United States Senate
Committee on Homeland Security and Governmental Affairs

Rob Portman, Ranking Member

AMERICA'S DATA HELD HOSTAGE: CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES

STAFF REPORT

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

MARCH 2022

AMERICA'S DATA HELD HOSTAGE: CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

More than ever before, cyber criminals have the ability to disrupt Americans' lives from anywhere in the world. Over time, attackers' tactics have evolved and improved and cyberattacks now have the potential to paralyze entire industry sectors. Organizations are racing to update their systems and improve their defenses to counter this threat. The proliferation of ransomware attacks is a primary example of this challenge.

Ransomware is a type of malware that encrypts victims' computer systems and data, rendering the systems unusable and the data unreadable. Perpetrators then issue a ransom demand—often in cryptocurrency—allowing remote and anonymous payment to attackers. If the victim pays, hackers *may* provide the victim with a key to decrypt their systems and data. But there is no guarantee. In a new trend, called double extortion, attackers first steal sensitive data from a victim before deploying the ransomware. Then, cyber criminals threaten to release the stolen data if the victim refuses to pay the ransom—so even ransomware victims who are able to restore their data without paying the ransom are at risk.

Ransomware is on the rise. While the first recorded instance of ransomware was in 1989, the frequency of these attacks has increased exponentially, at least in part because of the establishment of cryptocurrencies. One cybersecurity firm estimated there were 623.3 million attempted ransomware attacks worldwide in 2021 alone—an average of 20 attempted attacks every second. The United States suffered the most ransomware attempts at 421.5 million, a 98 percent increase from 2020. Americans have become all too familiar with the real-world impact of high-profile ransomware attacks like those on Colonial Pipeline, America's largest fuel pipeline, and JBS, the world's largest beef producer.

* * * * * * * * * *

This report details the attacks by Russia-based ransomware group REvil on three American companies, and the experiences of those companies during the incident response. The goal of this report is to provide information companies and agencies can use to prepare for and respond to ransomware attacks.

REvil targeted entities of all sizes and sophistication. The three companies have little in common in terms of business model, purpose, or number of employees. Entity A is a global multi-sector Fortune 500 company with roughly 100,000 employees. Entity B is a global manufacturing company with several thousand employees. Entity C is a technology firm with only 50 employees. Nevertheless, all three were targeted by the same ransomware group. This underscores the broad

threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

Ransomware criminals often use phishing attacks to gain initial access. Cybercriminals gained access to Entity A's networks by compromising a known vulnerability on a legacy server of one of its vendors. Attackers then impersonated that vendor, and sent an unsuspecting Entity A employee an email attachment corrupted with ransomware.

A phishing attack—a malicious email disguised as a legitimate email—was also the entry point for REvil's ransomware attack on Entity B. REvil compromised Entity B when a mid-level employee opened a phishing email disguised as a message from their bank. Even organizations with sophisticated cybersecurity protections are susceptible to a single employee falling victim to a well-crafted phishing email.

Offline backups and well-defined incident response plans helped ransomware victims mitigate successful ransomware attacks. All three entities interviewed by the Committee had established incident response plans when REvil attacked them. This proactive measure allowed each entity to take quick remedial action, onboard third-party experts, and in the case of Entity B cut off the attacker's access before they encrypted its networks with ransomware.

In addition to restoring access to their critical data, backups permitted these three entities to resume normal business operations, like payroll. As a result, these entities avoided the attacks' worst effects, including the need to pay the ransom.

Two victim companies reported little help from the Federal Government. All three companies reported their incidents to the Federal Government. Of these, one company did not need the Government's help. The other two companies reported they got little help. They told the Committee that the Federal Bureau of Investigation (FBI) prioritized its investigative efforts into REvil's operations over protecting the companies' data and mitigating damage. Both companies also indicated they did not receive advice on best practices for responding to a ransomware attack or other useful guidance from the Federal Government.

Because there is no central repository to collect information on and provide insight into the ransomware attacks taking place across the United States, CISA and the National Cyber Director should work quickly with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA. This law will enhance the Federal Government's ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through information sharing.

II. FINDINGS AND RECOMMENDATIONS

Findings of Fact

(1) All organizations, regardless of size and sophistication, are susceptible to ransomware attacks.

(2) Ransomware groups often use phishing attacks to gain initial access to victim networks.

(3) In past ransomware attacks, multifactor authentication, zero trust principles, and network segmentation helped prevent attackers from gaining or increasing access to sensitive data in a victim's networks.

(4) Maintaining offline backups and a well-defined incident response plan helped victims resume critical operations quickly without paying a ransom, when attackers did get in.

(5) The laws and regulations at the time discouraged victims from sharing information with other potential victims that could prevent future ransomware attacks.

(6) In two cases reviewed in this report, the FBI prioritized its investigative and prosecutorial efforts to disrupt attacker operations over victims' need to protect data and mitigate damage.

(7) Until recently, there was no Federal agency charged with collecting and tracking reports of cyber incidents to prevent and mitigate future attacks.

REvil Findings

(8) REvil monetized access to victim networks and sold that access to other REvil affiliates.

(9) Before encrypting victim organization networks, REvil used double extortion methods to first steal sensitive data from victims and then publish that data on REvil's public blog.

(10) REvil harassed victim company employees via email and telephone in an attempt to coerce the companies into paying ransoms.

Recommendations

(1) CISA should immediately share all incident reports received under the Cyber Incident Reporting for Critical Infrastructure Act with the FBI. The FBI and CISA should also strengthen their partnership to assist ransomware victims. Close coordination between these two entities will best position the FBI to investigate those responsible for ransomware attacks while also allowing CISA to provide the technical assistance victims need to recover.

(2) FBI should ensure it considers ransomware victim priorities like protecting data and mitigating damage. This will preserve FBI's constructive working relationship with the private sector and provide it with the information necessary to hold attackers accountable.

(3) CISA and the National Cyber Director should work quickly with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA. This legislation will enhance the Federal Government's ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through the sharing of timely and actionable threat information.

(4) Increase costs for attackers by eliminating low hanging fruit. Organizations can increase the difficulty for ransomware criminals by patching vulnerabilities, implementing multi-factor authentication, maintaining accurate device and software inventories, and instituting complex password requirements. Adhering to these cyber best practices will increase the likelihood that attackers move on to less prepared targets.

(5) Organizations should implement a defensive posture that assumes the organization has been breached. Sophisticated cyber adversaries with near unlimited resources can compromise most networks if given enough time. Employing zero trust networking (continuous authentication and monitoring) with need-to-know access privileges will give organizations critical time to detect attackers and cut off their access before they exfiltrate or encrypt sensitive data. Flat networks and enterprise-wide shared drives give users more access than they need, allowing hackers to do more damage if they compromise one of those accounts.

(6) Have a cyber incident response plan in place before an attack occurs. When a cyber incident inevitably takes place, organizations should know in advance who needs to be notified and when. Incident response plans should detail explicit processes for notifying the Government and retaining an incident response provider. Entities should also determine which systems are most critical to its operations and how long those systems can be offline before business operations suffer significant impacts. For critical infrastructure owners and operators, organizations should go a step further to determine how long systems can be offline before there are regional or national effects.

(7) Maintain offline backups and encrypt sensitive data when stored and in transit. These two solutions can help mitigate the otherwise debilitating impact of ransomware attacks. With offline backups, organizations can reconstitute impacted systems without having to pay a ransom for the decryption key. Encrypting sensitive data addresses the second half of double extortion attacks because the data is unreadable. Together, offline backups and encryption of sensitive data are the most effective ways to mitigate the damage and cost associated with a successful ransomware attack.

III. BACKGROUND

Ransomware is a critical national security threat that can affect the daily lives of all Americans. During ransomware attacks, criminals deploy malicious software that encrypts a victims' files and renders its systems unusable.[1] In 2021, there were 623.3 million attempted ransomware attacks globally.[2] This was a 105 percent increase from 2020.[3] The United States was the top target for attempted ransomware attacks globally in 2021, increasing 98 percent from the prior year.[4] Of the 623.3 million attempted ransomware attacks in 2021, the United States had 421.5 million—accounting for over 67 percent of all attacks globally.[5]

Ransomware's rapid growth is problematic not only for the private sector but also for government.[6] During the first six months of 2021, there were more ransomware attack attempts on government than any other industry, and three times the number of attacks seen in 2020.[7] Testifying before the Senate Homeland Security and Governmental Affairs Committee, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly summarized the ransomware threat saying, "incidents like Colonial Pipeline, JBS Foods and the scourge of ransomware attacks . . . on our schools and hospitals and small businesses illustrate how cybersecurity impacts our daily lives."[8]

A. Evolution of Ransomware

Encrypting files in attempt to prevent user access is an attack technique that dates back to the late 1980s.[9] The first ransomware attack on record is the AIDS Trojan deployed by floppy disk in 1989.[10] Roughly 20,000 malware-corrupted floppy disks were distributed to attendees of the World Health Organization's

---

[1] *Ransomware 101*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware/ransomware-101.
[2] SONICWALL, 2022 SONICWALL CYBER THREAT REPORT 29 (2022), https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf.
[3] *Id.*
[4] *Id.* at 31.
[5] *Id.*
[6] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.
[7] SONICWALL, MID-YEAR UPDATE: 2021 SONICWALL CYBER THREAT REPORT 11 (2021), https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf.
[8] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Jen Easterly, Director, CISA).
[9] SYMANTEC, THE EVOLUTION OF RANSOMWARE 7 (2015).
[10] *Id.*

international AIDS conference that year in Stockholm.[11] To restore access to their files, victims were instructed to send $189 to a P.O. Box in Panama.[12]

AIDS Trojan Floppy Disk
Source: Andrada Fiscutean, A history of ransomware: The motives and methods behind these evolving attacks, *CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-*

A Belgian-based information technology (IT) professional impacted by the malware recalled he quickly determined it was not sophisticated and only took him ten minutes to restore all of his files.[13] The malware failed to encrypt file contents to prevent user access, and only changed file names to random characters.[14]

An American evolutionary biologist named Dr. Joseph Popp developed the AIDS Trojan.[15] Popp was arrested and charged with blackmail before being declared mentally unfit to stand trial.[16]

---

[11] Anthony M. Freed, *A Brief History of Ransomware Evolution*, CYBEREASON (Nov. 30, 2021), https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution.
[12] *Id.*
[13] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
[14] *Id.*
[15] Anthony M. Freed, *A Brief History of Ransomware Evolution*, CYBEREASON (Nov. 30, 2021), https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution.
[16] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.

Modern ransomware arrived in 2005 with malware called PGPCoder.[17] This virus encrypted all files with extensions such as .doc, .html, and .jpg.[18] It also created "!_READ_ME_!.txt" files in each folder instructing victims to pay several hundred dollars to an e-gold or Liberty Reserve account to decrypt their files.[19]

While viruses like PGPCoder ushered in the modern ransomware construct, these attacks remained uncommon because payment collection was difficult.[20] At the time, hackers had few reliable options for collecting anonymous payments, free from law enforcement scrutiny.[21] Cryptocurrencies like Bitcoin changed this dynamic by streamlining the ransom collection process and providing some degree of anonymity.[22]

Ransomware continued to proliferate through the early 2010s, but hackers had yet to perfect using cryptocurrencies for ransom payments.[23] During this timeframe, cryptocurrencies remained a foreign concept to many, and so non-tech-savvy victims struggled to pay the ransoms.[24] As a result, some cybercriminals set up call centers to help victims purchase Bitcoin, a cryptocurrency often used to pay ransom demands.[25] This helped ensure payment, but was also expensive and time consuming for hackers.[26]

Cryptocurrency exchanges allowed cybercriminals to receive instant and anonymous payments outside of traditional financial institutions. [27] Armed with this newfound convenience and anonymity, cybercriminals realized they could make

---

[17] SYMANTEC, THE EVOLUTION OF RANSOMWARE 9 (2015).
[18] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
[19] *Id.* Liberty Reserve was a money transfer business that only required a valid email address to open an account. Brian Krebs, *Reports: Liberty Reserve Founder Arrested, Site Shuttered*, KREBS ON SECURITY (May 25, 2013), https://krebsonsecurity.com/2013/05/reports-liberty-reserve-founder-arrested-site-shuttered/. In 2013, the U.S. Department of Justice shut down Liberty Reserve alleging the service processed $6 billion in criminal proceeds. Brian Krebs, *A Light at the End of Liberty Reserve's Demise?*, KREBS ON SECURITY (Feb. 14, 2020), https://krebsonsecurity.com/2020/02/a-light-at-the-end-of-liberty-reserves-demise/.
[20] CROWDSTRIKE, THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT AGAINST NEW ADVERSARY TRENDS AND METHODS 2 (2021).
[21] SYMANTEC, THE EVOLUTION OF RANSOMWARE 22 (2015).
[22] *Id.* at 22–23.
[23] *History of Ransomware*, CROWDSTRIKE (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.
[24] *Id.*
[25] CROWDSTRIKE, THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT AGAINST NEW ADVERSARY TRENDS AND METHODS 2 (2021).
[26] *History of Ransomware*, CROWDSTRIKE (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.
[27] SYMANTEC, THE EVOLUTION OF RANSOMWARE 22–23 (2015).

millions in just a few weeks.[28] Once someone sets up a Bitcoin wallet linked to an exchange, transactions to and from that wallet are not easily traceable to a specific person.[29] A digital currency wallet is a software application that allows a user to hold, store, and transfer digital currency.[30]

CrowdStrike, a prominent cybersecurity firm, conducted a survey in 2020 of 2,200 senior IT leaders and security professionals from organizations with 250 or more employees that revealed 56 percent of participating organizations experienced a ransomware attack in the last year.[31] The same survey found 54 percent of participating IT professionals now rank ransomware among the most concerning cyber threats facing their organizations.[32]

B. Recent Ransomware Trends

In recent years, ransomware criminals have improved their techniques to increase the pressure on victims to pay ransoms. As these techniques evolve over time, several recent trends have emerged. These include: (1) stealing and threatening to release sensitive victim data in what are called "double extortion attacks"; (2) targeting high-value organizations and data; (3) rebranding to evade law enforcement; and (4) using ransomware services-for-hire affiliate structures.

1. Double Extortion Attacks

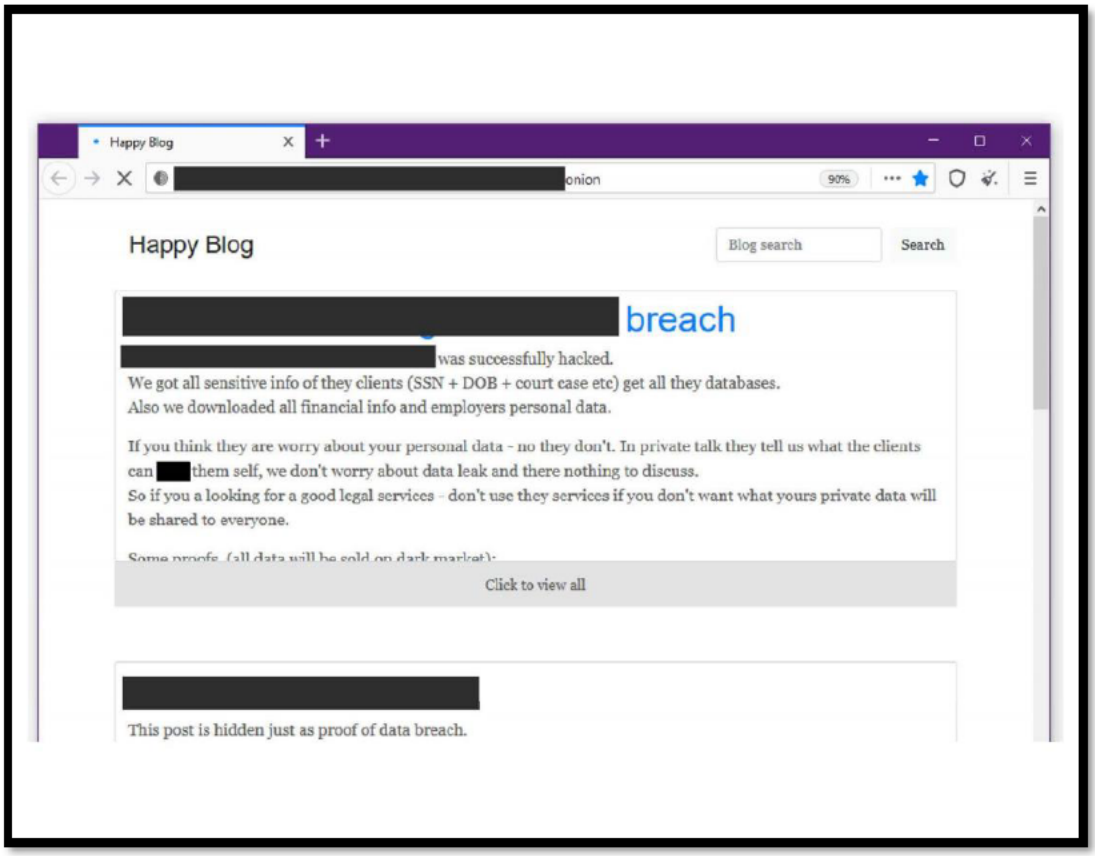
Double extortion refers to hackers making an additional threat to release stolen victim data on top of encrypting its systems if the victim does not pay.[33] In double extortion attacks, hackers exfiltrate files from victims before encrypting their host systems.[34] This allows hackers to threaten to publish the stolen victim data to further coerce victims into making a ransom payment as shown in the REvil

---

[28] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
[29] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,842 (Dec. 23, 2020) (codified at 31 C.F.R. pt. 1010, 1020, 1022).
[30] *Questions on Virtual Currency*, U.S. DEP'T OF TREASURY (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.
[31] CROWDSTRIKE, 2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY: INSIGHTS INTO SECURITY TRANSFORMATION AND PREVALENT ATTACK VECTORS IN A WORK-FROM-ANYWHERE WORLD 3 (2020), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CSGlobalSecurityAttitudeSurveyReport.pdf.
[32] *Id.* at 4.
[33] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 3 (2021); IVANTI, RANSOMWARE: THROUGH THE LENS OF THREAT AND VULNERABILITY MANAGEMENT 38 (2022).
[34] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 3 (2021).

"Happy Blog" screenshot below.[35] Ransomware operators use these websites called "leak sites" to post screenshots of a victim's directory structure to prove they possess and are prepared to release the victim's sensitive files.[36]

Tactics like double extortion have emboldened attackers, who now issue ransom demands larger than ever before. For example, during the first half of 2021, financial institutions reported $590 million in ransomware payments, exceeding the amount reported for all of 2020.[37] This was a 42 percent increase from the $416 million total reported in 2020.[38]



REvil Happy Blog Post
Source: Catalin Cimpanu, REvil ransomware group returns following Kaseya attack, RECORDED FUTURE (Sept. 7, 2021), https://therecord.media/revil-ransomware-group-returns-following-kaseya-attack/.

[35] *Id.*; Catalin Cimpanu, *REvil ransomware group returns following Kaseya attack*, RECORDED FUTURE (Sept. 7, 2021), https://therecord.media/revil-ransomware-group-returns-following-kaseya-attack/.
[36] PALO ALTO NETWORKS: UNIT 42, 2021 RANSOMWARE THREAT REPORT 5 (2021).
[37] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 1 (2021).
[38] *Id.* at 3.

In 2021, the manufacturing industry experienced the most double extortion leaks, followed by professional and legal services and construction.[39] The double extortion tactic is prevalent in the Americas, accounting for 62 percent of victim data posted on leak websites.[40] Forty-seven percent of those victims were in the United States.[41] Late in 2021, ransomware criminals sometimes added an additional layer, called "triple extortion", where attackers also notify a ransomware victim's partners, shareholders, and suppliers of the incident.[42]

2. High-Value Target Attacks

Another trend in ransomware is high-value target attacks, sometimes referred to as "big game hunting" (BGH).[43] With this strategy, hackers target specific organizations with substantial financial resources or sensitive information.[44] BGH is so prevalent that CrowdStrike referred to it as "one of the most prominent trends" affecting digitally perpetrated crimes like ransomware.[45]

BGH also includes targeting entities important to the United States economy, like those in the industrial and manufacturing sectors.[46] Because disruption in day-to-day operations affect the core business of these sectors, these entities are more likely to pay a ransom to resume normal operations.[47] In some critical infrastructure sectors, regulations prescribe reliability and restrict downtime, providing further incentive to pay ransoms and restore service quickly.[48] For example, the Federal Energy Regulatory Commission, which regulates electric utilities, in some cases will fine electric utilities for violating reliability standards when a blackout occurs.[49] The attack on Colonial Pipeline, which is the largest refined products pipeline in the United States,[50] is an example of this.[51]

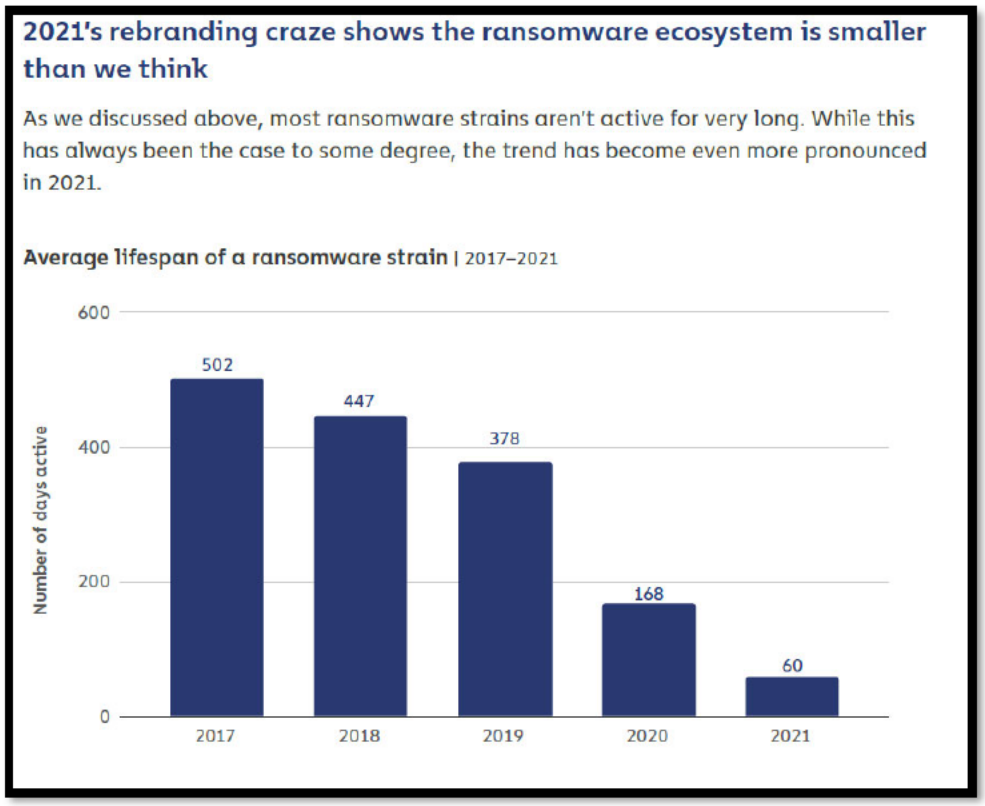
---

[39] PALO ALTO NETWORKS: UNIT 42, 2021 RANSOMWARE THREAT REPORT 8 (2021).
[40] *Id.* at 6.
[41] *Id.*
[42] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.
[43] CROWDSTRIKE, 2021 GLOBAL THREAT REPORT 6 (2021).
[44] *History of Ransomware*, CROWDSTRIKE (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.
[45] *Id.*
[46] CROWDSTRIKE, 2021 GLOBAL THREAT REPORT 21 (2021).
[47] *Cf.* CROWDSTRIKE, 2021 CROWDSTRIKE GLOBAL THREAT REPORT 21 (2021).
[48] *E.g.*, *Orders, Reliability Enforcement Orders*, Fed. Energy Reg. Commission (2020), https://www.ferc.gov/industries-data/electric/industry-activities/orders-reliability-enforcement-orders.
[49] *Id.*
[50] *About Us/Our Company*, Colonial Pipeline, https://www.colpipe.com/about-us/our-company.
[51] *See generally Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company):

By the middle of 2021, and after high-profile attacks like Colonial Pipeline and JBS Foods, the FBI observed some ransomware threat actors shifting their efforts to mid-size victims to reduce scrutiny.[52] This shift also follows U.S. authorities disrupting several ransomware groups around the same time.[53]

3. Rebranding

Rebranding is a third trend where ransomware groups claim retirement only to reemerge shortly thereafter under a new name.[54] With this deceptive tactic, cybercriminals attempt to distract or evade law enforcement and continue normal operations.[55] This includes setting up new victim payment sites and other attack infrastructure.[56]



Rebranding Frequency and Short Lifespan of Ransomware Stains in 2021
Source: CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 45 (2022).

Cyberattack halts fuel movement on Colonial petroleum pipeline, U.S. ENERGY INFORMATION ADMIN. (May 11, 2021), https://www.eia.gov/todayinenergy/detail.php?id=47917.

[52] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

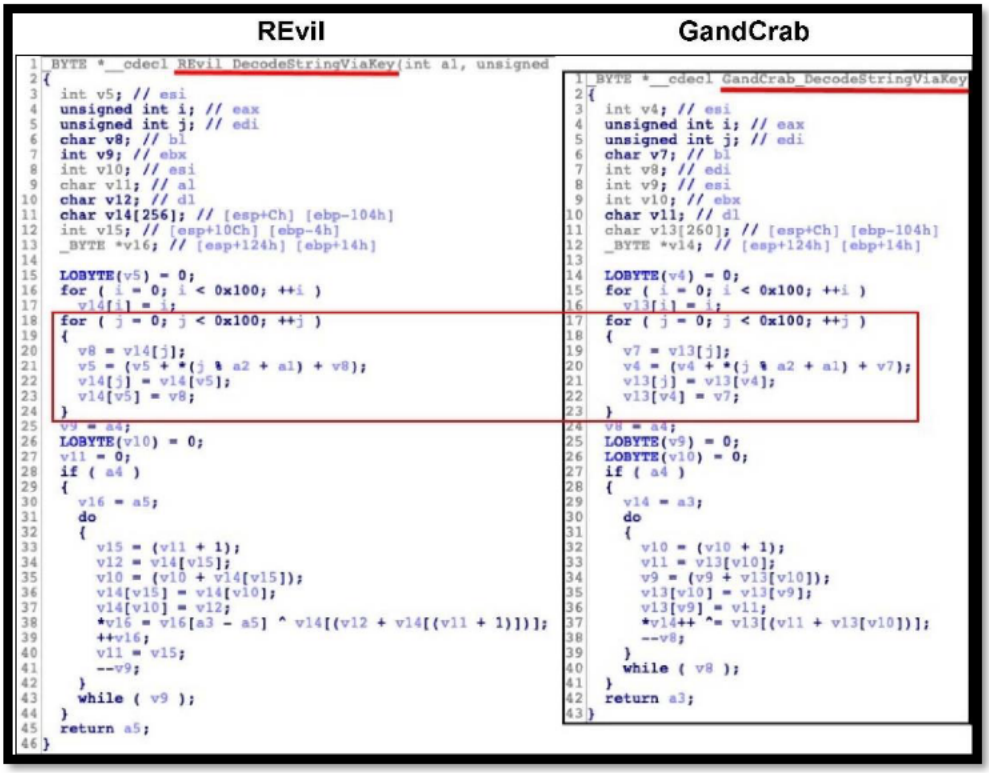
[53] *Id.*

[54] CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 45 (2022).

[55] *Id.* at 47.

[56] *Id.* at 46.

As an example, some consider REvil a rebrand of GandCrab, which announced its retirement in 2019.[57] GandCrab claimed to extort over $2 billion from victims and boasted "we are living proof that you can do evil and get off scot-free."[58] Below is a screenshot depicting the near identical code used by both REvil and GandCrab.

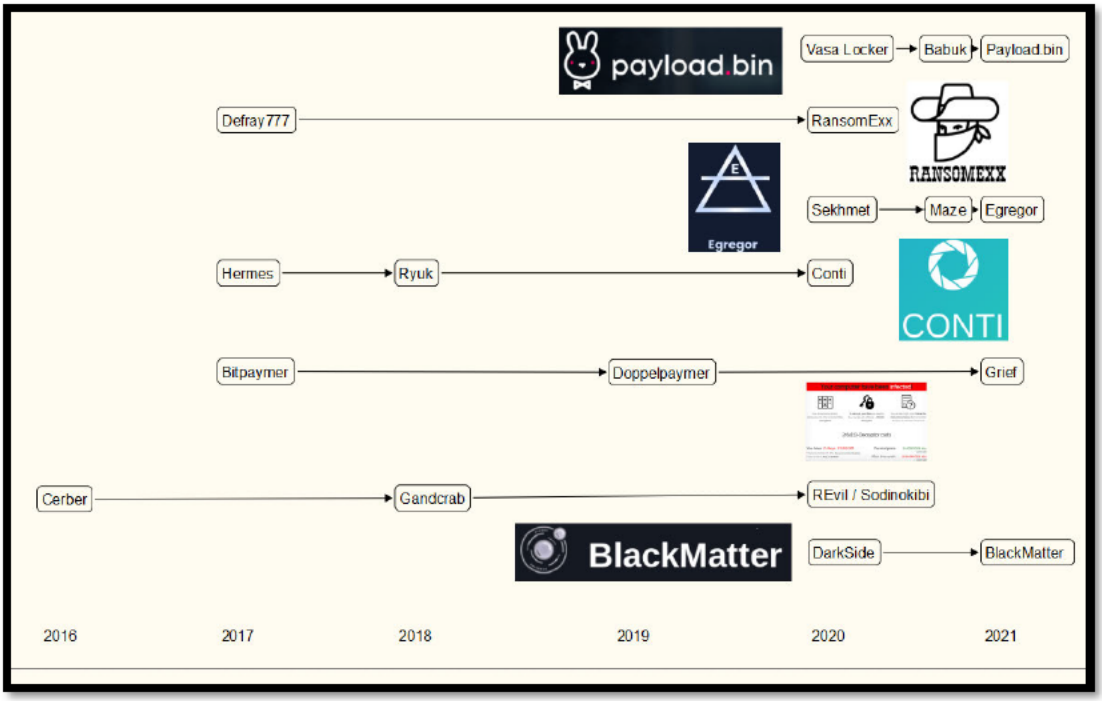


Similar Code Used by Both REvil and GandCrab
Source: DEP'T OF HEALTH & HUMAN SERVICES, REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR 7 (2021), https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf.

Rebranding is a process ransomware gangs undertake with relative ease. The graphic below shows the rebrandings of several prominent ransomware gangs over just the last few years. At least one reason for rebranding is to avoid scrutiny and sanctions—ransomware groups can change their name, create a new website, and resume operations under the new name.[59]

---

[57] DEP'T OF HEALTH & HUMAN SERVICES, REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR 4 (2021), https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf.
[58] *Id.* at 4–5.
[59] CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 47 (2022); *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. DEP'T OF TREASURY (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.



Ransomware Group Rebranding Timeline
Source: Brian Krebs, Ransomware Gangs and the Name Game Distraction, KREBS ON SECURITY (Aug. 5, 2021), https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/.

4. Ransomware-as-a-Service

Over the last year, ransomware groups have professionalized their operations using a business model often called ransomware-as-a-service (RaaS).[60] Under this configuration, ransomware developers sell or deliver their malware to separate individuals or groups who have illicit access to a target victim network.[61] The two parties then enter into a profit sharing arrangement where the initial developer receives a percentage of all ransoms paid by victims.[62] Examples of RaaS groups include REvil, DarkSide, and Conti.[63]

---

[60] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[61] *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, U.S. DEP'T OF TREASURY (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[62] *Id.*

[63] DEP'T OF HEALTH & HUMAN SERVICES, REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR 3 (2021), https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf; *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, U.S. DEP'T OF TREASURY (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf; *Alert (AA21-265A): Conti Ransomware*, CYBERSECURITY AND INFRASTRUCTURE AGENCY (Mar. 9, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa21-265a.

C. Role of the Private Sector in Ransomware Incident Response

Complex cyber attacks, including ransomware, make it difficult for victims to respond alone—often requiring specific technical and legal experts companies may not have on their payroll. As a result, third-party experts play a significant role in shaping ransomware incident response efforts. Examples of third-party experts include cyber insurers, law firms, cyber incident response firms, and ransomware negotiators. The high cost of retaining these experts can make responding to a ransomware attack difficult for all but the most well-financed businesses. According to a recent IBM report, the average total cost of a ransomware attack is $4.62 million.[64]

1. Cyber Insurance

The growth in ransomware attacks has caused a corresponding growth in cyber insurance. Companies can select standalone policies exclusively covering cyber risk or broader liability policies that also cover cyber incidents, like ransomware attacks.[65] As of 2020, United States domiciled insurers reported roughly $1.62 billion in direct written premiums for standalone cyber insurance policies, and $1.13 billion in direct written premiums for cyber coverage as part of broader insurance policies.[66] During 2020 alone, standalone cybersecurity insurance direct written premiums increased by 28.1 percent.[67]

Cyber insurance policies cover risk categories including liability for suffering a data breach, breach remediation costs, and coverage for legal or regulatory penalties.[68] In particular, this often covers costs associated with: business interruption, notifying consumers after a breach, providing credit monitoring services, and restoring or replacing impacted systems.[69] Costs associated with ransomware attacks are also covered by many cyber insurance policies.[70] Also, as discussed in the next subsection, cyber insurance policies often cover the cost of retaining outside legal counsel.[71]

Because coverage determinations and premiums are based on risk, cyber insurance can also incentivize better cyber hygiene and adherence to practices that

---

[64] IBM, 2021 COST OF A DATA BREACH REPORT 8 (2021).
[65] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 4 (2021).
[66] NAT'L ASS'N INS. COMMISSIONERS, REPORT ON THE CYBERSECURITY INSURANCE MARKET 7 (2021).
[67] *Id.* at 5.
[68] *See* Adrejia Boutte Swafford, *Cyber Risk Insurance: Law Firms Need It, Too*, 67 LA. B. J. 326, 328 (2020).
[69] Adrejia Boutte Swafford, *Cyber Risk Insurance: Law Firms Need It, Too*, 67 LA. B. J. 326, 329 (2020).
[70] *Ransomware*, NAT'L ASS'N OF INSURANCE COMMISSIONERS (Aug. 25, 2021), https://content.naic.org/cipr_topics/topic_ransomware.htm.
[71] *See generally* Part III.C.2.

reduce the risk of ransomware attacks.[72] These include discouraging policyholders from configuring their networks in ways that expose them to unnecessary risk.[73] Policyholders have a significant interest in trying to implement these measures because doing so demonstrates to insurers that the policyholder has an effective cybersecurity program that reduces cyber risk, thereby reducing insurance premiums.[74] Nonetheless, cyber insurance may also incentivize ransomware attackers by assuring payment of the ransom.[75] As discussed below, some ransomware attackers will even seek out cyber insurance policy information to aid in their negotiations with victims.

Although more companies now have cyber insurance policies, there is still significant cost uncertainty in this market.[76] More attacks mean more demand for cyber insurance, but also higher premiums as insurers take on more risk.[77] During the last quarter of 2020 alone, a survey of insurance brokers showed a 10 to 30 percent increase in cyber insurance prices.[78] In a similar way, the attack frequency and severity has caused insurers to scale back cyber coverage for at-risk sectors like healthcare and education.[79]

To minimize risk, many cyber insurance providers now rely on reinsurance.[80] Reinsurance allows insurers to mitigate risk by insuring the policy they are providing to a customer with a third-party insurer in return for a percentage of the premiums.[81] Outsized risk for insurers could cause significant changes to the cyber insurance products offered to customers or even a decline in the number of insurers offering cyber policies altogether.[82] According to one cyber insurer, this scenario

---

[72] *Cf.* CARNEGIE ENDOWMENT FOR INT'L PEACE, ADDRESSING THE PRIVATE SECTOR CYBERSECURITY PREDICAMENT: THE INDISPENSABLE ROLE OF INSURANCE 11 (2018).
[73] *Id.*
[74] *See* Tristan Hinsley & Holden Wegner, *The rising tide of cyber insurance premiums in the age of ransomware*, SECURITY MAGAZINE (Nov. 18, 2021), https://www.securitymagazine.com/articles/96549-the-rising-tide-of-cyber-insurance-premiums-in-the-age-of-ransomware.
[75] *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. DEP'T OF TREASURY (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.
[76] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 8 (2021).
[77] *Id.*
[78] NAT'L ASS'N INS. COMMISSIONERS, REPORT ON THE CYBERSECURITY INSURANCE MARKET 6 (2021).
[79] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 8 (2021).
[80] Tristan Hinsley & Holden Wegner, *The rising tide of cyber insurance premiums in the age of ransomware*, SECURITY MAGAZINE (Nov. 18, 2021), https://www.securitymagazine.com/articles/96549-the-rising-tide-of-cyber-insurance-premiums-in-the-age-of-ransomware.
[81] *Id.*
[82] Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARVARD BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

would remove a valuable risk management strategy for organizations with substantial cyber exposure.[83]

2. Outside Legal Counsel

One way companies constrain liability after ransomware attacks is by retaining outside counsel immediately after a cyber incident is confirmed.[84] According to a recent CrowdStrike report, 49 percent of the company's incident response engagements were referred to CrowdStrike by third-party counsel.[85]

By retaining outside counsel, victims may be able to protect some details of its investigation from disclosure under the attorney-client privilege.[86] It is common for victims to delegate their incident response efforts to outside counsel.[87] The outside counsel then retains third-party experts to help respond to the incident, including cybersecurity response firms.[88] As a result, organizations often assert the attorney-client privilege and work-product doctrine to shield documents and opinions of third-party firms retained by the outside counsel from discovery.[89] Organizations bear the burden of demonstrating those communications were for the purpose legal counsel or the documents were prepared in reasonable anticipation of litigation.[90]

The issue of whether third-party investigative documents were prepared for the purpose of legal advice or in anticipation of litigation, and thus shielded from discovery, is complicated and often the subject of litigation.[91] Target's 2013 data breach is an example of when a court determined the attorney-client privilege protected third-party investigative documents.[92] After Target discovered the breach, the company launched a dual-track investigation.[93] On the first track, Target retained Verizon to conduct a non-privileged investigation examining how

---

[83] *Id.*
[84] *See* infra section 2; *see also* Robert Lemos, *Breach Response Shift: More Lawyers, Less Cyber-Insurance Coverage*, DARK READING (Jan. 10, 2022), https://www.darkreading.com/attacks-breaches/changes-to-breach-response-more-lawyers-less-cyber-coverage.
[85] CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 15 (2021).
[86] Brian Mund & Leonard Bailey, *Privilege in Data Breach Investigations*, 69 DOJ J. FED. L. & PRAC. 39, 41 (2021).
[87] *Id.*
[88] *Id.*
[89] *Id.* at 43, 45.
[90] *Id.*
[91] Todd Presnell & Benjamin William Perry, *A Tale of Two Functions: Weighing Business and Legal Considerations in the Wake of a Data Breach to Preserve Attorney-Client Privilege and Work Product Protections*, NAT. L. REV. (Mar. 9, 2022), https://www.natlawreview.com/article/tale-two-functions-weighing-business-and-legal-considerations-wake-data-breach-to.
[92] *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14–2522, 2015 WL 6777384, at 2–3 (D. Minn. Oct. 23, 2015).
[93] *Id* at 2.

the breach occurred and to develop an appropriate response.[94] With the second track, Target created its own "Data Breach Task Force" and according to a Target court filing engaged a separate Verizon team "to enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries."[95] Target only asserted privilege for documents created during the second track investigation.[96]

The plaintiffs suing Target argued none of the investigative documents prepared by Verizon should be protected by attorney-client or work product privilege.[97] The plaintiffs claimed the assertion of privilege was improper because "Target would have had to investigate and fix the data breach regardless of any litigation to appease its customers and ensure continued sales, discover its vulnerabilities, and protect itself against future breaches."[98] The court sided with Target holding "the Data Breach Task Force was focused not on the remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation."[99]

Marriott's 2018 breach is another example of the attorney-client and work product privilege protecting third-party investigative documents. When Marriott identified the breach, the company retained the law firm BakerHostetler to investigate the incident.[100] BakerHostetler then entered a new statement of work with IBM on behalf of Marriott "to assist BakerHostetler in providing legal advice to Marriott."[101]

The plaintiffs suing Marriott claimed all documents generated during the investigation were not privileged because IBM and Marriott had a pre-existing business relationship and the "the services IBM provided after the breach were the same kind of services IBM provided before the breach."[102] The court rejected the plaintiffs' claims reasoning "that the post-November 2018 work yielded a result or results similar to the work done before that date cannot negate the universal agreement of the witnesses that Marriott had retained IBM for a specific purpose—to aid [BakerHostetler] in [its] defense of Marriott."[103]

---

[94] *Id.*
[95] *Id.* at 1 (internal quotation marks omitted).
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.* at 3; *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14–2522, 2015 WL 6777384, at 3 (D. Minn. Oct. 23, 2015).
[100] *In re Marriott International Inc. Customer Data Security Breach Litigation*, MDL No. 19-MD-2879, 2021 WL 2660180, at 3 (D. Md. Jun. 29, 2021).
[101] *Id.* at 5.
[102] *Id.* at 3.
[103] *Id.* at 6.

Unlike Target and Marriott, healthcare insurance company Premera was unable to assert the attorney-client or work product privileges to protect third-party investigative documents after its breach in 2015. Before discovering the breach, Premera hired Mandiant in October 2014 to review its data management system.[104] After the breach in February 2015, Premera hired outside counsel in anticipation of litigation.[105] The next day, Premera amended its existing statement of work with Mandiant and shifted supervision over Mandiant from the company to outside counsel.[106] This amended statement of work "did not otherwise change the scope of Mandiant's work from what was described in the Master Services Agreement between Mandiant and Premera entered into on October 10, 2014."[107]

The court distinguished Premera from Target saying "[w]ith Premera . . . there was only one investigation, performed by Mandiant, which began at Premera's request."[108] Although supervision was later shifted to outside counsel, this "by itself, is not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product."[109]

Moreover, unlike Marriott, Premera did not articulate a separate and distinct purpose for the post-breach investigative work.[110] Concluding privilege did not apply, the court ruled "the amended statement of work did not change the scope of work and there is no evidence that Mandiant changed its scope or purpose at the direction of outside counsel."[111]

3. Cyber Incident Response Firms

As discussed in the case law above, cyber incident response firms help victim companies understand the impact of cyber incidents and devise an effective response. Assistance from these firms is necessary for most victims because it is difficult to know the appropriate investigative procedures, data collection, reporting requirements, and legal precautions a victim must take to understand an incident.[112]

Once retained, cyber firms provide several services to mitigate incident impact. Among other things, these services include dispatching on-site experts to

---

[104] *In re Premera Blue Cross Customer Data Security Breach Litigation*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017).
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.* at 1246.
[111] *Id.*
[112] CTR. FOR INTERNET SEC., CIS CONTROL 17: INCIDENT RESPONSE MANAGEMENT (2022), https://controls-assessment-specification.readthedocs.io/en/stable/control-17/.

triage the incident response.[113] These experts then conduct an investigation to identify the relevant threat vector, neutralize escalation, and work to maintain victim business continuity.[114] To achieve this, incident response professionals often stand up around the clock security operations centers to monitor threats.[115]

For companies seeking a more proactive approach, cyber incident response firms offer their services on a retainer basis.[116] Retainer services help companies optimize "remediation measures with advanced planning, forward-deployed capabilities and on-demand resources for incident response."[117] Pre-deploying cyber defense capabilities can help shorten incident response times when attacks do occur.[118]

Incident response firms not only help victims remediate and contain incidents, but also make recommendations for how victims can implement more resilient cyber defenses.[119] Recommendations often include cyber best practices like offline backups, endpoint detection, behavior-based detection, and multi-factor authentication.[120]

4. Ransomware Payment Negotiators

Ransomware created a new niche market for ransom negotiators that did not exist a few years ago.[121] There are now roughly a half-dozen ransomware negotiation companies who help victims "navigate the world of cyber extortion."[122] As more victims rely on these experts, some have criticized ransom negotiators for facilitating payments to criminal hackers.[123]

---

[113] *See, e.g., Modern Ransomware and Incident Response Solutions*, MANDIANT, https://www.mandiant.com/resources/modern-ransomware.
[114] *Modern Ransomware and Incident Response Solutions*, MANDIANT, https://www.mandiant.com/resources/modern-ransomware.
[115] *Id.*
[116] *See, e.g., Rapid Response Retainer,* VERIZON (2022), https://www.verizon.com/business/products/security/incident-response-investigation/rapid-response-retainer/?_ga=2.114554183.1531745227.1644877823-843136888.1644877823.
[117] *Rapid Response Retainer,* VERIZON (2022), https://www.verizon.com/business/products/security/incident-response-investigation/rapid-response-retainer/?_ga=2.114554183.1531745227.1644877823-843136888.1644877823.
[118] *Id.*
[119] *See, e.g.,* CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 23 (2021).
[120] CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 23–24 (2021).
[121] Rachel Monroe, *How to Negotiate with Ransomware Hackers*, NEW YORKER (May 31, 2021), https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.
[122] *Id.*
[123] *Id.*

Negotiations with ransomware gangs often take place over a short time period using instant messaging platforms.[124] Because many hackers are not native English speakers, "one-sentence messages from the hackers in broken English is the norm."[125] Entire negotiations sometimes conclude after only ten to fifteen exchanges with attackers.[126]

Experienced ransomware negotiators give victim companies an edge at the bargaining table because they have detailed profiles on ransomware groups they have dealt with in the past.[127] The profiles detail standard threat actor operations, including past ransom demand patterns.[128] This allows victims to enter negotiations with a clear strategy and avoid expensive mistakes with hackers.[129]

These mistakes include aggressive negotiation tactics and quickly offering to increase ransom demand counteroffers which signals to adversaries that there is more money on the table.[130] Ransomware groups have also begun stealing victims' cyber insurance policies so they know the deductible and coverage limits of their victims—key information in the negotiation.[131]

Example of Defaced Ukrainian Government Website
Source: Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html

D. Russian Cyber Aggression

Well before its unlawful and unprovoked invasion of Ukraine, Russia executed several coordinated cyberattack campaigns against Ukraine and other

---

[124] Brian Fung & Clare Sebastian, *What it's really like to negotiate with ransomware attackers*, CNN (Jul. 13, 2021), https://www.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html.
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] Rachel Monroe, *How to Negotiate with Ransomware Hackers*, NEW YORKER (May 31, 2021), https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.
[131] Brian Fung & Clare Sebastian, *What it's really like to negotiate with ransomware attackers*, CNN (Jul. 13, 2021), https://www.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html.

eastern European countries.[132] Indeed, researchers and government agencies have attributed dozens of debilitating attacks on eastern European countries to Russia since 2007.

In April 2007, Russia orchestrated a Denial of Service (DDOS) attack against Estonia.[133] The attack impacted Estonian government websites, parliament, banks, ministries, newspapers, and broadcasters.[134] Russia executed another DDOS attack against Georgia in August 2008 impacting 54 Georgian websites and 90 percent of state institution websites.[135] The attack left the Georgian government barely able to communicate on the Internet.[136] In 2009, Russia launched DDOS attacks against Kyrgyzstan's two primary internet servers for the country's websites and email.[137] The attack came on the same day Russia was pressuring Kyrgyzstan to cut off United States access to Manas Air Base.[138]

Following anti-government protests in March 2014, Russia likely deployed "snake" malware against the Ukrainian Prime Minister's Office and several Ukrainian embassies.[139] According to a subsequent report by BAE Systems, the snake malware provided full remote access and was difficult to detect because of its ability to remain inactive for several days.[140] In March 2015, another likely Russian malware campaign—Operation Potao Express—targeted the Ukrainian government, military, and one major Ukrainian news agency.[141] In December 2015, Russia used malware to compromise three Ukrainian power companies causing

---

[132] *See, e.g.*, Press Release, Ukraine Ministry of Digital Transformation, Russia Intends to Reduce Trust in the Government with Fakes About the Vulnerability of Critical Information Infrastructure and the "Drain" of Ukrainian Data (Jan. 16, 2022), https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv (translated to English); *see also, e.g.*, Brad Smith, *Digital technology and the war in Ukraine*, MICROSOFT (Feb. 28, 2022), *https*://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/; Robert Falcone, Mike Harbison, & Josh Grunzweig, *Threat Brief: Ongoing Russia and Ukraine Cyber Conflict*, PALO ALTO NETWORKS (Jan. 20, 2022), https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

[133] U.S. DEP'T OF STATE, INTEGRATED COUNTRY STRATEGY: ESTONIA 3 (Jan. 2021), https://www.state.gov/wp-content/uploads/2021/01/ICS_EUR_Estonia_Public-Release.pdf.

[134] EUR. UNION INST. FOR SEC. STUDIES, HACKS, LEAKS, AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES 18–19 (Oct. 2018), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

[135] *Id.* at 59.

[136] Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, U.S. ARMY WAR COLLEGE (2008), https://apps.dtic.mil/sti/pdfs/ADA636632.pdf.

[137] Maj. William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, U.S. ARMY COMMAND & GEN. STAFF COLLEGE (2009), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

[138] *Id.*

[139] Chester Wisniewski, *Cyberthreats during Russian-Ukrainian tensions: what can we learn from history to be prepared?* SOPHOS (updated Mar. 7, 2022), https://news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/.

[140] BAE SYSTEMS, THE SNAKE: CYBER ESPIONAGE TOOLKIT 33 (2014).

[141] ESET, OPERATION POTAO EXPRESS: ANALYSIS OF A CYBER-ESPIONAGE TOOLKIT 2, 14 (2015), https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf.

power outages for roughly 225,000 customers.[142] These campaigns reportedly include defacing websites as shown in the adjacent graphic. Other examples related to the subject of this report include deploying wiper malware disguised as ransomware that targets and deletes startup files and user data.[143] According to analysis by Ukraine's State Service of Special Communication and Information Protection (SSCIP), the malware, dubbed "WhisperKill," masquerades as ransomware.[144] Both SSCIP and Cisco's Talos Cyber Intelligence Group identified WhisperKill as similar and likely a modification of previously seen ransomware, WhiteBlackCrypt (encrypt3d).[145] When deployed, it encrypts the contents of the Master Boot Record (MBR) and C:\ partition of the system, likely in a false-flag attempt to disguise its true origins and intent.[146] WhisperKill's fake ransom note contained a trident—also part of the Ukrainian coat of arms—

Fake ransom message presented by WhisperKill. Source: Ukraine State Service of Special Communications & Information Protection, Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480

---

[142] *ICS Alert (IR-ALERT-H16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (revised Jul. 20, 2021), https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[143] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

[144] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation, https://cip.gov.ua/services/cm/api/attachment/download/44480 (Jan. 26, 2022 13:35).

[145] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

[146] A false-flag is the fabrication of pretext to justify an invasion. Press Release, U.S. Dep't of Defense, Pentagon Press Secretary John F. Kirby Holds a Press Briefing (Feb. 3, 2022), https://www.defense.gov/News/Transcripts/Transcript/Article/2922998/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/. Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

bolstering SSCIP's assessment this was a false flag attack.[147]

In short, WhisperKill was disguised to be motivated by financial or ideological considerations, instead of a destructive Russian-sponsored attack.[148] Unlike ransomware, however, WhisperKill deletes the decryption key after completing the encryption operation, making it impossible to decrypt the data, even if the victim pays the ransom. [149] This makes WhisperKill a useless tool for ransomware attackers because victims will never pay the ransom. From the user's perspective, all their data is deleted irrecoverably.

WhisperKill is not Ukraine's first experience with wiper malware masquerading as ransomware. In June 2017, Ukraine was hit with an aggressive wiper malware called NotPetya, with similar characteristics to WhisperKill, including masquerading as ransomware and destroying the MBR.[150] The White House, publicly attributed the NotPetya attack to the Russian military, describing it as "the most destructive and costly cyber-attack in history . . . causing billions of dollars in damage" and "part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrat[ing] ever more clearly Russia's involvement in the ongoing conflict."[151] The statement went on to call it "a reckless and indiscriminate cyber-attack that will be met with international consequences."[152] The following month, in response to Russia's "significant efforts to undermine U.S. cybersecurity," the United States imposed sanctions against Russian intelligence agencies and officials.[153]

Both Ukraine and the United States have warned that U.S. agencies and critical infrastructure could be Russia's next target in retaliation for our unwavering support of Ukraine.[154]

---

[147] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480 (translated to English).
[148] *Id.*
[149] *Id.*
[150] Release, White House, Statement from the Press Secretary (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.
[151] Release, White House, Statement from the Press Secretary (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.
[152] *Id.*
[153] Fact Sheet, White House, President Donald J. Trump is Standing Up To Russia's Malign Activities (Apr. 6, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-standing-russias-malign-activities/.
[154] Ukraine Ministry of Digital Transformation, Russia Intends to Reduce Trust in the Government with Fakes About the Vulnerability of Critical Information Infrastructure and the "Drain" of Ukrainian Data (Jan. 16, 2022), https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv

E. Notable Known Ransomware Attacks

In the last year, several ransomware attacks caused substantial disruptions to critical industry sectors. Three examples include the attacks on Colonial Pipeline, JBS Foods, and Kaseya. Each is profiled in greater detail below.

1. Colonial Pipeline

Based in Georgia, Colonial Pipeline (Colonial) operates the largest refined fuel pipeline in the United States.[155] Spanning more than 5,500 miles, Colonial provides roughly half of the transportation fuel consumed on the East Coast and provides energy to more than 50 million Americans.[156] The United States Senate Committee on Homeland Security and Government Affairs held a hearing on the attack on June 8, 2021 with Colonial Pipeline Chief Executive Officer (CEO) Joseph Blount.[157]

Colonial detected its attack in the early morning of May 7, 2021 after an employee discovered the ransom note.[158] To contain the attack, Colonial initiated the shutdown process soon after discovery.[159] In just over an hour, Colonial shut down operations for all 5,500 miles of the pipeline.[160] It total, Blount testified that it took Colonial "fifteen minutes to close down the conduit, which has about 260 delivery points across 13 states and Washington, D.C."[161]

(translated to English); *Shields Up*, CYBERSECURITY & INFRA. SEC. AGENCY, https://www.cisa.gov/shields-up.

[155] *About Us/Our Company*, COLONIAL PIPELINE, https://www.colpipe.com/about-us/our-company.

[156] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

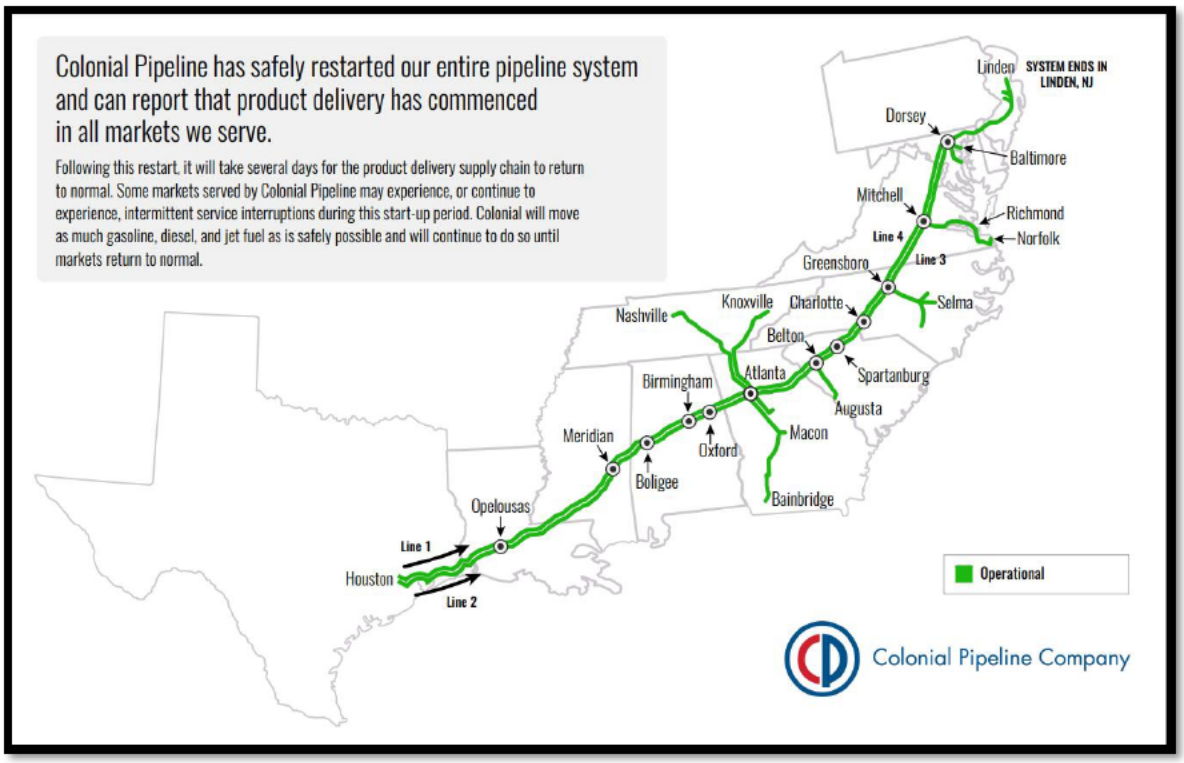
[157] *See generally Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021).

[158] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (written testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

[159] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

[160] *Id.*

[161] *Id.*



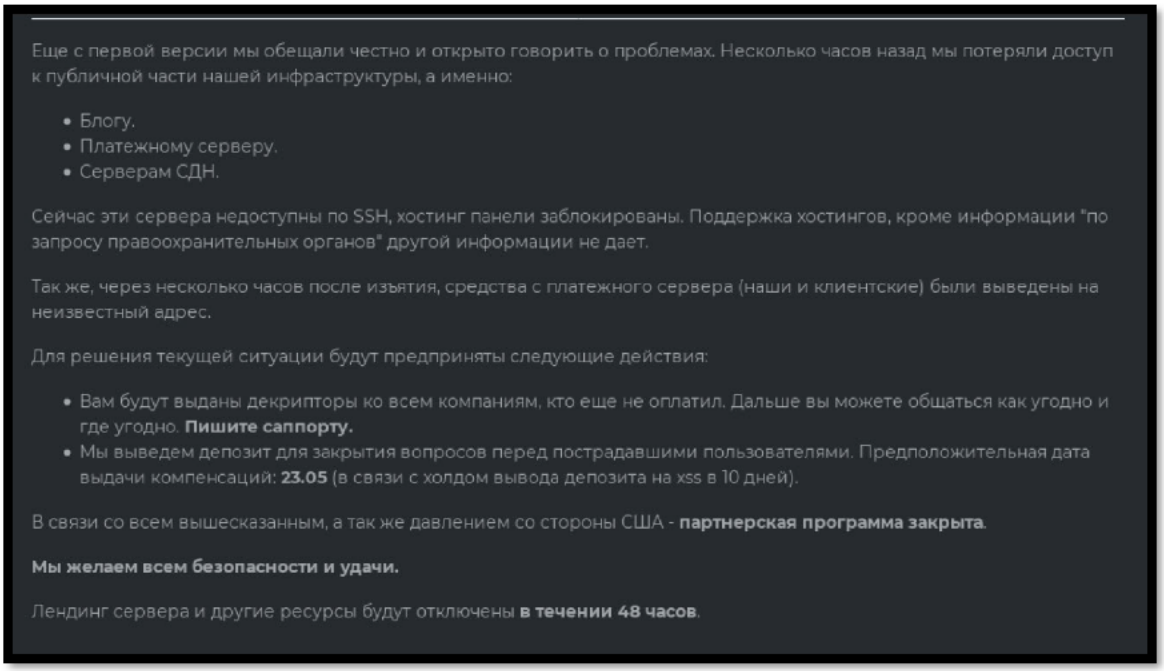
Colonial Pipeline Map
Source: Press Release, Colonial Pipeline, Media Statement Update: Colonial Pipeline System Disruption (May 17, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

By the evening of May 7th, Blount made the decision to negotiate with the attackers and paid a $4.4 million ransom the next day.[162] Blount called this "one of the hardest decisions I have had to make in my life," but believed "restoring critical infrastructure as quickly as possible, in this situation, was the right thing to do for the country."[163] Colonial's shutdown led to the highest gas prices in six and a half years and left thousands of East Coast gas stations without fuel.[164] On May 17th, Colonial issued a press release saying its normal operations were restored and it was "transporting refined products at normal levels."[165]

---

[162] *Id.*
[163] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (written testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).
[164] Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, WALL ST. J. (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.
[165] Press Release, Colonial Pipeline, Media Statement Update: Colonial Pipeline Systems Disruption (May 17, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

The FBI attributed the attack on Colonial to a criminal gang based in Russia, known as DarkSide.[166] On May 13th, just days after Colonial discovered the attack, DarkSide announced it lost access to its attack infrastructure and discontinued all operations.[167] A screenshot of the message DarkSide sent to its affiliates is pictured below. Translated to English, the message says "due to pressure from the U.S., the affiliate program is closed. Stay safe and good luck."[168]



Еще с первой версии мы обещали честно и открыто говорить о проблемах. Несколько часов назад мы потеряли доступ к публичной части нашей инфраструктуры, а именно:

- Блогу.
- Платежному серверу.
- Серверам СДН.

Сейчас эти сервера недоступны по SSH, хостинг панели заблокированы. Поддержка хостингов, кроме информации "по запросу правоохранительных органов" другой информации не дает.

Так же, через несколько часов после изъятия, средства с платежного сервера (наши и клиентские) были выведены на неизвестный адрес.

Для решения текущей ситуации будут предприняты следующие действия:

- Вам будут выданы декрипторы ко всем компаниям, кто еще не оплатил. Дальше вы можете общаться как угодно и где угодно. **Пишите саппорту.**
- Мы выведем депозит для закрытия вопросов перед пострадавшими пользователями. Предположительная дата выдачи компенсаций: **23.05** (в связи с холдом вывода депозита на xss в 10 дней).

В связи со всем вышесказанным, а так же давлением со стороны США - **партнерская программа закрыта**.

Мы желаем всем безопасности и удачи.

Лендинг сервера и другие ресурсы будут отключены **в течении 48 часов**.

DarkSide Closure Message to Affiliates
Source: The moral underground? Ransomware operators retreat after Colonial Pipeline hack, INTEL 471 (May 14, 2021), https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.

In June, the Department of Justice (DOJ) recovered roughly $2.3 million of Colonial's initial ransom payment.[169] After paying the ransom to DarkSide, Colonial sent the FBI the Bitcoin address where the company transmitted the

[166] Press Release, Fed. Bureau of Investigation, FBI Statement on Compromise of Colonial Pipeline Network (May 10, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks; Press Release, FBI Deputy Director Paul M. Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline (Jun. 7, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline.
[167] *The moral underground? Ransomware operators retreat after Colonial Pipeline hack*, INTEL 471 (May 14, 2021), https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.
[168] *Id.*
[169] Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

payment.[170] Investigators then traced the funds through several addresses before landing at a specific address for which the United States Government had a private key allowing it to seize the illicit funds.[171]

2. JBS Foods

JBS Foods (JBS) is the world's largest beef producer and a leading chicken and pork supplier in the United States.[172] JBS has operations around the world, including in the United States, Australia, United Kingdom, Mexico, Brazil, and Canada.[173]

Closed JBS Plant on June 1, 2021
Source: Derek B. Johnson, Ransomware, SolarWinds forced cybersecurity into public's consciousness, says CISA chief, SC MEDIA (Nov. 10, 2021), https://www.scmagazine.com/analysis/policy/ransomware-solarwinds-forced-cybersecurity-into-publics-consciousness-says-cisa-chief?es_p=13943087.

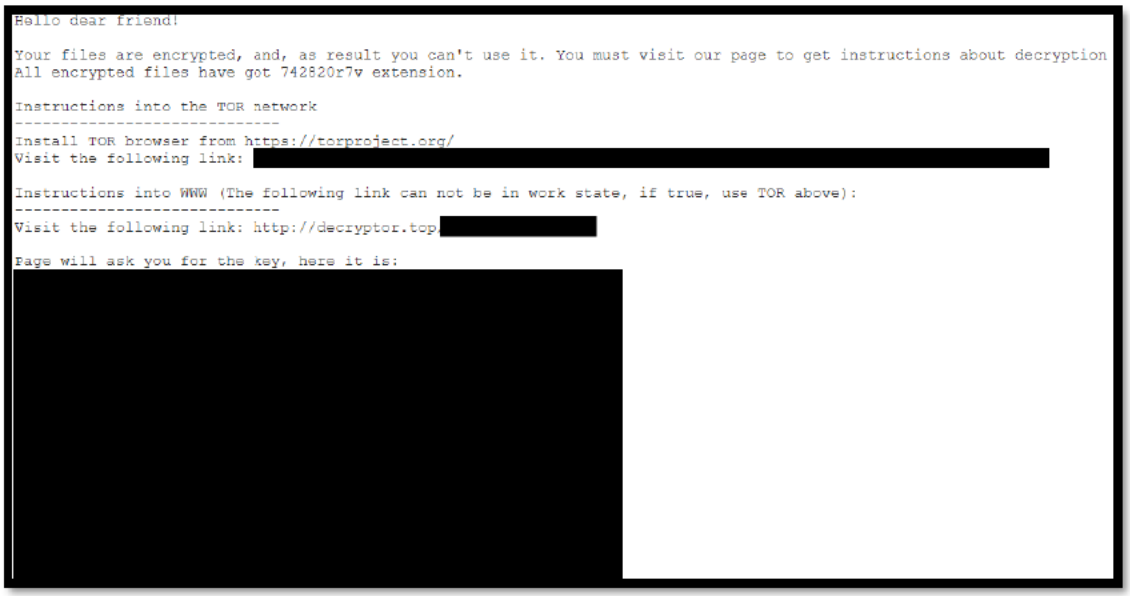
On May 30, 2021, JBS's American subsidiary, JBS USA, announced it "determined that it was the target of an organized cybersecurity attack, affecting

---

[170] Aff. In Support of App. for a Seizure Warrant at ¶28, June 7, 2021, 3:21-mj-70945-LB, https://www.justice.gov/opa/press-release/file/1402056/download.
[171] *Id.* at ¶¶ 29–34; Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. Private keys allow users to make digital currency transfers. *Questions on Virtual Currency*, U.S. DEP'T OF TREASURY (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.
[172] *Our Business*, JBS FOODS, https://jbsfoodsgroup.com/our-business.
[173] *Id.*

some of the servers supporting its North American and Australian IT systems."[174] After discovery, JBS reported it shut down all affected systems, notified relevant authorities, and retained third-party IT experts to resolve the situation.[175] JBS's announcement also added "the company's backup servers were not affected, and it is actively working with an [i]ncident [r]esponse firm to restore its systems as soon as possible."[176]

JBS's initial announcement did not explicitly mention a ransomware attack, but the FBI attributed the incident to the notorious Russia-based ransomware group REvil on June 2nd.[177] On June 9th, JBS made an $11 million ransom payment to REvil saying, "this decision had to be made to prevent any potential risk for our customers."[178] Public reports indicate REvil's initial ransom demand was $22.5 million.[179] Below is an example of an REvil ransom note.



Example of REvil Ransomware Note
Source: Email from U.S. Senate Sergeant at Arms to Committee staff (Mar. 11, 2022) (on file with the Committee).

---

[174] Press Release, JBS USA, LLC, Media Statement: JBS USA Cybersecurity Attack (May 31, 2021), https://www.globenewswire.com/news-release/2021/05/31/2239049/17532/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html.
[175] *Id.*
[176] *Id.*
[177] Press Release, Fed. Bureau of Investigation, FBI Statement on JBS Cyberattack (Jun. 2, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-jbs-cyberattack.
[178] Press Release, JBS USA, LLC, JBS USA Cyberattack Media Statement-June 9 (Jun. 9, 2021), https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.
[179] Lawrence Abrams, *JBS paid $11 million to REvil ransomware, $22.5M first demanded*, BLEEPING COMPUTER (Jun. 10, 2021), https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/.

The attack shuttered several of the largest meat plants in the United States, including JBS facilities in Colorado, Iowa, Pennsylvania, Minnesota, Nebraska, and Texas compounding existing food supply chain strains from labor shortages and high transportation costs.[180] The U.S. Department of Agriculture issued a statement urging JBS competitors to ramp up their production to offset JBS's shutdown.[181]

3. Kaseya

Kaseya is a Miami-based software company that provides network management services.[182] Founded in 2000, more than 40,000 organizations use Kaseya's products globally, and its services help customers "efficiently manage, secure, and backup IT."[183]

Kaseya Headquarters
Source: Alex Marquardt, Ransomware group demands $70 million for Kaseya attack, CNN (Jul. 5, 2021), https://www.cnn.com/2021/07/05/business/ransomware-group-payment-kaseya/index.html.

Hackers targeted Kaseya's virtual systems administrator (VSA) software used by managed service providers to track and distribute software updates.[184] On July 3, 2021, Kaseya announced "a potential attack against the VSA that has been

---

[180] Jacob Bunge, *Meat Buyers Scramble After Cyberattack Hobbles JBS*, WALL ST. J. (Jun. 2, 2021), https://www.wsj.com/articles/meatpacker-jbs-hit-by-cyberattack-affecting-north-american-australian-operations-11622548864?mod=article_inline.

[181] Press Release, U.S. Dep't of Agric., Statement from the U.S. Department of Agriculture on JBS USA Ransomware Attack (Jun. 1, 2021), https://www.usda.gov/media/press-releases/2021/06/01/statement-us-department-agriculture-jbs-usa-ransomware-attack.

[182] *Contact Us*, KASEYA, https://www.kaseya.com/contact-us/; *We are Kaseya*, KASEYA, https://www.kaseya.com/company/.

[183] *We Are Kaseya*, KASEYA, https://www.kaseya.com/company/.

[184] *VSA*, Kaseya, https://www.kaseya.com/products/vsa/;Press Release, Continued Advisory, Kaseya (Jul. 4, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.

limited to a small number of on-premises customers."[185] After further investigation, the company announced its "VSA product has unfortunately been the victim of a sophisticated cyberattack."[186] Compromising this software allowed hackers to distribute ransomware through corrupted updates to Kaseya's broad customer base.[187] The attack was attributed to REvil, but Kaseya did not pay a ransom or communicate with the attackers.[188]

Kaseya estimates this supply chain attack compromised 60 direct customers and impacted roughly 1,500 downstream non-customers.[189] REvil issued a $70 million ransom demand to decrypt all impacted systems, but made demands between $25,000 and $5 million for individual victims to unlock their networks.[190] Below is a screenshot of one such demand.

REvil Ransom Demand to Kaseya Ransomware Victim
Source: Lawrence Abrams, REvil is increasing ransoms for Kaseya ransomware attack victims, BLEEPING COMPUTER (Jul. 4, 2021), https://www.bleepingcomputer.com/news/security/revil-is-increasing-ransoms-for-kaseva-ransomware-attack-victims/.

According to public reporting, the FBI had a decryption key obtained by accessing REvil's internal servers, but did not share the key with Kaseya victims for

---

[185] Press Release, Continued Advisory, Kaseya (Jul. 3, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[186] Press Release, Continued Advisory, Kaseya (Jul. 6, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[187] *Incident Overview & Technical Details*, KASEYA (2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961.
[188] Press Release, Continued Advisory, Kaseya (Jul. 26, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[189] *Incident Overview & Technical Details*, KASEYA (2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961.
[190] Robert McMillan, *Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack*, WALL ST. J. (Jul.5, 2021), https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076?mod=article_inline.

several weeks while the FBI planned an operation to disrupt REvil's criminal activity.[191] REvil's platform went offline before the FBI could execute this plan.[192]

The total number is unknown, but several Kaseya victims made ransom payments before the decryption key became available.[193] These payments reportedly ranged from $40,000 to $220,000.[194] Other impacted companies restored their systems from backups—a time consuming and expensive process.[195] Regardless, the downstream impact was substantial. For example, one downstream Kaseya victim, Swedish grocery store chain Coop closed 700 stores for six days, likely costing millions in lost revenue.[196]

F. REvil Arrests

Over the past year, several REvil hackers have been arrested. This includes the individuals allegedly responsible for the Kaseya and JBS attacks. One hacker, Yaroslav Vasinskyi, was arrested in Poland and extradited to the United States. In January 2022, Russian authorities claimed to arrest fourteen others.

1. Yaroslav Vasinskyi

On October 8, 2021, Polish authorities detained Yaroslav Vasinskyi as he crossed the border from Ukraine.[197] Vasinskyi, 22, is a Ukrainian national allegedly responsible for orchestrating the Kaseya attack.[198] In August 2021, a Federal grand jury in the United States indicted him for his role in the incident.[199]

The Department of Justice charged Vasinskyi with "conspiracy to commit fraud and related activity in connection with computers, substantive counts of

---

[191] Ellen Nakashima & Rachel Lerman, *FBI held back ransomware decryption key from businesses to run operation targeting hackers*, WASH. POST (Sept. 21, 2021), https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.
[192] *Id.*
[193] *Id.*
[194] OFFICE OF THE CYBER EXEC., NAT'L COUNTERINTELLIGENCE & SEC. CTR., KASEYA VSA SUPPLY CHAIN RANSOMWARE ATTACK (Aug. 10, 2021), https://www.odni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf.
[195] Ellen Nakashima & Rachel Lerman, *FBI held back ransomware decryption key from businesses to run operation targeting hackers*, WASH. POST (Sept. 21, 2021), https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.
[196] *Id.*
[197] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charge with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.
[198] *Id.*
[199] Indictment at 1, United States v. Vasinskyi, 3-21CR0366-S (N.D. Tex. 2021).

damage to protected computers, and conspiracy to commit money laundering."[200] If convicted on all counts, Vasinskyi could face up to 145 years in prison.[201] On March 9, 2022, the United States successfully extradited and arraigned Vasinskyi in the Northern District of Texas.[202]

At the same time the Department of Justice disclosed Vasinskyi's arrest, it also announced the seizure of $6.1 million from another REvil hacker named Yevgeniy Polyanin.[203] Polyanin is a Russian national linked to "3,000 ransomware attacks that netted $13 million in ransom from entities across the United States."[204] He was separately charged with the same crimes as Vasinskyi.[205] Polyanin remains at large.[206]

2. Russian Federal Security Service Arrests

On January 14, 2022, Russia's Federal Security Service (FSB) arrested 14 alleged REvil gang members, including the individual senior U.S. officials claim was responsible for the Colonial Pipeline attack.[207] This individual switched to work for REvil after his previous gang, DarkSide, disappeared after the Colonial attack.[208]

---

[200] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.
[201] *Id.*
[202] Press Release, U.S. Dep't of Justice, Sodinokibi/REvil Ransomware Defendant Extradicted to United States and Arraigned in Texas (Mar. 9, 2022), https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas.
[203] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charge with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; *See also generally* United States v. Vasinskyi, 3-21CR0366-S (N.D. Tex. 2021).
[204] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; Ellen Nakashima & Dalton Bennett, *Ring of ransomware hackers targeted by authorities in United States and Europe*, WASH. POST (Nov. 8, 2021), https://www.washingtonpost.com/national-security/revil-ransomware-arrests-doj/2021/11/08/9432dfc2-409f-11ec-a88e-2aa4632af69b_story.html.
[205] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.
[206] *Id.*
[207] Robyn Dixon & Ellen Nakashima, *Russia arrests 14 alleged members of REvil ransomware gang, including hacker U.S. says conducted Colonial Pipeline attack*, WASH. POST (Jan. 14, 2022), https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/.
[208] *Id.*

REvil Hacker Arrested by Russian Authorities
Source: REvil ransomware gang arrested in Russia, *BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.*

Russian authorities raided 25 addresses "seizing more than $1 million in U.S. currency, euros, Bitcoin, and rubles, as well as computer equipment and 20 luxury cars."[209] U.S. law enforcement provided FSB with information on the identity and criminal activities of REvil's leader.[210] The 14 individuals arrested will be prosecuted in Russia and will not be extradited to the United States.[211] Below is money the FSB seized during the arrests.

Money Seized Duirng FSB Arrests
Source: REvil ransomware gang arrested in Russia, *BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.*

---

[209] *Id.*
[210] *Id.*
[211] *REvil ransomware gang arrested in Russia*, BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.

IV. CASE STUDIES

The section below provides three REvil ransomware victim case studies. All three entities voluntarily cooperated with the Committee's requests for information and interviews. To protect the victim companies against any retaliation by ransomware criminals, the report does not reveal their identities and has not included certain information that could be used to identify them.

The entities discussed below are from different business sectors with significant differences in size and revenue. Despite these differences, all three fell victim to an REvil ransomware attack. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

A. Entity A

Entity A is a global multi-sector Fortune 500 company with over 100,000 employees. Committee staff met with members of Entity A's senior leadership to discuss its REvil ransomware attack. Reflecting on the incident, one senior employee of Entity A remarked, that broadly speaking, U.S. companies are, "just sitting ducks" without more effective government and industry collaboration going forward.[212] As noted below, Entity A's state of cyber preparedness allowed it to effectively respond to the threat.

1. IT Structure and Incident Response Plan

IT Structure. Entity A has over 200 employees devoted to IT security, and dedicates approximately 10 percent of its overall IT budget to IT security.[213] Entity A has 146,000 total endpoints.[214]

Entity A analyzes cyber risks and threats on a continuous and on-going basis to ensure the confidentiality, integrity, and availability of its information systems.[215] As determined appropriate, Entity A supplements this analysis with

[212] Committee Briefing with Entity A (Apr. 4, 2021).
[213] Email from Entity A to Committee staff (Mar. 15, 2022) (on file with the Committee).
[214] *Id.* An endpoint is any remote device that communicates with a network. Examples include desktops, laptops, smartphones, tablets, and servers. *What is an Endpoint*, PALO ALTO NETWORKS (2022), https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint.
[215] Email from Entity A to Committee staff (Mar. 15, 2022) (on file with the Committee).

third-party cybersecurity products.[216] Entity A senior leadership receives regular briefings on security issues and no less than once per month.[217]

Incident Response Plan. Entity A had a formal incident response plan in place when the attack occurred.[218] Among other things, this plan specifies that Entity A implement network segmentation, disable business-to-business connections, implement aggressive endpoint controls, engage outside counsel and third-party response services, sever internet access, and perform forensic analysis.[219]

Entity A informed the Committee it adhered to its incident response plan during the attack.[220] Entity A continually updates this plan to address gaps and account for the constant changes in attacker techniques.[221]

2. Attack Background

According to Entity A, REvil compromised a known vulnerability on a legacy server of one of its vendors.[222] From there, attackers impersonated the vendor and sent an unsuspecting Entity A employee an email attachment corrupted with ransomware.[223] After opening the attachment, the ransomware encrypted Entity A's networks.[224]

After locking down Entity A's networks, REvil issued a $70 million ransom demand.[225] To assist with incident response, Entity A retained Microsoft's Detection and Response Team.[226] After forensic analysis, Entity A confirmed REvil was responsible and traced the Internet Protocol (IP) addresses back to servers in Amsterdam.[227]

3. Attack Impact

Entity A did not pay the ransom demanded by REvil.[228] After its networks were encrypted, Entity A shut down all impacted systems to protect data and was forced to rebuild several of these systems following the attack.[229] There is no

---

[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Id.*
[221] *Id.*
[222] Committee Briefing with Entity A (Apr. 4, 2021).
[223] *Id.*
[224] *Id.*
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] *Id.*
[229] *Id.*

indication REvil exfiltrated customer data or accessed any proprietary or classified information.[230]

During the incident response, Entity A observed the threat actors moving around its networks and the information they were attempting to access.[231] REvil did not demonstrate a particular interest in specific information held by Entity A, but instead moved around randomly trying to access whatever information they could.[232]

It took Entity A roughly a week to evict the hackers and secure its networks from subsequent attacks.[233] Entity A suggested it would have taken much longer to cut off hacker access without its vast resources and robust backups.[234] REvil claimed its motivation for the attack was purely financial and did not provide a more targeted explanation for selecting Entity A as a victim.[235] After Entity A declined to make a ransom payment, REvil started making threatening phone calls to leadership attempting to coerce a ransom payment.[236]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. After confirming the attack, Entity A notified the FBI and other law enforcement agencies.[237] Overall, Entity A found the FBI to be unhelpful throughout the process. Entity A asked the FBI for best practices and other guidance documents, but did not receive helpful assistance when responding to the attack.[238] For example, the FBI offered their hostage negotiator who appeared to have little expertise in responding to ransomware attacks.[239] Entity A indicated the FBI prioritized investigating those responsible for the attack over helping Entity A respond and secure its network—the top priority for Entity A.[240] Entity A had no interaction with Department of Homeland Security or CISA during the incident.[241]

Lessons Learned. Entity A said its biggest takeaway is the sophistication of hostile actors and the financial means at their disposal.[242] Entity A has sophisticated cybersecurity, and yet it was unable to prevent this attack.[243] Entity

---

[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*
[238] *Id.*
[239] *Id.*
[240] *Id.*
[241] *Id.*
[242] *Id.*
[243] *Id.*

A recommended the Federal Government better coordinate its approach to responding and defending against such sophisticated and well-funded adversaries.[244] Entity A said it wished it could have shared more information with others about its experience with REvil, and that previous victims could have shared more information to help them.[245] According to Entity A, such information sharing continues to be penalized or discouraged under the current legal and regulatory framework.[246]

Finally, this incident solidified the importance of Entity A's IT backups.[247] Without viable offline backups after REvil's deployed its ransomware, Entity A told the Committee, it may have taken weeks to get its systems back online.[248] Such a disruption would almost certainly have caused serious national economic repercussions across several business sectors.[249]

B. Entity B

Entity B is a global manufacturing company with several thousand employees. Three members of Entity B's senior leadership met with Committee staff to discuss its REvil ransomware attack.

1. IT Structure and Incident Response Plan

IT Structure. Entity B has 170 employees in its IT department, roughly ten of whom are devoted to IT security.[250] Entity B's total annual IT budget is $65 million.[251] This includes all in-house software subscriptions.[252] Approximately eight percent of that $65 million is devoted to IT security, and this percentage has increased since the attack.[253] In total, Entity B has roughly 6,000 endpoints.[254]

Entity B employs traditional endpoint security, multi-factor authentication, anti-virus software, virtual private network (VPN), and single sign-on solutions.[255] Senior leadership is briefed on all significant cyber incidents, and the Chief

---

[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] Committee Briefing with Entity B (Jan. 6, 2022). Entity B also employs IT security professionals in other departments. *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] *Id.*
[255] *Id.*

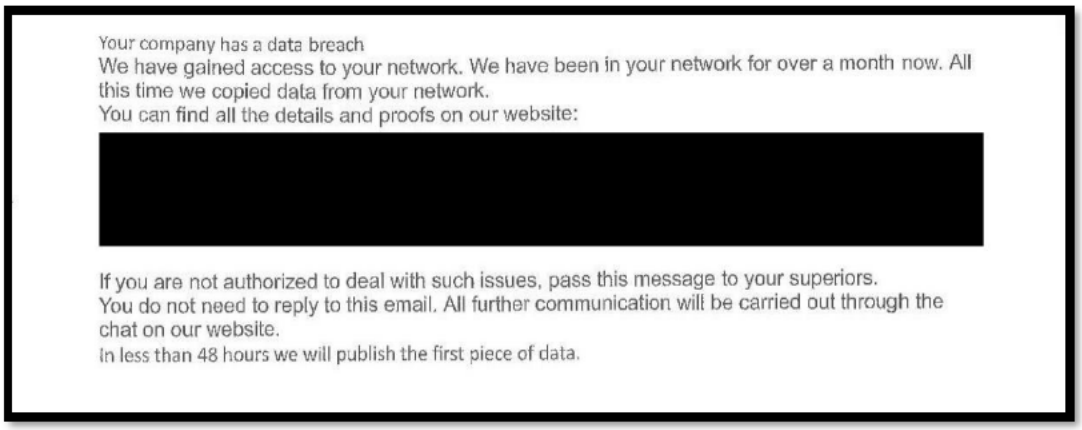
Information Officer (CIO) briefs the audit committee of the Board of Directors eight times a year.[256]

Incident Response Plan. Entity B had an established incident response plan at the time of the attack.[257] The incident response plan was implemented years before the attack, and was updated in the fall prior to the attack.[258] This plan provides that Entity B will keep external consultants on retainer and documents key points of contact in the event of a breach.[259] It also provides for annual table top exercises to test Entity B's cyber preparedness.[260]

Entity B told the Committee its incident response plan enabled Entity B's immediate ability to hire the external consultants necessary to understand the incident's impact.[261] Any gaps identified during the attack were in the company's cyber infrastructure and not the incident response plan.[262]

2. Attack Background

An IT security employee discovered the attack after noticing an unusual log-in to the company's Google cloud environment.[263] The CIO was notified of the incident immediately, and senior leadership including the General Counsel, CEO, and CFO were briefed within four days.[264]



REvil Message to Entity B
Source: Email from Entity B to Committee staff (Mar. 10, 2022) (on file with the Committee).

256 *Id.*
257 *Id.*
258 *Id.*
259 *Id.*
260 *Id.*
261 *Id.*
262 *Id.*
263 *Id.*
264 *Id.*

After discovering the attack, Entity B initiated its incident response plan and sealed off its networks so its data could not be encrypted by REvil.[265] At this point, REvil made its initial ransom demand confirming Entity B was breached.[266]

REvil compromised Entity B's networks through an email phishing attack.[267] The email was opened by a mid-level employee who thought it was a legitimate email from their bank.[268] Following initial access, hackers spent a month trying to elevate privileges, but were limited to the one compromised employee's access.[269] After a month and a half, attackers elevated privileges and moved laterally across Entity B's networks.[270] After that lateral movement, there was a lull in activity while it is suspected the initial attackers sold their access to another REvil affiliate.[271] Entity B's forensic review seemed to confirm this theory, as they were able to observe two distinct attack vectors.[272] The second actor informed Entity B they were on its networks for about a month when they made their demand, and Entity B representatives told the Committee they did not uncover any evidence to the contrary.[273]

REvil attackers used a post-exploitation attack known as Kerberoasting to move laterally

Kerberoasting explained.

Kerberoasting is an attack technique that exploits a Windows authentication protocol called Kerberos. The technique involves a hacker with low level access on a network obtaining a hashed password to a service account through the Kerberos authentication service. Service accounts often enjoy higher level access than regular users and have simple, infrequently changed passwords that make them easier to guess. As result, an attacker may be able to use the hashed password for the service account to guess the password to the service account, and escalate access on the network. (Attackers with access to a password hash can guess a simple password very quickly and automatically through a process called "brute forcing" and widely available software tools. These tools use a dictionary file of potential passwords to try thousands of different password combinations a second until they find the right one.)

See generally Steal or Forge Kerberos Tickets: Kerberoasting, MITRE (Oct. 20, 2020), https://attack.mitre.org/techniques/T1558/003/.

[265] *Id.*
[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *Id.*
[270] *Id.*
[271] *Id.*
[272] *Id.*
[273] *Id.*

through Entity B's networks.[274] With this kind of attack, threat actors target domain administrator privileges in the hopes of gaining unrestricted access and control of the IT landscape.[275] At the time of the incident, Entity B did not have multi-factor authentication for its internal networks.[276] As a result, and because the compromised employee had already logged into the company's VPN, attackers could move freely around Entity B's networks.[277] When the breach occurred, Entity B did not have a zero trust architecture or segmented networks.[278]

REvil specifically accessed Entity B's on premises Windows drives.[279] Entity B started moving to Google Cloud several years before the attack for storage purposes, but not every employee successfully migrated.[280] REvil executed searches such as "finance" and "paycheck" and successfully stole large amounts of sensitive information.[281] All told, REvil exfiltrated about 1.5 terabytes of data from Entity B networks.[282]

REvil specifically exfiltrated Excel sheets, PowerPoints, and Word documents from company employee personal network Windows drives.[283] Attackers also obtained and posted certain employee pension information, personally identifiable information (PII), and Social Security Numbers (SSNs).[284] Entity B was most upset about the posting of employee PII.[285] No proprietary information was publicly released.[286]

---

[274] *Id.*
[275] *Id.*
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] *Id.*
[286] *Id.*

Monero.

Monero is a type of anonymity enhanced cryptocurrency (AEC) often called "privacy coins." AECs offer a greater degree of anonymity over their better-known cousin Bitcoin because they use non-public or private ledgers that make it more difficult to trace or attribute transactions.

U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 4 (2020).

3. Attack Impact

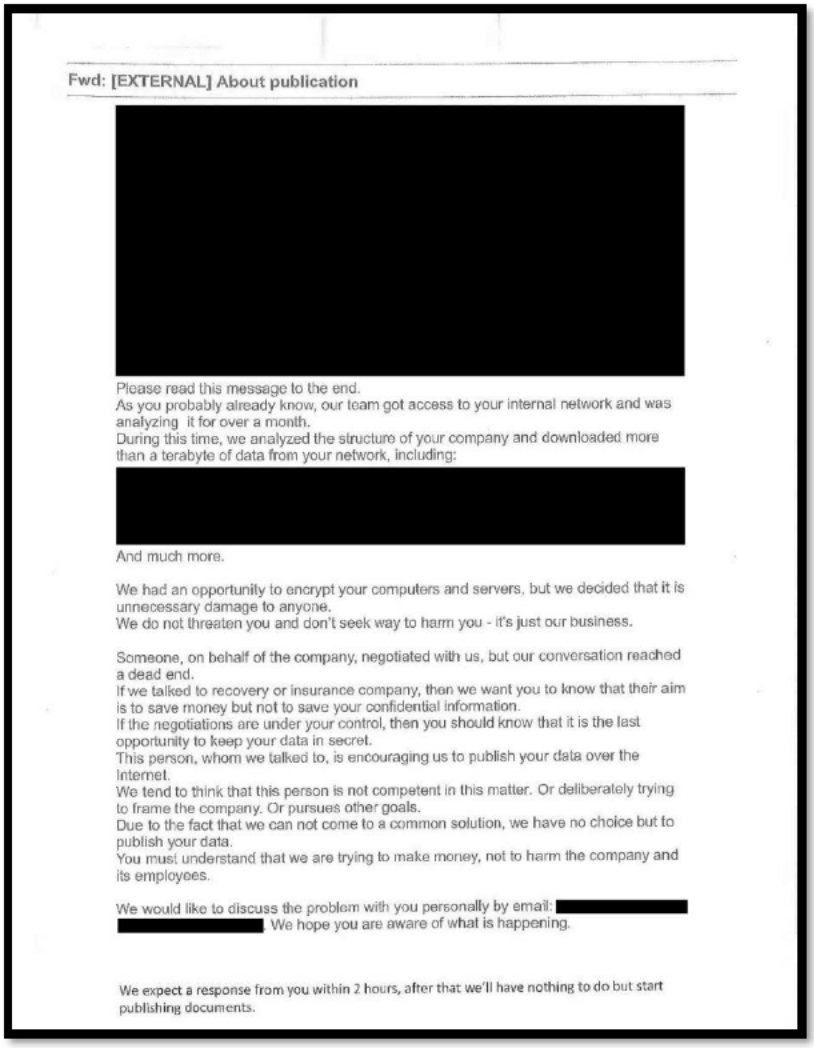
It took about a month to understand the full impact of the breach and how much data was stolen.[287] REvil issued an initial $2 million ransom demand in Monero cryptocurrency.[288] This demand escalated to $10 million before a final demand of several hundred thousand dollars.[289]

As outlined in its response plan, Entity B retained an incident response firm, outside counsel, and a ransomware negotiator.[290] It also had cyber insurance to cover the costs of retaining these experts; however, its insurance premiums rose substantially after the breach.[291]

Entity B communicated with REvil through a third-party ransomware negotiation company.[292] These communications lasted for one month after which Entity B discontinued all communications with REvil.[293] A month later, REvil harassed Entity B employees via email saying the company was allowing their PII to be publicly released.[294] According to Entity B, this harassment was the most significant follow-on activity after discovery of the breach.[295]

---

[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*
[295] *Id.*



Fwd: [EXTERNAL] About publication

[redacted]

Please read this message to the end.
As you probably already know, our team got access to your internal network and was analyzing it for over a month.
During this time, we analyzed the structure of your company and downloaded more than a terabyte of data from your network, including:

[redacted]

And much more.

We had an opportunity to encrypt your computers and servers, but we decided that it is unnecessary damage to anyone.
We do not threaten you and don't seek way to harm you - it's just our business.

Someone, on behalf of the company, negotiated with us, but our conversation reached a dead end.
If we talked to recovery or insurance company, then we want you to know that their aim is to save money but not to save your confidential information.
If the negotiations are under your control, then you should know that it is the last opportunity to keep your data in secret.
This person, whom we talked to, is encouraging us to publish your data over the Internet.
We tend to think that this person is not competent in this matter. Or deliberately trying to frame the company. Or pursues other goals.
Due to the fact that we can not come to a common solution, we have no choice but to publish your data.
You must understand that we are trying to make money, not to harm the company and its employees.

We would like to discuss the problem with you personally by email: [redacted]. We hope you are aware of what is happening.

We expect a response from you within 2 hours, after that we'll have nothing to do but start publishing documents.

REvil Message to Entity B Threatening to Release Sensitive Data
Source: Email from Entity B to Committee staff (Mar. 10, 2022) (on file with the Committee).

Entity B did not make a ransom payment to REvil in part because it was able to cut off REvil's access before they encrypted Entity B's data.[296] An Entity B representative told the Committee attackers got greedy and tried to access its Google cloud environment.[297] When REvil did this, an IT security employee observed the unusual activity and sealed off Entity B's networks.[298] According to the representatives interviewed by the Committee, the incident did not impact any

[296] *Id.*
[297] *Id.*
[298] *Id.*

Entity B operational systems.[299] In addition, Entity B maintains backups and severed connection to those once the breach was identified.[300]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. Entity B notified its local FBI Field Office within a week of detecting the incident.[301] Entity B recalled there was no "here's a playbook" discussions with the FBI regarding how to best respond.[302] The FBI did provide several contacts to help Entity B respond to the incident.[303] To assist with its investigation of REvil, Entity B submitted all relevant incident information to the FBI.[304] Entity B did not interact with CISA during the attack but does receive CISA's cybersecurity vulnerability alerts now.[305]

Lessons Learned. After the attack, Entity B acknowledged it needs to migrate to the cloud more aggressively, improve patching, and implement multi-factor authentication for its internal networks. Entity B has already improved its patching process and implemented multi-factor authentication for its internal networks.[306] In retrospect, one representative said Entity B should have forced employees to migrate to the cloud sooner, but they are able to "swing a bigger hammer" after the breach.[307] Overall, Entity B felt its incident response plan worked well, but the breach exposed gaps in its cyber architecture.[308]

C. Entity C

Entity C is a technology firm with approximately 50 total employees. Senior leadership from Entity C met with the Committee to discuss the impact of its REvil ransomware attack.

1. IT Structure and Incident Response Plan

IT Structure. Entity C has two employees devoted to IT and IT security.[309] Its overall IT budget is between $300,000 and $800,000 per year.[310] Entity C's representative did not know how much of that total budget is devoted to IT security

---

[299] *Id.*
[300] *Id.*
[301] *Id.*
[302] *Id.*
[303] *Id.*
[304] *Id.*
[305] *Id.*
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] Committee Briefing with Entity C (Jan. 27, 2022).
[310] *Id.*

or how many cyber incidents are reviewed on a daily basis.[311] In total, Entity C has roughly 55 endpoints.[312]

To protect its networks, Entity C employs endpoint detection, anti-virus software, and maintains offline network backups.[313] Senior leadership receives weekly briefings on cybersecurity matters.[314]

Incident Response Plan. Entity C had an established incident response plan at the time of the attack.[315] While one Entity C representative acknowledged its incident response plan only becomes relevant at the very end of preparedness, it allowed Entity C to respond and reconstitute its systems within a short timeframe.[316] For example, the company made payroll three days after the attack and sent invoices to customers within eight days.[317]

According to senior leadership, this incident exposed weaknesses in Entity C's incident response plan and specifically the processes for reconstituting impacted systems after an attack.[318] Following the incident, Entity C is working to implement data segregation, need-to-know access controls, and encryption.[319]

2. Attack Background

An employee discovered the attack after watching all of the files in an Entity C system get encrypted in real time.[320] IT staff received alerts of this malicious activity around the same time, and shortly thereafter, began severing internet connectivity as a risk reduction measure.[321]

Forensic analysis provided Entity C with significant evidence that hackers compromised its networks by exploiting a Microsoft vulnerability.[322] A few days after the incident, Entity C had evidence to conclude REvil was responsible for the attack.[323] Entity C does not have high confidence of precisely when its systems were breached.[324]

---

311 *Id.*
312 *Id.*
313 *Id.*
314 *Id.*
315 *Id.*
316 *Id.*
317 *Id.*
318 *Id.*
319 *Id.*
320 *Id.*
321 *Id.*
322 *Id.*
323 *Id.*
324 *Id.*

After the initial breach, the attackers were disjointed as they moved across Entity C's network.[325] Through either an effective set of human actors or automated processes, hackers identified several files and packaged them for exfiltration.[326] An Entity C representative indicated hackers spent a lot of time preparing to exfiltrate this information, but luckily never accessed Entity C's most sensitive information.[327] Attackers established persistence and moved laterally, but were cut off because Entity C discovered the breach at the same time.[328]

Entity C only knows what company data was exfiltrated based upon what REvil posted on their public blog.[329] An Entity C representative broadly described this information as PII.[330] It also included invoices for contracts, project descriptions, and payroll sheets containing full names and SSNs of Entity C employees.[331] None of the information exfiltrated by REvil was classified or proprietary.[332]

3. Attack Impact

Entity C informed the Committee the attack impact was significant during the first 24 hours, but lessened as it worked to bring its systems back online over the next six months.[333] Entity C understood the scope of the attack fairly quickly, but spent a lot of time searching for indicators of compromise that might go undetected with the help of an outside cyber forensics company.[334] In general though, REvil's tactics and activity on Entity C's networks were consistent with other ransomware attacks orchestrated by this organization.[335]

As mentioned above, REvil successfully encrypted several Entity C systems, requiring Entity C to acquire new hardware for a few of these systems.[336] Entity C had low confidence the encrypted systems could be securely reconstituted or otherwise had older firmware.[337] For the systems with older firmware, acquiring the new hardware had less to do with what the perpetrators did and more to do with desired level of confidence before they turned the systems back on.[338] The

[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*
[331] *Id.*
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] *Id.*

decryption process for systems not requiring new hardware took between several days and three months.[339]

Entity C's offline backups helped it restore its systems following the attack.[340] Entity C did not experience any substantial or irregular financial costs as a result of the attack and only had to pay for the new hardware discussed above.[341]

While the financial costs were manageable, Entity C did experience the customary stress and inconvenience associated with a ransomware attack.[342] When discussing this inconvenience, an Entity C representative noted its cyber insurance policy covered most incident response costs, but added further, "if you want to talk about *** pain . . . that is different."[343]

Entity C's cyber insurance policy transferred the risk of handling the incident from Entity C to a law firm.[344] The law firm then selected all of the providers to assist Entity C with responding to the attack.[345] Because these service providers handled most issues during the incident response, Entity C had limited interaction with the perpetrators.[346] Entity C declined to discuss specific ransomware payments or demands, but did confirm REvil made its ransom demand in cryptocurrency.[347] When asked if insurance premiums have gone up, Entity C's representative replied, "everyone's will, it doesn't have anything to do with the fact that you were hacked."[348]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. After confirming the incident, Entity C notified its contracting Federal agencies who then notified law enforcement including the FBI.[349] Entity C believes this was an opportunistic attack attributable to weaknesses in its internet-facing architecture, and not because of the information it holds.[350] Entity C preferred to respond to the attack on its own and, for the most part, the Federal Government allowed it to do so.[351] Nonetheless, Entity C said its contracting Federal agencies were helpful.[352] After the critical

[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] *Id.*
[343] *Id.*
[344] *Id.*
[345] *Id.*
[346] *Id.*
[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.*
[351] *Id.*
[352] *Id.*

incident response phase concluded, Entity C met with officials from the its contracting Federal agencies to share information relevant to the incident.[353] As a general matter, Entity C found the Federal Government's response teams were caught off guard by the idea that a group or entity would launch attacks like this on such a large scale in such a small time frame.[354]

Lessons Learned. When asked if they would have done anything differently, Entity C said they would have done more of "everything."[355] After the attack, Entity C is taking steps to ramp up its security protections with the goal of having all systems back online within 24 hours should another attack occur.[356]

V. CONCLUSION

The Committee's investigation and the case studies above demonstrate that ransomware is a significant threat for all organizations—regardless of size and sophistication. At the same time, the case studies also illustrate the steps an organization can take to lessen the worst impacts of a ransomware attack—like maintaining offline backups and encrypting sensitive data. To help address this threat and facilitate information sharing, CISA and the National Cyber Director should work with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA. Implementing this legislation will enhance the Federal Government's visibility into cyberattacks taking place across the United States and enable a coordinated response against the hostile nation-states and criminal organizations responsible.

[353] *Id.*
[354] *Id.*
[355] *Id.*
[356] *Id.*