Written Testimony of Jacqueline Koven
Head of Cyber Threat Intelligence
Chainalysis Inc.

Before the
House Financial Services Committee,
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

Hearing on
"Held for Ransom: How Ransomware Endangers our Financial System"

April 16, 2024

Chairman Luetkemeyer, Ranking Member Beatty, and distinguished members of the Subcommittee: Thank you for inviting me to testify before you today on this very important topic.

My name is Jacqueline Burns Koven and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis. In this role, I track ransomware operators and their enablers on the blockchain to empower policymakers and US government agencies with the data they need to investigate, attribute, and disrupt the ransomware supply chain. I also coordinate global ransomware research, partnerships, and joint initiatives. Prior to joining Chainalysis, I served in the US Intelligence Community, including in Iraq and held several interagency assignments.

For the past ten years, Chainalysis compliance and investigative solutions have been used by law enforcement, regulators, financial institutions, cryptocurrency businesses, and cybersecurity and incident response firms to investigate and disrupt threat actors engaged in ransomware and other illicit activities. Our data and software solutions have been involved in law enforcement activities resulting in the seizure of over $10 billion in assets held by illicit actors and numerous high-profile cyber-crime cases, including those involving some of the most notorious ransomware actors. Chainalysis plays an integral role for law enforcement as the only blockchain analytic solutions to have been tested for reliability under exacting admissibility standards by a federal court.

We are encouraged that this subcommittee is interested in learning more about the impact of ransomware on our financial system and about what can be done to mitigate the harm from ransomware attacks. We strongly believe that blockchain intelligence solutions like Chainalysis are key to helping fight back on this growing form of cyber attack. To that end, we invite Congress' continued engagement on this topic as addressing this issue requires an all-of-government approach in collaboration with the private sector, and we recommend

that Congress ensure that law enforcement and other federal agencies have the resources necessary to comprehensively combat this issue.

## Blockchain transparency and the role of Chainalysis

The use of cryptocurrencies by ransomware actors provides a unique opportunity to investigate and disrupt their activities. Cyber extortion dates back to before the introduction of cryptocurrencies. However, the current form of these attacks almost always involves a demand for ransom payment in some form of cryptocurrency. Moreover, ransomware actors frequently utilize cryptocurrencies to launder ransoms they receive and to facilitate payments for services and tools used for carrying out ransomware attacks.

It is a common misconception that these cryptocurrency transactions are completely anonymous and untraceable. While some may suggest that the nature of cryptocurrency facilitates the crime of ransomware, the reality is that its nature facilitates incomparable visibility — on individual transactions as well as the structure of organized criminal networks — and that benefits law enforcement immensely.

Cryptocurrency transactions are inherently public and the data from those transactions is preserved on a transparent, immutable ledger. At Chainalysis, we analyze the transaction data from blockchain networks in conjunction with open source intelligence information and proprietary data to map the ecosystem of participants in these networks. We then provide software solutions, investigative support, and best-in-class data to allow government investigators to trace the flow of transactions and identify potential illicit activity.

With respect to ransomware, we have significant experience in identifying the illicit actors engaging in ransomware attacks and connecting the identities of those entities to the wallet addresses they control on various blockchain networks. From a single cryptocurrency wallet address, such as one used for a ransom payment, we can trace the movement of funds to illuminate the full network of tools and services underpinning the attack. By providing this intelligence to the law enforcement and other US government agencies with speed and accuracy, agents are provided with a new and powerful tool to track down these bad actors, identify centers of control, and inhibit their ability to profit from these terrible attacks.

For example, using Chainalysis' blockchain analysis solutions, law enforcement can trace cryptocurrency transactions to identify their origination and/or its cashout points at cryptocurrency exchanges. Law enforcement can serve legal process to cryptocurrency businesses to request identifying information related to accounts associated with the illicit transactions, or request that the associated accounts be frozen. This information can be very

powerful in furthering investigations into the illicit use of cryptocurrency, including ransomware.

## Leveraging blockchain intelligence to disrupt ransomware

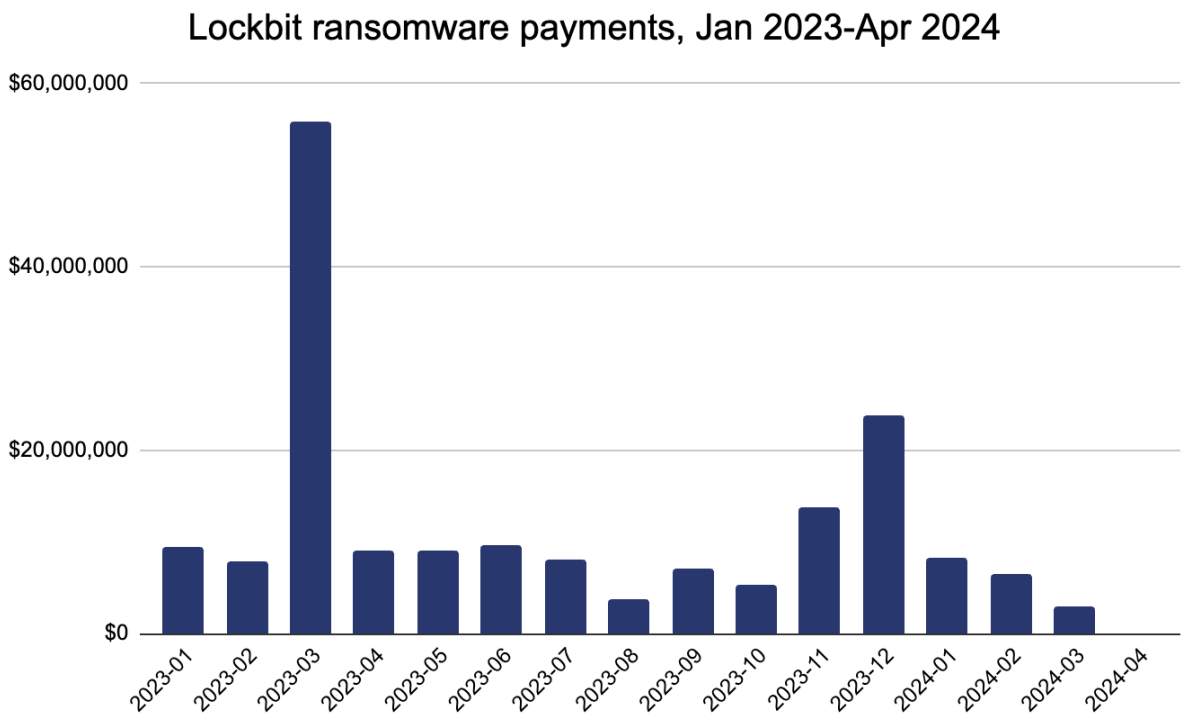
Chainalysis solutions and investigators have supported a number of successful government operations involving arrests, asset seizures, and ransomware takedowns. These operations have helped disrupt threat actors responsible for some of the most notorious ransomware attacks, including attacks on the Colonial Pipeline and financial infrastructure provider ION.

- In 2021, Chainalysis solutions aided the FBI investigation of the Colonial Pipeline ransomware attack, which had led to fuel shortages throughout the southeastern United States.[1] The Department of Justice (DOJ) was able to identify the perpetrators of the attack as DarkSide, a Russia-based cybercriminal group, and announced that it was able to seize $2.3 million worth of Bitcoin from the ransom payment made by Colonial Pipeline.[2]

- Recently, Chainalysis was leveraged as part of the multi-national law enforcement operation to disrupt Lockbit, a Russia-based "Ransomware-as-a-Service" (RaaS) group responsible for some of the most brazen attacks on the U.S. financial system last year, including attacks on ION, ICBC, and Equilend.[3] On February 20, 2024, the U.S. DOJ and the U.K.'s National Crime Agency (NCA) announced that it had successfully seized servers and public-facing websites that were integral to Lockbit's operations, seized 200 cryptocurrency accounts, and obtained decryptor keys for Lockbit victims to recover their data without paying a ransom. NCA also identified 2200 BTC, more than $110 million, in unspent funds on the blockchain that Chainalyisis is actively monitoring today. [4] The DOJ also announced charges against two Russian nationals accused of acting as Lockbit RaaS affiliates and using the strain in ransomware attacks. Additionally, OFAC sanctioned both individuals for their ransomware activities, and included ten total cryptocurrency addresses as SDN

[1] "Chainalysis In Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack," *Chainalysis*, Feb. 10, 2022, https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/.
[2] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," *U.S. Dept. of Justice*, June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[3] "U.S. and U.K. Disrupt Lockbit Ransomware Group and Indict Two Russian Nationals While OFAC Levies Sanctions," *Chainalysis*, Feb. 21, 2024, https://www.chainalysis.com/blog/lockbit-takedown-sanctions-february-2024/.
[4] "U.S. and U.K. Disrupt LockBit Ransomware Variant," *U.S. Dept. of Justice*, Feb. 20, 2024, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

List identifiers.




- In 2021, the U.S. led an international law enforcement action to disrupt the NetWalker ransomware along with the support of Chainalysis.[5] The disruption included the seizure of nearly 30 million dollars in cryptocurrency, the disablement of a dark web resource used to communicate with NetWalker ransomware victims, and the arrest of a Canadian national who obtained tens of millions of dollars by acting as a NetWalker affiliate.

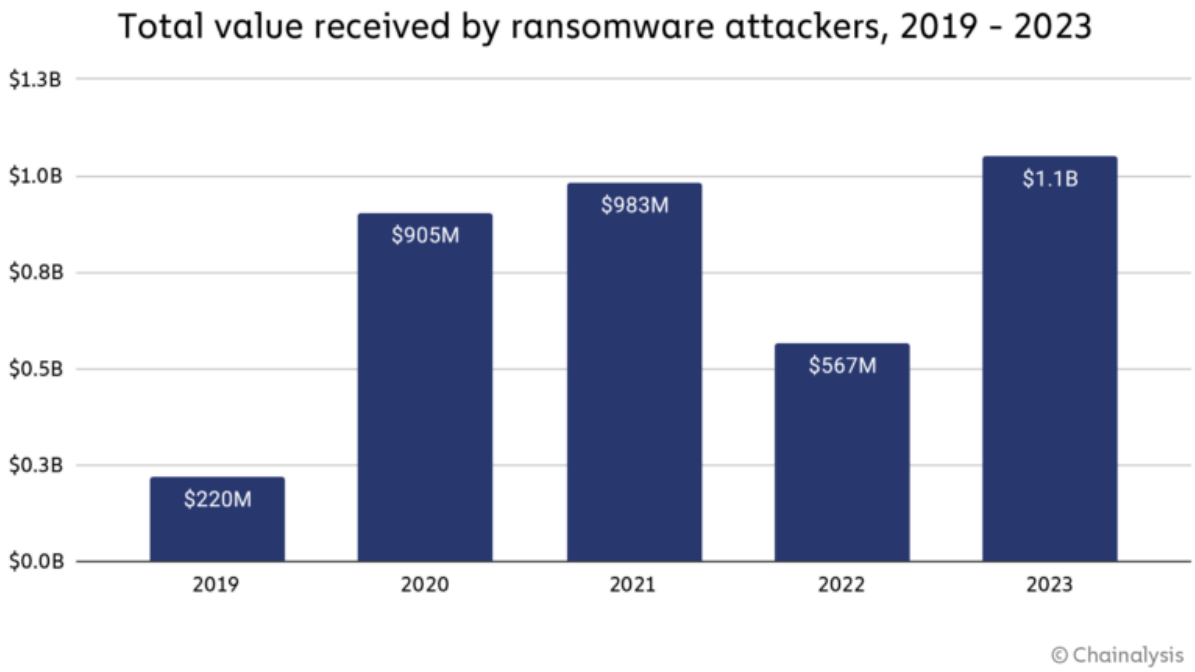
Disruptions play a critical role in the short term mitigation of ransomware activities, but the adaptability and resilience of affiliates poses ongoing challenges. Varying effects of disruptions demonstrate the importance of the type of disruption, with deep infiltration and direct takedowns proving particularly effective. Continuous investment by ransomware actors in future attacks and the diversification of malware strains used by affiliates show the evolving and persistent nature of the ransomware threat.

[5] "Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware," *Chainalysis*, Jan. 27, 2021, https://www.chainalysis.com/blog/netwalker-ransomware-disruption-arrest/.

## Ransomware statistics and trends

*Payment trends over 2022-2023*

The subcommittee's focus on ransomware is well-timed as 2023 proved to be a landmark year in terms of ransom payments. According to our data, ransomware gangs reached an unprecedented milestone, surpassing $1 billion in extorted cryptocurrency payments from victims, the highest annual amount ever observed.[6] This comes after a significant decrease in the total amount of ransomware payments observed in 2022.

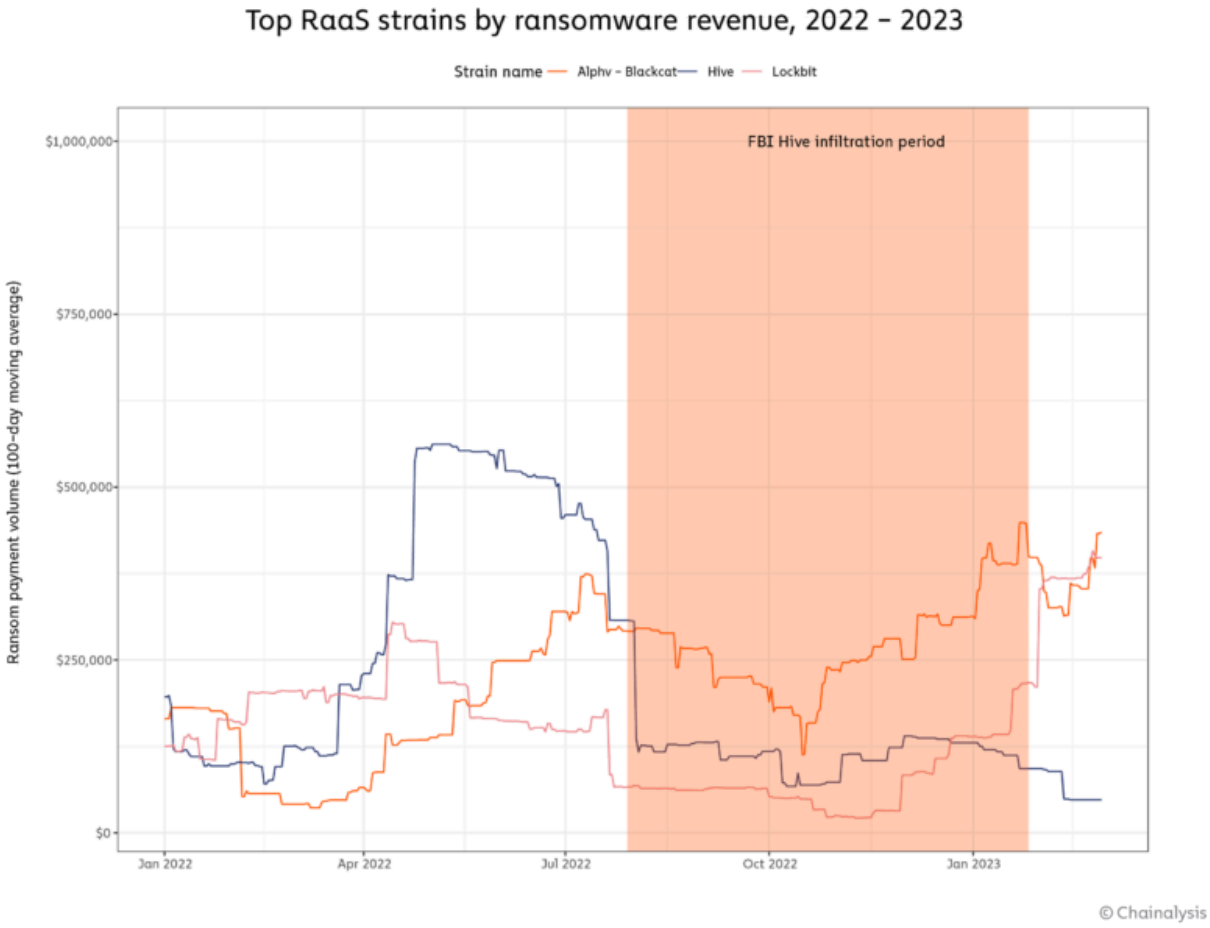



We attribute the decline in ransom payments in 2022 to several factors including geopolitical events like the Russian-Ukrainian conflict, which not only disrupted the operations of some cyber actors but also shifted their focus from financial gain to politically motivated cyberattacks aimed at espionage and destruction.[7] Other factors that likely played a role in this downturn included a reluctance among some Western entities to pay ransoms to certain strains due to potential sanctions risks, and more stringent insurance policies requiring entities they cover to have more robust security policies, tools and training to be better prepared for attacks and possibly negate the need to pay if attacked.

[6] "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," *Chainalysis*, Feb. 7, 2024, https://www.chainalysis.com/blog/ransomware-2024/.
[7] *See* McLaughlin, "Ukrainian hacktivists fight back against Russia as cyber conflict deepens," *NPR*, Nov. 21, 2023, https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war.

Another significant factor in the reduction of ransomware in 2022 was the successful infiltration of the Hive ransomware strain by the Federal Bureau of Investigation (FBI), as announced by the Department of Justice early in 2023.[8] During the infiltration of Hive, the FBI was able to provide decryption keys to over 1,300 victims, effectively preventing the need for ransom payments. The FBI estimates that this intervention prevented approximately $130 million in ransom payments to Hive.[9]

But the impact of this intervention extends further than that. Total tracked ransomware payments for 2022 currently stand at just $567 million, indicating the ransom payments prevented by the Hive infiltration significantly altered the ransomware landscape as a whole.

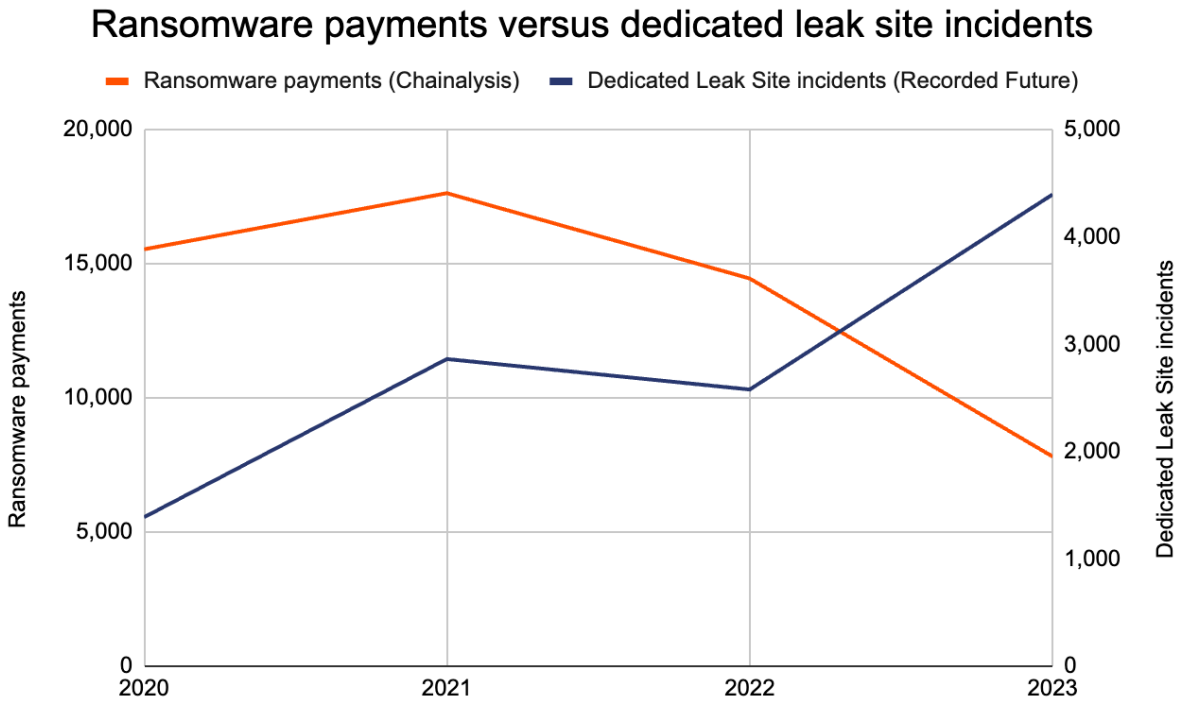



The upswing in total ransom payments in 2023 can likely be attributed to a major escalation in the frequency, scope, and volume of attacks. The professionalization of the criminal

[8] *See* "U.S. Department of Justice Disrupts Hive Ransomware Variant," *Dept. of Justice*, Jan. 26, 2003, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.
[9] *Id.*

ecosystem has lowered the barriers to entry for this type of crime, and given way to numerous different ransomware "strains" or malware programs. Threat actors are opportunistic. The same threat actors that are attacking financial institutions are also attacking healthcare facilities, non-profits, municipalities, schools and other businesses.

According to *Recorded Future*, the number of ransomware victims in 2023 went up 70% from the year prior.[10] However, it is important to highlight that, according to our data at Chainalysis, the actual number of ransomware incidents resulting in payments declined 46%. These findings are corroborated by reports from incident response firms that the overall percentage of payments has decreased starkly with respect to ransomware incidents they have assisted with over the years.[11]

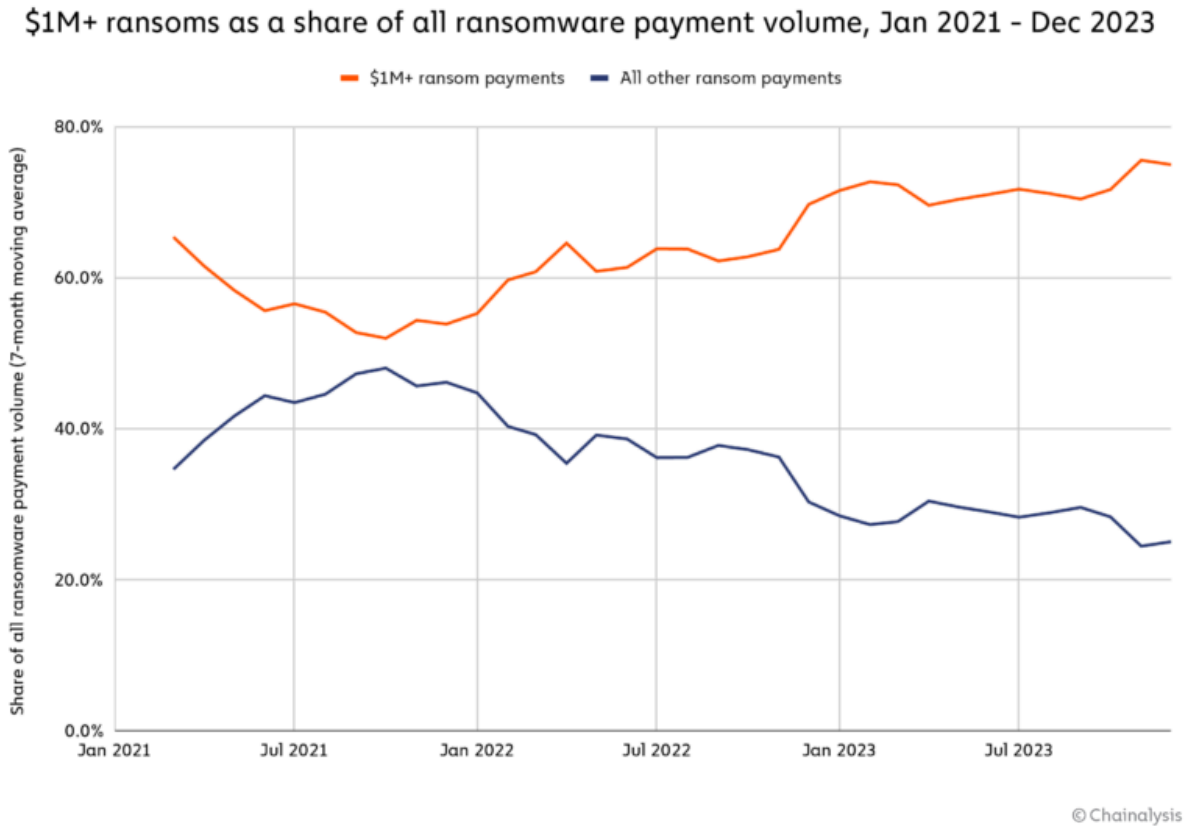



One potential significant takeaway from this data is that it is becoming easier for threat actors to deploy ransomware, yet harder to profit.

[10] "Ransomware payments doubled to more than $1 billion in 2023," *The Record*, Recorded Future, Feb. 7, 2024, https://therecord.media/ransomware-payments-doubled-to-more-than-1-billion-2023.
[11] *See* "New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying," *Coveware*, Jan. 26, 2004, https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

Another important observation from our data is that so-called “big game hunting” has become the dominant strategy especially over the last few years.

Based on the data we have collected, over 70% of all ransom payments from 2021 to 2023 were payments over $1 million and this percentage has steadily grown over the years. So even though the discrete number of ransoms paid declined in 2023, the outlier larger ransom payments were a driving factor behind the record-setting year.

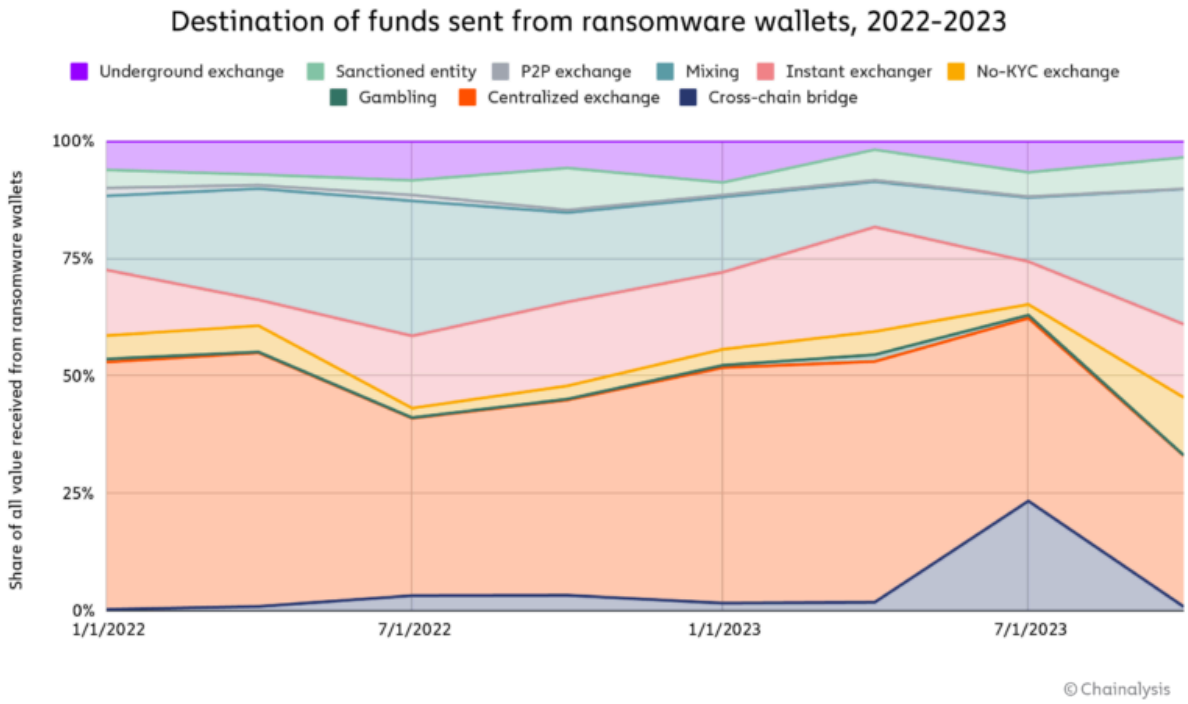



*Payment laundering trends*

Beyond just monitoring ransomware payments activity, Chainalysis also follows how ransomware actors are attempting to launder their ill-gotten funds. It is important to keep in mind that threat actors may take weeks, months, or even years to launder their proceeds from ransomware, and so some of the laundering observed in 2023 is from attacks that occurred well into the past.

Our data shows that cryptocurrency exchanges and mixers are the most common destination for ransomware payments, suggesting they are preferred methods for laundering funds.

However, this year saw the embrace of new services for laundering, including bridges, instant exchangers, and gambling services. We assess that this is a result of takedowns disrupting preferred laundering methods for ransomware, some services' implementation of more robust AML/KYC policies, and also as an indication of new ransomware actors' unique laundering preferences.




In sum, the ransomware landscape underwent significant changes in 2023, marked by shifts in tactics and affiliations among threat actors, as well as the continued spread of RaaS strains and swifter attack execution, demonstrating a more efficient and aggressive approach. The movement of affiliates highlighted the fluidity within the ransomware underworld and the constant search for more lucrative extortion schemes.

## Recommendations

Given the increase in ransomware attacks, as well as their potentially devastating impacts, Chainalysis believes it is important to enact meaningful policies to deter, detect, and disrupt ransomware. We support the numerous on-going ransomware initiatives and believe the foundation of US policies must be a comprehensive, whole-of-US government strategy leveraging collaborative private-public sector partnerships and information sharing for reducing ransomware attacks. We believe that clear guidance and direction will enable a unified inter-agency response and facilitate government agencies to work more effectively

with the private sector to combat this important issue and protect US national security interests. This threat is too big for one agency or entity to attack themselves -- it must be a concerted joint public-private effort with strong, unequivocal leadership.

Most importantly, as ransomware actors expand and become more sophisticated, it's critical for the US government to keep up. Government agencies that have embraced blockchain analysis have seized billions of dollars in cryptocurrency and successfully shut down ransomware groups—further evidence that with the proper tools, investigators can cut ransomware groups off from their ill-gotten funds. Many government agencies have limited or inconsistent personnel dedicated to investigating the illicit use of cryptocurrency because of a lack of training resources and a lack of funding for new personnel, tools, and training. Ensuring that these efforts are well-funded would ensure that when cryptocurrencies are exploited by criminals, investigators can trace these illicit transactions, seize funds, and bring criminals to justice. Further, where our solutions are being utilized, the government should more effectively and efficiently utilize and distribute these tools so government personnel can better respond to incidents.

—

Thank you again for the opportunity to provide testimony on this important topic.