CAPINTECH

A Cyber Attack of Unprecedented Scale: What You Need to Know About the WannaCry Ransomware Program

Just days after President Trump signed a much-anticipated executive order on cybersecurity, a massive cyberattack — potentially the largest the world has ever seen, with more than 75,000 ransomware attacks in 153 countries — stole headlines.

The "WannaCry" ransomware program hit organizations around the world on Friday, May 12, encrypting computer files and demanding roughly the equivalent of $300 in Bitcoin (increasing over time) to restore user access.

Russia, Ukraine, India, and Taiwan were reportedly the most affected countries, but organizations across Europe, Asia and North America — with an estimated 3,300 infections in the U.S. alone — were also attacked. Notable targets included, among others, the Russian Interior Ministry, logistics carrier FedEx, automakers Renault and Nissan, a number of Chinese universities and secondary schools, as well as Britain's National Health System (NHS). Forty-seven of the 248 NHS trusts were attacked by the ransomware program, and as of May 15, seven trusts had yet to regain control of their computer systems.

The rapid spread of WannaCry is slowing, for two primary reasons: 1) Microsoft took the rare step of issuing patches for outdated versions of Windows operating systems it no longer supports, going back as far as 14 years; and 2) the accidental discovery of a "kill switch" by a security researcher in Britain, which spared much of the U.S. However, neither "fix" helps systems that are already infected, and hackers could easily create a new strain of WannaCry that bypasses or negates the kill switch.

In response to the threat, the FBI issued a FLASH (FBI Liaison Alert System) report with confirmed threat indicators and recommended steps for prevention, remediation, and defending against ransomware generally.

What is ransomware?

Ransomware is a type of malware that targets critical data and information systems for purposes of extortion, preventing users from accessing their data files until a ransom is paid. The software frequently infects computers through spear-phishing — a targeted attack via a malicious link or email attachment. Ransom demands are most often made in the difficult-to-trace virtual currency Bitcoin.

What's different about WannaCry?

In April, an elusive cyber group called the "Shadow Brokers" leaked a cache of powerful NSA hacking tools, including highly sophisticated (and expensive) software exploits. WannaCry is purportedly based on one or more of these exploits, taking advantage of a zero-day vulnerability in Microsoft Windows that enables it to spread itself laterally. Microsoft issued a security update to address this bug in March, but users that didn't make the update remain vulnerable.

WannaCry is the first cyber program to make use of the leaked NSA tools — but likely not the last.

Why were healthcare organizations the hardest hit?

The healthcare sector remains uniquely at risk to cyber incidents due to a variety of factors, including a lack of resources devoted to cybersecurity, the complexity of networks, and the vast array of Internet-connected

75,000+
Ransomware attacks

153
countries

devices. Because many hospitals still maintain and rely on end-of-life technologies, and may prioritize immediate access to data over data security, cybercriminals have found their systems relatively easy to penetrate.

The healthcare sector is also one of the most targeted sectors by cybercriminals and nation states because it is the only sector which combines highly valuable and sought-after bulk data sets of personal health information, personally identifiable information, payment information, medical research, and intellectual property.

Hospitals also don't have the luxury of time: A ransomware infection that blocks access to critical medical data endangers patients' health. Ahead of a scenario where patients' lives are at risk, organizations should ensure they have preventive measures in place.

The WannaCry attack was entirely preventable. It succeeded at infecting computers because users failed to install a months-old patch.

Is your organization safe?

The FBI recommends the following preventative measures:

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017. (Organizations using unsupported Windows operating systems including Windows XP, Windows 8, and Windows Server 2003 should follow customer guidance from Microsoft.)
- Enable strong spam filters to prevent phishing emails from reaching end users and authenticate in-bound email using technologies like Sender Policy Framework, Domain Message Authentication Reporting and Conformance, and DomainKeys Identified Mail.
- 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, assigning administrative access only when absolutely needed.
- Configure access controls including file, directory, and network share permissions with least privilege in mind.
- 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.
- Have regular penetration tests run against the network, no less than once a year, and ideally, as often as possible/practical.
- Test your backups to ensure they work correctly upon use.

We offer these additional recommendations:

- **Don't forget the human element.** The WannaCry attack was entirely preventable. It succeeded at infecting computers because users failed to install a months-old patch — in other words, because of human negligence and a lack of awareness. Change user behavior by introducing a training program based on employees' organizational roles, implementing cyber hygiene best practices (i.e., not opening suspicious emails or attachments), and regularly testing the program's effectiveness.
- **Implement a risk-based, threat-driven patch management program.** Patch management should be a dynamic, risk-based process rather than a check-the-box compliance approach. Organizations must be able to identify system vulnerabilities and relevant patches in a timely manner, understand the degree of risk the vulnerability presents, and work with asset owners to deploy the update.
- **Monitor, monitor, monitor.** To be cyber resilient, organizations need to have threat monitoring and analytics tools to detect an attack, as well as the investigative and digital forensics capabilities to understand what went wrong and the scope of the damage. The sooner a cyberattack is detected, the sooner incident response and mitigation strategies can be put into effect. When it comes to ransomware, early detection can make all the difference in salvaging critical data and information systems.

What should you do when preventative measures fall short?

- **Isolate the issue.** Buy more time to respond to the attack by removing infected systems from the network and cutting off access to the parts of the network that are not corrupted. Change the passwords to those isolated segments, if possible.

- **Secure backup data or systems by taking them offline.** Make sure your backups are clean.
- **Contact your local FBI field office's Cyber Task Force immediately.** The FBI is there to help; its role is not to find fault or lay regulatory blame on a victim organization, but rather to conduct the investigation in cooperation with the victim organization and determine who perpetrated the attack.
- **Implement your incident response plan.** Ensure all stakeholders have been notified and understand their respective responsibilities.
- **Change all passwords.** Once your networks are back up and running, change all online account and network passwords.

All organizations are at risk of a cyberattack. Visit capintech.com to learn how we can help your organization assess and reduce your cybersecurity risk.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.