HIMSS
transforming health through IT™

HIMSS Healthcare and Cross-Sector Cybersecurity Report

Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 13 – July 2017

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

Threat, Vulnerability, and Mitigation Information

1. Researchers have discovered a server message block ("SMB") vulnerability called "SMBLoris." This vulnerability reportedly affects every version of the SMB protocol and every version of the Windows operating system since Windows 2000. According to reports, Microsoft does not plan to address this vulnerability with a security update, but has recommended that enterprise customers should consider blocking access from the Internet to SMBv1. Additional information can be found here.

2. Certain devices running the Android operating system reportedly have malware built into the firmware (Android.Triada.231). The researchers state that this malware is embedded into one of the system libraries, libandroid_runtime.so, which is reportedly used by all Android applications. The researchers have reportedly notified the device manufacturers and recommend that users install all possible updates for such devices. Additional technical analysis may be found here.

3. Win32/Industroyer (also known as CrashOverride) is a sophisticated piece of malware designed to disrupt the working processes of industrial control systems (e.g., electrical substations). The malware relies on four payload

components that each use industrial control systems ("ICS") protocols. The payload has the capability of controlling certain electricity substation' switches and circuit breakers. The final component of the malware has a destructive wiper component. The researchers also warn that attackers could adapt the malware to other industry environments as well, in light of logs produced by the malware toolset and highly configurable payloads.

4. A chemical engineer recently posted his (or her) experience about a coffee machine infecting factory computers with ransomware. This was puzzling—at least initially—since these computers were not connected to the Internet. Apparently, something had hit the local control system and all of the computers were down and showing an error. The coffee machines had shown the same error too. As it turns out, the person who had installed the coffee machines connected them to the control room's network and then to an isolated WiFi network (which connects to the Internet). This person worked for the company responsible for managing the coffee machines.

   Thus, as the story goes, this company (i.e., the one responsible for managing the coffee machines) received a rather angry letter and their clients, too, were without working coffee machines for a few days.

   Nonetheless, at the factory, the affected computers were monitoring systems and the company reportedly had failover mechanisms in place.

5. Adobe has announced that it will stop updating and distributing the Flash Player at the end of 2020. To date, Adobe has been regularly issuing security patches to address security vulnerabilities that have been found. Adobe encourages content creators to migrate any existing Flash content to new, open formats. Previously, Adobe stated that HTML5 will be the web platform of the future across all devices.

Reports and Tools

1. Based upon the findings of a recent survey, most companies are overly confident about the effectiveness of their IT security policies and procedures. However, the reality is that most of these companies still have lax security policies and procedures. The focus of many companies still appears to be perimeter security, but not necessarily defense in depth.

2. Developers have released an application programming interface ("API") security checklist for what they deem to be the most important security countermeasures when designing, testing, and releasing an API.

3. Researchers have developed an exploit kit landscape map, which gives some insight into which exploit kits are currently active, how computers are being directed to them, and which malware they are dropping.

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!