OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN BRIEF

23 SEPTEMBER 2020 IA-44761-20

CYBERSECURITY

(U//FOUO) COVID-19: Malicious Cyber Actors Likely to Target Schools with Ransomware

(U//FOUO) ***Scope****: This* Intelligence In Brief (IIB) *seeks to raise awareness of cyber threat actors and their use of ransomware attacks against schools and the potential impacts on school operating environments. This IIB also seeks to provide information on ransomware mitigation methods.*

(U//FOUO) ***We assess malicious cyber actors increasingly will conduct ransomware attacks against schools during the 2020-21 school year, given widespread adoption of virtual or hybrid learning due to the COVID-19 pandemic.*** Such attacks probably will yield more disruption than past years, given schools' reliance on online systems for virtual learning. At least 21 of the country's 25 largest school districts are using an online format for the fall semester and FBI and local press report an increase in ransomware attacks, which have resulted in school delays or closures.

- *(U)* Ransomware attacks against schools have been increasing since at least September 2019, according to a June FBI report. In 2019, 1,233 individual schools were potentially affected by ransomware attacks, while in the first quarter of 2020 there were already approximately 422 individual schools affected, according to the same source.
- *(U)* In July and August 2020, unidentified malicious cyber actors targeted several schools with ransomware, resulting in a delayed start to the school year for in-person learning, or suspended virtual learning, according to local news outlets. In one incident the school district paid the $50,000 ransom and delayed the start of school by one week, according to a local Texas news outlet.
- *(U)* In at least one incident in August 2020, ransomware attacks encrypted all data stored on district servers, including "a few hundred" computers and multiple data backups, according to a local Oklahoma news outlet. A separate July 2020 ransomware attack disabled main and auxiliary servers within the school district, according to a local Texas news outlet.

(U) Prepared by Field Operations Division – New England Region. Coordinated within the DHS Intelligence Enterprise (CYMC and CISA).

(U) Appendix – Ransomware Mitigation Methods

(U) Mitigation

(U) CISA recommends the following precautions to protect users against the threat of ransomware:

- (U) Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- (U) Never click on links or open attachments in unsolicited e-mails.
- (U) Backup data on a regular basis. Keep it on a separate device and store it offline.
- (U) Follow safe practices when browsing the Internet.

(U) In addition, CISA also recommends that organizations employ the following best practices:

- (U) Restrict users' permissions to install and run 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 a network.
- (U) Use application whitelisting to allow only approved programs to run on a network.
- (U) Enable strong spam filters to prevent phishing e-mails from reaching the end users, and authenticate inbound e-mail to prevent e-mail spoofing.
- (U) Scan all incoming and outgoing e-mails to detect threats and filter executable files from reaching end users.
- (U) Configure firewalls to block access to known malicious IP addresses.

(U) The use of Remote Desktop Protocol (RDP) creates risk. Since RDP can remotely control an entire system, usage should be closely regulated, monitored, and controlled. The FBI and DHS recommend implementing the following best practices to protect against RDP-based attacks:

- (U) Audit networks for systems using RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- (U) Verify all cloud-based virtual machine instances with a public IP do not have open RDP ports—specifically port 3389—unless a valid business reason exists to do so. Place any system with an open RDP port behind a firewall, and require use of a Virtual Private Network (VPN) to access the system through the firewall.
- (U) Enable strong passwords and account lockout policies to defend against brute-force attacks.
- (U) Apply two-factor authentication, where possible.
- (U) Apply system and software updates regularly.

- *(U)* Maintain a good back-up strategy.
- *(U)* Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- *(U)* When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- *(U)* Ensure third parties who require RDP access follow internal policies on remote access.
- *(U)* Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- *(U)* Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as VPNs, recognizing VPNs are only as secure as the connected devices.

Source, Reference, and Dissemination Information

Source Summary Statement	*(U)* We have **medium confidence** in our assessment that malicious cyber actors increasingly will conduct ransomware attacks against schools during the 2020-21 school year given widespread adoption of virtual or hybrid learning due to the COVID-19 pandemic. We base the information in this product on FBI Private Industry Notices relating to ransomware, as well as US local media. We have **high confidence** in the information obtained from FBI reporting, based on their proximity to the information and typical analytic rigor derived from FBI law enforcement investigations. We have **medium confidence** in the information obtained from open sources, including credibly sourced and plausible information from US local media reports, but which may contain biases or unintentional inaccuracies. Our confidence level would be higher with a greater ratio of official government reporting to open source reporting on this topic.
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 incidents 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 US 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.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and private sector network defenders.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document contains UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) 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 critical infrastructure and key resource personnel or 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) COVID-19: Malicious Cyber Actors Likely to Target Schools with Ransomware

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 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? 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**

Product Serial Number: IA-44761-20 REV: 01 August 2017