FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021

Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021: Russia-Related Malware Dominates Ransomware Landscape

This Financial Trend Analysis builds on the previous Financial Crimes Enforcement Network (FinCEN) report, "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," published on 15 October 2021.[1] This report focuses on ransomware pattern and trend information identified in Bank Secrecy Act (BSA) data for the second half of 2021, including links to Russia-related variants. This report is issued pursuant to section 6206 of the Anti-Money Laundering Act of 2020 (AMLA), which requires FinCEN to periodically publish threat pattern and trend information derived from BSA filings.[2] FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy on 30 June 2021, which included cybercrime as a government-wide priority. FinCEN highlighted ransomware as a particularly acute cybercrime concern and issued an updated Advisory on Ransomware, FIN-2021-A004, on 8 November 2021 to reflect information contained in the October 2021 Financial Trend Analysis report. The information contained in this report is relevant to the public, including a wide range of businesses, industries, and critical infrastructure sectors.

Executive Summary: This Financial Trend Analysis covers pertinent ransomware activities for calendar year 2021, focuses on the second half of 2021, and builds on the BSA data underlying FinCEN's October 2021 report.[3] This analysis, which is in response to the increase in number and severity of ransomware attacks against U.S. critical infrastructure since late 2020, addresses the extent to which a substantial number of ransomware attacks likely emanate from, or at a minimum are connected to, actors in Russia.[4][5][6]

1. See FinCEN Financial Trend Analysis "Ransomware in Bank Secrecy Act Data Between January 2021 and June 2021", 15 Oct. 2021, https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.
2. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
3. The data in this report consists of information filed with FinCEN pursuant to the Bank Secrecy Act (BSA), hereinafter referred to as "BSA Data," and is not a complete representation of all ransomware attacks or payments during the review period. Trends represented in this report illustrate identification and reporting of ransomware events and may not reflect the dates actually associated with incidents.
4. This analysis does not include statistics on certain information analyzed in FinCEN's previous Financial Trends Analysis, such as payment method, communication method, filer types, or attacker money laundering typologies as these trends remain largely unchanged
5. FinCEN relied on open source information to determine whether a variant was Russia-related. Indicators include the presence of Russian-language code in the ransomware malware, the malware being coded not to attack targets in Russia or post-Soviet states, or threat actors advertising the ransomware or participation in ransomware-related activities primarily on Russian-language sites.
6. FinCEN analyzed the nexus to Russia in response to various cybersecurity industry reports that link a majority of ransomware attacks to Russia-linked hackers.

FinCEN's analysis of ransomware-related BSA filings for 2021 indicates that ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, businesses, and the public. For example:

Ransomware-related incidents and dollar values, calendar year 2020 vs. 2021: BSA data for 2020 suggests that at least 602 ransomware-related incidents occurred between 1 January 2020 and 31 December 2020. The total value of these incidents was roughly $527 million. BSA data for 2021 suggests that at least 1,251 ransomware-related incidents occurred between 1 January 2021 and 31 December 2021. The total value of these incidents was roughly $886 million.

Ransomware-related incidents and dollar values, calendar year 2021 — First Half vs. Second Half: BSA data for 2021 suggests at least 458 ransomware-related incidents occurred between 1 January 2021 and 30 June 2021. The total value of these incidents was roughly $398 million. At least 793 ransomware-related incidents occurred between 1 July 2021 and 31 December 2021. The total value of these incidents was roughly $488 million.

Ransomware-related activities with a nexus to Russia — 2021, Second Half: Of the 793 ransomware-related incidents reported to FinCEN in BSA data that occurred between 1 July 2021 and 31 December 2021, 75% (or 594) had a nexus to Russia, its proxies, or persons acting on its behalf.[7] [8]

FinCEN's analysis of ransomware-related filings highlights average ransomware-related incident amounts for the second half of 2021, top Russia-related ransomware variants, and total trends for the year:

Russia-related ransomware variants responsible for majority of ransomware activity: Russia-related ransomware variants accounted for 69% of ransomware incident value, 75% of ransomware-related incidents, and 58% of unique ransomware variants reported for incidents in the review period. All of the top five highest grossing ransomware variants in this period are connected to Russian cyber actors.

Average monthly amount of ransomware-related incidents: The mean average total monthly amount of ransomware-related incidents in the review period was $81.4 million, and the median was $80 million.

Top ransomware variants: Ransomware actors develop their own versions of ransomware, known as "variants," and these versions are given new names based on a change to software or to denote a particular threat actor behind the malware. FinCEN identified 84 ransomware variants reported in BSA data for incidents during the review period.

7. The 858 BSA filings during the review period include 793 filings reporting incidents that occurred in the same timeframe. The remaining 65 filings report incidents that occurred prior to July 2021 but were reported to FinCEN between July and December 2021.
8. FinCEN identified numerous filings received between 1 July 2021 and 31 January 2022 that referred to the same ransomware incident as another filing. These filings were categorized as duplicates and excluded from both the incident date and filing date data sets for the purpose of this report. However, filings on the same incident from different financial intermediaries are highly valuable for investigative purposes. Moreover, they illustrate reporting compliance and how many entities involved in the ransomware payment process report the incident to FinCEN.

Scope and methodology: FinCEN examined ransomware-related BSA filings between 1 July 2021 and 31 January 2022 to determine trends. FinCEN uses a cutoff date of 31 January 2022 because filing institutions have 30 days from the discovery of suspicious activity to file a report with FinCEN, therefore some reports filed in January 2022 relate to incidents that occurred in 2021. The full data set consisted of 1,013 filings reporting $750 million in ransomware-related activity.[9] [10] For the purpose of analysis, FinCEN divides BSA data gathered into two data sets: filing date and incident date.

Filing date data: The filing date data set consists of BSA filings sent to FinCEN between 1 July 2021 and 31 December 2021. These reports may refer to incidents that occurred in previous months or years. Of the 1,013 total filings reviewed, 858 were filed between 1 July 2021 and 31 December 2021, with the remainder being filed in January 2022. These 858 filings comprise the filing date data set.[11]

Incident date data: The incident date data set consists of BSA filings sent to FinCEN between 1 July 2021 and 31 January 2022 that pertain to incidents that occurred between 1 July 2021 and 31 December 2021. Of the 1,013 total filings reviewed, 793 report actual incidents that occurred during the review period worth $488 million. These filings comprise the incident date data set.

FinCEN reviewed and verified each filing to remove any amount unrelated to ransomware. FinCEN then combined this data with data previously gathered on ransomware-related filings in the first half of 2021 to generate statistics for the entire year. FinCEN compared data gathered for the whole of 2021 to BSA data gathered in previous years in order to track ransomware trends. This data set consisted of 3,193 BSA filings reflecting roughly $2.31 billion in ransomware-related activity filed between 1 January 2011 and 31 January 2022.

9. Incident date data for 2021 include BSA filings in January 2022 with an incident date in 2021. FinCEN assessed filings between 1 January 2020 and 31 January 2022 for accuracy, duplication, and false positives using both the narrative and the note to FinCEN field on BSA forms. Data from BSA filings between 1 January 2011 and 31 December 2019 reflect reports that contain "ransomware" in the narrative.
10. For the purposes of this report, filings pertaining to the first half of 2021 and 2020 that were submitted after the filing review period were omitted for consistency.
11. Amounts associated with ransomware-related incidents may include extortion amounts, attempted transactions, and payments that were unpaid.

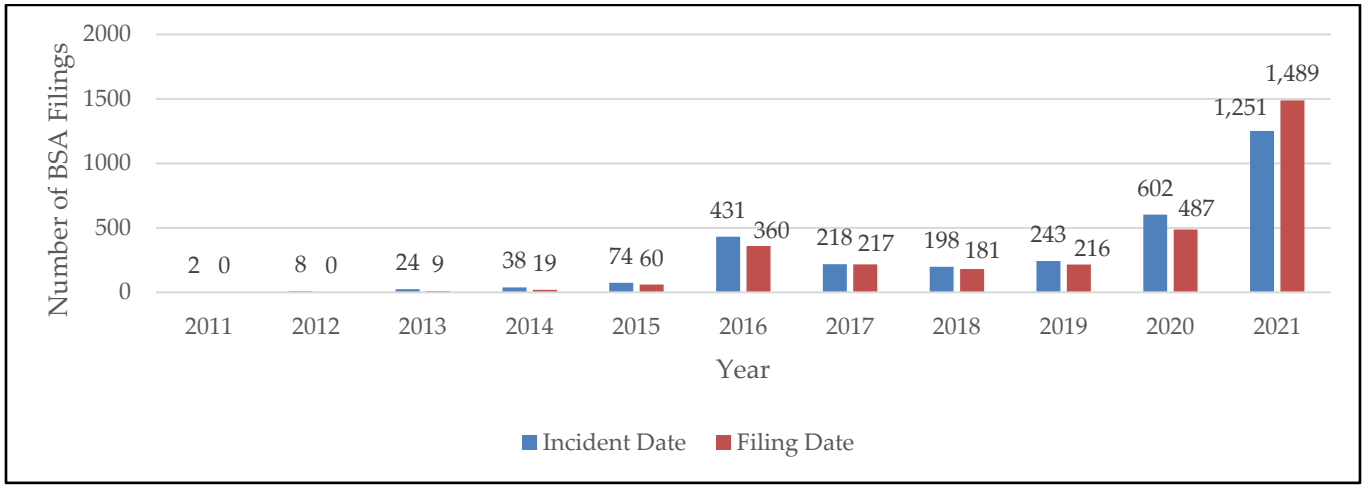
What is Ransomware?

Ransomware is malicious software that encrypts a victim's files and holds the data hostage until a ransom is paid, most often in Bitcoin. In the last two years, ransomware actors have shifted from a high-volume opportunistic approach to a more selective methodology in choosing victims, targeting larger enterprises, and demanding bigger payouts to maximize their return on investment. Some ransomware actors have diversified their revenue streams using a ransomware-as-a-service (RaaS) business model in which ransomware creators sell user-friendly ransomware kits on the dark web or outsource ransomware distribution to affiliates in exchange for a percentage of the ransom. Additionally, since at least late 2019, ransomware groups have adopted new extortion tactics to maximize revenue and create an additional incentive for victims to pay. In one such tactic, known as "double extortion," ransomware operators exfiltrate massive amounts of a victim's data encrypting it and then threaten to publish the stolen data if ransom demands are not met.

Ransomware-Related Filings in 2021 Approach $1.2 Billion

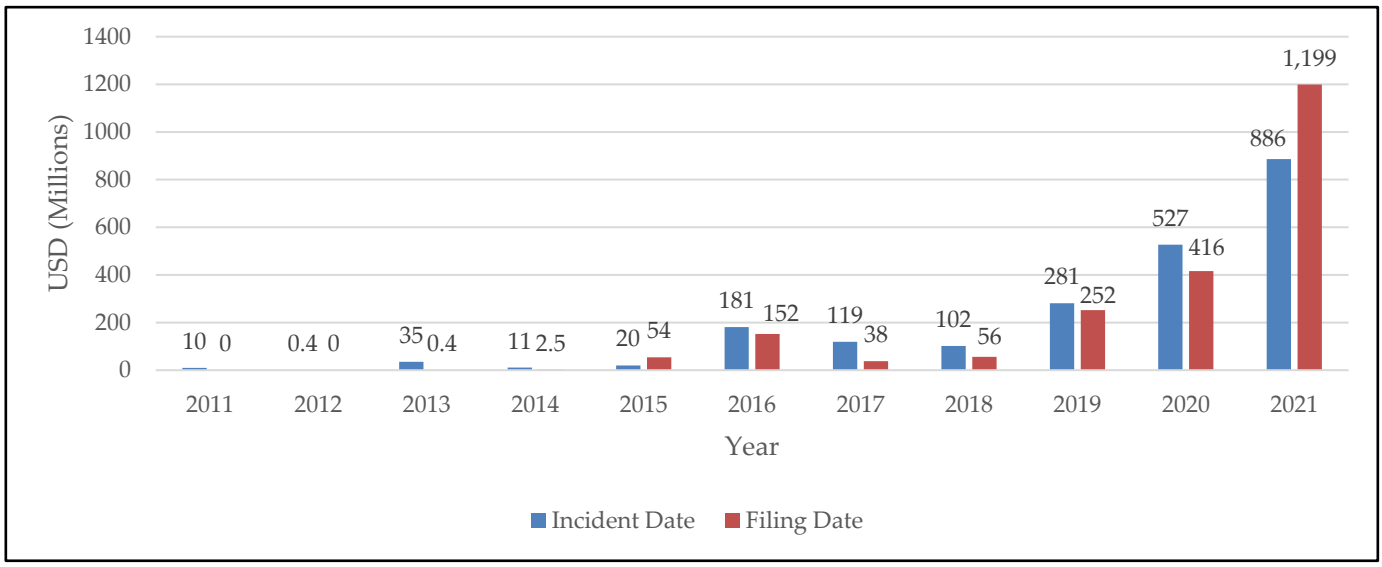
Both the number of and total U.S. dollar value for ransomware-related incidents reported in BSA filings during 2021 far exceeds data for any year. In 2021, FinCEN received 1,489 ransomware-related filings worth nearly $1.2 billion, a 188 percent increase compared to the total of $416 million for 2020 (see Figures 1 and 2). This potentially reflects an increase of ransomware-related incidents or improved reporting and detection.

Figure 1. Number of Ransomware-Related BSA Filings by Filing and Incident Dates, 2011 to 2021[12]



12. Data in Figures 1 and 2 differ slightly between filing date and incident date, as the filing date can denote ransomware events that occurred outside the timeframe covered in this report. Filing date reflects detection and compliance, whereas incident date reflects the actual date of payments or demanded payments associated with ransomware events.

Figure 2. Total Amount from Ransomware-Related BSA Filings and Incidents, 2011 to 2021

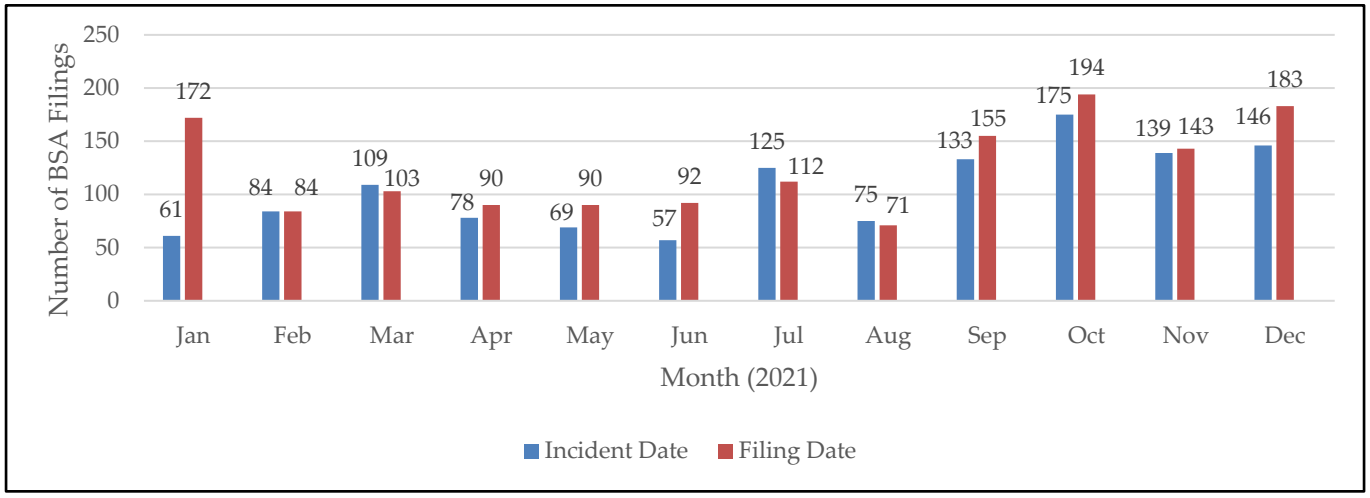


Reported Ransomware-Related Incidents Substantially Increased from 2020

BSA data reports an average of 132 and a median of 136 ransomware-related incidents per month during the review period although significant month-to-month variability was observed across the entire year. During the second half of 2021, FinCEN and Treasury's Office of Foreign Assets Control (OFAC) released ransomware-related advisories and actions that seek to promote reporting of ransomware-related incidents. Treasury's fall 2021 efforts to draw attention to ransomware and potential associated reporting obligations may have contributed to the overall rise in 2021 filings (see Figure 3).[13] [14] [15]

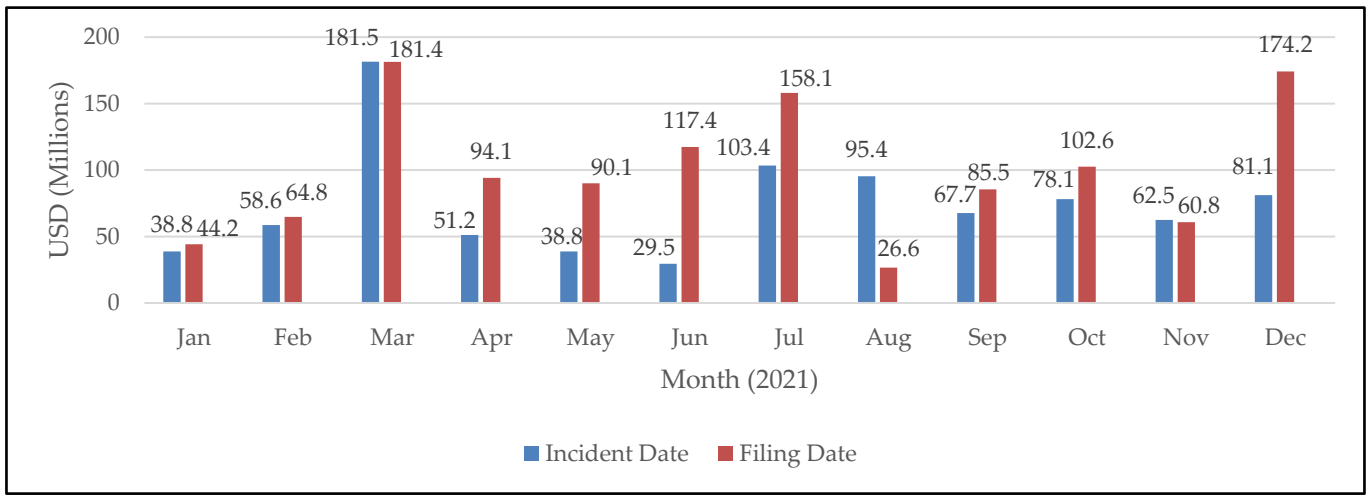
13. For more information see "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," U.S. Department of the Treasury Advisory, 21 Sept. 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.
14. For more information see "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", U.S. Department of Treasury Press Release, 8 Nov. 2021, https://home.treasury.gov/news/press-releases/jy0471.
15. For more information see "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," FinCEN Advisory #FIN-2021-A004, 8 Nov. 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

Figure 3. Number of Ransomware-Related Incidents, January 2021 to December 2021



Ransomware-related incident values during the review period do not differ significantly from the incident values observed in the first half of 2021, with values fluctuating noticeably from month-to-month across the entire year (see Figure 4). The median incident amount for ransomware-related transactions during the review period was $135,000, a slight increase from the median incident amount of $102,273 previously reported for incidents between 1 January 2021 and 30 June 2021, according to BSA data.[16]

Figure 4. Total Amount of Ransomware-Related Incidents, January 2021 to December 2021



16. Ransomware-related payment amounts vary greatly from as little as $1 to as much as $74 million in 2021. To reduce the effect of outliers only the median is reported for this data set. Null values were excluded.

Russia-Related Ransomware Variants Prevalent in Second Half of 2021

Ransomware Variants: Of the 84 unique ransomware variants reported to FinCEN for incidents during the review period, FinCEN identified 49, or roughly 58%, that may be related to suspected Russian cyber actors.[17] While attribution of malware is difficult, these variants were identified in open source information as using Russian-language code, being coded specifically not to attack targets in Russia or post-Soviet states, or as advertising primarily on Russian-language sites. FinCEN assesses that four of the overall top five ransomware variants reported during the review period are connected to Russia, as a result of at least one of these attributes. Of 793 ransomware-related incidents reported to FinCEN during the second half of 2021, 594, or roughly 75%, pertained to Russia-related variants. These variants also make up 69% of the total ransomware-related incident value during the review period, as illustrated in Figure 5.

Figure 5. Russia-Related Ransomware Variants Relative to Total Ransomware Activity Between July 2021 and December 2021

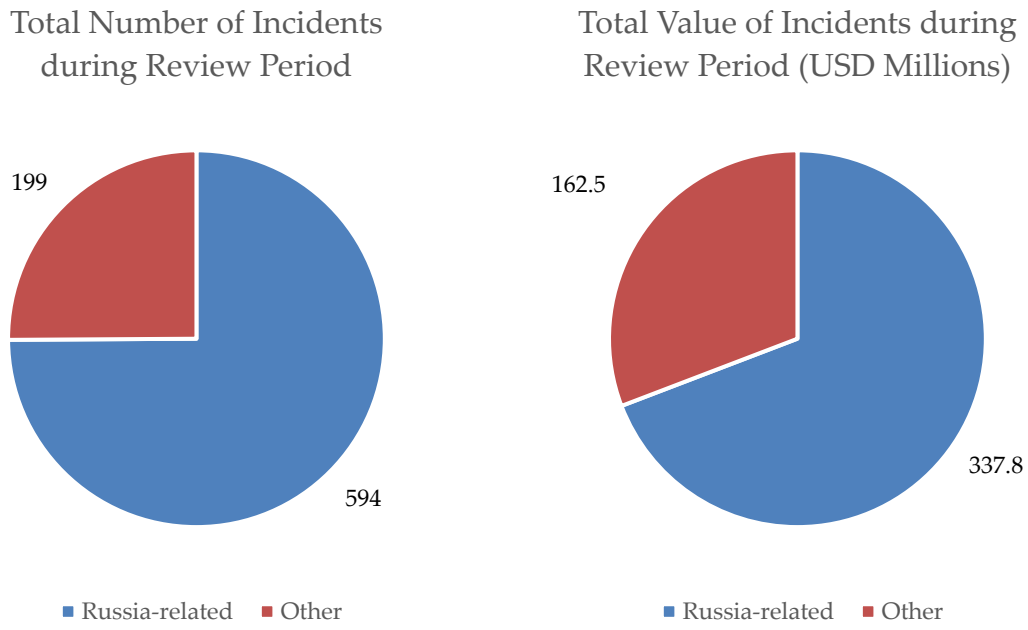


Figure 6 depicts the amounts, number, and value of incidents for the top five Russia-related ransomware variants. These variants alone account for two-thirds of Russia-related ransomware incidents (376 out of 594) and the majority of Russia-related ransomware incident value ($220 million out of $337.8 million).

17. Ransomware groups are known to change and evolve rapidly, therefore many of these 84 variants were not observed in the previous report. A number of ransomware groups ceased operations in 2021, while others began operating only recently.

Figure 6. Russia-Related Ransomware Variants by Number and Value of Incidents with Incident Dates between July 2021 and December 2021

Ransomware Variant	Number of Incidents	Total Dollar Value of Incidents	Median Incident Value[18]
Variant 1	124	~$84.2 million	~$300,000
Variant 2	117	~$22.8 million	~$40,000
Variant 3	53	~$73.7 million	~$160,000
Variant 4	46	~$37.6 million	~$400,000
Variant 5	36	~$1.2 million	~$10,000
Total	**376**	**~$219.5 million**	**~$149,000**

Ransomware Detection, Mitigation, and Reporting

Financial institutions play an important role in protecting the U.S. financial system from ransomware- related threats through compliance with BSA obligations. Financial institutions should determine if a suspicious activity report (SAR) filing is required or appropriate when dealing with a ransomware incident, including ransomware-related payments made by financial institutions that are victims of ransomware.[19] [20] Financial institutions may also file with FinCEN a report of any suspicious transaction it believes relates to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X.

Detection and Mitigation Recommendations

Ransomware is a serious cybersecurity and illicit finance concern for which FinCEN recommends the following actions:

1. Incorporate indicators of compromise (IOCs) from threat data sources 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 ransomware, and contact OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[21] Please see contact information for the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), OFAC, and U.S. Secret Service at the end of this report.

18. To reduce the effect of outliers only the median is reported for this data set. Null values were excluded.
19. For more information see "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," FinCEN Advisory #FIN-2021-A004, 8 Nov. 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508.pdf.
20. For more information see "FinCEN Combats Ransomware", https://www.fincen.gov/fincen-combats-ransomware.
21. For more information see "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," U.S. Department of the Treasury Advisory, 21 Sept. 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

3. Promptly report suspicious activity to FinCEN, highlighting the presence of "Cyber Event Indicators." IOCs, such as suspicious email addresses, file names, hashes, domains, and IP addresses, can be provided in the SAR form. Information regarding ransomware variants, requested methods of payment, or other information may also be useful to law enforcement and for trend analysis in addition to virtual currency addresses and transaction hashes associated with ransomware payments.
4. Review financial red flag indicators of ransomware in the "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" issued by FinCEN in November 2021.[22]

Further, ransomware is a complex cybersecurity problem requiring a variety of preventive, 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 the Multi-State Information Sharing and Analysis Center's (MS-ISAC's) Ransomware Guide provides high-level prevention best practices and a response checklist while the National Institute of Standards and Technology's (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 Cyber Activity

To report a ransomware incident, contact CISA at report@cisa.gov, (888)282-0870 or www.cisa.gov/stopransomware, your local FBI or U.S. Secret Service field office, or the FBI's Internet Crime Complaint Center (IC3) www.ic3.gov. Contact OFAC at ofac_feedback@treasury.gov if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus. For formal guidance to financial institutions on reporting ransomware-related incidents, please refer to FinCEN's resource page on advisories, at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets.

The information in this report is based on ransomware-related information obtained from analysis of BSA data, trade publications, and commercial reporting, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.

22. For more information see "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," FinCEN Advisory #FIN-2021-A004, 8 Nov. 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf