Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 32 – December 2019

Authored by: Lee Kim, BS, JD, CISSP, CIPP/US, FHIMSS
Director, Privacy and Security, HIMSS

Threat, Vulnerability, and Mitigation Information

1. A critical vulnerability has been discovered in a popular remote access software. The software manufacturer has issued patches for the vulnerability (CVE-2019-19781).

2. A software manufacturer for advanced server security solutions has issued a security bulletin for StartTLS LDAP confidentiality and local arbitrary file overwrite vulnerabilities (CVE-2019-15626 (information exposure) and CVE-2019-15627 (arbitrary file deletion or overwrite)). Exploits targeting these vulnerabilities have been publicly released. The time to patch is now.

3. According to reports, Shade ransomware is the most popular variant that is delivered by way of email. It is a multinational threat that has targeted the United States, Canada, Russia, Japan, Thailand, and elsewhere.

4. LooCipher is another new ransomware family that is reportedly in the early stages of development. The ransomware is said to be delivered through a DOC file. If a user enables macros, then LooCipher is downloaded from a remote server once the document has been opened. Decryptors are available for this ransomware family.

5. An authentication bypass vulnerability (previously analyzed as CVE-2018-9022) in certain versions of a privileged access manager allows remote attackers to execute arbitrary code or commands by poisoning a configuration file. Additionally, an authentication bypass vulnerability (previously analyzed as CVE-2018-9021) in certain versions of a privileged access manager allows remote attackers to execute arbitrary commands with specially crafted requests. Proof of concept code may be found here.

6. Potential indicators of compromise of an alleged nation state-backed actor APT20 for Operation Wocao have been disclosed by researchers. Victims are reportedly in at least ten countries and in government entities, managed service providers, and across a wide variety of industries including healthcare. Additionally, it has been reported that the APT20 group has been able to bypass two-factor authentication.

7. Emotet malware has been quite prolific around the world, including in Japan. JPCERT/CC recently issued a revised bulletin on the topic, along with potential indicators of compromise.

8. Predictions for cybersecurity threats in 2020 are in no short supply. However, one source has analyzed these predictions from a variety of sources. Top predictions include significant ransomware activity, cyber-attacks exploiting unpatched vulnerabilities outpacing the rate of patching systems, increased attacks on cloud computing platforms (fueled, in part, by cloud misconfigurations), and the rise of deep fakes. On a related note, a cloud misconfigurations may include something simple such as failing to secure sensitive data with a password.

9. Yet another source had a bot analyze over one-thousand predictions for 2020 and it had written predictions of its own. Predictions include a growth of zero trust attacks, more cloud weaponization, and a steady growth of Internet of Things-related attacks. Additionally, 5G will open up a new vector of attack, albeit at unprecedented speeds.

Research and reports

1. A certain package manager for JavaScript reportedly has an "open system" which allegedly introduces significant security risks. According to researchers, attackers need to compromise a very small number of maintainer accounts to inject malicious code into a majority of the JavaScript packages.

2. Researchers have discovered that hackers are exploiting the remote desktop service for fileless malware attacks. Attackers are allegedly trying to reach as many victims as possible. Clipboard stealers, ransomware, cryptocurrency miners, and Trojan stealers are deployed by the attackers.

3. Researchers report that 1 in 172 active RSA certificates may be compromised due to a recently discovered vulnerability (random number generation). Additionally, researchers state that a quarter million keys from the past five years are vulnerable to the attack, even for an attacker with limited resources.

4. Researchers espouse the merits of artificial intelligence and machine learning as applied to cybersecurity challenges of the future. A repository of training data, shared data logs, and attack details can be generated as results from grand challenges.

5. Researchers disclose a novel methodology for providing strongly deniable authenticated key exchanges for secure messaging. A deniable authenticated key exchange protocol establishes a secure channel without providing cryptographic evidence of the communication.

6. Researchers have developed a phishing database with phishing domains, websites, and other relevant information. Another phishing database that is said to gather phishing uniform resource locators (URLs) in real-time may be found here.

7. The U.S. government released a software reverse engineering framework to the open source community (Ghidra). The Ghidra Suite may be obtained here.

8. An in-depth report on patient safety and cybersecurity helps to demonstrate that the two are intertwined. Cybersecurity in healthcare organizations is different from other sectors in that cyber defense measures must be considered carefully, especially when patient lives are on the line.

9. A breakdown of cybersecurity professional salaries by role, years of experience, region, and industry shows that North American salaries generally ahead of Europe and Asia. Healthcare salaries, at times, lag behind other sectors according to the study.

10. Basic tips can be implemented by anyone and at any time, including while on holiday travel. Sometimes, to need to get back to the basics when it comes to keeping our assets and data safe and secure. As an example, passwords should not be reused. Another example is to increase your situational awareness about the latest threats (such as cryptojacking).

11. While there are many cybersecurity courses available online, one source has a free course for beginners.

Special Announcements

1. Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders and healthcare constituents to discuss and learn about advancing the state of cybersecurity in the healthcare sector. Please note: HIMSS membership is required to join the HIMSS Healthcare Cybersecurity Community.