Healthcare Cybersecurity Environmental Scan Report

Volume 4 -June 2016

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

Threat, Vulnerability, and Mitigation Information

1. News releases of high-profile data breaches have been used by fraudsters to initiative extortion campaigns. As a result, e-mail extortion attempts have been reported to the Internet Crime Complaint Center (IC3) (Alert No. I-060116-PSA). According to these reports, a ransom payment is demanded from the victim to prevent the release of embarrassing and/or sensitive information. Victims of this extortion are warned that their name, phone number, address, credit card information and embarrassing personal details will be released publicly, such as to their contacts on social media, if they don't pay. More details are available from IC3.

2. IC3 has received reports of tech support scam calls where the subject claims to be an employee or an affiliate of a major software or computer security company offering technical support (Alert No. I-060216-PSA). Some claim to provide technical support services for cable and Internet companies. Additionally, there are claims that the tech support company has received notifications of errors, viruses, or security issues from the victim's computer. The IC3 has received in excess of 3,600 complaints and adjusted losses of $2.2 million from January 1st through April 1st of this year. More details are available from IC3.

3. The Chief of the National Security Agency's Tailored Access Operation talks about security practices and capabilities that may disrupt activity from nation state actors in this video.

4. The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Information on how to participate in AIS can be found here.

5. Copycat extortionists have threatened to distribute denial of service attacks, unless ransom is paid in victim according to reports.

6. Hackers claim to have knowledge of a zero-day vulnerability that gives administrative access to any Windows machine, including a fully patched Windows 10 machine. The zero day vulnerability is allegedly on sale on the black market for $90,000 according to reports.

7. To date, researchers have found over 7,000 variants of FLocker (also known as Frantic Locker or ANDROIDOS_FLOCKER.A). The latest variant of FLocker is reportedly a Trojan program that pretends to be the US Cyber Police or another law enforcement agency. It accuses potential victims of various crimes. Android mobile devices and smart televisions are reportedly affected by this ransomware strain. More technical information can be found here.

8. Researchers have discovered a new RAA ransomware which is created entirely using Javascript. According to reports, it is distributed via e-mail. The malicious attachments appear to be .DOC files at first glance, but they are actually Javascript files (with a .JS extension at the end). When the malicious attachment is opened, the files on the computer will be encrypted and ransom is demanded from the victim. State of the art AES

encryption is used by RAA ransomware. More technical information can be found here.

9. "RansomWeb" attacks are on the rise in 2016. Researchers state that about sixty-percent of all websites contain a vulnerability which can be exploited. These vulnerable websites are exploited by the attackers and ransom is demanded in return for the website database or files. More information can be found here.

10. Adobe published a security advisory (Vulnerability Identifier: APSA16-03), which describes a critical vulnerability in Adobe Flash Player version 21.0.0.242 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. As stated in this advisory, Kaspersky researchers helped Adobe uncover this vulnerability. Additionally, Kaspersky has attributed targeted attacks which exploit this vulnerability to an advanced persistent threat (APT) group called ScarCruft. More information can be found here.

Research and Reports

1. Researchers have found that the United States and Brazil have the poorest performance for preventing and mitigating botnet infections, whereas Germany and the United Kingdom perform the best. Companies based in the United States, Germany, and the United Kingdom have the highest aggregate security rating, whereas Brazil has the lowest rating. More details are available from this report.

2. Researchers have shown that a fabrication-time attack of a fabricated malicious processor. The fabrication-time attack applies to a wide range of hardware and spans the digital and analog domains. The attack affords control to the remote attacker. Further, such attacks are not detectable with state of the art testing. Additionally, an attacker can activate the attack and escalate the privilege of an unprivileged process, without operating system intervention. More details are available from this paper.

3. According to researchers, a strategy deployed by some companies in the face of the ransomware threat is stockpiling Bitcoin currency so that they can pay up quickly, in the event of a compromise.

4. According to researchers, there has been over a 125% increase in distributed denial of service attacks from the previous year. There also was a 138% increase in attacks in excess of 100 gigabits per second. Denial of service attacks remains a top threat for organizations.

5. According to researchers, Mobile App Collusion is a stealthy attack which can be used to break into mobile devices. Malware developers may split their malicious code across different mobile applications or shared code libraries (e.g., software development kits). Using any of these means, mobile app collusion is an attack which is difficult to detect, especially with mobile application sandboxing which is used across many mobile operating systems.

Special Announcements

Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders (from government, the private sector, and academia) and healthcare constituents to discuss and learn about advancing the state of cybersecurity in our healthcare industry. HIMSS members and non-members are welcome!