Could BlueKeep become the next WannaCry? What you should do to protect your organization.

ARTICLE 05.23.19 DEAN DORTON

By: Corey Shell, Senior Cybersecurity Consultant

The WannaCry ransomware struck across the globe in May 2017, affecting more than 200,000 victims and 300,000 computers in 150 countries. Cyence, a cyber-risk modeling firm, estimated the economic losses from the campaign reached up to $4 billon. WannaCry was able to spread by exploiting a known weakness in Windows computers. While Microsoft had previously released patches to close the exploit, much of WannaCry's spread was from organizations that had not applied these or were using older Windows systems that were past their end-of-life (such as Windows XP and Server 2003).

Last week, Microsoft released fixes for a critical Remote Code Execution vulnerability known as BlueKeep (CVE-2019-708) in Remote Desktop Services—formerly known as Terminal Services—that affects some older versions of Windows. This vulnerability is pre-authentication and requires no user interaction. In other words, the vulnerability is "wormable," meaning that any future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017. While malware has not yet been observed exploiting this vulnerability, there is publicly available exploit code that can be easily integrated into current malware variants to create a WannaCry-like worm at any time.

It is important that affected systems are patched as quickly as possible to prevent such a scenario from happening. In response, Microsoft has taken the unusual step of providing a security update for all customers to protect Windows platforms, including some unsupported versions of Windows.

Vulnerable supported systems include Windows 7, Windows Server 2008 R2, and Windows Server 2008. Downloads for in-support versions of Windows can be found in the Microsoft Security Update Guide. Customers who use a supported version of Windows and have automatic updates enabled are automatically protected.

Unsupported systems include Windows 2003 and Windows XP. If you are on an end-of-life version, the best way to address this vulnerability is to upgrade to the latest version of Windows. Even so, Microsoft has released fixes for these end-of-life versions of Windows in KB4500705.

It is very possible that a malware campaign in the near future will spread similarly to the WannaCry malware, and may perhaps even be called "Wannacry 2.0." Failing to mitigate this vulnerability could lead to significant business disruption for organizations and may result in significant losses for any organizations that fail to prepare for such an attack.

Dean Dorton recommends that organizations consider the following to prevent an outbreak of a "Wannacry 2.0" type of malware in their environment:

- Install the latest security updates available from Microsoft.
  - If you are using supported operating systems such as Windows 7 and Server 2008, you can find the relevant updates here.
  - If you are using unsupported operating systems such as Windows XP and Server 2003, you can find the relevant updates here.

    - You should migrate from these end-of-life operating systems to supported operating systems as soon as possible. These systems should be segregated from the rest of the network until they are upgraded.
- If not necessary for business purposes, disable Remote Desktop.
- Ensure Remote Desktop services (TCP port 3389) are not directly internet accessible.
- Enable Network Level Authentication (NLA) (this is a mitigation against the exploit if immediate patching is not available).
- Implement firewall rules which only allow access to RDP from approved IP address ranges.
- To prevent lateral movement (Pass-the-Hash), you should assign unique passwords for local administrator accounts. Microsoft has released a free tool called "Local Administrator Password Solution" (LAPS) which can automate this process.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Test your backups to ensure they work correctly upon use.
- For remote administrative access and highly sensitive systems, consider deploying two-factor authentication (2FA).
- If possible, block access to newly seen domains, using a solution such as Cisco Umbrella.
- Perform regular cybersecurity assessment and penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical. Dean Dorton can perform these tests for you.