UPDATE: U.S. DHS Issues Revised Alert on WannaCry Ransomware

New Alert Details Indicators Associated with Ransomware and Recommended Steps for Prevention and Remediation
By: Linda Perkins
Cyber Law and Data Protection Alert
5.15.17

Previously, White and Williams Cyber News blog reported on the WannaCry ransomware attack that started Friday afternoon and has already impacted over 200,000 computers across 150 countries. Today, US-CERT (the United States Computer Emergency Readiness Team), through its National Cyber Awareness System, released new information with an overview of the WannaCry ransomware attack. In this new alert, US-CERT addresses the impact on Microsoft Windows operating systems.

Key portions of today's US-CERT alert are provided for your convenience below:

Description

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers either through Remote Desktop Protocol (RDP) compromise or through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 operating systems on May 13, 2017. According to open sources, one possible infection vector is via phishing emails.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Solution

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.

  - Enable strong spam filters to prevent phishing e-mails from reaching the end users and authenticate in-bound e-mail using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent e-mail spoofing.
  - Scan all incoming and outgoing e-mails 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 e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Develop, institute and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Have regular penetration tests run against the network. No less than once a year. Ideally, as often as possible/practical.
- Test your backups to ensure they work correctly upon use.

Recommended Steps for Remediation

- Contact law enforcement. We strongly encourage you to contact a local FBI field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Report Notice

DHS and FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to DHS or law enforcement immediately. We encourage you to contact DHS's National Cybersecurity and Communications Integration Center (NCCIC) (NCCICcustomerservice@hq.dhs.gov or 888-282-0870), or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

* * *

As always, we encourage our clients to remind their employees to also be vigilant in updating any personal devices they may use, especially if those devices connect to business or workplace servers or network systems in any manner.

US-CERT regularly updates its Current Activity webpage as new advisories and alerts are issued. This information is made available to the public and business owners in an effort to keep them informed of current online threats. White and Williams monitors US-CERT alerts in an effort to keep its clients well informed when critical threats emerge.

White and Williams reminds its clients that internet security remains a critical component of any workplace policy or business operation plan. If you have questions or would like to discuss your policies and plans related to data privacy and cybersecurity, please contact Richard Borden (bordenr@whiteandwilliams.com; 212.631.4439), Josh Mooney (mooneyj@whiteandwilliams.com; 215.864.6345), Jay Shapiro (shapiroj@whiteandwilliams.com; 212.714.3063) or Linda Perkins (perkinsl@whiteandwilliams.com; 215.864.6866).

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.