HIMSS
transforming health through IT™

HIMSS Healthcare and Cross-Sector Cybersecurity Report

Healthcare and Cross-Sector Cybersecurity Report

Volume 8 – January 2017

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

Threat, Vulnerability, and Mitigation Information

1. Cisco has disclosed a vulnerability in the Docker Engine configuration of Cisco CloudCenter Orchestrator (CCO; formerly CliQr) that could allow an unauthenticated, remote attacker to install Docker containers with high privileges on the affected system. The Common Vulnerability Scoring System (CVSS) severity base score for this vulnerability is a 9.8 on a scale of 10 (a critical vulnerability). Cisco has reported the release of software updates that address this vulnerability. Additional information is available here.

2. The Vawtrak v2 banking Trojan, with domain generation algorithm and SSL pinning capabilities, has been discovered in the wild. Additional information about this highly evolved malware can be found here.

3. Researchers have discovered that the Killdisk malware has now evolved into ransomware. In terms of an initial infection vector, attackers are reported to have used spear-phishing e-mails with malicious e-mail attachments (namely, Microsoft Excel documents with malicious macros). Additional analysis about the Killdisk malware may be found here.

4. Researchers have discovered a ransomware variant in development called BadEncript. The decryption key is reported to be not saved and the ransomware program window cannot be closed. Files which are reported to be associated with this malware variant includes badencript.exe, badencriptupdate.exe, and happybadencript.exe. Files encrypted with BadEncript are said to have the ".bript" file extension. The ransom note is said to be located in a file called "more.html." Some potential indicators of compromise may be found here and here.

5. Researchers have discovered another ransomware variant in development called Koolova, which may be a variant of the Jigsaw ransomware. If infected, the Koolova ransomware will reportedly decrypt your files after you read the two specified articles on staying safe online while browsing the Internet and Jigsaw ransomware. The decryption key is then reportedly displayed in a dialog box and you may then enter in the key to decrypt the files. Some potential indicators of compromise may be found here, here, and here.

6. Researchers have discovered a ransomware variant in development called Alphabet ransomware. Some potential indicators of compromise may be found here and here.

7. According to this video, a smart television set appears to have been infected by ransomware, but the television set manufacturer has given instructions on performing a factory reset on the device in response to the reported problem. Additionally, the manufacturer is reportedly taking steps to proactively address the problem.

8. The DROWN attack is not new and neither is SSL v2. However, researchers report that about 28% of servers listening on port 25 (SMTP) (which use the IPv4 address space) still support SSL v2. A presentation on how the DROWN attack works can be *found* here. Other SSL/TLS attacks include Triple Handshake, SMACK, FREAK, Logjam, and SLOTH.

   On a related note, a recent research paper states, in pertinent part, "a large fraction of Internet communication depends on Diffie-Hellman key exchanges that use a few small, widely shared [Diffie-Hellman] groups." Additional information on this research may be found here.

9. The FTC has issued an alert on fake mobile applications. These fake mobile applications may steal a person's credit card or bank information, install ransomware, or steal other sensitive information. The FTC also includes tips on spotting fake mobile applications in the alert.

10. Analysts have produced a report on the top ten most exploited vulnerabilities in exploit kits. The reported vulnerabilities include operating systems, web plug-ins, and web browsers.

Reports and Tools

1. The FDA has released its final guidance on the post-market management of medical device cybersecurity, which aligns with the NIST Cybersecurity Framework.

2. A company experienced a 650 Gigabit per second (Gbps) distributed denial of service (DDoS) attack (namely, a large SYN attack) by the Leet botnet at the tail end of 2016. A first-hand technical analysis of the attack provides additional details on attack patterns, payload analysis, and more.

3. Abuse of the .ch (Switzerland) top level domain (TLD) by the Tofsee botnet has been stopped, according to reports. The domains queried by the

Tofsee malware seem to be algorithmically generated with half of the domains using the .ch TLD. But, the Tofsee botnet has infections worldwide—not just in Switzerland—according to this heat map. An additional botnet tracker, in the form of a live, updated map, can be found here.

4. Researchers anticipate that e-mail, social media, and mobile applications will be primary attack vectors in 2017. Further, activity from government-backed hackers are anticipated to continue into 2017, according to researchers. Proliferation of malware and crimeware as a service is also expected to continue. Additionally, researchers anticipate distributed-denial-of-service attacks and remote access Trojan (RAT) malware distribution using enslaved Internet of Things (IoT) devices. Finally, more man-in-the-browser attacks are anticipated.

5. Researchers have developed a tool called PortEx for static malware analysis of portable executable files.

6. Researchers have developed a tool called Yara which helps malware researchers to identify and classify malware samples. A repository for Yara rules can be found here for malware, malicious documents, and other items.

7. A map which shows reported events in the last 24-hour time period may be found here. In addition, this service is an aggregator of feeds and provides a malicious activity timeline on IP addresses and domains.

8. The Ransomware Chronicle resource provides a listing of ransomware variants from May through December of 2016.

9. The Ransomware Tracker website states that it tracks and monitors the status of domain names, IP addresses, and URLs associated with ransomware.

10. The OpenPhish project provides a free phishing feed, using "proprietary Artificial Intelligence algorithms to automatically identify zero-day phishing sites and provide comprehensive, actionable, real-time threat intelligence."

11. Radio Frequency Identification Devices (RFIDs) are used to identify and authenticate people, objects, and animals. Yet, there are privacy and security concerns since an RFID tag may communicate with a reader over an insecure wireless channel.

    Researchers report that improperly designed RFID authentication protocols, namely poor implementation of random number generators, can lead to significant vulnerabilities. As a result, an attacker may compromise the protocols and recover the secrets because the entropy of the random number generators is likely insufficient. The (improperly implemented) random number generators are thus reported to be the "weakest link" in the RFID authentication protocol.

12. Building control systems (BCS) include physical security access control systems, fire alarm systems, energy management systems, and the like. BCS can be an entry point into an organization. Tactics, techniques, and procedures are provided in this article for detecting, responding to, and recovering from a cyber-attack vis-à-vis BCS. On a related note, please see the Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS).

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!