WannaCrypt Ransomware Briefing*

Philipp Hunold
Lead Cybersecurity Specialist WE

*as information is available on May 16th 2017

Attack details

- Ransomware as a threat type has been around for a while
- This wave is unique due to the vulnerability it uses to spread in networks
- Initial attack vector is still mostly email attachments containing droppers

Attack vectors

- Ransomware threats do not typically spread rapidly.
- Usually leverage social engineering or email as primary attack vector
- Exploit code for the patched SMB "EternalBlue" vulnerability, CVE-2017-0145 was used
- Fixed in security bulletin MS17-010, which was released on March 14, 2017.
- The exploit code used by WannaCrypt was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems, so Windows 10 PCs are not affected by this attack.
- 2 main infection vectors:
  - **Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit**
  - **Infection through SMB exploit when an unpatched computer is addressable from other infected machines**

Dropper

- The threat arrives as a dropper Trojan that has the following two components:
  - A component that attempts to exploit the SMB CVE-2017-0145 vulnerability in other computers
  - The ransomware known as WannaCrypt
- The dropper tries to connect the following domains using the *API InternetOpenUrlA()*:
  - www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- "kill switch" for sandbox detection
  - If the malware can connect to these domains, it stops execution and doesn't spread
  - If the domains are not accessible, it drops the malware and creates the service to continue infection

Please note the kill switch mechanism was remove in 2nd variant, and it is not recommend to rely on such for protection!

Security Response

- In March, we released a security update which addresses the vulnerability that these attacks are exploiting
- We suggest you immediately deploy Microsoft Security Bulletin MS17-010.
- Windows Defender detects this threat as Ransom:Win32/WannaCrypt
- We released security updates for unsupported Windows XP and Server 2003

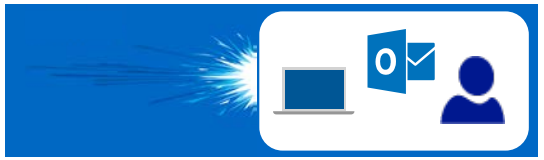
Mitigations

- **If you are unable to update systems**, to contain the spread of the malware
  - **Disable SMB v1 on all systems**
- If not block ports tcp445/139 to further isolate
- **If you are unable to use** an advanced threat protection mechanism such as Office 365 Exchange Online Protection + Office 365 Advanced Threat Protection, consider disabling email attachments in the interim

If you believe you are currently under attack…

1. Contact your Microsoft Service Delivery Manager immediately and we will work with your engineering teams to respond to the threat
2. Cleanup and Restore
   https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx
   https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/
3. Submit a new Sample
   https://www.microsoft.com/en-us/security/portal/submission/submit.aspx

Immediate Front Line Defenses

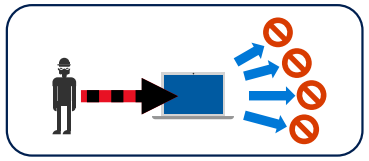


Workstation and User Defenses

1. Mail & App Content Protections
   https://blogs.technet.microsoft.com/office365security/how-to-deal-with-ransomware/
2. Apply Security Updates
3. User Education

Internet Server Defenses

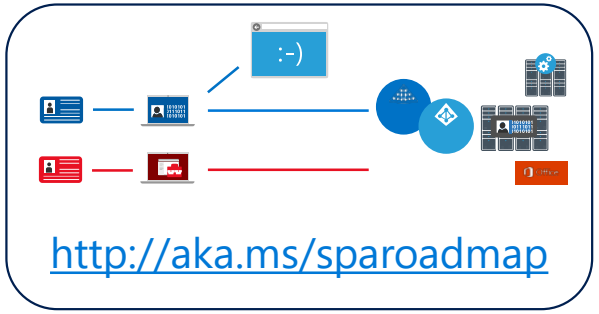
1. Apply Security Updates (Update OS and App as needed)
2. Operational Hygiene (Restrict exposure of privileged access from endpoints)
3. Configuration Hygiene (Change default passwords, apply security configurations)



Defenses to contain attackers

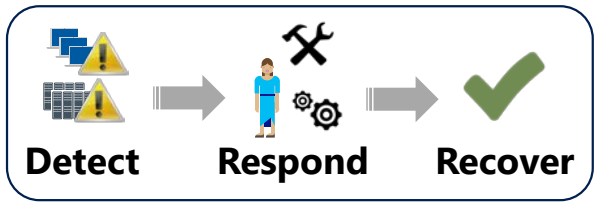
1. Remove Excessive Access to Shared Files

- Remove file share & SharePoint permissions for large groups to overwrite data (Everyone, Authenticated Users, Domain Users, etc.)



2. Securing Privileged Access (SPA) Roadmap

- Immediately implement Stage 1 (separate admin accounts and workstations, random local admin passwords)
- Begin planning Stages 2 and 3



3. Security Operations: Fast Detect and Cleanup

- Leverage cloud enabled anti-malware capabilities for real-time analysis/response (e.g. Windows Defender with Microsoft Active Protection Service (MAPS) enabled and Defender ATP)
- Ensure availability of experienced analysts & responders

Data backup in case of emergency

Disaster Recovery Best Practices

- Backups must include all critical business data
- Backups should be validated

Backups must be inaccessible to attacker

- Offline backup

  or

- Prevent delete/overwrite of online archives by your administrator accounts (which can be stolen by adversaries)

Public cloud provides native offsite backup capabilities

- Basic natural resistance to ransomware (subscription must also be secured appropriately)
- https://blogs.microsoft.com/microsoftsecure/2017/01/05/azure-backup-protects-against-ransomware/

Additional Resources

- MS17-010 Security Update: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Extensive WannaCrypt informaiton: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
- Customer Guideance: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Comment from Brad Smith's President MSFT: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0001tce9xsi6lfglrbg1dwwppt3t0
- https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt
- http://blogs.microsoft.com/cybertrust/2016/04/22/ransomware-understanding-the-risk/
- http://aka.ms/ransomware