CorporateOne
FEDERAL CREDIT UNION

FinCEN updates ransomware red flags: BSA/AML and OFAC compliance impacts

Jennifer Morrison, VP, Senior Risk Manager

Ransomware is a real and growing threat to credit unions and your members. On November 8, the Financial Crimes Enforcement Network (FinCEN) updated its year-old list of red flags raised by ransomware payments. This update was part of a coordinated effort with the Department of Justice against two foreign cyberthieves and the Baltic cryptocurrency exchanges they used to launder the funds. FinCEN's update is timely and has an impact on your credit union's BSA/AML compliance efforts, as well as on your Office of Foreign Assets Control (OFAC) compliance.

New resources
The Department of Justice and the Department of Homeland Security, together with federal partners, launched a new website to combat the ransomware threat: StopRansomware.gov. This is a one-stop hub with educational resources for businesses, individuals, and other organizations. I encourage you to visit the site and share its insights with your compliance and IT teams.

Today's article discusses the advisory and includes guidance on how to help your credit union proactively improve your security safeguards. You can also view FinCEN's advisory in full here.

Summary and background

On November 8, 2021, federal prosecutors said that the Ukrainian national Yaroslav Vasinskyi and Russian-national Yevgeniy Polyanin infected tens of thousands of computers around the world with the Sodinokibi/REvil ransomware over the past two years. Federal prosecutors also said that the two helped extort financial institutions, governments, and other victims out of $200 million worth of Bitcoins and Monero.

A month prior, FinCEN issued a multi-page analysis that disclosed that banks, cryptocurrency exchanges, and other regulated companies filed 635 Suspicious Activity Reports (SARs) on suspected ransomware transactions in the first six months of 2021. (This was after filing fewer than 500 in all of 2020.) The combined value of the transactions flagged in these SARs already reached $590 million as of June 2021, which was up from $416 million in all of 2002; the total is on course to exceed that of the previous10 years combined. This is evidence of the rapid increase in such attacks, as SARs are likely filed on just a fraction of the ransomware attacks because much of the ransom is paid to or through offshore entities that may or may not have an obligation to file a SAR.

Breaking down the SARs

More than 60% of this year's SARs originated from digital forensic incident response firms, or DFIRs, that manage payments, usually in bitcoins, that victims of ransomware give their attackers to decrypt their IT systems. Nearly 20% of these DFIRs came directly from cryptocurrency exchanges and another 17% from depository institutions.

Many of the SARs from this year show perpetrators requesting payment in Bitcoin or Monero, according to FinCEN, but others do not specify a method of payment. This challenges the bureau's ability to draw conclusions about the most commonly sought cryptocurrencies during these attacks. SARs from financial institutions concluded that ransomware perpetrators often engaged in "chain hopping," an industry term for exchanging one type of cryptocurrency for another before shifting the digital tokens to another platform.

Perpetrators also avoided using the same wallet addresses more than once and instead sought to avoid detection by routing their funds through cryptocurrency mixers, decentralized financial-technology platforms, and overseas, centralized exchanges with opaque ownership to avoid detection. "Non-compliant centralized exchanges are possibly a key step in the layering and obfuscation process of laundering funds from CVC [virtual currency] to fiat currency," FinCEN wrote in its advisory.

Previous reminders and guidance from OFAC

On November 5, 2021, OFAC reminded cryptocurrency companies of their obligation to comply with U.S. sanctions while highlighting new technologies and procedures for avoiding illicit finance and potential enforcement. Many of the recommendations align with practices already used by traditional financial institutions, such as risk assessments, training in compliance processes, commitment from the company's executives, and know-your-member checks.

Other OFAC reminders appear tailored to the cryptocurrency industry specifically, including a recommendation that exchanges, miners, wallet providers and other businesses adopt protocols for geo-locating users based on their IP addresses, and to also incorporate data from member emails, payments and other sources when screening transactions for matches to U.S. sanctions. The guidance further advises the cryptocurrency sector to develop methods for automatically rejecting links to U.S.-blacklisted wallets and to employ capabilities for tracing and monitoring their connections to other addresses.

During 2021, OFAC has been active, blacklisting several cryptocurrency exchanges for their role in helping ransomware perpetrators, including the exchange used by Messrs. Vasinskyi and Polyanin located in Estonia, along with three other firms in Estonia and Latvia. Firms have also landed on the OFAC Specially Designated Nationals And Blocked Persons List (SDN) for providing IT support to such firms. OFAC SDN-listed firms are also located in the Czech Republic and Russia.

Application for your credit union

Credit unions should be especially careful of funds transfers going to countries in the Baltic region and Russia and the former Soviet bloc countries. This means educating and coordinating with staff who conduct foreign wire transfers. Many of these transactions also flow through the darknet markets and unlicensed traders in cryptocurrency. The aforementioned hackers left messages on the computers of their victims, directing them to an address on the Tor privacy network or a second address on the open web; there they would then find an address of a digital wallet to send their ransom payment in cryptocurrency and have their files decrypted.

Victims who did not pay the ransom often found their data stolen or were told that their data was sold to third parties, and the victims were unable to access their files.

Ransomware attacks continue to rise, financial institutions among primary targets

In analyzing the huge increase in ransomware attacks, FinCEN's advisory noted that the severity and sophistication of such attacks continues to rise with government entities and financial, educational, and healthcare institutions among the primary targets. Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the perception that these institutions have weaker cybersecurity controls, such as weaker system backups and ineffective incident response capabilities.

These crimes speak to the necessity for credit unions to have a thorough and secure data backup process and procedure in addition to a response team and cyber-insurance where available and applicable.

Tactics used by cybercriminals, tips for prevention

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns. These tactics 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. For a thorough explanation of each of the following ransomware categories, please review FinCEN's advisory:

- Extortion Schemes
- Use of Anonymity-Enhanced Cryptocurrencies
- Unregistered CVC Mixing Services
- Ransomware Criminals Forming Partnerships and Sharing Resources
- Use of "Fileless" Ransomware
- "Big Game Hunting" Schemes

Proactive prevention through effective cyber hygiene, cybersecurity controls, and business continuity resiliency is often the best defense against ransomware, according to FinCEN. And, it bears repeating that the key to compliance and prevention is communication and education between BSA/AML and staff who have wire transfer credentials. Staff should also educate their IT teams to report any criminal attacks and attempts, and in turn, convey the expectation that IT teams should keep compliance staff apprised as the cyber threat landscape continues to evolve. Many of the red flags, as noted above, involve offshore entities, highlighting the OFAC connection.

- A credit union or its member detects IT enterprise activity that is connected to ransomware cyber indicators or known cyber threat actors. Malicious cyber activity may be evident in system log files, network traffic, or file information.

- When opening a new account or during other interactions with the credit union, a member provides information that a payment is in response to a ransomware incident.
- A member's CVC address, or an address with which a member conducts transactions, is connected to ransomware variants, payments, or related activity. These connections may appear in open sources or commercial or government analyses. This means the BSA/AML team should be monitoring such sites for member information and investigating a member's unusual transaction by searching such sites.
- An irregular 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. Are such organizations among your membership? If so, ramp up your monitoring of these member accounts.
- A DFIR or CIC member receives funds from a counterparty and shortly after receipt of funds sends equivalent amounts to a CVC exchange. While unlikely among your membership, search your membership for these entities periodically.
- A member shows limited knowledge of CVC during onboarding or via other interactions with the credit union, yet asks about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the member is a victim of ransomware.
- A member that has no or limited history of CVC transactions sends a large CVC transaction, particularly when outside a member's normal business practices.
- Again, unlikely to be among your membership, any member 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 member is acting as an unregistered money services business (MSB).
- A member uses a foreign-located CVC exchanger in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities. Remember to educate and collaborate with staff who conduct funds transfers.
- A member receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs, especially AECs, with no apparent related purpose, followed by a transaction off the platform. This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction. Again, your funds transfer staff should be educated!
- A member initiates a transfer of funds involving a mixing service. Again, your funds transfer staff is critical here.
- A member uses an encrypted network (e.g., the onion router) or an unidentified web portal to communicate with the recipient of the CVC transaction.

SAR filing for cyber events

We are all called upon to help combat ransomware, and it is therefore critical for your credit union to immediately report any suspicious transactions potentially associated with ransomware attacks.

- First, FinCEN directs credit unions aware of recent or ongoing ransomware attacks to contact the FinCEN Financial Institution Hotline at 1-866-556-3974.
- Next, file a SAR using the E-filing System with relevant details available at the time.
- Amended SARs should also be filed to include any additional information learned later. New activity should be filed under a new "initial" SAR filing. Specifically, in SAR field 2 and in the narrative, FinCEN directs the credit union to make a connection to the cyber event.

- Filers are also reminded that SAR field 42 is to be used (Cyber event) as the associated suspicious activity type, as well as SAR field 42z to indicate a connection between the suspicious activity reported and possible ransomware activity.
- For any relevant technical cyber indicators related to ransomware and associated transactions within the available structured cyber event indicator, use SAR fields 44(a)-(j), (z).

As each of us does our part to combat the threat of ransomware, we can all help bring these perpetrators to justice and help keep our members safe.