Kentucky Intelligence Fusion Center
FIELD ANALYSIS REPORT
Regional Analysis with National Perspective.
U.S. Department of Homeland Security

21 JULY 2016

(U) Growing Trend of Ransomware Attacks Targeting Hospitals and Healthcare Facilities

(U//FOUO) Prepared by the Oregon Terrorist Information and Threat Analysis Network (TITAN) Fusion Center, with contributions from the Kentucky Intelligence Fusion Center (KIFC) and the Office of Intelligence and Analysis (I&A).

(U//FOUO) ***Scope:*** *This* Field Analysis Report (FAR) *was prepared to highlight the growing trend of cybercriminals attacking hospital and healthcare provider computer systems—operations, patient files, and records—in an effort to obtain a ransom payment for the "return" of control of those systems. It is intended to inform federal, state, local, and private sector partners about the ongoing threat posed by ransomware, specifically as targeted against the healthcare community.*

(U) **Key Judgments:** An uptick in ransomware attacks directed against the healthcare community in the first four months of 2016 underscores the potential vulnerability of all hospital and healthcare provider computer systems.[2,*]

- (U//FOUO) TITAN, KIFC, and I&A have not identified any specific impending or future threats to hospitals or healthcare providers in Oregon or Kentucky.
- (U//FOUO) Recent incidents in the United States, Canada, and New Zealand, however, indicate that hospitals and healthcare providers could become victims. There have been six reported ransomware attacks on healthcare organizations in the United States, affecting at least 16 hospitals during the first four months of 2016.

- (U) End-user training and education about cybersecurity, threats such as ransomware, and systems vulnerabilities could mitigate such attacks in the future.

(U) Targeting Hospital and Healthcare Providers with Ransomware

(U) A number of recent incidents highlight the increasing trend of cybercriminals deploying ransomware attacks to target computer systems of hospitals and healthcare facilities:

- (U) **Los Angeles, California**: For more than a week in February 2016, ransomware infected the IT systems of a medical center, denying access to online patient information. The facility was possibly

[*] (U) DHS defines ransomware as a type of malware that infects a computer and restricts a user's access to it until a ransom is paid to unlock it.

infected via spam e-mails or an affected webpage before spreading to the hospital network. The perpetrator demanded payment in bitcoins to "unlock" the files and return control of the system. Initially, the facility attempted to weather the attack through workarounds; it was later reported, however, the hospital ended up paying the 40 bitcoin ($17,000US) ransom "in the best interest of restoring normal operations… ."[4,5,*]

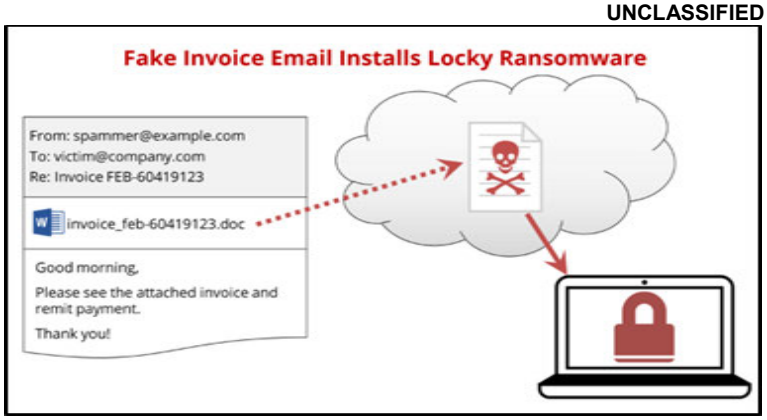
- (U) **Wanganui, New Zealand**: The Wanganui District Board of Health was hit with a ransomware attack in late February. The facility reports paying no ransom and operations continued despite the attack. The facility claims to run up-to-date operating systems with antivirus and malware protection.[7]

- (U) **Ottawa, Canada**: In March 2016, an Ottawa hospital weathered a ransomware attack after 9,800 of its computers were affected by an attempt to lock the files and demand a ransom.[9] The hospital reported that it was able to isolate the computers, wipe the drives, and restore its ability to operate from backup files.[10]

(U) Figure 1: Map depicting targeted hospitals [6]

- (U//FOUO) **Henderson, Kentucky**: Also in March 2016, a Kentucky hospital became the third to be infected with ransomware, limiting its use of electronic web-based services and e-mail.[11] The hackers reportedly made copies of patient records, locked access to the records, and then deleted the originals.[12] The hospital was able to continue normal operations upon activating back-up systems while the main network was locked.[13] A subsequent investigation indicated that the ransomware likely was delivered using e-mails containing malicious attachments.[14]

UNCLASSIFIED



(U) Figure 2: Example of Locky Ransomware lifecycle [8]

- (U) **Madison, Indiana**: In late March, a single-user's files were infected with ransomware at a hospital.[15] An infected e-mail with the subject line "Invoice" contained the name of the hospital's new printer and fax machine in the From field, paired with its official e-mail domain. Systems were intentionally placed offline for approximately 48 hours while the infected device was cleaned.[16]

[*] (U) Bitcoin is a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

- (U) **Southern California:** Two more California healthcare facilities owned by the same parent company were attacked with unidentified ransomware in mid- to late March via the server's network. Confirmation of the type and source of the ransomware has not been received. The company reports refusing to pay the ransom.[17]

- (U) **Baltimore, Maryland**: At the end of March, malware infected some systems at hospitals in Baltimore, preventing users from logging in. The health company quickly shut down its systems to prevent the virus from spreading throughout the organization. Reporting indicates ransomware was a factor.[18]

(U) The attacks in Los Angeles, New Zealand, Kentucky, and Indiana were via a version of ransomware called "Locky," which is spread through e-mail using malicious attachments that encrypt data on the infected system and deletes the originals.[19] Locky-related e-mails include instructions such as "you can download and view a copy of your invoice from the attached document."[20]

(U//FOUO) The healthcare sector has been a desirable target for hackers due to the sensitive nature of patient information contained in their systems. The stakes are very high in the healthcare industry because any disruption in operations and care can have significant repercussions for patients. As such, this industry offers an ideal victim for ransomware, and these attacks are likely to continue—disrupting employee access to important documents and patient data and hampering the ability to provide critical services—creating a public safety concern.[21]

(U//FOUO) Locky will likely decline in the coming months as a new ransomware strain known as SamSam begins to emerge. According to researchers, SamSam, which exploits server vulnerabilities to spread across and infect enterprise networks, may be a precursor to a new generation of ransomware known as "cryptoworms." Cryptoworms are predicted to penetrate networks through previously known vulnerabilities, blending modern network intrusion tactics based off SamSam with past computer worms that targeted unpatched server vulnerabilities, such as the Conficker and SQL Slammer worms. Organizations that operate on typically less-secure networks should remain especially diligent in prevention efforts.[22]

(U) Preventive Measures

(U) The United States Computer Emergency Readiness Team recently issued an alert (US-CERT Alert TA16-091A, dated 31 March 2016) recommending that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- (U) Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- (U) Use application whitelisting—a computer administration practice used to prevent unauthorized program from running—to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.

- (U) Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks, ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

- (U) Maintain up-to-date anti-virus software and scan all software downloaded from the Internet prior to executing.

- (U) Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

- (U) Avoid enabling macros from e-mail attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block e-mail messages with attachments from suspicious sources. (For information on safely handling e-mail attachments, see US-CERT's "Recognizing and Avoiding E-mail Scams.")

- (U) Follow safe practices when browsing the Internet. (See US-CERT's "Good Security Habits" and "Safeguarding Your Data" for additional details.)

- (U) Do not follow unsolicited links in e-mails. Refer to the US-CERT Security Tip on Avoiding Social Engineering and Phishing Attacks for more information.

(U) **Source Summary Statement**

(U//FOUO) The information in this *FAR* is drawn from open sources, interviews, fusion center products, and DHS reports. We have **medium confidence** in the information obtained from open sources, which includes media reports and websites where information is credibly sourced and plausible but may contain biases or unintentional inaccuracies. We have **high confidence** in the validity of our sources and the characterization of the ransomware threat to hospitals and healthcare providers for the foreseeable future.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and **complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security **policies, acceptable use policies, or standard computer security practices.** In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge.

(U) Tracked by: HSEC-1, HSEC-1.6.2, HSEC-1.8.1, HSEC-1.8.2, HSEC-1.8.4, HSEC-1.9.7, HSEC-9

[1] (U); HIPPAJournal.com; “Ransomware and HIPAA: Are Attacks Reportable?”; 01 APR 2016; http://www.hipaajournal.com/ransomware-hipaa-attacks-reportable-3379/; accessed on 11 APR 2016; (U); Healthcare news website.
[2] (U); Kim Zetter; Wired.com; “Why Hospitals Are the Perfect Targets for Ransomware”; 30 MAR 2016; http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets; accessed on 11 APR 2016; (U); Technology news website.
[3] (U); Emily Norton; Preparis.com; “Ransomware in the Health Care Industry”; 05 APR 2016; http://www.preparis.com/blog/ransomware-in-the-health-care-industry/; accessed on 11 APR 2016; (U); Cybersecurity, healthcare, and planning and compliance blog website.
[4] (U); Trevor Mogg; Digital Trends; “Hollywood hospital pays $17,000 to ransomware hackers”; 18 FEB 2016; http://www.digitaltrends.com/computing/hollywood-hostpital-ransomware-attack; accessed on 11 APR 2016; (U); Technology news website.
[5] (U); Tom Simonite; MIT Technology Review; “Hospital Forced Back to Pre-Computer Era Shows the Power of Ransomware”; 16 FEB 2016; https://www.technologyreview.com/s/600817/hospital-forced-back-to-pre-computer-era-shows-the-power-of-ransomware/; accessed on 11 APR 2016; (U); Technology news website.
[6] (U//FOUO); Map Source: DHS I&A
[7] (U); Sophie Ryan; *The New Zealand Herald*; “Hackers attack hospital system”; 24 FEB 2016; http://www.nzherald.co.nz/wanganui-chronicle/news/article.cfm?c_id=1503426&objectid=11594628; accessed on 22 APR 2016; (U); Newspaper website.
[8] (U); Allice Dennie; mracenter.com; “Decrypt Essential Files and Folders Encrypted by Locky Ransomware”; 10 MAY 2016; http://www.mramcenter.com/decrypt-essential-files-folders-encrypted-locky-ransomware; accessed 28 JUN 2016; (U); hacking news website.
[9] (U); Fred Bazzoli; *Health Data Management*; “Ottawa Hospital weathers ransomware attack”; 21 MAR 2016; http://www.healthdatamanagement.com/news/ottawa-hospital-weathers-ransomware-attack; accessed on 22 MAR 2016; (U); Website covering healthcare IT news.
[10] (U); Max Metzger; SC Magazine; “Canadian hospital infected with ransomware”; 21 MAR 2016; http://www.scmagazine.com/canadian-hospital-infected-with-ransomware; accessed on 22 MAR 2016; (U); News website for systems security professionals.
[11] (U); Joseph Goedert; *Health Data Management*; “Ransomware attack hits Methodist Hospital in Henderson, Kentucky”; 21 MAR 2016; http://www.healthdatamanagement.com/news/ransomware-attack-hits-methodist-hospital-in-henderson-ky; accessed on 11 APR 2016; (U); Website covering healthcare IT news.
[12] (U); Ms.Smith; Network World; “Three more hospitals hit with ransomware attacks”; 23 MAR 2106; http://www.networkworld.com/article/3047180/security/three-more-hospitals-hit-with-ransomware-attacks; accessed on 28 MAR 2016; (U); News website for network and IT executives.
[13] (U); Akanksha Jayanthi; *Becker's Hospital Review* ; “Methodist Hospital in Kentucky declares internal emergency due to ransomware attack”; 21 MAR 2016; http://www.beckershospitalreview.com/healthcare-information-technology/methodist-hospital-in-kentucky-declares-internal-emergency-due-to-ransomware-attack; 22 MAR 2016; (U); Hospital business news and analysis website.
[14] (U//FOUO); Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; (U); “Ransomware Targeting Kentucky Healthcare Providers”; 25 MAR 2016.
[15] (U); King’s Daughter’s Health (KDH); Press release; 30 MAR 2016; https://kdhhs.netreturns.biz/NewsReleases/Article_Detail.aspx?id=e067d2ba-d8ca-4174-b789-144d34d83075; accessed on 22 APR 2016; (U); Press release published on hospital website.
[16] (U//FOUO); Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; (U); “Ransomware Targeting Kentucky Healthcare Providers”; 25 MAR 2016.
[17] (U); Ms.Smith; Network World; “Three more hospitals hit with ransomware attacks”; 23 MAR 2106; http://www.networkworld.com/article/3047180/security/three-more-hospitals-hit-with-ransomware-attacks; accessed on 28 MAR 2016; (U); News website for network and IT executives.
[18] (U); Kim Zetter; Wired.com; “Why Hospitals Are the Perfect Targets for Ransomware”; 30 MAR 2016; http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets; accessed on 11 APR 2016; (U); Technology news website.
[19] (U); Christine Kern; Health IT Outcomes; “Backup and Recovery System Allows Methodist Hospital to Regain Control After Ransomware Attack”; 28 MAR 2016; http://www.healthitoutcomes.com/doc/backup-recover-system-contro-ransomware-attack-0001; accessed 28 MAR 2016; (U); Healthcare IT news and information website.
[20] (U//FOUO); Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; (U); “Ransomware Targeting Kentucky Healthcare Providers”; 25 MAR 2016.
[21] (U); Kim Zetter; Wired.com; “Why Hospitals Are the Perfect Targets for Ransomware”; 30 MAR 2016; http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets; accessed on 11 APR 2016; (U); Technology news website.
[22] (U); William Largent; Cisco Talos Blog; “Ransomware: Past, Present, and Future”; 11 APR 2016; http://blog.talosintel.com/2016/04/ransomware.html; accessed on 10 MAY 2016; (U); Blog run by Cisco Systems Inc’s Talos security research group.