

To: Members of the National Security Council
From: Adalberto Trujillo
Subject: Nation-State Ransomware Attacks



Memorandum: Nation-State Ransomware Attacks

Executive Summary

Ransomware is a form of malware that encrypts files on a network-connected device, making them unusable and disrupting the other systems that rely on them. Due to the growing nature of the threat, ransomware has become more destructive, shutting down businesses and critical infrastructure across the United States.

Ransomware is a threat to national security. The FBI's Internet Crime Complaint Center (IC3) received approximately 2,474 complaints identified as ransomware, with reported losses of over \$29.1 million, in its 2020 annual report.¹ That total reflects only what victims chose to report. Over the same year, financial institutions reported \$416 million in ransomware-related payments to the Treasury Department, and another \$590 million in the first six months of 2021 alone.²

The federal response so far — sanctions against ransomware operators and the virtual currency exchanges that launder their proceeds, indictments and asset seizures by the Department of Justice, and new coordination bodies at CISA — has imposed real costs on individual actors. It has not reduced the volume of attacks, reached the actors who remain inside Russia, or changed the calculation that leads victims to pay quietly and report late or not at all.

I recommend that the Council prioritize three actions: first, require critical infrastructure owners and operators to report ransomware incidents and ransom payments to the federal government on a fixed deadline, with penalties for failing to do so; second, expand Treasury designations and anti-money laundering enforcement against the exchanges and over-the-counter desks that convert ransom payments into usable funds; and third, drive zero trust adoption into the private sector, extending the standard the federal government has already set for its own agencies. These and the remaining recommendations are set out at the end of this memo.

Assessment of the Threat and Severity of the Problem

The most damaging attacks of the past year were carried out by criminal enterprises operating from jurisdictions that shelter them. DarkSide was behind the May 2021 attack on Colonial Pipeline, which took a major fuel pipeline out of operation and caused shortages across the East Coast. REvil, also known as Sodinokibi, was behind the attacks on JBS and on Kaseya, the second of which spread through a single software provider to businesses worldwide. Evil Corp, sanctioned by the Treasury Department in 2019, continues to operate from Russia. These groups are not state units, but the protection they enjoy

¹"2020 Internet Crime Report," Federal Bureau of Investigation, Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

²Financial Crimes Enforcement Network, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," October 15, 2021, https://www.fincen.gov/system/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

makes them a state problem: Russia does not extradite its nationals, and the charged individuals who remain inside its borders are effectively beyond the reach of prosecution.³

Ransom payments sustain the ecosystem. The Office of Foreign Assets Control has warned that facilitating a payment demanded as a result of malicious cyber activity may enable criminals and adversaries to profit and advance their illicit aims.⁴ Payments fund the next round of operations and confirm that the business model works, which invites further attacks.

Underreporting hides the scale of the problem and slows the federal response. Businesses decline to notify law enforcement in order to protect their reputations or avoid scrutiny, and those that do report often wait weeks. The Ransomware Task Force concluded that the true cost and scope of ransomware cannot be measured because many victims never come forward, and directed a substantial share of its recommendations at fixing incident reporting.⁵ The gap is visible inside the government's own data: IC3 recorded \$29.1 million in ransomware losses for all of 2020, while the Treasury Department's Financial Crimes Enforcement Network identified \$416 million in ransomware-related payments reported by financial institutions over the same period.⁶ Two federal datasets describing the same crime differ by more than a factor of ten, and the larger of the two captures only payments that passed through a regulated financial institution.

Current Measures in Place and Their Effectiveness

Sanctions authorities. The International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act prohibit engaging in transactions, directly or indirectly, with sanctioned individuals or with those covered by comprehensive country or regional sanctions.⁷ Treasury has begun applying that authority to ransomware infrastructure rather than to operators alone, designating the over-the-counter exchange SUEX in September 2021 — the first virtual currency exchange ever sanctioned⁸ — and the exchange Chatex, its support network, and two REvil affiliates that November.⁹ The effect so far is narrow. However, private business entities still pay the ransom, and designation moves more slowly than the market it targets: Chatex had been routing transactions through SUEX and was designated roughly seven weeks later.

Indictments and seizures. The Department of Justice and the FBI have charged ransomware actors and recovered funds. In June 2021 the Department seized 63.7 bitcoin, then worth approximately \$2.3 million, from the ransom Colonial Pipeline paid to DarkSide.¹⁰ In November 2021 it unsealed charges against Yaroslav Vasinskyi, arrested in Poland at U.S. request and held pending extradition, and against

³Maggie Miller, "New Hacking Efforts Show Russia Undeterred by US Actions," The Hill, October 25, 2021, <https://thehill.com/policy/cybersecurity/578367-new-hacking-efforts-show-russia-undeterred-by-us-actions>.

⁴"Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Office of Foreign Assets Control, U.S. Department of the Treasury, September 21, 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

⁵Institute for Security and Technology, Ransomware Task Force, "Combating Ransomware: A Comprehensive Framework for Action," April 2021, <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf>.

⁶FinCEN, "Financial Trend Analysis," 3; IC3, "2020 Internet Crime Report," 21.

⁷OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments."

⁸"Treasury Takes Robust Actions to Counter Ransomware," U.S. Department of the Treasury, September 21, 2021, <https://home.treasury.gov/news/press-releases/jv0364>.

⁹"Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," U.S. Department of the Treasury, November 8, 2021, <https://home.treasury.gov/news/press-releases/jv0471>.

Yevgeniy Polyanin, seizing \$6.1 million traceable to Polyanin's ransom proceeds.¹¹ Those two cases show both the value and the limit of this tool: it works when a suspect travels to a cooperating jurisdiction or moves money through infrastructure U.S. law enforcement can reach. Polyanin is believed to be abroad and has not been arrested. Against actors who stay inside Russia, an indictment functions as a travel restriction rather than a prosecution.

Task forces and international operations. The FBI's Ransomware and Digital Extortion Task Force and its foreign partners have disrupted several criminal enterprises; REvil's operations were interrupted in the fall of 2021, and Romanian authorities arrested two additional affiliates alongside the November indictments.¹² Disruption of this kind is real but reversible. Operators rebrand and reconstitute, and researchers have tied REvil itself to the operators of the earlier GandCrab strain.¹³

Guidance and coordination. CISA's Stop Ransomware initiative consolidates federal guidance on preventing and responding to attacks,¹⁴ and the Joint Cyber Defense Collaborative brings public and private sector partners together to plan against them.¹⁵ Both are worth sustaining, but both are voluntary and neither has operated long enough to evaluate. Neither creates an obligation to report an incident, which is where the data gap described above originates.

Recommendations

The following actions are recommended, in order of priority:

- **Require reporting.** Critical infrastructure owners and operators should be required to report ransomware incidents to CISA and the FBI within 72 hours, and any ransom payment within 24 hours, with penalties for non-compliance. Voluntary reporting has not closed the gap between what victims experience and what the government can see. Mandatory reporting legislation is pending before Congress, and the Council should support a version that covers payments and not only incidents.
- **Expand Treasury action against the cash-out layer.** Continue designating the exchanges, kiosks, and over-the-counter desks that launder ransom proceeds, and press for consistent know-your-customer and anti-money-laundering requirements across that sector so that designations are not simply outrun by successor services.
- **Cut non-compliant exchanges off from the U.S. banking system.** Direct federal banking regulators to require enhanced due diligence on virtual currency exchanges and to restrict relationships with those that cannot demonstrate compliance with know-your-customer and anti-money-laundering obligations.

¹⁰"Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," U.S. Department of Justice, June 7, 2021, <https://www.justice.gov/archives/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

¹¹"Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," U.S. Department of Justice, November 8, 2021, <https://www.justice.gov/archives/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>.

¹²"Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," U.S. Department of Justice.

¹³Chainalysis Team, "P2P Cryptocurrency Exchange Chatex and Two Russian Nationals Indicted and Sanctioned for Roles in Ransomware Operations," Chainalysis, November 8, 2021, <https://www.chainalysis.com/blog/ofac-sanction-chatex-revil-sodinokibi-november-2021/>.

¹⁴"CISA Stop Ransomware: General Information," Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/stopransomware/general-information>.

¹⁵"Joint Cyber Defense Collaborative," Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/jcdc>.

- **Drive zero trust adoption into the private sector.** Businesses and organizations should move to a zero trust model that requires continuous verification from multiple sources rather than trust based on network position.¹⁶ Federal agencies are already committed to this model under Executive Order 14028; critical infrastructure sectors should be held to the same standard through their sector risk management agencies.
- **Build geopolitical context into private sector risk planning.** Owners and operators should understand which actors target their sector, where those actors are based, and how U.S. policy toward those countries shapes their exposure, rather than treating ransomware as an undifferentiated criminal risk.

Bibliography

"2020 Internet Crime Report," Federal Bureau of Investigation, Internet Crime Complaint Center.
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Chainalysis Team. "P2P Cryptocurrency Exchange Chatex and Two Russian Nationals Indicted and Sanctioned for Roles in Ransomware Operations." Chainalysis, November 8, 2021.
<https://www.chainalysis.com/blog/ofac-sanction-chatex-revil-sodinokibi-november-2021/>.

"CISA Stop Ransomware: General Information." Cybersecurity and Infrastructure Security Agency.
<https://www.cisa.gov/stopransomware/general-information>.

"Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." U.S. Department of Justice, June 7, 2021.
<https://www.justice.gov/archives/opa/pr/departement-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

"Embracing a Zero Trust Security Model." National Security Agency, February 2021.
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

Financial Crimes Enforcement Network. "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021." U.S. Department of the Treasury, October 15, 2021. https://www.fincen.gov/system/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

Institute for Security and Technology, Ransomware Task Force. "Combating Ransomware: A Comprehensive Framework for Action," April 2021. <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf>.

"Joint Cyber Defense Collaborative." Cybersecurity and Infrastructure Security Agency.
<https://www.cisa.gov/jcdc>.

Miller, Maggie. "New Hacking Efforts Show Russia Undeterred by US Actions." The Hill, October 25, 2021. <https://thehill.com/policy/cybersecurity/578367-new-hacking-efforts-show-russia-undeterred-by-us-actions>.

"Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange." U.S. Department of the Treasury, November 8, 2021. <https://home.treasury.gov/news/press-releases/jy0471>.

¹⁶"Embracing a Zero Trust Security Model," National Security Agency, February 2021,
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

"Treasury Takes Robust Actions to Counter Ransomware." U.S. Department of the Treasury, September 21, 2021. <https://home.treasury.gov/news/press-releases/jy0364>.

"Ukrainian Arrested and Charged with Ransomware Attack on Kaseya." U.S. Department of Justice, November 8, 2021. <https://www.justice.gov/archives/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>.

"Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." Office of Foreign Assets Control, U.S. Department of the Treasury, September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.