HIMSS
transforming health through IT™

HIMSS Healthcare and Cross-Sector Cybersecurity Report

Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 18 – December 2017

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

Threat, Vulnerability, and Mitigation Information

1. US-CERT released a malware analysis report (MAR-10135536) of the Trojan BANKSHOT. The associated STIX file may be found here. In addition, a researcher has published Yara rules for BANKSHOT may be found here.

2. The Centers for Disease Control ("CDC") has released its supply chain disaster preparedness manual to help healthcare supply chain managers prepare for disasters.

3. The Securing Mobile Applications for First Responders report describes the findings of a mobile application vulnerability testing program. 32 out of 33 public safety applications had significant and critical flaws. Security concerns of these mobile applications included access to the phone's camera, contacts, recording of audio, sending of SMS messages, the use of hard-coded credentials, and more.

4. An exploitable vulnerability has been found in Western Digital MyCloud PR4100 2.30.172 devices. The web administration component provides

multipart upload functionality that allows unauthenticated attackers to upload a PHP shell onto the device and obtain root level privileges. Additional information on CVE-2017-17560 may be found here: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17560.

Reports and Tools

1. Chubb recently published an infographic titled, "Healthcare by the Numbers: Cybersecurity." Interestingly, Chubb reported that 38% of the reporter cyber incidents over the past *ten years* involved healthcare organizations, the most of any other industry. Chubb also reported that the majority of the reported healthcare breaches was the result of human error and rogue employees (what others may deem to be "negligent insiders" and "malicious insiders"). Additional information may be found in this infographic.

2. The Identity Theft Resource Center, in its 2017 Data Breach Reports, has done its own tracking of data breaches across various sectors and industries. Breaches in the business category tops the list with over 159 million records breached. On the other hand, in the medical and healthcare fields, over 5 million records have been breached. In the ITRC report, there are pages of healthcare organizations with breached records ranging from health plans, various types of healthcare providers, specialty practices, and more. Additional information may be found here.

3. The Chartered Institute of Internal Auditors has issued a bulletin on the General Data Protection Regulation (GDPR). This bulletin also includes a self-assessment table which may be used for internal audit involvement in GDPR activity before, during, and after May 25, 2018 (the enforcement date of GDPR). Additional information may be found here.

4. As one academic paper recently notes, many websites are still vulnerable to Bleichenbacher's RSA vulnerability from 1998, reportedly affecting almost one-third of the top 100 domains in the Alexa top 1 million list. Additional information may be found on sites such as this.

5. A think tank organization in the United Kingdom recently published a paper on the insecurity of undersea cables. This paper states that 97% of global communications relies upon undersea cables. Yet, this paper also calls for more redundancy and resiliency for enhanced security measures. Another resource which identifies jurisdictional and other issues may be found here.

6. A researcher has developed a script to let users scan files with Yara rules and optionally submit the matching rule names to the VirusTotal website. Additional information on the Yara VirusTotal Commenter may be found here.

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!