FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024

December 2025

Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024

This Financial Trend Analysis (FTA) focuses on ransomware patterns and trends identified in Bank Secrecy Act (BSA) data. The Financial Crimes Enforcement Network (FinCEN) is issuing this report pursuant to section 6206 of the Anti-Money Laundering Act of 2020 (codified at 31 U.S.C. § 5318(g)(6)(B)), which requires periodic publication of BSA-derived threat pattern and trend information.[1] *FinCEN has issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy, including, as a government-wide priority, cybercrime.*[2] *FinCEN has also previously highlighted ransomware as a particularly acute cybercrime concern.*

The information contained in this report is relevant to the public, including a wide range of businesses, industries, and critical infrastructure sectors. The report also highlights the value of BSA information filed by regulated financial institutions.

Executive Summary: This FTA provides threat pattern and trend information regarding ransomware incidents based on BSA data filed with FinCEN between 1 January 2022 and 1 February 2025 reporting ransomware-related incidents that occurred between 1 January 2022 and 31 December 2024 (the review period).[3] During the three year review period, FinCEN received 7,395 BSA reports related to 4,194 ransomware incidents totaling more than $2.1 billion in ransomware payments.[4] During the previous nine year period—from 2013 through the end of 2021—FinCEN received 3,075 BSA reports totaling approximately $2.4 billion in ransomware payments. Ransomware incidents and payments reached an all-time high in 2023—at 1,512 incidents, totaling approximately $1.1 billion in payments—an increase of 77 percent in total payments year-over-year from 2022 to 2023. In 2024, incidents decreased slightly to 1,476 while total payments were approximately $734 million. Overall, the trend in the number of incidents and payments varied throughout the review period.

[1] The Anti-Money Laundering Act of 2020 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).

[2] *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," 30 June 2021, https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[3] Ransomware is a form of malicious software (malware) designed to gain access to a computer system or data to extort ransom payments from victims in exchange for restoring victims' access to their systems or data or not leaking exfiltrated data to other cyber criminals.

[4] Trends represented in this report illustrate financial institutions' identification and reporting of ransomware events and may not reflect the actual dates associated with ransomware incidents. FinCEN's analysis of ransomware-related BSA reports highlights median ransomware payment amounts, top ransomware variants, and insights from FinCEN's blockchain and open-source analysis. Both actual and attempted transactions are included as part of this analysis.

FinCEN also identified common malicious cyber facilitators and money laundering typologies used by threat actors during ransomware incidents. Previous FinCEN Financial Trend Analyses of ransomware have focused on reported ransomware payments and incidents by the date the activity was filed with FinCEN.[5] This report shifts the focus to the reported incident date of each ransomware attack to provide further detail on the activities conducted by ransomware actors.

Overview of Key Findings:

Reported Ransomware Incidents and Payments Reach All-Time High in 2023: In 2023, the value of reported ransomware payments reached an all-time high, totaling approximately $1.1 billion, marking a 77 percent increase in aggregate payment value year-over-year from 2022 to 2023. In 2023, the number of reported incidents reached an all-time high of 1,512.[6] In 2024, there were 1,476 reported ransomware incidents, and approximately $734 million in reported ransomware payments in BSA reports. The value of all reported ransomware payments in 2024 reached the third-highest yearly total since the first ransomware-related reports began in 2013. In 2022, the number of reported ransomware incidents and the number of reported payments declined after reaching the previous all-time high marks in both incidents and payments in 2021.

Median Ransomware Payment Varied Over Reporting Period: The median amount of a single ransomware transaction was $124,097 in 2022; $175,000 in 2023; and $155,257 in 2024. Between January 2022 and December 2024, the most common payment range was below $250,000.

Financial Services, Manufacturing, and Healthcare Most Affected Industries: By measures of both the most incidents and highest amount of aggregate payments sent to ransomware actors, the financial services, manufacturing, and healthcare industries were the most affected during the review period.

Of the 267 Ransomware Variants Identified, ALPHV/BlackCat Most Prevalent: FinCEN identified 267 unique ransomware variants reported in BSA data during the review period.[7] The most reported variants were Akira, ALPHV/BlackCat, LockBit, Phobos, and Black Basta.

The Onion Router (TOR) Most Common Communication Method: Roughly 42 percent of BSA reports indicated the method that ransomware threat actors used to communicate with their targets. Among these BSA reports, 67 percent of the reports indicated ransomware actors used TOR, and 28 percent of reports indicated that ransomware actors used email to communicate with their targets.[8]

[5] *See* FinCEN, Financial Trend Analysis, "Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021," 1 November 2022, https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

[6] *See* FinCEN, Financial Trend Analysis, "Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021," 1 November 2022, https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

[7] Ransomware actors develop specific versions of ransomware, known as "variants," and these versions are given new names based on software adjustments or to denote a particular threat actor behind the malware.

[8] According to the Cybersecurity and Infrastructure Security Agency (CISA), TOR uses software and network infrastructure "that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes." CISA, "Defending Against Malicious Cyber Activity Originating from Tor," 2 August 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a.

Bitcoin Used Most Frequently for Reported Ransomware Payments: FinCEN identified Bitcoin (BTC) as the most common ransomware-related payment method, accounting for 97 percent of reported transactions. Monero (XMR) was cited in two percent of BSA reports involving ransomware.

FinCEN Identified Ransomware Money Laundering Typologies: FinCEN identified several common money laundering typologies used by threat actors during ransomware incidents. For example, threat actors overwhelmingly collected payments in unhosted convertible virtual currency (CVC)[9] wallets and continued to exploit CVC exchanges for money laundering purposes after receiving payment. Different ransomware threat actors also continued to use several common preferred malicious cyber facilitators, such as shared initial access vendors.[10]

[9] *See* FinCEN, Guidance, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," 9 May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (discussing the meaning of CVC).

[10] An initial access vendor is a cyber actor that identified a persistent method of entrance into a targeted victim network. The vendor then sells that persistent "access" to other illicit cyber actors, such as a ransomware operator.

Scope and Methodology: For the purposes of this report, FinCEN analyzed BSA reports that reference variations of "ransomware," as a key term, and that were submitted to FinCEN between 1 January 2022 and 1 February 2025 to identify trends and patterns in ransomware activity. The full data set consisted of 7,395 BSA reports involving potentially ransomware-related incidents that occurred between the review period of 1 January 2022 and 31 December 2024.[11] [12] [13]

FinCEN reviewed and verified each filing to remove any values unrelated to ransomware and assessed ransomware reports for accuracy, duplication, and false positives. FinCEN compared data gathered for the review period to earlier data to track ransomware trends. The earlier data set consisted of 3,038 BSA reports reflecting approximately $1.56 billion in suspicious ransomware-related activity related to incidents reported to have occurred between 1 January 2013 and 31 December 2021.[14]

A Note About BSA Data

BSA reporting reflects only suspicious activity that has been identified and reported, and therefore should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, and transfers between accounts. The reported suspicious activity in any individual BSA filing may include both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity, and therefore may reflect cumulative transactions from a single filer involving the same subject.

[11] As previously noted, while prior FinCEN Financial Trend Analyses on ransomware have focused on reported ransomware payments and incidents by the date the BSA form was filed with FinCEN, this report shifts the focus to the reported date that an incident first occurred.

[12] The data set includes 176 BSA reports involving ransomware-related incidents in which the affected entity did not make a payment to the ransomware actor.

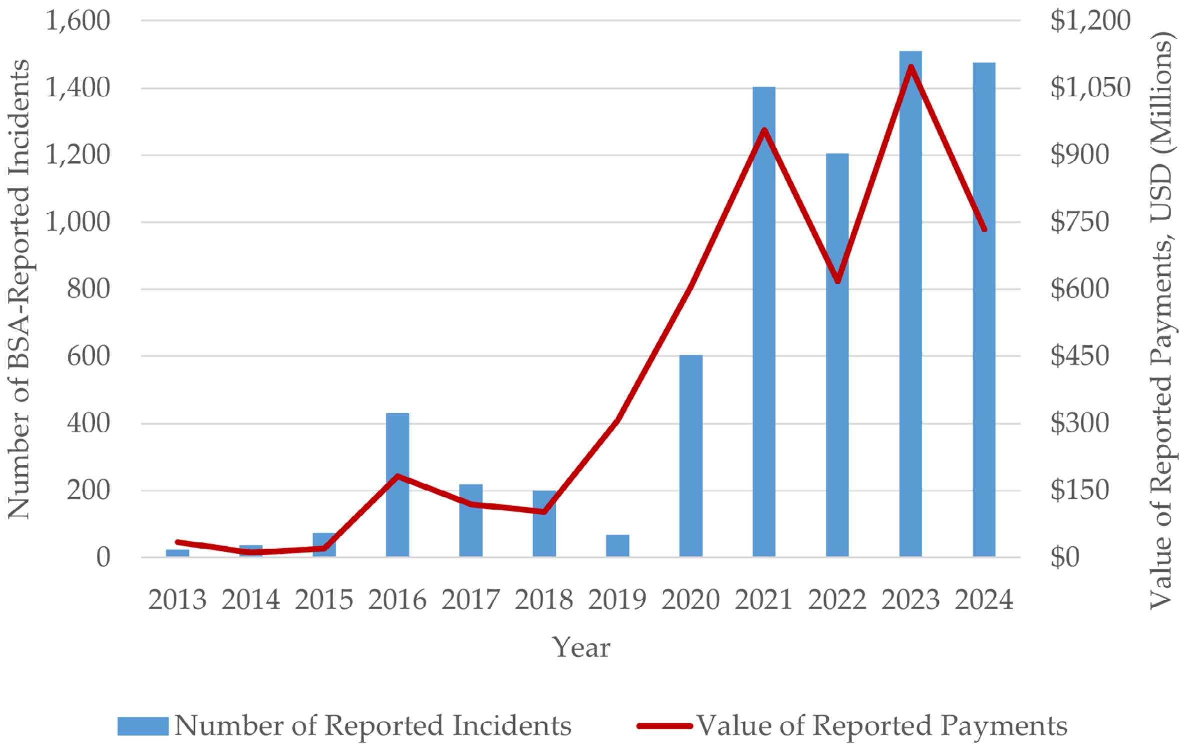
[13] The data in this report consists only of information received through BSA reporting and is not a complete representation of all ransomware attacks or payments during the review period.

[14] *See* FinCEN, Financial Trend Analysis, "Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021," 1 November 2022, https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

Reported Ransomware Incidents and Payments Reached All-Time High in 2023, Total Payments Dip in 2024

According to FinCEN analysis of ransomware-related BSA data reporting incidents that occurred between January 2022 and December 2024, ransomware activity remains a threat to the U.S. public, including the financial services industry and other industries. In 2023, the value of reported ransomware payments reached an all-time high value of approximately $1.1 billion, marking an increase of 77 percent in total value of payments year-over-year from 2022 to 2023. However, following U.S. federal law enforcement disruption of the ALPHV/Blackcat ransomware group in December 2023[15] and U.S. and UK authorities disruption of the LockBit ransomware group in February 2024,[16] total reported ransomware incidents fell in 2024, with 1,476 incidents and a reported $734 million in ransomware payments, reflecting a significant decrease in the aggregate value of reported payments in BSA reports from the previous year (*see* Figures 1 and 2).

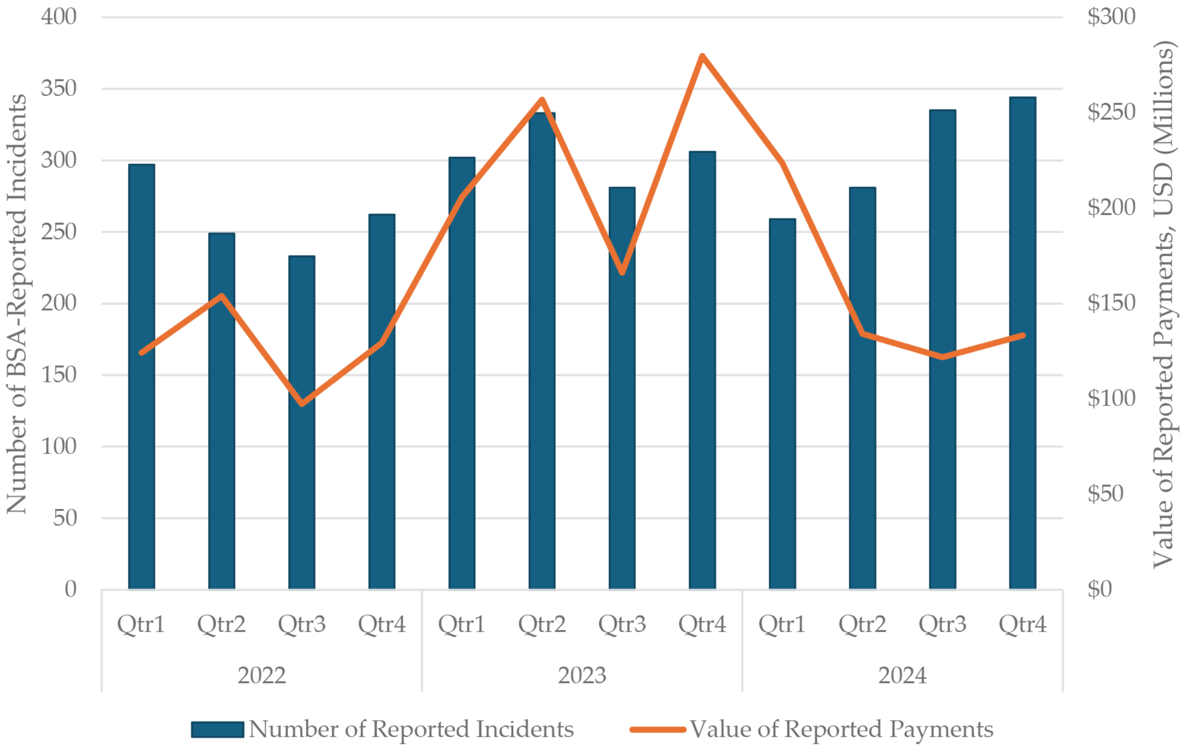
Figure 1. Total Suspicious Incidents and Amounts from Ransomware-Related BSA Reporting, 2013 to 2024



[15] *See* U.S. Department of Justice, Press Release, "Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware variant," 19 December 2023, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

[16] *See* U.S. Department of Justice, Press Release, "U.S. and U.K. Disrupt LockBit Ransomware Variant," 20 February 2024, https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

Figure 2. Quarterly Suspicious Incidents and Amounts from Ransomware-Related BSA Reporting, 2022 to 2024

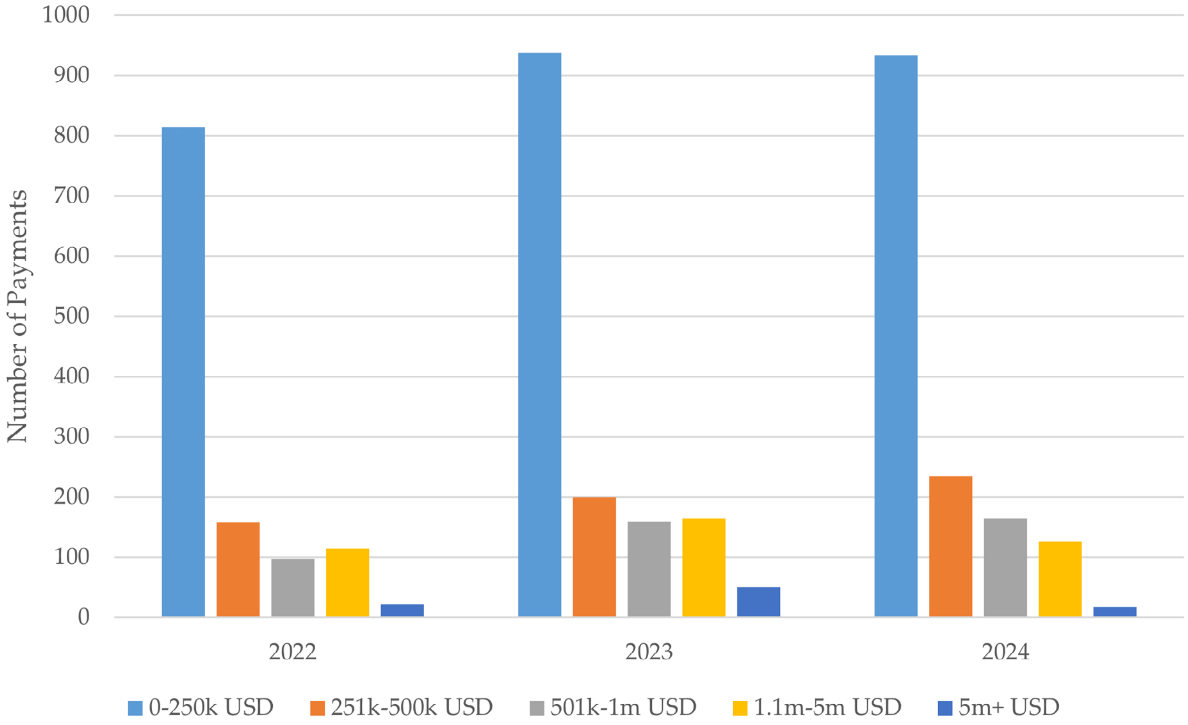


The number of ransomware-related BSA reports and the value of reported payments declined in 2022 after reaching previous all-time high marks in 2021. However, after a 14 percent decrease in reported incidents from 1,403 to 1,206 between 2021 and 2022, the total number of incidents increased by 25 percent from 1,206 incidents in 2022 to 1,512 in 2023. In 2024, the total number of incidents decreased incrementally (two percent) from 1,512 in 2023 to 1,476 in 2024 (*see* Figure 1).

Most Common Payment Range for Ransomware Payments Was Below $250,000

Between January 2022 and December 2024, the most common payment range was below $250,000 (*see* Figure 3). The median value of a single ransomware transaction was $124,097 in 2022. This value increased by 41 percent to $175,000 in 2023. The median value of a ransomware transaction then decreased by 11 percent to $155,257 in 2024.

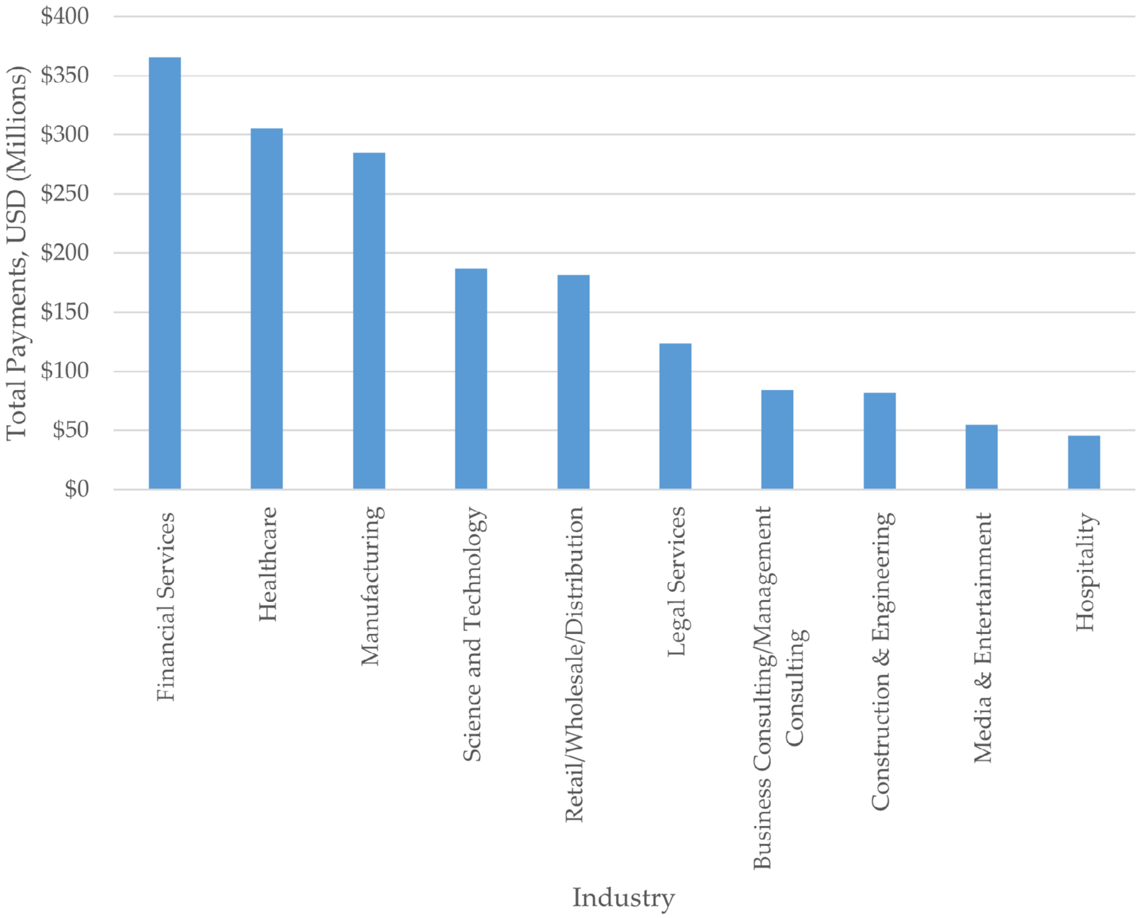
Figure 3. Ransomware-Related Payment Range by Year, January 2022 to December 2024



Financial Services, Manufacturing, and Healthcare Most Affected Industries

Between January 2022 and December 2024, the most commonly targeted industries (by number of incidents identified in ransomware-related BSA reports during the review period) were manufacturing (456 incidents), financial services (432 incidents), healthcare (389 incidents), retail (337 incidents), and legal services (334 incidents). The most affected industries by the total amount of ransom paid during the review period were financial services (approximately $365.6 million), healthcare (approximately $305.4 million), manufacturing (approximately $284.6 million), science and technology (approximately $186.7 million), and retail (approximately $181.3 million) (*see* Figure 4). By both measures, financial services, manufacturing, and healthcare were the most affected industries by ransomware during the review period.

Figure 4. Top 10 Industry Total Payments in Ransomware Incidents, January 2022 to December 2024



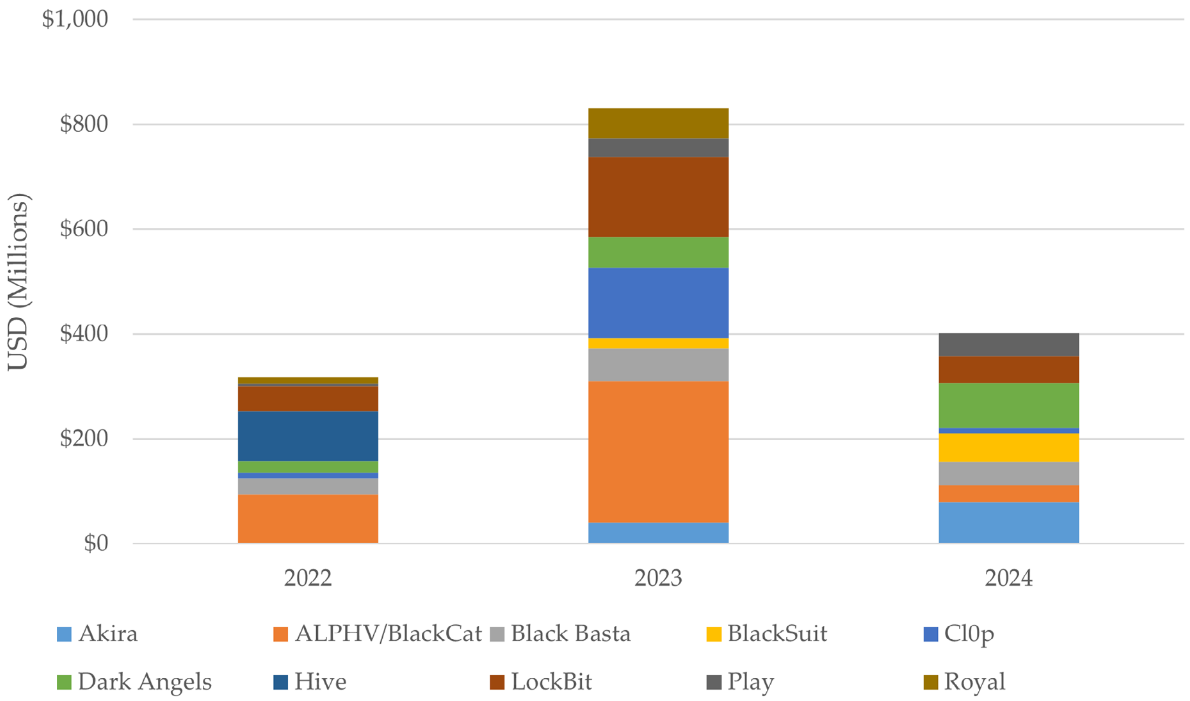
Over 200 Ransomware Variants Identified; ALPHV/BlackCat Most Prevalent and Impactful

FinCEN identified 267 ransomware variants reported in BSA data during the review period. Ransomware variant analysis can help determine the threat actors potentially behind an attack.[17] Figures 5, 6, and 7 depict the total payment values, number of incidents, and median value of transactions for the 10 ransomware variants with the highest payment amounts and highest number of incidents in BSA data during the review period.

[17] Some BSA reports detailed multiple incidents involving more than one variant, and 429 BSA reports did not name the ransomware variant used in the attack.

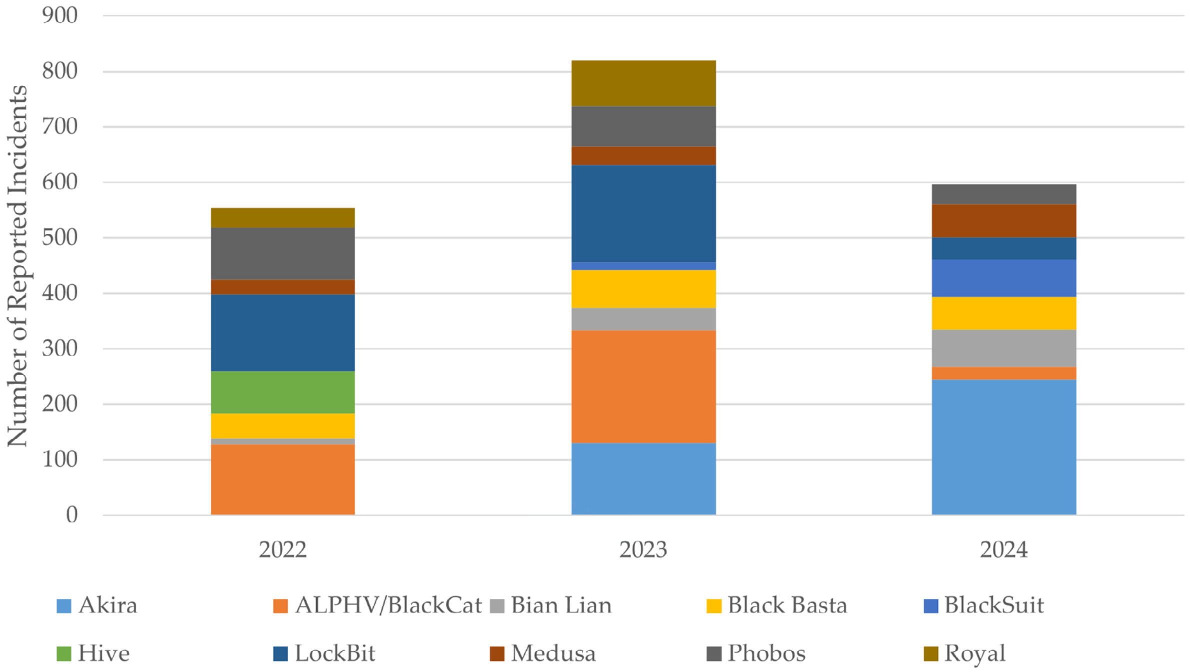
The 10 variants with the highest cumulative payment amounts identified in BSA reports accounted for approximately $1.5 billion in suspicious activity during the review period (*see* Figure 5). The total payment amounts received for these individual variants range from approximately $69.8 million to $395.3 million, according to BSA data during the review period. Monthly suspicious payment amounts for the top 10 variants range from approximately $1.9 to $10.9 million. The highest cumulative suspicious payment amounts were associated with ALPHV/BlackCat (approximately $395.3 million) and LockBit (approximately $252.4 million), according to BSA reports filed with FinCEN during the review period.

Figure 5. Top Ransomware Variants by Payment Value, January 2022 to December 2024



FinCEN identified 1,969 BSA reports filed on the top 10 most frequently reported variants with transaction dates during the review period (*see* Figure 6). These BSA reports most frequently report Akira (376 reports), followed by ALPHV/BlackCat and LockBit (each with 353 reports).

Figure 6. Top Ransomware Variants by Number of Incidents, January 2022 to December 2024



Akira had the highest number of incidents (376) and ALPHV/BlackCat had the highest total dollar value of transactions (approximately $395.3 million) during the review period, according to FinCEN's analysis of reported ransomware-related transactions (*see* Figure 7).

Figure 7. Ransomware Variants by Number of Incidents with Transaction Dates Between January 2022 and December 2024

Ransomware Variant	Number of Incidents	Total Dollar Value of Incidents	Median Incident Value[18]
Akira	376	~$120.9 million	~$160,000
ALPHV/BlackCat	353	~$395.3 million	~$258,896
LockBit	353	~$252.4 million	~$156,880
Phobos	202	~$13.3 million	~$32,500
Black Basta	171	~$137.7 million	~$350,000
Medusa	120	~$23.5 million	~$80,000
Bian Lian	119	~$39.3 million	~$200,000
Royal	117	~$69.8 million	~$265,043
BlackSuit	81	~$73.2 million	~$200,000
Hive	77	~$96.3 million	~$411,283

[18] To reduce the effect of outliers only the median is reported for this table.

Reported Communication Most Commonly Conducted via The Onion Router and Email Systems

BSA ransomware reports included information on the communication method used by ransomware attackers in 42 percent of the incidents during the review period. Of the methods mentioned in BSA reports, ransomware threat actors most often communicated with their intended ransomware targets via messages sent over TOR protocol (67 percent of reported communications channels), email (28 percent), or through other private encrypted messaging systems (three percent). When using TOR, the targets of ransomware incidents, or their representatives, primarily engaged with threat actors using messages exchanged over a ".onion" website provided by the attackers to negotiate the ransomware-related payment, according to BSA data (*see* Figure 8). After negotiating the ransom amount, the negotiating firm or target made payment in exchange for decryption keys. Some threat actors demanded further negotiation even after initial payments were made, often escalating payment demands.

Figure 8. Ransomware-Related Payments by Communication Method, January 2022 to December 2024

Communication Method	Number of Incidents	Value of Payments
TOR	1,248	~$849.4 million
Email	523	~$164.8 million
Encrypted Messenger Applications	63	~$18.1 million
Text File	5	~$41,000
Embedded Message in Blockchain	1	~$1,000
Unknown Communication	2,436	~$1.4 billion

Note: The communication methods reflected above in Figure 8 are not mutually exclusive; in some cases, communications were conducted across multiple methods.

Majority of Reported Ransomware-Related Payments in Bitcoin (BTC)

While there are thousands of CVCs in the market, BSA ransomware data only indicated attackers requesting BTC, XMR, Ether (ETH), Litecoin (LTC), and Tether (USDT) on the Ethereum blockchain as methods for ransomware-related payment during the review period. BTC was, overwhelmingly, the most common ransomware-related payment method used in transactions reported to FinCEN, with most reported payments made in BTC (*see* Figure 9).[19] [20]

[19] As noted in FinCEN's 2021 Advisory on Ransomware, cybercriminals usually require ransomware payments to be transmitted in CVCs, most commonly in BTC. *See* FinCEN, Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," 8 November 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[20] An additional 387 BSA reports did not identify a specific CVC address. A further 206 reported payments were identified conducted in BTC without providing details of the transaction, and seven reported payments in XMR without providing details of the transaction.

Figure 9. BSA-Reported Ransomware-Related Payments by Convertible Virtual Currency, January 2022 to December 2024

Convertible Virtual Currency	Number of Reported Payments	Value of Total Reported Payments (USD)[21]
Bitcoin	3,489	~$2.0 billion
Monero	55	~$25.8 million
Ether	4	$196,350
Litecoin	2	$82,687
Tether on Ethereum	1	$125,000

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. According to FinCEN's 2021 "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," "[f]inancial 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."[22] 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 may not be required by 31 CFR Chapter X.

Detection and Mitigation Recommendations

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

1. Incorporate into intrusion detection systems and security alert systems Indicators of Compromise (IOCs) from threat data sources to enable active blocking or reporting of suspected malicious activity.

2. Contact law enforcement immediately regarding any ransomware-related activity and contact OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be a Specially Designated National (SDN) or otherwise have a sanctions nexus.[23] Please see contact information for the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Secret Service, and OFAC at the end of this report.

[21] Not all reported incidents included a reference to the specific means of payment.

[22] *See* FinCEN, Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," 8 November 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[23] *See* U.S. Department of the Treasury, Advisory "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," 21 September 2021, https://ofac.treasury.gov/media/912981/download?inline.

3. 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 BSA reporting form. Information regarding ransomware variants, anonymity enhancing CVCs (AEC) requested for 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.[24] FinCEN requests that all financial institutions include the key term "CYBER-FIN-2021-A004" to indicate a connection between the suspicious activity being reported and ransomware-related activity.[25]

4. Review and incorporate into AML/CFT programs 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.[26]

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, FBI, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and NSA'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.

[24] *See* FinCEN, Advisory, FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," 25 October 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

[25] *See* FinCEN, Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," 8 November 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[26] *See* FinCEN, Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," 8 November 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

Reporting Suspicious Cyber Activity

To report an intrusion and request technical assistance, contact CISA at cisaservicedesk@cisa.dhs.gov or 888-282-0870, or FBI through a local field office or FBI's Cyber Division at CyWatch@fbi.gov or 855-292-3937, or any U.S. Secret Service local field offices to report a crime. Contact OFAC at ofac_feedback@treasury.gov if there is any reason to suspect the cyber actor demanding ransomware payment may be a Specially Designated National or otherwise have a sanctions nexus. For additional resources regarding ransomware incidents, please refer to FinCEN's resource page on ransomware, at https://www.fincen.gov/resources/fincen-combats-ransomware.

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 https://fincen.gov/contact.