JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: AA20-345A

December 10, 2020

Co-Authored by:

Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

SUMMARY

This Joint Cybersecurity Advisory was coauthored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The FBI, CISA, and MS-ISAC assess malicious cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services. Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year. These issues will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.

THREAT DETAILS

As of December 2020, the FBI, CISA, and MS-ISAC continue to receive reports from K-12 educational institutions about the disruption of distance learning efforts by cyber actors.

Ransomware

The FBI, CISA, and MS-ISAC have received numerous reports of ransomware attacks against K-12 educational institutions. In these attacks, malicious cyber actors target school computer systems, slowing access, and—in some instances—rendering the systems inaccessible for basic functions, including distance learning. Adopting tactics previously leveraged against business and industry, ransomware actors have also stolen—and threatened to leak—confidential student data to the public unless institutions pay a ransom.

According to MS-ISAC data, the percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July.

The five most common ransomware variants identified in incidents targeting K-12 schools between January and September 2020—based on open source information as well as victim and third-party incident reports made to MS-ISAC—are Ryuk, Maze, Nefilim, AKO, and Sodinokibi/REvil.

Malware

Figure 1 identifies the top 10 malware strains that have affected state, local, tribal, and territorial (SLTT) educational institutions over the past year (up to and including September 2020). *Note*: These malware variants are purely opportunistic as they not only affect educational institutions but other organizations as well.

ZeuS and Shlayer are among the most prevalent malware affecting K-12 schools.

- ZeuS is a Trojan with several variants that targets Microsoft Windows operating systems. Cyber actors use ZeuS to infect target machines and send stolen information to command-and-control servers.
- Shlayer is a Trojan downloader and dropper for MacOS malware.[1] It is primarily distributed through malicious websites, hijacked domains, and malicious advertising posing as a fake Adobe Flash updater.

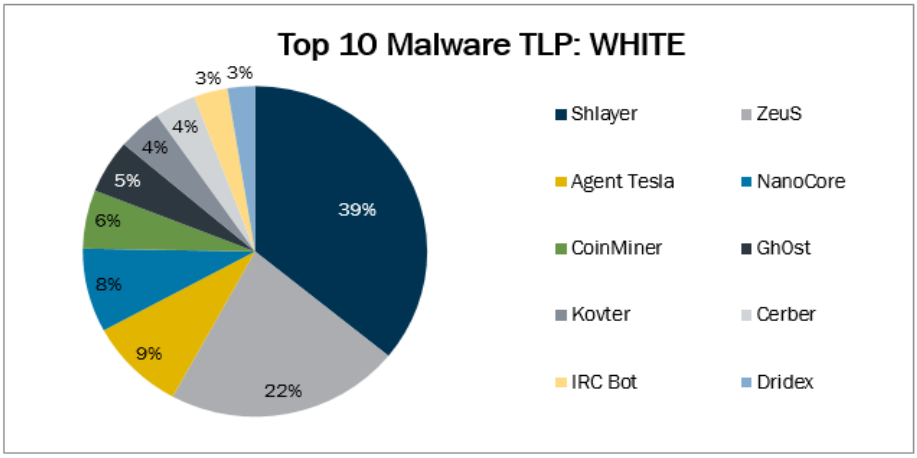

Figure 1: Top 10 malware affecting SLTT educational institutions

Distributed Denial-of-Service Attacks

Cyber actors are causing disruptions to K-12 educational institutions—including third-party services supporting distance learning—with distributed denial-of-service (DDoS) attacks,[2] which temporarily limit or prevent users from conducting daily operations. The availability of DDoS-for-hire services provides opportunities for any motivated malicious cyber actor to conduct disruptive attacks regardless of experience level.

[1] Shlayer is the only malware of the top 10 that targets MacOS; the other 9 affect Microsoft Windows operating systems.
[2] DDoS attacks overwhelm servers with a high level of internet traffic originating from many different sources, making it impossible to mitigate at a single source.

Video Conference Disruptions

Numerous reports received by the FBI, CISA, and MS-ISAC since March 2020 indicate uninvited users have disrupted live video-conferenced classroom sessions. These disruptions have included verbally harassing students and teachers, displaying pornography and/or violent images, and doxing[3] meeting attendees. To enter classroom sessions, uninvited users have been observed:

- Using student names to trick hosts into accepting them into class sessions, and
- Accessing meetings from either publicly available links or links shared with outside users (e.g., students sharing links and/or passwords with friends).

Video conference sessions without proper control measures risk disruption or compromise of classroom conversations and exposure of sensitive information.

ADDITIONAL RISKS AND VULNERABILITIES

In addition to the recent reporting of distance learning disruptions received by the FBI, CISA, and MS-ISAC, malicious cyber actors are expected to continue seeking opportunities to exploit the evolving remote learning environment.

Social Engineering

Cyber actors could apply social engineering methods against students, parents, faculty, IT personnel, or other individuals involved in distance learning. Tactics, such as phishing, trick victims into revealing personal information (e.g., password or bank account information) or performing a task (e.g., clicking on a link). In such scenarios, a victim could receive what appears to be legitimate email that:

- Requests personally identifiable information (PII) (e.g., full name, birthdate, student ID),
- Directs the user to confirm a password or personal identification number (PIN),
- Instructs the recipient to visit a website that is compromised by the cyber actor, or
- Contains an attachment with malware.

Cyber actors also register web domains that are similar to legitimate websites in an attempt to capture individuals who mistype URLs or click on similar looking URLs. These types of attacks are referred to as Domain Spoofing or Homograph attacks. For example, a user wanting to access *www.cottoncandyschool.edu* could mistakenly click on *www.cottencandyschool.edu* (changed "o" to an "e") or *www.cottoncandyschoo1.edu* (changed letter "l" to a number "1").[4] Victims believe they are on a legitimate website when, in reality, they are visiting a site controlled by a cyber actor.

[3] Doxing is the act of compiling or publishing personal information about an individual on the internet, typically with malicious intent.
[4] This is a fictitious example to demonstrate how a user can mistakenly click and access a website without noticing subtle changes in website URLs.

Technology Vulnerabilities and Student Data

Whether as collateral for ransomware attacks or to sell on the dark web, cyber actors may seek to exploit the data-rich environment of student information in schools and education technology (edtech) services. The need for schools to rapidly transition to distance learning likely contributed to cybersecurity gaps, leaving schools vulnerable to attack. In addition, educational institutions that have outsourced their distance learning tools may have lost visibility into data security measures. Cyber actors could view the increased reliance on—and sharp usership growth in—these distance learning services and student data as lucrative targets.

Open/Exposed Ports

The FBI, CISA, and MS-ISAC frequently see malicious cyber actors exploiting exposed Remote Desktop Protocol (RDP) services to gain initial access to a network and, often, to manually deploy ransomware. For example, cyber actors will attack ports 445 (Server Message Block [SMB]) and 3389 (RDP) to gain network access. They are then positioned to move laterally throughout a network (often using SMB), escalate privileges, access and exfiltrate sensitive information, harvest credentials, or deploy a wide variety of malware. This popular attack vector allows cyber actors to maintain a low profile, as they are using a legitimate network service that provides them with the same functionality as any other remote user.

End-of-Life Software

End-of-Life (EOL) software is regularly exploited by cyber actors—often to gain initial access, deface websites, or further their reach in a network. Once a product reaches EOL, customers no longer receive security updates, technical support, or bug fixes. Unpatched and vulnerable servers are likely to be exploited by cyber actors, hindering an organization's operational capacity.

MITIGATIONS

Plans and Policies

The FBI and CISA encourage educational providers to maintain business continuity plans—the practice of executing essential functions through emergencies (e.g., cyberattacks)—to minimize service interruptions. Without planning, provision, and implementation of continuity principles, institutions may be unable to continue teaching and administrative operations. Evaluating continuity and capability will help identify potential operational gaps. Through identifying and addressing these gaps, institutions can establish a viable continuity program that will help keep them functioning during cyberattacks or other emergencies. The FBI and CISA suggest K-12 educational institutions review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by cyber actors.

Network Best Practices

- Patch operating systems, software, and firmware as soon as manufacturers release updates.

- Check configurations for every operating system version for educational institution-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as student database servers and distance learning infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

User Awareness Best Practices

- Focus on awareness and training. Because end users are targeted, make employees and students aware of the threats—such as ransomware and phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- Ensure employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.
- Monitor privacy settings and information available on social networking sites.

Ransomware Best Practices

The FBI and CISA do not recommend paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, regardless of whether your organization decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office. Doing so provides the FBI with the critical information they need to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under U.S. law.

In addition to implementing the above network best practices, the FBI and CISA also recommend the following:

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

Denial-of-Service Best Practices

- Consider enrolling in a denial-of-service mitigation service that detects abnormal traffic flows and redirects traffic away from your network.
- Create a partnership with your local internet service provider (ISP) prior to an event and work with your ISP to control network traffic attacking your network during an event.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.

Video-Conferencing Best Practices

- Ensure participants use the most updated version of remote access/meeting applications.
- Require passwords for session access.
- Encourage students to avoid sharing passwords or meeting codes.
- Establish a vetting process to identify participants as they arrive, such as a waiting room.
- Establish policies to require participants to sign in using true names rather than aliases.
- Ensure only the host controls screensharing privileges.
- Implement a policy to prevent participants from entering rooms prior to host arrival and to prevent the host from exiting prior to the departure of all participants.

Edtech Implementation Considerations

When partnering with third-party and edtech services to support distance learning, educational institutions should consider the following:

- The service provider's cybersecurity policies and response plan in the event of a breach and their remediation practices:
    - How did the service provider resolve past cyber incidents? How did their cybersecurity practices change after these incidents?
- The provider's data security practices for their products and services (e.g., data encryption in transit and at rest, security audits, security training of staff, audit logs);
- The provider's data maintenance and storage practices (e.g., use of company servers, cloud storage, or third-party services);
- Types of student data the provider collects and tracks (e.g., PII, academic, disciplinary, medical, biometric, IP addresses);
- Entities to whom the provider will grant access to the student data (e.g., vendors);
- How the provider will use student data (e.g., will they sell it to—or share it with—third parties for service enhancement, new product development, studies, marketing/advertising?);

- The provider's de-identification practices for student data; and
- The provider's policies on data retention and deletion.

Malware Defense

Table 1 identifies CISA-created Snort signatures, which have been successfully used to detect and defend against related attacks, for the malware variants listed below. *Note*: The listing is not fully comprehensive and should not be used at the exclusion of other detection methods.

Table 1: Malware signatures

Malware	Signature
NanoCore	`alert tcp any any -> any $HTTP_PORTS (msg:"NANOCORE:HTTP GET URI contains 'FAD00979338'"; sid:00000000; rev:1; flow:established,to_server; content:"GET"; http_method; content:"getPluginName.php?PluginID=FAD00979338"; fast_pattern; http_uri; classtype:http-uri; metadata:service http;)`
Cerber	`alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains 'host|3a 20|polkiuj.top'"; sid:00000000; rev:1; flow:established,to_server; flowbits:isnotset,<unique_ID>.tagged; content:"host|3a 20|polkiuj.top|0d 0a|"; http_header; fast_pattern:only; flowbits:set,<unique_ID>.tagged; tag:session,10,packets; classtype:http-header; metadata:service http;)`
Kovter	`alert tcp any any -> any $HTTP_PORTS (msg:"Kovter:HTTP URI POST to CnC Server"; sid:00000000; rev:1; flow:established,to_server; flowbits:isnotset,<unique_ID>.tagged; content:"POST / HTTP/1.1"; depth:15; content:"Content-Type\|3a 20\|application/x-www-form-urlencoded"; http_header; depth:47; fast_pattern; content:"User-Agent\|3a 20\|Mozilla/"; http_header; content:!"LOADCURRENCY"; nocase; content:!"Accept"; http_header; content:!"Referer\|3a\|"; http_header; content:!"Cookie\|3a\|"; nocase; http_header; pcre:"/^(?:[A-Za-z0-9+\/]{4})*(?:[A-Za-z0-9+\/]{2}==\|[A-Za-z0-9+\/]{3}=\|[A-Za-z0-9+\/]{4})$/P"; pcre:"/User-Agent\x3a[^\r\n]+\r\nHost\x3a\x20(?:\d{1,3}\.){3}\d{1,3}\r\nContent-Length\x3a\x20[1-5][0-9]{2,3}\r\n(?:Cache-Control|Pragma)\x3a[^\r\n]+\r\n(?:\r\n)?$/H"; flowbits:set,<unique_ID>.tagged; tag:session,10,packets; classtype:nonstd-tcp; metadata:service http;)`

Dridex	`alert tcp any any -> any $HTTP_PORTS (msg:"HTTP URI GET contains 'invoice_########.doc' (DRIDEX)"; sid:00000000; rev:1; flow:established,to_server; content:"invoice_"; http_uri; fast_pattern:only; content:".doc"; nocase; distance:8; within:4; content:"GET"; nocase; http_method; classtype:http-uri; metadata:service http;)`  `alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains 'Host|3a 20|tanevengledrep ru' (DRIDEX)"; sid:00000000; rev:1; flow:established,to_server; flowbits:isnotset,<unique_ID>.tagged; content:"Host|3a 20|tanevengledrep|2e|ru|0d 0a|"; http_header; fast_pattern:only; flowbits:set,<unique_ID>.tagged; tag:session,10,packets; classtype:http-header; metadata:service http;)`

CONTACT INFORMATION

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting organization; and a designated point of contact.

To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

RESOURCES

MS-ISAC membership is open to employees or representatives from all public K-12 education entities in the United States. The MS-ISAC provides multiple cybersecurity services and benefits to help K-12 education entities increase their cybersecurity posture. To join, visit https://learn.cisecurity.org/ms-isac-registration.

CISA Telework Guidance and Resources

CISA Cybersecurity Recommendations and Tips for Schools Using Video Conferencing

CISA Ransomware Publications

CISA Emergency Services Sector Continuity Planning Suite

CISA-MS-ISAC Joint Ransomware Guide

CISA Tip: Avoiding Social Engineering and Phishing Attacks

CISA Tip: Understanding Patches

CISA and CYBER.ORG “Cyber Safety Video Series” for K-12 students and educators

FBI PSA: “High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations

Note: Contact your local FBI field office (www.fbi.gov/contact-us/field) for additional FBI products on ransomware, edtech, and cybersecurity for educational institutions.