1. US-CERT and the Canadian Cyber Incident Response Centre have issued Alert (TA16-091A), entitled “Ransomware and Recent Variants.” Locky and Samas, two ransomware variants, have been observed infecting healthcare facilities and hospitals worldwide. It also has been reported that systems infected with ransomware are infected with other malware (e.g., CryptoLocker and GameOver Zeus). Previously, June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOver Zeus and CryptoLocker.

2. Researchers have observed a widespread campaign leveraging the Samas/Samsam/MSIL.B/C ransomware variant, thus changing the threat landscape for ransomware delivery. Researchers have also estimated that there are 3.2 million vulnerable machines running unpatched versions of JBoss, which this ransomware variant targets. Information for securing JBoss application servers can found from resources such as this one.

3. Researchers have reported that Manamecrypt (MSIL/Manamecrypt.A, CryptoHost) is a new and severe type of ransomware variant. Manamecrypt is reported to be bundled with “clean” software. It is also reported to not encrypt files, but rather compress files into a password-
protected RAR file. Researchers have provided instructions on how to remove the ransomware, such as here.

4. Security researchers have reportedly developed an online service and a desktop tool for generating a password needed to decrypt a computer which has been infected by Petya ransomware.

5. A security researcher has reportedly developed a tool called “RansomWhere?” to help thwart ransomware attacks against OS X machines.

6. The FBI Cyber Division has released an uncaveated, unclassified document on ransomware (appended to this report). Because ransomware can be highly sophisticated and is constantly evolving, the FBI Cyber Division recommends that organizations have a robust security program with special emphasis on prevention, business continuity, and remediation. The FBI Cyber Division also provides mitigation information in its guidance.

The FBI Cyber Division’s guidance also makes clear that there is no guarantee against exploitation, even with the most robust controls in place. Further, this guidance states that the FBI does not recommend that victims pay the requested ransom. Individuals are encouraged to contact their local FBI Field Office or the FBI’s Internet Crime Complaint Center (IC3) for assistance. Contacting your local FBI Field Office may result in a quicker response.

7. The NSA has released an uncaveated, unclassified document on the Locky variant of ransomware (appended to this report). According to this bulletin, Locky’s main delivery mechanism is through Microsoft Word, Excel, or Outlook attachments. Locky attacks are resilient against countermeasures through updates, code corrections, and new capabilities. Its botnet delivery mechanism has been reported to be similar to the Dridex
trojan horse program. Locky generally evades traditional antivirus defenses. The NSA provides mitigation information, including guidance on application whitelisting, in this bulletin.

8. The FBI has recently issued an announcement about a dramatic increase in business e-mail compromise (“BEC”) targeted companies. According to the FBI, the schemers spoof company e-mail or use social engineering techniques to assume the identity of the company’s CEO, a company attorney, or a trusted vendor. The schemers research who manages money and use language specific to the company which they are targeting and typically request wire transfer payments. From October 2013 through February 2016, is reported that law enforcement has received reports about BEC from 17,642 victims and that the losses have amounted to more than $2.3 billion. The FBI’s IC3 has issued an alert (I-082715a-PSA) on BEC which provides additional information, including where to turn to if you are a victim.

9. ICS-CERT has issued Alert (IR-ALERT-H-16-056-0), entitled “Cyber-Attack Against Ukrainian Critical Infrastructure.” In this report, the BlackEnergy malware variant is suspected to have played a role in this reported cyber attack. An advanced persistent threat group (BlackEnergy) is said to be the originators of the malware. Of particularly note, ICS-CERT strongly encourages organizations across all sectors to review and employ the mitigation strategies as set forth in this alert.

10. US-CERT has issued Alert (TA16-105A), entitled “Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced.” In this alert, Trend Micro is reported to have stated that Apple has ended support for Quicktime for Windows. This alert also states that two new vulnerabilities have been discovered. Since this software is no longer supported, it is recommended that this software be uninstalled from machines as a mitigation strategy.

© 2016 Healthcare Information and Management Systems Society (HIMSS)
11. Adobe has announced a critical vulnerability (CVE-2016-1019) in Adobe Flash Player 21.0.0.197 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. Successful exploitation may cause a crash and potentially allow an attacker to take control of an affected system. A mitigation introduced in Flash Player 21.0.0.182 currently prevents exploitation of this vulnerability, thereby protecting users running Flash Player 21.0.0.182 and later.

12. Reports of a newly evolved Qakbot/Qbot network-aware worm targeting hospitals and other public institutions have surfaced. According to reports, Qakbot is primarily designed as a credential harvester.

13. As noted in this SANS paper, Remote Desktop Protocol (RDP) connections are common intrusion vectors for botnets and other attackers. The default RDP port is port 3389. By changing this to another unused port, organizations may be able to evade certain attacks. It is important for all organizations to know the difference between normal and suspicious behavior or activity on their systems and networks. Resources such as the SANS DFIR “Find Evil” poster may be helpful.

Research and Reports

1. The 2016 Verizon Data Breach Digest states that insider threat continues to be a problem for the healthcare sector. Source of insider threat problems can be from infected USB drives, rogue employees, and third party partners. Additional detection and mitigation information can be found here (posted with permission).

2. The Gone in Six Characters: Short URLs Considered Harmful for Cloud Services reveals the danger of using shortened uniform resource locators (URLs), especially for sensitive information. Using a brute force technique, online resources which may have been intended to be shared with a few
trusted friends or collaborators may be effectively shared with the public and thus accessible to anyone.

3. The ‘PowerShell’ Deep Dive report states that malware created with Powershell is on the rise. The PowerShell-based malware has been reportedly distributed via social engineering techniques, targeting mainly corporate networks, intellectual property, customer data, and financial data. 13% of the attacks were targeted or advanced attacks. 87% of the attacks were a result of click-fraud, fake antivirus, ransomware, and other opportunistic malware.

4. The Return of Qbot report provides an in-depth technical analysis of the Qbot/Qakbot network-aware worm targeting hospitals and other public institutions. To date, many websites have been compromised, including in the United States. The academic, healthcare, and information technology sectors (e.g., IT service companies) have been victims of this compromise.

Special Announcements

Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders (from government, the private sector, and academia) and healthcare constituents to discuss and learn about advancing the state of cybersecurity in our healthcare industry. HIMSS members and non-members are welcome!