



(U) RANSOMWARE: GOALS OF MALICIOUS ACTORS AND CURRENT SYSTEM VULNERABILITIES

(U) Prepared By: Office of Cyber and Infrastructure Analysis

(U) KEY FINDINGS

- (U) The most susceptible systems to ransomware attacks are personal computers and Internet-facing servers, in particular, those utilizing common, but outdated operating systems or security.
- (U) OCIA assesses that the Healthcare and Public Health Sector is one of the most prevalent targets of ransomware because of its reliance on immediate access to patient records.
- (U//FOUO) OCIA assesses that if specific industrial control systems (ICS) were successfully infected with ransomware, it could affect the ability of certain sectors to provide real-time management and control of large networks of geographically scattered equipment. Although security researchers have demonstrated the possibility of ransomware targeting control systems, OCIA assesses that such an attack is highly unlikely given the higher success rate against consumer and business systems, the likelihood that business and process control networks are segmented, and the ability for operators to take a control system out of service and employ manual overrides.

(U) SCOPE NOTE: The U.S. Department of Homeland Security (DHS)/Office of Cyber and Infrastructure Analysis (OCIA) produces Critical Infrastructure Security and Resiliency Notes to provide an overview of risks to critical infrastructure from all hazards. The information in this assessment is intended to inform U.S. Government leadership and private sector partners on the potential vulnerabilities and impacts to critical infrastructure from Ransomware infections. The information contained in this assessment is based on government and open source reporting.

(U) This product was coordinated with the DHS/National Protection and Programs Directorate/Office of Cybersecurity & Communications/National Cybersecurity and Communications Integration Center and the DHS/Office of Intelligence and Analysis.

(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 is introduced through an exploitation of a computer vulnerability. The payment of the ransom is almost always the desired goal; 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 trace once completed. Once infected, organizations enter into a cost benefit analysis of the following questions:

- (U) How critical it is to access their own data?
- (U) Is the system adequately backed up?
- (U) Whether the (usually) low cost of paying to regain access is appropriate.
- (U) What is the likelihood that malicious actors will return access and control to the infected systems once a ransom is paid?

(U) INTENTIONS, SUSCEPTIBILITY, AND IMPACTS

(U) Malicious Cyber Actors use Ransomware to Target Users and Organizations Most Likely to Pay

(U) Malicious actors who employ ransomware are often focused on a very narrow goal, making money. Unlike other malicious actors whose goal is to steal or disrupt data integrity, those who employ ransomware are often focused on preventing user access to their data or systems. OCIA assesses that because data theft is not the ultimate goal, malicious actors using ransomware overwhelmingly seek out users or organizations that might pay the ransom.¹ Malicious actors only need a few users out of numerous targets to pay in order for a ransomware campaign to be worthwhile. A recent report highlighted that the average ransom demand in 2016 had risen to \$1,077, up from an average of \$294 dollars in 2015.²

- (U) Ransomware often targets a range of organizations that require immediate access to their systems and their data to operate. The 2016 Verizon Data Breach Report found that the top three industries targeted by ransomware were Public Administration, Healthcare, and Financial Services.³

(U) The number of ransomware attacks has increased year after year. Symantec found detections of ransomware against customers it protects increased from 340,000 in 2015 to 463,000 in 2016.⁴ Kaspersky Lab found that between 2014-15 and 2015-16 the number of ransomware attacks targeting its customers had increased five times (131,111 to 718,536).⁵ Malicious actors are not limited to randomly targeting organizations with ransomware. Openly available Personally Identifiable Information (PII) allows actors to identify targets and potentially design a more believable email message (with a ransomware executable) that the user is more likely to open. In November 2016, a ransomware email phishing campaign targeted thousands of government workers who had information exposed during the 2015 Office of Personal Management's breach of PII.^{6,7}

(U) Organizations that Require Continuous Access to Business Systems are Most Susceptible to Ransomware Disruptions

(U) OCIA assesses that organizations and individuals whose systems contain personal computers and Internet-facing servers are the most susceptible to ransomware attacks.⁸ In particular, those utilizing common, but outdated operating systems or security are most at risk. For example, the operating system Windows XP was launched in

¹ (U) Department of Justice. (2017). "Ransomware: What it is and What to do about it." <https://www.justice.gov/criminal-ccips/file/872766/download>. Accessed May 15, 2017.

² (U) Symantec Corporation. (2017). "Internet Security Threat Report, Volume 22. April 2017." https://www.symantec.com/about/newsroom/press-kits/istr-22?om_ext_cid=biz_social_pr_vanity-istr22-press-kit. Accessed May 15, 2017.

³ (U) Verizon. (2017). "Data Breach Investigations Report." <http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017>. Accessed May 15, 2017.

⁴ (U) Symantec Corporation. (2017). "Internet Security Threat Report, Volume 22. April 2017." https://www.symantec.com/about/newsroom/press-kits/istr-22?om_ext_cid=biz_social_pr_vanity-istr22-press-kit, accessed May 15, 2017.

⁵ (U) Drozhzhin, A. (2016). "Ransomware's history and evolution." <https://blog.kaspersky.com/ransomware-blocker-to-cryptor/12435/>. Accessed May 25, 2017.

⁶ (U) Wagstaff, K., Deluca, M., and Eng, J. (2017). "OPM:21.5 Million People Affected By Background Check Breach." <http://www.nbcnews.com/tech/security/opm-hack-security-breach-n389476>. Accessed May 16, 2017.

⁷ (U) Griffin, B. (2016). "Unscrupulous Locky Threat Actors Impersonate US Office of Personnel Management to Deliver Ransomware." *Phish me*. <https://phishme.com/unscrupulous-locky-threat-actors-impersonate-us-office-personnel-management-deliver-ransomware/>. Accessed May 16, 2017.

⁸ (U) Rains, T. (2016). "Ransomware: Understanding the Risk." *Microsoft Secure Blog*. <https://blogs.microsoft.com/microsoftsecure/2016/04/22/ransomware-understanding-the-risk/>. Accessed May 15, 2017.

2001, but discontinued its free security patches in 2014. However, as of April 2017, an estimated 7 percent of global desktop computers still use Windows XP operating systems.⁹

- (U) Though the use of unprotected or outdated operating systems represents a critical vulnerability, email is often the primary vehicle used to carry out a ransomware attack. Individual users targeted with phishing emails that contain malicious links or applications remain the most common way systems become infected. According to a 2016 report on phishing attacks, ransomware comprised 93 percent of reported malicious emails.¹⁰

(U) OCIA assesses that the Healthcare and Public Health Sector is one of the most prevalent targets of ransomware because of its reliance on immediate access to patient records. A 2017 study by Verizon found that in 2016 ransomware accounted for 72 percent of malware incidents reported by the Healthcare and Public Health Sector.¹¹ Numerous ransomware attacks have occurred against healthcare provider networks, resulting in local, isolated impacts to healthcare service systems.^{12,13,14} Denial of access to patient data or Internet-connected medical devices can create situations when healthcare providers deliver care with incomplete information or capability, potentially endangering patients. In some cases, an affected healthcare facility can operate temporarily with a less efficient paper backup system, but often the facility stops accepting new patients or transfers patients to other unaffected facilities.

- (U) In May 2016, a Kansas-based hospital was the subject of multiple ransomware attacks attributed to the Samsam malware. The initial ransom demand was paid by the hospital, but the attackers refused to return full access to the hospital's files and instead demanded another payment. The hospital refused to pay and updated their policy to no longer pay ransoms.¹⁵ Open source reporting does not indicate whether the hospital had a contingency plan to mitigate the threat of a ransomware attack or if a second payment was made and whether the hospital was given the decryption key.
- (U) On March 29, 2016, it was reported that a large medical consortium (made up of 10 hospitals and over 250 outpatient centers) was forced to shut down its computer systems as a result of a likely ransomware attack.¹⁶ It was further reported that medical personnel were forced to resort to less comprehensive paper records, which were often missing crucial pieces of data such as patient history, drugs prescribed, allergies, etc. Non-emergency patients were diverted to other medical centers or had their appointments rescheduled for a later date.¹⁷
- (U) On February 5, 2016, malicious actors encrypted the email system and patient records of a California-based hospital and demanded a ransom in excess of \$3 million. After approximately 2 weeks, the hospital settled with the actors for \$17,000.¹⁸

⁹ (U) NetMarketShare. (2017). "Desktop Operating System Market Share." <https://www.netmarketshare.com/operating-system-marketshare.aspx?qprid=10&qpcustomd=0>. Accessed May 13, 2017.

¹⁰ (U) PhishMe. (2017). "2016 Phishing Susceptibility Report." <https://phishme.com/2016-enterprise-phishing-susceptibility-report/>. Accessed May 16, 2017.

¹¹ (U) Verizon. (2017). "2017 Data Breach Investigations Report." <http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017>. Accessed May 15, 2017.

¹² (U) Dietsche, E. (2016). "12 Healthcare ransomware attacks of 2016." *Becker's Health IT & CIO Review*. <http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html>, Accessed on January 18, 2017.

¹³ (U) Davis, J. (2016). "Ransomware: See the 14 hospitals attacked so far in 2016." *Healthcare IT News*. <http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=2>. Accessed on December 1, 2016.

¹⁴ (U) Winton, R. (2016). "Hollywood Hospital pays \$17,000 in bitcoin to hackers; FBI investigating." *LA Times*. <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>. Accessed May 15, 2017.

¹⁵ (U) Trend Micro. (2016). "Security News: Kansas Hospital Hit by Ransomware, Extorted Twice." <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kansas-hospital-hit-by-ransomware-extorted-twice>, Accessed August 30, 2016.

¹⁶ (U) Cox, W., and John W. (2016). "MedStar Health turns away patients after likely ransomware cyberattack." *Washington Post*. 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=.330fbd1c4d36. Accessed May 25, 2017.

¹⁷ (U) Ibid.

¹⁸ (U) Winton, R. (2016). "Hollywood Hospital pays \$17,000 in bitcoin to hackers; FBI investigating." *LA Times*. <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>. Accessed May 15, 2017.

(U) In general, healthcare organizations devote fewer resources to information technology security spending, despite their high reliance on information technology (IT) to access medical data and Internet-connected medical devices.¹⁹

- (U) A 2016 survey conducted by HIMSS (Healthcare Information and Management Systems Society) Analytics found that data security spending in healthcare lags behind other top cybercrime targets such as financial services.²⁰

(U) The Emergency Services Sector is also a common target for ransomware attacks. This is likely because they require continuous access to their systems. While large organizations such as Federal law enforcement organizations have resources with which to increase their resilience (through redundant systems and backups), smaller organizations, such as state and local police departments, have been faced with the choice of potentially losing access to files or paying the ransom.

- (U) In early 2017, a Texas-based police department was infected with ransomware. The malware encrypted videos, photographs, and other data file evidence going back a number of years. The police department ultimately declined to pay the ransom and was unable to restore files from 2009 to 2017.²¹
- (U) On February 25, 2016 the systems belonging to a Massachusetts-based police department were infected with ransomware from a malicious email that was sent to the entire department. The malware encrypted a software tool, which police officers used for computer-aided dispatch and as a record management system during patrol. The program also enables law enforcement officers to log incident reports. The department later paid the Bitcoin ransom, which was equal to \$489.²²

(U) Not all targeted systems are necessarily vulnerable to ransomware or will have their core operations disrupted. For example, the impacts to the Communications Sector from ransomware incidents will be limited because ransomware typically does not target the systems that manage communications routing. Ransomware attacks against communications companies typically affect internal business networks, which could affect business operations, but not communications services.²³

- (U) In May 2017, Telefonica, a Spanish telecommunications company, was a victim of the ransomware WannaCry, which infected an internal server, and subsequently spread to internal computers, but did not disrupt Internet or telephone services.^{24,25,26}

(U) Disruptive ICS Attacks with Ransomware are Possible, but Unlikely

(U//FOUO) OCIA assesses that if ICS were successfully infected with ransomware, it could affect the ability of operators to provide real-time management and control of large networks of geographically scattered equipment, and destabilize assets resulting in a loss of operator control and potential damage or destruction of critical operational equipment. Researchers from Georgia Tech created a proof-of-concept ransomware strain named

¹⁹ (U) Sans Institute. (2016). "IT Security Spending Trends." <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>. Accessed May 16, 2017.

²⁰ (U) Symantec. (2016). Addressing Healthcare Cybersecurity Strategically. https://img03.en25.com/VWeb/Symantec/%7B7ed5a2f6-12fa-4e09-a318-3772a3578197%7D_Addressig_Cybersecurity_Strategically_whitepaper.pdf?aid=elq_&om_sem_kw=elq_15895126&om_ext_cid=biz_email_elq, p. 1. Accessed June 1, 2017.

²¹ (U) CSO Staff. (2017). "Ransomware steals 8 years of data from Texas police department." CSO. <http://www.csoonline.com/article/3163045/security/ransomware-steals-8-years-of-data-from-texas-police-department.html>. Accessed May 17, 2017.

²² (U) Leibowitz, A. (2016). "Update: Melrose Police pay hackers in Bitcoin to recover encryption key." *Melrose Free Press*. <http://melrose.wickedlocal.com/article/20160229/NEWS/160226126>. Accessed May 16, 2017.

²³ (U) Reuters. (2017). "Telefonica, Other Spanish Firms Hit in 'Ransomware' Attack." <http://www.reuters.com/article/us-spain-cyber-idUSKBNI881TJ>. Accessed May 13, 2017.

²⁴ (U) Cimpanu, C. (2017). "Telefonica Tells Employees to Shut Down Computers Amid Massive Ransomware Outbreak." <https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/>. Accessed May 15, 2017.

²⁵ (U) Secure List. (2016). "Threat Intelligence Report for the Telecommunications Industry." <https://securelist.com/analysis/publications/75846/threat-intelligence-report-for-the-telecommunications-industry>. Accessed May 13, 2017.

²⁶ (U) BBC (2017). "TalkTalk Hack Affected 157,000 Customers." <http://www.bbc.com/news/business-34743185> <http://www.bbc.com/news/business-34743185>. Accessed May 13, 2017.

LogicLocker that can alter programmable logic controller (PLC) parameters.²⁷ Although security researchers have demonstrated the possibility of ransomware targeting control systems, OCIA assesses that such an attack is highly unlikely given the higher success rate against consumer and business systems, the likelihood that business and process control networks are segmented, and the ability for operators to take a control system out of service and employ manual overrides.

- (U) A move to targeting ICS would require more sophisticated malware and knowledge of specialized protocols used by control systems. OCIA assesses that most malicious actors are unlikely to judge that the effort required to develop customized ransomware for control systems are worth the potential benefits.
- (U) Process control systems like ICS and Supervisory Control and Data Acquisition (SCADA) are often segregated from business systems and often have services such as server message block disabled, which minimizes the likelihood of an attack successfully harming physical control systems. Attacks targeting business systems could affect customer-facing services and lower priority activities ranging from email communications to accounting and billing activities, but would not likely be able to infect or disrupt ICS and SCADA devices.^{28,29} Disruptions to business systems can have operational impacts, as was seen during the 2012 cyber attack that targeted Saudi ARAMCO (see *Malware Attack Caused Saudi Aramco to Suspend Domestic Oil Sales*), which although not a ransomware incident demonstrates possible operational effects of the loss of business systems.

(U) MALWARE ATTACK CAUSED SAUDI ARAMCO TO SUSPEND DOMESTIC OIL SALES

(U) In 2012, Saudi ARAMCO experienced a cyber attack on its business systems. The malware (named Shamoon after a word in its code) wiped the hard drives of tens of thousands of computers and replaced them with the image of a burning American flag. The Shamoon attack did not impact the company's systems that directly enable technical operations; the company reported that the damage was limited to office computers. Disruptions to drilling, pumping, and other production operations were not apparent. Oil production remained steady at 9.5 million barrels per day.³⁰ Although Shamoon apparently did not directly impact production and drilling, the disruption to the availability of data and services access did have other significant effects on business operations, which ultimately caused ARAMCO to suspend domestic oil sales.

(U) As a result of the attack, managing supplies, shipping, contracts with governments and business partners were done manually. Corporate email and Internet service experienced severe disruptions, as did office phone communications. Employees wrote reports on typewriters and contracts were sent via interoffice mail. Lengthy, lucrative deals needing signatures were faxed one page at a time. The company temporarily stopped selling oil to domestic gas tank trucks; and, after 17 days, the corporation started giving oil away for free to keep it flowing within Saudi Arabia.³¹

(U) RANSOMWARE MITIGATION

(U) US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:³²

- (U) Ensure that your applications and operating systems have been patched with the latest updates. Vulnerable applications and operating systems are the target of most attacks.

²⁷ (U) Toon, J. (2017). "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls." *Georgia Tech Horizons*. <http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls>. Accessed May 25, 2017

²⁸ (U) Budd, C. (2016). "Ransomware's newest target: The electric grid." *Trend Micro*. <http://blog.trendmicro.com/ransoms-newest-target-the-electric-grid/>. Accessed May 15, 2017.

²⁹ (U) Palmer, K. (2016). "BWL paid \$25,000 ransom after cyberattack." *The Lansing State Journal*. <http://www.lansingstatejournal.com/story/news/local/2016/11/08/bwl-paid-25000-ransom-after-cyberattack/93488502/>. Accessed May 15, 2017.

³⁰ (U) Pagliery, J. (2015). "The Inside Story of the biggest Hack in History." *CNN*. <http://money.cnn.com/2015/08/05/technology/aramco-hack/>. Accessed May 15, 2017.

³¹ (U) Ibid

³² (U) US-CERT. (2017). "Ransomware." <https://www.us-cert.gov/security-publications/Ransomware>. Accessed May 18, 2017.

- (U) Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- (U) Avoid providing personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- (U) Avoid revealing personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- (U) Be cautious about sending sensitive information over the Internet before checking a website's security.
- (U) Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- (U) If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- (U) Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

(U) Table I provides a snapshot look at threats and susceptibility of critical infrastructure sectors.













(U) The contents of the following table are U//FOUO.




(U) TABLE I—RANSOMWARE TARGETING AND SUSCEPTIBILITY BY SECTOR



INFRASTRUCTURE SECTOR	ADVERSARY TARGETING	INFRASTRUCTURE SUSCEPTIBILITY	ANALYSIS
Financial Services			Successful ransomware attacks against smaller financial sector companies have occurred in the past and continue to increase. The Financial Services Sector is well aware of ransomware threats and has sophisticated cyber defenses in place. Although, such impacts are unlikely, sustained persistent disruption of particular systems could have systemic implications for this sector.
Chemical: Plants			Chemical plants have manual overrides in place to ensure the safe containment of chemical processes in case cyber defenses fail. In some cases, it may be possible to run the chemical plant independently of cyber controls, otherwise the plant will most likely shut down.
Dams			Although malicious actors can potentially infect a dam's Supervisory Control And Data Acquisition (SCADA) computer with ransomware, many systems have physical overrides if digital controls are unavailable.
Commercial Facilities			There is a high likelihood that ransomware will have a broad impact when large enterprise systems are affected that connect to local branches, stores, and venues.
Emergency Services			The Emergency Services Sector is a common target for ransomware attacks because it requires continuous access to the systems. Smaller organizations such as State and local police departments have been faced with the choice of potentially losing access to files or paying the ransom.

Adversary Targeting: Rarely Targeted Moderately Targeted Frequently Targeted

Infrastructure Susceptibility: Low Susceptibility Moderate Susceptibility High Susceptibility

INFRASTRUCTURE SECTOR	ADVERSARY TARGETING	INFRASTRUCTURE SUSCEPTIBILITY	ANALYSIS
Energy			<p>The Energy Sector's control systems are typically separated from business process systems, making the spread of a ransomware infection unlikely. Safeguards exist that prevent cyberattacks (including ransomware) against a nuclear power plant. These attacks are unlikely to succeed without the aid of authorized personnel within the restricted access areas.</p> <p>The delivery of oil and natural gas can be interrupted because of disruptions to business systems supporting these entities. Significant regional and national consequences would only be likely if disruptions were long lasting and affected multiple companies or segments of the subsector. In 2012, Saudi ARAMCO experienced a cyber-attack on its business systems. Although the attack did not directly impact production and drilling, the disruption to the availability of data and services access had other significant effects on business operations, which ultimately caused ARAMCO to suspend domestic oil sales.</p>
Healthcare and Public Health			<p>The need for the Healthcare and Public Health Sector to have immediate access to patient records will continue to make the sector a significant target for ransomware attacks.</p>
Information Technology			<p>Information Technology assets are commonly targeted by malicious actors. The Sector itself is quite resilient based on the redundant hardware, software, routing, and virtual system redundancy available to them. Outdated or poorly secured systems used by other critical infrastructure systems have a higher risk.</p>
Communications			<p>Ransomware impacts to the primary Communications Sector backbone will be limited because typical ransomware does not target the systems used for core communications routing. Communications companies have still seen business impacts from ransomware incidents.</p>
Transportation Systems			<p>In the event of a ransomware attack, the Aviation Subsector has the potential for significant consequence. Aviation business and operational systems, including but not limited to reservation and ticketing services, may be impacted by ransomware creating potential flight delays and cancellations. Mass Transit and Passenger Rail Systems can have systems infected by ransomware, disrupting ticketing, communication within their networks, and other business systems.</p>
Water and Wastewater Systems			<p>The primary risks to Water and Wastewater Systems from ransomware are utilities' business systems, with consequences likely to be restricted to financial costs to the utility. Ransomware attacks have occurred in the past against water and wastewater business systems with no disruption to water or wastewater services. In most cases, utilities were able to restore their systems from backed up data or by replacing equipment.</p>

Adversary Targeting: Rarely Targeted  Moderately Targeted  Frequently Targeted 

Infrastructure Susceptibility: Low Susceptibility  Moderate Susceptibility  High Susceptibility 

(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>.

(U) PDM17112