Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)

INFRASTRUCTURE INTELLIGENCE NOTE

(U) June 21, 2017; 0930 EDT

(U) RANSOMWARE: A PRIME CYBER THREAT FOR THE HEALTHCARE AND PUBLIC HEALTH SECTOR

(U) Prepared By: Operational Analysis Division

(U//FOUO) SCOPE NOTE: This note is intended to inform infrastructure and cybersecurity professionals in the Healthcare and Public Health Sector about the threats and potential consequences of successful ransomware attacks against the Sector.

(U//FOUO) The U.S. Department of Homeland Security (DHS)/Office of Cyber and Infrastructure Analysis (OCIA) developed this note using government and open source reporting and has high confidence in the accuracy of the multiple government reports referenced. OCIA has high confidence in the accuracy of the open source reporting based on recognized expertise of cybersecurity firms and healthcare companies that specialize in cybersecurity.

(U//FOUO) This product was coordinated with DHS/National Protection and Programs Directorate (NPPD)/Infrastructure Protection/Sector Outreach and Programs Division, DHS/NPPD/Cybersecurity & Communications (CS&C)/National Cybersecurity and Communications Integration Center (NCCIC), DHS/Office of Intelligence and Analysis/Cyber Infrastructure Analysis Division, Department of Health and Human Services (HHS)/Office of the Chief Privacy Officer/Office of the National Coordinator for Health Information Technology, HHS/Office of Civil Rights, HHS/Office of the Assistant Secretary for Preparedness and Response/Office of Emergency Management, HHS/Office of Security and Strategic Information, the Food and Drug Administration/Center for Devices and Radiological Health, and the National Health Information Sharing and Analysis Center.

(U) KEY FINDINGS

- **(U//FOUO) OCIA assesses that the increase in ransomware threats that may affect the Healthcare and Public Health Sector presents a risk to ongoing efforts to develop, maintain, and increase the interoperability of health information systems.**
- **(U//FOUO) Ransomware attacks on the Healthcare and Public Health Sector can have negative effects on the care and safety of patients as well as the efficiency of the affected healthcare organizations.**
- **(U//FOUO) A number of key components contribute to the success of a contingency plan, including practicing good cyber hygiene, the training of personnel on paper record backup procedures, the breadth and depth of data backups, the timeline for backups, the type of data included in the backups, and the duration to restore systems with backups.**

(U) BACKGROUND

(U) Ransomware is a specific type of malicious software (malware) that denies access to data by encrypting files or by locking the user out of the operating system. After establishing control, malicious actors hold access to the data in exchange for a ransom payment. Ransomware attacks have the potential to disrupt operations and inflict costs on owners to restore systems. Ransomware is typically sent to an individual through a phishing email or introduced through an exploitation of a computer vulnerability. The ransom payment is usually the desired goal in

order to coerce victims into paying for the encryption key. The payment methods are often in a cryptocurrency easily accessible around the globe and difficult to trance once completed.[1]

(U//FOUO) The May 2017 WannaCry ransomware attack on organizations across the world underscored the continued ransomware threat posed to critical infrastructure, including the Healthcare and Public Health Sector. Denial of access due to malware infection of patient care delivery systems and devices can result in healthcare providers delivering care with incomplete information or capabilities, potentially endangering patients' lives. Cybercriminals may perceive that organizations within the Healthcare and Public Health Sector will be more willing than other sectors to pay ransom demands more quickly, to regain control of lifesaving systems; avoid putting patients at additional risk of serious medical harm; and reduce the potential of negative open source media reporting.

(U) RANSOMWARE POSES A GROWING THREAT

(U//FOUO) OCIA assesses that the increase in ransomware threats that may affect the Healthcare and Public Health Sector presents a risk to ongoing efforts to develop, maintain, and increase the interoperability of health information systems. The increasing interoperability within the Healthcare and Public Health Sector allows computers and Internet of Things (IoT) devices within a network to communicate more efficiently. Those individual networks are able to connect and communicate with other networks nationwide, allowing healthcare professionals and patients quick and seamless access to electronic health records. The transition to increased interoperability also creates vulnerabilities for cybercriminals using malware, such as ransomware, to exploit.

- (U) Cybersecurity experts anticipate ransomware developers are continuing to devise more persistent and complicated malware that evades detection, has the ability to self-propagate through connected networks, and requires less infrastructure to operate.[2]
- (U) An April 2016 survey conducted by Healthcare IT News and the Healthcare Information and Management Systems Society Analytics found that as many as 75 percent of U.S. hospitals participating in the survey were affected by a ransomware attack within the past 12 months.[3] Another 25 percent of participants were either unsure or had no way of knowing whether they had been subject to ransomware attacks.[4]

(U) THREE VERSIONS OF RANSOMWARE AFFECTING THE HEALTHCARE AND PUBLIC HEALTH SECTOR

(U//FOUO) Three prevalent versions of ransomware used to attack the Healthcare and Public Health Sector in 2016 were the Samsam, Locky, and Cerber ransomware malware. OCIA assesses that all three versions of ransomware are considerable threats to the Healthcare and Public Health Sector. The current versions of each ransomware, discovered in early 2016, have been responsible for highly public cyber attacks.

- (U) Samsam, also known as Samas or Samsa, discovered in early 2016, is a significant threat to the Healthcare and Public Health Sector's interoperability. The malware has the capability to maintain persistence on a system and seek other connected systems to infect, without requiring activation or execution by the victim.[5,6]
- (U) Locky, a type of crypto ransomware, discovered in February 2016, infects computers and systems through email phishing campaigns that contain attached Word documents with embedded macros. The ransomware propagates by exploiting Adobe Flash and Windows Kernel Exploits. Locky uses the Advanced Encryption Standard (AES)[i] encryption algorithm.[7] In the process of encrypting files, Locky will delete all of the Volume Shadow Copies[ii] so victims cannot locally restore their files.[8,9]

[i] (U) Advanced Encryption Standard (AES), is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.
[ii] (U) The Volume Shadow Copy Service provides the backup infrastructure for the Microsoft XP and Microsoft Windows Server 2003 operating systems, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. The Volume Shadow Copy Service can produce consistent shadow

- (U) Cerber, first discovered in March 2016, can be pushed out quickly in large spam campaigns. According to a 2016 study, Cerber is reportedly capable of adding the infected computer to a botnet, which can be used to carry out distributed denial of service attacks. One of Cerber's novel features lets the threat read the ransom note aloud to the victim, using a text-to-speech module.[10]

(U) RANSOMWARE ATTACKS CAN AFFECT PATIENT SAFETY

(U//FOUO) Ransomware attacks on the Healthcare and Public Health Sector have negative effects on the care and safety of patients as well as the efficiency of affected healthcare organizations. Previous ransomware attacks on healthcare organizations resulted in patients being redirected to hospitals not affected by the attacks. Additionally, medical staff often have to revert to using paper and pen when ransomware malware prevents them from accessing electronic records. Doctors and staff have to consider the difficulties they would encounter if their computers, medical devices, and networks were compromised and inaccessible.

- (U) After the May 2017 WannaCry ransomware attack, hospitals in the United Kingdom effectively shut down and were forced to turn away non-emergency patients.[11]
- (U) The March 2016 ransomware attack on a Washington D.C.-area healthcare provider forced the company to shut down their computers and email in 10 hospitals and 250 outpatient centers. The company employees were unable to update thousands of patient records in its central database for several days following the attack.[12]
- (U) The February 2016 ransomware attack on the Los Angeles-based medical center forced employees to resort to paper and faxed documents to communicate. The medical center declared a state of emergency because of the attack.[13]

(U) A ransomware attack on a healthcare organization can affect patients and their medical providers in a number of ways, including delays in the processing of medical orders and inaccessible patient records. Patients are also adversely affected when medical devices are rendered inoperable because of ransomware attacks. U.S. hospitals average 10 to 15 connected devices per bed and larger hospitals can have more than 5,000 beds.[14] Since patients often rely on these devices to survive, ransomware can result in life-threatening situations.

- (U) Most of the attention following a ransomware attack on a healthcare organization is on patient data; however, medical hardware such as MRI machines, ventilators, and some types of microscopes can also be affected by ransomware.[15]

(U) MITIGATING THE THREAT

(U//FOUO) A number of key components contribute to the success of a contingency plan, including practicing good cyber hygiene, the training of personnel on paper record backup procedures, the breadth and depth of data backups, the timeline for backups, the type of data included in the backups, and the duration to restore systems with backups. HHS, the U.S. Computer Emergency Readiness Team (US–CERT), and the Center for Internet Security (CIS) have released documents on best practices for protecting and recovering from a ransomware attack.

- (U) In July 2016, HHS released a fact sheet, *Ransomware and HIPAA*, that "describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the HIPAA has in assisting HIPAA-covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack." The fact sheet also provides information on the HIPAA Security Rule[iii] requirements for the implementation of security measures that can help prevent the introduction of malware, including ransomware.[16]

copies by coordinating with business applications, file-system services, backup applications, fast-recovery solutions, and storage hardware. Several features in the Windows Server 2003 operating systems use the Volume Shadow Copy Service, including Shadow Copies for Shared Folders and Backup.

[iii] (U) For further information, see the HIPAA Security Rule: 45 Code of Federal Regulations (C.F.R.) 164.308(a) (7)

- (U) US–CERT provides recommendations to help individuals and businesses avoid becoming victims of ransomware. The recommendations are general, but provide basic techniques and procedures that users and administrators can apply as preventive measures to protect computer networks from ransomware infections.[17]
    - (U) For information on safely handling email attachments, see Recognizing and Avoiding Email Scams at https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf.
    - (U) For safe practices when browsing the Web, see Good Security Habits at https://www.us-cert.gov/ncas/tips/ST04-003 and Safeguarding Your Data at https://www.us-cert.gov/ncas/tips/ST06-008.
    - (U) Do not follow unsolicited Web links in emails. Refer to the US-CERT Security Tips on Avoiding Social Engineering and Phishing Attacks or the Security Publication on Ransomware at https://www.us-cert.gov/ncas/tips.
- (U) CIS provides recommendations for cybersecurity best practices that are endorsed by leading IT security vendors and governing bodies. To review CIS's best practice techniques for cyber hygiene, see https://www.cisecurity.org/cybersecurity-best-practices/.[18]

(U) The Office of Cyber and Infrastructure Analysis (OCIA) provides innovative analysis to support public and private sector stakeholders' operational activities and effectiveness and to inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis.

PDM16060

(U) SOURCES

[1] (U) June 2, 2017. (U) Ransomware: Goals of Malicious Actors and Current System Vulnerabilities. Overall classification U//FOUO.
[2] (U) NTT Security. SERT Quarterly Threat Intelligence Report Q2 2016. https://www.solutionary.com/_assets/pdf/research/sert-q2-2016-threat-report.pdf, p. 18. Accessed August 30, 2016.
[3] (U) Sullivan, T. (2016). More than half of hospitals hit with ransomware in last twelve months. *Healthcare IT News.* http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months. Accessed September 12, 2016.
[4] (U) Ibid.
[5] (U) Paganini, P. (2016). Why malware like the Samsam ransomware are so dangerous for hospitals? *Security Affairs.* http://securityaffairs.co/wordpress/45974/malware/samsam-ransomware.html. Accessed September 27, 2016.
[6] (U) Symantec. Samsam may signal a new trend of targeted ransomware. http://www.symantec.com/connect/blogs/samsam-may-signal-new-trend-targeted-ransomware. Accessed August 29, 2016.
[7] (U) EAS Encryption. (2016). What is EAS encryption? http://aesencryption.net/. Accessed October 19, 2016.
[8] (U) Microsoft TechNet. (2014). Volume Shadow Copy Service. https://technet.microsoft.com/en-us/library/ee923636(v=ws.10).aspx. Accessed January 31, 2017.
[9] (U) Abrams, L. (2016). The Locky Ransomware Encrypts Local Files and Unmapped Network Shares. *Bleepingcomputer.* https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/. Accessed October 19, 2016.
[10] (U) Symantec. (2016). "An ISTR Special Report: Ransomware and Business 2016." http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf. Accessed May 18, 2017.
[11] (U) The Register. (2017). "UK hospital meltdown after ransomware worm uses NSA vulnerability to raid IT." https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/. Accessed May 16, 2017
[12] (U) Washington Post. "MedStar Health turns away patients after likely ransomware cyberattack." https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.46c24de044df. Accessed May 16, 2017.
[13] (U) Healthcare IT News. "Hollywood Presbyterian hack signals more ransomware attacks to come." http://www.healthcareitnews.com/news/hollywood-presbyterian-hack-signals-more-ransomware-attacks-come. Accessed May 16, 2017.
[14] (U) Wired. "Medical Devices are the Next Security Nightmare." https://www.wired.com/2017/03/medical-devices-next-security-nightmare/. Accessed June 5, 2017.
[15] (U) CNN. "Why hospitals are so vulnerable to ransomware attacks." http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html. Accessed June 5, 2017.
[16] (U) The Department of Health and Human Services. Fact Sheet: Ransomware and HIPAA. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. pp. 1 and 2. Accessed August 23, 2016.
[17] (U) US–CERT. (2016). Alert (TA16-091A). Ransomware and Recent Variants. https://www.us-cert.gov/ncas/alerts/TA16-091A. Accessed August 22, 2016.
[18] (U) Center for Internet Security. "Cybersecurity Best Practices." https://www.cisecurity.org/cybersecurity-best-practices/. Accessed May 18, 2017.

OMB Control No.: 1670-0027
Expiration Date: 10/31/2017

UNCLASSIFIED

Homeland Security

National Protection and Programs Directorate

NPPD Customer Feedback Survey

1. Product Title: Ransomware - A Prime Cyber Threat for the Healthcare and Public Health Sector (FOUO)

2. Please rate your satisfaction with each of the following:

	Very Satisfied (5)	Somewhat Satisfied (4)	Neither Satisfied Nor Dissatisfied (3)	Somewhat Dissatisfied (2)	Very Dissatisfied (1)
Timeliness of product	◯	◯	◯	◯	◯
Relevance of product	◯	◯	◯	◯	◯

3. How did you use this product in support of your mission?

☐ Yes ☐ No Integrated into one of my own organization's information or analytic products
If so, which products?

☐ Yes ☐ No Used contents to improve my own organization's security or resiliency efforts or plans
If so, which efforts?

☐ Yes ☐ No Shared contents with government, private sector, or other partners
If so, which partners?

☐ Yes ☐ No Other uses (please specify)

4. Do you have questions that this product didn't answer?

Yes ◯ No ◯ (Please specify)

5. How could this product be improved?

6. Would you like to see more on this topic?

Yes ◯ No ◯ (Please specify)

7. Are there other topics or questions you would like to see addressed by OCIA?

To help us understand more about your organization so we can better tailor future products, please provide (OPTIONAL):

Name:
Organization:
Contact Number:
Sector: Select One
Partner Type: Select One
State: Select One

SUBMIT FORM

Privacy Act Statement
Paperwork Reduction Act Compliance Statement

UNCLASSIFIED

REV: 14 July 2016