HIMSS

transforming health through IT™

HIMSS Healthcare and Cross-Sector Cybersecurity Report

Healthcare and Cross-Sector Cybersecurity Report

www.himss.org/cyberreport

Volume 16 – October 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 has published Alert No. TA17-293A titled "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors." This report is the result of analytic efforts between the US Department of Homeland Security and the Federal Bureau of Investigation. Both government entities and critical infrastructure organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors may be targeted by an advanced persistent threat group called DragonFly. This is an ongoing campaign since at least May of 2017.

2. FEMA has recently updated its National Incident Management System (NIMS). NIMS provides a common, nationwide approach to enable the whole community to work together to manage all threats and hazards. In addition, NIMS applies to all incidents, regardless of cause, size, location, or complexity. On a related note, FEMA provides training opportunities—additional information is available through its website.

3. Researchers have reported that it may be possible to deploy Dynamic Data Exchange (DDE) attacks in Outlook using e-mails and calendar invites that

have been formatted in Rich Text Format (RTF). Mitigation techniques include viewing e-mail in plaintext.

4. Researchers have devised a method for key reinstallation attacks on Wi-Fi networks which use the WPA2 protocol.   As explained by the researchers, all protected Wi-Fi networks use a four-way handshake to generate a fresh session key. However, these researchers demonstrate that the four-way handshake is vulnerable to the key reinstallation attack (i.e., the adversary has tricked the victim to reinstalling a key which is already in use through manipulation and replay of handshake messages). The researchers further assert that nearly every Wi-Fi device is vulnerable to some variant of the key reinstallation attack. A Youtube video, based upon the paper, is available here. In addition, vendors have issued alerts (such as this one) warning about such WPA2 key reinstallation attacks.

5. Security Service of Ukraine (also known as the SBU) issued a warning a few weeks ago of a possible large-scale cyber attack on private sector companies and government agencies. According to the SBU, the main goal is to cause disruption. Organizations are advised by the SBU to regularly update antivirus software signatures, back up their data, and also regularly check for any software and operating systems updates (including in regard to Windows operating system updates). Various media reports have reported that several transportation organizations and government agencies have been victims of this malware campaign.

   Furthermore, in recent weeks, the BadRabbit ransomware has been quite prolific. According to US-CERT, multiple infections have been reported around the world. US-CERT also states the following: "US-CERT discourages individuals and organizations from paying the ransom, as this does not guarantee that access will be restored. Using unpatched and unsupported software may increase the risk of proliferation of cybersecurity threats, such as ransomware."

On another note, an analysis, which compares EternalPetya (also known as NotPetya) to BadRabbit, may found here. Researchers have also correlated BadRabbit with the BACKSWING Framework. Additional analysis may be found here and here.

Please note: Since the malware campaign may be evolving and the associated findings may be evolving, any such analysis or research should be viewed in that perspective—i.e., the data provided is for informational purposes, but may be subject to change as new findings or situations may arise.

Reports and Tools

1. Researchers have devised automated methods for breaking text-based CAPTCHAs (Completely Automated Public Turing Test To Tell Computers and Humans Apart). CAPTCHAs are images used by websites to block automated interactions (e.g., brute forcing or otherwise). According to the researchers, the ability to learn and generalize is one of the hallmarks of human intelligence. Yet, these researchers appear to have devised methods for emulating the same with this CAPTCHA-breaking technology.

2. Analysts have found that, worldwide, information security hiring managers at healthcare organizations are expecting to increase their workforce by 15% or more. At the top of the list is the healthcare industry with 9% of respondents stating that their workforce will increase by 16-20% and 30% of respondents stating that their workforce will increase by more than 20%.

3. Analysts report that relatively few countries in the Asia-Pacific region have developed national cybersecurity programs and that cybersecurity is still a relatively nascent field. However, on a positive note, 74% of Asia-Pacific organizations devote 5-15% of their total IT budget to cybersecurity. Additionally, 66% of Asia-Pacific organizations reported that their cybersecurity budgets had increased from the previous year. Nonetheless, 33% of healthcare organizations in the Asia-Pacific region experienced a decrease in their cybersecurity budgets from the previous year. Furthermore, the top barrier to ensuring cybersecurity at one's organization was confusion in terms of evolving cybersecurity solutions. Simply put, there are too many evolving cybersecurity solutions to keep up with.

4. Analysts predict that the targeting of medical devices with ransomware will likely increase. Medical devices are part of the "operational technology" of an organization (as opposed to the traditional "information technology" of

an organization). Like other critical infrastructure sectors (including water, electrical, and manufacturing), operational technology is a “soft spot” in regard to cybersecurity. Traditionally, these devices were “walled off” from each other and thus security was not really thought of in terms of the conceptual and design phases of these products. However, now that such devices are increasingly connected and intertwined with our IT infrastructure, these devices pose an even greater security risk than ever before.

Another interesting observation by analysts is that over 40% of healthcare organizations experience thousands of security alerts daily, but only 50% of these alerts are actually investigated.

Analysts also noted that two-thirds of security professionals reported that they use cybersecurity solutions from more than 10 vendors. In pertinent part, analysts stated the following: “The apparent profusion of vendors and products used by healthcare security professionals may result from confusion, or a lack of visibility, about exactly what tools are in place. … Security executives higher up on the leadership ladder—that is, not on the front lines of day-to-day security management—may not have a deep understanding of all the tools on their networks.”

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! Also, please join us in celebrating National Cyber Security Awareness Month this October and check out our resources at www.himss.org/ncsam!