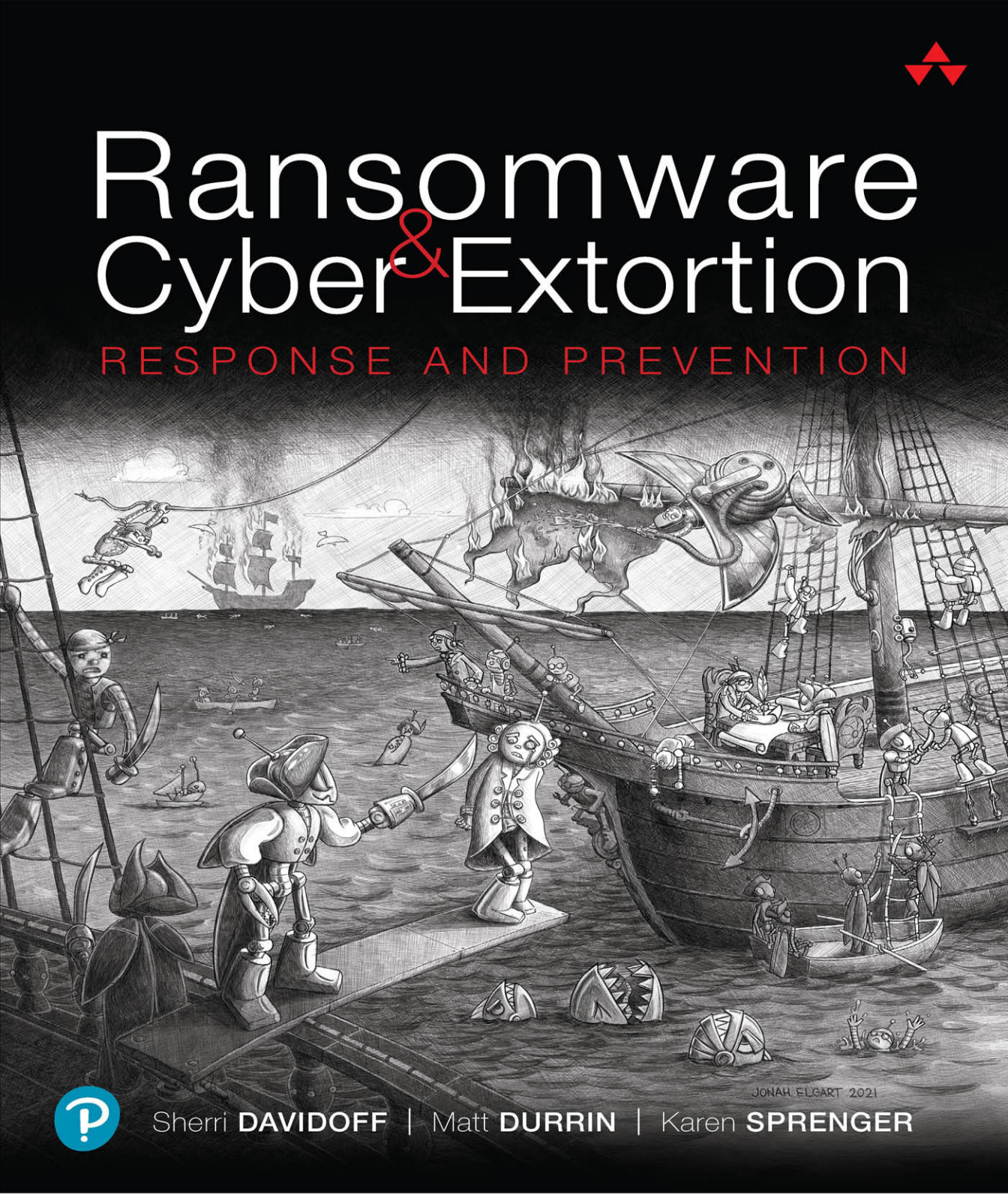
Ransomware & Cyber Extortion

RESPONSE AND PREVENTION



Sherri **DAVIDOFF** | Matt **DURRIN** | Karen **SPRENGER**

FREE SAMPLE CHAPTER |

Praise for *Ransomware and Cyber Extortion*

"*Ransomware and Cyber Extortion* is a masterstroke that will lead both technical and non-technical readers alike on a journey through the complex and sometimes dark world of cyber extortion. The encore of practical advice and guidance on preventing ransomware can help organizations of all sizes."

—Russ Cohen, Head of Cyber Services US, Beazley Group

"Davidoff and team have built a magisterial and yet still approachable guide to ransomware. This just became the definitive and classic text. I've been writing about some of these attacks for years and still was blown away by how much more they taught me. I'll hand this to every infosec newcomer and senior consultant from now on."

—Tara Wheeler, CEO, Red Queen Dynamics

"Ransomware attacks are no longer encrypt-and-export incidents; they have evolved into sophisticated, multipronged attacks that require a multidisciplinary response of forensic, technical, and compliance expertise and savvy cybercrime negotiation skills. Sherri Davidoff, Matt Durrin, and Karen Sprenger are that 'Dream Team' and concisely help the reader understand how to prepare for and respond to ransomware attacks. This book is a must-read for every member of an internal or external incident response team."

—Jody R. Westby, CEO, Global Cyber Risk LLC, Chair, ABA Privacy & Computer Crime Committee (Section of Science & Technology Law)

"A thoroughly delightful read, *Ransomware and Cyber Extortion* takes the topic everyone is talking about and deconstructs it with history and actionable guidance. A must-read before you next brief your board or peers on your own incident response plans."

—Andy Ellis, CSO Hall of Fame '21

This page intentionally left blank

Ransomware and Cyber Extortion

This page intentionally left blank

Ransomware and Cyber Extortion

Response and Prevention

Sherri Davidoff
Matt Durrin
Karen Sprenger

Addison-Wesley
Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Cover illustration by Jonah Elgart, bolognasalad.com

Screenshots by LMG Security have been reprinted with permission.

Definition icon courtesy of Colorlife/Shutterstock
Head's Up icon courtesy of iDesign/Shutterstock
Tip icon courtesy of maya_parf/Shutterstock

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2022942883

ISBN-13: 978-0-13-745033-6
ISBN-10: 0-13-745033-8

ScoutAutomatedPrintCode

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

This page intentionally left blank

To my husband and best friend, Tom.
– Sherri

To my caring, loving, and PATIENT wife Karah.
– Matt

To my mom, my dad, and my sister, for love and support through all of my adventures.
– Karen

This page intentionally left blank

Contents

I want to devise a virus
To bring dire straits to your environment
Crush your corporations with a mild touch
Trash your whole computer system and revert you to papyrus
—Deltron 3030, "Virus," May 23, 2000

This page intentionally left blank

Preface

No one realized when the hip hop song "Virus," was released in 2000 that it would turn out to be prophetic. Featuring a protagonist (Deltron Zero) who wanted to "develop a super virus," the lyrics describe his plans to infect and destroy computers around the world: "Crush your corporations with a mild touch / Trash your whole computer system and revert you to papyrus."[1]

More than two decades later, ransomware has reached epidemic proportions, shutting down hospitals, schools, law firms, municipalities, manufacturers, and organizations in every sector. Victims around the globe are routinely infected and forced to revert to pen and paper (for those lucky enough to still maintain supplies).[2,3] Worse, cyber attackers have discovered that threatening to publish information can give them similar leverage, leading to enormous—and purposeful—data leaks.

Today, data is wielded as a weapon. By threatening the confidentiality, integrity, and availability of data, criminals reap profits and force victims to bend to their will. After years of escalating ransomware attacks, brazen data publication, and a daily barrage of new victims touted in the headlines, they have honed their strategies and developed a scalable, successful business model.

The impacts of cyber extortion are far-reaching. Business operations have been halted, both temporarily and in some cases permanently. Medical records have been destroyed and patients' lives put in jeopardy. Key intellectual property has been sold to competitors. Private emails and personal details are routinely dumped so that they become visible to the public eye.

Court cases resulting from ransomware and data leaks are multiplying, even as victims and insurers pour funds into victim compensation and corrective action. Law enforcement agencies around the world are working every day to dismantle cyber extortion rackets, even as the criminals themselves crow to the media that they are not afraid.

"Extortion fatigue" is real. The problem is so pervasive that people can't digest the full scope and impact. At the same time, cyber extortion is wildly underreported. After all, no victim purposefully calls the media when they find out they've been hacked. Cases are routinely negotiated quietly, in secret. As a result, the true extent of cyber extortion cannot be known but is undoubtedly far greater than any statistics indicate.

Response is crucial. The steps taken by a victim organization in the hours, days, and months after a cyber extortion attack can dramatically impact the outcome.

1. Deltron 3030, "Virus," *Deltron 3030*, May 23, 2000, https://genius.com/Deltron-3030-virus-lyrics.
2. www.beckershospitalreview.com/cybersecurity/georgia-health-system-reverts-to-paper-records-after-ransomware-attack-5-details.html.
3. www.forbes.com/sites/tommybeer/2020/09/28/report-big-us-hospital-system-struck-by-cyberattack-forcing-staff-to-resort-to-paper-and-pen/.

This book is a practical guide to responding to cyber extortion threats, including ransomware, exposure extortion, denial-of-service attacks, and more. Throughout the book, we'll draw heavily from real-world case studies, as well as the vast library of unpublished cases handled by the authors during their work as response professionals. Readers will emerge better prepared to handle a cyber extortion attack properly, which will help minimize damage and expedite recovery.

As highlighted throughout the book, cyber extortion is typically the last and most visible phase of an intrusion. Often, cybercriminals have access to a victim's environment or data for an extended period of time, siphoning off key information, researching the victim, and installing malware and other tools that will maximize their leverage.

By employing effective cybersecurity prevention measures throughout society, we can reduce the risk of cyber extortion and cybercrime more generally. In the last chapter of this book, we delve into the underlying causes of cyber extortion and provide recommendations for reducing this risk.

Since cyber extortion actors, tools, and tactics evolve constantly, throughout this book we emphasize response and prevention techniques that will stand the test of time.

Who Should Read This Book?

This book is intended to be a valuable resource for anyone involved in cyber extortion prevention, response, planning, or policy development. This includes

- Chief information officers (CIO) and chief information security officers (CISO) who are involved with planning, their organizations' cyber extortion response or developing prevention strategies
- Cybersecurity professionals, incident responders, forensics investigators, ransom negotiators, cryptocurrency payment processors, and anyone involved in ransomware and cyber extortion response
- Technology staff, including system administrators, network technicians, help desk workers, security teams, and other individuals responsible for responding to cyberattacks or securing their environments
- Executives who want a deeper understanding of the cyber extortion threat and effective response and prevention strategies
- Legislators, regulators, law enforcement agents, and anyone involved in establishing policy relating to cyber extortion
- Anyone interested in learning more about ransomware and cyber extortion attacks

How This Book Is Organized

This book is designed to be a practical guide for response and prevention of ransomware and cyber extortion threats. Here is a summary of our journey in this book:

- **Chapter 1, Impact:** Cyber extortionists threaten the confidentiality, integrity, and availability of information in an effort to gain leverage over a victim. The four types of cyber extortion are denial, modification, exposure, and faux extortion. Impacts of cyber extortion range from operational disruption to financial loss, reputational damage, lawsuits, and more. In addition to targeting victims directly, adversaries compromise technology suppliers such as managed services providers (MSPs), cloud providers, and software vendors.
- **Chapter 2, Evolution:** Ransomware and cyber extortion attacks have been around longer than most people realize and come in a variety of forms. In this chapter, we cover the history of ransomware and its impact on affected organizations, and then follow its evolution into the bustling criminal economy that drives it today.
- **Chapter 3, Anatomy of an Attack:** Extortion is the last phase of a cyber extortion attack. Adversaries first gain access to the victim's technology environment and then take steps to expand their access, assess the victim, and prepare prior to extortion. In this chapter, we step through the phases of a cyber extortion attack. Along the way, we identify indicators of compromise and provide response tips that can mitigate or even stop the attack in progress.
- **Chapter 4, The Crisis Begins:** The early stages of cyber extortion response significantly impact how quickly an organization recovers and is able to resume its normal operations. In this chapter, we provide insight on recognizing the common early indicators of a cyber extortion attack. We also walk through the concept of triage and explain how development of a clear and effective response strategy is critical early in the response process.
- **Chapter 5, Containment:** When a cyber extortionist strikes, quick action can reduce the damage and help speed recovery. In this chapter, we discuss techniques for halting data exfiltration and file encryption/deletion, resolving denial-of-service attacks, and locking the adversary out of the victim's environment. We end the chapter by talking about threat hunting, including methodology, sources of evidence, tools and techniques, staffing, and results.
- **Chapter 6, Investigation:** Taking the time to conduct an investigation is critical for both short- and long-term resolution of cyber extortion incidents. In this chapter, we discuss reasons for investigating, techniques for identifying the adversary, methods for scoping an attack and tracking down "patient zero," and the fundamentals of data breach investigations. We also cover evidence preservation, which has the potential to reduce the long-term damage of cyber extortion attacks.

- **Chapter 7, Negotiation:** How do you reach an agreement with criminals? This chapter is a practical guide to initiating, managing, and completing a ransom negotiation. You'll learn about haggling, proof of life, and closing the deal. We also discuss common mistakes made during cyber extortion negotiations and ways to avoid them.
- **Chapter 8, Payment:** Although paying a ransom may be undesirable or even unthinkable for some, in many cases it is the victim's chosen path forward. In this chapter, we discuss the pros and cons of paying a ransom, and then the practicalities of the payment process, including forms of payment, types of intermediaries, timing issues, and what to do after payment has been made. We also discuss payments prohibited due to sanctions and consider the due diligence that victims should conduct before any payment is made.
- **Chapter 9, Recovery:** The goal of every incident is to return to normal operations. In this chapter, we cover the process of recovery, as well as strategies for reducing the risk of data loss and reinfection, which can enable the victim to resume operations with confidence. Along the way, we also describe key improvements for your environment that can reduce future risk and increase defensive capabilities.
- **Chapter 10, Prevention:** Cyber extortion is typically the last phase of a cyberattack. Fundamentally, prevention is best accomplished by implementing a strong, holistic cybersecurity program. In this chapter, we highlight the keys to building such a cybersecurity program, and then delve into specific defensive steps that help to reduce the risk of cyber extortion attacks or mitigate their impact. We conclude by discussing broad-scale, macro changes that are needed to effectively combat the cyber extortion epidemic.

Other Chapter Elements

Throughout each chapter we have included other elements meant to highlight important information, concepts, or examples, some with graphical icons to easily identify each element:

- **Learning Objectives:** A bulleted list of the material covered in that chapter
- **Case Studies:** Real-world cyber extortion cases that demonstrate the concepts being discussed
- **Definition:** Explanations of terms that are specific to cyber extortion or cybersecurity
- **A Word About:** Discussion of a key term and how it is used in this book
- **Tip:** Actionable information for the reader
- **Heads Up!:** Useful background information for the reader

Discussion Questions

At the end of each chapter, we include a section called "Your Turn!" in which we provide the opportunity for you to create your own scenario. We then offer questions for you to consider and discuss with others. Our hope is that this section will provide you with countless opportunities to evaluate cyber extortion incidents from all angles and understand that there is no one right answer when responding to such attacks.

Checklists

At the end of this book, you will find a series of checklists meant to be used (and reused) to help you prevent, and if necessary respond to, cyber extortion. They compile information found in the book in a high-level, quick-and-easy reference format.

Stay Up to Date

For regular updates and commentary on the latest cyber extortion and ransomware developments, visit the authors' website: ransombook.com.

Adversary tactics are rapidly evolving, and best practices for response and prevention evolve with them. In this book, we present a foundation for responding to cyber extortion events and preventing these devastating attacks.

Visit the authors' website for the latest news, response tips, discussion topics, and more. As we all share information and experiences, it is our hope that our global community can work together to shine a light on cyber extortion and reduce the risk.

This page intentionally left blank

Acknowledgments

It takes a village to produce a book, and this one is no exception. We'd like to thank the many people who contributed, from concept to production and everything in between.

First and foremost, thanks to our editors Haze Humbert and James Manly, whose wealth of publishing experience and professional insights were invaluable. We especially appreciated your expert cat-herding skills, and how you patiently kept the process moving forward while giving us grace and time as we all navigated the uncharted waters of working together during the pandemic.

We are grateful to our colleagues Michael Ford and Ben Mayo, who took the time to review the book outline in the early phases to ensure we comprehensively addressed our audience's needs. Michael also provided deep and substantive feedback throughout the entire book, for which we cannot thank him enough. We'd also like to thank Pearson's excellent editing and production teams, including Julie Nahil, Menka Mehta, Aswini Kumar, and Jill Hobbs.

You *can* judge a book by its cover, and we feel so fortunate that artist Jonah Elgart lent his incredible skills to this work—researching actual pirate ship designs, sharing paintings and ideas, and even putting some "Easter eggs" into the illustration (see if you can find all three authors and the artist himself on the cover!). Thank you, Jonah, for gracing our written words with such a beautiful and thought-provoking work of art.

Cryptocurrency payment expert Marc Grens, co-founder of DigitalMint, kindly gave his time for an extensive interview and answered our many in-depth questions on the evolving cryptocurrency due-diligence and payment processes. His firsthand expertise in this area was invaluable, and we are grateful for the opportunity to bring this information to our readers.

Cyber insurance veterans Bob Wice and Frank Quinn took the time to give in-depth interviews that gave us a behind-the-scenes perspective on cyber insurance and risk management. Thank you for your trust and enabling us to share your wisdom with the readers of this book.

Ransomware and cyber extortion is a deep and quickly evolving topic. We've learned through experience by handling a variety of cases at LMG Security, with the support of our incredible team. Many thanks to all of our colleagues at LMG, particularly Derek Rowe, Madison Iler, and Dan Featherman. Thanks also to our longtime attorney (now judge) Shane Vannatta, for helping us to navigate the early days of ransomware and cyber extortion.

We are also grateful to our many colleagues who helped to shape our understanding of ransomware and cyber extortion over the years, including Scott Koller, Ryan Alter, Randy Gainer, David Sande, Marc Kronenberg, Bill Siegel, David Sherman, Katherine Keefe, Brett Anderson, Luke Green, Sue Yi, Mike Wright, Jody Westby, Sean Tassi, Peter Enko,

Dave Chatfield, Mark Greisinger, Vinny Sakore, Andrew Lipton, Michael Phillips, Marc Schein, and Michael Kleinman.

On a personal level, each of us would like to share our gratitude individually as well.

From Sherri: Many thanks to my dear little ones, Violet and Thunder, whose love and enthusiasm buoyed me every day. My husband, Tom Pohl, and my amazing friends, Annabelle Winne and Jeff Wilson, were there for me every day: cheering me on, listening, and providing wise advice. I couldn't have done this without you. I am grateful for my friends and family, especially my father, E. Martin Davidoff, my mother, Sheila Davidoff, my sister, Laura Davidoff Taylor, as well as Jessie Clark, Shannon O'Brien, Kaloni Taylor, Steve McArthur, Kevin Head, Samantha Boucher, Deviant Ollam, Kelley Sinclair, and so many others. Your constant support got me through the long journey of book writing once again. Above all, I feel so lucky to work with Karen Sprenger and Matt Durrin, my incredible co-authors! I have learned so much from you, both in the trenches while responding to extortion cases and during the process of crafting this book. No one could ask for a better team.

From Matt: I'd like to specifically thank my wife, Karah Durrin, and my daughter, Lauren Durrin, for being my quiet inspiration during the writing process. I could not have done this without your amazing and tireless support. I'd also like to thank all of the friends and family who helped me keep going throughout the journey. In addition to the people in my personal life, I'd like to extend a huge thank you to the LMG Security team for giving me the opportunity to make cybersecurity my career. It has been a wild ride, but I feel so blessed to be surrounded by such a wonderful and talented group of people. Finally, I'd like to thank my partners in crime (stopping), Sherri Davidoff and Karen Sprenger. I likely would have never discovered my passion for cybersecurity without both of you amazing women. Sherri believed in me enough to give me an opportunity to dive into the industry. Karen, in addition to being a fantastic security expert, was the person who first taught me how to properly capture a forensic hard drive image. I'm so grateful to have you both as friends and mentors. Thank you both and here's to continuing our shenanigans together!

From Karen: In addition to those listed above, I'd like to thank my mom, Genie Thorberg, my biggest champion and the person who taught me how to use a computer; my dad, Bob Sprenger, who gave equal parts love and life lessons; and my sister, Rhonda Johnson, the first and best of many strong women who led the way for me. To my partners in shenanigans, Sherri Davidoff and Matt Durrin, thank you for the love, laughter, and commitment throughout this project. Although you have not yet succeeded in turning me into a night owl, you have made a daunting task achievable and, dare I say, enjoyable. I'll look forward to swapping cybercrime news links for many years to come. I've had the great blessing of working for women-led companies at key points during my career. Thank you to Linda Wright and Desiree Caskey, who gave me my start many years ago—before I realized that women in technology were few and far between. And especially to Sherri, a particularly heartfelt thank you to you for taking a chance on me all those years ago and giving me a place to spread my wings in cybersecurity and business development. I've learned and grown so much working with you. Finally, thank you to my pack of poodles, Jasper and Gracie, who spent hours lying at my feet to keep me company throughout the whole process, and Sadie, who joined us near the end. I couldn't have done it without the three of you.

About the Authors

Sherri Davidoff (left), Matt Durrin (center), Karen Sprenger (right)

Sherri Davidoff is the CEO of LMG Security and the author of *Data Breaches: Crisis and Opportunity*. As a recognized expert in cybersecurity, she has been called a "security badass" by *The New York Times*. Sherri is a regular instructor at the renowned Black Hat trainings and a faculty member at the Pacific Coast Banking School. She is also the co-author of *Network Forensics: Tracking Hackers Through Cyberspace* (Addison-Wesley, 2012). Sherri is a GIAC-certified forensic analyst (GCFA) and penetration tester (GPEN) and received her degree in computer science and electrical engineering from the Massachusetts Institute of Technology (MIT).

Matt Durrin is the Director of Training and Research at LMG Security and a Senior Consultant with the organization. He is an instructor at the international Black Hat USA conference, where he has taught classes on ransomware and data breaches. Matt has conducted cybersecurity seminars, tabletop exercises, and classes for thousands of attendees in all sectors, including banking, retail, healthcare, government, and more.

A seasoned cybersecurity and IT professional, Matt specializes in ransomware response and research, as well as deployment of proactive cybersecurity solutions. Matt holds a bachelor's degree in computer science from the University of Montana, and his malware research has been featured on *NBC Nightly News*.

Karen Sprenger is the COO and chief ransomware negotiator at LMG Security. She has more than 25 years of experience in cybersecurity and information technology, and she is a noted cybersecurity industry expert, speaker, and trainer. Karen is a GIAC Certified Forensics Examiner (GCFE) and Certified Information Systems Security Professional (CISSP) and holds her bachelor's degree in music performance (yes, really). She speaks at many events, including those held by the *Wall Street Journal* Cyber Pro, Fortinet, the Internal Legal Tech Association, and the Volunteer Leadership Council. In her spare time, Karen considers "digital forensics" a perfectly acceptable answer to the question, "But what do you do for fun?" A lifelong Montanan, she lives in Missoula with oodles of poodles.

Chapter 3

Anatomy of an Attack

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

—Sun Tzu

Learning Objectives

- Identify the key activities associated with a cyber extortion incident
- Understand common technical methods that cyber extortion gangs use to gain access to victim networks
- Describe tools and tactics that adversaries use to gain entry, expand, appraise, prime the environment, and gain leverage over their victims
- Identify opportunities for detection at each phase

A cyber extortion attack is never *just* a cyber extortion attack. There is always an escalation in activities from the adversary's initial entry, expansion throughout the environment, and ultimately the extortion threat.

While every attack is different, there are common adversary activities associated with most, if not all, cyber extortion attacks. Understanding these common threads can help victims more effectively respond to cyber extortion attacks, minimize damage, and in some cases, prevent extortion from occurring in the first place.

In this chapter, we deconstruct a cyber extortion attack into key components and present these along with common indicators of compromise and effective response tactics.

3.1 Anatomy Overview

Cyber extortion attacks do not begin and end with the extortion demand itself, although this is often the most visible part. The authors of this book have analyzed hundreds of

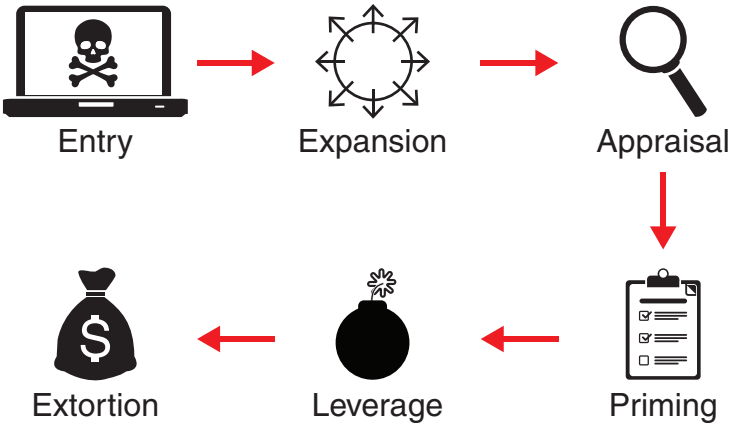


Figure 3.1 Anatomy of a cyber extortion attack

(Illustration courtesy of LMG Security. Graphics: computer, grmarc/Shutterstock; skull and crossbones, Sergey Siz`kov/123RF; circle with arrows, bloomua/123RF; magnifying glass, olesya k/Shutterstock; clipboard, HSDesain/Shutterstock; bomb, AcaG/Shutterstock; money bag, Pensiri Saekoung/123RF)

extortion cases, many firsthand, and identified common adversary tactics observed throughout these attacks. A visual representation of this anatomy is shown in Figure 3.1.

Importantly, cyber extortion attacks are not a linear process. An adversary may cycle through various components multiple times, or even repeat the entire process as part of a single overarching attack.

The common components of cyber extortion attacks include:

- **Entry:** The adversary gains unauthorized access to the victim's information technology resources.
- **Expansion:** The adversary engages in a recursive process of expanding access. During this phase, the adversary typically gains persistence, conducts reconnaissance, increases the scope of their access, and transfers access to other adversaries.
- **Appraisal:** The adversary assesses the victim's strengths and weaknesses, including data repositories, financial posture, operational infrastructure, and more. This information is used to define and refine the adversary's ongoing attack strategy.
- **Priming:** The adversary modifies the environment to maximize leverage in the following phases. This may include destroying backups, dismantling security, monitoring systems, and more.
- **Leverage:** The adversary actively threatens the confidentiality, integrity, or availability of the victim's information resources. This is commonly accomplished by detonating ransomware, exfiltrating data to systems under the adversary's control, launching a denial-of-service attack, or all of these.
- **Extortion:** The adversary demands payment or services in exchange for restoring availability, integrity, or confidentiality of data or technology resources.

In the following sections, we discuss each of these components in detail, highlight opportunities for early detection, and discuss effective response strategies.

A Word About "Kill Chains" and "Attack Frameworks"

In general, a "kill chain" is a detailed breakdown of the phases and structure of an attack. Originally a military term, this concept was adapted for use in a cybersecurity response by Lockheed Martin[1] in 2011. Each step of the kill chain describes a specific activity or element of an attack and is used to develop defensive strategies that can potentially stop or prevent the attack at each point.

In 2013, MITRE developed the ATT&CK framework[2] and expanded the kill chain model to include detailed tactics and procedures for each of the portions of an attack. The MITRE framework is an excellent model for analyzing and communicating the latest adversary tactics, and understanding different types of cyber extortion attacks.

Since cyber extortion attacks constantly evolve, the authors of this book elected to present a general, high-level "anatomy" of cyber extortion attacks. This anatomy is intended to be used as a foundation for understanding all types of cyber extortion attacks. It can be used in conjunction with a more detailed kill chain model such as the MITRE ATT&CK framework when analyzing specific cases or attack trends.

3.2 Entry

In the entry phase, the adversary gains a foothold inside the victim's technology environment. While this may mean that the adversary gains access to a computer inside the victim's network, it could also be a cloud-based resource such as a virtual machine, a hosted application such as email, or a remote system such as an employee's personal computer. Whatever the point of entry, the adversary will leverage this initial access during the next phase (expansion) to spread throughout the environment.

Common methods of entry include:

- **Phishing:** The adversary sends an email, text, or other message designed to trick the victim into taking an action that gives the adversary information and/or access to the victim's environment.

1. "The Cyber Kill Chain," Lockheed Martin, www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

2. "ATT&CK," Mitre, https://attack.mitre.org/.

- **Remote logon:** The adversary successfully gains access to an interactive session via a remote logon interface such as Remote Desktop Protocol (RDP), using credentials that have been guessed, stolen, purchased, or otherwise obtained.
- **Software vulnerability:** A vulnerability is found in the victim's Internet-facing applications, servers, or network equipment.
- **Technology supplier attack:** The adversary has access to a supplier's technology resources (such as a software provider or managed service provider [MSP]), whether legitimately or through compromise, and leverages this to gain access to the victim's environment.

Let's discuss how adversaries execute each entry method, and highlight the corresponding opportunities for detection and effective response techniques.

Definition: Indicators of Attack and Compromise

Throughout this book, we will refer to the terms "indicators of attack" and "indicators of compromise." Here are their definitions to set the stage:

- **Indicators of attack** (IoA): Evidence that an adversary is attempting to gain unauthorized access to devices or services. It can include detections of multiple failed login attempts, exploitation attempts, and more.
- **Indicators of compromise** (IoC): Evidence of successful unauthorized access, such as logs of successful authentication, IDS/IPS alerts, or other system behaviors indicative of suspicious activity.

Sources of evidence may include log alerts, forensic artifacts, or system behavior. See Chapter 6 for more detail regarding sources of evidence.

3.2.1 Phishing

Cyber extortion events often start with a phishing attack, in which the adversary sends a message designed to trick the intended victim into taking an action, such as clicking on a link or opening an infected attachment. Phishing kits, which automate the attack process, often sell for $5 to $15 on the dark web.

Phishing attacks can be conducted via any form of messaging, from email to SMS messages to social media. (Carrier pigeon, anyone?[3]) However, cyber extortionists typically aim to get a foothold within an organization's network, and email is the most widely

3. D. Waitzman, "A Standard for the Transmission of IP Datagrams on Avian Carrier," April 1, 1990, https://tools.ietf.org/html/rfc1149.

used method for transmitting messages from external to internal senders in these types of environments.

3.2.1.1 Remote Access Trojans

The payload of phishing messages is often a remote access Trojan (RAT), which is a software utility designed to enable an adversary to remotely control or access a computer system.

The features of RATs vary widely, but typically they enable an adversary to do the following:

- Establish a communication channel between the compromised endpoint and a controlling server
- View data about the infected computer
- Control the infected computer remotely
- Evade detection

Sophisticated RATs can include advanced capabilities, enabling the adversary to take the following steps:

- Automatically steal sensitive information from the victim's computer, such as credit/debit card numbers, stored passwords, computer system information, and more
- Interactively log on using Virtual Network Computing (VNC) or a similar program
- Produce reports of user activity, account balances, web history, and more
- Execute advanced privilege escalation attacks and facilitate the adversary's lateral movement
- Install addition malware (including ransomware)
- Leverage the victim's computer(s) to attack other organizations

Malicious Swiss Army knives such as Emotet and Trickbot rely on phishing campaigns to deliver their malware, which adversaries leverage to gain persistent access, steal information, and distribute other threats. The presence of a RAT is often a precursor of a cyber extortion attack.

Traditionally, RATs are delivered via social engineering attacks such as phishing emails, malicious websites, or compromised applications. The adversary who installs a RAT may conduct cyber extortion, or sell or rent access to other criminals, who in turn may choose to conduct cyber extortion themselves.

Opportunities for Detection

When an extortion attack starts with phishing, typically a user device is "patient zero," the first system entered by the adversary. From there, the adversary establishes persistence,

which typically involves a reverse shell of some kind (since most devices are blocked by the firewall from direct inbound Internet access). The adversary then leverages stolen credentials or unpatched vulnerabilities to escalate their account privilege, move laterally, and spread throughout the environment.

Specific indicators include the following:

- **Warnings and alerts in email security software:** In some cases, the suspicious email may be automatically quarantined; in others, the email is sent along with a warning to the users, email administrator, or both. The user's email system may also insert a warning in the subject or body of an email if the email meets certain criteria that are in line with characteristics of a phishing attack.
- **User report:** A user may report the phishing message to the response team. When this happens, IT staff should quickly look for other users who received the same or similar phishing emails and remove those emails from other users' inboxes. If any user clicked on a link or attachment in the suspected email, this should activate the organization's incident response processes to ensure that any resulting infection is contained.
- **Malware sample:** By analyzing a malware sample, you can often match it to specific known phishing campaigns or hacker groups and obtain lists of additional indicators to search for in the affected environment.
- **Email application logs:** Application logs may contain warnings related to emails that have been processed, or alerts on blocked attempts, which can help you identify high-risk users, periods of unusual activity, changes in user risk profiles, and more.
- **Antivirus log entries:** When a user clicks on a link or attachment in a phishing email and downloads or runs malware, it may generate an antivirus software alert.
- **Event logs:** Similarly, when a user clicks on a link or attachment in a phishing email that results in code execution, it may generate records of unusual activity such as privileged command execution, scheduled task creation, or application and service starts or stops.

3.2.2 Remote Logon

Many cyber extortion attacks occur because the adversary gained access to a remote logon interface, such as an RDP platform. Quite often, cyber extortionists purchase stolen credentials on the dark web from an initial access broker rather than stealing or guessing them.[4] Then, the extortionists use these credentials to gain a foothold in the network and deploy their attack.

4. Victoria Kivilevich and Raveed Laeb, "The Secret Life of an Initial Access Broker," KELA, August 6, 2020, https://ke-la.com/the-secret-life-of-an-initial-access-broker/.

There are good reasons why "open" RDP services have traditionally been the root cause of a large percentage of extortion attacks:

- No special tools are needed to gain remote access to the service.
- RDP is a common protocol that often does not trigger alerts, particularly if it is actively used by employees or an IT administrator.
- The adversary can often pivot through the compromised computer to gain access to other systems using RDP inside the network.

Many organizations use RDP or other remote access tools so that employees can log in to their workstations from home or while traveling, or so IT administrators or vendors can access an internal network remotely at all hours. This is also—and unfortunately—convenient for adversaries, who frequently steal credentials or use password-spraying attacks to gain unauthorized access.

The vast supply of stolen passwords available for free or for sale on the dark web has fueled these attacks. By the summer of 2020, researchers had identified more than 15 billion stolen username and password combinations on the dark web.[5] At the time of this writing, stolen RDP credentials sell for $16 to $24 each.[6]

Many people reuse the same password for multiple accounts.[7] Adversaries leverage this tendency by conducting "credential stuffing" attacks, in which they take stolen credentials and attempt to use them on a wide variety of logon interfaces. When they successfully log in to another account, they can either leverage it themselves or sell access to the newly compromised account.

In 2020, the COVID-19 pandemic suddenly created a rush to remote work. In response, many organizations rapidly enabled remote access with little security oversight, and were compromised as a result.

Opportunities for Detection

Common signs of remote authentication attack or compromise include the following:

- **Failed logon attempts:** When an adversary conducts password spraying or credential stuffing attacks, there are often repeated failed logons (sometimes followed by a successful logon). This can occur at the perimeter, or it can occur within the network as the adversary attempts to move laterally. Unfortunately, many networks are not configured to record or report failed logon attempts on Microsoft Windows hosts within

5. Davey Winder, "New Dark Web Audit Reveals 15 Billion Stolen Logins from 100,000 Breaches," *Forbes*, July 8, 2020, www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/.

6. "The Price of Stolen Remote Login Passwords Is Dropping. That's a Bad Sign," Threats Hub (blog), July 8, 2022, www.threatshub.org/blog/the-price-of-stolen-remote-login-passwords-is-dropping-thats-a-bad-sign/.

7. "Online Security Survey: Google/Harris Poll," February 2019, https://services.google.com/fh/files/blogs/google_security_infographic.pdf.

their network, meaning that an adversary can automate attempts to authenticate within the network without being detected.

- **Unusual successful logon attempts:** These may include logins at odd times or places, distinct user-agent strings, and "impossible travel" alerts notifying of logons from geographically distant locations in a quick succession.
- **Creation of new accounts:** Such accounts may suddenly be used for remote access.

3.2.3 Software Vulnerability

Adversaries routinely search for exploitable vulnerabilities in widely used software and leverage these to launch cyber extortion attacks, as seen in the Kaseya attacks, as well as adversaries' response to the ProxyShell and Log4j vulnerabilities (among many others). In the case of Accellion, the Cl0p group was able to exploit a critical vulnerability in Accellion FTA devices and steal sensitive data affecting more than 9 million individuals, resulting in a $8.1 million class-action settlement in January 2022.[8]

The "Shodan.io" search engine, which indexes Internet-connected devices, can be used by adversaries and defenders alike to identify potentially vulnerable Internet-facing services.

Timely patch deployment can dramatically reduce the risk of a perimeter device compromise. However, IT administrators are often unaware that their specific firmware or software version is vulnerable, particularly in organizations that have limited resources for IT management. Furthermore, zero-day vulnerabilities exist for perimeter devices, and may be incorporated into high-end exploit kits before the manufacturer has time to identify the issue.

Opportunities for Detection

Common signs of attack via perimeter software vulnerability include the following:

- Alerts on port or vulnerability scans on perimeter devices (although this is a normal occurrence, so it's important to review such alerts carefully and resist the urge to be lulled into complacency)
- Strange error messages relating to that application or system, performance degradation (processes that overwhelm the processor or memory), or system/application crash
- Unexpected outbound connections from servers or even workstations
- Unusual and unrecognized processes or applications running on perimeter systems

8. Sara Merken, "Accellion Reaches $8.1 Mln Settlement to Resolve Data Breach Litigation," Reuters, January 13, 2022, www.reuters.com/legal/litigation/accellion-reaches-81-mln-settlement-resolve-data-breach-litigation-2022-01-13/.

Case Study: VPN Vulnerability

A school district in the Midwest was infected with the Dharma ransomware, circa 2021. All of its primary servers were down. While the district managed to hobble along and hold classes, all administrative functions were effectively halted: payroll, supply ordering, bill payment, and so on.

How did the hackers break in? Two things had gone wrong. First, the FortiGate VPN/firewall on which the school district relied had a terrible vulnerability. A patch had been released more than 8 months prior to the attack, but the school district had never applied it. Second, the local administrator accounts on the servers and workstations all shared the same passwords. Once the adversary hacked one system, they were able to log in to all the rest using standard remote access tools. RDP was available to the local administrator, which made the adversary's job even easier.

Once inside, the adversary worked very quickly to encrypt the systems. They logged in for only a few minutes at a time—just long enough to install the ransomware and log out. Once the VPN was compromised, it took only 15 to 20 minutes for the adversaries to detonate ransomware on the primary servers. They didn't bother touching the workstations at all.

Luckily, the school district had backups that were offline and off network, and that were not encrypted. Even so, it took 10 days to get its systems back up and running. Unfortunately, the servers held large volumes of private student information, including medical, mental health, and disciplinary data. The district was required to launch an investigation to determine the risk of a data breach.

Forensic investigators were able to determine that the attack was largely automated. The interactive logons were extremely short and not long enough to support any significant data acquisition or access. This was consistent with most Dharma attacks up to this point. A specialized team of data breach attorneys concluded that there was very low risk of data exposure, and the incident did not meet the definition of a data breach.

3.2.4 Technology Supplier Attack

Frighteningly, the entry point for a cyber extortion attack may be a supplier, such as an IT provider, MSP, equipment vendor, or cloud provider. In 2019, 22 towns in Texas were hit with a devastating REvil ransomware attack, which was traced back to their common MSP.[9] After infiltrating the MSP's network, the adversary leveraged the MSP's normal remote administration tool, ConnectWise Control, to deploy the ransomware throughout

9. "Texas Municipalities Hit by REvil/Sodinokibi Paid No Ransom, Over Half Resume Operations," Trend Micro, September 10, 2019, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations.

customer networks. Thanks to an effective backup and recovery strategy and strong response plan, the towns' operations were successfully restored within a week.[10]

Cloud providers, too, suffer ransomware attacks that can dramatically impact customers. In May 2020, Blackbaud, a leading provider of cloud-based fundraising software, was hit with a ransomware attack. Customers were notified in July and told that "the cybercriminal removed a copy of a subset of data from our self-hosted (private cloud) environment … we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed."[11]

Blackbaud's ransom payment was little consolation to the thousands of customers who stored sensitive data in the cloud, many of whom were required to conduct their own investigations—often at their own expense. Without direct access to evidence, however, their response was hampered. Within just a few months, Blackbaud had been sued in 23 proposed class-action lawsuits, received approximately 160 claims from customers and their attorneys, and been hit with inquiries from a plethora of government agencies and regulators.[12]

Opportunities for Detection

Customers typically have little visibility into the operations and risk management practices of suppliers, even those that have a high level of access to their sensitive data or network resources. They also have no way to directly detect an intrusion into supplier networks and must rely on suppliers to implement effective detection capabilities to prevent the spread of ransomware.

Visible signs of a supplier compromise may include the following:

- Unusual logins or activity from supplier accounts
- Spam emails originating from a supplier's address
- Unusually slow service or full outages
- Notification or media reports of a cybersecurity compromise relating to the supplier

3.3 Expansion

Once an adversary gains access to the target's technology resources, typically they engage in a recursive process in which they establish persistence, conduct reconnaissance, update their attack strategy, and broaden their access. These activities build off each other and often occur at the same time, rather than in a clear linear progression, as illustrated in Figure 3.2.

10. O'Ryan Johnson, "MSP at Center of Texas Ransomware Hit: 'We Take Care of Our Customers'," *Channel Program News*, September 17, 2019, www.crn.com/news/channel-programs/msp-at-center-of-texas-ransomware-hit-we-take-care-of-our-customers-.

11. "Security," Blackbaud, www.blackbaud.com/securityincident.

12. Sergui Gatlan, "Blackbaud Sued in 23 Class Action Lawsuits After Ransomware Attack," *Bleeping Computer*, November 3, 2020, www.bleepingcomputer.com/news/security/blackbaud-sued-in-23-class-action-lawsuits-after-ransomware-attack/.

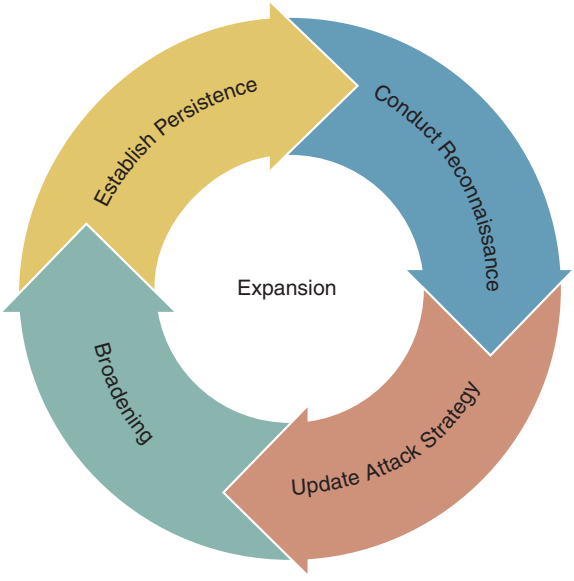


Figure 3.2 The "expansion" phase of a cyber extortion attack

Activities at this stage include the following steps:

- **Establish persistence:** The adversary works to establish sustained, reliable access over an extended period of time and evade detection. To accomplish this, the adversary may install remote access tools, neutralize antivirus software, add new accounts, and so on.
- **Conduct reconnaissance:** The adversary gathers information that will enable them to expand the scope of compromise. This may include network mapping, password cracking and interception, and more.
- **Update the attack strategy:** The adversary uses the information gleaned to refine their goals, plan, and processes.
- **Broadening:** The adversary increases their access to systems, accounts, or other network resources, by escalating privileges, moving laterally through the network, and gaining access to different applications and technology resources.

Along the way, all of the adversary's activities provide defenders with opportunities to detect and eradicate the threat. Each interaction generates unique and identifiable indicators that a security team can monitor to identify the threat.

In particular, during the early stages of an attack, the adversary is at their most vulnerable, since they are likely still unfamiliar with the network topography and may unwittingly create "noise" while engaging in network reconnaissance and other expansion activities.

The method of access and the adversary's skill set can also vary significantly, leading to variations in IoCs and detection strategy.

In the following sections, we describe specific indicators of compromise that can facilitate detection and enable defenders to break the chain of attack.

3.3.1 Persistence

Simply gaining access to a victim's network once is not usually sufficient to gain extensive leverage over a victim. Instead, the adversary must find a way to access resources on the victim's network repeatedly over a sustained period of time.

Frequently, the adversary lurks on the network for an extended period of time (even weeks or months) prior to gaining leverage (e.g., exfiltrating data, detonating ransomware). This means that the target has an opportunity to detect and eradicate the compromise before the worst occurs.

Opportunities for Detection

The specific indicators of compromise vary based on the method of access, but almost universally, the adversary needs to generate periodic network traffic. They often use a command-and-control server, otherwise known as a C2 server, in which an infected endpoint "phones home" to an adversary-controlled server. They may also use standard IT remote access tools such as RDP, Anydesk, or others.

Defenders should be on the lookout for telltale signs of suspicious network activity:

- Suspicious source/destination IP addresses and domains
- Network communication originating from unfamiliar or unexpected processes
- Malformed communications—for example, DNS requests with Base64 encoded content instead of normal URLs
- Unauthorized remote access attempts

3.3.2 Reconnaissance

Now that the adversary has established a consistent method of entering the environment, they will often perform information gathering tasks to better understand the network, its connected devices, and potential targets for further exploitation. The adversary can perform these activities using built-in system tools, third-party software, or both. The adversary will often look for the following items:

- Local IP address range information
- Available subnets
- Domain information

- Available network services
- DNS information

Using information gathered from the network, the adversary can effectively map the environment they now have access to and determine their best options for additional actions after the initial compromise. Additionally, because system administrators often include function descriptions in network computer names (i.e., Fileserver-01 or DC-01), the adversary can specifically target anything that they identify as a potentially high-impact target.

Often, indicators of network reconnaissance are observed during the early stages of an incident. This provides an opportunity to greatly reduce an adversary's ability to spread through the network or possibly stop it entirely.

Opportunities for Detection

The following indicators can signal potentially malicious network reconnaissance:

- Indicators of port scanning (NMAP)
- Increased network resource usage from suspicious computers
- Outbound network traffic spikes at irregular hours
- Increased outbound network traffic

3.3.3 Broadening

Once the initial foothold is secured, the adversary works to expand access to additional network resources, including high-value systems that hold confidential information or can be used to control resources. Along the way, the adversary will attempt to gain additional privileges, specifically targeting domain administrator privileges and administrative access to cloud tenants/applications. Typically, the adversary's activities include at least the following:

- **Privilege escalation:** The adversary attempts to gain a higher level of user privileges. In the early stages, this is often accomplished by scraping credentials from system memory using a tool such as Mimikatz, extracting saved passwords from web browsers, capturing Kerberos tokens, or simply searching the infected host for documented credentials. Once the adversary has moved laterally throughout the network, they may engage in more sophisticated privilege escalation attacks involving theft of private keys, Security Assertion Markup Language (SAML) token forgery, and more.
- **Lateral movement:** The adversary attempts to gain access to other hosts on the network by using stolen passwords, exploiting vulnerabilities, or applying other tactics. Commonly, this process is facilitated by the widespread practice of configuring a static local administrator password shared by all endpoints.

- **Application/cloud access:** The adversary accesses applications and cloud tenants, typically by using stolen passwords or leveraging trust relationships between local systems and services.

If an adversary is able to establish a significant breadth of access, it becomes much more difficult to fully eradicate the threat.

Opportunities for Detection

Common indicators of broadening or expanding access by adversaries include the following:

- Unusual Local Administrator account activities, including network authentications or shared folder access
- Connections to core assets from unusual or unauthorized workstations
- Suspicious application access
- Impossible travel alerts

3.4 Appraisal

Once inside a victim's environment, adversaries often explore and identify any valuable data. This can include information that is useful for the following purposes:

- **Applying pressure in extortion:** The adversary can use regulated data such as electronic protected health information (ePHI) or Social Security numbers to remind the victim of the potential for fines, regulatory investigation, or other government actions. In some cases, victims may store direct contact information for data subjects, whom adversaries can contact and attempt to intimidate.
- **Setting a ransom demand:** Financial details and cyber insurance coverage can inform the amount of the adversary's ransom demand.
- **Sale:** Intellectual property and personally identifiable information (PII) are valuable information that can be sold to third parties.

The adversary may update their attack strategy based on these findings. This may include determining whether to install ransomware, identifying information to exfiltrate, setting a ransom demand, and more.

Opportunities for Detection

Look for the following indicators that an adversary may be appraising your infrastructure (among others):

- Unexpected or unauthorized access to files. Typically this is identified using third-party security software or security information and event management (SIEM) conditional alerting.
- Last read/modified dates on files that are more recent than expected.
- Forwarded or copied emails containing information about insurance coverage, finances, and so on.

3.5 Priming

Prior to gaining leverage, the adversary will typically "prime" the environment to maximize the potential damage and impact. For example, before detonating ransomware, the adversary may modify key network configuration settings and disable antivirus software. These steps are intended to remove roadblocks and improve the chances of a successful detonation during the next stage of the attack.

Adversaries commonly modify and/or disable the following network components:

- Antivirus/security software
- Processes and applications
- Logging/monitoring systems
- Filesystem permissions and configuration

In the remainder of this section, we discuss each of these in turn.

3.5.1 Antivirus and Security Software

Security and antivirus software present hurdles for adversaries and can issue alerts during any phase in the compromise. Signature-based antivirus software may detect and delete the malicious files used by the adversary, or heuristic security software may detect the actions associated with file encryption and stop the process before it completes. As a result, neutralizing security software is often a top priority for the adversary. Typically, this will take the form of one or more of the following actions:

- **Disabling security software:** If the adversary is not worried about making too much noise on the network, a common tactic is to simply disable the active security software currently in use by the victim by killing the active process. This can prevent the

software itself from alerting, but it can also set off alerts within the victim's network notifying IT security personnel that something is wrong.

- **Modifying configuration:** In some cases, an adversary may gain access to the centralized console used to manage a security application. If the software allows for global changes, the adversary may modify the configuration so as to neutralize the software across the entire domain. For example, often the adversary will put the security software into a "monitor-only" mode, allowing the adversary to freely distribute malware without interference.
- **Allowlisting signatures:** An adversary with sufficient access may simply allowlist signatures associated with their specific malware in the victim's security software. Like service alteration, this type of change requires access to a central administration platform but will rarely generate an alert from the software itself. While not the most common method of evasion, signature exceptions can often be nearly invisible to the victim.

Opportunities for Detection

The following indicators suggest that security software on your network may be under attack:

- Alerts for nonresponsive antivirus software on endpoints
- State-change alerts from security software

3.5.2 Running Processes and Applications

Many software applications are designed to prevent other services from modifying open files or databases while they are in use, thereby minimizing the risk of corruption. This is especially common in software that maintains a database, such as a SQL server application or a financial application like QuickBooks. One unexpected silver lining is that these applications may inherently block ransomware from encrypting important databases and files if they are actively in use.

Opportunities for Detection

How can you recognize that an adversary may be actively compromising services and applications on your network? Look for the following indicators:

- System health indicators, which you can use to flag modifications of this type
- Signature identification of tools such as ProcessHacker

3.5.3 Logging and Monitoring Software

Event logging and monitoring software can enable victims to:

- Detect anomalous activity quickly and thwart the adversary
- Trace the adversary's activities through the network and close any security gaps
- Quickly eradicate the adversary from the network
- Gain information that could be leveraged in a negotiation

As a result, adversaries often take steps to undermine event logging and monitoring capabilities. Without accurate logging, activities including access times, filesystem exploration, indicators of exfiltration, and other valuable information may no longer be available. Many small and midsized organizations rely on local log files on the affected host, and do not have a central SIEM, which makes the adversary's job easier.

Often, adversaries will undermine event logging and monitoring using the following tactics:

- **Log deletion:** The adversary may delete key elements of the available log data to completely obscure local system activities. These sources of data commonly include Windows Event Log data, Link files, Jump lists, Windows Explorer history, web browser history, and more.
- **Stop services**: If a log collection service like Winlogbeat or Rsyslog is in use to centralize log collection, the adversary may simply kill the export service on the local system, effectively stopping the collection of data.
- **Time-stomping**: The adversary may alter timestamps on log data to make investigating the attack and correlating logs between multiple systems difficult, if not impossible. This may also be done to obscure the identification of files or programs used in the attack.

Opportunities for Detection

The following evidence suggests that logging and monitoring solutions have been tampered with:

- Event log data indicating that logs have been cleared (i.e., Event ID 1102 on a Windows host)
- Use of a specialized utility such as the Sysinternals SDelete tool to make deleted log recovery impossible
- Alerts for data stoppage from monitored hosts

3.5.4 Accounts and Permissions

To ensure an effective rollout of ransomware encryption software, the adversary typically adds at least one account and carefully modifies access permissions to ensure that the ransomware spreads as quickly and effectively as possible. Here are some specific, commonly used tactics:

- **Create new administrative user accounts:** By the time the adversary is in the "priming" phase, they usually already have domain administrator access. However, the adversary will typically create a different account to use for the ransomware deployment. This will make it more difficult for the victim to trace the attack back to the actual accounts that the adversary used prior to detonation.
- **Add the account to the "remote users" groups:** This gives the newly created user access to all endpoints that have remote access enabled.
- **Gain unauthorized network share access:** This enables the ransomware to encrypt shared drives and connected devices (including, much of the time, backups).
- **Perform unauthorized software installations:** The adversary uses common administrative tools (such as PsExec) to automate deployment of the ransomware.

Opportunities for Detection

Set up logging and automated alerts for the following indicators:

- New or unknown administrative user accounts
- Increases in remote connection activity or unusual accounts accessing remote services
- Unauthorized access to network shares
- Installation of unauthorized software

3.6 Leverage

To actually launch an extortion attack, the adversary first needs to gain leverage by actively threatening the confidentiality, integrity, and/or availability of information resources. Most commonly, adversaries accomplish this by encrypting files with ransomware, or stealing sensitive data so they can later threaten to publish it if they do not receive payment.

In this section, we discuss the two most common scenarios: ransomware detonation and data exfiltration. Keep in mind that these are only selected examples—there are many other ways for adversaries to gain leverage over a victim. Ultimately, adversaries are limited only by their imaginations.

3.6.1 Ransomware Detonation

The detonation phase represents the last piece of "hands-on" access that an adversary will normally execute. Once the adversary has mapped their targets, obtained sufficient access, and potentially exfiltrated everything they want, the final fireworks show at the end of the incident is the detonation of a ransomware executable. This phase of the attack is often the first indicator of compromise a victim sees directly and, unfortunately, at this point it is usually too late to prevent the attack.

An adversary can distribute and detonate their encryption software in many different ways. Here are three common methods:

- **Group policy:** An adversary with access to a domain controller and domain administrator credentials can use the software distribution system built into most Windows networks as a springboard to distribute their malicious software. This activity is typically accompanied by the creation of a scheduled task that can simultaneously detonate the ransomware payload on all computers within the victim's environment. This shortens the overall period in which a defender could stop the attack, and also makes investigating the attack more difficult because it can effectively obfuscate the origin of the malware execution.
- **System administration toolkit:** Adversaries are frequently observed using the PsExec toolkit or similar utilities to distribute their malicious payload. Configuring a network to accept this type of software push is trivial, and the previous expansion steps taken by the adversary usually provide them with exactly what they need to initiate this form of detonation. The PsExec utility is part of the Microsoft SysInternals toolkit and automates the process of distributing executable programs to domain-connected hosts.
- **Manual distribution and detonation:** In some cases, the adversary may choose to avoid automated distribution and simply install and execute the encryption software manually on selected targets within the overall network. This tactic is observed in both small networks with a minimal number of overall targets and large organizations. In the latter case, an adversary is more concerned with encrypting the "crown jewels" of the network than with encrypting every individual host.

Once the ransomware payload is detonated, the exact sequence of events varies depending on the strain. However, there are some common actions that the software typically executes:

- Adds malicious software to startup sequences, which facilitates persistence between reboots.
- Creates ransom notes.
- Deletes shadow volume copies, to prevent file restoration.
- Enumerates drives, often starting with drive A:\ and moving alphabetically through the hosts' mapped drives.

- Encrypts files. Most ransomware strains encrypt a targeted list of files, often based on a preloaded list of file extensions.
- Encrypts backup files once found on the network.

Opportunities for Detection

While some might seem obvious, here are the signs indicating that ransomware has been detonated on a network:

- Unauthorized software installations
- Unauthorized or unusual scheduled task creation
- Registry modification
- Visible ransom notes
- Encrypted files

3.6.2 Exfiltration

The adversary may deliberately exfiltrate data to use it as leverage in extortion, commit fraud, or sell it. This type of exfiltration is distinct from the network reconnaissance discussed in Section 3.2.3, in that the purpose is to gain some benefit beyond simply increasing access.

For example, the Conti playbook that was leaked in 2021 (discussed in Section 2.9.6) illustrated how adversaries now purposefully search for financial documents, accounting information, client data, and more.[13] The adversaries also seek out details that are specifically useful for negotiating extortion payments, such as cyber insurance policies. Today, this has become standard practice, and the exfiltration often occurs quickly and in bulk.

Adversaries could exfiltrate data from any repository, including systems on a local network, mobile device, or cloud repository. In today's cloud-driven technology landscape, sensitive data is often stored via Amazon S3, Dropbox, SharePoint, and other cloud-based storage systems. Adversaries often access the data held within the cloud using credentials and access keys obtained during their takeover of their victims' local network, and vice versa.

Because the adversary might transfer or sell access to the victim's technology environment at any point, it is entirely possible for a victim's data to be stolen multiple times by different adversaries.

Adversaries commonly use the following tools for exfiltrating data:

- **Mainstream cloud services:** The advantage of these services—which include Dropbox, Google, OneDrive, and others—is that they are often already supported by the local environment and can blend with normal usage.

13. Leaked Conti playbook, September 2021, translated from Russian to English using Microsoft and author research.

- **File transfer programs:** The adversary can use common Windows utilities such as WinSCOP or Powershell to send data to a server under their control. Typically the data is encrypted or encoded in transit.[14]
- **Anonymous file sharing services:** MEGA, FreeFileSync, and similar services are very convenient aids for adversaries, since they require little effort to set up and are free up to a certain volume of data. MEGA has become particularly popular. It includes built-in end-to-end encryption, making it difficult for data loss prevention systems to detect, and the user can transfer files using a web browser or desktop app. Since these services are not normally used in a standard enterprise environment, it can be easy to detect and block applications of this type.

Three data exfiltration patterns are commonly seen in cyber extortion cases:

- Automated RAT exfiltration
- Mass repository theft
- Curated theft

Each of these exfiltration patterns leaves a different footprint in the network and may require different response tactics. In the following subsections, we discuss each in turn.

3.6.2.1 Automated RAT Exfiltration

Quite often, a RAT installed on the victim's network is configured to automatically steal files and upload them to a system controlled by the adversary. When this occurs, the RAT typically has a configuration file that allows the operator to select files based on an extension and/or keywords in the filename. For example, the authors of this book studied one widely used RAT, Atmos, which shipped with a default configuration that exfiltrated all files with .pdf and .docx extensions, plus any documents containing the keywords "bank" or "payroll" in the filename. In this case, as in many others, the adversary's goal was likely to facilitate financial fraud.

Modern RATs are sophisticated and typically include built-in techniques to help the user avoid detection. When files are automatically exfiltrated, typically the data transfer is slowly metered so that it doesn't set off network monitoring alerts.

RATs typically transfer data over the built-in command-and-control channel, which is often encrypted, again for evasion purposes. Although the functionality of RATs varies, the data normally winds up on a server under the adversary's control—often another hacked server that is part of a botnet. Depending on the RAT's level of sophistication, the adversary may even have point-and-click access to view and sort stolen files through the RAT's interface.

14. Jeremy Kennelly, Kimberly Goody, and Joshua Shilko, "Navigating the MAZE: Tactics, Techniques and Procedures Associated with MAZE Ransomware Incidents," Mandiant (blog), May 7, 2020, www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html.

3.6.2.2 Mass Repository Theft

Today, "smash-and-grab" data exfiltration is a popular technique. Many adversaries enter the network with the goal of stealing data, and invest little time in curation before theft. Why bother sorting through the data while on the victim's network, when the adversary can steal it en masse and analyze it on their own systems?

In cyber extortion cases, typically there is no need to pick through data extensively to accomplish the adversary's objectives. Once the adversary has access to the victim's network, they seek out large data repositories and transfer them out in bulk. Then, during the negotiation phase, they can share screenshots of the stolen data or provide file lists. No matter if the bulk of the stolen files is unimportant; the presence of even a few documents containing PII can spell reputational disaster for the victim.

In some cases, bulk file transfer can cause significant headaches for the victim. Once the victim is aware that data may have been stolen, typically the next step is to take an inventory of the potentially exposed data and create a notification list. Firms that conduct e-discovery normally charge by the gigabyte, so even if the majority of the stolen files contain no sensitive data, the cost for verifying this fact may be large.

In some cases, the adversary "stages" data on a single system prior to exfiltration. This process gives the adversary time to organize files, ensure everything is compressed and encrypted, and then exfiltrate it all at once, giving the victim limited time to respond before all the data flies out the door. The Lockbit extortion gang was observed staging data and organizing files based on the system from which they were stolen, and then copying the directories to a single MEGA console before uploading them. However, quite often adversaries do not bother "staging" data at all, but simply copy it directly from the hacked systems.

As RaaS kits become more automated, adversaries are curating less and automatically exfiltrating data more. The Netwalker RaaS platform advertised "[a] fully automatic blog, into which the merged data of the victim goes, the data is published according to your settings."[15] The RaaS automatically exfiltrated the victim's data to MEGA, and then created a blog where the MEGA links would appear at the proper time.[16]

3.6.2.3 Curated Theft

In some cases, an adversary may steal only specific files of value, such as source code, databases of PII, or other material. To accomplish this, the adversary needs to first identify these files on the network, typically through manual examination. Often, content of this type is curated due to the size of the repository, or because the attack is targeted and the adversary has a predetermined goal in mind.

---

15. Jim Walter, "NetWalker Ransomware: No Respite, No English Required," Sentinel Labs, June 4, 2020, https://labs.sentinelone.com/netwalker-ransomware-no-respite-no-english-required/.

16. Lawrence Abrams, "Ransomware Recruits Affiliates with Huge Payouts, Automated Leaks," *Bleeping Computer*, May 15, 2020, www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/.

For example, the gaming company CD Projekt Red was hit with a ransomware attack in 2021, when adversaries specifically leveraged stolen source code in their ransom note. "We have dumped FULL copies of the source codes from your Perforce server for Cyberpunk 2077, Witcher 3, Gwent and the unreleased version of Witcher 3!!!"[17]

Due to the size of the source code repositories, and the fact that these were stored in the dedicated Perforce software, exfiltration of this material was undoubtedly purposeful and curated. The adversary also explained that they had stolen materials relating to accounting, human resources, and more, but specifically leveraged the intellectual property in their extortion efforts. "If we will not come to an agreement," they threatened, "then your source code will be sold or leaked online, and your documents will be sent to our contacts in gaming journalism."[18]

Opportunities for Detection

Signs of data exfiltration may include the following unexplained or unusual activities:

- Increases in network traffic, particularly outbound direction
- Connections to cloud file sharing services
- Use of MEGA and other third-party file sharing websites that are not typically used
- File movement and staging activities
- Connected sessions with unknown or suspicious destinations

3.7 Extortion

The final phase of a cyber extortion incident is often the loudest and most aggressive. The adversary has already taken the time to infect the network, compromise assets, exfiltrate data, and/or encrypt the filesystem, and now the adversary is looking to monetize the attack.

With the need for stealth gone, the adversary begins the process of extortion. The primary extortion notification methods typically include:

- Passive notification (i.e., the ransom note)
- Active notification (e.g., phone calls, voicemails)
- Third-party outreach (e.g., direct communications with customers, data subjects)
- Publication (e.g., dark web blogs, Telegram channels, Twitter feeds)

We discuss each of these tactics in turn in the following subsections.

17. Catalin Cimpanu, "CD Projekt Red Game Studio Discloses Ransomware Attack, Extortion Attempt," *ZDNet*, February 9, 2021, www.zdnet.com/article/cd-projekt-red-game-studio-discloses-ransomware-attack-extortion-attempt/.

18. Lily Hay Newman, "*Cyberpunk 2077* Maker Was Hit with a Ransomware Attack—and Won't Pay Up," *Wired*, February 9, 2021, www.wired.com/story/cd-projekt-red-ransomware-hack-cyberpunk-2077-source-code/.

3.7.1 Passive Notification

The adversary typically makes it obvious to the victim that they are being extorted. This can be, and often is, as simple as a ransom note left on the desktop. However, many adversaries have leveled up, and now include multimedia such as audio versions of the ransom demand.

The ransom note commonly includes the following information:

- An announcement of what happened
- Instructions for how to recover files
- A clear deadline (this may be a countdown timer or a simple deadline)
- Contact information for the adversary (typically an email address or link to a portal)
- Advice for obtaining cryptocurrency
- Psychological pressure, such as threats (e.g., "Your business is at serious risk."[19]) as well as reassurances (e.g., "But do not worry. You have a chance! It is easy to recover in a few steps."[20])

Figure 3.3 shows an example of a ransom note left by the Maze hacking group in 2020.[21]

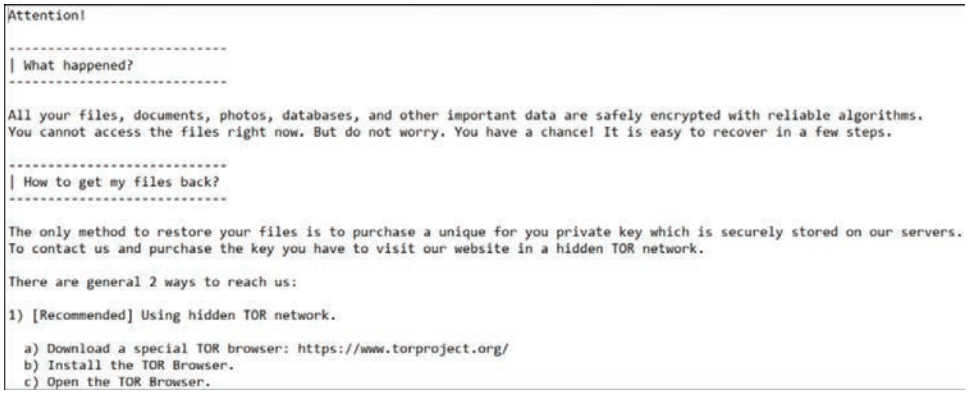


Figure 3.3 A sample Maze ransom note from the LMG Security malware lab

(Illustration courtesy of LMG Security)

19. Ryuk ransom note, https://blog.malwarebytes.com/wp-content/uploads/2019/12/ryuk-ransom-note-versions-600x415.png.
20. Alexandre Mundo, "Ransomware Maze," McAfee (blog), March 26, 2020, www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/.
21. Maze ransom note, LMG Laboratory, 2020.

3.7.2 Active Notification

The adversary might actively engage in communicating with the victim throughout the extortion phase. This commonly includes sending emails, but can also involve phone calls, text messages, voicemails, Telegram messages, and other methods. Typically, the aim is to intimidate the victim and demonstrate the adversary's level of access. In many cases, adversaries monitor the victim's emails and may even make snide comments on current response activities.

3.7.3 Third-Party Outreach

Adversaries have been known to reach out directly to third parties affected by the compromise, including customers, patients, data subjects, and business associates, to encourage them to pressure the victim organization into paying a ransom. In some cases, they may also reach out to competitors or others in an effort to sell stolen data.

As discussed in Section 2.7, The Dark Overlord (TDO) cyber extortion group hacked the Johnston Community School District Iowa in 2017 and texted threatening messages to parents. More recently, cyber extortion gangs have taken to leveraging scalable communications methods such as email so as to connect directly with data subjects and affiliates. For example, one convenience store chain that was extorted by the Clop ransomware gang discovered that its customers had received the following email notifying them of the compromise:[22]

> Good day!
>
> If you received this letter, you are a customer, buyer, partner or employee of [VICTIM-REDACTED]. The company has been hacked, data has been stolen and will soon be released as the company refuses to protect its peoples' data.
>
> We inform you that information about you will be published on the darknet (http://[redacted]) if the company does not contact us.
>
> Call or write to this store and ask to protect your privacy!!!!

3.7.4 Publication

Adversaries may publish extortion notification on dark web sites, Telegram channels,[23] social media platforms, and more, anticipating that victims will view their posts and receive pressure from third parties. In addition, adversaries routinely leverage the mainstream media, particularly when threatening to publish data, as discussed in Section 2.8.

---

22. Brian Krebs, "Ransom Gangs Emailing Victim Customers for Leverage," Krebs on Security, April 5, 2020, https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/.

23. Lily Hay Newman, "The Lapsus$ Hacking Group Is Off to a Chaotic Start," *Wired*, March 15, 2022, www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/.

3.8 Conclusion

In this chapter, we stepped through the anatomy of a cyber extortion attack, including each of its components: entry, expansion, appraisal, priming, leverage, and extortion. Along the way, we described the adversary's activities in depth, and provided indicators of compromise that can help responders identify these activities.

In the next chapter, we will discuss the initial response once an intrusion has metastasized into a cyber extortion attack.

3.9 Your Turn!

Every cyber extortion incident is unique. The response team's options and priorities will vary depending on the victim organization's industry, size, and location, as well as the details of the incident itself.

Based on what you learned in this chapter, let's think through key elements of a cyber extortion attack.

Step 1: Build Your Victim

Choose one characteristic from each of the three columns to describe your victim's organization:

Industry	Size	Location
Hospital	Large	Global
Financial institution	Midsized	United States
Manufacturer	Small	European Union
Law firm		Australia
University		India
Cloud service provider		Country/location of your choice
Organization of your choice		

Step 2: Choose Your Incident Scenario

Select from one of the following incident scenarios:

A	Ransomware strikes! All of the victim's files have been locked up, including central data repositories, servers, and workstations.
B	A well-known cyber extortion gang claims to have stolen all of the victim's most sensitive data and threatens to release it unless the victim pays a very large ransom demand. The gang posts the victim's name on their dark web leaks site, along with samples of supposedly stolen data.
C	Double extortion! Both A and B occur at the same time.
D	The victim is hit with a denial-of-service attack on their Internet-facing infrastructure that slows their access and services to a crawl. The adversary threatens to continue and even escalate the attack unless a ransom is paid.

Step 3: Discussion Time

Your victim organization has experienced a cyber extortion event. Given what you know about the victim and the scenario, answer the following questions:

1. Should the victim organization assume that the extortion demand was the adversaries' only activity relating to their environment? Why or why not?
2. Name the steps that adversaries often take in the leadup to cyber extortion.
3. Describe at least one way that the victim can often detect early signs of this type of attack prior to the extortion phase.
4. What are the most common methods of entry that the victim organization should check for?
5. Which means might the adversary use to try to notify the victim of the extortion demand?

This page intentionally left blank

Index