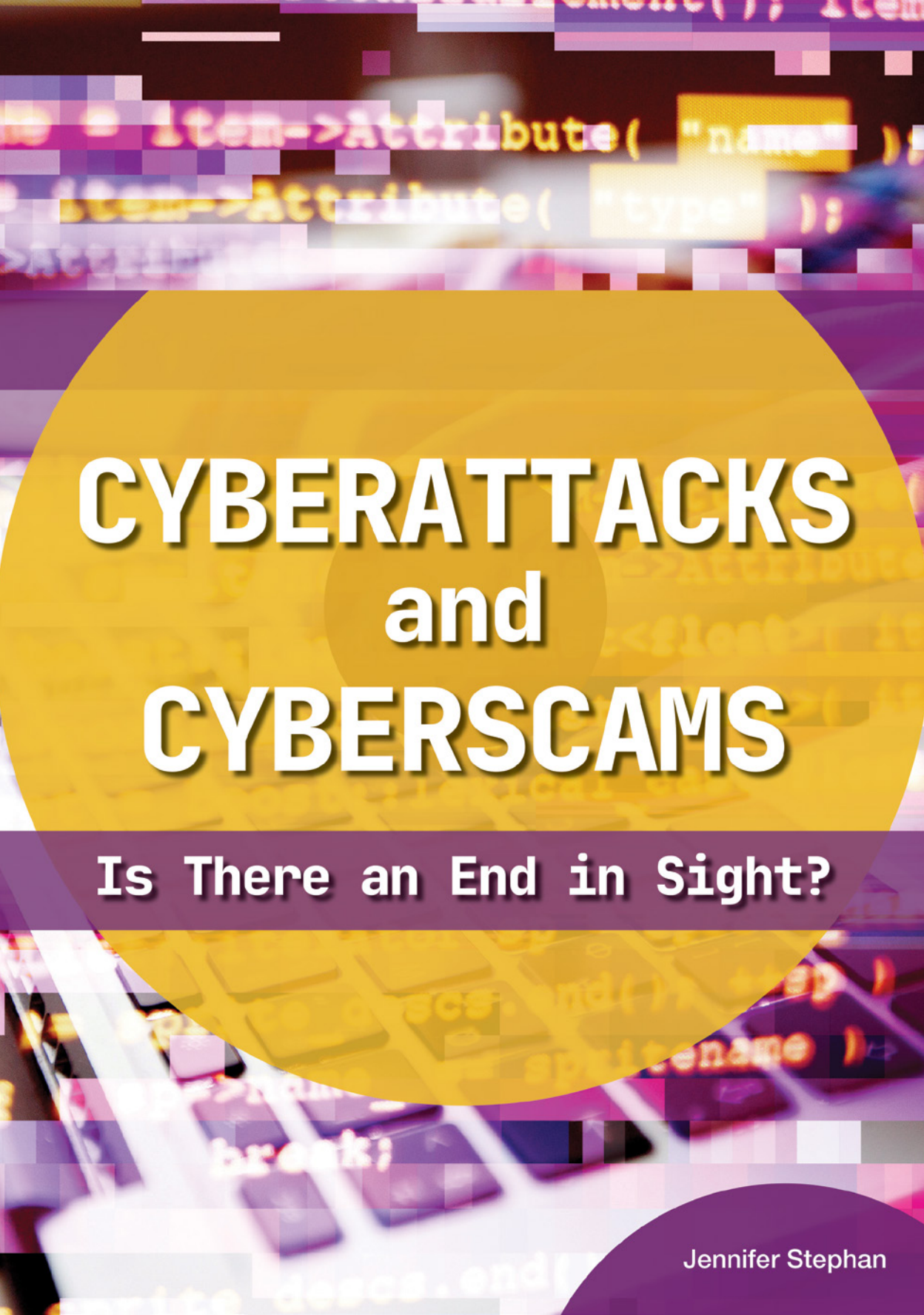

CYBERATTACKS
and
CYBERSCAMS
Is There an End in Sight?
Jennifer Stephan

Contents

Ransomware Attacks

Anxiety simmered inside the cars wrapped around gas stations and snaked down roads. In early May 2021 a seemingly endless queue of drivers lined up across the Southeast for a dwindling supply of fuel. While they waited, drivers calculated distances and gas mileage. Would they have enough gas to go to work? Which errands could they skip? How long would the gas shortage last? When the gas ran out, people had little reason to stop in the convenience stores at gas stations for a forgotten necessity or a snack. Revenues, not just gas supplies, were drying up. Hurricanes and floods had choked the regional economy before, but this was no act of nature. This was a ransomware attack.

Days before the major gas shortages, an employee had discovered a ransom note on Colonial Pipeline's computer network. The company provides almost half of the East Coast's fuel. It carries gasoline, diesel, jet fuel, and home heating oil to communities extending from Texas, across the Southeast, and up to New York. Criminal hackers had breached Colonial Pipeline's network, encrypted the company's data, and stolen almost six thousand personal records, mostly of employees and their family members. The ransomware froze Colonial Pipeline's business operations. To contain the attack, the company shut down all 5,500 miles (8,851 km) of its pipeline. The ransomware

In May 2021 a ransomware attack against Colonial Pipeline forced the company to shut down its lines, resulting in fuel shortages from Texas to New York.

developers, later identified as the Russia-linked group DarkSide, demanded millions of dollars in Bitcoin to unlock the files.

The pipeline shutdown and ensuing panic led to severe gas shortages and price increases across the Southeast. Governors in five states declared a state of emergency. The US Department of Transportation declared a federal emergency for the region. American Airlines rerouted flights, and some military bases in the affected areas limited gasoline consumption. Biden urged Americans to remain calm, and the White House called Russia to discuss dismantling ransomware networks.

Colonial Pipeline paid the Bitcoin ransom, worth about $4.4 million, but it still took nearly a week to restart the pipeline. Turning on a pipeline, as Biden said, "is not like flicking on a light switch."[12] A week after the cyberattack, 72 percent of stations in North Carolina and 88 percent in Washington, DC, were out of gas, according to the real-time fuel price app GasBuddy. In some areas, gas supplies did not recover for another week or more. "As far as I know, this is the first cybersecurity incident that has led to a measurable economic impact on the American population,"[13] says cybersecurity expert Jonathan Reiber. A cyberattack on one

company had hit the pocketbooks of consumers and gas station owners in an entire region.

Ransomware Attacks Surge

A volley of headline-grabbing ransomware attacks landed in the spring and summer of 2021. Just one month after the Colonial Pipeline hack, REvil extorted an $11 million ransom from JBS, a global meat supplier. One month later REvil demanded $70 million in the Kaseya ransomware attack. While these high ransom demands are unusual, ransomware attacks are not. In 2020 the FBI received almost twenty-five hundred ransomware complaints. Most cyberexperts, including those in the FBI, believe many attacks go unreported. Companies may fear that reporting an attack will tarnish their brand or make them look like easy prey. Cybersecurity firm SonicWall estimates that in 2020 there were actually more than 300 million ransomware attacks worldwide. "The number of these hacks and the scale of them is wildly out of control," says cybersecurity expert Matt Tait. It "is impacting ordinary folks' lives in a way that is very upsetting."[14]

Whatever the true number of ransomware attacks, it is growing. From 2019 to 2020, global ransomware attacks increased 62 percent, according to SonicWall. Ransom payments are also increasing. Over the same period, the average ransom payment rose 171 percent to $312,493, according to Palo Alto Networks.

Ransomware attacks on large companies with high ransoms grab big attention, but most ransomware attacks target small and midsize companies. Veterinarian offices, law firms, local libraries, and even individuals have all suffered. In 2020 ransomware attacks also impacted American cities, schools, and health care facilities. While the targets and the stakes vary, ransomware attacks follow a similar script.

> **"The number of these hacks and the scale of them is wildly out of control. . . . [It] is impacting ordinary folks' lives in a way that is very upsetting."[14]**
>
> —Matt Tait, cybersecurity expert

VIEWPOINT

Ransomware Payments Should Be Banned

The FBI generally discourages but does not prohibit companies from paying ransoms. Benjamin Wittes and Alvaro Marañon, both from the Lawfare Institute, argue for a stricter policy. They believe ransom payments should be banned, with a few exceptions. They explain:

> Most ransomware victim companies or entities are not innocent victims. . . . They've left systems vulnerable. . . . Whenever one of these companies pays a ransom, they are effectively encouraging future attacks. They're feeding a marketplace. Unlike human ransoms where the cost is human life, in most of these situations, the cost is data, which may be catastrophic for the [affected] entity but is not catastrophic for the society. . . .
>
> [Companies] should be generally prohibited from making these payments with the exception of circumstances in which they apply for and receive permission from federal authorities to do so. Federal authorities should review those applications with an eye toward larger public policy considerations like is there an imminent loss of human life at issue, is there going to be catastrophic damage to the economy generally rather than simply to a company that failed to do cybersecurity due diligence.

Quoted in Scott R. Anderson, "How Can Congress Take on the Ransomware Problem?," August 16, 2021, in *Lawfare Podcast*, produced by Jen Patja Howell, podcast. www.lawfareblog.com.

The Hack

To launch ransomware, hackers need to breach the network of an organization or individual. Joseph Blount, chief executive officer (CEO) of Colonial Pipeline, testified in a Senate hearing that he believes hackers used a compromised password to access the Colonial Pipeline computer system through an old virtual private network (VPN). The VPN used single-factor authentication, which only requires a username and password for access. How the hackers got the password in the Colonial Pipeline breach is unknown. In some cases, hackers simply guess a password. This "brute-force" method sometimes involves remarkably little brute force. According to a 2019 Google/Harris poll, almost

VIEWPOINT

Ransomware Payments Should Not Be Banned

Jen Ellis, a vice president at cybersecurity firm Rapid7, argues that banning ransomware payments will harm the most vulnerable organizations. She told the BBC:

> Banning payments would almost certainly result in a pretty horrific game of "chicken," whereby criminals would shift all their focus towards organizations which are least likely to be able to deal with downtime—for example hospitals, water-treatment plants, energy providers, and schools. The hackers may expect the harm to society caused by this downtime to apply the necessary pressure to ensure they get paid. They have very little to lose by doing this—and potentially a big payday to gain. Let's say the government creates a fund to support these organizations so they don't have to pay. If that happens, the attackers could then just switch their focus to small businesses and non-profit organizations which don't have the resources to protect themselves. They could face complete ruin if they don't pay. . . . Prohibiting payments is a great goal to shoot for. But we must be pragmatic in our approach to ensure we do not create significant economic and societal harm.

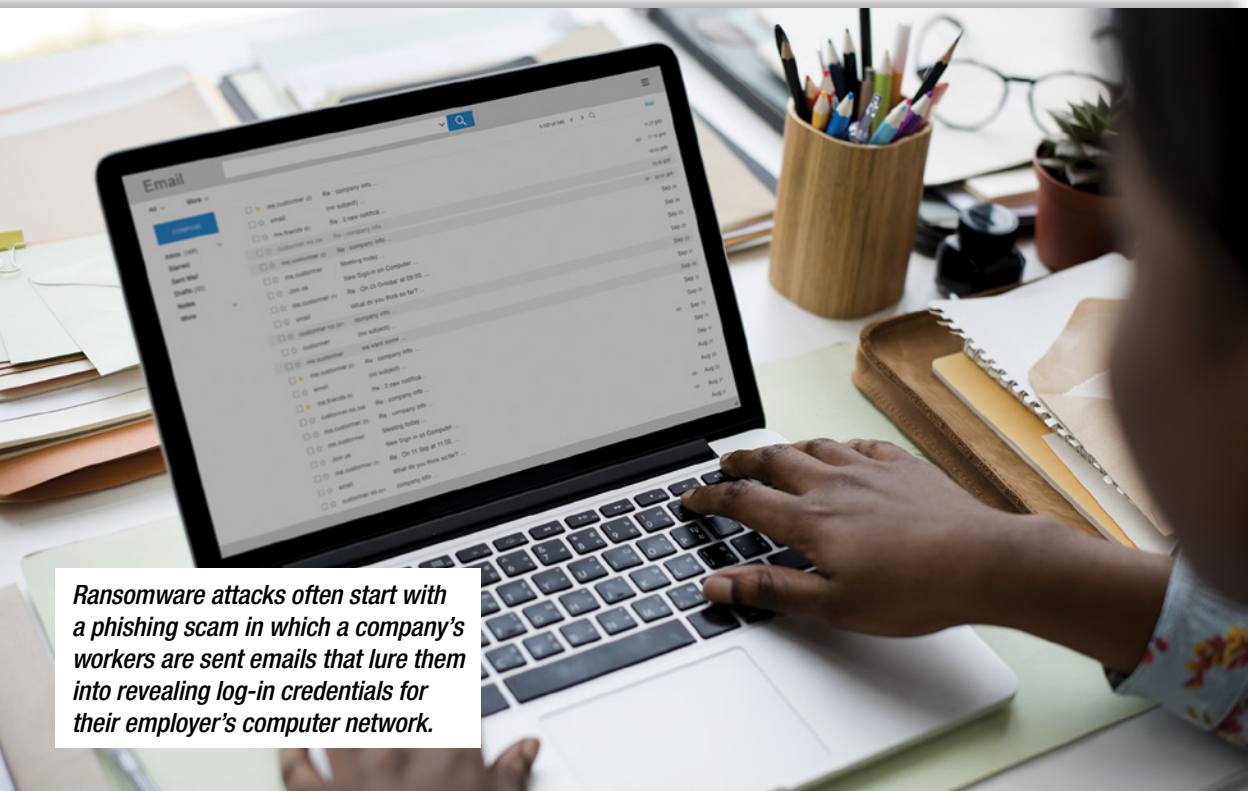
Quoted in Joe Tidy, "Ransomware: Should Paying Hacker Ransoms Be Illegal?," BBC, May 20, 2021. www.bbc.com.

one-quarter of Americans have used a password as simple as *123456* or *iloveyou*. In the case of Colonial Pipeline, however, Blount testified, "It was a complicated password. . . . It was not a 'colonial123'-type password."[15]

A Colonial Pipeline employee could have instead fallen victim to phishing. Ransomware attacks commonly begin with emails or texts sent to a wide pool of targets (phishing) or a specific target (spear phishing). Phishing can dupe users into divulging log-in credentials—usernames and passwords—or clicking a link or attachment that deploys malware on a computer. Phishing scams can be sophisticated. Attackers can research a target to personalize emails with the names of colleagues, company-specific

acronyms, or visuals like logos or photos that add credibility to emails or fake log-in pages. Compromising passwords is not the only method of deploying ransomware. Hackers can also breach a network through software vulnerabilities or with previously stolen credentials.

Before launching ransomware, some attackers snoop around the breached network. Documents like financial statements or cyberinsurance policies stored on company servers can help the criminals determine how much ransom to demand. Hackers may also seek out confidential documents or personal data to sell. The threat of releasing the sensitive information can further pressure companies to pay the ransom. In some cases, hackers find and delete backups to give organizations even more reason to pay the ransom. When hackers finally deploy ransomware, it encrypts the files on a computer network so they become unusable. A ransom note appears on a computer informing the company it has been the victim of a ransomware attack and giving instructions about how to pay the ransom. The attackers usually demand cryptocurrency in return for a decryptor.



Ransomware attacks often start with a phishing scam in which a company's workers are sent emails that lure them into revealing log-in credentials for their employer's computer network.

Source Notes

Introduction: Cyberscams and Cyberattacks Surge

1. Quoted in Leila Fadel, "A Ransomware Attack Hit Up to 1,500 Businesses. A Cybersecurity Expert on What's Next," NPR, July 6, 2021. www.npr.org.
2. Cyberspace Solarium Commission, *Executive Summary*, 2020. www.solarium.gov.
3. Quoted in White House, "Remarks by President Biden at the Office of the Director of National Intelligence," July 27, 2021. www.whitehouse.gov.
4. Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin, 2019, p. 297.

Chapter One: Cyberscams

5. Mark Button and Cassandra Cross, *Cyber Frauds, Scams and Their Victims*. New York: Routledge, 2017, p. 62.
6. Quoted in Marissa Parra, "'Something Was Not Right': Chicago Area Teen Warns of Job Scam Seeking Personal Information," CBS Chicago, July 1, 2021. https://chicago.cbslocal.com.
7. Quoted in Hugh Lessig, "'It Broke My Heart:' The Cruelty of Military Romance Scams," *Newport News (VA) Daily Press*, August 11, 2018. www.dailypress.com.
8. Quoted in Paula Span, "When Romance Is a Scam," *New York Times*, March 27, 2020. www.nytimes.com.
9. Quoted in Jon Emont, "This Year's Big Online Scam—Puppies," *Wall Street Journal*, September 2, 2020. www.wsj.com.
10. Quoted in NBC Bay Area, *Hackers Steal Millions from Bay Area Residents by Targeting Cellphones in "SIM Swap" Scams*, YouTube, May 29, 2019. www.youtube.com/watch?v=jc62Z8ABMel.
11. Quoted in NBC Bay Area, *Hackers Steal Millions from Bay Area Residents by Targeting Cellphones in "SIM Swap" Scams*.

Organizations and Websites

Cyber Operations Tracker, Council on Foreign Relations
https://microsites-live-backend.cfr.org/cyber-operations
The Council on Foreign Relations is an independent research institute focused on international policy. The Cyber Operations Tracker provides details on nation-state cyberattacks since 2005. It includes a map and a tool to search attacks by type of operation, victim, and state sponsor.

CyberSeek
www.cyberseek.org
The National Institute of Standards and Technology sponsored the creation of this website to help employers, job seekers, and students better understand the cybersecurity job market. The website includes an interactive map, a career pathway tool, statistics, and job descriptions.

Darknet Diaries
https://darknetdiaries.com
Jack Rhysider developed the *Darknet Diaries* podcast to educate and entertain audiences about hacking and cybersecurity. Using journalistic standards and methods, Rhysider tells the stories of nation-state attacks, penetration testers, criminal hackers, and more.

Internet Crime Complaint Center (IC3), Federal Bureau of Investigation
www.ic3.gov
The FBI's IC3 collects and reports on complaints of cybercrimes from personal scams to ransomware. The website provides current news, alerts, annual reports with statistics, and tips for protecting individuals and businesses from cybercrime.

Lawfare Institute
www.lawfareblog.com
The Lawfare Institute hosts multiple podcasts and a blog focusing on issues of national security, including cybersecurity. The blog posts and podcasts feature leaders, experts, and policy makers discussing current cybersecurity news.

For Further Research

Books

Frank W. Abagnale, *Scam Me If You Can: Simple Strategies to Outsmart Today's Rip-Off Artists*. New York: Portfolio, 2019.

Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin, 2019.

Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, 2019.

Nicole Perlroth, *This Is How They Tell Me the World Ends the Cyberweapons Arms Race*. New York: Bloomsbury, 2021.

Jeremy N. Smith, *Breaking and Entering: The Extraordinary Story of a Hacker Called "Alien."* Boston: Houghton Mifflin Harcourt, 2019.

Internet Resources

Better Business Bureau, *Online Scams Rise During COVID-19 Pandemic: 2020 BBB Scam Tracker Risk Report*, 2021. www.bbb.org.

Dorothy E. Denning, "Is Quantum Computing a Cybersecurity Threat?," *American Scientist*, vol. 107, no. 2, 2019. www.americanscientist.org.

Garrett M. Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army," *Wired*, October 13, 2020. www.wired.com.

Rachel Monroe, "How to Negotiate with Ransomware Hackers," *New Yorker*, May 31, 2021. www.newyorker.com.

Ransomware Task Force, *Combating Ransomware: A Comprehensive Framework for Action*, 2021. https://securityandtechnology.org.

Index

Note: Boldface page numbers indicate illustrations.