Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 31 – November 2019

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

Threat, Vulnerability, and Mitigation Information

1. US-CERT has issued an alert (AA19-339A) regarding Dridex malware. It has been previously reported that Dridex may evade detection by anti-virus software. Certain variants of Dridex malware have contained malicious Visual Basic code.
2. Purelocker is an example of relatively new ransomware that has been written in the PureBasic programming language. PureLocker targets both Linux and Windows systems. Potential indicators of compromise and other related information have also been disclosed by analysts.
3. Researchers have discovered serious vulnerabilities that affect billions of laptops and desktop computers within the Trusted Platform Module (TPM). Researchers have also developed a proof of concept dubbed "TPM-Fail" that demonstrates the timing leakage problem.
4. Point of sale systems are used frequently in the restaurant and hospitality industries. Yet, these businesses may be slow to patch the point of sale software. While a critical patch (CVE 2018-2636) was released for a popular point of sale operating system over a year ago, it is likely that there are many businesses that have yet to implement this patch. Point of sale systems are popular targets of attackers. Additionally, cybercriminal

groups such as ProCC and RevengeHotels have launched worldwide campaigns against the hospitality industry.

Research and reports

1. Researchers have found that there has been a significant uptick in ransomware targeting businesses for the last two years with local governments, healthcare, and educational institutions being the hardest hit.
2. Researchers have proposed a new methodology for covert communications. The two main components of this methodology are as follows: (1) hiding the secret information and (2) hiding the behavioral aspects of communicating the information. The methodology also focuses on the behavioral security of both the sender and the receiver. The net result is that a third party would not be tipped off regarding the content of the communication or the fact that there has been a transmission of such information.
3. Researchers have disclosed several potential vulnerabilities in blockchain, including structural attacks, peer-to-peer architecture attacks, and application services attacks. Threats to both public and private blockchains are discussed, as well as countermeasures.
4. Tools that are used for offensive purposes can be used for good (such as penetration testing). But, often, these tools can also be used by individuals and entities with malevolent intentions. As a result, threats are much stronger than before on many fronts. Additionally, many environments are still quite insecure.
5. Charging your laptop or device at a public location can lead to a compromise of data. Juice jacking can lead to the installation of malware which, in turn, can lead to bricking your device and/or stealing photos, videos, text messages, and contacts from your device.

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.