COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

July 16, 2021

To: Subcommittee on Oversight and Investigations Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on "Stopping Digital Thieves: The Growing Threat of Ransomware"

On **Tuesday, July 20, 2021, at 10:30 a.m. (EDT), in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco WebEx online video conferencing**, the Subcommittee on Oversight and Investigations will hold a hearing entitled, "Stopping Digital Thieves: The Growing Threat of Ransomware." The hearing will examine the growing threats posed by ransomware to U.S. businesses and critical infrastructure and will discuss recommendations for combatting those threats.

I. BACKGROUND ON RANSOMWARE

Ransomware is malicious software designed to encrypt files on a device, resulting in the affected files, data, and software being unusable until a ransom payment is made in exchange for a decryption key.[1] The tactics of malicious actors have evolved beyond simple encryption on a particular device, often targeting entire organizational networks with the intent of disrupting business operations, stealing data, and threatening public release in order to further encourage payment.[2]

Locking down computer networks (and stealing related data) through the application of ransomware has evolved into a sophisticated criminal industry involving a complex supply chain, gangs of cyber criminals, and sometimes even foreign governments.[3] A number of the most active cybercriminal gangs are believed to operate from Russia and other countries that

---

[1] U.S. Cybersecurity & Infrastructure Security Agency, *Ransomware Guide* (Sept. 2020) (www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf).

[2] *Id*.

[3] U.S. Cybersecurity & Infrastructure Security Agency, Ransomware FAQs: What is ransomware and how do malicious cyber actors use ransomware to attack their victims (www.cisa.gov/ransomware) (accessed July 7, 2021); Institute for Security & Technology, *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, at 16 (Apr. 2, 2021).

have demonstrated a reluctance to prosecute activities that cause harm outside of their borders.[4]

Ransomware is commonly introduced by exploiting vulnerabilities in an organization's information technology system or by tricking users into visiting a malicious website or downloading malicious software (e.g., phishing).[5] Once a network has been infiltrated, the malicious actors will often remain hidden within the system for some time, gather information on the target, identify and exfiltrate sensitive or critical data, and spread throughout the network before launching the actual ransomware attack.[6] After the attack has been launched, a message typically appears on affected devices demanding payment—almost always requiring payment in difficult-to-trace and easily transferrable cryptocurrency—in order to decrypt affected files and restore access to the network.[7]

In recent years, cyber criminals have developed a ransomware as a service ("RaaS") business model, which has significantly lowered the barrier to entry into the ransomware industry.[8] Malicious actors no longer require technical coding expertise in order to carry out attacks.[9] Rather, the bad actors can simply license ransomware from a malware developer, typically for a flat fee or a share of the ransom payment. Other service providers in the supply chain offer additional support, such as those selling information on potential targets and vulnerabilities to exploit, or providing cryptocurrency brokering and laundering services.[10]

II. RECENT ATTACKS UNDERSCORE A BROAD SCOPE OF VULNERABILITY

Low barriers to entry and the increasing interconnectedness of business and operational networks—including the proliferation of remote work accelerated by the coronavirus disease of 2019 (COVID-19) pandemic—have contributed to an increased number of ransomware attacks

---

[4] *Code in huge ransomware attack written to avoid computers that use Russian, says new report*, NBC News (July 7, 2021); *Secret Chats Show How Cybergang Became a Ransomware Powerhouse*, The New York Times (June 3, 2021).

[5] Institute for Security & Technology, *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, at 11 (Apr. 2, 2021); National Cyber Investigative Joint Task Force, *Ransomware: What It Is & What To Do About It* (Jan. 2021) (www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf).

[6] Institute for Security & Technology, *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, at 11 (Apr. 2, 2021).

[7] *Id*. at 11.

[8] *Id*. at 16.

[9] *Id*. at 16.

[10] Id. at 16; *Biden Tells Putin To Crack Down On Ransomware. What Are The Odds He Will?*, NPR (June 17, 2021).

in recent years.[11] Experts warn that critical infrastructure industries, which rely on networked industrial control systems such as the water, pipeline, and electricity sectors, are at high-risk for cybersecurity and ransomware attacks.[12]

For example, the May 2021 attack on Colonial Pipeline's information technology system resulted in a days-long shutdown of the entire pipeline.[13] This led to delivery delays, gas shortages, and sky-rocketing gasoline prices due to panic buying, despite Colonial Pipeline's early decision to pay the ransom.[14] A portion of the approximately $4.3 million ransom payment, which was made in bitcoin, was ultimately recovered and returned to Colonial Pipeline by the Federal Bureau of Investigation.[15]

Similar concerns exist in other critical infrastructure and sensitive industries, such as the food, healthcare, financial, and insurance sectors.[16] According to data published by the Department of Health & Human Services (HHS) Cybersecurity Program, ransomware impacted more than 560 healthcare organizations in 2020.[17] Those attacks resulted in delays in critical patient treatment, lost medical records, and hundreds of staff furloughs.[18] Similarly, a number of insurance companies, including those providing cyber insurance coverage, have been targeted and extorted through the theft of sensitive customer data.[19] In some instances, the malicious actors have stolen lists of cyber insurance customers and their coverage terms, which they then use to target customers and tailor ransom negotiations.[20]

Most recently, the Russian-language cybercriminal group REvil claimed responsibility for one of the largest ransomware attacks to date—an attack on an IT solutions software company, Kaseya, which quickly spread to thousands of organizations.[21] REvil is also widely believed to be responsible for the $11 million attack against JBS, the world's largest meat

---

[11] *How remote work opened the floodgates to ransomware*, The Guardian (June 17, 2021); *Secret Chats Show How Cybergang Became a Ransomware Powerhouse*, The New York Times (June 3, 2021).

[12] *Hackers have a devastating new target*, CNN (June 4, 2021).

[13] *U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021).

[14] *Id*.

[15] *Feds recover more than $2 million in ransomware payments from Colonial Pipeline hackers*, The Washington Post (June 7, 2021).

[16] *Hackers have a devastating new target*, CNN (June 4, 2021).

[17] U.S. Department of Health and Human Services, *2020: A Retrospective Look at Healthcare Cybersecurity* (Feb. 18, 2021) (Report #: 202102181030).

[18] *Id*.

[19] *In crosshairs of ransomware crooks, cyber insurers struggle*, Associated Press (July 5, 2021).

[20] *Id.*

[21] *The Kaseya ransomware attack: Everything we know so far*, ZDNet (July 7, 2021).

producer, earlier this year.

Finally, the size of ransom payments is also growing. A recent report found that the average ransomware payment made by an organization reached $312,493 in 2020—a more than 170 percent increase over 2019.[22] The full scale of the problem remains unknown due to many victims' reluctance to report attacks and payments made.[23]

III. POLICIES AND ACTIONS TAKEN TO ADDRESS RANSOMWARE

The broad scale and scope of recent attacks demonstrate the real-world impacts and vulnerabilities associated with ransomware, which have led to discussions of several potential policy approaches. These include requiring mandatory reporting of cyberattacks,[24] prohibiting ransom payments,[25] increasing cybersecurity requirements in regulated industries,[26] requiring additional transparency into cryptocurrency transactions and exchanges,[27] and evaluating the role of cyber insurance companies in ransom-payment consideration and prevention of attacks.[28]

The Biden Administration has identified ransomware as a national security threat[29] and describes its ransomware strategy to include "disruption of ransomware infrastructure and actors by working closely with the private sector; international cooperation to hold countries who harbor ransom actors accountable; expanding cryptocurrency analysis to find and pursue

---

[22] *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, Bloomberg (May 20, 2021); *see also, Highlights from the 2021 Unit 42 Ransomware Threat Report*, Unit 42 (Mar. 17, 2021).

[23] *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, Bloomberg (May 20, 2021).

[24] *Senate Intel chairman calls for mandatory reporting of hacks after Colonial Pipeline attack*, CNBC (May 12, 20121).

[25] *The Cybersecurity 202: Cybersecurity pros are split on banning ransomware payments*, The Washington Post (May 21, 2021).

[26] *The Cybersecurity 202: Our expert network says it's time for more cybersecurity regulations*, The Washington Post (June 11, 2021).

[27] *Government and industry push bitcoin regulation to fight ransomware scourge*, CNBC (April 28, 2021).

[28] Institute for Security & Technology, *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, at 13 (Apr. 2, 2021).

[29] Department of Homeland Security, *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience* (March 31, 2021); *Biden sees ransomware attacks as rising national security concern*, Reuters (June 4, 2021).

criminal transactions; and the federal government's review to build a cohesive and consistent approach towards ransom payments."[30]

On May 12, 2021, President Biden issued an executive order aimed at "modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur."[31] The President has also addressed the issue internationally, leading commitments on ransomware last month during the G7 conference and subsequently pressuring Russian President Vladimir Putin to rein in the cybercriminals working within Russia's borders.[32] Following another major attack by the Russian-language group REvil, President Biden again addressed the issue with President Putin.[33] President Biden reportedly "underscored the need for Russia to take action to disrupt ransomware groups operating in Russia" and "reiterated that the United States will take any necessary action to defend its people and its critical infrastructure."[34]

In addition to the President's actions, a number of federal agencies have taken steps to address the threat. For example, the Department of Justice (DOJ) formed a ransomware task force in April 2021 focused on developing a strategy to disrupt the criminal ecosystem.[35] DOJ also recently issued internal guidance that reportedly "elevat[es] investigations of ransomware attacks to a similar priority as terrorism."[36] The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) has initiated a series of 60- and 100-day sprints in conjunction with the Department of Energy, other relevant agencies, and private industry focused on critical cyber issues, including ransomware, the electrical grid, industrial control systems, and pipelines.[37] In response to the Colonial Pipeline attack, the DHS Transportation Security Administration issued updated cybersecurity rules for pipelines and

---

[30] The White House, *Readout of Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger's Meeting with Bipartisan U.S. Conference of Mayors* (July 6, 2021).

[31] The White House, *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks* (May 12, 2021) (press release).

[32] *Id.*; *U.S.-Russia Summit: Biden Tells Putin "Critical Infrastructure Should Be Off-limits" to Cyberattacks*, CISO Mag (June 17, 2021).

[33] The White House, *Readout of President Joseph R. Biden, Jr. Call with President Vladimir Putin of Russia*, (July 9, 2021).

[34] *Id.*

[35] *Ransomware Targeted by New Justice Department Task Force*, The Wall Street Journal (Apr. 21, 2021).

[36] *U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021).

[37] Department of Homeland Security, *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience* (March 31, 2021); Department of Energy, *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats* (April 20, 2021).

liquefied natural gas facilities, including mandatory incident reporting requirements, and indicated additional mandatory measures may be forthcoming.[38]

Most recently, the Administration launched the StopRansomware.gov website, which provides a one-stop hub of ransomware resources to assist individuals and businesses in protecting their networks and responding to ransomware incidents.[39] The Administration also announced the Rewards for Justice program, which will provide up to $10 million for information that leads to the identification or location of state-sponsored cyberactivity against key infrastructure.[40]

V. WITNESSES

The following witnesses have been invited to testify:

Kemba Walden
Assistant General Counsel
Microsoft Corporation

Robert M. Lee
Chief Executive Officer
Dragos

Christian Dameff, M.D., M.S.
Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate)
University of California San Diego
Medical Director of Cybersecurity
UC San Diego Health

Charles Carmakal
Senior Vice President and Chief Technical Officer
FireEye-Mandiant

Philip Reiner
Chief Executive Officer
Institute for Security and Technology

---

[38] U.S. Department of Homeland Security, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (May 27, 2021) (press release).

[39] U.S. Cybersecurity & Infrastructure Security Agency, *New StopRansomware.gov website – The U.S. Government's One-Stop Location to Stop Ransomware* (July 15, 2021) (press release).

[40] U.S. Department of State, *Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure* (July 15, 2021) (media note).