FINANCIAL CRIMES ENFORCEMENT NETWORK
OFFICE OF CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION
U.S. DEPARTMENT OF THE TREASURY

CTIIN-FIN-2022-0010

July 14, 2022

Cyber Threat Intelligence & Indicators Notice – Snatch Ransomware

TRAFFIC LIGHT PROTOCOL (TLP): AMBER – RECIPIENTS MAY ONLY SHARE **TLP: AMBER** INFORMATION WITH MEMBERS OF THEIR OWN ORGANIZATION, AND WITH CLIENTS OR CUSTOMERS WHO NEED TO KNOW THE INFORMATION TO PROTECT THEMSELVES OR PREVENT FURTHER HARM. THIS REPORT MAY BE SHARED WITH RECIPIENTS' CYBERSECURITY SERVICE PROVIDERS.

Purpose

In the interest of detecting and preventing financial crime, the Financial Crimes Enforcement Network (FinCEN) and the Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) are issuing this Cyber Threat Intelligence & Indicators Notice to provide relevant information on cybercriminal activity and indicators potentially associated with cyber-enabled financial crime.

Cyber Threat Intelligence & Indicators Notices consist of indicators of compromise and relevant information derived from various sources, including U.S. government research and private financial sector reporting. This information is provided "as-is," for informational purposes only. FinCEN and OCCIP do not provide any warranties of any kind regarding any information contained within.

This Cyber Threat Intelligence & Indicators Notice is not intended to, and does not, create any new regulatory obligation or expectation. As a reminder, financial institutions must report suspicious transactions conducted or attempted by, at, or through their institution that involve or aggregate to specific threshold amounts in funds or other assets, including suspicious transactions that are conducted, facilitated, or affected by a cyber event. For more information on mandatory and voluntary reporting of cyber events via suspicious activity reports (SARs), see FinCEN Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016, and FinCEN Advisory FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," November 8, 2021, which updates FinCEN Advisory FIN-2020-A006.

If related or other malicious cyber activity is detected, please notify appropriate law enforcement and other relevant authorities, as appropriate, based on the facts and circumstances of the detected activity.[1]

[1] Additionally, financial institutions should consider contacting Response and Recovery within the U.S. Treasury's Office of Cybersecurity and Critical Infrastructure Protection, available at OCCIP-Coord@treasury.gov.

Summary

This report identifies technical information associated with Snatch ransomware. The Snatch ransomware strain has affected financial sector firms, including firms in the United States, since at least January 2022, according to FinCEN and OCCIP analysis of financial sector ransomware incidents. Cybercriminals have continued to victimize financial sector firms with successful Snatch ransomware attacks in the first quarter of 2022, making Snatch an ongoing cybersecurity concern for the financial sector.

Indicators

Snatch Ransomware Associated Emails:	
RichardSHibbs@seznam[.]cz	edwardwint@tutanota[.]com
funny385@tutanota[.]com	
Snatch Ransomware Associated Malicious Files and Executables:	
safex86[.]exe	VboxUpdate[.]exe
unlocker[.]exe	
Snatch Ransomware Associated MD5, SHA-1, or SHA-256:	
24ff151a091552d7aead4ecf4ee02a22	
3f252a9638a386a644af51dcd155c0d5	
95a22b607cf191d0cc7680b189463a4d	
E10ACDD63DFE0348D00A9757B51E05DA68AF8CF2	
F5CB3A0CCEAECD37E3999A1A1DE46B566812C238	
DA1615E7BDBE908053F25E7E47BE4AEC56872F45	

Identifiers

Snatch Associated Payment Wallets:
bc1qtxlh6r9gmjmsrvrkgyys0s5jv95h697v0z809q
bc1qw95kxhfucmrfvza49p3ps9x4avr7jpypftaepe

Detection & Mitigation Recommendations

Snatch ransomware is a serious cybersecurity concern requiring immediate and advanced mitigation efforts. We encourage the following immediate actions:

1. Incorporate the indicators of compromise identified in this report into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.
2. Contact law enforcement immediately regarding any identified activity related to Snatch ransomware. Please see contact information for FBI, CISA, and U.S. Secret Service at the end of this report.
3. Report suspicious activity according to BSA requirements, highlighting the presence of “Cyber Event Indicators.” Indicators of Compromise, such as suspicious email addresses, file names, hashes, domains, and IP addresses, can be provided under Item 44 of the Suspicious Activity Report (SAR) form.

Further, ransomware is a complex cybersecurity problem requiring a variety of preventative, protective, and preparatory best practices. CISA's StopRansomware.gov offers a one-stop-shop for government resources containing alerts, guides, fact sheets, and training all focused on reducing the risk of

ransomware. CISA and MS-ISAC's Ransomware Guide provides high-level prevention best practices and a response checklist while NIST's Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events offers a comprehensive focus on detailed methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network.

Reporting Suspicious Intrusions

To report an intrusion and request technical assistance, contact CISA at central@cisa.dhs.gov or 888-282-0870, or FBI through a local field office[2] or FBI's Cyber Division at CyWatch@fbi.gov or 855-292-3937, or any of the U.S. Secret Service's local field offices[3] to report a crime.

We want to hear from you on the usefulness of these reports to continuously improve them! Please take a moment to let us know what works and how we can better meet your needs.

The Cyber Threat Intelligence & Indicators Notice is being provided "as-is" for informational purposes only. The Treasury Department does not provide any warranties of any kind regarding any information contained within.

For Further Information

Questions or comments regarding the contents of this Cyber Threat Intelligence & Indicators Notice should be addressed to OCCIP-Coord@treasury.gov.

Financial institutions wanting to report suspicious transactions (including those involving cyber activity) that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

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

[2] https://www.fbi.gov/contact-us/field-offices
[3] https://www.secretservice.gov/contact/field-offices