M E M O R A N D U M

To: Members of the Committee on Financial Services

From: Financial Services Committee Staff

Date: April 11, 2024

Subject: April 16, 2024, National Security, Illicit Finance, and International Financial Institutions Subcommittee Hearing Entitled "Held for Ransom: How Ransomware Endangers our Financial System."

On Tuesday, April 16, 2024, at 10:00 a.m. in Room 2128 of the Rayburn House Office Building, the Subcommittee on National Security, Illicit Finance, and International Financial Institutions of the Committee on Financial Services will hold a hearing titled "Held for Ransom: How Ransomware Endangers our Financial System." Testifying at the hearing will be:

- **Ms. Jacqueline Burns Koven:** Head of Cyber Threat Intelligence, Chainalysis
- **Mr. Daniel Sergile:** Senior Consulting Director, Unit 42 by Palo Alto Networks
- **Ms. Megan Stifel:** Chief Strategy Officer, Institute for Security and Technology
- **Ms. Kemba Eneas Walden,** President, Paladin Global Institute

Hearing Goals

The hearing will provide Members of the Financial Services Committee (Committee) with the opportunity to:

- Understand how ransomware attacks occur in real time;
- Analyze how ransomware has changed in a post-COVID 19 world; and
- Develop policy solutions to impede ransomware attacks.

Additionally, this hearing will enable Members to gain insight into the current threat landscape of the ransomware industry and how victim organizations deal with the consequences of a ransomware attack. While attacks may affect industries outside of the Committee's jurisdiction, financial institutions (FIs) play an integral role in processing ransomware payments and cybersecurity defense.

Background

Ransomware is defined as "malicious software, or malware, that prevents an individual from accessing computer files, systems, or networks and demands a ransom payment for their return."[1] The software or malware attacks a system by encrypting files in an organization's

[1] FBI Ransomware Page.

system, holding the data captive, until the victim organization pays a sum of money. Attackers can infiltrate a victim's system in several different ways, including phishing, adware, corrupting email addresses, corrupting email attachments, and visiting malware embedded websites. There are many different types of ransomware, and criminals are creating new methods of attack every day.

One of the most common ways to initiate an attack is through the "ransomware as a service" (RaaS) model. RaaS occurs when "attackers, known as affiliates, 'rent' usage of a particular ransomware strain from its creators or administrators, who in exchange get a percentage of the payment from each successful attack that the individual affiliates carry out."[2] The RaaS model is one that has generated some of the most successful attacks in the ransomware ecosystem, with law enforcement indicating that it expects RaaS attacks to only grow in future years.

RaaS allows a few, strong ransomware strains to exist in the ecosystem, but grants countless interested outsiders, known as affiliates, the ability to utilize a strain in a pay-to-play environment. RaaS affiliates pay for an available, proven ransomware strain, in the darknet market ethos that is tailored to a specific victim targeted by an affiliate.

ALPHV-BlackCat (ALPHV) is arguably one of the most notorious RaaS strains. However, ALPHV "is… selective in the affiliates it allows to use its malware, actively recruiting and interviewing potential candidates for their hacking capabilities."[3] Because of its success, RaaS is becoming a more prolific and advanced tool for attackers, particularly as more interest, and success, arise in the field.

The first instance of ransomware was reported in 1989 but became notable in 2012 when the Federal Bureau of Investigation (FBI) announced a "New Internet Scam", ransomware. This novel 'drive-by malware' would lock a victim's computer when a compromised file was downloaded by clicking a link on a fake website. To unlock the compromised computer, a victim was required to pay a "fine" using a prepaid money card service.[4] From 2012 to the present day, ransomware actors have evolved attack methods and payment methods to circumnavigate law enforcement and expedite the payments of ransomware.

Ransomware attackers move stolen funds, including cryptocurrency, in several different ways. For cryptocurrency, attackers extract funds from victims in one of two ways: high-risk exchanges or custodial crypto mixing services ("mixers"). According to financial forensics firms, a high-risk crypto exchange embodies little to no legal/regulatory compliance requirements. A

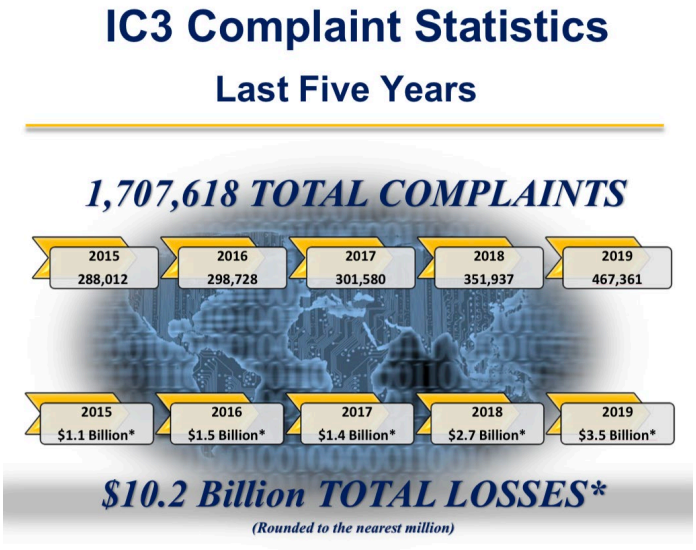
[2] Chainalysis 2021 Crypto Crime Report, page 28.
[3] Chainalysis 2024 Crypto Crime Report, page 17.
[4] FBI 2012 new report on ransomware, https://www.fbi.gov/news/stories/new-internet-scam/new-internet-scam

crypto mixer "blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds."[5] Crypto mixers are unique because cybercriminals can "clean" their stolen funds alongside genuine, non-criminals utilizing the platform, thus obfuscating connections between their illicit profit wallets and their wallets transferring funds from crypto-to-fiat currency exchanges.

Ransomware Over the Years: Then versus Now

Then: Cyber Landscape during the COVID-19 Era

"As the United States and the world grapple with the immediate public health and economic fallout of the coronavirus pandemic, a related crisis has simultaneously emerged: a wave of criminals seeking to prey upon an anxious public."[6]



[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2015 to 2019. Over that time period, IC3 received a total of 1,707,618 complaints, reporting a loss of $10.2 billion.

Since its inception, cyberspace has been exploited for illicit purposes and gain by bad actors such as nation-state adversaries, hackers, hacktivists, industrial spies, and cyber criminals.[7] While a persistent threat, a surge of cyberattacks against U.S. targets marked the COVID-19 pandemic. According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), "the number of cybersecurity complaints to the IC3 in the last four months had spiked from 1,000 daily before the pandemic to as many as 4,000 incidents in a day."[8] As shown in the adjacent figure, the increased number of cyber-crime reports during the COVID crisis are alone near the total reported amount of 2019 complaints.[9]

The financial services sector, already facing challenges of countering sophisticated cyber-criminals, experienced an increase in cyber-related crime during COVID-19. A May 2020 survey of financial institutions (FIs) found that 80 percent of surveyed banks reported a year-over-year increase in cyberattacks against the sector. According to the survey, attacks surged 238 percent at

[5] Chainalysis Team, "Crypto Mixers and AML Compliance," *Chainalysis,*23 August 2024.
[6] FBI and Secret Service Working Together Against COVID-19 Threats, *FBI News*, FBI website, 15 Apr 2020.
[7] McElroy, Foss, and Costis, 2020 Cybersecurity Outlook Report, *VMware Carbon Black*, Mar 2020.
[8] Maggie Miller, FBI sees spike in cybercrime reports during coronavirus pandemic, *The Hill*, 16 Apr 2020.
[9] 2019 Internet Crime Report, *FBI: Internet Crime Complaint Center (IC3) website*.

the start of the COVID-19 crisis (February- April 2020).[10] From there, the volume of attacks moved in synch with the COVID-19 news cycle – meaning, the more media reports of hysteria, the more bad actors and criminals preyed on peoples' fears. For example, the number of phishing emails increased with news reports.[11]

A review of ransomware trends in 2020 demonstrates the total value of attacks increased 311 percent, from $220 million in 2019 to $905M in 2020.[12] Ransomware saw the highest growth rate in crypto-based crime in the year of 2020. This coincides with a shift to remote work, during which time many people used unsecure networks and lacked proficient knowledge of cybersecurity preparedness and prevention measures.[13]

Now: Current Landscape of the Ransomware Ecosystem

Despite a downward trend in 2022, ransomware attacks, and their subsequent payments, surged in 2023. In fact, 2023 was the first year that ransomware payments exceeded $1 billion. By comparison, ransomware payments totaled $567 million in 2022 and $983 million in 2021.[14] According to Chainalysis, 2022 was "an anomaly, not a trend," and geopolitical events, like the outbreak of the Russia-Ukraine conflict, are credited for the decline in 2022. Nation state threat actors were occupied carrying out "politically motivated cyberattacks aimed at espionage and destruction" versus cyberattacks motivated by financial gain.[15] However, in 2023, threat actors shifted their focus and took greater risks by escalating their operations, strengthening, and rebranding existing ransomware strains. They also introduced new elements of intricacy into their attacks for maximum profit.

Ransomware is projected to remain the "primary extortion method through 2024."[16] This is in large part because ransomware actors are moving away from small scale attacks and focusing on more prolific, high-valued organizations – commonly referred to as "Cyber Big Game Hunting" (BGH). CrowdStrike, a leading cyber security and resiliency firm, reported that "victims are chosen based on their ability to pay a ransom, as well as the likelihood that they will do so in order to resume business operations or avoid public scrutiny."[17] In May 2021, BGH became a widely used term following the infamous Colonial Pipeline Co. cyberattack. Currently, banks and non-bank FIs, hospitals, government agencies, public corporations, and supply chain conglomerates are all targets for attacks.

---

[10] Tom Kellermann, R. Murphy, Modern Bank Heists 3.0, *VMware Carbon Black*, May 2020.
[11] *Ibid.*
[12] Chainalysis 2021 Crypto Crime Report, page 26.
[13] *Ibid.*
[14] Chainalysis 2024 Crypto Crime Report, page 12.
[15] *Ibid*, page 13.
[16] CrowdStrike's 2024 Global Threat Report, page 44.
[17] Lenaerts-Bergmans, "Cyber Big Game Hunting," *CrowdStrike*, 22 Feb 2024.

In September 2023, MGM Resorts and Caesars Entertainment were both victims of ransomware attacks. Caesars opted to pay $15 million of the $30 million ransom. However, MGM decided *not* to pay the ransom but suffered $110 million in revenue loss and operational damages. More recently, in February, Change Healthcare was victim to what is being recognized as, "one of the worst ransomware attacks in years."[18] Change Healthcare is one of the largest healthcare intermediaries of payments, digital offerings, and innovations. It serves as the interface between providers, payers, and consumers. Since the attack, the healthcare industry has been forced to reevaluate and reestablish every facet of its operational structure. This includes, but is not limited to, supply chain efficiencies, payment cycle management, and daily preventative cybersecurity readiness.

Additionally, threat actors are using the mandatory disclosure requirements to expediate ransomware payments. The new SEC cybersecurity disclosure rule, effective December 2023, requires SEC registrants to disclose a cyber security incident within 4-business days of the company deeming the event to be material to a reasonable investor. According to the SEC, cybersecurity incidents include both unauthorized occurrences and accidental occurrences that are not caused by a malicious attack.[19]

Savy ransomware actors are using mandatory disclosures to further pressure victim organizations to make ransomware payments. "BGH adversaries will increasingly emphasize stolen-data exploitation as a means to pressure victims into payment," including leaking the story to U.S. press and threatening to notify the SEC of the "material incident" before the four-day disclosure deadline.[20] According to ransomware response firms, the SEC rule, outlined below in greater detail, will continue to impact *when* and *why* organizations ultimately pay the ransom or not.

In addition, small/medium sized entities like municipal and state governments, state banks, local hospitals, and credit unions are easy targets for "in-and-out" ransomware attack operations. These quick hitting ransomware attacks are analogous to "smash and grab" heists where criminals are looking for quick and easy payouts. Attacks on these institutions are becoming more frequent, allowing for affiliates and ransomware operators to learn from mistakes and educate themselves on steps victims are taking to strengthen their cyber hygiene and defenses. According to the Conference of State Bank Supervisors, "ransomware is much more than a financial issue of paying a ransom or a fee to recover stolen data…[it] represents an

[18] Greenberg, "Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment," *Wired*, 4 Mar 2024.
[19] Bob Zukis, "Companies are Already Not Complying With the New SEC Cybersecurity Incident Disclosure Rules," *Forbes*, 4 Mar 2024.
[20] CrowdStrike 2024 Global Threat Report, page 44.

operational threat [to the financial sector] and, in some instances, a threat to the very survival of the institution."[21]

Legislation for Consideration

1. **H.J. Res. 100,** ***providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Securities and Exchange Commission relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."*** (Rep. Garbarino)

2. **H.R. _____,** the ***"Public and Private Sector Ransomware Response Coordination Act of 2024"***. (Rep. Nunn) [DRAFT]
    a. This legislation will require the Secretary of the Treasury to submit a report to Congress on cybersecurity coordination efforts. This includes both public and private coordination programs, as well as any reasoning behind possible delays of reporting information to the United States Government.

3. **H.R. _____,** the **"*Ransomware and Financial Stability Act of 2024*"** (Rep. Pettersen)
    a. This bill requires financial institutions to inform the Financial Crimes Enforcement Network of a ransomware attack and any associated demand of payment. Further, the institution may not make such a payment in an amount greater than $100,000 without authorization from the appropriate federal law enforcement agency. The President may waive the notification requirement if it is in the national interest.

[21] The Conference of State Bank Supervisors (CSBS), "Ransomware: Lessons Learned by Banks that Suffered an Attack."