FIELD ANALYSIS REPORT

Regional Analysis with National Perspective.

22 April 2020

(U) Ransomware Overview: Threat to Rhode Island-based Critical Infrastructure and Private Sector Partners

(U) Prepared by the Department of Homeland Security Intelligence Enterprise (DHS IE) Field Operations Division (FOD) – New England Region, Rhode Island Fusion Center (RISFC), and the Rhode Island Joint Cyber Task Force. Coordinated with the DHS IE Cyber Mission Center (CYMC) and the Cybersecurity and Infrastructure Security Agency (CISA).

(U) ***Scope:*** *This* Field Analysis Report (FAR) *identifies and analyzes the cyber threat to Rhode Island-based critical infrastructure and private sector partners. This* FAR *focuses on the homeland security threat of malicious cyber activity—specifically ransomware—targeting our state, local, and private sector partners.*[a] *The unclassified information in this product is intended for the broadest dissemination possible to help prioritize cybersecurity efforts to identify vulnerabilities and mitigate future cyber threats. The information cutoff date is 20 February 2020.*

(U) Key Judgments

- (U) **We assess opportunistic cybercriminals who are financially motivated are responsible for the majority of ransomware activity targeting Rhode Island's critical infrastructure and private sector partners.**

- (U) **We judge partners—operating in an environment with constrained resources and an abundance of exploitable data—are potential victims who fail to employ sound cyber hygiene practices remain at risk of losing access to their systems and files.**

(U) Uptick in Ransomware Attacks Driven by Profit

(U) **We assess opportunistic cybercriminals who are financially motivated are responsible for the majority of ransomware activity targeting Rhode Island's critical infrastructure and private sector partners.**[1] We have no information to indicate the ransomware threat to critical infrastructure and private sector partners in Rhode Island differs from that at the national level.

- (U) Over the past year, the number of ransomware incidents has surged, and cyber criminals continue to use ransomware to infect victims. In the summer of 2019 malicious cyber actors targeted Rhode Island-based school systems and municipalities across the state, a clear indicator of the growing number of targets for ransomware, according to DHS liaison information with the Rhode Island Joint Cyber Task Force who is responsible for preventing and responding to cyber security events and defending the security of critical infrastructure.[2]

- (U) Ransomware has rapidly emerged as the most visible cybersecurity tactic developing across our nation's networks, obstructing private sector organizations and government agencies alike. Many more infections are going unreported, ransoms are being paid, and the ransomware cycle continues, according to CISA, who is responsible for leading the national effort to understand and manage cyber and physical risk to critical infrastructure.[3]

[a] (U) Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

(U) ***Warning:*** *This document is UNCLASSIFIED (U). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Unclassified information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) Fiscal Limitations Hindering Cyber Hygiene Practices

(U) **We judge partners—operating in an environment with constrained resources and an abundance of exploitable data—are potential victims who fail to employ sound cyber hygiene practices, in particular maintaining up-to-date backups, remain at risk of losing access to their systems and files.** Potential financial impacts include: loss of revenue, legal costs, increased insurance premiums, and costs of credit monitoring services for employees and customers.[4] Continued timely reporting of attempted cyber attacks against state critical infrastructure and private sector partners enables further analysis of malicious cyber actor intent and capabilities, to inform both law enforcement and policy makers.

- (U) Budget constraints and resource limitations are likely limiting the efforts of Rhode Island-based critical infrastructure and private sector partners—particularly smaller organizations—to successfully prevent or mitigate cyber incidents. Recovery of networks, systems, data, and the resulting technical support costs for some victimized agencies and municipalities during and after an attack may place an undue burden upon agency resources, even with assistance from the Rhode Island Joint Cyber Task Force and state and federal partners, according to DHS liaison information from the Rhode Island Joint Cyber Task Force.[5]

- (U) Significant amounts of data to analyze, lack of skilled personnel, and low security awareness among employees ranked as the top barriers to establishing effective defenses against cyber threats, according to the survey findings of a research and marketing consulting firm.[6] The survey was comprised of 1,200 responses from qualified information technology (IT) security decision makers and practitioners from organizations with more than 500 employees, spanning across 19 industries and 17 countries.

(U) Outlook

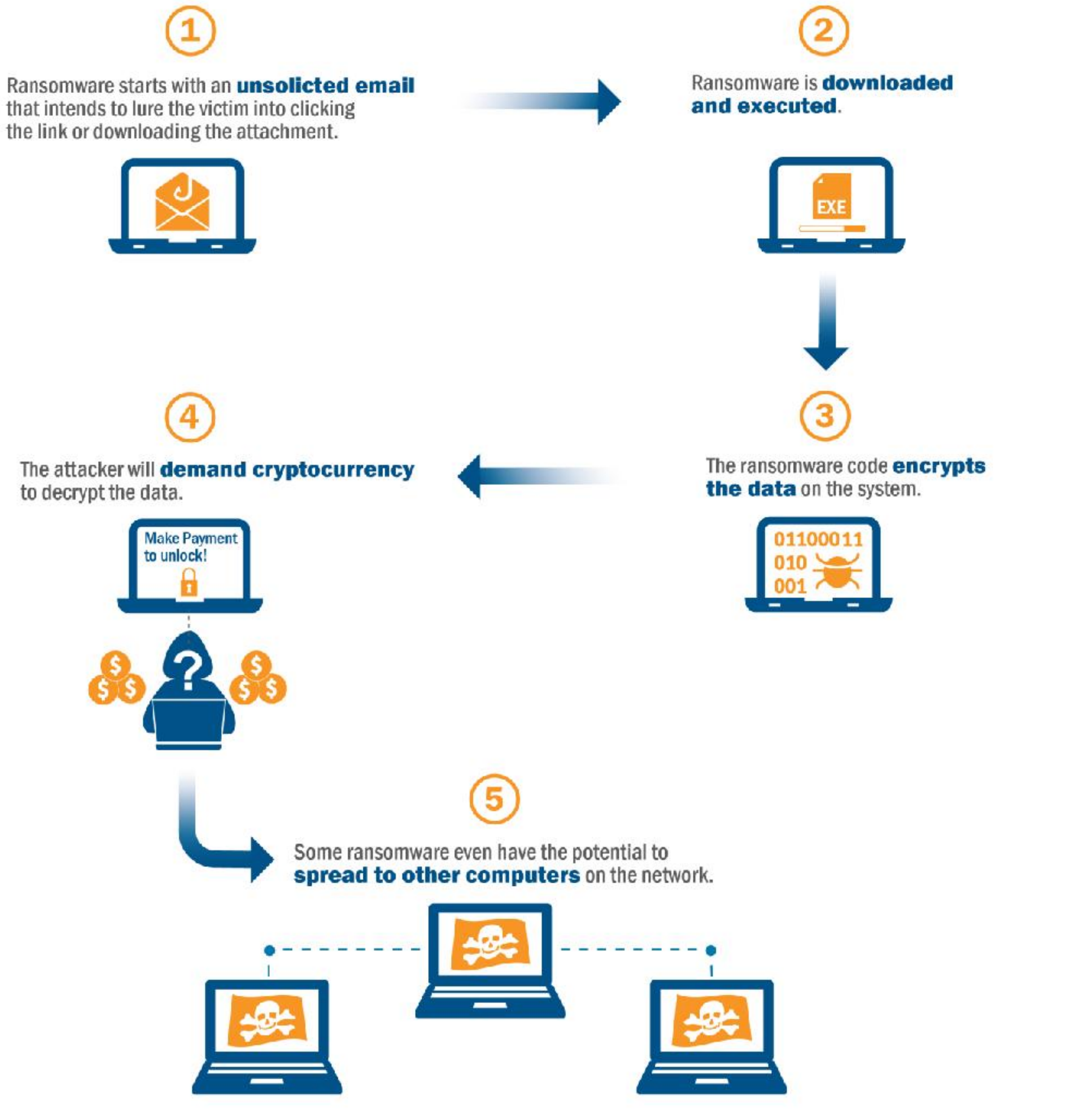
(U) We assess these attacks will almost certainly continue as long as current cyber infrastructure remains highly vulnerable to ransomware. Successful ransomware attacks targeting Rhode Island's critical infrastructure and private sector partners during the past year highlights the need for successful prevention and mitigation practices, especially as the potential for cyber criminals to profit from malicious cyber activity remains a lucrative endeavor.

(U) Analysis of Alternatives

(U) We considered the alternative that malicious cyber actors are primarily motivated by ideological beliefs when targeting critical infrastructure and private sector partners vice financially motivated. If ideological beliefs were the cause for the uptick in ransomware activity it would likely be designed to hinder our critical infrastructure partners' capabilities and identify weaknesses in their electronic security posture for possible future attacks. We view this alternative as less likely, largely because malicious cyber actors can use alternative means of conducting cyber attacks against our critical infrastructure partners that would likely cause more harm to daily operations and proprietary information.

UNCLASSIFIED

(U) How Ransomware Works[7]



1 Ransomware starts with an **unsolicted email** that intends to lure the victim into clicking the link or downloading the attachment.

2 Ransomware is **downloaded and executed**.

3 The ransomware code **encrypts the data** on the system.

4 The attacker will **demand cryptocurrency** to decrypt the data.

5 Some ransomware even have the potential to **spread to other computers** on the network.

UNCLASSIFIED

20-175-IA

(U) Appendix

(U) Steps to Increase Resilience Against Ransomware[8]

- (U) **Back-up systems** - Regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, reokace fauked security system(s) with stronger systems, fully patched and updated to the latest version.

- (U) **Reinforce Basic Cybersecurity Awareness and Education Ransomware** - Attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing, and suspicious links—the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate IT staff in a timely manner, which should include out-of-band communication paths.

- (U) **Revisit and Refine Cyber Incident Response Plans** - Agencies must have a clear plan to address attacks. Make sure response plans include how to request assistance from external cyber first responders, such as the Rhode Island Fusion Center, the Rhode Island Joint Cyber Task Force, or CISA in the event of an attack.

(U) What to do in the event of a Ransomware Incident[9]

(U) Should preventive measures fail, organizations should consider taking the following steps:

- (U) Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives.

- (U) Isolate or power-off affected devices suspected of being infected. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.

- (U) Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.

- (U) Contact law enforcement immediately. We strongly encourage you to contact the Rhode Island Fusion Center and Rhode Island Joint Cyber Task Force immediately upon discovery to report a ransomware event and request assistance.

- (U) If available, collect and secure portions of the ransomed data that might exist.

- (U) If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.

- (U) Delete registry values and files to stop the program from loading.

(U) Important Details Needed to Further the Investigation

- (U) Include a picture/screenshot of the ransom demands.

- (U) MD5 hash for the ransomware.

- (U) Type of network/system the ransom was found on and what type of data is located on the network/system.

- (U) Note if the ransom could or could not have affected the functioning of that system/process.

- (U) How was the malware initially delivered? E.g. The malware traversed the network/system via [phishing, cross site scripting, wateringhole, etc]

- (U) How were you notified of the ransom?

- (U) The demand requested payment via XX (e.g., bitcoin) method to XX (e.g., Bitcoin Wallet) place.

- (U) The demand was placed by a group/individual claiming to be XX.

- (U) Include an Excel spreadsheet of the IP addresses used to target the victim, as well as any IP addresses affected by the event, including the ports that were targeted and whether the event was successful or unsuccessful against each port/IP combination.

UNCLASSIFIED

Rhode Island State Fusion Center
401-444-1117

Rhode Island Joint Cyber Task Force
401-921-1170

CISA
888-282-0870

(U) Report Suspicious Activity

(U) **To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. 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, instruction, or consent.

(U) **To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every U.S. state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

(U) Comments, requests, or shareable intelligence may be directed to the Rhode Island State Fusion Center at 401-444-1117 or fusion@risp.gov.

(U) Tracked by: HSEC-1.1; HSEC-1.3; HSEC-1.5

(U) Source Summary Statement

(U) We have **medium confidence** in our assessment that the majority of ransomware activity targeting Rhode Island's critical infrastructure and private sector partners is opportunistic low-level cybercrime that is financially motivated and is not meant to be destructive. The low attribution rates of ransomware incidents, coupled with the highly personalized nature of cyber crime, makes assessing specific indicators of the nefarious actor's intent difficult.

(U) We base our **medium confidence** on reporting derived primarily from conversations with our local law enforcement partners and private sector experts who collectively have multiple decades of experience dealing with cyber-related crimes and mitigation efforts. We also leveraged insights from an aggregation of federal government and private industry best practices and mitigation strategies on the prevention and response to ransomware incidents, helping to corroborate our assessment. Additional reporting from credible and corroborative sources would raise our confidence level in our assessment of the malicious actor's motivations when deploying ransomware attacks against our critical infrastructure and private sector partners.

(U) We have **high confidence** in the judgment that our partners—operating in an environment with constrained resources and an abundance of data to defend—who fail to employ sound cyber hygiene practices remain at risk of losing access to their systems and files. These fiscal limitations are directly hindering cyber hygiene practices, based on a combination of conversations over the past year between law enforcement partners and private sector experts within the Rhode Island Joint Cyber Task Force with decades of practical cybersecurity experience.

(U) We base our **high confidence** on analysis from the Rhode Island Joint Cyber Task Force of identified cyber threat prevention, protection, response and recovery for our state and local governments as the focal point for deterring ransomware incidents and a private sector entity who obtained 1,200 responses from qualified IT security decision makers and practitioners from organizations with more than 500 employees, spanning across 19 industries and 17 countries also provided unique insight into the challenges of cyber hygiene. Additional reporting specific to Rhode Island would raise our confidence level in our assessment; however, we intentionally refrained from identifying any ransomware victims within the state to maintain their anonymity.

[1] (U); DHS; DHS I&A Intel Officer and Rhode Island Joint Cyber Task Force; Analytic exchange; 20 FEB 2020; DOI 1 JAN 2019 to 20 FEB 2020; (U); Analytic exchange-Ransomware Incidents within Rhode Island; Extracted information is UNCLASSIFIED; Overall document classification is U//LES.

[2] (U); DHS; DHS I&A Intel Officer and Rhode Island Joint Cyber Task Force; Analytic exchange; 20 FEB 2020; DOI 1 JAN 2019 to 20 FEB 2020; (U); Analytic exchange-Ransomware Incidents within Rhode Island; Extracted information is UNCLASSIFIED; Overall document classification is U//LES.

[3] (U); DHS/CISA; CISA Insights: Ransomware Outbreak; 21 AUG 2019; DOI UNK; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[4] (U); MS-ISAC; (U) Security Primer; 21 NOV 2019; DOI 1 JAN 2019 to 24 SEP 2019; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[5] (U); DHS; DHS I&A Intel Officer and Rhode Island Joint Cyber Task Force; Analytic exchange; 20 FEB 2020; DOI 1 JAN 2019 to 20 FEB 2020; (U); Analytic exchange-Ransomware Incidents within Rhode Island; Extracted information is UNCLASSIFIED; Overall document classification is U//LES.

[6] (U); CyberEdge Group; (U) 2019 Cyberthreat Defense Report, CyberEdge Group, LLC.; 2020; DOI 2019; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[7] (U); DHS; DHS I&A Intel Officer and Rhode Island Joint Cyber Task Force; Analytic exchange; 20 FEB 2020; DOI 1 JAN 2019 to 20 FEB 2020; (U); Analytic exchange-Ransomware Incidents within Rhode Island; Extracted information is UNCLASSIFIED; Overall document classification is U//LES.

[8] (U); CISA, MS-ISAC, NGA, NASCIO; Joint Recommendation Document; (U) Take the First Three Steps to Resilience Against Ransomware for State and Local Partners; 29 JUL 2019; DOI UNK; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[9] (U); DHS, DOJ, HHS; Joint Technical Document; (U) Ransomware: What It Is and What To Do About It; 2016; DOI 2015; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

CLASSIFICATION:

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

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

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- □ Drive planning and preparedness efforts, training, and/or emergency response operations
- □ Observe, identify, and/or disrupt threats
- □ Share with partners
- □ Allocate resources (e.g. equipment and personnel)
- □ Reprioritize organizational focus
- □ Author or adjust policies and guidelines
- □ Initiate a law enforcement investigation
- □ Intiate your own regional-specific analysis
- □ Intiate your own topic-specific analysis
- □ Develop long-term homeland security strategies
- □ Do not plan to use
- □ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

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

Name:

Organization:

Contact Number:

Position:

State:

Email:

Submit Feedback

Privacy Act Statement

CLASSIFICATION:

Product Serial Number:

REV: 01 August 2017