UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) May 14, 2017; 1700 EDT.

(U) POTENTIAL IMPACTS OF WANNACRY RANSOMWARE ON CRITICAL INFRASTRUCTURE

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

(U) KEY FINDINGS

- **(U//FOUO) OCIA assesses the majority of impacts will be short-term financial losses to companies from business interruption. It is unlikely but possible, that impacts to systems could manifest as physical consequences.**
- **(U//FOUO) OCIA assesses that the WannaCry ransomware, particularly a variant circumventing the inadvertently activated "kill switch," could have impacts on human life by denying healthcare providers access to clinical systems and Internet-connected medical devices.**
- **(U//FOUO) OCIA assesses that the WannaCry ransomware could infect millions of devices if it continues to spread. The majority of ransomware victims are likely to be consumers and not critical infrastructure owners and operators.**

(U) SCOPE NOTE: The U.S. Department of Homeland Security (DHS)/Office of Cyber and Infrastructure Analysis (OCIA) produces Infrastructure Impact Assessments 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 partners on the potential impacts to critical infrastructure related to the WannaCry Ransomware infections, which infected numerous systems in many countries across the world beginning on May 12, 2017. 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, Federal Cyber Centers and the Department of Health and Human Services.

(U) BACKGROUND

(U) On May 12, 2017, organizations across the world reported ransomware infections impacting their computer systems. The infections, caused by a ransomware strain referred to as WannaCry, restricts users' access to a computer and demands a ransom to unlock it. The U.S. Department of Justice defines ransomware as, a type of malicious software cyber actors use to deny access to systems or data until the ransom is paid. After the initial infection, ransomware attempts to spread through systems and networks.[1]

(U) WannaCry was initially delivered through phishing attacks, but was able to spread more quickly than normal ransomware, as it exploited security vulnerabilities to move remotely between unpatched computers.[2] As of 1515 EDT on May 12, 2017, the security firm Avast reported 75,000 detections of the ransomware in 99 countries.[3] Significant impacts were reported by the British National Health Service, the Spanish telecommunications firm Telefónica, and FedEx, amongst others. **The spread of WannaCry was inhibited after the implementation of a "kill switch" on May 12, 2017. This "kill switch" prevented lateral movement of that strain of the malware, but researchers warned that the cyber actors could modify the ransomware or alter the kill switch to circumvent this feature.**[4]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) IMPACT ASSESSMENT

(U//FOUO) Consumers more likely to be impacted than critical infrastructure

(U//FOUO) Based on a review of ransomware incidents over past years, OCIA assesses that the majority of ransomware victims are likely to be consumers and not critical infrastructure owners and operators. Between January 2015 and April 2016, consumers made up 57 percent of ransomware infections.[5] Of the ransomware attacks against critical infrastructure sectors, 55 percent affected the services or manufacturing industries; 10 percent were public administration; 10 percent were financial; and 7 percent were transportation, communications, and utilities.[6]

(U//FOUO) Impacts will be largely financial from business interruption

(U//FOUO) OCIA assesses the biggest impact will be short-term financial losses to companies from business interruption, some of which could be covered by cyber insurance, based on a review of previous ransomware attacks. In addition to paying ransom demands, companies reported costs related to information technology staff working to remediate ransomware attacks.

- (U) One of the largest ransomware incidents was CryptoLocker in 2013, which infected over 250,000 computers worldwide, according to open source reporting.[7] Security researchers estimated that tens of millions of dollars were paid by victims, and hundreds of millions more were paid because of clones of the ransomware.[8,9] No significant disruptions of critical infrastructure related to these or other ransomware strains were reported, although there were instances of business systems being publically announced as compromised.

(U//FOUO) Impacts will likely be to business control systems than process control systems

(U//FOUO) OCIA assesses that business control systems (BCS) are more likely to be impacted by ransomware

attacks than process control systems (PCS), but are less likely to have significant impacts. Most organizations managing critical infrastructure assets rely on functions enabled by BCS to manage day-to-day operations, store records, and enable computer-based communication.

- (U//FOUO) Disruptions to BCS, like a ransomware attack, can be significantly disruptive to day-to-day operations until processes are reengineered. Disruptions can result in the temporary or permanent loss of records used by critical infrastructure owners and operators.
- (U//FOUO) Compromises of BCS can result in the theft of sensitive data, including personally identifiable information, intellectual property, and financial information.

(U//FOUO) OCIA assesses that impact to PCS, which could manifest as physical impacts, are possible but unlikely. In many sectors, critical infrastructure owners and operators employ PCS to operate other devices or systems. PCS include industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Critical infrastructure owners and operators employ ICS environments that utilize many of the same information technology (IT) components as BCS, and as a result, malware intended to affect IT networks can also have operational impacts within ICS environments.[10]

- (U//FOUO) Disruptions to these systems can have significant impacts to infrastructure operations. Most infrastructure assets retain legacy or redundant manual controls to override the failure of a PCS, however, making these disruptions easier to mitigate.
- (U//FOUO) As a security best practice, PCS should be segregated from networks with Internet access, making them less susceptible to attacks such as ransomware.

- (U//FOUO) There are no documented instances of PCS being significantly disrupted by ransomware, although security researchers from the Georgia Institute of Technology demonstrated it was possible in February 2017.[11]

(U//FOUO) Five sectors have entities with potential catastrophic impacts from cyber incidents, but not from ransomware

(U//FOUO) OCIA assesses that a ransomware event such as WannaCry by itself is unlikely to result in catastrophic impacts from disruptions, but the exploitation of the same vulnerability to deploy more sophisticated malware designed to compromise critical systems cannot be ruled out. In analysis done under Section 9 of Executive Order 13636, OCIA found that the Financial Services Sector, Energy Sector, Communications Sector, Healthcare and Public Health Sector, and Transportation Systems Sector have assets or systems for which a cybersecurity incident could result in catastrophic impacts to public health and safety, the economy or national security.[12] In general, entities from these sectors had a high reliance on cyber infrastructure, limited resilience or backup systems, and are dependent on other sectors. The scenarios OCIA assessed to have catastrophic consequences in these sectors were more strategic, persistent, and widespread than those that have been reported associated with this attack.

(U) Healthcare and Public Health Sector faces significant threat

(U//FOUO) OCIA assesses that the WannaCry ransomware, particularly a variant circumventing the inadvertently

activated “kill switch,” could have impacts on human life by denying healthcare providers access to clinical systems and Internet-connected medical devices. Without access to these, healthcare providers deliver care with incomplete information or capability and potentially endanger the life of the patient. The impacts to the United Kingdom National Health Service have still not been fully reported, but they illustrate that larger-scale attacks can affect patient care on a regional or national level.

(U) In previous events, the impacts of ransomware attacks have been local and isolated.[13,14] 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. Healthcare organizations are more vulnerable than other sectors because they devote fewer resources to information technology security, despite their high reliance on using IT to access to medical data and Internet-connected medical devices.[15]

- (U) WannaCry installs the DoublePulsar backdoor, which means that infected machines may still be vulnerable to future attacks.[16] In addition to making these machines vulnerable to future ransomware attacks that would deny healthcare providers access to their systems and devices, this could make hacker-targeted medical records vulnerable to theft. In previous attacks, hackers used malware targeting Internet-connected medical devices to install backdoors on healthcare provider networks and exfiltrate health information.[17,18]

(U//FOUO) Millions of systems could be impacted by WannaCry

(U//FOUO) OCIA assesses that millions of devices could be compromised if malicious cyber actors modify the ransomware.[19,20] The systems most vulnerable to WannaCry are those running older version of Windows (Windows XP and Windows 8), for which Microsoft no longer regularly provides security patches. As of April 2017, almost 8 percent of desktops worldwide still use these versions of Windows.[21] According to media reporting, nearly 200,000 machines have been infected by the DoublePulsar backdoor exploited by WannaCry.[22] Security researchers estimated that machines could be exploited using the backdoor for years, even with the availability of a patch.[23]

- (U) Microsoft released a patch to mitigate the vulnerability exploited by WannaCry on March 14, 2017. Microsoft also provided a patch for older-unsupported operating systems on May 12, 2017. All systems running Windows without up-to-date patches are vulnerable, and security researchers have found that vulnerabilities are exploitable for years after their discovery, patches are deployed inconsistently.[24]

(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) PDM17107

SOURCES

[1] (U) Department of Justice, “Ransomware what it is and what to do about it,” 2016, https://www.justice.gov/criminal-ccips/file/872766/download. Accessed May 12, 2017.

[2] (U) Craig Timberg, Griff Witte, and Ellen Nakashima, “Malware, described in leaked NSA documents, cripples computers worldwide,” The Washington Post, May 12, 2017, https://www.washingtonpost.com/world/hospitals-across-england-report-it-failure-amid-suspected-major-cyber-attack/2017/05/12/84e3dc5e-3723-11e7-b373-418f6849a004_story.html?hpid=hp_rhp-top-table-main_britain-240pm%3Ahomepage%2Fstory&utm_term=.84e175a7e681. Accessed May12, 2017.

[3] (U) Jakub Kroustek, "Ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far, today," Avast Blog, May 12, 2017, https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today. Accessed May 12, 2017.

[4] (U) Mark Scott, The New York Times. "Hacking Attack Has Security Experts Scrambling to Contain Fallout," The New York Times, May 13, 2017.

[5] (U) "Ransomware and Businesses 2016," Symantec, 2016.

[6] (U) Ibid.

[7] (U) Leo Kelion, "Cryptolocker ransomware has 'infected about 250,000 PCs,'" BBC, December 24, 2013, http://www.bbc.com/news/technology-25506020, accessed May 13, 2017.

[8] (U) Violet Blue, "CryptoLocker's crimewave: A trail of millions in laundered Bitcoin," ZDNet, December 22, 2013, http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/, accessed May 13, 2017.

[9] "CryptoWall Version 4 Threat," Cyber Threat Alliance, September 2016.

[10] Idaho National Laboratory. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. August 2016. INL/EXT-16-40692. Page 7. https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[11] "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls," Georgia Tech Research Horizons, February 13, 2017, http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls, accessed May 13, 2017.

[12] (U//FOUO) Catastrophic impacts are defined as first-year economic consequences of $50 billion, first-year economic consequences of $25 billion and greater than 2,500 prompt fatalities, or the severe degradation of national security or defense.

[13] (U) Becker's Health IT & CIO Review. 12 Healthcare ransomware attacks of 2016. http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html, Accessed on January 18, 2017.

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

[15] (U) "IT Security Spending Trends," SANS Institute, February 2016.

[16] (U) Martine Lee et al, "Player 3 Has Entered the Game: Say Hello to 'WannaCry'," Talos Intelligence Blog, May 12, 2017, http://blog.talosintelligence.com/2017/05/wannacry.html, accessed May 14, 2017.

[17] (U) TrapX Security, MEDJACK.2 Hospitals Under Siege," http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf, accessed October 24, 2016.

[18] (U) Computerworld, "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks," June 8, 2015, www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html, accessed December 23, 2015.

[19] (U) Microsoft estimates that 400 million devices are running Windows 10 (https://news.microsoft.com/bythenumbers/), which has been estimated to be running on 26.3 percent of active devices worldwide as of April 2017 (http://www.netmarketshare.com/). Windows XP and Windows 8, which are no longer supported by Microsoft, are estimated to be running on 8.6 percent of devices over the same timeframe, which amounts to roughly 130 million devices assuming the same denominator as the Microsoft data.

[20] (U) Mark Scott, "Hacking Attack Has Security Experts Scrambling to Contain Fallout," The New York Times, May 13, 2017.

[21] (U) "Desktop Operating System Market Share," NetMarketShare, April 2017, https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0, accessed May 13, 2017.

[22] (U) Patrick Howell O'Neill, "Leaked NSA tools now infecting over 200,000 machines will be weaponized for years," CyberScoop, April 24, 2017, https://www.cyberscoop.com/leaked-nsa-tools-now-infecting-over-200000-machines-will-be-weaponized-for-years/, accessed May 14, 2017.

[23] (U) Ibid.

[24] (U) "2016 Data Breach Investigations Report," Verizon, 2016.

1. Product Title: Potential Impacts of WannaCry Ransomware on Critical Infrastructure (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 +RZ GLG \RX XVH WKLV SURGXFW LQ VXSSRUW RI \RXU 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