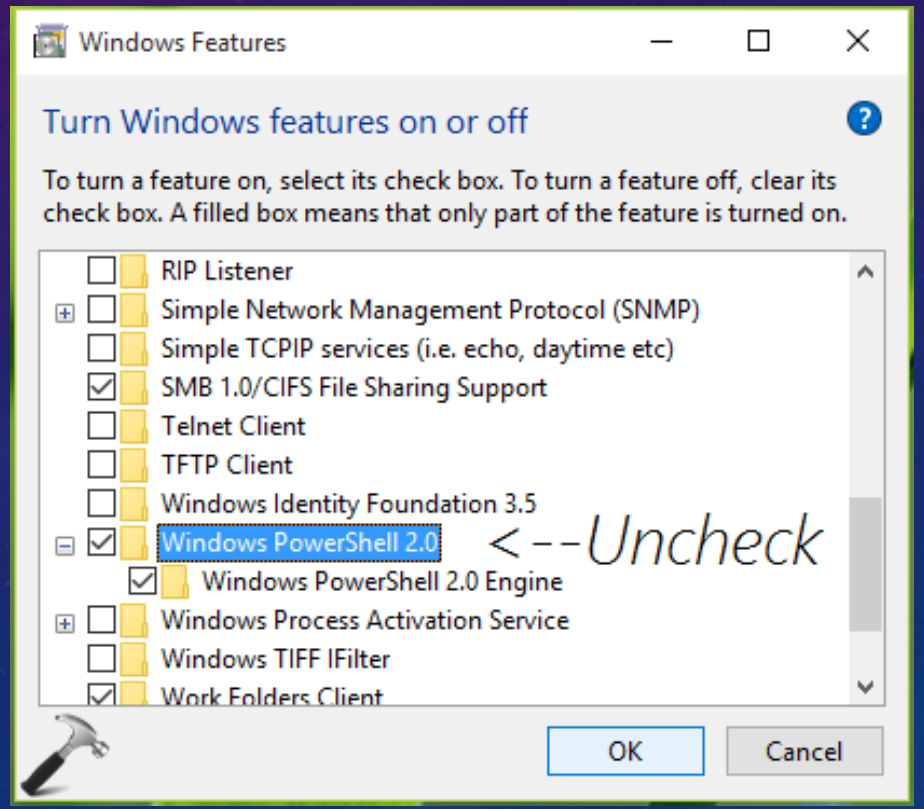
Powershell is a native application. If not disabled an attacker can run the –Version command to switch to an older version that does not have the new security features.

This may not work on Windows 10. Powershell 2.0 requires 2.0 .Net framework, but this framework is not included by default in Windows 10. An attacker could enable or install it on Windows ten. If you are running Windows 10 and have not enabled .Net 2.0, look for instances of this framework being enabled. Could be a sign of an attacker activity in your organization.

DISABLE POWERSHELL 2.0 TO PREVENT DOWNGRADE ATTACKS

It’s fairly easy to disable Powershell 2.0, however it’s a house keeping item that’s often overlooked.

- Open Control Panel and click on the Programs and Features icon.
- Click on the Turn Windows Features on or off link on the left side
- Uncheck Windows PowerShell 2.0 box.
- Click on Close when finished



POWERSHELL EXECUTION POLICY & CODE SIGNING

Some malware will try and pull powrshell scripts from third party sites, like patesbin and box. If you setup to require code signing that will prevent these instances of powershell scripts from running.

If customers can deploy Windows certificate services, which is free, they can digitally sign all their good powershell scripts and then set GPO so powershell won't run anything that isn't signed.
This has the same affect as constrained language mode since malware and pen-test tools don't sign their code. They could, but they don’t.

https://docs.microsoft.com/en-us/windows/win32/seccrypto/certificate-services

AUTHENTICATION HARDENING IN WINDOWS 10

Windows 10 has a password replacement technology called Windows Hello for Business:

https://www.microsoft.com/en-us/itshowcase/implementing-strong-user-authentication-with-windows-hello-for-business

This should ease the adoption of authentication with something other than passwords in the enterprise where single sign-on is desirable

ENABLING PROCESS CREATION LOGGING

enable Audit Process Creation auditing

enable Include command line in process creation

make sure default policy doesn't overwrite the process creation policy

Turning on Process Creation logs: to get Event 4688

admin templates > System > Audit process creation

Policies > Windows > Security > Advanced Audit settings set default file size to large

OTHER TOPICS

Antivirus Signatures

Attackers use an undetected version of the ransomware encrypter or partially disable antivirus so the ransomware can be spread and encrypt files without antivirus interfering.

Using behavior based ransomware detection is recommended. MS ATP Defender has this feature and most newer (2018 – 2019) versions of antivirus software do as well. Sometimes the feature is disabled by default.

CONCLUSIONS

Preventive measures, such as reviewing vulnerabilities on servers, segmentation and reviewing user access rights, are easy to suggest but evidently harder to implement. Endpoint hardening is cheaper and easier.

Start by focusing on how attackers are getting in:

- Email – malware to steal passwords, including RDP passwords
- Managed IT Services providers

Enabling 2-factor authentication mitigates both of these

Since all these targeted attacks abuse Microsoft scripting and Active Directory, harden powershell and AD configuration to remove or limit abused functions

Test backup/restore processes and determine time to recover
Have offsite backup for greater segmentation of backup network

Harden infrastructure against mimikatz activity and elevation of privileges by pass the hash attack

Verify you've done the basics of managing passwords, use least privileges, don't use default security settings, enable Windows logging, collect and audit logs, don't give network login rights to too many accounts