United States Senate Committee on

Homeland Security & Governmental Affairs

U.S. Senator Gary Peters | Chairman

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

A HSGAC Majority Staff Report

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

EXECUTIVE SUMMARY

Ransomware is a dangerous form of cyber-attack where threat actors prevent access to computer systems or threaten to release data unless a ransom is paid. It has the power to bankrupt businesses and cripple critical infrastructure – posing a grave threat to our national and economic security. The use of cryptocurrencies has further enabled ransomware attacks, particularly because crypto currency is decentralized and distributed and illicit actors can take steps to obscure transactions and make them more difficult to track.

In recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors. In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States. According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."

Many of these attacks generated significant losses and damages for victims. A three-year comparison of the number of complaints of ransomware submitted to the Federal Bureau of Investigation (FBI) between 2018 and 2020, demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses. In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million.

However, even these figures likely drastically underestimate the actual number of attacks and ransom payments made by victims and related losses. In fact, the FBI acknowledges that its data is "artificially low." Further evidence of this under-reporting is that the government data is significantly lower than several private sector estimates. For instance, Chainalysis, a blockchain data and analysis company that works with financial institutions, insurance and cybersecurity companies, and as a contractor for the U.S. government, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, close to a 300 percent increase over a two-year period. A separate study by the anti-malware company Emsisoft found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.

To better understand this growing threat, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced in July 2020 an investigation into the role of cryptocurrency in incentivizing and enabling ransomware attacks, and the resulting harm of such attacks to victims. As a part of this ten-month investigation, Committee staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands. While not exhaustive, this report addresses key pieces of the larger landscape of the increasing national security threat from ransomware attacks and the use of cryptocurrency for ransom payments.

The report details recommendations to address current gaps in information on ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

The report finds that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks. While multiple federal agencies are taking steps to address the increasing threat of ransomware attacks, more data is needed to better understand and combat these attacks. In interviews with Committee staff, federal officials and private sector companies each acknowledged the need for more compliance and data (*e.g.*, reporting of incidents and ransom payments). When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery. Such information also facilitates more efficient investigation and prosecution of illicit actors.

To address the current lack of information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022. The incident reporting provisions later became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the Consolidated Appropriations Act of 2022 in March 2022. The new reporting mandates in the law will begin to address this problem. Nevertheless, as indicated by the findings in the report, the Administration and Congress must remain vigilant against this growing threat.

Almost 40 million Americans – including approximately three-in-ten Americans age 18 to 29 – have engaged in some form of investment, trade, or other legitimate use of cryptocurrencies according to a November 2021 estimate by the nonpartisan Pew Research Center. The global market value of all cryptocurrencies reached $3 trillion in 2021, up from $14 billion in 2016.

However, according to multiple agencies interviewed by Committee staff, cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed. The payment structure's decentralized nature, as well as irregular regulatory compliance by some entities within the space and new anonymizing techniques contribute to the challenges law enforcement faces when seeking to arrest criminal actors, particularly foreign-based actors. High profile attacks, such as Colonial Pipeline, demonstrate ransomware attackers' threat to national security. The FBI's recovery of over half of the ransom paid by Colonial Pipeline, however, shows that with access to the right information, law enforcement can leverage cryptocurrency's unique features as well as other investigative techniques to track down cyber criminals and recover stolen funds.

Unfortunately, data reporting and collection on ransomware attacks and payments is fragmented and incomplete. Two federal agencies claim to host the government's one stop location for reporting ransomware attacks – the Cybersecurity and Infrastructure Agency (CISA) StopRansomware.gov website and the FBI's IC3.gov. These two websites are separate and, while the agencies state that they share data with each other, in discussions with Committee staff, ransomware incident response firms questioned the effectiveness of such communication channels' impact on assisting victims of an attack.

Many federal regulators have taken steps to address the rising threat of ransomware attacks by issuing new, and expanding existing, regulations and guidance. Generally, with respect to cryptocurrency, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has clarified that "money service businesses", *e.g.*, persons that accept and transmit "value that substitutes for currency", are subject to key financial regulations. Over the past few years, the Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and FinCEN have each issued new guidance and regulations subjecting cryptocurrency to additional oversight. In 2021, the Department of Justice (DOJ), SEC, and the Treasury Department's Office of Foreign Assets Control (OFAC), among other agencies, also issued guidance recognizing the need for more ransomware incident reporting.

On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies. Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity." The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, however, is fragmented and incomplete.

This limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security and limits private sector and federal government efforts to assist cybercrime victims. As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows. Approximately 74 percent of global ransomware revenue in 2021 went to entities either likely located in Russia or controlled by the Russian government. Further, CISA and other federal agencies have warned that Russia's invasion of Ukraine could lead to additional malicious cyber activity, including ransomware attacks, in the United States. Therefore, as the report finds, prioritizing the collection of data on ransomware attacks and cryptocurrency payments is critical to addressing increased national security threats.

I. FINDINGS OF FACT AND RECOMMENDATIONS

FINDINGS OF FACT

1. **The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.** The government largely relies on voluntary reporting of ransomware attacks and cyber extortion demands, which only captures a fraction of the attacks that occur. As of July 2021, the Cybersecurity and Infrastructure Security Agency (CISA), which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.

2. **Current reporting is fragmented across multiple federal agencies.** Data on ransomware attacks is reported to numerous federal agencies including CISA, the FBI, and the Treasury Department's FinCEN, among others. These agencies do not capture, categorize, or publicly share information uniformly.

3. **Lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against national security threats.** The lack of data on ransomware attacks and cryptocurrency ransom payments blunts the effectiveness of available tools for fighting ransomware attacks including U.S. sanctions, law enforcement efforts, and international partnerships, among other tools.

4. **Currently available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.** The private sector and the federal government are not able to fully and effectively assist victims to prevent or recover from ransomware attacks without a comprehensive dataset on ransomware attacks, ransom demands, and payments. Such a dataset does not currently exist.

RECOMMENDATIONS

1. **The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.** CISA should complete the required rulemaking as soon as possible to implement the requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law as part of the Consolidated Appropriations Act of 2022, which mandates incident reporting of substantial cyber-attacks and ransomware payments against critical infrastructure. Federal agencies should implement the requirement in the law to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.

2. **The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.** Agencies should standardize how data from existing reporting requirements for ransomware incidents and ransom payments is organized and formatted across federal government agencies to enable more comprehensive information sharing and analysis.

3. **Congress should establish additional public-private initiatives to investigate the ransomware economy.** The federal government should promote public-private partnerships to research the ransomware economy, in particular, the interrelationships between cybercriminals who conduct or facilitate ransomware attacks and the financial structures facilitated by cryptocurrencies that sustain cybercriminals' illicit activities, including privacy coins. These partnerships should also examine ransomware infrastructure to help design and promote effective countermeasures.

4. **Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.** Congress and relevant agencies should consider ways to support partners within the private, nonprofit, and academic sectors seeking to expand the collection and organization of information on ransomware attacks including by examining federal funding options and sharing anonymized data regarding ransomware attacks and payments. In addition, government agencies should collaborate with partners to identify viable crowdsourcing initiatives to pool information regarding ransomware attacks and extortion payments.