WannaCry/WannaCrypt Ransomware

SANS Technology Institute

The best. Made better.

What Happened?

- On Friday May 12th 2017, several organizations were affected by a new Ransomware strain.
- The Ransomware was very successful in part because it used a SMB vulnerability to spread inside networks.
- The vulnerability was patched by Microsoft in March for supported versions of Windows.
- The exploit, known under the name ETERNALBLUE, was released in April as part of a leak of NSA tools.
- Variants have been seen spreading Saturday/Sunday.

SANS Technology Institute

How many infections?

- Several large organizations world wide are known to be affected.
- No obvious targeting. The organizations are from various countries and appear not to be related.
- While large enterprises made the news, small business users and home users may be affected as well.
- Estimated > 200,000 victims according to various anti virus vendors

How do systems get infected?

- E-Mail: Some organizations suggest that the initial infection originated from e-mail attachments, but little is known about the e-mails. It is easily possible that other malware was confused with WannaCry.
- SMB: Affected organizations may have had vulnerable systems exposed via port 445.
- Up to know, affected organizations have not shared a lot of proof to show how the initial infection happened.

What happens to the victim?

- Files with specific extensions will be encrypted.
- The victim will see a ransom message asking for approx. $300. Ransomware demands will increase to $600 after 3 days. After 7 days, the files may not longer be recoverable.
- The ransomware will also install a backdoor to access the system remotely via port 445 (Double Pulsar, also part of the NSA tool set).

How to Prevent Infection: Patch

- Newer Windows Versions (Windows Vista, 7-10, Windows Server 2008-2016) can be patched with MS17-010 released by Microsoft in March.
- Microsoft released a patch for older systems going back to Windows XP and Windows 2003 on Friday.
- Confirm that patch is installed

Other Mitigating Controls

- Segment Network
  - Prevent internal spreading via port 445 and RDP.
  - Block Port 445 at perimeter.
- Disable SMBv1
- Implement internal “kill switch” domains / do not block them
- Set registry key.
- At least one additional variant of the malware was seen this weekend. It uses a different “kill switch”.

SANS Technology Institute

Detect Affected Systems

- Systems that are infected by WannaCry will try to connect to a specific domain.
- Encrypted files will have the “wncry” extension.
- Systems will scan internally for port 445.
- Ransom message will be displayed.
- In addition, infected systems will reach out to sites for crypto keys.
- Anti-Malware has signatures now for WannaCry.

Ransom Note

SANS Technology Institute

Cleaning Up Infected Systems

- Anti-Malware vendors are offering removal tools.
- Removal tools with remove malware, but will not recover encrypted files.
- WannaCry will install a backdoor that could be used to compromise the system further.
- Note that not all files with the .wncry extension are encrypted. Some may still be readable.

SANS Technology Institute

Kill Switch

- The malware will not run if it can access a specific website.
- This web site has been registered to stop the spread of malware.
- But proxies may prevent connections. An internal website may be more reliable and allows detecting infections.
- A registry entry was found that will prevent infection as well, and a tool was released to set the entry.
- Future versions will likely remove these kill switches or change the name of the registry entry.

Will Paying the Ransom Help Us?

- There is no public report from victims who paid the ransom.
- About a hundred victims paid so far.
- The unlock code is transmitted in a manual process that requires the victim to contact the person behind the ransomware to transmit an unlock code.
- Due to the law enforcement and public attention, it is possible that the individual(s) behind this malware will disappear and not release unlock codes in the future.

Impact / Summary

- Availability

  Affected organizations will loose access to the files encrypted by the malware. Recovery is uncertain even after paying the ransom.

- Confidentiality

  The malware does install a backdoor that could be used to leak data from affected machines, but the malware itself does not exfiltrate data

- Integrity

  Aside from encrypting the data, the malware does not alter data. But the backdoor could be used by others to cause additional damage

Additional Links

- Technical Webcast: https://www.sans.org/webcasts/massive-ransomware-crisis-uk-health-system-105150
- Microsoft Guidance https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Internet Storm Center: https://isc.sans.edu

SANS Technology Institute