PLAYBOOK: RANSOMWARE

PREPARE/PREVENT

Endpoint Protection
Updated. Ideally with a blend of techniques such as ML, Signatures, Memory Protection, Script Control

Harden
Patch!, Powershell Script Execution Protection, Windows Exploit Guard with Controlled Folder Access, FSRM for Shared Folders on Win Servers, Known extension blocking on Email.

Backup
Backup Critical Data from endpoints. Ideally offsite such as cloud. R/W access to only a service account.

DETECT

Logging
IOC detection such as Powershell script execution logging, Shadow Backup Deletion - ID4688, with Sysmon or EDR; DNS monitoring for C&C attempts

Filter
Firewall AV/IPS filter, SSL Decryption, Malware / Suspicious Domain blocking at URL Filter.

Threat Intelligence
TI feeds at firewalls, YARA rules at endpoints, MITRE ATT&CK TTP monitoring

RESPOND

Isolate
Isolate any affected endpoint from the network – NAC or EDR for quick/remote isolation.

Investigate
Sandbox Analysis of samples, IOC scanning, determine RCA

Reimage & Restore
Reimage endpoint, restore backup.

LEARN

AUTOMATE – SOAR?

CRITICAL RESOURCES

App Control
Only Run what is allowed

File Integrity Monitoring
Monitor files for changes

Detect
Monitor allowed Apps for behavioral changes/TTPs

Don't Forget
Educate users on phishing & malicious emails, run phishing simulations.

Author:
Ashish Chalke
@theashishchalke

ZERO DEGREES

HARDENING

- ❑ Setting up File Server Resource Manager for Windows Server: https://community.spiceworks.com/how_to/128744-prevent-ransomware-by-using-fsrm?source=start&pos=3
- ❑ Using Windows Exploit Guard: https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/
- ❑ Powershell Script Execution: https://www.mssqltips.com/sqlservertip/2702/setting-the-powershell-execution-policy/
- ❑ Powershell Security Best Practices: https://www.digitalshadows.com/blog-and-research/powershell-security-best-practices/
- ❑ Microsoft – Powershell Script Security: https://docs.microsoft.com/en-us/configmgr/apps/deploy-use/learn-script-security
- ❑ IOC Scanning: LOKI - https://www.nextron-systems.com/loki/
- ❑ Sandbox Analysis: Virus Total, Any.run, hybrid-analysis
- ❑ Phishing Simulation: Gophish – https://getgophish.com

Other Guides:

- Zero Degrees – Phish Defense with Gophish
- CISSP Study Notes

Available at: https://github.com/theashishchalke

Author:
Ashish Chalke
@theashishchalke

ZERO DEGREES