NAVIGATING CYBERSECURITY CHALLENGES

helm
INFORMATION SECURITY

# Easy Playbooks to Make Ransomware Criminals Cry

info@helminfosec.com
www.helminfosec.com

## Playbook 1: Learn about Ransomware!

Review these sources and sample blog entries:

- Ransomware specific
    - DFIR Report: https://thedfirreport.com/
        - Malware-less ransomware (BitLocker): https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/
        - Ransomware under 4 hours: https://thedfirreport.com/2022/04/25/quantum-ransomware/
    - Insights into Conti ransomware group:
        - Translated (By Cisco Talos Intelligence): https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/639/original/Conti_playbook_translated.pdf?1630583757
        - https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/
        - https://media.defense.gov/2021/Sep/22/2002859507/-1/-1/0/CSA_CONTI_RANSOMWARE_20210922.PDF
    - Unit 42: https://unit42.paloaltonetworks.com/bluesky-ransomware/
    - Vitali Kremez on the future of Ransomware as a Service (podcast): https://risky.biz/RBTALKS3/

- General malware capabilities
    - SentinelOne: https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/
    - AdvIntel: https://www.advintel.io/post/bazarcall-advisory-the-essential-guide-to-call-back-phishing-attacks-that-revolutionized-the-data
    - Malware Traffic Analysis: https://www.malware-traffic-analysis.net/
    - Red Canary Intelligence Insights: https://redcanary.com/blog/intelligence-insights-july-2022/
    - Huntress: https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug
    - SANS ISC: https://isc.sans.edu/

Twitter feeds to follow:

- https://twitter.com/phish_report
- https://twitter.com/pr0xylife
- https://twitter.com/JAMESWT_MHT
- https://twitter.com/Cyberknow20
- https://twitter.com/malwrhunterteam
- https://twitter.com/SOSIntel

## Playbook 2: Understand your Footprint

What is your external IP address(es)?

- Check with your documentation from your internet provider
- Google “what’s my IP?”
- You may have several IP addresses reserved around that IP address (some business plans include 5 or more IP addresses)
- Your remote workforce may also have exposed assets. Do you have a way to determine their external IP addresses (EDR visibility, VPN logs, Cloud Apps, etc)?

What is your domain(s):

Are you regularly scanning these using a vulnerability scanner?

If you have no vulnerability scanner, free resources to check for external exposure:

- DNS Dumpster: https://dnsdumpster.com/
    - Free options will show all subdomains for your domain and their likely IP addresses and other information
- Shodan: https://www.shodan.io/dashboard
    - Free options are limited in terms of history and API usage
    - Look for Shodan deals if you can
- Spiderfoot: https://www.spiderfoot.net/
    - Free and paid scanning options with multiple tools

Are your externally exposed resources (email, VPN, VDI servers, MDM, etc.) all protected with strong MFA where possible?

- Best: FIDO2 / YubiKey / Titan Key MFA
- Second Best: Number matching with login context (location and application)
    - Duo “Verified Push”: https://duo.com/docs/policy#verified-push
    - Okta “Number Challenge”: https://help.okta.com/oie/en-us/Content/Topics/identity-engine/authenticators/configure-okta-verify-options.htm
    - Microsoft Number Matching: https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
    - Microsoft App and Location Context: https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
- Good enough (sometimes!): SMS, TOTP (Google Authenticator, Microsoft authenticator, Authy)
- 😢 Push notifications are not great!

## Playbook 3: Risk-based inventory management

What tool(s) in your network can you use to scan for software installed on your computers? Antivirus, EDR, vulnerability scanner, ITSM, etc.?

Commonly abused tools ran by ransomware operators you should look for:

- TeamViewer
- ScreenConnect
    - Multiple instances of ScreenConnect can exist on a single device. Ensure all install instances are legitimate
- AnyDesk
    - Often does not actually require installation; can be run from C:\programdata or another user folder
    - Sometimes the logs can be in the following locations:
        - C:\Users\%username%\AppData\Roaming\AnyDesk\ad.trace
        - C:\Users\%username%\AppData\Roaming\AnyDesk\connection_trace.txt
        - C:\ProgramData\AnyDesk\ad_svc.trace
        - C:\ProgramData\AnyDesk\connection_trace.txt
- Atera
- Splashtop
    - Often installed with Atera
- Remote Utilities Host - https://www.remoteutilities.com/download/
    - Often binaries are renamed to look benign (VMware, etc.)
- WinSCP
- 7-zip
- Winrar / rar.exe
- PuTTY / Plink
    - Plink can be used as a persistent tunnel
- Rclone
    - Command line file transfer utility; does not require install
- Mega / MegaCMD / MegaSync
    - Used to upload data to Mega.nz file sharing site
- ngrok
    - Creates a remote tunnel for operators to use RDP
- PsExec

Does your firewall or other network equipment log application traffic, specifically to file sharing sites (Pastebin, Mega, etc.), RMM tools, and/or outgoing SSH traffic?

## Playbook 4: Mauve Teaming

- Is tamper protection enabled on your AV/EDR? Is it centrally managed? How often are you looking for inactive agents?
- Do you detect suspicious usage of nltest (network discovery) or PsExec (lateral movement)?
    - Nltest
        - Can you run the following commands?
            - `nltest /domain_trusts`
            - `nltest /dclist`
        - Do you have any alerts on EDR/AV after running those commands?
    - PsExec
        - Download here: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
        - Can you use PsExec to perform any commands on another computer?
            - `psexec -i \\your-domain-controller ipconfig /all`
        - Do you get alerts from PsExec usage?
- Do you get any alerts for running executables or other files from C:\Users\Public?
- Are there alerts for new RMM tools?
    - Try to download and run any of the tools from Playbook 3.
    - Do you get alerts?
- Can you connect to file sharing sites like Mega? Can you connect to an external SSH server? Can you see this traffic in your network logs and/or do you get alerts?

## Playbook 5: Test your Backups

When was the last time you restored files from backups?

How long did that take?

Is that fast enough for your business to recover operations?

What users can interact with backups? Can your domain administrators access or tamper with backups?

Do you have offline backups?

## Playbook 6: Prepare for the Worst

When was the last tabletop your organization did? How many scenarios did you run? Did they include ransomware along with different circumstances?

Do you have a list of Incident Response (IR) and/or Managed Detection and Response (MDR) vendors you work with?

Do you have all your contracts and contacts saved securely? Do you know your notification obligations?

Do you have a way to quickly gather triage evidence?

- Velociraptor - https://docs.velociraptor.app/blog/2020/2020-07-14-triage-with-velociraptor-pt-4-cf0e60810d1e/
- KAPE - https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape
- Unix-like Artifact Collector (Linux, Mac, etc.) - https://github.com/tclahr/uac
- AutoLLR (Linux) - https://github.com/Dead-Simple-Scripts/AutoLLR

## Playbook 7: Stay Calm

Keep systems running

- Disconnect from network
- Restarting systems can cause loss of volatile data
- Suspend VMs

If you suspect ransomware or serious intrusion, reset all administrator passwords

- Identify them with the following PowerShell if not using AD Users and Computers MMC Console:
  - `Get-ADGroupMember 'Administrators' -Recursive`
- Disable any suspicious admins you do not recognize

Reset the krbtgt user password **twice**

- In an emergency you can reset the password more quickly than 10 hours (the minimum wait time recommended by Microsoft)
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password
  - More on krbtgt: https://adsecurity.org/?p=483

If needed, engage cyber insurance and breach coaches

- Do you have their contact information saved offline (Playbook 6)?