2022

Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware.

John Keary

Introduction

"America's computers are under attack and every American is at risk," [1] warned Congressman Michael McCaul in 2012, when he served as Chairman of the Homeland Security Committee. Congressman McCaul proclaimed that the U.S. Government, critical infrastructures, American business institutions, and personal data had all been compromised by various nation-states and hacker groups.[2] These groups of malicious actors aim to conduct cyber warfare on the United States, attacking infrastructure, stealing intellectual property, conducting espionage, and gaining access to individuals' sensitive private information.[3]

According to the 2021 Annual Threat Assessment published by the Office of the Director of National Intelligence, "cyber threats from nation-states and their surrogates will remain acute."[4] Russia, China, Iran, and North Korea remain the most prevalent cyber threat to the United States.[5] Additionally, other foreign cybercriminals that target the United States maintain a mutually beneficial relationship with these nations, which offer them a safe haven from, or benefits for their criminal activity.[6] States are currently increasing their use of cyber operations as a tool of national power.[7] How the United States and the current administration choose to deal with that fact will have profound impacts well beyond the borders of North America.[8]

---

[1] America is Under Attack: Why Urgent Action is Needed: Hearing Before the Subcomm. On Oversight, Investigations, and Management, 112 Cong. (2012) (Statement of Michael McCaul).
[2] *Id.*
[3] *Id.*
[4] OFFICE OF THE DIR. OF NAT'L. INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY, 20, (2021).
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *Id.*

Among the categories of cybersecurity, ransomware is one that should currently garner an increase in resources and attention due to the significant uptick in attacks.[9] Ransomware is a type of malware that encrypts a user's files or locks the user's system by keeping and taking their files hostage.[10] In exchange for access to the locked files or system, malicious actors demand a ransom in exchange for decryption.[11] If the ransom goes unpaid, it is likely that either the price demanded by the malicious actors will increase, the files will be rendered useless, or sensitive information will be leaked to the public.[12]

As the Biden Administration begins its second year in office, there is hope in the cybersecurity community. President Biden has promised to make cybersecurity one of the top priorities for the Administration.[13] The United States has been bombarded by malicious actors seeking to cause daily disruptions and extort American people and businesses.[14] Russia is a major source for many of the ransomware attacks that affect the United States and its allies.[15] This is in large part due to the "hands-off" approach taken by Moscow regarding the network of hackers who reside in Russia. [16] Without help from the Russian government, fighting against ransomware will continue to be a treacherous uphill battle.

---

[9] Tara Seals, *Ransomware Volumes Hit Record Highs as 2021 Wears On*, THREATPOST, Aug. 4, 2021, https://threatpost.com/ransomware-volumes-record-highs-2021/168327/.
[10] Faizan Ullah, et al., *Modified Decision Tree Technique for Ransomware Detection at Runtime through API Calls*, 2020 Hindawi 1, (2020), https://www.hindawi.com/journals/sp/2020/8845833/.
[11] *Stop Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/stopransomware (last visited Oct. 16, 2021).
[12] *Id*.
[13] Fact sheet: *Biden Administration and private sector leaders announce ambitious initiatives to bolster the nation's cybersecurity*, THE WHITE HOUSE (Aug. 25, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.
[14] *Id*.
[15] *See generally* Samara Lynn & Catherine Thorbecke, *Why ransomware cyberattacks are on the rise*, ABC NEWS (Jun. 4, 2021), https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650.
[16] Katie Canales, *Experts say Russia gives hackers a 'tacit blessing' to attach foreign nations – as long as they don't target Russia or its allies*, BUSINESS INSIDER, Jun. 15, 2021, https://www.businessinsider.com/russia-safe-haven-hackers-cybercriminals-putin-ransomeware-blessing-2021-6.

In May 2021, the United States was hit by two high-profile ransomware attacks.[17] One attack was on Colonial Pipeline ("Colonial"), the largest fuel pipeline in the United States.[18] The second attack was on JBS USA ("JBS"), the world's largest meat-packing company which handles twenty percent of all the cattle and hog slaughtered in the United States.[19] Within just weeks of each other, the United States had both their fuel and food supplies hacked by ransomware actors. Furthermore, both attacks were carried out by Russian cyber gangs, and both attacks ended in the ransom being paid via crypto currency.[20] These attacks should be used as a learning moment to better prepare for the future fight against ransomware.

The United States should use the Colonial Pipeline and JBS hacks as a guide in formulating potential strategies to minimize or prevent similar attacks in the future. Since both hacks were the product of Russian gangs, the United States must take action by putting pressure on President Putin to begin cracking down on the Russian cyber gangs operating within his borders. Furthermore, the United States can begin to target and sanction the virtual currency exchanges that cybercriminals use to receive their ransom payment. Finally, there should be additions made to existing cybersecurity legislation in the form of mandatory trainings for businesses that would directly mitigate the human error involved in allowing these types of attacks to occur. In support of this claim, this paper will be broken down into three sections. The first section will be an introduction to ransomware that provides a brief history of the topic and examines the JBS and Colonial Pipeline attacks. The second section will look at past legislative

[17] Frank Bajak, *Ransomware, Explained: How the Gangs That Shut Down Colonial Pipeline, JBS USA operate*, USA TODAY, Jun. 3, 2021, https://www.usatoday.com/story/tech/2021/06/03/how-does-ransomware-work-colonial-pipeline-jbs-usa-attacks-explainer/7520704002/.
[18] *Id*.
[19] *Id*.
[20] *Id*.

and executive actions taken by the United States in an effort to suppress ransomware attacks. The final section will expand on the three posed suggestions for dealing with ransomware.

I. WHAT IS RANSOMWARE

Ransomware is malware that employs data encryption to hold a victim's information at ransom. [21] The criminal actor or actors will encrypt an individual's or an organization's data, making it impossible for them to access their files, databases, or applications. [22] In exchange to regain access to the data, a ransom is requested by the hackers. If the ransom goes unpaid, ransomware actors will often threaten to sell or leak any data or information that they were able to seize from the computer or network they attacked. [23] Reviewing the history of ransomware attacks presents the juxtaposition in sophistication between attacks that occurred at ransomware's inception and the attacks of today.

A. History of Ransomware

It is December of 1989 in Western Europe – Belgium, to be specific. Your boss hands you a floppy disk and asks you to see what is on it. Being a reasonable employee who wants to keep their employed status, you slide the floppy disk into your desktop to view whatever exciting content may have been stored on the 720 KB sleek black square. Up until this point, you only know that this floppy disk was distributed to individuals, like your boss, who had attended the World Health Organization's AIDS conference. As you wait for the computer to read the information, you begin to pontificate over just what type of data will be displayed on your 10-inch by 10-inch monitor. In your mind there is absolutely no possibility that this disk is really a

[21] *What Is Ransomware?*, MCAFEE, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html (last visited Oct. 15, 2021).
[22] *Id.*
[23] *Ransomware 101*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/stopransomware/ransomware-101 (last visited Oct. 15, 2021).

ploy to effectively lock your computer's data in hopes of exploiting you for a whopping $189, but it is! This is exactly what happened to Eddy Willems, the first documented individual to be attacked by a ransomware virus. [24]

It has been thirty-two years since the ransomware attack on Mr. Willems, and ransomware has had ample time and opportunity to evolve. Unfortunately, ransomware attacks no longer happen via floppy disk, nor are they occurring as isolated incidents. Today there are numerous ways one might fall victim to an attack, and a single attack can wind up impacting thousands of individuals. The Colonial Pipeline hack, which forced the shutdown of the pipeline that stretches from Texas to New Jersey, perfectly captures the magnitude of the effect an attack can have.[25] Colonial is a company that has invested over $200 million dollars on information technology ("IT") in the past 5 years.[26] So, how does an attack like this still slip through the cracks after that type of investment? The truth is that ransomware attacks may be difficult to spot, thus tricking the victim into granting the malicious actor entrance into a system without even knowing what they have done.

B. How Ransomware Attacks Transpire

There are several techniques hackers use to infect a computer with a ransomware virus. One technique is the "drive-by download."[27] A drive-by download refers to malicious programs that install onto a person's device without the individual's consent.[28] For this download, the user

[24] Samantha Murphy Kelly, *The Bizarre Story of the Inventor of Ransomware*, CNN, May 16, 2021, https://www.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html.
[25] Michael Shear, et al., *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.
[26] Stephanie Kelly & Jessica Resnick, *One Password Allowed Hackers to Disrupe Colonial Pipeline, CEO Tells Senators*, Reuters, Jun. 8, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
[27] Paul R. DeMuro, *Keeping Internet Pirates at Bay: Ransomware Negotiation in the Healthcare Industry*, 41 NOVA L. REV. 349, 355 (2017), https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2035&context=nlr.
[28] *What Is a Drive by Download*, KASPERSKY RESOURCE CENTER, https://www.kaspersky.com/resource-center/definitions/drive-by-download (last visited Oct. 15, 2021).

does not have to actually click a link, agree to a download, or open any attachment.[29] The drive-by takes advantage of a website or application that contains security flaws which allow the download to occur.[30] Once the ransomware is downloaded, the malicious actor can hijack one's device, spy on one's activity, or even delete data and disable the device. [31]

Outside of exploiting an existing vulnerability, hackers will also legitimately purchase advertising space on certain websites.[32] If an individual clicks on the advertisement, the user is directed to the hacker's website. Once the website is loaded, the devices will become infected with the ransomware virus. [33] A seemingly legitimate advertisement is now the Trojan horse that has delivered a ransomware virus straight into one's device.

Perhaps the most popular tactic used by hackers is "spear phishing."[34] As almost anyone who works in an office knows, phishing is often done through false emails.[35] The emails will often look like they are coming from within the company, possibly a coworker or supervisor. [36] The email may contain a link that the user is instructed to click on, or some task for the recipient to follow. [37] By following these instructions, the employee ultimately infects their device with a ransomware virus, which may go on to spread throughout the network, infecting other devices that are connected to the same network. [38]

While some ransomware attacks have enormous impacts, like with JBS and Colonial, there are also countless attacks that target the average technology user. For example, certain

---

[29] *Id*.
[30] *Id*.
[31] *Id.*
[32] DeMuro, *supra* note 27.
[33] *Id*.
[34] *Id.* at 7.
[35] *Id*.
[36] *Id.*
[37] *See generally id.*
[38] *Id.*

ransomware attacks have been developed to target mobile phones by changing the PIN number of the devices, thus requiring a ransom to be paid in order to obtain the new PIN.[39] It is estimated that ransomware is able to extort hundreds of millions from victims each year, which comes as no surprise considering how many individuals have access to, and rely on technology today.[40]

Within the last six months, there have been several sizable attacks in the United States.[41] The hacking of the Colonial Pipeline and JBS revealed the vulnerability of U.S. companies and infrastructure, as both fuel and food production were temporarily halted. Behind both attacks were Russian cyber gangs that acted without consequence and within the purview of the Russian government.[42] If the United States is going grapple with the issue of ransomware, they are going to have to deal with Russia.

C. Russia and Ransomware

While a ransomware attack can stem from anywhere, certain countries in particular, such as Russia, seem to facilitate more attacks than others.[43] There are several reasons why Russia is the host of so many of these attacks, all centered around the fact that Russia takes a "hands-off approach."[44] Russia has created a safe haven for the actors who launch the ransomware attacks.[45]

---

[39] Ronny Richardson & Max M. North, *Ransomware: Evolution, Mitigation and Prevention*, 13 KENNESAW STATE UNIV. FAC. PUB. 10, Jan. 1, 2017. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs.

[40] *Id.*

[41] *The 10 Biggest Ransomware Attacks of 2021: Recent Cyber Attacks Hit Infrastructure and Critical Facilities Across US*, TOURO COLL. ILL., Nov. 12, 2021, https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php. Besides for JBS and Colonial Pipeline attacks, there has also been an attack on Steamship Authority of Massachusetts, the Washington DC Metropolitan Police Department, and several attacks taking place in the healthcare space.

[42] Julian E. Barnes, *Russia influences hackers but stops short of directing them, report says*, The New York Times (2021), https://www.nytimes.com/2021/09/09/us/politics/russia-ransomware-hackers.html

[43] *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure*, Hearing Before the Comm. on Homeland Security, 117 Cong. 6 (2021) [hereinafter *Pipeline Hearing*] (statement of John Katko).

[44] Isabelle Khurshudyan, *Ransomware's suspected Russian roots point to a long détente between the Kremlin and hackers,* THE WASHINGTON POST, Jun. 12, 2021, https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html.

[45] *Supra 31*.

The hackers are granted leniency as long as they do not target Russia or its allies.[46] V.S. Subrahmanian, Director of Dartmouth's Institute of Security, Technology, and Society, stated that cybercriminal networks in Russia exist with the tacit blessing of the Russian state, as long as they do not carry out the nefarious activities in Russia itself.[47] It is likely that Russia does not want the actual hacking done *directly* in the State for deniability purposes. If the hacking is not conducted within the State, Russia is able to declare confidently that since the hacks did not originate there, this absolves them from any wrongdoing or involvement.

As is the case with most crimes, the motivation behind the ransomware hackings is money.[48] One hacker-turned-analyst believes the reason that so many educated youths in Russia are turning to cybercrime is due to the vast sums of money to be made.[49] Additionally, it is believed that in certain situations, cybercriminals may be working with or for the Russian government.[50] "There's just too much of this going on right now for this not to have at least implicit hands-off policy by the Russian state… and at the very worst, it could be an explicit go-ahead."[51]

The New York Times reported that Russian intelligence officials have longstanding ties to criminal groups, and in some cases, it is almost certain that the intelligence agencies maintain a relationship with criminal threat actors.[52] A report by the cybersecurity company Recorded Future lends support to the belief that Russia does not *directly* tell the groups what to do, but is

---

[46] Katie Canales, *Experts say Russia gives hackers a 'tacit blessing' to attach foreign nations – as long as they don't target Russia or its allies*, BUSINESS INSIDER, Jun. 15, 2021, https://www.businessinsider.com/russia-safe-haven-hackers-cybercriminals-putin-ransomeware-blessing-2021-6.
[47] *Id.*
[48] *Id.*
[49] *Id*.
[50] *Id*.
[51] *Id*.
[52] Barnes, *supra* note 42

aware of their activities and asserts influence.[53] There are American officials who believe that Russian intelligence agencies will even recruit talent from these groups of cybercriminals.[54] Although it may be unclear exactly which, if any, attacks the Russian government is behind, what is clear is that certain attacks do emanate from Russia and become an economical and logistical burden on American businesses and citizens.[55]

D. Colonial Pipeline Hacking

In May 2021, both JBS and Colonial Pipeline fell victim to ransomware attacks. During a hearing before the Committee on Homeland Security, Congressman Jefferson Van Drew expressed his concern regarding the recent hacks. According to Congressman Van Drew, "[W]e have a serious problem on our hands. Hackers, who are primarily located in Russia, have developed sophisticated methods of infiltrating…entities in the United States."[56] Congressman Van Drew was referencing the Colonial Pipeline ransomware attack as well as the JBS meat processor ransomware hack. These hacks "raised serious questions about the cybersecurity practices of critical infrastructure owners and operators, and whether voluntary cybersecurity standards are sufficient to defend" against cyberattacks.[57] To grasp how serious the effects of these hacks can be, it is important to understand exactly what happened with Colonial Pipeline and JBS.

The first of these attacks occurred in early May 2021 on the Colonial Pipeline. The cyber criminals who attacked the pipeline did so by exploiting the legacy virtual private network

[53] INSIKT GROUP, DARK COVENANT: CONNECTION BETWEEN THE RUSSIAN STATE AND CRIMINAL ACTORS (2021), https://www.recordedfuture.com/russian-state-connections-criminal-actors/.
[54] Barnes, *supra* note 42
[55] *Id.*
[56] *Pipeline Hearings, supra* note 43 at 32.
[57] *Id*. at 1.

("VPN") profile, which was believed to no longer be in use. [58] The account was originally used to allow employees to remotely access the company's computer network.[59] The account's password was discovered inside a batch of leaked passwords on the dark web.[60] It is believed that an employee may have used the same password on a different account that had been previously hacked.[61] There is no evidence the password was obtained via phishing email, which may often be the case in similar situations.[62] Once the hackers were in the system, they were able to encrypt the IT systems of Colonial.[63] The Colonial Pipeline system spans over 5,500 miles in the United States.[64] Per day, the pipeline transports more than 100 million gallons of fuel and other refined products.[65] Nearly half of the fuel consumed on the East Coast comes from the Colonial Pipeline system, so when hackers brought the supply to a screeching halt, there was cause for some panic.[66]

The group that hacked Colonial goes by the name "DarkSide."[67] DarkSide is a ransomware service that enables a network of different groups to conduct cyber intrusions under the name "DarkSide."[68] Those individuals who are affiliated with DarkSide seek to coerce victims into paying their extortion demands.[69] If their demands go unmet, they threaten to

---

[58] *Id*. at 10.
[59] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG, Jun. 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
[60] *Id*.
[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] *Pipeline Hearing, supra* note 43 at 10.
[65] *Id*.
[66] *See generally id*.
[67] *Id*.
[68] *Id*. at 16.
[69] *Id*.

publish the stolen data to victim-shaming sites.[70] DarkSide is credited with affecting organizations in over fifteen countries and multiple industries since August 2020.[71]

DarkSide demanded a financial payment from Colonial in exchange for a key to unlock the encrypted IT systems.[72] The ransom note sent by DarkSide appeared on a system in the Colonial control room.[73] The threat from the ransom note forced Colonial to shut down the pipeline system and all IT associated with the pipeline.[74] Joseph Blount, President and CEO of Colonial Pipeline, stated that shutting down the pipeline was necessary once the ransomware note appeared. According to Blount, "we had no choice at that point. It was absolutely the right thing to do…we had no idea who was attacking us or what their motives were." [75] With Colonial shut down, the Eastern Seaboard was going to be short some 2.5 million barrels of fuel that was usually transported daily via their pipeline. The shutdown led to long lines at gas stations, higher fuel prices, and even a total depletion of fuel in certain areas.[76] Beyond the gas shortage and price increase, the hack also caused Colonial to take on an extensive examination of the pipeline, looking for visible damage that may have been caused from the stoppage or hack.[77]

With the Colonial Pipeline shutdown and gas prices quickly rising, Colonial decided to pay the ransom demanded by DarkSide. In total, the ransom paid was $4.4 million dollars – only a fraction of the $200 million that had been spent by Colonial securing the IT system.[78] Colonial

---

[70] *Id*.
[71] *Id*.
[72] *Id*. at 12.
[73] *Id*. at 19.
[74] *Id*. at 12.
[75] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG, Jun. 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
[76] *Id*.
[77] *Id*.
[78] CYBER THREATS IN THE PIPELINE: USING LESSONS FROM THE COLONIAL RANSOMWARE ATTACK TO DEFEND CRITICAL INFRASTRUCTURE (https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/pdf/CHRG-117hhrg45085.pdf)

paid the ransom to receive the decryption key, which was somewhat incomplete and did not work immediately.[79] However, Colonial was able to "manipulate" the key in a manner that provided them with the de-encryption ability. [80] Luckily for Colonial, the F.B.I. was able to recover $2.3 million in ransom that was paid to DarkSide.[81]

E. JBS Hacking

Beyond disrupting fuel lines and causing a rapid increase in gas prices, ransomware can affect the food supply of a nation. The United States knows about this all too well after the meat processing plants operated by JBS, which handles a fifth of all the cattle and hog slaughter in the United States, was shut down by ransomware hackers earlier this spring. [82] In total, nine beef plants belonging to JBS were shut down, disrupting production at poultry and pork plants. [83] Panic spread instantly as the disruption would likely impact wholesale beef prices. [84] The attack even extended from the United States into Canada as the shutdown resulted in canceled shifts that affected nearly 2,500 workers at beef plants in Brooks, Alberta.[85]

JBS was the target of a ransomware attack that affected their North American and Australian systems. The perpetrators of the attack were identified as REvil, a Russian-based cybercriminal group known for its attacks on American companies. [86] The Federal Bureau of Investigation ("F.B.I.") believes REvil to be "one of the most prolific ransomware organizations that cybersecurity experts track." [87] REvil is a "ransomware as service" organization, meaning they will lease their ransomware to other criminals, giving them the potential to commit their

---

[79] *Id*. at 34.
[80] *Id*. at 48.
[81] *Id*. at 45.
[82] https://www.nytimes.com/2021/06/02/business/jbs-beef-cyberattack.html
[83] https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html
[84] *Id*.
[85] *Id.*
[86] https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html
[87] *Id*.

own attacks without any technical knowhow. [88] Like their affiliate DarkSide, REvil resides in Russia under the protection of Moscow's hands-off approach. REvil is among the most sophisticated ransomware groups, and it is believed that since 2020, they have targeted over 237 organizations. REvil's sophistication allows them to command large sums of money from companies as notable as Apple.[89]

Like what happened with Colonial, a digital ransom note, this time particular to REvil, appeared demanding payment.[90] JBS paid the ransom of $11 million in Bitcoin to REvil "in order to mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated."[91] JBS spends more than $200 million dollars annually on IT and employs more than 850 IT professionals.[92] Despite this, JBS was still unable to prevent the ransomware attack that temporarily halted production at their plants.

Within just weeks of each other, two major companies were hacked and their IT systems were held for ransom. The Colonial Pipeline hack and JBS hack display just how susceptible companies are to these malicious actors, and how fragile the U.S. infrastructure is. In a matter of weeks, half the fuel that is delivered to the Eastern Seaboard, and twenty percent of all meat that is distributed in the United States were under attack by ransomware hackers from Russia. American food and fuel were being held hostage, and the companies had no choice but to pay the ransom and hope for a swift resolution. Past cybersecurity legislation had not done enough to stop these attacks from occurring. Therefore, the United States must take the cybersecurity

---

[88] *Id*.
[89] *Id*.
[90] *Id*.
[91] *JBS USA Cyberattack Media Statement*, JBS FOODS, Jun. 9, 2021, https://jbsfoodsgroup.com/articles/jbs-usacyberattack-media-statement-june-9.
[92] *Id*.

legislation currently in place and expand upon it, otherwise this type of criminal activity will likely continue to plague American businesses and infrastructure.

II. PRIOR CYBERSECURITY LEGISLATION

Upon examination of the recent JBS and Colonial Pipeline hacks, is apparent that ransomware attacks are a palpable threat to the United States. The United States must implement new legislation that focuses on decreasing the susceptibility of American businesses and individuals to these attacks. The existing legislation must be reviewed and expanded upon, filling in the gaps that leave companies like JBS and Colonial open to criminal incursion. This section will provide a brief overview of cybersecurity legislation in the United States, review past executive orders pertaining to cybersecurity, then discuss what changes and additions the current administration has enacted before recommending how to proceed with future legislation.

A. History of Cybersecurity Legislation

Understanding where cybersecurity legislation is today requires first looking back at its history.[93] Before there was any cybersecurity legislation there was legislation directly tied to computer use. The Computer Fraud and Abuse Act ("CFAA") was enacted in 1986 as an amendment to the first federal computer fraud law.[94] Since its implementation into law, the CFAA has been revised four times, the latest revision being in 2008.[95] The CFAA prohibits intentionally accessing a computer without authorization.[96] "It prohibits 'transmission of a program, information, code, or command' that causes damage to a computer or computer

[93] Joseph Skertic, Cybersecurity Legislation and Ransomware Attacks in the United States, 2015-2019, 42 (2021) (Ph.D. dissertation, Old Dominion University).
[94] *Computer Fraud and Abuse Act (CFAA)*, NAT'L ASSOC. OF CRIMINAL DEF. LAW., https://www.nacdl.org/Landing/ComputerFraudandAbuseAct [hereinafter *Computer Fraud*] (last visited Oct. 16, 2021).
[95] Skertic, *supra* note 93 at 30.
[96] *Computer Fraud, supra* note 94.

program, which makes the distribution of malware and other cybercrimes illegal." [97] The CFAA protects a broad range of computers and devices and empowers the Department of Justice to bring charges in the ransomware context.[98] Under the CFAA, different provisions correlate with the nature of the ransomware attack.[99] For example, the "archetypal ransomware attack where an individual uses malware to encrypt files until a ransom is paid for decryption, will probably violate § 1030(a)(7)(C), which governs certain extortive threats involving computers."[100] Although the CFAA is still crucial today, it is impeded by the scope of cybercrime and its ability to cross borders.[101]

Legislation that directly focuses on cybersecurity has a brief history, beginning in 1996 with the passing of the Health Insurance Portability and Accountability Act ("HIPAA").[102] HIPAA required health organizations to secure their systems in order to safeguard Protected Health Information ("PHI"), which is a patient's private information.[103] In 1999, the Gramm-Leach-Bliley Act ("GLBA") was passed and required financial institutions to protected consumers' personally identifiable data.[104] The GLBA requires financial institutions to explain their information-sharing practices to their customers and to safeguard any sensitive data.[105] Lastly, in 2002 the Federal Information Security Management Act ("FISMA") requires "federal agencies to provide information security protection commensurate with the risk and magnitude

[97] Skertic, *supra* note 93.
[98] Peter G. Berris & Jonathan M. Gaffney, *Ransomware and Federal Law: Cybercrime and Cybersecurity*, CONG. RES. SERV. REP., 3, Oct. 5, 2021, https://crsreports.congress.gov/product/pdf/R/R46932.
[99] *Id*.
[100] *Id*.
[101] *Id*.
[102] Skertic, *supra* note 56 at 31.
[103] *Id*.
[104] *Id*.
[105] *Gramm-Leach-Bliley Act*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Oct. 16, 2021).

of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of" information collected by or for an agency.[106]

In 2009, President Obama announced that cybersecurity would be a top priority for his administration.[107] In 2014, the Obama Administration passed four laws that addressed cybersecurity reform.[108] Of these four laws, the Cybersecurity Enhancement Act of 2014 and Cybersecurity Information Sharing Act ("CISA") were aimed at strengthening cybersecurity through a voluntary public-private partnership that would "provide for research and development, workforce development and education," and promote a voluntary sharing of information between the public and private sectors.[109]

B. Executive Orders Pertaining to Cybersecurity

There were several executive orders during the Obama and Trump administrations that enabled sanctions due to malicious cyber activities. The sanctions imposed on Russian persons are based on four authorities: Executive Order ("EO") 13694 and EO 13757, EO 13848, the Countering Russian Influence in Europe and Eurasia Act ("CRIEEA"), and EO 14024.[110] Several of these executive orders relate directly to election interference by Russia via cyberspace.[111] However, they also give broader authorization to issue sanctions for other cyber-related crime.[112]

The Obama Administration took action in response to Russia's cyber-related interference in the 2016 election.[113] On April 1, 2015, Obama issued EO 13694, invoking national emergency

---

[106] Skertic, *supra* note 93 at 31.
[107] Skertric, *supra* note 93 at 33.
[108] *Id*.
[109] *Id*.
[110] *U.S. Sanctions on Russia: An Overview*, CONG. RES. SERV. REP. [hereinafter *Sanctions on Russia*], 1, Sep. 1, 2021, https://sgp.fas.org/crs/row/IF10779.pdf.
[111] *Id.*
[112] *Id*.
[113] *Id*.

authorities.[114] The executive branch is authorized to draw on national emergency authorities to impose sanctions for various cyber-enabled activities.[115] EO 13694 declared that "the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located…outside the United States constitute an unusual and extraordinary threat."[116] EO 13694 targeted those who engage in cyberattacks (1) against critical infrastructure, (2) for financial or commercial gain, or (3) to significantly disrupt the availability of a computer network.[117] EO 13694 did not target any specific state, but it was issued just four months after the Sony Pictures hack.[118]

In December of 2016, Obama issued EO 13757, amending EO 13694. EO 13757 expanded the sanctionable types of cyber-related activities.[119] EO 13757 established sanctions against those engaged in tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election process or instructions.[120] Under the EO, the Officer of Foreign Assets Control ("OFAC") designated several entities and individuals for election-related malicious cyber activities. Among these designees was Russia's leading intelligence agency.

In 2017, the CRIEEA was signed into law by President Trump.[121] CRIEEA broadened the previous executive orders by imposing sanctions on Russian persons who have engaged in activities undermining cybersecurity against any person, including a democratic institution, or

---

[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] *Id*.
[118] *Id*.
[119] Beau D. Barnes et al., *National Security Law*, 52 THE YEAR IN REVIEW 459, 463 (2017).
[120] Skertric, *supra* note 93 at 33.
[121] Peter Jeydel et al., *A Detailed Look at the Countering America's Adversaries Through Sanctions Act*, STEPTOE, AUG. 10, 2017, https://www.steptoe.com/en/news-publications/a-detailed-look-at-the-countering-america-s-adversaries-through-sanctions-act.html

government, on behalf of the Russian government.[122] Under CRIEEA, the United States has imposed sanctions on foreign entities engaged in significant transaction with Russia's defense or intelligence sectors. [123] Again in 2018, several individuals and entities were designated for election-related malicious cyber activities. Among the designees was the Internet Research Agency, also known as the Russian "troll factory."[124] On March 15, 2018, OFAC made its first designation under the new CRIEEA authorities. OFAC designated two entities and six individuals for a global ransomware attack that occurred in 2017.[125]

The acts and executive orders of past administrations are the foundation which the Biden Administration must expand upon if the United States is going to be successful in fighting cybercrime. Many of the executive orders have focused on broadening what constitutes a cybercrime, and allow the United States to sanction certain actors who commit these crimes. The Biden Administration has taken action in an attempt to strengthen efforts in the fight against ransomware, but there is still more that should be done.

C. Biden Administration

"Ransomware now poses a national security threat."[126] Secretary Alejandro Mayorkas was unambiguous during his virtual address earlier this year in which he outlined his vision and roadmap for the Department of Homeland Security's cybersecurity efforts – ransomware is a national threat. Acknowledging that ransomware is a matter of national security is a step in the right direction. During the Biden Administration, there have been several changes surrounding cybersecurity, including the creation of a new Office, the first appointment of a National Security

[122] *Id.*
[123] *Id.*
[124] Press Release, U.S. Department of the Treasure, Treasury Sanctions Russia-Linked Election Interference Actors (Sept. 10, 2020).
[125] *Id.*
[126] Alejandro Mayorkas, Secretary, Dept. of Homeland Sec., Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience (Mar. 31, 2021).

Advisor for Cyber and Emerging Technology, and the implementation of a cybersecurity executive order.

In 2020, Congress created the Office of the National Cyber Director, which advises the president on cybersecurity and coordinates the implementation of the National Cyber Strategy.[127] This will hopefully allow for greater coordination among the federal government when an attack does take place. As Secretary Mayorkas mentioned in his vision for cybersecurity resilience, too many channels are spoken through, which can confuse and distract those who need to immediately act on information.[128] Furthermore, the Biden Administration has created the new position of Deputy National Security Advisor for Cyber and Emerging Technology, appointing Anne Neuberger to the role. [129] Deputy Neuberger is coordinating a whole-of-government response to Build Back Better and modernize cyber defenses.[130]

Secretary Mayorkas also discussed a series of "60-day sprints" in which there would be a focus on the most important and urgent priorities.[131] The first of these "sprints" would be a focus on the fight against ransomware.[132] Mayorkas stated that governments which do not use the full extent of their authority to stop these malicious actors should be held accountable – a clear stab at the Russian government.[133] In an effort to prevent ransomware incidents, Mayorkas plans to launch an awareness campaign and engage with industry and key partners.[134] On the other end, the response to ransomware attacks will involve strengthening capabilities to disrupt those who launch the attacks, as well as the marketplaces that enable the attacks.[135]

---

[127] Berris, *supra* note 98 at 9.
[128] Mayorkas, *supra* note 126.
[129] *Id*
[130] *Id*
[131] *Id*.
[132] *Id*.
[133] *See generally id*.
[134] *Id*.
[135] *Id*.

On May 28, 2021, Biden signed into law EO 14028 – "Improving the Nation's Cybersecurity." The order "charges multiple agencies with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain." [136] Although ransomware is not specifically mentioned, the order is designed to develop and enhance guidelines for software supply chain security. [137] Part of those guidelines include criteria to evaluate software security and innovate tools or methods to demonstrate conformance with secure practices. [138]

Moreover, on October 14, 2021 and October 15, 2021, the White House held a virtual ransomware summit, inviting over 30 countries. [139] Notably, Russia was not invited to attend. The summit was a significant step in building an international coalition to address the issue of ransomware. [140] A senior Biden Administration official stated that this would be the first of many conversations to come. [141] The official also articulated that the reason Russia did not receive an invite was based on a lack of faith in the Russian government to address ransomware activity coming from within Russia.[142]

Overall, the Biden Administration is viewing both cybersecurity and ransomware as top priorities. The Administration has made efforts to defend against cyberattacks by opening dialogue between nations, implementing executive orders, and creating new cybersecurity positions. The ransomware summit reinforces the position that ransomware is truly an

---

[136] Improving the Nation's Cybersecurity: NIST's Responsibilities under the Executive Order, INFORMATION TECHNOLOGY LABORATORY, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity (last visited Dec. 3, 2021).
[137] *Id*.
[138] *Id*.
[139] Kevin Collier, White House to host virtual ransomware summit with 30 countries – but not Russia, CBS NEWS, Oct. 13, 2021, https://www.nbcnews.com/tech/security/white-house-host-virtual-ransomware-summit-30-countries-not-russia-rcna2933.
[140] *Id*.
[141] *Id*.
[142] *Id*.

international problem. Now, using the Colonial Pipeline and JBS hacks as a guide, the United States can work on establishing a strategy to minimize future risk of ransomware attacks.

III. SUGGESTIONS MOVING FORWARD

Ransomware attacks in the United States are on the rise.[143] Between 2019 and 2020, ransomware attacks rose by 62 percent worldwide, and by 158 percent in North America.[144] This increase in attacks emphasizes the need for additional measures by the United States to mitigate future cybercrime. After analyzing the Colonial Pipeline and JBS hacks, three suggestions for the United States emerge. First, the United States should expand on current legislation to require training that will help better identify malicious links and emails to avoid a repeat of the JBS and Colonial hacking. Legislation should also implement regulations that update cyber hygiene and standards which align with the recommended Ransomware Framework set out by the Ransomware Task Force. Next, the United States must put pressure on Russia, forcing Putin to crack down on the cyber gangs like the ones responsible for JBS and Colonial. Finally, the United States should target and sanction virtual currency exchanges that enable cybercriminals to receive their ransom in a heavily untraceable manner. This section will explain and support each suggestion in turn.

A. Expanding Legislation

In an effort to strengthen resilience against ransomware attacks, the United States must begin to pass legislation that expands on existing cybersecurity regulations. This expansion should incorporate both an updated incorporation of ransomware frameworks that are nationally

[143] Lynsey Jeffery & Vignesh Ramachandran, *Why ransomware attacks are on the rise – and what can be done to stop them*, PBS NEWS HOUR, Jul. 8, 2021, https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.
[144] *Id*.

accepted, and new laws requiring certain cybersecurity training to be carried out by American businesses.

In April 2021, the Ransomware Task Force released a comprehensive framework that detailed various actions that should be taken in order to reduce the threat of ransomware attacks.[145] Among the suggestions was the need for existing cybersecurity regulations and standards to be reviewed and updated to incorporate the recommended Ransomware Framework.[146] The belief is that a single, internationally accepted framework that lays out clear, actionable steps to defend against, and recover from, ransomware attacks would be crucial in reducing the confusion that surrounds current ransomware guides.[147]

There are many guides and tools currently available that aim to mitigate ransomware attacks, but the problem becomes that many are either insufficient, overly complicated or too simplistic to properly handle the issue.[148]If states are all using their own frameworks, the issue may then become one of winners and losers.[149] For example, the efforts taken in one jurisdiction may be regionally effective, but this might push attacks on to different regions with less stringent regulations.[150] Having one nationally accepted framework can allow for a coordinated response by states, which would create greater long-term impacts and effectively disrupt cybercrime.[151] Beyond that, if the Framework were to be universally implemented, organizations that operate in more than one country would have the advantage of already using the required cybersecurity procedures.[152]

---

[145] RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., A COMPREHENSIVE FRAMEWORK FOR ACTION: KEY RECOMMENDATIONS FROM THE RANSOMWARE TASK FORCE [hereinafter *Task Force*] (2021)
[146] *Id*.
[147] *Id*. at 35.
[148] *Id*.
[149] *Id*.
[150] *Id.* at 36.
[151] *See generally id.*
[152] *Id*.

If a national framework were to be adopted, it should be consistent with existing cybersecurity frameworks, such as the National Institute of Standards and Technology ("NIST") framework, but should be specific to ransomware.[153] The Ransomware Task Force is not alone in their suggestion of adhering to the NIST framework. Various experts in the field of cybersecurity suggest adhering to the NIST framework, as it entails five key functions, ""identify, protect, detect, respond, and recover."[154] The framework provides a repeatable, cost-effective approach to managing cybersecurity risk.[155] As of September 2021, the NIST also released a "Cybersecurity Framework Profile for Ransomware Risk Management."[156] The framework supports preventing, responding to, and recovering from ransomware events.[157] Future legislation should adopt a national ransomware framework that addresses the concerns pointed out by the Ransomware Task Force, and incorporates the suggestions by the NIST.

In addition to the adoption of a national ransomware framework, legislation that provides or mandates cybersecurity training for workers is likely to be advantageous in stopping attacks.[158] As discussed previously, phishing is a main tactic used by ransomware actors to bypass cybersecurity measures.[159] Humans are one of the most vulnerable aspects of cybersecurity[160]. Phishing tactics are only so successful because individuals are tricked into believing that an email or link is genuine.[161] Although there are anti-phishing programs that are designed to assist users and reduce the likelihood of falling victim to the phony emails, these

[153] *Id.* at 18.
[154] Skertic, *supra* note 93 at 124
[155] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY NIST 9 (2014)
[156] Barker et al, *Cybersecurity Framework Profile for Ransomware Risk Management*, NIST, Sep. 2021, https://csrc.nist.gov/publications/detail/nistir/8374/draft
[157] *Id*.
[158] Skertic, *supra* note 93 at 70.
[159] *Id*. at 68.
[160] *Id*.
[161] *Id.* at 62.

programs are often outdated and unable to keep up with modern phishing techniques.[162] One suggestion is to have the combination of anti-phishing training for individuals along with a software that automatically filters or blocks phishing attacks.[163] Overall, there is significant literature that supports the claim that anti-phishing training should be part of an effective prevention strategy.[164]

Legislation that creates a national ransomware framework and mandates cybersecurity training would be a start to combating ransomware. However, the issue of Russia allowing cyber gangs to attack the United States must still be addressed. If the United States is going to properly address ransomware, they must put pressure on Russia to begin cracking down on the Russian gangs that are behind ransomware attacks.

B. Dealing with Russia

It is estimated that nearly fifty-eight percent of all cyberattacks emanate from Russia.[165]Both the JBS and Colonial Pipeline hacks have been traced back to Russian cyber gangs such as REevil and DarkSide. If the United States hopes to be successful in its ploy to reduce ransomware attacks, they will need Russia to begin coordinating efforts to crack down on the cybercriminals living within their borders. Russia is believed to not only be aware of the presence of the cyber gangs, but it is also believed that there are instances in which these gangs are working with the consent of the Russian security services[166]. The United States needs to make it apparent that this type of criminal activity will not go unacknowledged or unpunished.

---

[162] *Id*. at 69.
[163] *Id*. *See also id* at 70 (experts have argued that machine learning is critical to dealing with phishing in the future as phishing tactics are evolving faster than they can be implemented into training programs).
[164] *Id.* at 70.
[165] Tom Burt, *Russian cyberattacks pose greater risk to governments and other insights from our annual report*, MICROSOFT, OCT. 7, 2021, https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/#:~:text=During%20the%20past%20year%2C%2058,a%2032%25%20rate%20this%20year.
[166] Giannis Papanikos, *How the Kremlin provides a safe harbor for ransomware*, NBC NEWS, Apr. 16, 2021, https://www.nbcnews.com/tech/security/kremlin-provides-safe-harbor-ransomware-rcna699.

Therefore, in order to compel action on the part of Russia, the United States should define specific "red activities" which would constitute cybercrimes that would be met with immediate and significant action.[167] Additionally, the United States, along with its allies, should continue to publicly condemn Russia for their inaction, which will put international pressure on Putin to act on Russia's internal issue of cybercrime[168].

In April 2021, the United States sanctioned Russia for malign activities including state-backed hacking, where the Treasury Department stated that Russian intelligence had enabled ransomware attacks by providing safe harbor for those who commit the hackings[169]. In response, Biden signed a new executive order that targets aggressive and harmful activities by the Government of the Russian Federation[170]. The sanctions were targeted at technology companies that support the Russian Intelligence Services' efforts to carry out cybercrimes against the United States[171].

There is an understanding amongst the Russian cyber gangs that as long as you are not working against Russia, you are free to steal from Americans[172]. When two members of the Russian hacking group Evil Corp were indicted in 2019 for a banking fraud scheme, it was believed by Treasury officials that the Russian government was well-aware of Evil Corp's malicious activities[173]. Although there is no indication that Russia's government benefits directly

---

[167] JOE R. REEDER & TOMMY HALL, CYBERSECURITY'S PEARL HARBOR MOMENT: LESSONS LEARNED FROM THE COLONIAL PIPELINE RANSOMWARE ATTACK 25 (2021).
[168] Scott Montgomery, *How Joe Biden could increase pressure on Vladimir Putin if their June 16 meeting fails to deter Russia's harmful behavior*, THE CONVERSATION, Jun. 9, 2021, HTTPS://THECONVERSATION.COM/HOW-JOE-BIDEN-COULD-INCREASE-PRESSURE-ON-VLADIMIR-PUTIN-IF-THEIR-JUNE-16-MEETING-FAILS-TO-DETER-RUSSIAS-HARMFUL-BEHAVIOR-159194.
[169] Papanikos, *supra* note 166.
[170] Press Release, U.S. Department of the Treasure, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021).
[171] *Id*.
[172] Giannis, *supra* note 166.
[173] Bobby Allyn, *Russia Hacking Group Evil Corp. Charged By Federal Prosecutors In Alleged Bank Fraud*, NPR, Dec. 5, 2019, https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f.

from ransomware crime, the chaos and havoc it creates is likely incentive enough for Putin[174]. Putin may allow these attacks because he believes they create animosity toward democratically elected governments and cause citizens to lose faith in their financial systems[175]. Additionally, the hacks allow cybercriminals to hone their skills, which is an asset that may be called upon[176]. With Putin turning an apparent blind eye toward cybercrimes, it is hard to find confidence that Russia will help the United States deal with the issue of ransomware.[177]

There is little faith coming out of Washington that the Russian government has taken, or will take, action to crack down on ransomware actors operating out of Russia[178]. "We've asked for help and cooperation with those who we know are in Russia, who we have indictments against, and we've seen no action,"[179] said Paul Abbate, the deputy director of the Federal Bureau of Investigation[180]. One suggestion to get the Russians to play ball is by defining "red activities." These red activities would be defined cybercrimes that would trigger consequences in hopes of deterring additional hackings.[181]

The posture of deterrence is used against nuclear, chemical, biological, and other existential threats, where the United States draws red lines that are not to be crossed under the threat of severe consequence[182]. In 2012, Obama stated "a red line for us is we start seeing a whole bunch of chemical weapons moving around or being utilized," when discussing the Syrian

---

[174] Giannis, *supra* note 166.
[175] Michael Williams, *Make Russia Take Responsibility for Its Cybercriminals*, FP, Nov. 9, 2021, https://foreignpolicy.com/2021/11/09/cyberattacks-russia-responsibility-ransomware/.
[176] *Id*.
[177] *See generally id.*
[178] Jeff Seldin, *US Accuses Russia of Stonewalling on Cybercrime*, VOA, Sept. 14, 2021, https://www.voanews.com/a/6227401.html.
[179] *Id*.
[180] *Id*.
[181] Reeder & Hall, *supra* note 167.
[182] *Id*. at 26

use of chemical weapons.[183] Drawing red lines has value in having clear-cut parameters for intervention and response, but red lines are not without their risk. Now, if a line is crossed, intervention becomes necessary at the risk of a country looking weak and allowing issues to advance.[184]

The United States should make it clear that if Russia is going to allow these attacks to continue without any form of intervention, then Russia is choosing to accept the defined consequences.[185] The facilitating, harboring, tolerating, or leaning of a crime and failing to respond would all be red activities.[186] Each activity would come with its own consequence, hopefully motivating action from the Russian government to begin clamping down on cyber gangs.[187] Exposing Russia to an unbearably high cost if it chooses to continue its policy of nonfeasance may be the most effective way to push for real action.[188]

Beyond implementing a set of defined consequences, the United States should continue to pressure Putin to crack down on ransomware groups operating from Russia. In June 2021, Biden met with Putin to discuss various issues, one being cyberattacks.[189] At the meeting, Putin denied Russia's role in cyberattacks, but both parties agreed to task cyber experts to work on coming to an express understanding of what would be considered off limits.[190] Biden also told Putin that the United States would mount a significant cyber response if attacks were to continue.[191]

---

[183] CNN Wire Staff, *Obama warns Syria not to cross 'red line,'* CNN, Aug. 21, 2012, https://www.cnn.com/2012/08/20/world/meast/syria-unrest/.
[184] Neal Conan & David Miller, *The Value And Risk of Drawing A Red Line*, NPR, Mar. 20, 2013, https://www.npr.org/2013/03/20/174849033/the-value-and-risk-of-drawing-a-red-line
[185] Reeder & Hall, *supra* note 167 at 27.
[186] *Id*.
[187] *Id*.
[188] *Id*.
[189] Kevin Liptak, *5 takeaways from the summit between Biden and Putin*
[190] *Id*.
[191] *Id*.

Just weeks after both Presidents ended talks, the Russian hacker group REvil, went off-line.[192] The group's sites on the dark web suddenly disappeared overnight.[193] There are three contending theories as to why REvil went dark.[194] The first being that Biden ordered the United States Cyber Command to take down the group's sites.[195] Second, there is some belief that Putin ordered the sites to be taken down, which would display some response to the earlier talks between Biden and Putin.[196] The third theory is that REvil took its own sites down after deciding that the current attention was too great. Although nothing is certain, a senior intelligence analyst at Recorded Future believes that REvil abandoned their sites due to extrinsic pressures.[197] It seems overly coincidental that the group would go off-line only days after Biden demanded Putin shut down the ransomware group, leading some to the belief that Biden's warning was heeded.[198]

The disappearance of REvil is a win amongst the cybersecurity community, and may show the beginning of a Russian response to U.S. demands. Additionally, in October 2021, Mandiant, a U.S. cybersecurity firm that responds to ransomware incidents, reported a lull in activity from certain ransomware groups.[199] Unfortunately, it is still too soon to tell whether there will be any significant reduction in ransomware attacks.[200] Jen Easterly, the Director of the U.S. cybersecurity and Infrastructure Agency, said that thus far, she has not seen any significant

---

[192] David Sanger, *Russia's most aggressive ransomware group disappeared. It's unclear who made that happen*. N.Y. TIMES, July. 13, 2021, HTTPS://WWW.NYTIMES.COM/2021/07/13/US/POLITICS/RUSSIA-HACKING-RANSOMWARE-REVIL.HTML?REFERRINGSOURCE=ARTICLESHARE
[193] *Id*.
[194] *Id.*
[195] *Id*.
[196] *Id*.
[197] *Id*.
[198] *Id*.
[199] Sean Lyngaas, *US calls on Russia to do more to crack down on ransomware groups as White House hosts meeting with allies*, CNN, Oct. 13, 2021, https://www.cnn.com/2021/10/13/politics/white-house-ransomware-meeting/index.html
[200] *Id*. *See also* Maggie Miller, *Lawmakers increasingly anxious about US efforts against Russian hackers*, THE HILL, NOV. 19, 2021, HTTPS://THEHILL.COM/POLICY/CYBERSECURITY/582280-LAWMAKERS-INCREASINGLY-ANXIOUS-ABOUT-US-EFFORTS-AGAINST-RUSSIAN-HACKERS?RL=1 (Officials are hearing mixed messages on whether there has been a decrease in ransomware since the leaders met in June).

changes in Russian behavior since the talks between Biden and Putin[201]. Only time will tell if Russia is becoming more receptive to the United States' requests for intervention. In the meantime, the United States should hedge their bets and begin to take additional affirmative action in the fight against ransomware. While waiting to see the Russian response, the United States should begin to focus on the sanctioning of cryptocurrency exchanges as another method in preventing potential ransomware attacks.

C. Regulating Cryptocurrency Exchanges

Extorting an individual or company through ransomware requires two basic components: a target and a way to get paid by that target. Unlike with the original attack in 1989, ransom is generally no longer paid by sending cash to a P.O. box. Today, payment is most often received in the form of cryptocurrency – Bitcoin, to be exact.[202] Knowing that actors are using cryptocurrency to be paid their ransom, it would seem that a potential solution would be to heavily regulate, or stop, these currencies from passing through the United States. Therefore, the United States should target the virtual currency exchanges that enable cybercriminals to obtain payment.

First, cryptocurrency is "decentralized digital money, based on blockchain technology."[203] There are over 5,000 different cryptocurrencies in circulation, including the main actors like Bitcoin and Ethereum.[204] Cryptocurrency, like cash, can be used to purchase regular goods and services, along with other assets like stocks or precious metals.[205] What makes

[201] *Id*.
[202] *Ransomware: Paying Cyber Extortion Demands in Cryptocurrency*, MARSH, https://www.marsh.com/us/services/cyber-risk/insights/ransomware-paying-cyber-extortion-demands-in-cryptocurrency.html
[203] Kate Ashford & John Schmidt, *What is Cryptocurrency?,* FORBES, Dec. 18, 2020, https://www.forbes.com/advisor/investing/what-is-cryptocurrency/
[204] *Id*.
[205] *Id*.

cryptocurrency so appealing for cybercriminals is the fact that it is digital, encrypted, and decentralized.[206]

Bitcoin is the current go-to cryptocurrency for ransomware payments.[207] Bitcoin allows cybercriminals to receive funds with a high degree of anonymity, making it difficult to track.[208] Bitcoin is widely available and easy to acquire.[209] When payments are sent, both parties are identified only by an account number or address.[210] Although bitcoin transactions are visible to the public, there is no direct way to determine the account owner.[211] Cybercriminals will use obfuscation techniques to increase anonymity and avoid being tracked by law enforcement.[212] For example, "mixing" is a service provider that mixes the cryptocurrency funds of different users to break any traceable trail of transaction, making it near impossible that the original cybercriminal is caught.[213]

Knowing that cryptocurrency can be used for nefarious activities is one of the strong reasons for regulation. China is a prime example of a nation that has recently cracked down on cryptocurrencies.[214] In September 2021, China's central bank announces that all crypto-related transactions were illegal.[215] A statement by the People's Bank of China cited "legal risks for individuals and organizations participating in virtual currency and trading activities," as the reason behind the ban.[216] China is not alone in their decision to ban the use of Bitcoin. Algeria,

---

[206] *Id*.
[207] Marsh, supra note 202.
[208] *Id*.
[209] *Id*.
[210] *Id*.
[211] *Id*.
[212] *Id*.
[213] *Id*.
[214] Tim De Chant, *Bitcoin outlawed in China as country bans all cryptocurrency transactions,* ARS TECHNICA, Sept. 24, 2021, https://arstechnica.com/tech-policy/2021/09/bitcoin-outlawed-in-china-as-country-bans-all-cryptocurrency-transactions/.
[215] *Id*.
[216] *Id*.

Bolivia, Colombia, Indonesia, and several other countries have either banned or restricted the use of Bitcoin.[217]

Currently, the United States has no plans of banning Bitcoin and cryptocurrency.[218] However, in September 2021, the U.S. Department of Treasury announced a set of actions against the virtual currency exchange Suex, focusing on "disrupting criminal networks and virtual currency exchanges responsible for laundering ransoms."[219] This marks the first time that the United States has implemented sanctions against a virtual currency exchange.[220] The Treasury Department found that more than forty percent of the transactions through Suex were linked to criminal actors.[221] In a call with reporters previewing the sanction announcement, Treasury Deputy Secretary Wally Adeyemo said "exchanges like Suex are critical to attackers' ability to extract profits from ransomware attackers... [the sanctions] are a signal of our intention to expose and disrupt the illicit infrastructure using these attacks."[222] It is expected that new anti-money-laundering and terror-finance rules that seek to limit the use of cryptocurrency as a payment mechanism in ransomware attacks will be implemented later this year.[223]

With the state of cryptocurrency being unregulated, the sanctioning of virtual exchanges seems to be a sufficient workaround for now. There are experts who believe that regulating

---

[217] Chloe Orji, *Bitcoin ban: These are the coutnreis where crypto is restricted or illegal,* EURONEWS.NEXT, Nov. 24, 2021, https://www.euronews.com/next/2021/11/20/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2v

[218] Alex McShane, *Federal Reserve Chair Jerome Powell: US Has no Plans to Ban Bitcoin and Crypto*, NASDAQ, Sep. 30, 2021, https://www.nasdaq.com/articles/federal-reserve-chair-jerome-powell%3A-u.s.-has-no-plans-to-ban-bitcoin-and-crypto-2021-09.

[219] Robust Action, *supra* note 203

[220] *Id*.

[221] *Id*.

[222] Alexandra Alper, *Biden sanctions cryptocurrency exchange over ransomware attacks*, REUTERS, Sep. 21, 2021, https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/.

[223] *Id*.

cryptocurrency would vastly improve the ability to fight ransomware.[224] The Ransomware Task Force ("Task Force"), which was created in December 2020, issued a report in which one of its priority recommendations was the close regulation of cryptocurrency.[225] The Task Force recommends that governments require cryptocurrency exchanges, crypto kiosks, and over-the-counter trading "desks" to comply with existing laws, including Know Your Customer, Anti-Money Laundering, and Combatting Financing of Terrorism laws. [226]

For now, the United States should continue to monitor virtual currency exchanges, like Suex, that are known to be linked to criminal actors. When an exchange is discovered to be conducive to cybercrime, the United States should continue to issue sanctions, reinforcing the message that action will be taken against virtual exchanges that allow malicious actors to harm American infrastructure and citizens. Simultaneously, the U.S. should begin implementing regulation of cryptocurrency, following the suggestions of the Task Force. This two-pronged approach attacking both the virtual exchanges, and cryptocurrency, would hopefully be enough of a deterrent to dissuade the continuing increase of ransomware attacks.

Conclusion

In sum, ransomware is a significant issue that demands immediate attention. Ransomware is capable of bringing massive companies like Colonial and JBS, who provide essential goods and services, to a screeching halt. Moving forward, the United States should use the Colonial and JBS hackings as guiderails for shaping future cyber defense. The United States should continue to expand on existing cyber legislation, apply pressure on Putin, forcing him to begin cracking

[224] Joseph Menn & John Shiffman, *Govenrment and industry push bitcoin regulation to right ransomware scourge*, CNBC, Apr. 28 2021, https://www.cnbc.com/2021/04/28/government-and-industry-push-bitcoin-regulation-to-fight-ransomware.html.
[225] Task Force, *supra* note *145* at 6.
[226] *See generally, id*.

down on Russian cyber gangs, and continue the sanctioning of virtual currency exchanges that give cybercriminals the ability to receive their ransoms in an anonymous manner.