Ransomware: Could Your District Repel an Attack?

January 21, 2021

Cam Shilling founded McLane Middleton’s Information Privacy and Security Group in 2009. His expertise includes managing information privacy and security risk assessments under both domestic and international laws, preparing and implementing written policies, workforce trainings, addressing day-to-day information privacy and security issues, investigating and remediating breaches and other incidents, and handling governmental audits as well as consumer lawsuits asserted against organizations.
Trends in Malware Incidents

Ransomware as % of School District Malware Incidents

<table>
<thead>
<tr>
<th></th>
<th>Ransomware</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>26%</td>
<td>74%</td>
</tr>
<tr>
<td>2019</td>
<td>42%</td>
<td>58%</td>
</tr>
<tr>
<td>2020</td>
<td>80%</td>
<td>28%</td>
</tr>
</tbody>
</table>

Examples of Ransomware Victims

- **Tiplersville, MS**
  - CCSD: 330,000
  - North Tippah School District: 1,200

- **Tyngsborough, MA**
  - Fairfax County Public Schools: 187,000
  - 400

- **Bainville, MT**
  - Baltimore City Public Schools: 115,000
  - Athens: 3,000
  - 43

- **Other**
  - 52,000
Multitudes of Ransomware Incidents

K-12 Cyber Incident Map

Incidents Reported from 2016 to Present

Why Are School Districts Targets?

1. Limited personnel and resources to invest in cyber security defenses
2. Valuable sensitive personal information about children and families
3. Financial resources to pay ransom, or coverage by cyber liability insurance
Why Is Ransomware So Effective?

1. Zero day threats now normal
   - Undetectable by normal anti-malware
   - Industrialization and segmentation of activities

2. Sophisticated code operates covertly
   - Deployed on networks and devices, then wait
   - Undetectable by advanced systems until activated

3. Exportation and encryption
   - Backups no longer effective against ransom

So What Is a District To Do?

Can the School District Repel a Sophisticated Ransomware Attack?

How Much Harm Will the District Prevent if/when It Cannot Do So?
What Are Common Attack Vectors?

1. **Phishing** results in credential compromise or malware download
2. **Malicious Website** downloads malware
3. **Credential Compromise** from other hacked online accounts or websites
4. **Application Compromise** (e.g., SolarWinds)

---

**Protect Against Phishing**

- Training (though it is never effective enough)
- Banner for emails originating outside network
- Suspicious email alert button for users, with prompt responsive systemic quarantine and removal
- Sandboxing for all email attachments launched and links clicked within email
Protect Against Malicious Websites

- Robust website browsing limitations for all students, faculty, staff, other employees, volunteers, etc.
- Local firewalls activated on all desktops and laptops
- Multiple layers of advanced activity based threat detection and prevention applications

Protect Against Credential Compromise

- Proper password complexity or passphrases
- Routine password changes (not < every 6 months)
- Monitor dark web for compromised credentials
- Enable multi-factor authentication for applications and accounts whenever possible
## Protect Against Application Compromise

- Inventory all applications on networks and devices
- Implement mandatory routine patching (immediate for security patches and not < weekly for others)
- Remove administrator privileges from all users, and create restricted use administrator credentials
- Routine internal vulnerability scanning

## Additional Ransomware Protections

- Multi-layered advanced threat detection/prevention
- Robust actual and virtual partitioning of network
- Robust limitations on user access privileges
- Robust logging of user access and activity
- Full system backups in air-gapped or other secure storage, or secure failover redundancy
- Encryption of data at-rest on network and devices
- Appropriate cyber liability insurance coverage
Response to Ransomware Incident

1. Rapid Response: notify police, neutralize malware, forensics and recover logs, restore from backups
2. Rapid Notification: notice tailored to information encrypted by ransomware
3. Ransom Demand: verify information compromised, decide whether to pay, negotiate amount
   • Prohibition against paying ransom to actors on sanctions list or connected to actors sanctions list
4. Additional Notification If Necessary

Questions about Ransomware

Questions?
EDUCATION

Schools Struggling to Stay Open Get Hit by Ransomware Attacks

Districts around the U.S. are fighting a wave of increasingly aggressive hackers, who are publicly posting sensitive student information

By Tawnell D. Hobbs | Photographs by Justin Clemons for The Wall Street Journal

Nov. 13, 2020 9:52 am ET

Just as school was to start this semester, technology chief Tony Brooks rushed to his office in Athens, Texas. Colleagues said they were unable to access the school district’s network.

He logged into his computer. A message popped up: “All your important files are encrypted!”

“I immediately freaked out,” said Mr. Brooks. “I got my team together and said we need to go and unplug every computer. We didn’t want the virus to spread any more.”

Mr. Brooks, who works in the 3,000-student Athens Independent School District, soon found himself corresponding with a cyber pirate who demanded money in return for freeing the district’s systems, which were full of personal and financial information. The district shared screenshots of the interactions with The Wall Street Journal, revealing a rare close-up look at the details of a ransomware attack.

“How would payment be made?” Mr. Brooks responded.

“BTC,” the hacker wrote, meaning bitcoin, which allows payment with no middlemen.

Schools around the U.S. are fighting a wave of increasingly aggressive ransomware attacks by hackers. The U.S. Treasury Department warned last month that ransomware attacks in general have increased during the coronavirus pandemic—and districts make
an especially tempting target due to their often thinly staffed technology departments and networks full of personal data.

It’s a significant new source of stress in what’s already been a difficult year, with the pandemic forcing closures, a chaotic implementation of remote learning and complicated schedules.

Hackers have for years used ransomware, a type of malicious software, to lock up computers or files until the demanded sum was paid—but they generally left it at that for school districts. Now they are grabbing data such as addresses, phone numbers, Social Security numbers, grades and other sensitive student information to post online if payment isn’t made. The information can aid identity theft or be highly embarrassing for vulnerable young people.

“It is extortion,” said Elizabeth Clarke, spokeswoman for cybersecurity firm Armor Defense Inc. “The ransomware has gotten more heinous. To incite you to pay, they say, ‘Hey, we’ve got all the data, and we’ll be happy to post.’ ”

A server room at Athens High School.

There is no official U.S. clearinghouse to track ransomware cases, but some cybersecurity firms, which track known incidents from news reports along with their own private cases, say they are seeing an increase in cases involving schools and colleges, which are now heavily reliant on online learning and technology to run their operations.

Based on searches of hackers’ sites on the dark web—a network of websites accessed through special software that gives users anonymity—as well as publicly known cases,
the Journal has documented nearly three dozen ransomware attacks against school districts since the pandemic began in March.

That tally, affecting districts educating more than 700,000 students, doesn’t include numerous private schools, community colleges and universities that have also come under attack.

The figure underestimates the actual number of cases. Some districts switch to backup servers that escaped attacks or quietly pay ransom without ever making it public, reluctant to admit they were hacked and eager to move on, security experts say. Hackers often tell their victims not to call law enforcement.

Even those that have gone public often don’t reveal the amount of ransom paid. A tally of seven cases by the Journal found that school districts, colleges and universities have paid at least $2 million in the past 12 months, on top of the often burdensome costs of better securing their systems. Ransom amounts in those cases ranged from $35,000 to $1.14 million.

Average ransom payments across all industries have climbed in recent years, to $233,817 in the third quarter of this year from $41,198 a year earlier, according to cybersecurity firm Coveware Inc.

Security experts say that many ransomware hackers operate outside of the U.S. and are hard to capture.

**On their own**

Districts are often on their own when it comes to figuring out how to deal with hackers or how to keep their systems safe. In an October letter, U.S. Senators Jacky Rosen and Catherine Cortez Masto, both Nevada Democrats, asked U.S. Department of Education Secretary Betsy DeVos and Homeland Security Acting Secretary Chad Wolf to address ransomware attacks against schools and districts.

The letter cited an article in September by the Journal that revealed that hackers published student grades, employee Social Security numbers and other sensitive data from the 320,000-student Clark County School District in Las Vegas when a ransom wasn’t paid.
An attack in Ohio’s Toledo Public Schools has been especially egregious. Information posted on the hacker’s website in October includes Social Security numbers and dates of birth for students and employees, disciplinary and disability information on students, employee evaluations and exam grades. It included the identities of an eighth-grader listed as emotionally disturbed, a ninth-grader suspended for sexual activity and a roster of foster children.

As with other attacks, the hackers posted the data on the dark web.

Toledo parent Krista Wilcox is mad that her 8-year-old son could have his identity compromised, and that she found out about the release of information from media reports instead of from the district.

“My information is out there, and they could contact me,” she said. “How do I know it’s not child traffickers? I feel betrayed by the school system.”

Toledo Public Schools said in a written statement that the 23,000-student district reached out to the Federal Bureau of Investigation and contacted cybersecurity experts to determine the scope of the attack. The district is encouraging parents and guardians to monitor credit reports.

Hackers often negotiate with their victims. The Sheldon Independent School District in Houston, Texas, paid a ransom of $206,931, negotiated down from about $350,000, after an attack in March.

After payment, the 10,000-student district couldn’t recover about 10% of its files—not an unusual amount to lose in ransomware cases, security experts say. Administrators fear the hacker kept some of the district’s data, prompting them to notify parents and employees of the possibility.

Sheldon officials believe the hackers got into their system through a phishing email, meaning someone opened an email that had an attachment or link to malicious software. Hackers also enter from weak cybersecurity controls and user login information.
'School possibly could have been delayed many weeks,’ says Athens Superintendent Janie Sims.

School districts have a steady stream of revenue in the form of tax dollars, and their reserve funds are typically open to public view.

“High revenue and low cyber security is basically an open invitation,” said a person reached through the SunCrypt hacker’s site who identified as a member of the group in a typed chat interview with the Journal on the dark web.

SunCrypt recently hacked Haywood County Schools in Waynesville, N.C., and began posting data from the district in late August. The 7,100-student district said it called in law enforcement, but declined to comment further due to a continuing federal investigation.

The person identifying as a SunCrypt member said the group asked for about $500,000 from the district—about 17% of the district’s $2.9 million general reserve fund in June.

The first information released from Haywood included administrative files, such as an employee cellphone directory and a listing of students with absences. The first dump usually contains the least sensitive information, often used as proof of the theft or a warning to pay, experts say.

The person identifying as a SunCrypt member said the group doesn’t have plans to post any more information from Haywood, saying its scouts had mistakenly thought it was a private college. They said the group has provided some entities with a “Covid-19 discount” and ended negotiations with Haywood when the district involved a third party—in this case, law enforcement.
Infected

In Athens, the hacker locked the district’s roughly 30 servers, along with backup servers, and infected hundreds of computers connected to the network, Mr. Brooks said. The attack halted student registration six days before the start of the new school year.

In the initial pop-up message, the hacker provided a link and instructions for entering the dark web. Mr. Brooks brought in help from Brent Goerner, a technology specialist at the district’s regional education service center—an organization established by the state to provide a range of support services.

Mr. Brooks followed the hacker’s instructions the next day, ending up at a chat window.

“how many pc do you need decrypted?” the hacker asked. Mr. Brooks took the question to mean: How many servers and computers would need to be unlocked by a decryption key that the hackers would give him upon receipt of payment.

Before he could respond, the hacker said, “I want for everything pc 50 000$.”

Mr. Brooks planned to negotiate the figure, but before he could start, the hacker let him know it held the decryption key for more than 200 district devices.

“see I have a very big list of keys,” the hacker said in the chat. “more than 200 pc.”

“what about if we only needed 20 PC,” Mr. Brooks asked, thinking that the district might need decryption keys for only certain servers—mainly for a critical one holding student and financial data.

“then 1 PC - 1000$,” the hacker responded.

“ok, I need to discuss with my boss,” Mr. Brooks wrote.
The Athens school district believes a vendor doing work on the system may have left it vulnerable to hackers.

The hacker also told Mr. Brooks not to call police.

“*they won’t let you pay and won’t help you decrypt files,*” the hacker said in the chat. “*and you’ll lose data for always.*”

Mr. Brooks replied: “*we are not talking to the police. I just need to see how we can come up with the money...We are working with you and want to decrypt our data.*”

He added: “*how do we know our files will not be re-encrypted once we pay you?*”

The hacker said: “*Yes. I’m going to remove you...and tell you where to close the holes through that we’ve penetrated.*”

It’s not unusual for hackers to offer such security reports to paying victims, telling them how they got hacked. Some cybersecurity experts question the accuracy of such reports and discourage victims from paying.

“If the flow of money stops, the attacks will stop,” said Brett Callow, a threat analyst at cybersecurity firm Emsisoft, which also creates decryption tools to unlock files. “The alternative is that cybercriminals will continue to become better resourced, more motivated. It’s a vicious cycle.”

In June, the University of California, San Francisco paid a $1.14 million ransom to a hacker. The university said in a written statement that it made the decision to pay because the hacker encrypted data for important academic work, including research.
Hackers have about a 97% rate of delivering a decryption tool to victims once the ransom is paid, Coveware found. But the company recently reported that some hackers held on to data after payment, possibly selling it to other hackers or using it to re-extort the victim.

The FBI, which encourages victims to reach out to their local FBI field office, doesn’t support paying a ransom as it can embolden hackers to target others, but says it understands that organizations faced with an inability to function will evaluate all options to protect employees and customers.

Amy Kelley, an algebra teacher at Athens Middle School, connects with her students via an iPad that moves along with her.

A lone technology director oversees operations in the 1,250-student North Tippah School District in rural Tiplersville, Miss., which got hacked in August. “There’s not too many people I had to talk to, to say, ‘What do we do from here?’ ” said Superintendent Scott Smith, who added that the district paid no ransom but declined to say more as the matter is still being addressed.

Hackers can be in victims’ systems days or weeks, giving them time to take data before deploying ransomware, according to Emsisoft. Once they do take over, they treat it like a financial transaction, with some even referring to victims as clients.

“...it’s business,” the hacker told Mr. Brooks at the end of their conversation.

“perfect. understand,” Mr. Brooks said.

In an emergency meeting, the Athens school board approved paying $50,000 in ransom the day after the attack. The board also pushed back the new school year by a week due to
the hacking. Some community members didn’t like having to pay off a hacker, but the district said it had little choice.

“No one wants to do this. It feels awful,” Athens superintendent Janie Sims said. “But it could be worse if we didn’t pay. School possibly could have been delayed many weeks. We felt we had to.”

Mr. Brooks blamed himself. “I felt like a complete and total failure,” he said. He isn’t certain how the hacker got in but believes a vendor doing work in a server left open a meeting app, giving the hacker a way into the system.

Two days after the attack, Mr. Brooks, on little sleep, placed a late-night call to Dr. Sims. He’d made a big discovery—a copy of a backup server held the data from the compromised critical server.

“I jumped up out of my chair,” Mr. Brooks said. “I was screaming, ‘Yes, yes!’”

He broke off communications with the hacker, who hadn’t mentioned posting any of the school’s data.

Mr. Brooks said engineers found no indication that information had been stolen—it looked like the hacker had just locked the servers without ever taking any data. Computer hard drives were wiped and reinstalled.

The district paid no ransom.

Write to Tawnell D. Hobbs at Tawnell.Hobbs@wsj.com

Appeared in the November 14, 2020, print edition as ‘Hackers Target Schools in New Wave of Cyberattacks.’
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.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.
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. Shlayer is the only malware of the top 10 that targets MacOS; the other 9 affect Microsoft Windows operating systems.

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, 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 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.cottoncandyschool.edu (changed letter “l” to a number “1”). 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?);
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>
<thead>
<tr>
<th>Malware</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>NanoCore</td>
<td>alert tcp any any -&gt; any $HTTP_PORTS (msg:&quot;NANOCORE: HTTP GET URI contains 'FAD00979338'&quot;; sid:00000000; rev:1; flow established, to_server; content:&quot;GET&quot;; http_method; content:&quot;getPluginName.php?PluginId=FAD00979338&quot;; fast_pattern; http_uri; classtype:http-uri; metadata:service http;)</td>
</tr>
<tr>
<td>Cerber</td>
<td>alert tcp any any -&gt; any $HTTP_PORTS (msg:&quot;HTTP Client Header contains 'host</td>
</tr>
<tr>
<td>Kovter</td>
<td>alert tcp any any -&gt; any $HTTP_PORTS (msg:&quot;Kovter:HTTP URI POST to CnC Server&quot;; sid:00000000; rev:1; flow established, to_server; flowbits:isnotset,&lt;unique_ID&gt;.tagged; content:&quot;POST / HTTP/1.1&quot;; depth:15; content:&quot;Content-Type\x3a application/x-www-form-urlencoded&quot;; http_header; depth:47; fast_pattern; content:&quot;User-Agent\x3a Mozilla/&quot;; http_header; content:&quot;LOADCURRENCY&quot; nocase; content:&quot;Accept&quot;; http_header; content:&quot;Referer\x3a&quot;; http_header; content:&quot;Cookie\x3a&quot;; http_header; pcre:/(?:[\x28A-Za-z0-9+/-/&amp;?=]+\s(\S+))\s)/P&quot;; pcre:=&quot;/^\s*(?i:.?://[A-Za-z0-9-]+)?\s*(?:[A-Za-z0-9-.]+)?\s*(?:[A-Za-z0-9-.]+)?\s*(?:[A-Za-z0-9-.]+)?\s*(?:[A-Za-z0-9-.]+)?\s*/\P&quot;; pcre=&quot;/^\s*(?i:\s<em>User-Agent)\s</em>\x3a\s*(\S+)?\s*/\P&quot;; flowbits:set,&lt;unique_ID&gt;.tagged; tag:session,10,packets; classtype:nonstd-tcp; metadata:service http;)</td>
</tr>
</tbody>
</table>
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.
Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: October 1, 2020

The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.²

Background on Ransomware Attacks

Ransomware is a form of malicious software (“malware”) designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims’ access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims’ sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims’ access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation’s 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.³ While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

---

¹ This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, or otherwise addressing any particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

² This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners’ cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

businesses, local government agencies, hospitals, and school districts, which may be more vulnerable as they may have fewer resources to invest in cyber protection.

**OFAC Designations of Malicious Cyber Actors**

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.\(^4\) OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.\(^5\)

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two digital currency addresses used to funnel SamSam ransomware proceeds.\(^6\)

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.\(^7\)

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.\(^8\)

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

---


Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC’s Economic Sanctions Enforcement Guidelines (Enforcement Guidelines) provide more information regarding OFAC’s enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Under the Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions laws or regulations, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response (including the amount of civil monetary penalty, if any).

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services

---

10 31 C.F.R. part 501, appx. A.
11 To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published A Framework for OFAC Compliance Commitments, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The Framework is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.
businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.¹²

Under OFAC’s Enforcement Guidelines, OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company’s full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

**OFAC Licensing Policy**

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.

**Victims of Ransomware Attacks Should Contact Relevant Government Agencies**

OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm’s ability to perform critical financial services.

- U.S. Department of the Treasury’s Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

¹² See FinCEN Guidance, FIN-2020-A00X, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.
Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
- U.S. Secret Service Cyber Fraud Task Force
  o [www.secretservice.gov/investigation/#field](www.secretservice.gov/investigation/#field)
- Cybersecurity and Infrastructure Security Agency
  o [https://us-cert.cisa.gov/forms/report](https://us-cert.cisa.gov/forms/report)
- Homeland Security Investigations Field Office
  o [https://www.ice.gov/contact/hsi](https://www.ice.gov/contact/hsi)

*If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC’s Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.*
Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related financial red flag indicators; and (4) reporting and sharing information related to ransomware attacks.

The information contained in this advisory is derived from FinCEN’s analysis of cyber- and ransomware-related Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Ransomware is a form of malicious software (“malware”) designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims’ access to their systems or data.¹ In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities.

¹ Both extortion and computer fraud and abuse are specified unlawful activities and predicate offenses to money laundering. See 18 USC § 1956(c)(7).
The role of financial intermediaries in facilitating ransomware payments

Ransomware attacks are a growing concern for the financial sector because of the critical role financial institutions play in the collection of ransom payments. Processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more money services business (MSB). Many ransomware schemes involve convertible virtual currency (CVC), the preferred payment method of ransomware perpetrators. Following the delivery of the ransom demand, a ransomware victim will typically transmit funds via wire transfer, automated clearinghouse, or credit card payment to a CVC exchange to purchase the type and amount of CVC specified by the ransomware perpetrator. Next, the victim will send the CVC, often from a wallet hosted2 at the exchange, to the perpetrator’s designated account or CVC address. The perpetrator then launders the funds through various means, including mixers and tumblers3 to convert funds into other CVCs, smurfing4 transactions across many accounts and exchanges, and/or moving the CVC to foreign-located exchanges and peer-to-peer (P2P) exchangers5 in jurisdictions with weak anti-money laundering and countering financing of terrorism (AML/CFT) controls.

2. “Hosted wallets” are CVC wallets where the CVC exchange receives, stores, and transmits the CVCs on behalf of their accountholders. See FinCEN Guidance, FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,” (May 9, 2019).

3. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.

4. Smurfing refers to a layering technique in money laundering that involves breaking total amounts of funds into smaller amounts to move through multiple accounts before arriving at the ultimate beneficiary.

5. P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements or fora, social media, and by word of mouth. See FinCEN Advisory, FIN-2019-A003, “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).
Involvement of Digital Forensics and Incident Response and Cyber Insurance Companies in Ransomware Payments

The prevalence of ransomware attacks has led to the creation of companies that provide protection and mitigation services to victims of ransomware attacks. Among these entities are digital forensics and incident response (DFIR) companies and cyber insurance companies (CICs). Some DFIR companies and CICs, as well as some MSBs that offer CVCs, facilitate ransomware payments to cybercriminals, often by directly receiving customers’ fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts. Depending on the particular facts and circumstances, this activity could constitute money transmission. Entities engaged in money services business activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to BSA obligations, including filing suspicious activity reports (SARs). Persons involved in ransomware payments must also be aware of any Office of Foreign Assets Control (OFAC)-related obligations that may arise from that activity. Today, OFAC issued an advisory highlighting the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities.

Trends and Typologies of Ransomware and Associated Payments

The severity and sophistication of ransomware attacks continue to rise across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions. Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the victims’ weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site, exploit remote desktop protocol endpoints and software vulnerabilities, or deploy “drive-by” malware attacks that host malicious code on legitimate websites. Proactive prevention through effective cyber hygiene, cybersecurity controls, and business continuity resiliency is often the best defense against ransomware.

Increasing Sophistication of Ransomware Operations

Big Game Hunting Schemes: Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as “big game hunting.”

Ransomware Criminals Forming Partnerships and Sharing Resources: Many cybercriminals are sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit kits that come with ready-made malicious codes and tools. These kits can be purchased, although they are also offered free of charge. Some ransomware groups are also forming partnerships to share advice, code, trends, techniques, and illegally-obtained information over shared platforms.

“Double Extortion” Schemes: Ransomware criminals are increasingly engaging in “double extortion schemes,” which involve removing sensitive data from the targeted networks and encrypting the system files and demanding ransom. The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom.

7. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 37% more reports of ransomware incidents in 2019 than in 2018, with a 46% increase in associated financial losses. BSA reporting shows a stark increase in financial losses per ransomware incident, with the average dollar amount in financial institution SARs on ransomware increasing approximately $87,000 from 2018 to 2019 ($417,000 to $504,000) and $280,000 from 2019 to thus far in 2020 ($504,000 to $783,000). See FBI IC3, “2019 Internet Crime Report” (2019); and FBI IC3, “2018 Internet Crime Report” (2018).


Use of Anonymity-Enhanced Cryptocurrencies (AECs): Cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in bitcoin (see Figure 1). However, they are also increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of CVC financial flows, including ransomware payments, through anonymizing features, such as mixing and cryptographic enhancements. Some ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs.

Use of “Fileless” Ransomware: Fileless ransomware is a more sophisticated tool that can be challenging to detect because the malicious code is written into the computer’s memory rather than into a file on a hard drive, which allows attackers to circumvent off-the-shelf antivirus and malware defenses.

Financial Red Flag Indicators of Ransomware and Associated Payments

FinCEN has identified the following financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.

1. IT enterprise activity is connected to cyber indicators that have been associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes. Malicious cyber activity may be evident in system log files, network traffic, or file information.

2. When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.

3. A customer’s CVC address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.

---


14. For more information about red flags of illicit CVC use, see FinCEN Advisory, [FIN-2019-A003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).

15. For example cyber indicators of compromise on specific ransomware threats, see DHS CISA Technical Alerts, “Ransomware Alerts.” For other cyber indicator resources, see also FinCEN’s Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection’s CILs and circulars, available upon request; and DHS CISA’s cyber analytic products and services, including a comprehensive list of COVID-19-related indicators of compromise in CSV or STIX-formatted XML formats, the Cyber Information Sharing and Collaboration Program (CISCP), and the Automated Indicator Sharing (AIS) program. Public-private and industry partnerships, such as the Financial Services Information Sharing and Analysis Center, and open source and commercial cyber threat feeds can also be useful resources.
A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a DFIR or CIC, especially one known to facilitate ransomware payments.

A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.

A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.

A DFIR, CIC, or other company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company’s normal business practices.

A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB.

A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.

A customer initiates multiple rapid trades between multiple CVCs, especially AECs, with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting Involving Ransomware and USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

Financial institutions can play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Financial institutions should determine if filing a SAR is required or appropriate when dealing with an incident of ransomware conducted by, at, or through the financial institution, including ransom payments made by financial institutions that are victims of ransomware. As a reminder, a financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to $5,000 (or, with one exception, $2,000 for MSBs)\(^\text{16}\) or more in funds or other assets and involves

\[\text{16. See 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000. See also 31 C.F.R. § 1022.320(a)(2).}\]
funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is
designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful
purpose; or involves the use of the financial institution to facilitate criminal activity. Reportable
activity can involve transactions, including payments made by financial institutions, related
to criminal activity like extortion and unauthorized electronic intrusions that damage, disable,
or otherwise affect critical systems. SAR obligations apply to both attempted and successful initiated extortion transactions.17

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. When filing a SAR regarding suspicious transactions that involve cyber events (including ransomware), financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative. When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Valuable cyber indicators for law enforcement investigations for ransomware can include relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.18 Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.19 When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or anti-money laundering program. These procedures may include, for example, independent employment verification with the requestor’s field office or face-to-face review of the requestor’s credentials.20

17. FinCEN assesses that ransomware-related activity is under-reported.
18. See 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).
SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

"CYBER-FIN-2020-A006"

in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including "ransomware" as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity. Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving ransomware schemes. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (“SUAs”) and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including extortion and computer fraud and abuse. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.21

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

21 For further guidance related to the 314(b) Program, see FinCEN Fact Sheet, “Section 314(b)” (November 2016) and FinCEN Guidance, FIN-2009-G002, “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).