FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

This Financial Trend Analysis focuses on ransomware pattern and trend information identified in Bank Secrecy Act (BSA) data. This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 (AMLA) which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish threat pattern and trend information derived from financial institutions' Suspicious Activity Reports (SARs).[1] 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. 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 Financial Trend Analysis is in response to the increase in number and severity of ransomware attacks against U.S. critical infrastructure since late 2020. For example, in May 2021, hackers used a ransomware attack to extort a multi-million dollar ransom, which also disrupted the Colonial Pipeline and caused gasoline shortages. Other recent attacks have targeted various sectors, including manufacturing, legal, insurance, health care, energy, education, and the food supply chain in the United States and across the globe. As Treasury Secretary Janet L. Yellen recently noted, "Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy."[2]

FinCEN analysis of ransomware-related SARs filed during the first half of 2021 indicates that ransomware is an increasing threat to the U.S. financial sector, businesses, and the public. The number of ransomware-related SARs filed monthly has grown rapidly, with 635 SARs filed and 458 transactions reported between 1 January 2021 and 30 June 2021 ("the review period"), up 30 percent from the total of 487 SARs filed for the entire 2020 calendar year.[3] The total value of suspicious activity reported in ransomware-related SARs during the first six months of 2021 was $590 million, which exceeds the value reported for the entirety of 2020 ($416 million).

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 SARs highlights average ransomware payment amounts, top ransomware variants, and insights from FinCEN's blockchain analysis:

1. 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).
2. "Treasury Takes Robust Actions to Counter Ransomware," U.S. Department of the Treasury, 21 Sept. 2021, https://home.treasury.gov/news/press-releases/jy0364.
3. The 635 SARs filed during the review period include 458 SARs reporting transactions that occurred in the same timeframe. The remaining 177 SARs report transactions that occurred prior to 2021.

Average Monthly Suspicious Amount of Ransomware Transactions: According to data generated from ransomware-related SARs, the mean average total monthly suspicious amount of ransomware transactions was $66.4 million and the median average was $45 million. FinCEN identified bitcoin (BTC) as the most common ransomware-related payment method in reported transactions.

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 68 ransomware variants reported in SAR data for transactions during the review period. The most commonly reported variants were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos.

Insights from Blockchain Analysis: FinCEN identified and analyzed 177 unique convertible virtual currency (CVC) wallet addresses used for ransomware-related payments associated with the 10 most commonly reported ransomware variants in SARs during the review period.[4] Based on blockchain analysis of identifiable transactions with the 177 CVC wallet addresses, FinCEN identified approximately $5.2 billion in outgoing BTC transactions potentially tied to ransomware payments.

FinCEN Identified Ransomware Money Laundering Typologies: FinCEN identified several money laundering typologies common among ransomware variants in 2021 including threat actors increasingly requesting payments in Anonymity-enhanced Cryptocurrencies (AECs) and avoiding reusing wallet addresses, "chain hopping" and cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds.

Scope and Methodology: FinCEN examined ransomware-related SARs filed between 1 January 2021 and 30 June 2021 to determine trends. The full data set consisted of 635 SARs reporting $590 million in suspicious activity. Of the 635 SARs filed during the review period, 458 report actual transactions that occurred during the review period worth $398 million. The remaining 177 SARs report transactions that occurred before 1 January 2021.[5] FinCEN reviewed and verified each SAR to remove any suspicious activity amount unrelated to ransomware and to extract relevant indicators of compromise (IOCs).[6] From this data, FinCEN identified the top 10 most common ransomware variants and analyzed their IOCs through commercially available analytics tools. This analysis allowed FinCEN to chart the flow of ransomware payments in BTC to identify which CVC exchanges and services ransomware actors used to launder their proceeds. USD figures cited in this analysis are based on the value of BTC when the transactions occurred. FinCEN also compared data gathered for 2021 to SAR data gathered in previous years in order to track ransomware trends. This data set consisted of 2,184 SARs reflecting $1.56 billion in suspicious activity filed between 1 January 2011 and 30 June 2021.

4. CVC wallet addresses are alphanumeric public keys that store value and can be accessed using a password or "private key." Wallets are software used to organize multiple wallet addresses and their associate private keys.
5. 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.
6. IOCs are signatures or artifacts observed on a network that likely indicate computer or network intrusion.

What is Ransomware?

Ransomware is malicious software that encrypts a victim's files and holds the data hostage until a ransom is paid. 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. This lowers the technical expertise needed to carry out an attack. The transition to remote and online work in response to COVID-19 has also exacerbated risks and vulnerabilities of businesses to cyber attacks such as ransomware. Attacks on small municipalities and healthcare organizations have also increased, typically due to perceived weaker security controls and higher propensity of these victims to pay the ransom because of the criticality of their services, particularly during a global health pandemic. 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.[7] Lastly, ransomware attackers are finding new ways to obfuscate their identities by requesting payment in AECs.[8]

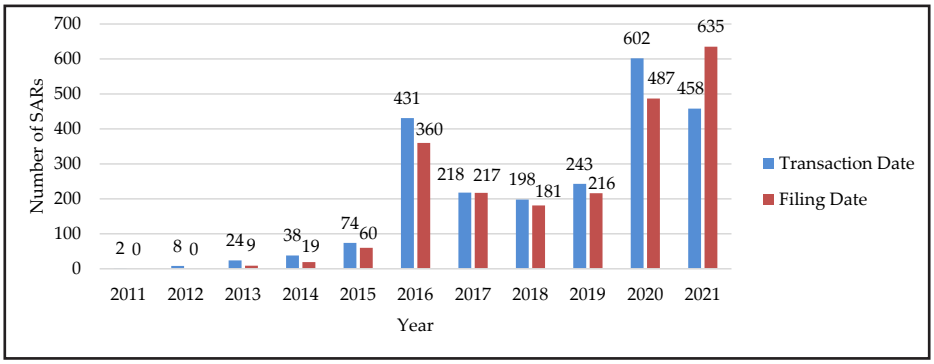
Ransomware Filings in First Six Months of 2021 Exceed 2020 Total

The total U.S. dollar value for ransomware-related transactions reported in SARs filed during the review period exceeds that of any previous year since 2011. In the first six months of 2021, FinCEN identified $590 million in ransomware-related SARs, a 42 percent increase compared to a total of $416 million for all of 2020 (see Figures 1 and 2).[9] [10] If current trends continue, SARs filed in 2021 are projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined, which would represent a continuing trend of substantial increases in reported year-over-year ransomware activity. This trend potentially reflects the increasing overall prevalence of ransomware-related incidents as well as improved detection and reporting of incidents by covered financial institutions, which may also be related to increased awareness of reporting obligations pertaining to ransomware and willingness to report.

7. "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," FinCEN Advisory #FIN-2020-A006, 1 Oct. 2020, https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory Ransomware FINAL 508.pdf.
8. As noted in FinCEN's 2020 Advisory on Ransomware, AECs reduce the transparency of CVC financial flows, including ransomware payments, through anonymizing features, such as mixing and cryptographic enhancements.
9. Data in Figures 1 and 2 differ slightly between filing date and transaction date, as the filing date can denote ransomware events that occurred outside the timeframe covered in this report. Filing date reflects financial institutions' detection and compliance, whereas transaction date reflects the actual date of payments associated with incidents.
10. This includes ransomware-related transactions reported in SARs and does not include additional ransomware-related transactions identified by FinCEN's blockchain analysis.

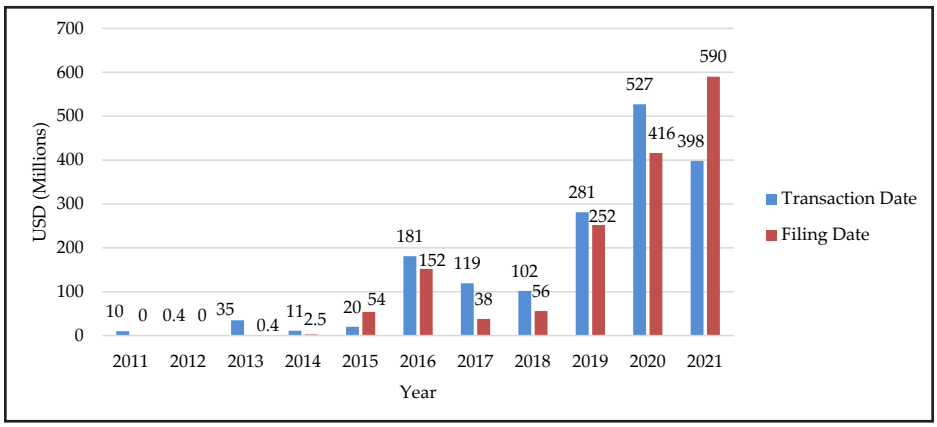
FinCEN and Treasury's Office of Foreign Assets Control (OFAC) have released ransomware-related advisories that, among other things, seek to promote reporting of ransomware-related incidents.[11] [12] [13] In the same month, the G7 released a ransomware annex to a statement on digital assets that emphasized the importance of implementation of international anti-money laundering and countering the financing of terrorism standards to counter ransomware-related money laundering.[14] Following the publication of these advisories, on 12 November 2020, FinCEN held a virtual FinCEN Exchange focused on the growing concern with ransomware-related events and efforts to combat the issue. This exchange included representatives from financial institutions, technology firms, digital forensic incident response (DFIR) firms, virtual asset service providers (VASPs), and federal government agencies.[15] Following Treasury's fall 2020 efforts to draw attention to ransomware and potential associated reporting obligations, FinCEN observed a notable increase in filings during the last quarter of 2020, which contributed to the overall rise in 2020 filings (see Figure 1). For example, during the first six months of 2021, of the 458 ransomware-related transactions, 335 SARs referenced the key term "CYBER-FIN-2020-A006" from FinCEN's October 2020 ransomware advisory.[16]

Figure 1. Number of Ransomware-Related SARs and Transactions, 2011 to June 2021[17]



11. *See* footnote seven.
12. "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," U.S. Department of the Treasury Advisory, 1 Oct. 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.
13. On 21 September 2021, OFAC updated its ransomware-related advisory to encourage reporting and cyber resilience, "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. "Ransomware Annex to G7 Statement," G7 Finance Ministers and Central Bank Governors, 13 Oct 2020, https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf.
15. "FinCEN Holds Virtual FinCEN Exchange on Ransomware," Financial Crimes Enforcement Network Press Release, 12 Nov. 2020, https://www.fincen.gov/news/news-releases/fincen-holds-virtual-fincen-exchange-ransomware.
16. A number of the 335 SARs appeared to reference FinCEN's 2020 Advisory on Ransomware and noted "CYBER-FIN-2021-A006," which FinCEN assesses to be a typographical error referring to "CYBER-FIN-2020-A006."
17. 2021 figures report transaction dates during the review period. Transaction date data include SARs filed in July 2021 with a transaction date before July 2021. FinCEN assessed SARs filed between 1 January 2020 and 31 July 2021 for accuracy, duplication, and false positives using both the narrative and the note to FinCEN field on SAR forms. Data from SARs filed between 1 January 2011 and 31 December 2019 reflect reports that contain "ransomware" in the narrative.

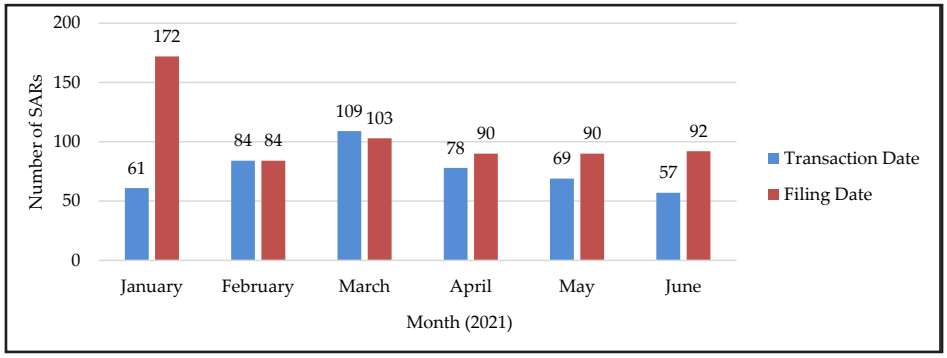
Figure 2. Total Suspicious Amount from Ransomware-Related SARs and Transactions, 2011 to June 2021[18]



Reported Ransomware-Related Transactions Substantially Increased from 2020

The number of ransomware-related SAR filings fluctuated in the first quarter of 2021 before stabilizing in the second quarter of 2021. Due to lookback SARs reporting ransomware attacks over the course of the preceding six months, January 2021 saw a sharp increase in the number of SARs filed. SAR data reports a mean average of 76 and a median average of 73.5 ransomware-related transactions per month during the review period (see Figure 3). The median average payment amount for ransomware-related transactions during the review period was $102,273, a slight increase from the median average payment amount of $100,000 for transactions between 1 January 2020 and 30 June 2020, according to SAR data (see Figure 4).[19] SARs report that during the review period the vast majority of ransomware-related payments were for less than $250,000 (see Figure 5).

Figure 3. Number of Ransomware-Related Transactions, January 2021 to June 2021[20]



18. 2021 figures report transaction dates during the review period. Transaction date data includes SARs filed in July 2021 with a transaction date before July 2021. FinCEN assessed SARs filed between 1 January 2020 and 31 July 2021 for accuracy, duplication, and false positives. Data from SARs filed between 1 January 2011 and 31 December 2019 reflect reports that contain "ransomware" in the narrative.
19. Ransomware-related payment amounts vary greatly from as little as $1 to as much as $45 million in 2021. To reduce the effect of outliers only the median average is reported for this data set.
20. Eighty-three of the 172 SARs filed in January 2021 are lookback filings that report transactions that occurred before December 2020.

Figure 4. Total Suspicious Amount of Ransomware-Related Transactions, January 2021 to June 2021[21]

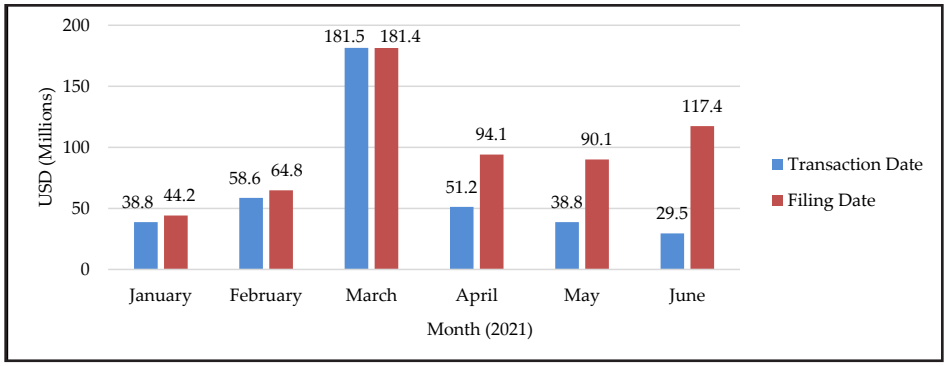
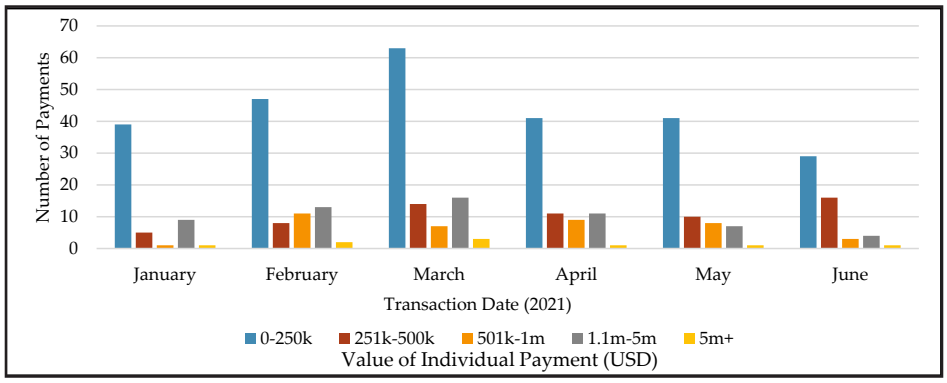


Figure 5. Ransomware-Related Payments by Value, January 2021 to June 2021



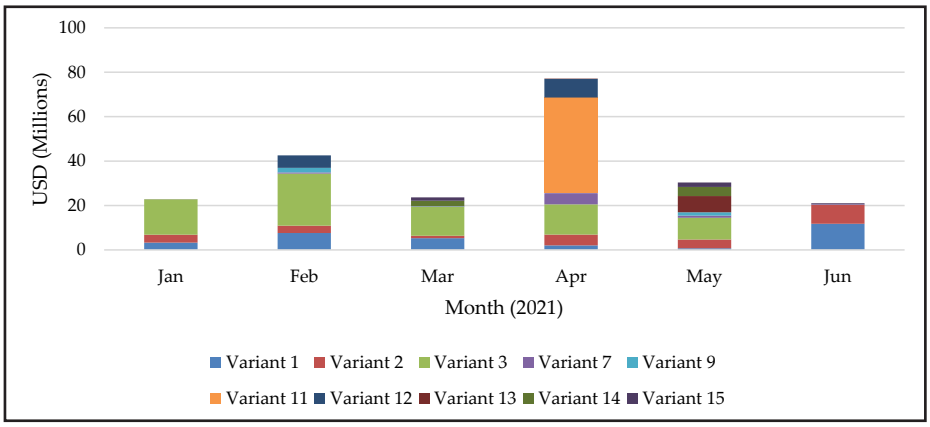
68 Variants Identified, Variant 1 Most Prevalent

Ransomware Variants: FinCEN identified 68 ransomware variants reported in SAR data for transactions during the review period. Ransomware variant analysis can help determine potential threat actors behind an attack. Ninety SARs did not name the ransomware variant used in the attack, and some SARs reported multiple incidents involving more than one variant. Figures 6, 7, and 8 depict the suspicious amounts, number, and value of transactions for the 10 variants with the highest payment amounts and highest number of incidents in SARs.[22]

The top 10 variants with the highest cumulative payment amounts identified in SARs during the review period accounted for $217.56 million in suspicious activity (see Figure 6). The highest total suspicious payment amounts for individual variants reported in SARs range from $30 to $76 million. Monthly suspicious payment amounts reported in SARs for the top 10 variants range from $3,095 to $43.06 million with a median average of $27 million and mean average of $36.26 million. In June 2021, the highest cumulative suspicious payment amounts were associated with Variant 1 ($11.78 million) and Variant 2 ($8.53 million), according to SAR data.

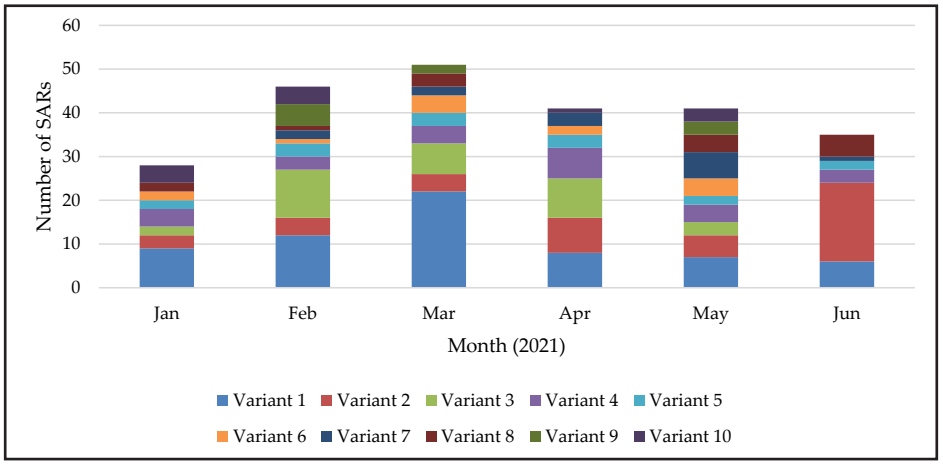
21. The sharp increase in total suspicious amount for March 2021 reflects two high-value SARs, and a single lookback SAR reporting multiple ransom payments over the course of a year that account for approximately 25 percent of the March total.
22. Actual variant names are redacted for operational security purposes.

Figure 6. Top Ransomware Variants by Suspicious Payment Amount with Transaction Dates Between January 2021 and June 2021



FinCEN identified 242 SARs filed on the top 10 most frequently reported variants with transaction dates during the review period (see Figure 7). These SARs most frequently report Variant 1 (64 reports), followed by Variant 2 (42 reports) and Variant 3 (32 reports). The number of monthly SARs for the top 10 variants range from 0 to 22 reports. In June 2021, SARs most frequently reported Variant 2 (18 reports) and Variant 1 (six reports).

Figure 7. Top Ransomware Variants by Number of SARs with Transaction Dates Between January 2021 and June 2021



FinCEN analysis of reported ransomware-related transactions during the review period determined that Variant 1 had the highest number of incidents (64), Variant 3 had the highest total dollar value of transactions ($75.8 million), and Variant 2 had the highest median average incident value ($353,800) for known variants (see Figure 8).[23]

23. 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.

Figure 8. Ransomware Variants by Number and Value of Transactions with Transaction Dates Between January 2021 and June 2021[24]

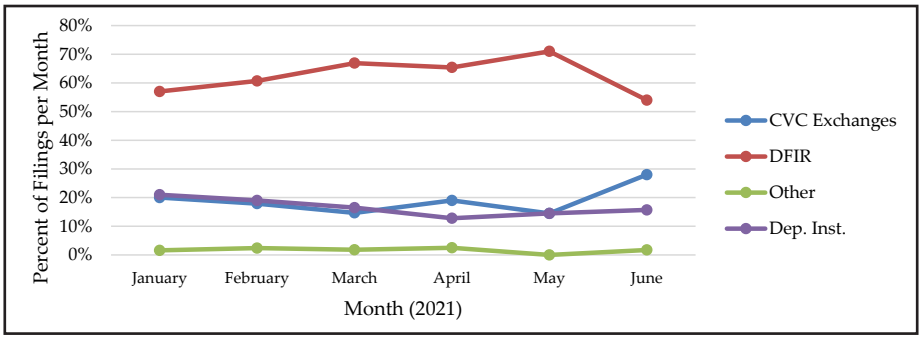
Ransomware Variant	Number of Incidents	Total Dollar Value of Incidents	Median Average Incident Value[25]
Variant 1	64	~$30.7 million	~$177,800
Variant 2	42	~$25.3 million	~$353,800
Variant 3	32	~$75.8 million	~$200,000
Variant 4	25	~$2.8 million	~$73,900
Variant 5	15	~$800,000	~$70,000
Variant 6	13	~$1.4 million	~$75,600
Variant 7	14	~$7 million	~$300,000
Variant 8	15	~$3.7 million	~$176,000
Variant 9	10	~$3.7 million	~$140,000
Variant 10	12	~$1.3 million	~$125,000
Total	**242**	**~$152.5 million**	**~$148,400**

Digital Forensic Incident Response Firms File Majority of Ransomware-Related SARs

During the review period, U.S.-based DFIR firms submitted the majority of ransomware-related SARs, or approximately 63 percent of ransomware-related SARs (see Figure 9).[26] In addition, depository institutions and CVC exchanges submitted over a third of SARs at 17 percent and 19 percent of SARs, respectively. Other institutions including broker-dealers, an insurance company, and casinos submitted less than 10 percent of the total SARs.

24. SARs report 90 transactions with a total value of $143.8 million and a median average incident value of $102,273 related to unknown variants.
25. To reduce the effect of outliers only the median average is reported for this data set.
26. As noted in FinCEN's 2020 Advisory on Ransomware, DFIR companies help victims respond to cyber-attacks and may facilitate ransomware payments to cybercriminals by converting customer fiat funds to CVC and then transferring the funds to criminal controlled accounts.

Figure 9. Ransomware-Related Transactions by Institution Type, January 2021 to June 2021[27]



A small number of DFIR firms submitted ransomware-related SARs for transactions conducted during the review period. These DFIR firms filed 290 ransomware-related SARs.[28]

Majority of Reported Ransomware-Related Payments in Bitcoin

FinCEN identified BTC as the most common ransomware-related payment method in reported transactions. FinCEN also observed that incidents requesting Monero (XMR), an AEC, is on track to increase slightly compared to 2020.

Ransomware-Related Payment Methods: Of the SARs reporting ransomware-related payments during the review period that identified a specific CVC, the vast majority reported payments made in BTC.[29] Sixty-four SARs that report a ransomware-related payment did not identify a specific CVC. While there are thousands of CVCs in the market, the SAR data only noted attackers requested BTC and XMR as methods for ransomware-related payment during the observed timeframe.

Monero Ransomware-Related Requests: FinCEN identified 17 ransomware-related SARs during the review period requesting payment in XMR (see Figure 10). In some instances, the attacker provided both an XMR and a BTC address, and imposed an extra fee if payment was made in BTC. In other instances, they exclusively requested payment in XMR, but accepted payment in BTC after negotiation.

27. The "CVC" category includes CVC kiosks. The "Other" category includes casinos, securities broker-dealers, wealth management firms, and insurance companies.
28. FinCEN identified a small number of DFIR firms that purport to negotiate on behalf of victims in SAR data. FinCEN does not have information on the total number of DFIR firms that exist.
29. As noted in FinCEN's 2020 Advisory on Ransomware, cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in BTC. 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.

Figure 10. Monero (XMR) Ransomware-Related Requests, January 2021 to June 2021

Circumstance of Request	Number of Payments	Value of Total Payments (USD)
Attacker provided both XMR and BTC wallet addresses	7	~$34 million
Attacker requested only XMR	7	~$2.4 million
Other[30]	3	~$500,000
Total	**17**	**~$37 million**

Communication via The Onion Router and Email Systems

Victims typically communicated with the threat actors via The Onion Router (Tor), encrypted email, non-encrypted email, and unidentified web portals provided by the attackers, according to SAR data. Tor employs encryption to allow for anonymous browsing as traffic moves within a network. The victims, or DFIR firms representing them, primarily engaged with the threat actors using a Tor website provided by the attackers to negotiate the ransomware-related payment, according to SAR data (see Figure 11). After negotiating the ransom amount, the DFIR firm or victim would make payment in exchange for decryption keys. Some variants required further negotiation and escalating payment demands even after initial payments were made.

Figure 11. Ransomware-Related Payments by Communication Method, January 2021 to June 2021

Communication Method	Number of Transactions	Transaction Value
Tor	192	~$165.6 million
Email	111	~$41.5 million
Other[31]	10	~$2.5 million
Unknown	145	~188.4 million
Total	**458**	**~$398 million**

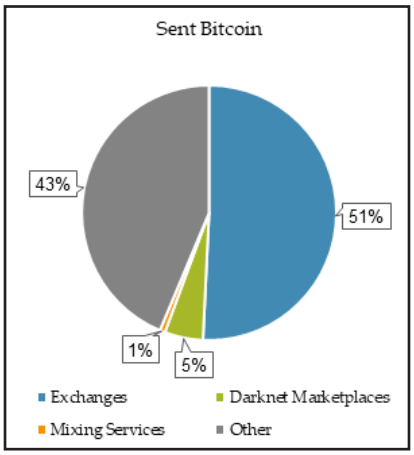
30. FinCEN identified three ransomware-related SARs mentioning Monero as a potential payment method, but did not explicitly state whether Monero was the exclusive payment method requested.
31. "Other" includes communication methods such as web portals and communication platforms not explicitly stated in SARs.

177 Unique Wallet Addresses Identified for Top 10 Ransomware Variants

FinCEN identified 177 unique wallet addresses used for ransomware-related payments by the top 10 most common ransomware variants reported in SARs during the review period (*see* Appendix 1 for detailed information on each variant).[32] FinCEN conducted analysis using commercially available analytics tools to determine the source of funds victims used to pay ransoms and the overall BTC sent from these threat actor wallet addresses to known entities. Not all of the funds sent from these wallet addresses are definitively related to ransomware payments; however, all of the exchanges and services identified below were at a minimum a direct counterparty to wallet addresses that received ransomware-related payments (see Figure 13).

Wallets associated with the 10 variants examined sent BTC valued at $5.2 billion to known entities, directly or indirectly, including 51 percent to exchanges, 43 percent to other CVC services, five percent to darknet marketplaces, and one percent to mixing services.[33] [34] [35] These percentages identify transactions traced to known entities and may not represent the final cash out locations after obfuscation of funds. While the total in Figure 13 indicates the 10 variants sent one percent of all funds to mixing services, this percentage varies when broken down by variant (*see* Appendix 1). The totals in Figure 13 include 177 wallet addresses identified in SARs and approximately 423,000 wallet addresses assessed to be associated with the relevant ransomware variants by commercially available analytics tools.[36]

Figure 13. Top 10 Ransomware Variant Transactions with Known Entities



32. Most of the 458 SARs FinCEN examined did not report the attacker's wallet address.
33. Victims predominantly sourced funds from U.S.-registered exchanges.
34. "Other" includes unidentified CVC services, as well as unspent and untraced CVC.
35. Direct transactions are funds sent from one party to another without intermediaries. Indirect transactions are funds sent from one party to one or more intermediary wallet address before the first encountered service.
36. FinCEN identified 177 wallet addresses associated with the 10 ransomware variants in SAR data and a total of 422,895 wallet addresses associated with the ransomware variants using commercially available analytics tools. This difference is likely due to underreporting of ransomware incidents. Not all of the funds sent from these wallet addresses are definitively related to ransomware payments; however, all of the exchanges and services identified in Figure 13 were at a minimum a direct counterparty to wallet addresses that received ransomware-related payments.

Ransomware-Related Money Laundering Typologies

FinCEN identified at least six money laundering typologies attributed to ransomware variants in 2021 by analyzing ransomware-related SARs, conducting blockchain analysis, and leveraging industry observations and outreach. For example, participants in this year's FinCEN Exchange on ransomware separately substantiated these observations citing their own analysis of ransomware activity.[37]

Threat Actors Increasingly Request Payments in AECs

FinCEN's analysis of ransomware-related SARs found ransomware-related payments are often initially requested in BTC, though threat actors may request payments in AECs, most commonly XMR. FinCEN observed a 10 to 20 percent surcharge or discount for victims paying in BTC, and, on some occasions, threat actors exclusively requested payment in XMR.

Threat Actors Avoided Reusing Wallet Addresses

After receiving illicit funds from a victim, ransomware actors layered funds through multiple wallet addresses and avoided reusing wallet addresses for each attack, according to SAR data. Threat actors laundered the payments from each ransomware event separately, to minimize consolidation into single wallet addresses.

Centralized CVC Exchanges are Preferred Cash-out Points

Threat actors identified from SARs primarily use foreign centralized exchanges for ransomware-related deposits, including exchanges incorporated in high-risk jurisdictions that may have opaque ownership structures or that may have inadequate AML/CFT compliance standards. This observation is also corroborated by commercial blockchain analytic companies that note the use of exchanges incorporated in jurisdictions that may not enforce know your customer (KYC) requirements or require the reporting of suspicious transactions.[38] Non-compliant centralized exchanges are possibly a key step in the layering and obfuscation process of laundering funds from CVC to fiat currency.

"Chain Hopping" is Used to Obfuscate Financial Trails on Blockchains

Illicit actors often engage in the practice of "chain hopping" to obfuscate the origin of their funds. Chain hopping refers to the practice of converting one CVC into a different CVC at least once before moving the funds to another service or platform. This practice allows threat actors to convert illicit BTC proceeds into an AEC like XMR at CVC exchanges or services. Threat actors can then transfer the converted funds to large CVC services and MSBs with lax compliance programs.

37. FinCEN held the second Ransomware FinCEN Exchange on 10 Aug. 2021. *See* https://www.fincen.gov/news/news-releases/fincen-holds-second-virtual-fincen-exchange-ransomware.
38. Dr. Tom Robinson, "DarkSide Ransomware has Netted Over $90 million in Bitcoin," Elliptic Blog, 18 May 2021, https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin, accessed 3 Sept. 2021.

Mixing Services are Prevalent in 2021

FinCEN observed an increased use of mixing services in SARs.[39] Mixers are websites or software designed to conceal or obfuscate the source or owner of CVC. Mixers may have obligations as money transmitters under the BSA. For example, in October 2020 FinCEN assessed a $60 million civil money penalty against Larry Dean Harmon for operating the mixing service Helix and failing to register with FinCEN, maintain an effective AML program, and file SARs on suspicious activity that went through the Mixer.[40] Mixing is done either as a general privacy measure or for covering up the movement of funds obtained from theft, darknet markets, or other illicit sources.

- According to a May 2020 report by Crystal Blockchain, there was a rapid growth in the amount of BTC sent from darknet entities to mixers in Q1 2020.[41]
- According to Chainalysis' mid-year report on ransomware, mixing services are still a preferred destination for illicit funds behind centralized exchanges.[42]
- FinCEN's analysis of the 10 most common ransomware variants in SAR data during the review period indicate use of mixers varies by variant. (*See* Appendix 1).

Decentralized Exchanges Likely Used to Convert Illicit Proceeds

Ransomware-related payments are being converted to other types of CVCs through decentralized exchanges or other DeFi applications. Some DeFi applications allow for automated peer-to-peer transactions without the need for an account or custodial relationship. FinCEN analysis of transactions on the BTC blockchain identified ransomware-related funds sent indirectly to addresses associated with open protocols for use on DeFi applications.

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 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.[43] 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.

39. For more information on mixers, see FinCEN Guidance FIN-2019-G001, 9 May 2019, p.19-20 https://www.fincen.gov/sites/default/files/2019-05/FinCEN Guidance CVC FINAL 508.pdf.
40. "In the matter of Larry Dean Harmon d/b/a Helix, Assessment of Civil Money Penalty Number 2020-02," FinCEN, 19 Oct. 2020, https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix Assessment and SoF_508_101920.pdf.
41. Crystal analytics team, "Darknet Use and Bitcoin — A Crypto Activity Report by Crystal Blockchain," Crystal Blockchain, 19 May 2020, https://crystalblockchain.com/articles/darknet-use-and-bitcoin-a-crypto-activity-report-by-crystal-blockchain/, accessed 26 Aug. 2021.
42. Chainalysis, "Ransomware 2021: Critical Mid-Year Update," July 2021, https://blog.chainalysis.com/reports/ransomware-update-may-2021, accessed 26 Aug. 2021.
43. For more information see FinCEN Advisory #FIN-2020-A006, 1 Oct. 2020, https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory Ransomware FINAL 508.pdf.

Detection and Mitigation Recommendations

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

1. Incorporate 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.[44] 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.

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 SAR form. Information regarding ransomware variants, AECs 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.

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 October 2020.[45]

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.

44. 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.

45. For more information see FinCEN Advisory #FIN-2020-A006, 1 Oct. 2020, https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory Ransomware 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 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.

Appendix 1: Ransomware Variant Analysis

FinCEN determined the top 10 most common ransomware variants reported in SAR data and reviewed open-source reporting to determine dates of activity and accepted payment method(s). FinCEN identified unique wallet addresses used for ransomware-related payments by the top 10 most common variants and conducted analysis using commercially available technology. These identified wallet addresses sent BTC to different CVC services including exchanges, darknet markets (DNM), mixers, licit and illicit CVC service categories including untraced and unspent BTC.

Ransomware Variant	Start/End Date	Accept XMR (Y/N)	Accept BTC (Y/N)	Sent BTC (USD)				
				Exchange	DNM	Mixer	Other [46]	Total
Variant 1	April 2019 - July 2021	Y	Y	~$6.3 million	~$826,000	~$6.5 million	~$32.3 million	~$46 million
Variant 2	December 2019 - present	N	Y	~$66.1 million	~$7.3 million	~$4 million	~$161 million	~$238.5 million
Variant 3	August 2020 - May 2021	Y	Y	~$14.3 million	~$609,000	~$6.5 million	~$76.8 million	~$98.2 million
Variant 4	June 2020 - June 2021	N	Y	~$4.9 million	~$660,000	~$1.6 million	~$6.3 million	~$13.5 million
Variant 5	September 2019 - present	N	Y	~$1.7 billion	~$241.6 million	~$9.7 million	~$1.7 billion	$3.6 billion
Variant 6	July 2018 - present	N	Y	~$604.4 million	~$622,700	~$2.2 million	~$184.5 million	~$791.7 million
Variant 7	October 2019 - present	N	Y	~$3 million	~$3,600	~$2.3 million	~$3.5 million	~$8.8 million
Variant 8	December 2019 - present	N	Y	~$240 million	~$740,000	~$1 million	~$64.3 million	~$305.8 million
Variant 9	November 2019 - present	N	Y	~$519,000	~$79,000	~$9,900	~$6.9 million	~$7.5 million
Variant 10	September 2019 - present	N	Y	~$8.4 million	~$76,300	~$1.3 million	~$11 million	~$20.7 million
Total				**~$2.6 billion**	**~$252.5 million**	**~$35.2 million**	**~$2.3 billion**	**~$5.2 billion**

46. "Other" includes unidentified CVC services as well as unspent and untraced CVC.