OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
10 APRIL 2024 DHS-IA-IF-2024-07223

CYBERSECURITY

(U//FOUO) Exploitation of Emergency Service Sector's Stolen Data Likely Poses Persistent Criminal Threat to Victims

(U//FOUO) **Cybercriminal exploitation of data stolen during ransomware attacks against the Emergency Service Sector (ESS) likely poses a persistent criminal threat due to the exposure and availability of victims' personal information.** Ransomware actors routinely leak, sell, or further exploit a victim's data for follow-on criminal schemes. In contrast to the long-term threat to personal information, ransomware disruptions and impacts to ESS operations—while often more acute—are generally temporary and are partially mitigated by reverting to manual processes. ESS networks are often interconnected, presenting challenges for any single state, local, tribal, or territorial (SLTT) government entity to independently protect its systems, which cybercriminals will probably continue to opportunistically target because of available personally identifiable information (PII) data and the possible perception that ESS entities are motivated to pay ransoms to ensure continuity of services.

- (U//FOUO) Ransomware actors typically exfiltrate data from the ESS networks that they exploit, including police records and sensitive PII of SLTT employees and citizens, according to open source reporting. These actors often leak, sell, or use the stolen data to facilitate additional crimes—including extortion, identity theft, and swatting—judging from a body of open source reporting.
- (U//FOUO) Ransomware attacks have disrupted the networks of police department and 911 call center operations and forced ESS entities to revert to manual dispatching to sustain their operations when computer-aided dispatching services were not functioning. Generally, such disruptions have delayed, but not prevented, critical services—such as medical transports and law enforcement services—from being provided, according to DHS and open source reports.
- (U//FOUO) ESS entities often rely on SLTT government networks that use legacy information and operational technology systems—the replacement of which can be prohibitively expensive or disruptive to operations—and lack sufficiently

trained and resourced information technology and cybersecurity personnel, according to cybersecurity industry reporting.[a]

(U//FOUO) **Incorporating a collaborative, cross-jurisdictional approach to cybersecurity and prioritizing cyber hygiene best practices throughout the ESS would likely mitigate many unsophisticated network intrusions that lead to ransomware and related data leaks**. SLTT governments manage the majority of ESS networks and are among the groups ransomware actors most often victimize, yet most do not have the resources to independently improve their cybersecurity posture, according to cybersecurity firm and open-source reporting. Ransomware actors typically gain network access through phishing or exploiting common vulnerabilities in unpatched systems. ESS network defenders—including third-party suppliers, SLTT governments, and technology vendors—have a range of preventative measures available that could help thwart these initial access attempts and strengthen data security and availability.

- *(U)* A collaborative, cross-jurisdictional—also called "whole-of-state"—approach allows state and local governments, including ESS entities, to pool their resources, collaborate more effectively, and improve their cybersecurity posture, judging from cybersecurity firm and industry reporting. The approach focuses on building partnerships and eliminating information-sharing constraints. Several states and counties have implemented their own version of the "whole-of-state" approach to meet their cybersecurity requirements. One state started a $30 million shared services program to provide counties with free endpoint detection and response services, improving the state's cybersecurity posture, judging from cybersecurity news reporting.
- *(U/FOUO)* Identification of a network's weaknesses and vulnerabilities is often the first step to practicing cyber hygiene. CISA offers no-cost scanning and testing services to a wide range of public and private sector critical infrastructure organizations, which includes the ESS. CISA's information security experts evaluate the requesting organization's public, static internet protocol address(es) for accessible services and vulnerabilities, culminating in weekly vulnerability reports and ad-hoc alerts as needed.[b]
- *(U//FOUO)* Cybercriminals often exploit a lack of network segmentation, password requirements, enforcement principle of least privilege, and outdated patching protocols across SLTT and ESS networks. Additional cyber hygiene best practices include enabling automatic updates; implementing phishing awareness training;

[a] *(U)* Hardware and software programs that are not supported by security updates and patches.
[b] *(U)* For more information, please visit CISA's "Cyber Hygiene Services" located at https://www.cisa/gov/topics/cyber-threats-and-advisoriers/cyber-hygiene-services.

testing and deploying patches quickly; and replacing unsupported operating systems, applications, and hardware. Additionally, CISA recommends requiring multi-factor authentication and access controls for accounts with privileged, administrative, and remote access.[c] Ransomware prevention and preparation techniques include maintaining regularly updated, offline, encrypted backups of data, establishing a cyber incident response plan, and employing security measures such as e-mail filters.[d]

(U//FOUO) **Additional Cybersecurity Resources**

(U//FOUO) For additional no-cost resources, please refer to the following:

(U) CISA's StopRansomware site is a centralized location for information and sources related to ransomware located at: https://www.cisa.gov/stopransomware.

(U) The US Department of Transportation shared services offers phishing testing and analysis through mock emails located at https://www.esc.gov/Services/IDServices/CybersecurityServicesMore.

(U) MS-ISAC offers a variety of free services such as malicious domain blocking located at https://www.cisecurity.org/ms-isac/services and MS-ISAC operates within a SOC to respond to SLTT cyber incidents. The SOC provides real-time network monitoring, early threat warnings, and vulnerability identification and mitigation. For additional information contact 866-787-4722 or soc@cisecurity.org.

[c] *(U)* For more information, please visit CISA's "Cyber Essentials" located at https://www/cisa.gov/resources-tools/resources/cyber-essentials.
[d] *(U)* For more information, please visit CISA's #StopRansomware Guide" located at https://cisa.gov/stopransomware/ransomware-guide.

Source, Reference, and Dissemination Information	
Definitions	*(U)* **Distributed Denial of Service (DDoS)**: a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. *(U)* **Remote Desktop Protocol:** a network communication protocol offered that allows users to execute remote operations on other computers. It facilitates secure information exchange between remotely connected machines over an encrypted communication channel. *(U)* **Swatting**: the action of making a false report of a serious emergency so that a SWAT team or other law enforcement response will go to a person's home, by someone who wants to frighten, upset, or cause problems for that person.
Reporting 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)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. *(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, instruction, or consent.

Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) 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 FOUO 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.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Exploitation of Emergency Service Sector's Stolen Data Likely Poses Persistent Criminal Threat

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: Select One **and function:** Select One

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

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

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 Disagree	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? Select One

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

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

Name: *Position:*
Organization: *State:*
Contact Number: *Email:*

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**