Healthcare Cybersecurity Environmental Scan Report

Volume 7 - December 2016

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

Threat, Vulnerability, Mitigation, and Awareness Information

1. US-CERT has released Alert No. TA16-336A on Avalanche (crimeware-as-a-service infrastructure). The Avalanche botnet has been used to host and distribute malware to victims, including QakBot (discussed previously in Volume 2) and TeslaCrypt (discussed previously in Volume 3). US-CERT provides remediation steps to take if a computer system has been infected with malware associated with Avalanche.

   A malware package called GozNym (please also see **item #3** under **Reports**, below), designed to steal banking information from infected computers, was also reported to have been used in association with Avalanche. On a related note, the US Department of Justice recently announced the dismantling of this international cybercrime operation with the assistance of law enforcement agencies from 40 countries.

2. The US Internal Revenue Service has released a security awareness publication (no. 4524). Healthcare organizations, among others, have been targeted by tax fraud schemes. More information can be found from the US Department of Justice.

3. Millions of readers who have visited popular news websites are reportedly being targeted by malicious ads which redirect to the Stegano exploit kit. This kit is said to exploit several Flash vulnerabilities and hides in pixels of malicious ads.

4. GoldenEye ransomware is reported to be very similar to the Petya and Mischa ransomware variants. Mischa is said to act as a regular file encryptor and Petya is said to act as the hard drive locker. GoldenEye ransomware may be potentially identified using services such as this one.

5. Popcorn Time ransomware reportedly does not charge victims to decrypt their files, so long as they try to infect two other of their friends. Popcorn Time ransomware may be potentially identified using services such as this one.

6. A new variant of Locky ransomware called "Locky Osiris" has been observed in the wild. It is said to be distributed via fake Excel invoices.

7. A new Cerber ransomware variant has been observed in the wild. An analysis of its behavior and target files can be found here.

8. Researchers have developed an APT Groups, Operations and Malware customized Google search engine.

9. Commentators have stated that the Domain Name System (DNS) may be used as a protocol for covert channels and may also be used to create a covert download channel. By the same token, Internet covert channels may be used as well to transfer information in a "secretive, unauthorized or illicit manner."

10. Nova Labs has developed a virtual cybersecurity lab to raise the level of awareness in regard to cybersecurity defense.

11. To help reduce credit card fraud with "card-not-present" transactions, a technology company has developed a credit card with a dynamic security code, which is said to automatically refresh automatically and randomly each hour.

Reports

1. The White House recently released a "Statement by the President on the Report of the Commission on Enhancing National Cybersecurity." A HIMSS blog post commented on the recommendations by the Commission and the ramifications for the health sector.

2. Traditional encryption can be broken. But, with perfect forward secrecy, keys automatically and frequently are refreshed for encryption and description of information. Researchers have devised an algorithm to accomplish this objective.

3. Researchers report that attackers have been actively involved in developing new banking trojans, such Panda Banker, Shifu, MidasBot, GozNym, Sphinx, and Corebot. Trojans such as these are actively in use all over the world. Researchers also predict that new types of Trojans will be capable of encrypting of blocking access to data on cloud services.

4. Researchers report that attackers have completely automated phishing and vishing attacks on individuals. In addition, these fully automated attacks may be completed in several minutes. No human interaction is needed on the part of the attacker.

5. Researchers report that implantable cardiac devices are vulnerable to denial of service (DoS) attacks and other attacks that can compromise patient safety. Countermeasures are also proposed to mitigate or prevent potential attacks.

6. Researchers report observing a new botnet launching daily massive, distributed denial of service (DDoS) attacks. Researchers have also said that attackers are working up to 24-hours a day.

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. All HIMSS members are welcome!