New Risks in Ransomware: Supply Chain Attacks and Cryptocurrency

SCIENCE, TECHNOLOGY, AND PUBLIC POLICY PROGRAM

New Risks in Ransomware

Supply Chain Attacks and Cryptocurrency

Amy Robinson
Casey Corcoran
Jim Waldo

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
MAY 2022

Science, Technology, and Public Policy Program
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/stpp

SCIENCE, TECHNOLOGY, AND PUBLIC POLICY PROGRAM

New Risks in Ransomware

Supply Chain Attacks and Cryptocurrency

Amy Robinson
Casey Corcoran
Jim Waldo

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
APRIL 2022

About the Program:

The Science, Technology, and Public Policy (STPP) Program draws on insights from scholarly and applied work in science and technology, technology assessment, political science, economics, management, and law to research and practice on the intersection of science and technology with public affairs. The goal is to help develop and promote public policies that advance the application of science and technology to improvement of the human condition.

For more, visit belfercenter.org/STPP

About the Authors:

Amy Robinson is a Belfer Young Leader Student Fellow and a joint Master of Public Policy and Juris Doctorate 2022 candidate at Harvard Kennedy School and Harvard Law School. She received her BA in English summa cum laude from Harvard University in 2015. During the following three years, Amy worked as the Communications Manager at the Schools, Health & Libraries Broadband (SHLB) Coalition, an advocacy nonprofit funded by the Bill & Melinda Gates Foundation. While with the SHLB Coalition, Amy founded and directed the Advocacy Committee as well as worked closely with schools, libraries, and health providers across the country. These interactions have fueled Amy's interest in telecommunications, digital inclusion, and community broadband as well as her aspirations to continue a federal public service career. While in school, Amy has interned at the National Telecommunications and Information Administration in the Commerce Department as well as in Commissioner Geoffrey Starks' office at the Federal Communications Commission. Due to her academic achievements and public service, Amy has been recognized as a member of Phi Beta Kappa, a John Harvard scholar, and a recipient of the Carl & Lilly Pforzheimer Fellowship.

Casey Corcoran is a Belfer Young Leader Student Fellow and a dual-degree Juris Doctorate and Master of Public Policy candidate at Harvard Law School and Harvard Kennedy School. While in school, he interned with the Cybersecurity and Infrastructure Agency, the Department of Justice, and Mayer Brown in Washington, D.C. He also served as Editor-in-Chief of the Harvard National Security Journal. Prior to graduate school, he was a Captain in the United States Army and received a BA in International Studies and English Literature from Boston College.

Jim Waldo is the Gordon McKay Professor of the Practice of Computer Science in the School of Engineering and Applied Sciences at Harvard, where he teaches courses in distributed systems and privacy; the Chief Technology Officer for the School of Engineering and Applied Sciences; and a Professor of Policy teaching on topics of technology and policy at Harvard Kennedy School. Jim designed clouds at VMware; was a Distinguished Engineer with Sun Microsystems Laboratories, where he investigated next-generation large-scale distributed systems; and got his start in distributed systems at Apollo Computer. While at Sun, he was the technical lead of Project Darkstar, a multi-threaded, distributed infrastructure for massive multiplayer online games and virtual worlds; the lead architect for Jini, a distributed programming system based on Java; and an early member of the Java software organization. Jim is the author of *Java: the Good Parts* (O'Reilly) and co-authored *The Jini Specifications* (Addison-Wesley). He edited *The Evolution of C++: Language Design in the Marketplace of Ideas* (MIT Press). He co-chaired a National Academies study on privacy and co-edited the report "Engaging Privacy and Information Technology in a Digital Age." He is the author of numerous journal and conference proceedings articles, and holds over fifty patents.

Table of Contents

Executive Summary **1**

1. Changing Landscape and Emerging Threats **2**

1.1. Increased Frequency of Ransomware Attacks 2

1.2. Increased Sophistication and Rise of Ransomware-as-a-Service (RaaS) 3

1.3. Increase of Availability and Confidentiality Combination Breaches 6

1.4. Rise of Double, Triple, and Quadruple Extortion 7

1.5. More Absolute Thread of Control through Software Updates 8

1.6. Supply Chain Attacks and Open Source Software 11

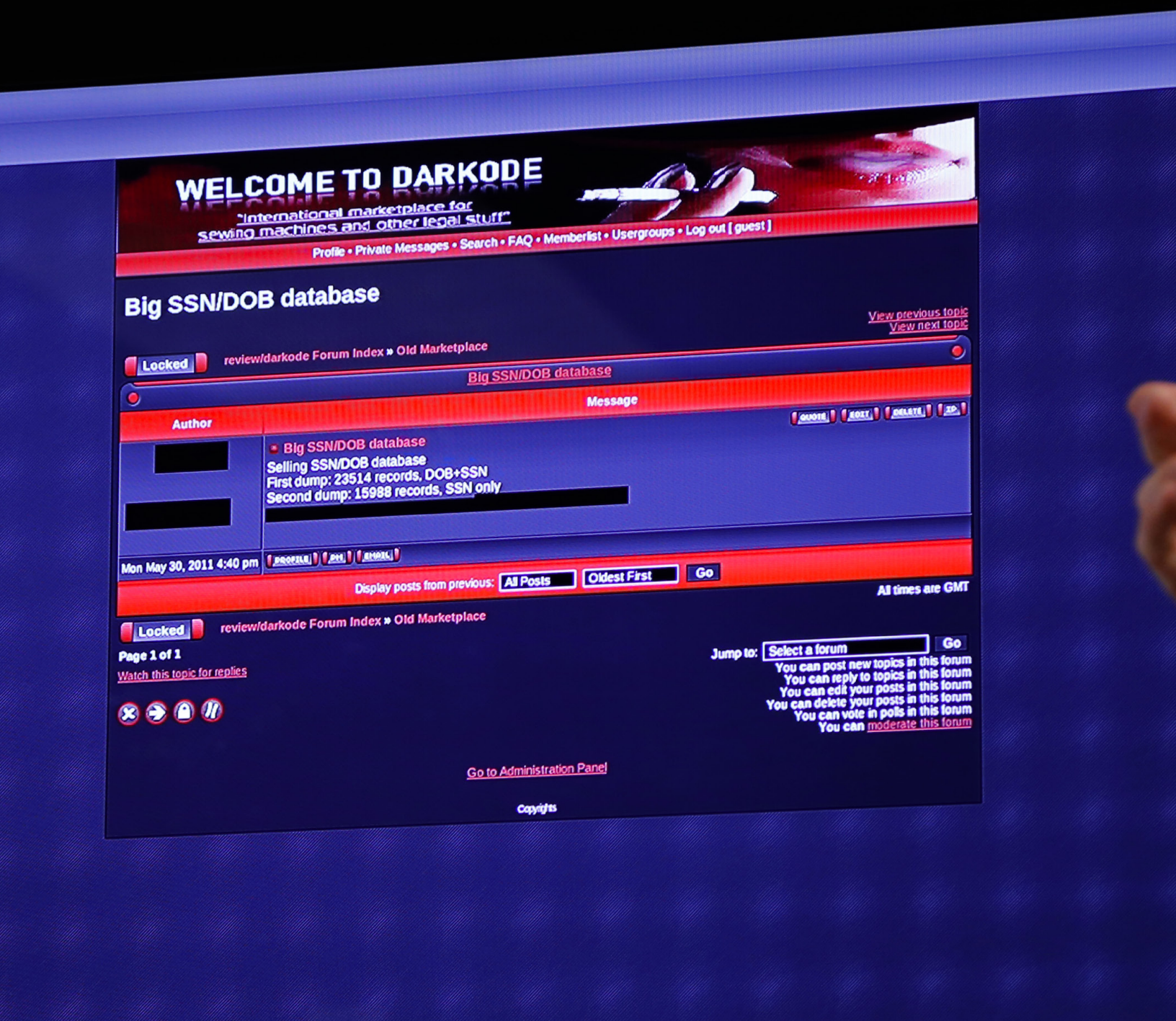
2. Emerging Solutions **14**

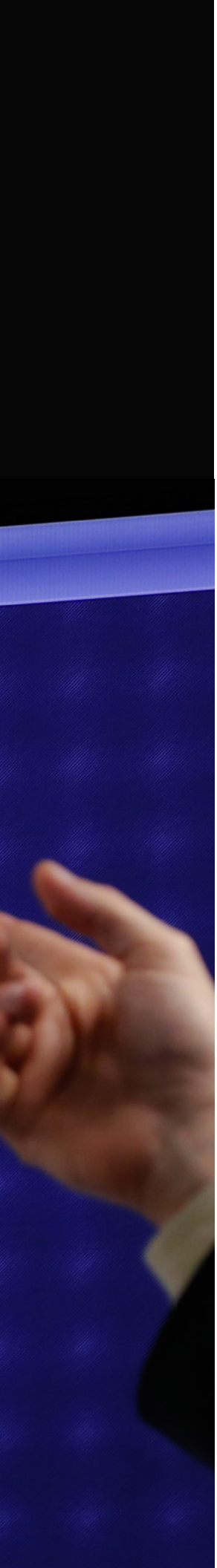
2.1. Software Bill of Materials and Bug Disclosures 14

2.2. Regulating Cryptocurrencies 17

3. Conclusion and Takeaways **21**

FBI Supervisory Special Agent J. Keith Mularski displays a screenshot from Darkcode, an English-language "marketplace for cybercriminals," the largest-known "English speaking malware forum" in the world, authorities said, at the National Cyber-Forensics & Training Alliance in Pittsburgh, Tuesday, July 14, 2015. (AP Photo/Gene J. Puskar)





Executive Summary

With the first attack dating back to 1989, ransomware is far from a new phenomenon. However, as of late, ransomware attacks have significantly changed in nature, becoming larger, more sophisticated, and more frequent. While once a rare and petty crime, ransomware has now proliferated and quickly matured into a lucrative business with the emergence of cryptocurrencies that have facilitated large, untraceable transactions. Now, organized and often state-backed hacking groups not only perpetuate sophisticated, targeted campaigns, but also franchise the infrastructure needed to carry such campaigns and sell it as Ransomware-as-a-Service (RaaS) on the dark web.

Just as concerning as the increased pace of ransomware is the emergence of a new delivery mechanism for malware that has been used in some of the most infamous ransomware attacks. As hacker groups have become increasingly sophisticated, modern software has become increasingly vulnerable to attack. Complex software must incorporate a multitude of pre-written code components from various sources, including open source code. Hacker groups can then target less secure software components, known as a supply chain attack, in order to extort a wide swath of companies or customers. Supply chain attacks are particularly dangerous if they establish a thread of control through an update package, such as the SolarWinds attack, which then provides hackers with the highest level of access to a machine's resources.

This paper seeks to provide an overview of the current ransomware landscape, such as the rise of RaaS and the increase of supply chain attacks, while also gesturing towards potential emerging solutions. While not an exhaustive list, promising solutions address the vulnerability of complex software reliant on outside code components, such as software bill of materials (SBOM) and vulnerability disclosure databases, or address the payout, such as stricter cryptocurrency regulations.

1. Changing Landscape and Emerging Threats

1.1 Increased Frequency of Ransomware Attacks

The number of ransomware incidents has recently spiked, breaking new records with each passing year. Ransomware attacks increased by 150 percent in 2020 over the previous year.[1] The FBI reported 2,084 ransomware complaints from January to July 31, 2021, which represents a 62 percent increase in incidents from January to July, 2020.[2] Unsurprisingly, the ransom payments have also drastically increased. In 2020, the amount companies paid by ransomware victims increased by more than 300 percent.[3] The trend of increased ransomware attacks has continued to grow in 2021, as shown by Blackfog's recent analysis of the year to date (see Figure 1).[4]

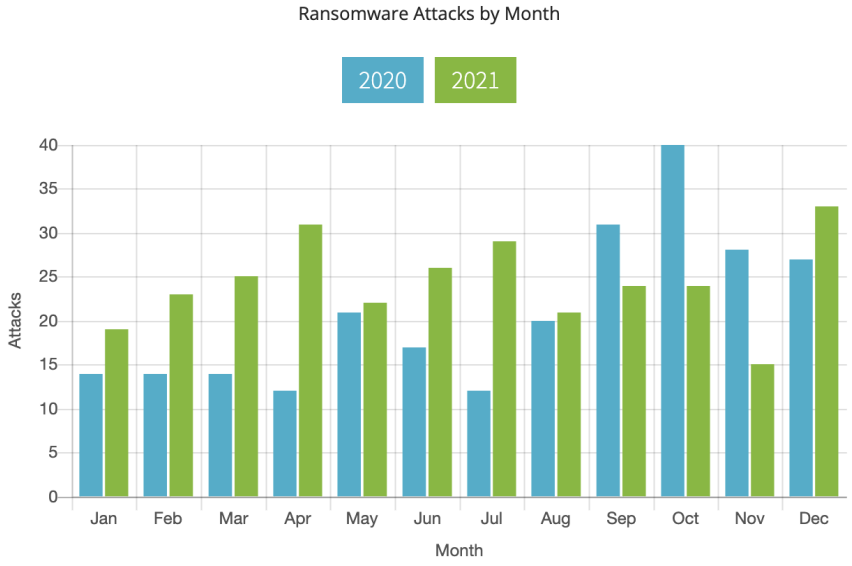


Figure 1. Ransomware Attacks by Month (Source: Blackfog, *The State of Ransomware in 2021*)

1 Brenda R. Sheraton, "Ransomware Attacks Are Spiking. Is Your Company Prepared?", *Harvard Business Review* (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared.

2 Alert (AA21-243A), Ransomware Awareness for Holidays and Weekends, CISA (Aug. 31, 2021), https://www.cisa.gov/uscert/ncas/alerts/aa21-243a.

3 Sheraton, *supra* note 1.

4 *The State of Ransomware in 2021,* Blackfog (Jan. 4, 2022) https://www.blackfog.com/the-state-of-ransomware-in-2021/.

Ransomware attacks affect nearly every sector. This can be especially dire when it impacts critical services, such as utility companies or healthcare organizations. In 2020, over 600 hospitals, clinics, and other healthcare organizations were targeted by 92 individual ransomware attacks, resulting in over $20 billion lost.[5] This amounts to a 60 percent increase in the number of attacks and a 470 percent increase in the number of patients and records affected from just the year before. In 2021, the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) recorded ransomware attacks in 14 of the 16 U.S. critical industry sectors.[6] Critical industry sectors include sectors such as communications, energy, healthcare, and emergency services.[7]

But ransomware's changing landscape extends beyond simply an increase in the number of attacks. Ransomware attacks have also become increasingly sophisticated with streamlined deployment and targeted campaigns.

1.2 Increased Sophistication and Rise of Ransomware-as-a-Service (RaaS)

Ransomware actors have evolved their targeting methods over time, shifting from near-random mass attacks to highly targeted campaigns. Early on, ransomware operators often engaged in a "spray and pray" strategy[8] in which they blindly sent out phishing emails to millions of users, encrypting the users' devices randomly.[9] These actors would then charge relatively low amounts of money to decrypt the device.[10] Recently, this pattern gave way to "big game hunting" in which ransomware actors target specific, large entities. This targeting is desirable from a ransomware

5 Paul Bischoff, *Ransomware Attacks on US Healthcare Organizations Cost $20.8bn in 2020,* Comparitech (Mar. 10, 2021), https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.

6 Alert (AA22-040A), 2021 Trends Show Increased Globalized Threat of Ransomware, CISA (Feb. 09, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a. [hereinafter Alert AA22-040A]

7 "Critical Infrastructure Sectors," CISA (last visited Mar. 30, 2022), https://www.cisa.gov/critical-infrastructure-sectors.

8 "History of Ransomware," CrowdStrike (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

9 Jonathan Fischbein, "The Evolution of Ransomware: Blocking Sophisticated 5th Generation Attacks," *Forbes* (Oct. 7, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/10/07/the-evolution-of-ransomware-blocking-sophisticated-5th-generation-attacks/?sh=6049ca2a38af.

10 CrowdStrike, *supra* note 8.

actor's perspective because it allows them to extort larger sums of money from deep pocketed organizations that have more to lose if they do not pay.[11] Big game hunting reached its peak at the start of 2021 with highly publicized attacks on Colonial Pipeline, JDS Foods, and Kaseya Limited.[12] However, since mid-2021, there has been a shift away from big game hunting,[13] since ransomware actors found that attacking large organizations attracted too much attention from law enforcement.[14] Thus, more recent ransomware operations have sustained the targeted approach of big game hunting, but aimed the attacks at mid-sized entities in order to optimize the balance between monetary return and reduced scrutiny.[15]

At the same time, ransomware has increasingly become a professionalized business model.[16] Most notably, ransomware is now offered as a service (RaaS) in which ransomware developers create a ransomware variant and any infrastructure needed to carry out the attack, such as a payment portal or a website where attackers can post a victim's sensitive information to extort payment. They then package these products in a RaaS kit and sell subscriptions to the kit on the dark web to affiliates.[17] These affiliates are the ones who select targets, interface with victims, and manage the decryption keys.[18] This business model allows affiliates who would ordinarily lack the expertise or resources to develop a ransomware variant to carry out an attack. It also increases the profitability of ransomware developers who can now collect revenue from more attacks than they could have carried out on their own.

The trend towards RaaS has led to a consolidation of the types of ransomware variants used. In the first half of 2021, nearly half of all ransomware variants detected came from four ransomware developer

11 CrowdStrike, *supra* note 8.

12 Alert AA22-040A, *supra* note 6.

13 *Id.*

14 *Id.*

15 *Id.*

16 *Id.*

17 Kurt Baker, "Ransomware as a Service (RAAS) Explained," CrowdStrike (Feb. 7, 2022), https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

18 *Id.*

groups.[19] These developer groups, or gangs, stand to make huge profits.[20] Yet, as was the case with big game hunting, with increased profits and notoriety comes increased scrutiny from law enforcement. Thus, while ransomware gang REvil claimed to make $100 million in 2020 and set a goal of reaching $1 billion, they were forced to stop operating under the combined attention of the FBI, Secret Service, and Cyber Command.[21]

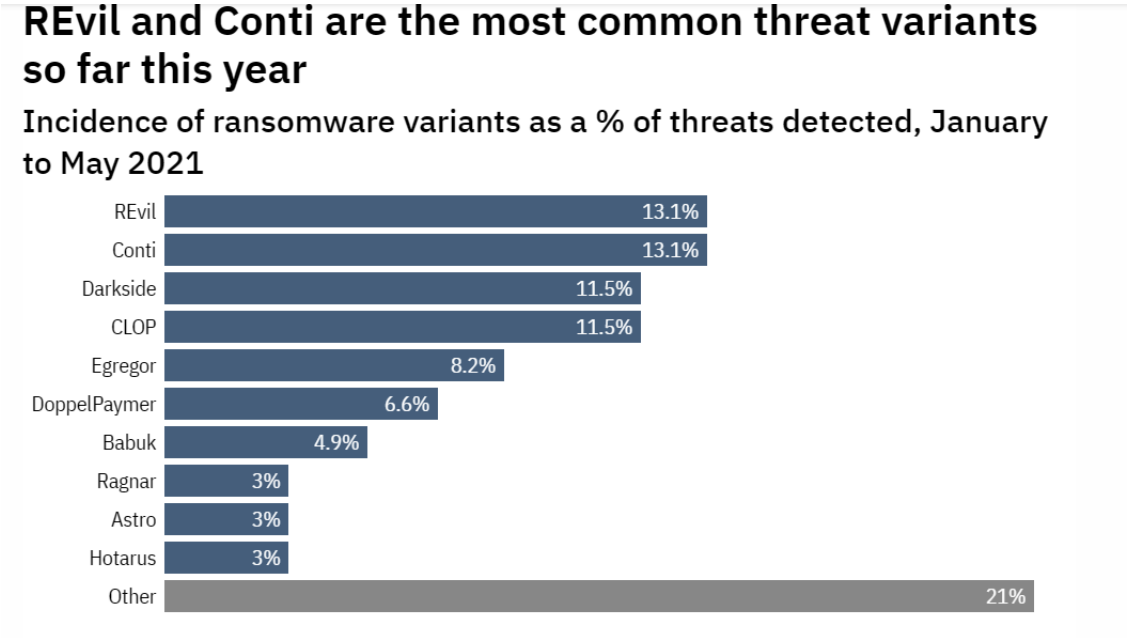


Figure 2. Incidence of ransomware variants as a percentage of threats detected, January to May 2021 (Source: Tech Monitor graph based on Blackfog, *The State of Ransomware in 2021*)

19 Claudia Glover, "Meet the Ransomware Gangs Fuelling a Global Cybercrime Spree," TECHMONITOR (Aug. 19, 2021), https://techmonitor.ai/technology/cybersecurity/top-ten-ransomware-gangs-fuelling-the-global-cybercrime-spree.

20 *Id.*

21 Mitchell Clark, "Feds Reportedly Take Down Top Ransomware Hacker Group REvil with a Hack of Their Own," *The Verge* (Oct. 22, 2021), https://www.theverge.com/2021/10/22/22740239/revil-ransomware-hacking-fbi-cyber-command-secret-service-down.

1.3 Increase of Availability and Confidentiality Combination Breaches

We can understand the evolution of both the frequency and the severity of ransomware attacks by placing that evolution within a framework of malware. As outlined in the recent Belfer Center publication, *A Framework for Cybersecurity*, common frameworks for understanding cyber attacks can help network defenders systemize their thinking and proactively counter attacks before they can occur.[22] There are two critical dimensions: (1) the goal of the attack and (2) how the attack gains a thread of control.

The various attack goals correspond to violations of the three foundational pillars of information security—confidentiality, integrity, and availability—commonly known as the CIA triad. **Confidentiality** refers to an organization's ability to keep its data private. As a corollary, violations of confidentiality occur when an adversary can read or otherwise access an organization's data. **Integrity** refers to an organization's ability to ensure that data is correct, authentic, and reliable. Violations of integrity occur when an adversary changes data within the system. **Availability** refers to an organization's ability to access information when they need it. Violations of availability occur when an adversary makes it difficult or impossible for an organization to use its system or access its data.

With the drastic rise of ransomware attacks, cybersecurity attacks have shifted from primarily availability breaches five years ago to a combination of availability and confidentiality breaches. By locking an organization's system and holding its data for ransom, ransomware attacks represent a classic attack on availability. Ransomware attacks that also threaten to release customers' sensitive information, known as double extortion, represent both an availability attack and confidentiality attack.

22 Jim Waldo, Katherine Mansted, Benjamin Goh, & Jiwon Ma, *A Framework for Cybersecurity,* Belfer Center for Science and International Affairs, Harvard Kennedy School (Dec. 2018), https://www.belfercenter.org/publication/framework-cybersecurity.

1.4 Rise of Double, Triple, and Quadruple Extortion

As noted, recent ransomware attacks have combined both confidentiality and availability attacks through the practice of "double extortion." In a typical ransomware attack, the attacker encrypts the organization's data and then demands payment in exchange for restored access.[23] This type of encryption represents "single extortion." However, in the case of double extortion, the attacker has the added threat that she will release the victims' sensitive data if the organization does not pay.[24] Double extortion therefore involves exfiltration, which is the practice of copying and transferring sensitive information. The threat of public exposure puts additional pressure on the victim organization to yield to ransom demands. The ransomware gang Maze pioneered this approach in 2019, making it a fairly novel practice.[25] As of June 2021, 35 ransomware groups had deployed double extortion.[26] In addition, according to Coveware's Q4 2020 Ransomware Report, 70 percent of all ransomware attacks during that quarter involved the threat of exfiltrated data, which represents a 43 percent increase from Q3 2020.[27]

There are additional levels of extortion beyond double extortion. "Triple extortion" occurs when the hackers launch a distributed denial-of-service ("DDoS") attack that shuts down the victim's public websites, threatens to expose confidential information, and encrypts the information held by the victim. DDoS attacks overwhelm the victim's servers with Internet traffic, resulting in a traffic jam that makes the website inaccessible to others. This triple extortion tactic puts additional pressure on the victim company to act since customers are unable to access the victim's website so long as they refuse to pay ransom.

---

23 Janus Agcaoili, Miguel Ang, Earle Earnshaw, Byron Gelera, & Nikko Tamaña, "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti," Trend Micro (Jun. 15, 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

24 *Id.*

25 *Id.*

26 *Id.*

27 "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware (Feb. 1, 2021), https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.

"Quadruple extortion" occurs when the hackers conduct triple extortion but also directly extort a compromised company's customers or suppliers.[28] A very new phenomenon, quadruple extortion was first observed in October 2020 when hackers gained access to Finnish psychotherapy records.[29] Patients of the psychotherapy company Vastaamo reported that they received emails demanding €200 in bitcoin to prevent sensitive conversations with therapists from being released to the public. By directly reaching out to customers or clients, quadruple extortion puts additional pressure on the company to pay the ransom.

The fast rise of double, triple, and quadruple extortion leads to new techniques to put additional pressure on victim companies. Now, ransomware does not just impact the company itself but can have big implications for the privacy and security of customers as well. This partially explains why paid ransom amounts have drastically increased.

1.5 More Absolute Thread of Control through Software Updates

In addition to analyzing cyber attacks in regards to the goal of the attack, *A Framework for Cybersecurity* also analyzes in regards to a second critical dimension—how the attack gains a thread of control. In short, a thread of control determines how a computer runs the sequence of instructions associated with a particular task.[30] A thread of control has an identity associated with it that determines its privileges. For instance, an administrator's thread of control would have much greater permissions on the system than another user's thread of control. Accordingly, the identity of the thread of control determines the level of permissions, such as the ability to read or write files on the local machine. The framework categorized three threads of control: (1) existing threads of control repurposed from their intended use; (2) threads of control obtained by standard means; and (3) threads of control created by extraordinary means/vulnerability. An **existing thread of control** repurposed from its

28 Nuni Snowden, "Triple Extortion Ransomware: A New Challenge for Defenders," Morphisec (Sept. 16, 2021), https://blog.morphisec.com/triple-extortion-ransomware-a-new-challenge-for-defenders.

29 "'Shocking' hack of psychotherapy records in Finland affects thousands," *The Guardian* (Oct. 26, 2020), https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland.

30 Waldo et al., *supra* note 22, at 5.

intended use occurs when an attacker uses a thread of control that they are authorized to use but abuses it to advance some malicious purpose.[31] A **thread of control obtained by standard means** occurs when an attacker gets someone else's login credentials, such as through phishing or social engineering. A **thread of control created by extraordinary means** occurs when an attacker exploits a vulnerability within the target system itself, such as using zero-day exploits.

Recently, attackers have begun exploiting existing threads of control embedded in software updates. The SolarWinds Attack in 2020 exemplifies this emerging threat.[32] While not a ransomware attack, the SolarWinds incident demonstrates a new mechanism for gaining a thread of control that allows the attack to run on the target computer. Believed to be the "worst hacking case in the history of America,"[33] the SolarWinds Attack compromised more than 200 government agencies, think tanks, and non-governmental organizations around the world as well as critical infrastructure.[34]

The hack, engineered by the Russian hacker group Nobelium, established its thread of control by embedding malicious code in an update for Orion software, made by the Texas company SolarWinds. Routine software patches provided by the vendor need to be installed in order to update or repair software being used by end users and organizations. In order to compromise the software upgrade's integrity, the attacker placed malicious code in the update package. Then, when customers of the vendor installed the update, the malicious code inserted into that update ran as part of the update process. So along with installing the update, the customer installed the attacker's software.

31 *Id.* at 7.

32 Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR* (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

33 Ben Fox, "Hack against US is 'Grave' Threat, Cybersecurity Agency Says," *AP News* (Dec. 17, 2020), https://apnews.com/article/technology-malware-hacking-russia-software-b3f993fb7bc9390302f0df26ecb6c10e.

34 William Turton, "At Least 200 Victims Identified in Suspected Russian Hacking," *Bloomberg* (Dec. 19, 2020), https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking.

This mechanism is exceptionally powerful since the rights given to the thread of control for installing or updating software are generally absolute. This means that during the installation process, the thread of control can read or modify any data, can start up any programs, and can install new programs that are given the highest level of access to the machine's resources.

While this cyber attack strategy still falls into the category of using an existing thread of control, it is far more powerful than other attacks that use existing mechanisms due to the unrestricted permissions it unleashes. Denial of service attacks, another example of an existing thread of control, that use the existing network listener thread, are not able to modify data on the attacked machine or install or run other programs; all they can do is bog the target machine down with excess requests. Even logging in using phished credentials, an example of a thread of control obtained by standard means, only gives the attacker the level of rights of the person whose credentials were phished; the usual attack using such credentials is to then find a way to elevate the privileges of the thread. However, by using the thread of control granted during software installations (and thus obtained using an existing thread of control), the attacker begins with the highest possible level of privilege. No such elevation or extra work needed.

The SolarWinds hack may have received the most publicity, but it is not the first time this approach had been seen. In June 2017, the malware NotPetya, which triggered the most destructive cyberattack witnessed to date, deployed a similar method of attack through a software update.[35] Conducted by the Kremlin-sponsored group Sandworm, NotPetya resulted in a global cyberattack that primarily targeted Ukraine, resulting in economic losses upwards of $10 billion.[36] NotPetya masqueraded as a ransomware attack; however, there was no way to obtain a decryption key, suggesting its primary aim was to wipe data and wreak havoc rather

35 "NotPetya," Security Encyclopedia, https://www.hypr.com/notpetya.

36 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED* (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

than to restore victim's data once payment was made.[37] It successfully wreaked havoc, as NotPetya resulted in a myriad of real work impacts, including crippling shipping ports and even shutting down the computers at Ukraine's Chernobyl Nuclear Power Plant.[38]

Like SolarWinds, NotPetya began with a compromised software update. Linkos Group, a small, family-run Ukrainian software house, had pushed an update for the accounting software M.E.Doc, which is the equivalent of TurboTax and used by almost all Ukrainian businesses. The mechanism of a compromised software update provided unfettered permissions on users' computers.

1.6 Supply Chain Attacks and Open Source Software

SolarWinds and NotPetya both also demonstrate the increased risk of supply chain attacks in modern software. Supply chain attacks occur when attackers compromise a block of code at its source, such as a software update that then infects any business or customer that uses it. Since it does not make sense for software developers to reinvent the wheel for common code elements, modern software incorporates many pre-written blocks of code from many different sources. This code could be licensed or it could be widely-available open source software.

Examples of supply chain attacks have proliferated in the past two years. The infection of Apple developer projects using the Xcode tool in August 2020 serves as yet another example.[39] Xcode is the free integrated development environment (IDE) in the Mac operating system used for developing software and applications. The compromised code in Xcode would, in turn, insert the XCSSET malware into any app that was produced using a version of the compromised Xcode tool.[40] The malware exploits two different vulnerabilities. The first vulnerability allows the malware to

37 Zeljka Zorz, "NotPetya Attacker Can't Provide Decryption Keys, Researchers Warn," Help Net Security (Jun. 29, 2017), https://www.helpnetsecurity.com/2017/06/29/notpetya-decrypt-fail/.

38 Greenberg, *supra* note 36.

39 Charlie Osborne, "Mac malware spreads through Xcode projects, abuses WebKit, Data Vault vulnerabilities," *ZD Net* (Aug. 14, 2020), https://www.zdnet.com/article/mac-malware-spreads-through-xcode-projects-abuses-previously-unknown-vulnerabilities.

40 *Id.*

steal cookies in the Safari browser. The second vulnerability, much more akin to the absolute permissions in the SolarWinds hack, allows the malware to compile a rogue Safari app and install it on the victim's computer.[41] Also like SolarWinds, developers would unknowingly distribute the malicious code inserted into their programs to their users.

In addition, several of the developers shared their projects on GitHub as open source software for other developers to use.[42] Researchers note that this risks "supply chain-like attacks for users who rely on these repositories as dependencies in their own projects."[43]

The Kaseya ransomware attack in July 2021 followed a similar supply chain attack.[44] In the recent attack, the REvil hacking group leveraged a vulnerability in Kaseya's VSA software, which is a cloud-based IT management product that enables businesses to handle complaints and ticketing as well as monitor performance,[45] to access the systems of multiple IT service providers and their customers.[46] As an IT management software, Kaseya held a high degree of trust with customers. Sophos, another IT security company, noted, "Some of the functionality of a VSA Server is the deployment of software and automation of IT tasks. As such, it has a high level of trust on customer devices. By infiltrating the VSA Server, any attached client will perform whatever task the VSA Server requests without question. This is likely one of the reasons why Kaseya was targeted."[47]

Most recently, the Internet vulnerability known as Log4Shell was discovered.[48] Log4Shell is a vulnerability that allows users to exploit the software program Log4j. Log4j is a piece of open source software that is

41 Jeffrey Orbegoso, "Malware infects MacOS using Zero-day vulnerability – XCSSET," Antivirus.com (Jul. 30, 2021), https://www.antivirus.com/2021/07/30/macos-malware.

42 Osborne, *supra* note 39.

43 Mac Threat Response & Mobile Research Team, "XCSSET Mac Malware: Infects Xcode Projects, Uses 0 Days," *Trend Micro* (Aug. 13, 2020), https://www.trendmicro.com/en_us/research/20/h/xcsset-mac-malware--infects-xcode-projects--uses-0-days.html.

44 *Id.*

45 "VSA," Kaseya (last visited Mar. 30, 2022), https://www.kaseya.com/products/vsa/.

46 *CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack,* CISA (July 6, 2021), https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa.

47 "Kaseya VSA Supply-Chain Ransomware Attack," Sophos Community Security Blog (Jul. 6, 2021), https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers.

48 Santiago Torres-Arias, "What is Log4j? A Cybersecurity Expert Explains the Latest Internet Vulnerability, How Bad it is and What's at Stake," *The Conversation (*Dec. 22, 2021), https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896.

used across the Internet to record events and communicate diagnostic messages about those events to both users and system administrators.[49] Log4Shell allows third parties to insert their own code into Log4j messages that then performs functions on a targeted computer, including allowing third parties to take control of a targeted system and spread their malicious code to others who communicate with that system.[50] Given that so many systems and devices interact with Log4j, a massive number of systems were compromised by this attack leading CISA Security Director Jen Easterly to refer to it as the "most serious" vulnerability she had ever seen.[51]

The possibility of a supply chain mechanism of attack has been known since it was first described in Ken Thompson's 1984 Turing lecture "Reflections on Trusting Trust."[52] Thompson explained that the bugs become harder and harder to detect as the program level gets lower. A well-installed bug, therefore, becomes impossible to detect. After demonstrating how he could easily hide malicious code in a compiler, Thompson pronounced, "The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code." Similarly, the fact that it took nearly 40 years for this kind of attack to be seen in the wild is a reflection of its subtle nature.

But the 40-year lag can also be seen as a reflection of changes in the way software is written and distributed. When Thompson first described this attack, software was generally written in-house or distributed on media (such as floppy disks) from trusted parties. Now software is distributed by companies over the Internet, and the software is often written using open source components from parties that may or may not be trustworthy. Taken together, the risk of supply chain attacks, much like compromised Xcode programs uploaded to Github, has never been higher.

---

49 *Id.*

50 *Id.*

51 "CISA Director Says the LOG4J Security Flaw is the 'Most Serious' She's Seen in Her Career," *CNBC* (Dec. 16, 2021), https://www.cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html.

52 Ken Thompson, *Reflections on Trusting Trust,* 27 Comm. of the ACM 761 (1984), https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf.

2. Emerging Solutions

2.1 Software Bill of Materials and Bug Disclosures

In regards to Ken Thompson's warning, it is true that a programmer will never be able to completely trust code that she did not write herself. However, recent emerging solutions, such as software bill of materials and bug disclosures, seek to minimize the risk and increase transparency in the software market. As President Biden's "Improving the Nation's Cybersecurity" Executive Order declared, "the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is."[53]

The "Improving the Nation's Cybersecurity" Executive Order, issued in the wake of the SolarWinds supply chain attack, directed the Secretary of Commerce, acting through the National Institute of Standards and Technology (NIST), to develop new standards, tools, and best practices to enhance software supply chain security and specifically mentioned that the guidelines should include software bills of material (SBOM) requirements.[54] The Executive Order required agencies, as software purchasers, to comply with NIST's published guidance. In accordance with Executive Order 14028, NIST published its Software Supply Chain Security Guidance on February 4, 2022.[55] Providing a standardized format for reporting incidents, such as through an SBOM, can reduce duplication efforts across multiple sectors.

Software bills of material (SBOMs) recognize that modern, sophisticated code is composed of pre-written building blocks. These pre-written blocks of code often come from multiple sources, which results in a complex and dynamic software supply chain. In addition, these pre-written blocks of code may themselves include code written by someone else. Therefore, SBOM seeks to provide a list of code components used in particular

53 Executive Order on Improving the Nation's Cybersecurity (EO 14028), White House (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

54 *Id.* § 4(e)(vii).

55 Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, NIST (Feb. 4, 2022), https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf.

software, much like the list of ingredients on food packaging. Allan Friedman, former Director of Cybersecurity Initiatives at the Department of Commerce's National Telecommunications Administration (NTIA) and now a senior advisor at Cybersecurity and Infrastructure Security Agency (CISA), explains, "You go to the store and buy a Twinkie. It comes with a list of ingredients. And why don't we expect the same level of transparency in our software that we get from a nonbiodegradable snack?"[56]

In order to be useful, a SBOM must include: (1) the identity of the component, (2) the relationship between components, and (3) extensions. Furthermore, to implement a SBOM solution there must be a uniform structure for capturing and presenting the information about the software's components, an ability to automate the process through techniques like machine reading so that this solution can be scaled, and a set of common best practices and processes that organizations can follow to effectively use a SBOM.[57] Finally, the SBOM must be updated and maintained when there is a change to a software component. In effect, the SBOM must allow the construction of a database that can be queried to find if a particular component is part of a piece of software.

A SBOM database can pull from some existing data. For instance, the Software Package Data Exchange (SPDX) is an international, grassroots-driven SBOM standard hosted by The Linux Foundation that communicates the components, licenses, security references, and other software metadata.[58] Another international standard, Software Identification (SWID) Tags also contain information about an installed application, such as whether the software includes patches and if it is part of a bundle.[59]

---

56 Security & Compliance Weekly Webinar, Episode 74, at 8:30 (May 25, 2021), https://securityweekly.com/shows/sbom-part-1-allan-friedman-scw-74/.

57 U.S. Department of Commerce, *The Minimum Elements For a Software Bill of Materials* (SBOM) (July 12, 2021), https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

58 The Software Package Data Exchange (last visited Mar. 20, 2022), https://spdx.dev/.

59 *Software Identification (SWID) Tagging,* NIST, https://csrc.nist.gov/projects/Software-Identification-SWID.

Safety-critical industries, such as healthcare, automotive, and energy, are already leading the charge on requiring SBOM.60 As Hilary Carter, vice president of the Linux Foundation noted, "There's a sense of urgency to implement cybersecurity best practices in health and safety applications because people's lives depend on the functionality of digital solutions across medical devices, from diagnostics to treatment and beyond."[61] Accordingly, hospitals have increasingly been adding SBoM requirements into procurement contracts.

However, SBOM cannot be a standalone solution. SBOM is primarily concerned with identifying the base components of open source software; it is not about labeling various components as dangerous or informing users that their software has a vulnerability. At best, an SBOM can be used to determine if some software is dependent on a compromised component once that compromise is identified; an SBOM does nothing to help identify such compromises. Thus, additional work would be needed by actors who could analyze SBOMs and compare them against public or proprietary vulnerability libraries to let users know if their software is known to be compromised. Furthermore, some form of an alert system could be implemented to inform users when some portion of their software has been found to be vulnerable. To run with Alan Friendman's Twinkie analogy, the nutrition facts on a Twinkie don't tell you which ingredients in what concentrations are harmful to your health. Instead, a diet coach works with individuals to identify their particular needs or the FDA sends out an alert and recall when a specific product is found to be contaminated. Similarly, the SBOM is not about normative statements about the health of a piece of software. Rather it is the infrastructure on top of which systems can build to address those health or vulnerability concerns.

60 Security & Compliance Weekly Webinar, Episode 74 (May 25, 2021) at 21:04 https://securityweekly.com/shows/sbom-part-1-allan-friedman-scw-74/.

61 Jessica Davis, "Could Healthcare Sector Serve as a Model for Adoption of Software bill of Materials?", SC Media (Feb. 8, 2022), https://www.scmagazine.com/analysis/asset-management/could-healthcare-serve-as-a-model-for-adoption-of-software-bills-of-materials.

2.2 **Regulating Cryptocurrencies**

Reducing the possibility of a supply chain attack will limit the distribution mechanisms for ransomware. But there are other mechanisms that could be used to reduce the effectiveness of this kind of malware, such as addressing the payout. One potential way to reduce ransomware payouts is to regulate cryptocurrency, which would make it harder for ransomware actors to receive cross-border payment anonymously.

The availability of cryptocurrency has enabled, and is correlated with, increased ransomware attacks.[62] This is largely because cryptocurrency allows ransomware groups to be paid virtually anonymously, in a liquid currency that is unregulated and easily flows across borders. While everyone, including law enforcement authorities, can view the public ledger of digital payments to see what accounts, or wallets, the ransomware payment is going into, these wallets are merely tied to digital addresses and do not identify who owns them. Thus, cryptocurrency has allowed ransomware actors in one part of the world to demand and receive instantaneous payment from another part of the world without revealing their identity.

This analysis highlights two aspects of cryptocurrency that are valuable to ransomware actors. First, the fact that cryptocurrencies transact digitally makes them ideal for cross-border payments. Historically, the first ransomware actors demanded payment by mail. This system has obvious flaws, not the least of which is having to give a return address which can then be traced by authorities. Furthermore, there are limits to the amount of money one can ask to be sent physically through the mail. Relying on the postal system to shepherd $40 million[63] in cash internationally is not a good business model. Therefore, cryptocurrencies are important because they are digital payments that allow large sums of money to be moved securely over distance.

62 Christopher Krebs, "Christopher Krebs on Cryptocurrency," interview by Bill Maher, *Real Time with Bill Maher*, HBO (Mar. 26, 2021), https://www.youtube.com/watch?v=GnPQTUD5f8o.

63 Kartikay Mehrotra & William Turton, "CNA Financial Paid 40 Million in Ransom After March Cyberattack,» *Bloomberg,* (May 22, 2021), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

Yet, financial institutions offer a range of digital options for transferring money and they are not the same type of enabler for ransomware. This is because financial institutions are heavily regulated and must comply with anti-money laundering (AML) regimes that include requirements about knowing your customer.[64] Conversely, cryptocurrencies can be transferred on a decentralized ledger without oversight from a financial institution and outside of traditional AML frameworks. The only piece of identifying information a "customer" needs to give on the blockchain is a digital address for the virtual wallet that is sending or receiving the funds. So cryptocurrencies have, to this point, existed largely outside of AML regimes and allowed ransomware actors to transfer funds while keeping their identities essentially secret.

There are at least three potential paths regulators might take to combat the use of cryptocurrencies for ransomware purposes: (1) an outright ban, (2) applying AML-type regulations to cryptocurrency transactions, and (3) tracing and seizing ransomware payments before ransomware actors can use them.

The first option is an outright ban. China has recently adopted this approach. In 2021, the People's Republic of China acted to criminalize cryptocurrency exchanges and transactions.[65] The effects of this law are meant to reach even international companies that interact with Chinese residents over the internet.[66] Notably, the purpose of the Chinese law was not primarily aimed at stemming the onslaught of ransomware. However, it is an example of how this strategy could be employed. Yet, it is unlikely, and perhaps undesirable, for such an approach to be taken in the rest of the world. As former-CISA director Christopher Krebs has said, "[l]ike many

64 Pia Singh, "CrowdStrike Co-Founder Says Rise in Ransomware Attacks Can be Addressed Without Banning Crypto," CNBC (Jun. 29, 2021), https://www.cnbc.com/2021/06/29/crowdstrike-co-founder-ransomware-attacks-can-be-addressed-without-crypto-ban.html.

65 China Securities Regulatory Commission Foreign Exchange Bureau et al., Notice on Further Preventing and Dealing with the Risk of Speculation in Virtual Currency Transactions (Sep. 24, 2021), http://m.safe.gov.cn/safe/2021/0924/19911.html.

66 *Id.*

other transformational technology developments, cryptocurrency has likely crossed a threshold where it is here to stay."[67] Thus, regulators should be looking for less blunt ways to reduce cryptocurrency's advantages for ransomware actors short of an outright ban.

Second, regulators could seek to apply AML-type regulations to cryptocurrency transactions. At first glance this might seem impossible. After all, the point of a distributed ledger system is that there is no overarching institution which could implement regulations. Yet, AML-type regulations could be implemented on virtual currency exchanges (VCE). VCEs are the entities that facilitate transfer between cryptocurrency and fiat currency. If VCEs were forced to know their customers and provide some level of oversight to ensure they were not abetting cyber criminals it could prevent ransomware actors from converting their cryptocurrency into more easily spent fiat currency.[68] This is an approach that has been supported by many experts including the co-founder of CrowdStrike who recently said, "I do think that regulations on cryptocurrency—know your customer, anti-money laundering regulations to make sure that large transfers are tracked and these criminals can't receive them anonymously—are going to be very, very important in stemming this problem."[69]

However, given that cryptocurrency may be easily transferred across borders to be exchanged for fiat currency almost anywhere in the world, this regime would have to be global in order to truly be effective. There is some hope on this front. In 2020, the Financial Action Task Force (FATF) published a report that discussed applying AML to virtual currencies.[70] FATF is the "inter-governmental body [that] sets international standards that aim to prevent" global money laundering.[71] FATF is made up of 39 member states and its regulations are implemented in 200 countries and

67 *Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis: Hearing before the House Comm. on Homeland Security,* 117th Congress 2 (May 5, 2021) (statement of Christopher Krebs, Director, CISA), https://homeland.house.gov/imo/media/doc/2021-05-05-CIPI-HRG-Testimony-Krebs.pdf.

68 See Daniel Holman & Barbara Stettner, *Anti-Money Laundering Regulation of Cryptocurrency,* Allen and Overy (2019), https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-international-comparative-legal-guide-to-anti-money-laundering.

69 Singh, *supra* note 64.

70 *FATF Report to the G20 Finance Ministers and Central bank Governors on So-called Stablecoins,* FATF (2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

71 "Who We Are," FATF (last visited Mar. 30, 2022), https://www.fatf-gafi.org/about/whoweare/.

jurisdictions. While FATF's report was particular to "stablecoins," a specific type of virtual currency, it professes to be "continuously strengthen[ing] its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity."[72] Thus, there is some hope for the global effort.

Lastly, law enforcement could focus their efforts on tracing ransomware payments and taking action to seize them before ransomware actors can use them. As the recent Colonial Pipeline case shows, it is possible to trace and seize cryptocurrency payments. Since cryptocurrencies rely on a public ledger, authorities can watch as the payments move from virtual wallet to virtual wallet. While they cannot discern the identity of the wallet holder from the wallet's digital address alone, they may be able to pair that information with other information to identify the holder. Furthermore, they may be able to use techniques and legal processes to seize the assets in a virtual wallet if they can show it came from a ransom payment. This is the strategy used by U.S. officials following the Colonial Pipeline hack. They were able to follow the ransomware payment from Colonial Pipeline, across several transfers between virtual wallets, and then seize the funds because "[t]he private key for the [online wallet] [wa]s in the possession of the FBI."[73] The FBI has not revealed how it obtained the wallet's private key. Whether the approach taken in the Colonial Pipeline incident is a scalable way to address ransomware payments will depend on whether getting a virtual wallet's private key is something officials can do with frequency or whether it depended in this instance on a unique aspect of the targeted transaction.

72 *Id.*

73 Affidavit in Support of an Application for a Seizure Warrant at ¶ 34 , Case No. 3:21-mj-70945-LB (N.D. Cal. Jun. 7, 2021), https://int.nyt.com/data/documenttools/affidavit-in-support-of-seizure-warrant/fd1288c50cc29e1b/full.pdf.

3. Conclusion and Takeaways

In recent years, ransomware has grown to be more prevalent and sophisticated, undertaken by organized crime groups in a systematic and targeted manner. This trend is concerning by itself. However, it is coinciding with an overall trend in cyberattacks toward supply chain attacks that allow criminals unprecedented levels of access across a vast number of systems through a single exploit. This frightening combination could lead to even more devastating ransomware attacks in the years to come if action is not taken. This article has put forward two potential, non-exclusive routes the United States could take to address such risks. First, the United States could continue to push software developers and purchasers to implement SBOM programs in tandem with vulnerability databases. This would enable subsequent efforts to identify vulnerabilities in open source software and notify users of those vulnerabilities. Second, the United States could focus on cryptocurrency to remove the financial incentive for performing ransomware attacks. This focus could take several forms including an outright ban, tighter regulations on crypto exchanges, or increased resources for tracing and seizing illicit crypto assets. By pursuing some combination of these strategies, the United States can mitigate the growing risks and scale of 21st century ransomware attacks.

Science, Technology, and Public Policy Program
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
www.belfercenter.org/stpp

Printed in the United States of America