WannaCry ransomware: Attack analysis

On Friday the world witnessed a cyber attack on a scale rarely seen, with a wide range of organizations including NHS England, the Russian Interior Ministry and Nissan Renault were all brought to a halt.

This attack represented a perfect storm of cyber threats exploiting a lack of user awareness, unpatched vulnerabilities and the failings of antivirus to detect new or unique threats.

Avecto has discovered several Bitcoin wallets valued at around £14k each linked to the Wannacry malware. Compared to Cerber ransomware which was estimated to be on track for about $2.4million this year, this is a low yield and suggests either a lack of technical sophistication or possibly a greater desire to disrupt than profit.

Patching with MS17-010 will prevent WannaCry from spreading via the SMB worm, but will not prevent users from being re-infected directly via phishing emails or downloads. It is essential to deploy privilege management and whitelisting to ensure these payloads cannot re-infect machines and cause another outbreak.

Avecto's analysis found that the initial infection requires local admin rights to install a payload into the Windows folder and begin spreading via the SMB worm. In our analysis, the combination of privilege management and application whitelisting was able to prevent the WannaCry ransomware from infecting systems and spreading.

The origin of the attack is still unknown. While phishing or malvertising remain likely candidates, there is also the possibility that the machines have been previously compromised and the attackers have been waiting to deploy this attack at scale for maximum impact. No matter what the origin, it is vital to implement least privilege and whitelist to prevent attackers gaining a foothold on systems.

It is for these reasons that it is more important than ever to recognize the best practice security advice that SANS, GCHQ, Government agencies and Avecto advocate:

1.1. Application whitelisting

Although the initial attack vector is not clear, attackers will look for ways to introduce malicious applications to a system. By implementing application whitelisting it's possible to prevent the initial infections and cut off the attack before it can spread. As whitelisting only allows the known good to run it is far more effective than antivirus, which tries to detect millions of possible bad applications.

1.2. Application patching

Attackers will commonly use vulnerabilities in Microsoft Office or browser plugins to launch malware on a victim's machine. Many of these attacks can be prevented by keeping applications patched. In the case of unpatched or zero day exploits, using least privilege and application whitelisting can mitigate the risk.

1.3. OS patching

In the case of this attack, a key part of the Windows operating systems contained a vulnerability which allows an attacker to move from machine to machine, spreading the infection further. Although Microsoft issued a patch for this in March 2017, many

*https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis organizations have been slow to roll this out, or are reliant on out of date Windows XP machines which are no longer officially supported by Microsoft.

1.4. Reducing admin users

Reducing local admin users is often seen as one of the most important steps to securing an organization. In this case, the initial payload was unable to execute successfully without access to admin rights stopping the attack at the earliest stage before it could spread.

The SMB flaw in the Windows operating system was so severe that the attackers were able to launch code in a privileged context. However, if the attackers did not have access to this vulnerability they would have had to exploit local admin rights in order to infect systems and spread in this way. Organizations who deploy the MS17-010 patch but still use local admin accounts could still be affected by a self-propagating attack using pass the hash techniques rather than vulnerabilities.

If the malware has access to admin rights it will successfully infect the machine and try to spread across the network.

Our analysis showed that the combination of privilege management and application whitelisting was able to prevent the WannaCry ransomware from infecting systems and spreading.

1.5. Summary of the Wanacry/Wcry attack

- Stage 1 - A initial machine was infected (likely via a phishing email).
    - Whitelisting could have prevented this initial malware payload from running stopping the attack at an early stage before it could spread
    - Privilege management could have prevented the payload launching successfully and prevented it from spreading across the network.

Privilege management also makes application whitelisting achievable, as it allows you to take control of the build.

- Stage 2 – If stage 1 wasn’t prevented, the infected machine would use a known Microsoft vulnerability to move laterally across the network infecting other machines.
    - As the malware is using a flaw in the Windows operating system it automatically runs with the highest level of privilege on unpatched systems
    - Although not used in this case, the most common way of achieving lateral movement is to perform a pass the hash attack using admin privileges which is why it is extremely important to both patch and remove admin rights on endpoints.

No one vendor has all the answers when it comes to cyber security, but our approach has repeatedly been supported by expert research as the most effective at dealing with attacks.

WannaCry is just the latest example of the importance of best practice security foundations to properly secure endpoints.

*https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis