DFRLab

CYBER STATECRAFT
INITIATIVE

ISSUE BRIEF

Behind the Rise of Ransomware

AUGUST 2022 **JOHN SAKELLARIADIS**

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

This issue brief investigates the drivers of the ransomware surge that menaced the United States in the summer of 2021, explains why these attacks remain a persistent threat today, and offers recommendations for mitigating the problem in the future. The 2021 surge in ransomware activity stems from a change in how criminals launch ransomware attacks. Between 2016 and 2019, cybercriminals shifted away from automated ransomware campaigns that emphasized scale to targeted extortion operations against organizations and established businesses. This adaptation made ransomware more disruptive and more profitable, eventually attracting the attention of well-organized cybercrime gangs. The intensification of the ransomware epidemic from that point until the attack on Colonial Pipeline resulted from the growing adoption of this new extortion model among criminals.

Though the US government has devoted more attention to ransomware over the ensuing months, ransomware remains a significant and long-term threat to the US economy. Three factors drive the persistence of the problem: the presence of a vast pool of security-poor organizations, the availability of a poorly regulated monetization pipeline in the form of cryptocurrency, and criminals' ability to evade law enforcement by exploiting jurisdictional boundaries. Mitigating just one of these conditions, let alone all three, will demand years of sustained effort.

Because the US government cannot eliminate ransomware overnight, it must begin planning how to manage the problem over the long term. To do so, it should start by investing in new efforts to improve the defenses of small- to medium-sized entities. The ease of compromising these organizations has been key to fueling the appetite for ransomware attacks. Yet, many of these organizations lack the personnel, incentives, and contracting power to secure their own networks.

Moreover, the US government should require all US-based organizations to report ransomware payments to the government and publish quarterly reports with anonymized versions of the data. Comprehensive payment transparency offers the best way to measure success against ransomware over the long term. It will ensure that success against targeted ransomware is judged in terms of the overall volume of ransomware payments, not just the absence of attacks on high-risk or high-profile entities.

INTRODUCTION

Since 1989, when an enigmatic evolutionary biologist named Joseph Popp shipped data-encrypting malware, via floppy disk, to the attendees of a scientific conference on AIDS, criminals have sought to leverage the techniques of computer exploitation and attack for the purposes of extortion.[1] But the problem—known today as ransomware—has grown exponentially in recent years, whether measured in the volume of attacks, the money flowing to criminals, or the harms inflicted on society. How did ransomware become so dangerous, so fast? Now that it is on the radar of world leaders, why is it proving so difficult to stop?

This paper makes three central arguments. First, the recent surge in ransomware activity stems from a shift in how criminals launch ransomware attacks, which transformed the digital extortion industry profoundly. From the rise of CryptoLocker in 2013 to the fall of GandCrab in 2018, cybercriminals primarily deployed ransomware in large, "spray-and-pray"-style campaigns targeting individual end users. These attacks demanded small ransoms from a vast pool of victims. Altogether, they pulled in modest revenues and inflicted limited damage.

Between 2016 and 2019, criminals made a small change that paid vast dividends: they began to burrow within networks and launch targeted extortion campaigns against the organizations that controlled them.[2] By creating a greater

incentive for criminals to apply pressure to any given victim, this adaptation made ransomware more disruptive. By generating higher profits, it drew top-tier cybercrime gangs into the digital extortion business. The intensification of the ransomware problem from that point until the summer of 2021 reflects the growing attention and investment that this new extortion model generated among criminals.

Second, despite renewed attention to the problem since the attack on Colonial Pipeline, ransomware remains a long-term threat to the US economy. Targeted ransomware may be new, but the conditions driving the problem are not—indeed, they have stymied the security community for the better part of the last decade. To wit, a sense of impunity among cybercriminals, widespread security deficiencies within the public and private sectors, and the emergence of a poorly regulated payment pipeline in the form of cryptocurrency present vexing hurdles for policymakers. Mitigating just one of these conditions, let alone all three, will demand years of sustained effort.

Finally, because ransomware cannot be eliminated overnight, the federal government should begin planning how to manage the problem over the long term. It can start by adopting three measures. First, Congress should establish a tax relief program for small- to medium-sized organizations that implement a series of security best practices. Second, drawing on the Work Opportunity Tax Credit (WOTC),[3] Congress should draft legislation offering federal tax credits to small- to medium-sized organizations that hire or retain employees with cybersecurity skills. The latter two measures will provide the most common victims of ransomware attacks—small- to medium-sized organizations—with the incentives and means to improve their own security.

Finally, it is imperative that policymakers measure success against targeted ransomware in terms of the overall volume of ransomware payments, not just the absence of attacks on high-risk entities. Therefore, Congress should require all US-based organizations to report ransom payments to the Department of Homeland Security (DHS). To encourage

---

1   Popp's history is curious, to say the least. For more, see Alina Simon, "The Strange History of Ransomware: Floppy Disks, AIDS Research, and a Panama P.O. Box," (Blog) *Medium*, March 26, 2015, https://medium.com/@alinasimone/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b.

2   There are two other terms that, for the purposes of this paper, might be used interchangeably with "targeted ransomware": "human-operated ransomware" and "big game hunting." The author uses "targeted" ransomware because it best captures those characteristics that distinguish modern ransomware from its predecessor. "Human operated ransomware" can generate confusion about the degree of automation resident in certain elements of the current and past ransomware life cycle. It also directs focus away from the most salient aspect of the shift, the movement away from the spray-and-pray approach to malware deployment. "Big game hunting" conveys the latter point, but it describes only a small portion of ransomware actors. It also obscures the degree of opportunism that suffuses the targeted ransomware economy.

3   See "Work Opportunity Tax Credit," Internal Revenue Service (website), accessed July 5, 2022, https://www.irs.gov/businesses/small-businesses-self-employed/work-opportunity-tax-credit. This tax credit was extended until December 31, 2025, via the Consolidated Appropriation Act of 2021.

compliance, DHS should anonymize the data it shares with the Department of Justice (DOJ), and Congress should offer limited liability protections to victims reporting attacks. To ensure transparency, DHS should be required to publish quarterly reports with the anonymized data.

While the recent Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) represents a positive step forward, the law only covers entities within critical infrastructure sectors. It therefore fails to rectify the fundamental limitation of existing ransomware data sets, which can delineate broad trends but provide insufficient granularity for effective policy.

It should not take another shock like the Colonial Pipeline attack for the US government to realize that ransomware has spiraled out of control. It is time to start investing in a more secure future.

PART 1: THE RISE OF RANSOMWARE

The story of the ransomware surge is the story of the discovery, professionalization, and growth of the targeted-attack extortion model. Prior to 2016, most ransomware campaigns targeted a large and effectively random pool of end users.[4] This "spray-and-pray" business model privileged quantity over quality, meaning ransomware actors spent less time focusing on how to apply pressure on a given victim and more time trying to reach as many victims as possible.[5] Until the tail end of this period, ransomware did not generate enormous profits. Being a second-tier avenue of cybercrime, it failed to attract as much talent or activity as it would in the years to come.

Ransomware experienced its first period of significant growth between 2013 and 2016, when refinements to ransomware payloads, the emergence of virtual currencies, and enhanced anti-fraud measures from banks and cybersecurity vendors increased the profitability of digital extortion relative to other common avenues of cybercrime.[6] What happened next remains unclear, but with more activity concentrating on ransomware, criminals appear to have learned how easy it was to extort organizations before piecing together how lucrative these attacks could be. Regardless, between 2016 and 2019, established cybercriminals gangs entered the targeted ransomware business en masse.[7]

From that point until the summer of 2021, cybercriminals invested growing time and resources to improve the targeted extortion model. During this period, digital extortion became more profitable because cybercriminal gangs and cybercrime markets reoriented around a near limitless demand for targeted ransomware. Moreover, as criminals learned how to best extract revenue from victims, they launched increasingly disruptive ransomware attacks.

Ransomware Before 2016

Prior to 2016, ransomware attacks infrequently involved elaborate pressure tactics and protracted negotiation processes. While criminals employed primitive methods of price discrimination among victims by using their Internet protocol (IP) address for geolocation, ransomware demands represented a take it-or-leave it proposition.[8] Depending on the malware and the victim, most ransoms ranged between $75 and $750.[9]

So long as ransomware demands remained so low, scale represented the principal means that ransomware groups

4   A. Kharraz et al., "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, eds. M. Almgren et al., DIMVA 2015, Lecture Notes in Computer Science 9148, Springer, Cham, https://doi.org/10.1007/978-3-319-20550-2_1.

5   Luca Invernizzi, Kylie McRoberts, and Elie Bursztein, "Tracking Desktop Ransomware Payments End-to-End," Presentation, BlackHat USA, July 26, 2017.

6   Herb Weisbaum, "Ransomware: Now a Billion Dollar a Year Crime and Growing," NBC News, January 9, 2017, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646.

7   This assessment is based on data from multiple sources, including author interviews. Brett Callow (threat analyst, Emsisoft), in discussion with the author, November 24, 2021; John Fokker (head of Cyber Investigations, Trellix Labs), in discussion with the author, January 18, 2022; Robert McArdle (director, Trend Micro's Forward Looking Threat Research Team), in discussion with the author, January 27, 2022); Allan Liska (intelligence analyst, Recorded Future), in discussion with the author, January 15, 2022; pancak3 (online security researcher), in discussion with the author, March 8, 2022; Azim Khodjibaev (senior intelligence analyst, Cisco Talos), in discussion with the author, January 17, 2022; and Mark Arena (CEO, Intel 471), in discussion with the author, February 18, 2022. Several written sources capture the development, e.g., Kris Oosthoek, Jack Cable, and Georgios Smaragdakis, "Ransomware: A Tale of Two Markets," arXiv: 2205.05028 [cs.CR], May 2022, https://doi.org/10.48550/arXiv.2205.05028; Institute for Security and Technology, "A Comprehensive Framework for Action: Recommendations from the Ransomware Task Force," Report, April 2021, https://securityandtechnology.org/ransomwaretaskforce/report/; and Symantec, "Internet Security Threat Report," February 2019, https://docs.broadcom.com/doc/internet-security-threat-report-volume-24-en.

8   Symantec, "The Evolution of Ransomware," August 2015, 22.

9   Kharraz et al., "Cutting the Gordian Knot"; and Bitdefender, "Ransomware: A Victim's Perspective," Report on US and European Internet Users, 2016, https://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf.

could maximize revenue. Consider one of the most successful early ransomware campaigns in history, CryptoLocker. Over a two-month period in the winter of 2013, CryptoLocker generated a remarkable $27 million.[10] The malware included several innovations that would become the hallmarks of modern ransomware, such as a robust encryption algorithm and the use of Bitcoin as a payment mechanism. Nonetheless, only 30 percent of CryptoLocker victims paid the ransom, which ranged between $300 and $750.[11]

CryptoLocker earned so much, so fast because it had unparalleled access to a vast pool of victims: at that time, the developers also controlled one of the world's largest botnets.[12] Through that botnet, they were able to deliver the malware at a scale and speed few criminals could rival.[13] In short, in the early days of ransomware, a fancy payload or sleek payment mechanism mattered less than how to obtain access to a large pool of victims.

Thus incentivized, ransomware groups before 2016 placed less emphasis on developing innovative extortion strategies or building more destructive payloads. According to one study of more than one-thousand ransomware samples collected between 2006 and 2014, most ransomware families at that time lacked "sophisticated destructive capabilities," while many "encrypt[ed] or delete[d] the victim's files using only superficial techniques."[14] A second group of researchers found that as late as 2018, several ransomware variants exhibited basic cryptographic flaws that permitted data recovery.[15] Early ransomware groups could get away with this because many users lacked the energy, money, or know-how to remediate a ransomware attack.

Just as it was less disruptive, early ransomware was less profitable. A 2018 study undertaken by researchers at Google estimated that the two most prolific pray-and-spray-style ransomware families at that time, Locky and Cerber, made $7.8 million and $6.9 million, respectively.[16] By contrast, eight of the top ten ransomware groups in 2020 made more than $10 million.[17] One of them, REvil, is thought to have made $100 million.[18]

Early ransomware gangs neither made nearly as much money, nor caused nearly as much harm as their successors. Many lacked the prestige and resources to recruit top-tier cybercrime talent. The most sophisticated cybercrime gangs of this era spent most of their time with bank fraud, where they could make larger paydays.

The Pivot to Targeted Attacks: 2016-2019

The shift to targeted ransomware attacks followed a period of significant growth in pray-and-spray-style ransomware attacks, with some companies estimating that ransomware had become a $1 billion industry by 2016.[19] Likely, growth in one form of digital extortion precipitated the shift to the next: as more criminals flowed into the ransomware business, they became bolder, savvier—and, perhaps, luckier.

Throughout the 2010s, improved anti-fraud defenses at major financial institutions and an exponential increase in the volume of stolen data on the cybercriminal underground squeezed margins in traditional, fraud-based avenues of crime.[20] Between 2011 and 2016, for example, the price of a stolen credit card on the black market dropped from $25 to $6.[21]

10   Josephine Wolff, "The $100 Million Bot Heist," *Nautilus*, November 28, 2018, https://nautil.us/the-100-million-bot-heist-7816/.

11   James A. Sherer et al., "Ransomware: Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web," Annual Survey, University of Richmond Journal of Law & Technology 23 (2017), http://jolt.richmond.edu/2017/04/30/volume23_annualsurvey_sherer/.

12   Sherer et al., "Ransomware."

13   Sherer et al., "Ransomware."

14   Kharraz et al., "Cutting the Gordian Knot."

15   Pranshu Bajpai, Aditya Sood, and Richard Enbody, "A Key-Management-Based Taxonomy for Ransomware," 2018 Anti-Phishing Working Group (APWG) Symposium on Electronic Crime Research (eCrime), 1-12.

16   Luca Invernizzi, Kylie McRoberts, and Elie Bursztein, "Tracking Desktop Ransomware Payments," Presentation, Security and Privacy Conference, 2018, https://elie.net/publication/tracking-ransomware-end-to-end/. The researchers involved in this study characterized their data as lower-bound estimates of the ransomware market because they excluded several transactions without a clear link to ransomware. While there is reason to believe the undercounting is significant—the Federal Bureau of Investigation reported that $209 million in ransom payments were made in the first three months of 2016 —the same could be said of subsequent efforts to track ransom payments.

17   "The Chainalysis 2021 Crypto Crime Report," Chainalysis.

18   "The Chainalysis 2021 Crypto Crime Report."

19   Weisbaum, "Ransomware: Now a Billion Dollar a Year Crime."

20   Brian Krebs, "Rogue Pharma, Fake AV Vendors Feel Credit Card Crunch," *Krebs on Security*, October 18, 2012.

21   Verizon, "2016 Data Breach Investigations Report," verizonenterprise.com/verizon-insights- lab/dbir/2016.

Meanwhile, the combination of file encryption, payment through virtual currency, and at-scale malware delivery offered a profitable business model that criminal groups increasingly emulated in the aftermath of CryptoLocker. The number of new ransomware strains discovered increased each year between 2011 and 2015, when the figure first broke one hundred.[22] During this time, criminals developed more effective ways to deliver their payloads, encrypt data, receive payments, and pressure victims.[23]

In the mid 2010s, changes introduced by major antivirus providers mitigated the effectiveness of end-user ransomware campaigns. According to Robert McArdle, a cybercrime expert at security company Trend Micro, ransomware gangs reacted by escalating privileges within a network, which allowed them to shut off organizations' improved defenses at the edge. Once criminals learned how easy it was to establish administrator-level access to an organization, McArdle speculates, it was only a matter of time before they began to deploy ransomware from the core of a network, encrypting thousands of machines at one time.[24]

The first ransomware group to focus exclusively on targeted attacks, SamSam, appeared in the winter of 2015.[25] Perhaps because the operators behind SamSam came from outside the Eastern European cybercrime scene, it took some time for its approach to catch on elsewhere. But in the unregulated world of cybercrime, when word about a lucrative form of cybercrime gets out, copycats are quick to pile on.

Starting in 2017, targeted ransomware began to displace end-user ransomware as the attack of choice in the digital extortion industry. Ransomware attacks on enterprises surpassed those on consumers for the first time in 2017.[26] By 2018, businesses accounted for 81 percent of all ransomware attacks.[27]

Between the summer of 2017 and April 2019, elite cybercrime gangs also jumped into the targeted ransomware game. In July 2017, the operators of the Dridex botnet launched BitPaymer; in August 2018, the operators of the TrickBot banking malware created Ryuk; and in April 2019, the former operators of the GandCrab ransomware spun off to create REvil.[28] All three groups specialized in targeted extortion.

2019-Present:
The Professionalization of Ransomware
As top-tier cybercrime groups entered the ransomware business and ransomware revenues climbed upward, criminals invested in new capabilities and cybercrime markets adjusted to meet a growing demand for resources to use in targeted ransomware attacks. Far more than their predecessors, contemporary ransomware actors therefore can purchase products and services or hire partners to make their attacks easier and more effective.

Perhaps the greatest indicator of how much ransomware has changed cybercrime markets—and how those markets have in turn facilitated the growth of ransomware—is the growth of illicit access brokers and the markets where they trade. Through illicit access markets, criminals that obtain a foothold into an organization can turn around and sell that access to ransomware groups or other cybercriminals.

Though such markets have existed in some form for years, they have experienced "meteoric growth" as a result of the ransomware surge.[29] Once servicing a wider range of criminal activity, access brokers now cater overwhelmingly to targeted ransomware attacks.[30] For example, listings on initial access markets now advertise the revenue of the organization a criminal has access to and the level of access that is available— indicators of how much a company might pay in the event of

22 Symantec, "An ISTR Special Report: Ransomware and Businesses 2016," August 10, 2016, https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5c_ISTR2016_Ransomware_and_Businesses.pdf.

23 Bajpai et al., "A Key-Management-Based Taxonomy."

24 McArdle, in discussion with the author. Separately, another factor that cut into the profitability of mass ransomware was the increased adoption of cloud-based services on consumer devices; see Symantec, "An ISTR Special Report."

25 United States v. Savandi and Mansouri, D.N.J. (2018), https://www.justice.gov/opa/press-release/file/1114741/download.

26 Symantec, "Targeted Ransomware: Proliferating Menace Threatens Organizations," July 18, 2019, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-threat.

27 Symantec, "Internet Security Threat Report."

28 CrowdStrike, "2020 Global Threat Report," 2020, 53, https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/; and John Fokker, "McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service—The All-Stars," McAfee (blog), October 2, 2019), https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/.

29 Allan Liska, *Understand, Prevent, Recover* (South Carolina: ActualTech Media, November 15, 2021).

30 "Steal, Then Strike: Access Merchants Are First Clues to Future Ransomware Attacks," *Intel471* (blog), December 1, 2020, https://intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service.

a ransomware incident and how much work criminals would need to do to launch one.[31]

By outsourcing this first stage of a ransomware attack, ransomware groups can focus on movement within an organization. That specialization is one reason for the increasing pace of targeted ransomware attacks. According to estimates by cybersecurity company Recorded Future, ransomware groups executed sixty-five thousand targeted ransomware attacks in 2020.[32] In the words of ransomware expert Allan Liska, that figure simply would not be possible without underground forums.[33]

Increasing specialization across different stages of the ransomware life cycle also is evident in the growth of the ransomware-as-a-service model (RaaS). In a RaaS structure, a core group of criminals manage a ransomware payload, while outsourcing ransomware deployment to so-called "affiliates." The model has the dual benefit of allowing ransomware groups to scale their operation and to off-load risk, with affiliates now drawing increasing attention from law enforcement. According to an interview given by a member of the REvil ransomware gang, the group at one point had sixty affiliates carrying out attacks on its behalf.[34] As of October 2021, eight of the ten leading ransomware groups employed an affiliate model to carry out attacks.[35]

In addition to external partnerships, ransomware groups have tapped increasingly large war chests to strengthen their organizations from within. Some of the wealthiest ransomware groups rent access to botnets, which provision a steady stream of targets for the groups and obviate the need to participate in public access markets.[36] Buoyed by past profits, ransomware groups also have thrown more money at recruiting top talent.[37] At one point, the REvil group advertised that it was investing $1 million as part of a new recruitment drive.[38]

The recent leak of internal communications from the Conti ransomware group demonstrates how years of steady revenue have turned ransomware groups into something that resembles a legitimate business. According to the leaks, at various points over the last two years, the group employed between sixty-five and one hundred salaried employees, whom it paid twice monthly through virtual currency.[39] The group had vacation policies for its employees, a human resources department, and a 24/7 support staff.[40] With an eye toward the future, the group also reinvested profits to improve its core business, studying weaknesses in popular cybersecurity products, researching new vulnerabilities and exploits, and identifying valuable partners.[41]

Whether measured in the volume of attacks or their effectiveness, the gradual professionalization of the market

31   "Steal, Then Strike," *Intel471*.

32   Liska, *Understand, Prevent, Recover*.

33   Liska, *Understand, Prevent, Recover*.

34   Dmitry Smilyanets, "'I Scrounged through the Trash Heaps . . . Now I'm a Millionaire': An Interview with REvil's Unknown," *The Record*, March 16, 2021, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/.

35   Fyodor Yarochkin, "Ransomware as a Service: Enabler of Widespread Attacks," Trend Micro (blog), October 5, 2021, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks. There are some signs the affiliate model may be in decline. Numerous instances in which affiliate groups and ransomware operators have tried to steal from one another have created distrust. Moreover, as increased government attention has been directed toward ransomware, groups have become increasingly wary of delegating so much independence to trigger-happy affiliate groups. There are some indications that top-tier ransomware groups are adopting a more centralized and hierarchical model, though the fluidity of these relationships make any prediction uncertain.

36   Yelisey Boguslavskiy and Vitali Kremez, "Corporate Loader 'Emotet': History of 'X' Project Return for Ransomware," *Advanced Intel* (blog), November 19, 2021, https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware.

37   Brian Krebs, "Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work," *Krebs on Security*, October 8, 2020, https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/.

38   Simon Chandler, "REvil Ransom Gang Offers $1 Million as Part of Recruitment Drive," *Forbes,* October 6, 2020, https://www.forbes.com/sites/simonchandler/2020/10/06/revil-ransomware-gang-offers-1-million-as-part-of-recruitment-drive/.

39   Brian Krebs, "Conti Ransomware Group Diaries, Part II: The Office," *Krebs on Security*, March 2, 2020, https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/.

40   Krebs, "Conti Ransomware Group Diaries, Part II."

41   Krebs, "Conti Ransomware Group Diaries, Part II."

for targeted ransomware attacks has transformed the digital extortion industry. The total value of cryptocurrency received by ransomware addresses grew from less than $25 million in 2016, when mass ransomware predominated, to roughly $692 million in 2020, when targeted ransomware had become the norm.[42] Likewise, between 2018 and 2020, the number of ransomware complaints submitted to the Federal Bureau of Investigation's Internet Crime Complaint Center increased 65.7 percent, while victim losses swelled 705 percent.[43]

Targeted Ransomware: A More Disruptive Form of Extortion

The pivot to extorting organizations strengthened a dangerous incentive that lay half-dormant within prior iterations of digital extortion: whereas older ransomware campaigns prioritized scale and automation, modern ransomware places a premium on coercion. These dynamics manifest in the increase in average ransom payments over time, as well as the uptick in incidents against vulnerable entities, like schools and hospitals.

As ransomware gangs spent more time extorting organizations, they developed more effective methods to extract revenue from victims. From the third quarter of 2018 to the third quarter of 2020, the average ransom payment grew from less than $6,000 to nearly $240,000, while the median payment grew from four figures to more than $100,000.[44] Three variables have driven the increase in average ransom payments over time: victim size, negotiating leverage, and negotiating savvy.

First, ransomware gangs started to attack larger victims. The median size of victim organizations, measured by the number of employees, jumped from twenty-five in 2018 to 250 by the end of 2020, according to Coveware.[45] Likewise, the security firm Sophos found that ransomware attacks against organizations with one thousand to five thousand employees were more likely in 2021 than those with less than one thousand employees.[46]

Second, attackers began to threaten to leak sensitive data stolen from victims, which is commonly referred to as "double extortion." Pioneered by the Maze group in November 2019, double-extortion threats provide additional bargaining leverage beyond data encryption. Leaks can lead to the loss of intellectual property and brand damage or, if victims otherwise intend to keep incidents quiet, trigger regulatory investigations.

The popularity of the data-extortion threat is undeniable. From the fourth quarter of 2019 to the fourth quarter of 2021, the percentage of ransomware attacks involving a threat to release data increased from less than 5 percent to roughly 70 percent, according to data collected by Coveware.[47] Likewise, CrowdStrike found an 82 percent increase in ransomware-related data leaks in 2021, as compared with 2020.[48]

Nonetheless, ransomware negotiators, cybercrime experts, and cyber insurance providers interviewed for this project insisted that business interruption losses—and not the threat of proprietary data loss or brand damage—represent the most consequential pain point for most victims. To explain the increase in ransom payments, they pointed to a third factor: criminals' use of open-source business intelligence tools, like ZoomInfo, and on-network reconnaissance of financial and insurance information, to determine how much victims could afford to pay.

Attacks on larger businesses, efforts to acquire additional leverage over victims, and better business intelligence represent three ways ransomware groups have adapted to the dynamics of targeted ransomware. A fourth involves victim selection: to maximize revenue, ransomware groups increasingly target entities with extensive and time-sensitive IT dependencies, like patient care, payroll, and just-in-time product delivery.

For example, during the peak of the COVID-19 crisis, ransomware groups deliberately targeted hospitals and healthcare providers in the United States, which had significant

42   "The Chainalysis 2021 Crypto Crime Report."

43   Federal Bureau of Investigation, *Internet Crime Report 2020*, FBI Internet Crime Complaint Center (IC3), March 17, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

44   Coveware, "Ransomware Attackers Down Shift to 'Mid-Game' Hunting in Q3 2021," Coveware (blog), October 21, 2020, https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts.

45   Coveware, "Ransomware Attackers Down Shift."

46   Sophos, "State of Ransomware 2021," August 19, 2021, 4, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

47   Coveware, "The Marriage of Data Exfiltration and Ransomware," Coveware (blog), January 10, 2020, https://www.coveware.com/blog/marriage-ransomware-data-breach.

48   CrowdStrike, "2022 Crowdstrike Global Threat Report," Report, February 15, 2022, https://www.crowdstrike.com/resources/reports/global-threat-report/.

consequences for patient care.[49] One attack, on United Healthcare, simultaneously affected 250 healthcare facilities in the United States.[50] A month later, US officials learned that a ransomware gang had acquired access to more than four hundred US-based healthcare providers and was threatening to attack a large number of them simultaneously.[51]

PART 2: WHY RANSOMWARE ISN'T GOING AWAY

While the Biden administration has taken major strides in the fight against ransomware since the attack on Colonial Pipeline, available data indicates that the volume of ransomware activity has declined slightly, if at all, during this period.[52] As recently as February 2022, cybersecurity authorities in the United States, the United Kingdom, and Australia warned that "if the ransomware criminal business model continues to yield financial returns . . . ransomware incidents will become more frequent."[53]

The persistence of the ransomware problem should not come as a surprise. Three factors underlie the persistence of targeted ransomware, and each presents significant hurdles for lawmakers: the presence of a vast pool of security-poor organizations; the availability of a poorly regulated payment vehicle in the form of cryptocurrency; and criminals' ability to exploit jurisdictional boundaries. Together, these factors ensure that ransomware will present a challenge for years to come.

Taking the Fight to Ransomware Actors

To reduce ransomware attacks, many governments have searched for ways to eliminate the legal sanctuaries where ransomware gangs operate. The proposals for doing so are manifold.[54] They include high-level diplomatic negotiations with offending countries, like Russia; offensive cyber operations against ransomware gangs; and more aggressive law enforcement action against affiliate groups and adjacent service providers.

Yet, the fluidity, decentralization, and dynamism of the digital extortion market complicate the process of identifying individual ransomware actors. The relationships that characterize each ransomware group fluctuate constantly, with individuals moving between ransomware gangs, gangs purchasing tools and services from other criminals, and various groups contributing to different elements of an attack. The resulting complexity means that "it is often difficult to identify conclusively the actors behind a ransomware incident," as cybersecurity authorities in the United States, Australia, and the United Kingdom recently observed.[55]

Just as the fluidity of the ransomware ecosystem complicates the process of identifying criminals, jurisdictional boundaries hinder enforcement. Historically, many leading cybercriminal groups have operated in Eastern Europe, where local law enforcement agencies lacked the capability or will to bring cybercriminals to justice. But ransomware has attracted

49 The Cyber Peace Institute, *Playing with Lives: Cyberattacks on Healthcare Are Attacks on People*, March 2021, https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

50 Office of Information Security, US Department of Health and Human Services, "Trickbot, Ryuk, and the HPH Sector," Bulletin, November 12, 2020, https://www.hhs.gov/sites/default/files/trickbot-ryuk-and-the-hph-sector.pdf.

51 Brian Krebs, "Conti's Ransomware Toll on the Healthcare Industry," *Krebs on Security*, April 18, 2021, https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/.

52 Allan Liska, "Are Ransomware Attacks Slowing Down? It Depends on How You Look at It," *Recorded Future* (blog), December 20, 2021, accessed April 2022. Error! Hyperlink reference not valid.

53 Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security, "2021 Trends Show Increased Globalized Threat of Ransomware," Alert, February 9, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

54 Several government and nonprofit groups have studied the ransomware problem extensively and offered thoughtful proposals for fixing it. See Institute for Security and Technology, *A Comprehensive Framework for Action: Recommendations from the Ransomware Task Force,* April 2021, https://securityandtechnology.org/ransomwaretaskforce/report/; "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns," US Senate Comm. on Homeland Security & Governmental Affairs, 117th Cong. (2022), https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf; and Mieke Eoyang, Allison Peters, Ishan Mehta, and Brandon Gaskey, "To Catch a Hacker: Towards a Comprehensive Strategy to Identify, Pursue and Punish Malicious Cyber Actors," Third Way, October 29, 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

55 Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security, "2021 Trends Show Increased Globalized Threat of Ransomware," Alert, February 9, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

criminals from across the world, and it will metastasize if extortion remains so profitable.

Russian noncompliance with transnational cybercrime investigations exacerbates the natural hurdles involved in transnational law enforcement. For more than a decade, major cybercriminal networks have operated with impunity out of Russia.[56] Mounting evidence suggests that many of these criminals purchase their immunity through cooperation with Russian intelligence and law enforcement agencies.[57]

The outbreak of the war in Ukraine reduces the likelihood that Russian authorities will respond constructively to US pressure to rein in domestic cybercrime elements. That presents a significant problem when it comes to ransomware: according to data collected by Chainalysis, 74 percent of money made by ransomware actors in 2021 went to groups that were "highly likely to be affiliated with Russia."[58]

Mitigating Cryptocurrency Cash-out Schemes

Since most ransomware payments are made in cryptocurrency, and no other payment vehicle can facilitate pseudonymous, high-value, and high-volume payments across borders, those seeking to address the ransomware threat have increasingly called for greater regulation of global cryptocurrency exchanges.[59] The hope is that better enforcement of existing Know-Your-Customer (KYC) and Anti-Money Laundering (AML) requirements would obstruct ransomware payments and empower cross-border law enforcement investigations.

As with law enforcement action, however, cryptocurrency regulation faces significant jurisdictional hurdles. Again, Russia plays a central role in noncompliance. For example, one investigation by Bloomberg traced four cryptocurrency exchanges involved in shady or illicit activity to a single office building in Moscow.[60] Subsequent research from Chainalysis found that between 29 percent and 48 percent of all funds received by cryptocurrency businesses in the district that includes that building come from illicit and risky cryptocurrency addresses.[61]

The regulatory challenge extends beyond Russia. In 2019, more than 50 percent of all funds traced from criminal entities to exchange-hosted wallets ended up in Binance and Huobi, major cryptocurrency exchanges based in China.[62] Tether, which claims to offer a dollar-backed stable coin and is key to modern money laundering tactics, is incorporated in Hong Kong.[63] Overall, the global nature of the money laundering networks that support cryptocurrency cash-out schemes inhibit the federal government from enforcing effective regulatory regimes cheaply or quickly.

56 Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," *Slate*, February 2, 2018, https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html.

57 Recorded Future, *Dark Covenant: Connections Between the Russian State and Criminal Actors*, Report, September 9, 2021, https://www.recordedfuture.com/russian-state-connections-criminal-actors/; and John Fokker and Jambul Tologonov, "Conti Leaks: Examining the Panama Papers of Ransomware," Trellix (blog), March 31, 2022, https://www.trellix.com/en-au/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html.

58 Chainalysis, "Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity," Chainalysis (blog), February 14, 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/.

59 Many people often point to business email compromise (BEC) scams and ask: why couldn't criminals use the traditional banking system to facilitate ransom payments? BEC scams rely on deception. Banks facilitate these payments because they *think* they are legitimate. By contrast, victims cooperate with criminals to make ransom payments. Because the better regulated banking system is unlikely to support these transactions, and victims could face liability if they lie to financial intermediaries, victims turn to cryptocurrencies.

60 Kartikay Mehrotra and Olga Kharif, "Ransomware HQ: Moscow's Tallest Tower Is a Cybercriminal Cash Machine," Bloomberg, November 3, 2021, https://www.bloomberg.com/news/articles/2021-11-03/bitcoin-money-laundering-happening-in-moscow-s-vostok-tower-experts-say.

61 Chainalysis, "Russian Cybercriminals Drive Significant Ransomware."

62 Chainalysis, "Crypto Money Laundering: How Criminals Cash Out Billions in Bitcoin and Other Cryptocurrencies," Chainalysis (blog), January 15, 2020, https://blog.chainalysis.com/reports/crypto-money-laundering-2019/.

63 Bruce Scheier and Nicholas Weaver, "How to Cut Down on Ransomware Attacks Without Banning Bitcoin," *Slate*, June 17, 2021, https://slate.com/technology/2021/06/banning-cryptocurrencies-bitcoin-ransomware-disruption-exchanges.html.

Since global cryptocurrency reform represents a long-term undertaking, it is also worth asking whether these efforts would undercut the ransomware market as much as some assume. While jurisdictional differences slow regulation, criminals adapt quickly. Between 2011 and 2019, large exchanges helped cash out 60 percent to 80 percent of Bitcoin transactions from known bad actors, according to data collected by blockchain analytics firm Elliptic.[64] Then, as exchanges bolstered their anti-money laundering policies, criminals turned elsewhere, to unlicensed exchanges, over-the-counter brokers, and decentralized finance (DeFi) protocols.[65]

If the goal is to interdict or to seize payments, cryptocurrency regulation also presents practical and ethical trade-offs. Interdicting a ransom payment risks harm to victims, since criminals who do not receive funds might withhold a decryption key. Moreover, if ransomware payments remain legal, interdiction or seizures will be difficult to implement at scale. Many victims will not share information with law enforcement if they fear that doing so will inhibit their ability to acquire a decryption key.

Reducing Widespread Security Deficiencies

Finally, governments have sought to reduce the impact of ransomware attacks by driving or incentivizing the reduction of widespread security deficiencies, in particular among government agencies and critical infrastructure identities. However, the most common victims of ransomware attacks, small- to medium-sized entities, face significant obstacles when it to comes to resources, contracting power, and incentives.

First, faced with razor-thin operating margins and business-critical operating dependencies, small- to medium-sized organizations cannot afford to build adequate security programs—something which demands steady investments in people, technology, and process. According to a January 2020 study of three thousand small businesses in the United States and the United Kingdom, 20 percent of companies use no endpoint security whatsoever, 33 percent of them use free consumer-grade software, and 43 percent of them have no cyber defense plan in place.[66] Likewise, one 2019 survey of businesses with between one hundred and one thousand employees found that just 45 percent of respondents described their security posture as "sufficient."[67]

Unlike their larger counterparts, small- to medium-sized organizations also lack the contracting power and resources to purchase software products with sufficient security protections, let alone security software. Many software providers upsell customers for baseline security features, like Single sign-on (SSO), while many security vendors are too expensive for small businesses. Too often, small- to medium-sized organizations must choose between security or affordability.

Many organizations also confront perverse incentives when it comes to delivering cybersecurity outcomes. Modern organizations rely on a complex network of software and IT suppliers.[68] Those suppliers are not held liable if their products are compromised to hack one of their customers. As a result, software providers have weak incentives to improve security for their users, while users are skeptical that cybersecurity investments can adequately reduce risk.

Overall, small- and medium-sized organizations face a nasty predicament when it comes to security. Because it is difficult and costly, security is often deferred in favor of critical operating needs. But it becomes more expensive to fix the longer you wait to address it. This negative feedback loop of cost-cutting and debt-accumulation has left many organizations incapable of defending themselves, while easing the way for predatory ransomware groups.

64 Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders*, 2020, https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf.

65 Elliptic, *Financial Crime Typologies in Cryptoassets*. This bolstering could also be interpreted as a win for law enforcement, in the sense that criminals were forced to resort to riskier exchanges with less liquidity on their balance sheets. However, profits made by ransomware groups continued to grow during this period, suggesting that criminals were not greatly affected by such reform. Decentralized finance refers to financial transactions that do not rely on intermediaries, like brokerages or exchanges, and instead use peer-to-peer technologies to establish trust between parties.

66 BullGuard, "New Study Reveals One in Three SMBs Use Free Consumer Cybersecurity and One in Five Use No Endpoint Security at All," February 19, 2020, https://www.bullguard.com/press/press-releases/2020/new-study-reveals-one-in-three-smbs-use-free-consu.aspx.

67 Ponemon Institute, *2019 Global State of Cybersecurity in Small- and Medium-sized Businesses*, 2019, https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf.

68 Trey Herr, William Loomis, Stewart Scott, and June Lee, *Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain*, Atlantic Council, July 26, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/#executive.

PART 3: ADDRESSING RANSOMWARE INTO THE FUTURE

To date, the US government has pursued a series of policies aimed at meeting the needs of today's ransomware threat, such as prosecuting ransomware actors, squeezing cryptocurrency cash-out schemes, and defending national critical infrastructure. But given the unlikelihood of eliminating digital extortion in the near future, the federal government also needs to start investing in better strategies for managing this problem over time.

It can start by considering the following three policies:

RECOMMENDATION 1: Congress should pass new legislation mandating that all US-based organizations report ransom payments to the government. The reports should be sent to the Cybersecurity and Infrastructure Security Agency (CISA) within seventy-two hours of payment, and be shared by CISA, in anonymized form, with the FBI. To encourage compliance, the legislation should include liability protection stipulating that the report cannot form the basis for regulatory or enforcement action against the victim.[69]

At a minimum, the reports should detail the size of the payment, the date of payment, and the sending and receiving addresses for the transaction. They should also include information on the victim, such as the size of the organization and the industry it is in. The reports should be anonymized, but CISA should be required to publish quarterly reports with the data.

At present, policymakers must rely on partial or anecdotal data streams about ransomware attacks.[70] The methodological limits of these data sets make it difficult to assess the ransomware threat empirically, instead inclining the public to assess the problem via newspaper headlines or press statements. According to one CISA estimate, just one-fourth of all ransomware attacks are reported to the government.[71]

A comprehensive ransomware reporting mandate would also represent a significant improvement on CIRCIA. Because the law only obliges entities in critical infrastructure sectors to report ransom payments to the government, it fails to resolve the core problem that handicaps lawmakers today: available data does not provide sufficient fidelity or granularity to inform effective policy.

Comprehensive payment visibility would provide multiple benefits. In the short term, it would illuminate how widespread payments are and who is most affected. Moreover, by funneling standardized information to CISA, it will avoid data silos and formatting inconsistencies—two flaws with today's reporting system highlighted by a recent Senate report.[72]

Over the long term, a reporting requirement will help law enforcement track the activity of ransomware groups, monitor money flows to, from, and within these organizations, and facilitate enforcement against criminals. It will also allow the government to monitor the ebb and flow of the digital extortion economy. Here, the quarterly reporting requirement is key. By forcing this data out into the open, it will ensure the problem is assessed at regular intervals and on a holistic basis.

Critics might counter that such a system is difficult to enforce. Some organizations may not know or understand their obligations. Others may resist, fearing the consequences of sharing sensitive information with the government.

In part, these objections rest on a misleading analogy to existing data breach notification regimes. Unlike data breach laws, which revolve around ambiguous definitions of access to personal data, ransom payments are clear and undeniable. No amount of creative lawyering can deny them. With minimal federal oversight, appropriate liability protections, and sufficient inducements for compliance—such as those outlined below—it stands to reason that most US-based organizations will be inclined to follow the law.

RECOMMENDATION 2: Congress should establish a tax relief program for small- to medium-sized organizations that implement a series of security best practices, including but not limited to the use of backups, the creation of an incident response plan, and the use of multifactor authentication (MFA) for remote access to administrative systems and services.

---

69 This recommendation was inspired by the Ransomware Task Force. See Institute for Security and Technology, *A Comprehensive Framework for Action: Recommendations from the Ransomware Task Force*, April 2021, 47, https://securityandtechnology.org/ransomwaretaskforce/report/.

70 State and federal data breach notification laws revolve around the protection of personally identifiable information. If ransomware actors never access such protected data—or if victims lack evidence of that access—victims do not have to report a breach, let alone the fact of payment.

71 Jonathan Greig, "CISA Exec: Lack of Ransomware Incident Reporting Is Crippling Defense Efforts," *The Record*, June 8, 2022, https://therecord.media/cisa-exec-lack-of-ransomware-incident-reporting-is-crippling-defense-efforts/.

72 "Use of Cryptocurrency in Ransomware Attacks," US Senate Comm. on Homeland Security & Governmental Affairs.

Mitigating the security deficiencies of smaller organizations represents an urgent public policy challenge. According to digital forensics and incident response (DFIR) firm Coveware, 55 percent of enterprise-targeted ransomware attacks hit companies with less than one hundred employees in 2021, and 75 percent of attacks victimized those with less than $50 million in revenue.[73] Since small businesses are less likely to have access to expensive DFIR firms or be represented in corporate surveys, it is likely the figure undercounts the problem, perhaps significantly.

One ransomware negotiator interviewed for this project, Kurtis Minder, began advertising free ransomware negotiation services for small organizations on his firm's website in 2020. In a matter of days, he said, he was flooded with new requests from small-business owners—a trend that continues to this day, according to Minder.[74]

A tax relief program would provide an incentive for these organizations to secure their networks before an attack, at which point many victims have limited resources to spare on security. The average organization faces twenty-six days of interruption following a ransomware attack, according to Coveware.[75] During this period and well after, costs add up fast, including downtime, data recovery, lost business, brand damage, and other emergency expenses. Globally, the average total cost of recovery from a ransomware attack stood at $1.4 million in 2021, according to a recent study by security firm Sophos.[76]

Because high recovery costs accrue whether or not one pays a ransom, an ounce of prevention is worth a pound of cure.[77] Fortunately, research indicates that simple changes can go a long way toward reducing a victim's likelihood of paying

a ransom. A recent study by the Cyentia Institute and Arete found that even partial implementation of MFA reduced a victim's likelihood of paying a ransom by 12.5 percent, while victims who could successfully recover data were 19.7 percent less likely to pay than those who couldn't.[78]

All told, the collective threat of ransomware to the US economy is enormous—and small organizations are desperate for help. According to a study by Cybersecurity Ventures, ransomware will cost global businesses $265 billion by 2031.[79]

RECOMMENDATION 3: Congress should draft legislation offering federal tax credits to small- to medium-sized organizations that hire or retain employees with cybersecurity expertise. The legislation could be modeled on the Work Opportunity Tax Credit, which provides federal tax credits to organizations that hire individuals who have consistently faced barriers to employment.

A WOTC for cyber should be drafted to encourage organizations not just to hire cybersecurity talent, which is in short supply, but also to develop it in-house. Through online education, part-time course work, and vocational training, cybersecurity skills development is increasingly available to the public. Moreover, given that most ransomware attacks exploit basic security deficiencies, like password reuse, the educational requirements would not have to be significant to have an impact.

First and foremost, a tax credit would help address a cybersecurity personnel shortage. A 2019 study sponsored by the National Institute of Standards and Technology (NIST) estimated that 450,000 cybersecurity positions remain unfilled in the United States.[80] The gap, already immense, is

---

73 Coveware, "Ransomware Attackers Down Shift."

74 Kurtis Minder (CEO and co-founder, GoodSense, a nonprofit organization) in discussion with the author, January 22, 2022.

75 "Ransomware Actors Pivot from Big Game to Big Shame Hunting," Coveware (blog), May 3, 2022, https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting.

76 Sophos, "State of Ransomware 2022," April, 2022, https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf.

77 The decryption keys proffered by ransomware groups are often imperfect and must be tested to ensure they do not cause further damage. Even then, the decryption process is slow and some data might prove unrecoverable. For example, it took the Irish Healthcare System four months to recover from a ransomware attack, even though Irish authorities received a decryption key six days after the ransomware was deployed. See PwC's report for the Health Services Executive, *Conti Cyber Attack on the HSE: Independent Post-Incident Review,* December 3, 2021, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.

78 See "Mitigating Ransomware's Impact," Report, Arete and the Cyentia Institute, June 2022, https://areteir.com/report/mitigating-ransomwares-impact-investigative-cybercrime-series-vol-1/.

79 Cybersecurity Ventures, "Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031," June 3, 2021, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

80 Data available via Cyber Seek's "CybersecuritySupply/Demand Heat Map," https://www.cyberseek.org/heatmap.html.

expected to grow over time. The Bureau of Labor Statistics projects that information security analyst jobs will increase 33 percent between 2020 and 2030.[81]

Second, the incentive would provide relief to smaller organizations, which are hard-pressed to find cybersecurity talent, let alone afford it.[82] These resource constraints are particularly acute in certain industries, such as healthcare. According to the 2017 Health Care Industry Cyber Task Force, most healthcare organizations face operating margins of less than 1 percent and many cannot afford to maintain in-house security personnel.[83] These constraints exacerbate the inherent complexities of hospital administration and represent a central reason that healthcare companies became such popular targets for ransomware attacks over the last two years.[84]

Though part-time security training is no substitute for a professional security vendor or a mature security program, it represents a step in the right direction. It could reinforce the other recommendations included in this report, providing a logical point of liaison with the federal government on ransomware reporting and reducing the cost of proactive security implementations.

CONCLUSION

The recent surge in ransomware attacks is often explained via an alphabet soup of metallic-sounding acronyms and epithets. Ostensibly, acronyms and terms like "RaaS" (ransomware-a-service), "IABs" (initial access brokers), and "double-extortion" (the data disclosure threat) identify the phenomena that have supercharged digital extortion.

In truth, ransomware poses an analytic challenge at once simpler and more complex: more complex insofar as several factors contribute to the ransomware problem in different degrees, like weighted variables in some inscrutable algorithm; and simpler insofar as the ransomware surge boils down to a single discovery. Organizations present vulnerable, lucrative, and near limitless targets for digital extortion—something cybercriminals had grasped firmly by 2019.

The shift to extorting organizations, instead of individuals, transformed the digital extortion industry profoundly. By increasing the importance of any single victim in the eyes of the attackers, it made ransomware more disruptive. By making digital extortion so profitable, it attracted a flurry of new activity and investment from cybercriminals.

Since the attack on Colonial Pipeline, the United States and its allies have made stopping ransomware a priority. Thus far, those initiatives have failed to reduce the threat as much as many had hoped.[85] But policymakers should not be discouraged.

The factors that made ransomware prolific may be new, but those that made it possible are familiar and deep-seated. To put ransomware in the rearview mirror, the United States will finally have to address the three conditions that have not just fueled digital extortion, but cybercrime, for much of the last decade: a large pool of security-poor victims, a poorly regulated payment vehicle in the form of cryptocurrency, and a sense of impunity among criminals.

Solving these problems will not just take time but understanding. Even though it is tempting to hope that we are just one diplomatic agreement, one technological leap, or one regulation away from its elimination, targeted ransomware is here to stay. As with other forms of crime, the government can expect better outcomes by planning how to manage the issue over time rather than searching for quick and complete solutions.

When it comes to ransomware, that means investing in the defense of broad swathes of the US economy—in particular small- to medium-sized organizations—and establishing more transparency about the problem. It also involves a continuation of efforts launched by the Biden administration over the past year: more pressure on ransomware groups and money laundering networks, better cryptocurrency regulation, and more support to national critical infrastructure.

If that answer is unsatisfying, so be it. In the words of a wise Jedi who tried, and failed, to solve a serious problem in a single afternoon: "Only a Sith deals in absolutes."

81   US Bureau of Labor Statistics, "Occupational Outlook Handbook: Information Security Analysts," https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

82   National Academy of Public Administration, *A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation*, January 2022, https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf.

83   Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Healthcare Industry*, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.

84   The CyberPeace Institute, *Playing with Lives: Cyberattacks on Healthcare are Attacks on People*, March 2021, https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

85   Liska, "Are Ransomware Attacks Slowing Down?"

ACKNOWLEDGMENTS

John Sakellariadis is a 2021-2022 Fulbright US Student Research Grantee, studying EU cybersecurity policy in Athens, Greece. John has worked as a journalist and researcher, and has written for Slate, The Record, and SupChina. He received a master's degree in Public Policy from Columbia University and a bachelor's degree in History & Literature from Harvard University.

Atlantic Council