Jeremy Sheridan
Assistant Director
Office of Investigations
United States Secret Service

U.S. Department of Homeland Security

Prepared Testimony
Before the
United States Senate
Committee on Judiciary

July 27, 2021

Good morning Chairman Durbin, Ranking Member Grassley, and members of this Committee: Thank you for inviting me to testify before you on the threat of ransomware and the risks it poses to the American people. My testimony today will seek to highlight how the ransomware environment has evolved in recent years, with attacks becoming more frequent, more hazardous, and more costly over time, and what the U.S. Secret Service and our partners across the Federal Government, and around the world, are doing to hold criminal actors accountable.

My name is Jeremy Sheridan and I am the Assistant Director of the Office of Investigations. In this role, I lead more than 160 Secret Service field offices and direct our network of Cyber Fraud Task Forces (CFTFs) in their investigations of sophisticated computer and financial crimes. I work to ensure our global network of field offices and task forces effectively detect and arrest those who are engaging in the criminal violations we are authorized to investigate,[1] while fully supporting our diverse protective requirements across the world.

Year-over-year, the U.S. Secret Service has observed a marked uptick in the frequency, sophistication, and destructiveness of ransomware attacks against the American people. While this surge is due to a number of complex and interrelated factors, we believe the principal forces driving it are 1) the swelling profitability of these attacks, in part as a result of the growth of cryptocurrencies as a form of extortion payment; 2) the lack of adequate defenses on the part of many U.S.-based organizations; and 3) perhaps most importantly, the maturation of a cybercriminal ecosystem that has grown more sophisticated and destructive over the decades, perpetrating increasingly brazen attacks.

There is no silver bullet for any of these contributing factors. We must recognize that ransomware will be with us for some time to come. But there is still much that we can do to improve the current situation.

- First, we must reduce the profitability of ransomware campaigns by scaling up law enforcement efforts to detect and interdict the proceeds of these extortion schemes.
- Second, we must work with private sector, state and local governments, and other vulnerable organizations to improve their own network defenses.
- Third, we must dramatically intensify national and international efforts to investigate, arrest, and prosecute those engaged in ransomware and other transnational cybercrimes.

Absent these combined efforts, I foresee an increase in both the severity and frequency of highly disruptive ransomware attacks. So long as greedy individuals lacking moral scruples can access the Internet, cybercrime will be with us. Even still, we can substantially reduce these harms by improving our collective defenses and by making cybercrime both less profitable and more risky to the criminals. I'm proud to say that the U.S. Secret Service stands ready to play our part in this effort.

The U.S. Secret Service Approach

The Secret Service has been at the forefront of combatting ransomware and related cybercrimes from their earliest iterations, and we continue this work today. Building upon our more than 150 years of experience fighting financial crimes, our approach has been, and continues to be, to "follow the money."

[1] *See* 18 U.S.C. §§ 1028-1030, and 3056(b).

We have investigated and arrested some of the world's most notorious cybercriminals, including many of whom were thought to be beyond the reach of law enforcement.[2]

Together with our partners, we have successfully investigated and ultimately shut down a number of illicit digital money providers and exchanges[3] that actively facilitated the laundering of transnational cybercriminal proceeds, including proceeds from ransomware. These include Liberty Reserve [4] in 2013 and BTC-e[5] in 2017, both of which have been accused of serving as key platforms for cybercriminals to transfer and launder proceeds through digital money.

With respect to ransomware specifically, the Secret Service has been investigating cases since at least 2013, when the ransomware variant known as CryptoLocker, the first known ransomware strain to leverage bitcoin as its extortion payment method, emerged on the cybercrime scene. At the time, ransomware attacks constituted only a small fraction of the overall cybercrime market. Ransom demands for CryptoLocker were typically low – often less than $300.[6]

Today, the situation has radically changed for the worse, as we all recognize. The average ransom demand has skyrocketed, according to industry estimates. Some ransomware groups are reportedly demanding as much as $10 million to $20 million to free their locked computer systems.[7] Ransomware actors are targeting not just big businesses with deep pockets, but also schools, city governments, and most tellingly, hospitals, even in the midst of a global pandemic.

The Secret Service has responded to ransomware attacks against a wide array of organizations, including municipalities and police departments. Our law enforcement partners around the nation share similar experiences. As the attacks on the Colonial Pipeline Company, JBS Foods, and Kaseya from this past year clearly reveal, these criminals will go to any length in their relentless pursuit of profit.

---

[2] See, "Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme," available at, https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme; "Russian National Admits Role in Largest Known Data Breach Conspiracy Ever Prosecuted," https://www.justice.gov/opa/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-prosecuted; "Russian National Pleads Guilty to Running Online Criminal Marketplace," https://www.justice.gov/usao-edva/page/file/1238961/download; "Ukrainian Citizen Sentenced To 41 Months In Prison For Using Army Of 13,000 Infected Computers To Loot Log-In Credentials, Payment Card Data," https://www.justice.gov/usao-nj/pr/ukrainian-citizen-sentenced-41-months-prison-using-army-13000-infected-computers-loot-log; "Ukrainian National Who Co-founded Cybercrime Marketplace Sentenced to 18 Years in Prison," https://www.justice.gov/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison.

[3] Exchanges are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as US dollars, or other digital currencies.

[4] *See* Manhattan District Attorney, "DA Vance Testimony on Digital Currency before the Department of Financial Services," https://www.manhattanda.org/da-vance-testimony-on-digital-currency-before-the-department-of-financial-services/.

[5] *See,* "Russian National and Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged."

[6] See, "CryptoLocker Ransomware," available at https://www.secureworks.com/research/cryptolocker-ransomware.

[7] *See*, "Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report," available at https://unit42.paloaltonetworks.com/ransomware-threat-assessments/.

Ransomware as an Evolution of Cybercrime

The evolution of ransomware from a relatively minor nuisance to a substantial threat to our homeland has been a gradual but steady process. Ransomware is just the latest and most pernicious trend to emerge out of a cybercriminal ecosystem that has been building in size and sophistication for decades.

The origins of ransomware can be traced back to the 1990s and early 2000s, when the vast majority of financially-motivated cybercrime – or "electronic crime," as the Secret Service called it at the time – was focused on the theft and sale of credit card numbers and personally identifiable information (PII). Cybercriminals would hack into an organization to steal its customer account data, including credit card numbers and PII, which would later be used to make fraudulent purchases, or to sell to other criminals to further other criminal schemes. This cycle of theft, sale, and resale of credit card numbers and PII created a vast underground digital marketplace, in which stolen account information or even access to a victim's computers could be bought and sold in a growing set of cybercriminal forums operating on the Internet.

As the marketplace matured, criminals began sharing best practices for hacking, laundering illicit proceeds, and avoiding detection by law enforcement. Cybercriminals who specialized in one particular area of cybercrime – such as network intrusion, malware development, or money laundering – began offering their products and services to others in exchange for a fee, or a percentage of the illicit proceeds of the scheme in which those products or services were to be used. Thus, the "crime-as-a-service" industry was born, an industry upon which much of today's ransomware environment depends.

This maturation coincided with, and in certain respects was the result of, two key technological developments. The first was the arrival of bitcoin as the first widely accepted cryptocurrency in 2009. Bitcoin, which is based on public-key cryptography and ongoing decentralized computation to form a blockchain, offered cybercriminals a novel means of accepting and transferring value, one that does always comply with the oversight and controls placed on traditional banking and financial systems.

Around the same time, we witnessed the second key technological development: the adoption of EMV chips by major U.S. and global credit card providers.[8] EMV chips, which require physical position of a card and an associated PIN number, made a variety of criminal schemes much more difficult to undertake. EMV adoption, while still ongoing to this day in the United States, served to dramatically reduce the profitability of credit card theft. It forced cybercriminals to look for alternative schemes. Many turned to ransomware, which, following the success of CryptoLocker in 2013, appeared to be the next "hot" criminal enterprise. And indeed it was.

Over the ensuing years, ransomware became increasingly sophisticated and professionalized. Today's ransomware gangs employ a vast array of specialists, from malware developers to human resources departments to public relations teams. They meticulously gather information on victim organizations and set extortion prices based on the information they collect. Gangs even employ encrypted text-over-the Internet chat services to facilitate communication between victims and ransomware operators, offer discounts for rapid payments, and charge penalties for payment delays by victims. Dozens of new ransomware strains have been developed and deployed against U.S. targets. These have been some of the

[8] See, "The President's BuySecure Initiative: Protecting Americans from Credit Card Fraud and Identity Theft," https://obamawhitehouse.archives.gov/blog/2014/10/17/president-s-buysecure-initiative-protecting-americans-credit-card-fraud-and-identity.

most destructive cyber-attacks in recent memory, such as Petya in 2016, WannaCry in 2017, and Darkside in 2021. Many new ransomware strains built upon those that came before them, adding layers of encryption and obfuscation, making defense and mitigation efforts far more challenging.

Alarmingly, ransomware actors also began experimenting with adding additional extortion demands, often referred to as "double extortion." Criminals now sometimes demand two separate ransom payments, the first to unlock a frozen computer network, and then a second to prevent the public disclosure of stolen information. Some are even extending this practice to "triple-extortion," adding denial-of-service attacks to further pressure victims of these extortion schemes.

Addressing the Ransomware Challenge

There are no easy answers to the ransomware challenge we face today. But it is abundantly clear that this fight will require a whole-of-government, and indeed a whole-of-society, approach. Cooperation and collaboration are and will remain vital.

Information Sharing and Timely Incident Reporting

As a starting point, there is a clear need for enhanced coordination between the government and industry, particularly as it relates to information sharing and incident reporting. This is an area where there has been notable progress in recent years, in no small part due to the passage of the Cybersecurity Information Sharing Act of 2015 (CISA 2015), which offered certain liability protections to companies that share threat information with the U.S. Government.

But, CISA 2015 should be viewed as just a foundation. The U.S. Government needs access to timely, actionable information. If victim companies fail to report ransomware attacks early, or if they fail to report them at all, it hinders law enforcement's ability to assist them with asset recovery orto prevent future incidents.

Accordingly, it remains worth considering whether there may be opportunities to establish additional incentives and/or requirements to strengthen this reporting process. Determining the exact contours of such programs will take time. However, the current status quo, in which firms have limited motivation to work with the government, may prove unsustainable in the long term.

Organizational Defenses, Cyber Hygiene, and Enterprise Network Security

But information sharing and reporting is just part of the puzzle. It is something we have been saying for years, but it is worth restating: every organization, big or small, public or private, must implement basic cybersecurity hygiene and best practices. Even simple steps – such as keeping operating systems, software, and applications up-to-date and patched, or making sure that anti-virus and anti-malware solutions automatically update and run regular scans can significantly raise an organization's defensive posture. Organizations should be encouraged to configure their enterprise networks to defend against, or at least mitigate, some of the worst harms of these attacks.

While many larger organizations have been able to design their systems effectively in this regard, many smaller and less well-resourced organizations have not been so well prepared and have suffered as a result. I'd like to commend the Cybersecurity and Infrastructure Security Agency (CISA) and our partners throughout the Department of Homeland Security (DHS) for their efforts in this regard. Specifically, the

DHS "Ransomware Sprint" [9] provided essential advocacy and support within DHS on these issues, and CISA's "Stop Ransomware" campaign[10] has been instrumental in providing guidance to industry to strengthen their own defenses and to effectively communicate with U.S. law enforcement. I believe more needs to be done along these lines to ensure that all U.S. organizations have the information needed to build resilient systems that can withstand a sophisticated ransomware attack.

Cyber Insurance

The insurance industry will likely play a key role in both enhancing incident reporting and raising organizational defenses. Cyber insurance is becoming a crucial element in response to a range of cybersecurity incidents, including ransomware attacks. The insurance sector and federal government can and must work collaboratively to encourage cyber insurance policyholders to improve security and avoid the hazard of financing the growth of transnational cybercrime.

Public and private sector stakeholders have a shared interest in a vibrant cyber insurance market that facilitates both cyber risk reduction and action to advance our Nation's cybersecurity. Sharing timely incident information with the government is critically important, as it facilitates the availability of federal response support (including, as appropriate, cybersecurity and law enforcement resources) to the impacted entity. It also enables the government to issue warnings and indicators to other potential victims. We continue to examine how we can best engage with the cybersecurity insurance industry.

Domestic and International Partnerships

Catching cybercriminals is a team sport, and partnerships form the bedrock of all of the Secret Service's investigative work. Specifically, within the Executive Branch, we work hand-in-hand with the Department of Justice (e.g., the Federal Bureau of Investigation, the Office of International Affairs, U.S. Attorney's Offices, and the Computer Crime and Intellectual Property Section), the Department of State (e.g., the Bureau for International Narcotics and Law Enforcement Affairs), and the Department of Treasury (e.g., the Financial Crimes Enforcement Network and the Office of Foreign Assets Control). We coordinate and deconflict our ransomware cases through the National Cyber Investigations Joint Task Force (NCIJTF), where we lead the Criminal Mission Center.

Within our own Department of Homeland Security, we closely partner with CISA to share cybersecurity alerts and best practices, and conduct joint criminal investigations with Immigration and Customs Enforcement (ICE) - Homeland Security Investigations. We also work with State, Local, Tribal, and Territorial (SLTT) partners to assist them with their local investigations, in addition to a variety of private sector and non-government groups, such as the National Cyber-Forensics and Training Alliance (NCFTA) and Ransomware Task Force (RTF).

Our foreign partners perform critical roles in assisting U.S. law enforcement with conducting investigations, making arrests, and seizing criminal assets.

Fostering overseas partnerships helps to develop a shared understanding of risks, to ensure timely legal assistance, and to support effective international anti-money laundering (AML) regulatory and enforcement programs. The Secret Service has been highly successful at partnering with other countries

[9] See, "Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience," https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience.
[10] See, "Stop Ransomware," https://www.cisa.gov/stopransomware.

on these issues, working collaboratively to arrest transnational cyber criminals when they travel. We at the Secret Service continue to build the relationships necessary for effective enforcement operations.

Focusing on Financial Transactions

As noted above, cryptocurrency is often used to facilitate cybercrime, allowing for instant, pseudo-anonymous extortion payments and money laundering operations. But cryptocurrencies have their limitations. To be utilized within the mainstream economy – namely, to exchange them for most goods or services – cryptocurrencies must generally be converted into government-backed fiat currency, such as the U.S. dollar, European Euro, or Chinese Yuan. This conversion typically occurs through "exchanges," financial services which allow for the purchase and sale of digital assets with fiat currency.

Exchanges have been particularly effective control points for governments to focus their efforts, both as on-ramps and off-ramps to the cryptocurrency economy. However, as the variety of digital assets increases, further attention is needed to address the risks of services that obscure digital transactions from law enforcement and regulatory oversight. Ransomware actors and those that support them persistently seek to avoid U.S. and foreign AML and know-your-customer (KYC) requirements by using exchanges that do not adhere to these laws or reporting requirements. Criminals are also increasingly exploiting over-the-counter (OTC) brokers, which facilitate transactions conducted directly between two parties through bilateral contracts.

Accordingly, it is vital that AML and KYC laws achieve their intended effects, regardless of the bad actor's motivations for exploiting them. The enactment of the Anti-Money Laundering Act of 2020 (AML 2020) was an important step in this direction. However, enhanced data reporting, collection, retention, and accessibility requirements may strengthen criminal investigations and effective oversight.

Workforce Development

Finally, combatting ransomware requires highly skilled criminal investigators. Hiring, developing, retaining, and equipping our investigative workforce is absolutely essential, as are programs to train our domestic and foreign law enforcement partners to develop their own investigative capabilities. This can be achieved by strengthening law enforcement training and capacity building programs that equip Federal law enforcement, and our partners, with the technical skills and tools necessary to pursue the most sophisticated transnational criminals.

Conclusion

It does us no service to sugarcoat the reality of today's situation: the cybercriminals are emboldened and getting stronger. Ransomware is menacing our economy and our institutions. Cybercriminals are using ransomware to make more money and do more harm ever before.

Progress is possible, as the success of the Secret Service and our partners has demonstrated, but it will take a continued commitment to make it clear that such purely criminal and destructive activities are unacceptable. I'm grateful for the support of Congress and our many partners, at home and abroad, for joining us in saying, "enough is enough."

Thank you again for your continued support for the mission of the U.S. Secret Service, and your work on these important issues. I look forward to working closely with this Committee, and with other Members of Congress, on our shared priorities.