Ransomware & Cyber Extortion

RESPONSE AND PREVENTION

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

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."

—Tarah 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

Ransomware and Cyber Extortion: Response and Prevention

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Preface

Acknowledgments

About the Authors

Chapter 1 Impact

- 1.1 A Cyber Epidemic
- 1.2 What Is Cyber Extortion?
  - 1.2.1 CIA Triad
  - 1.2.2 Types of Cyber Extortion
  - 1.2.3 Multicomponent Extortion
- 1.3 Impacts of Modern Cyber Extortion
  - 1.3.1 Operational Disruption
  - 1.3.2 Financial Loss
  - 1.3.3 Reputational Damage
  - 1.3.4 Lawsuits
- 1.4 Victim Selection
  - 1.4.1 Opportunistic Attacks
  - 1.4.2 Targeted Attacks

Pearson

Table of Contents

1.4.3 Hybrid Attacks

1.5 Scaling Up

1.5.1 Managed Service Providers

1.5.2 Technology Manufacturers

1.5.3 Software Vulnerabilities

1.5.4 Cloud Providers

1.6 Conclusion

1.7 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 2 Evolution

2.1 Origin Story

2.2 Cryptoviral Extortion

2.3 Early Extortion Malware

2.4 Key Technological Advancements

2.4.1 Asymmetric Cryptography

2.4.2 Cryptocurrency

2.4.3 Onion Routing

2.5 Ransomware Goes Mainstream

2.6 Ransomware-as-a-Service

2.7 Exposure Extortion

2.8 Double Extortion

2.9 An Industrial Revolution

2.9.1 Specialized Roles

2.9.2 Paid Staff

2.9.3 Automated Extortion Portals

2.9.4 Franchising

Table of Contents

2.9.5 Public Relations Programs

2.9.6 Standardized Playbooks and Toolkits

2.10 Conclusion

2.11 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 3 Anatomy of an Attack

3.1 Anatomy Overview

3.2 Entry

3.2.1 Phishing

3.2.2 Remote Logon

3.2.3 Software Vulnerability

3.2.4 Technology Supplier Attack

3.3 Expansion

3.3.1 Persistence

3.3.2 Reconnaissance

3.3.3 Broadening

3.4 Appraisal

3.5 Priming

3.5.1 Antivirus and Security Software

3.5.2 Running Processes and Applications

3.5.3 Logging and Monitoring Software

3.5.4 Accounts and Permissions

3.6 Leverage

3.6.1 Ransomware Detonation

3.6.2 Exfiltration

3.7 Extortion

Table of Contents

3.7.1 Passive Notifcation

3.7.2 Active Notifcation

3.7.3 Third-Party Outreach

3.7.4 Publication

3.8 Conclusion

3.9 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 4 The Crisis Begins!

4.1 Cyber Extortion Is a Crisis

4.2 Detection

4.3 Who Should Be Involved?

4.4 Conduct Triage

4.4.1 Why Is Triage Important?

4.4.2 Example Triage Framework

4.4.3 Assess the Current State

4.4.4 Consider Recovery Objectives

4.4.5 Determine Next Steps

4.5 Assess Your Resources

4.5.1 Financial

4.5.2 Insurance

4.5.3 Evidence

4.5.4 Staff

4.5.5 Technology Resources

4.5.6 Documentation

4.6 Develop the Initial Response Strategy

4.6.1 Establish Goals

4.6.2 Create an Action Plan

Table of Contents

4.6.3 Assign Responsibilities

4.6.4 Estimate Timing, Work Effort, and Costs

4.7 Communicate

4.7.1 Response Team

4.7.2 Affected Parties

4.7.3 The Public

4.8 Conclusion

4.9 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 5 Containment

5.1 The Need for Speed

5.2 Gain Access to the Environment

5.3 Halting Encryption/Deletion

5.3.1 Change File Access Permissions

5.3.2 Remove Power

5.3.3 Kill the Malicious Processes

5.4 Disable Persistence Mechanisms

5.4.1 Monitoring Process

5.4.2 Scheduled Tasks

5.4.3 Automatic Startup

5.5 Halting Data Exfiltration

5.6 Resolve Denial-of-Service Attacks

5.7 Lock Out the Hackers

5.7.1 Remote Connection Services

5.7.2 Reset Passwords for Local and Cloud Accounts

5.7.3 Audit Accounts

Table of Contents

5.7.4 Multifactor Authentication
5.7.5 Restrict Perimeter Communications
5.7.6 Minimize Third-Party Access
5.7.7 Mitigate Risks of Compromised Software
5.8 Hunt for Threats
5.8.1 Methodology
5.8.2 Sources of Evidence for Threat Hunting
5.8.3 Tools and Techniques
5.8.4 Staffing
5.8.5 Results
5.9 Taking Stock
5.10 Conclusion
5.11 Your Turn!
Step 1: Build Your Victim
Step 2: Choose Your Incident Scenario
Step 3: Discussion Time
Chapter 6 Investigation
6.1 Research the Adversary
6.1.2 Actionable Intelligence
6.1.3 Identification Techniques
6.1.4 Malware Strains
6.1.5 Tactics, Techniques, and Procedures
6.2 Scoping
6.2.1 Questions to Answer
6.2.2 Process
6.2.3 Timing and Results
6.2.4 Deliverables
6.3 Breach Investigation or Not?

Table of Contents

6.3.1 Determine Legal, Regulatory, and Contractual Obligations

6.3.2 Decide Whether to Investigate Further

6.3.3 Moving Forward

6.3.4 Outcomes

6.4 Evidence Preservation

6.4.1 Sources of Evidence

6.4.2 Order of Volatility

6.4.3 Third-Party Evidence Preservation

6.4.4 Storing Preserved Evidence

6.5 Conclusion

6.6 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 7 Negotiation

7.1 Its a Business

7.2 Establish Negotiation Goals

7.2.1 Budget

7.2.2 Time Frame

7.2.3 Information Security

7.3 Outcomes

7.3.1 Purchasing a Decryptor

7.3.2 Preventing Publication or Sale of Data

7.4 Communication Methods

7.4.1 Email

7.4.2 Web Portal

7.4.3 Chat Application

7.5 Pressure Tactics

Table of Contents

7.6 Tone, Timeliness, and Trust

7.6.1 Tone

7.6.2 Timeliness

7.6.3 Trust

7.7 First Contact

7.7.1 Initial Outreach

7.7.2 Initial Response

7.8 Sharing Information

7.8.1 What Not to Share

7.8.2 What to Share

7.8.3 What to Hold Back for Later Use

7.9 Common Mistakes

7.10 Proof of Life

7.10.1 Goals and Limitations

7.10.2 Denial Extortion Cases

7.10.3 Exposure Extortion Cases

7.10.4 What If the Adversary Refuses to Provide Proof of Life?

7.11 Haggling

7.11.1 Discounts

7.11.2 Setting the Price

7.11.3 Making Your Counteroffer

7.11.4 Tradeoffs

7.12 Closing the Deal

7.12.1 How to Close the Deal

7.12.2 Changing Your Mind

7.12.3 After the Deal Is Closed

7.13 Conclusion

7.14 Your Turn!

Step 1: Build Your Victim

Table of Contents

Step 2: Choose Your Incident Scenario
Step 3: Discussion Time
Chapter 8 Payment
8.1 To Pay or Not to Pay?
8.1.1 Is Payment Even an Option?
8.1.2 The Argument Against Paying
8.1.3 The Argument for Paying
8.2 Forms of Payment
8.3 Prohibited Payments
8.3.1 Compliance
8.3.2 Exceptions
8.3.3 Mitigating Factors
8.4 Payment Intermediaries
8.5 Timing Issues
8.5.1 Funds Transfer Delays
8.5.2 Insurance Approval Process
8.5.3 Fluctuating Cryptocurrency Prices
8.6 After Payment
8.7 Conclusion
8.8 Your Turn!
Step 1: Build Your Victim
Step 2: Choose Your Incident Scenario
Step 3: Discussion Time
Chapter 9 Recovery
9.1 Back up Your Important Data
9.2 Build Your Recovery Environment
9.2.1 Network Segments
9.2.2 Network Devices

Table of Contents

9.3 Set up Monitoring and Logging

- 9.3.1 Goals of Monitoring
- 9.3.2 Timing
- 9.3.3 Components
- 9.3.4 Detection and Response Processes

9.4 Establish Your Process for Restoring Individual Computers

9.5 Restore Based on an Order of Operations

- 9.5.1 Domain Controllers
- 9.5.2 High-Value Servers
- 9.5.3 Network Architecture
- 9.5.4 Workstations

9.6 Restoring Data

- 9.6.1 Transferring Data
- 9.6.2 Restoring from Backups
- 9.6.3 Current Production Systems
- 9.6.4 Re-creating Data

9.7 Decryption

- 9.7.1 Overview of the Decryption Process
- 9.7.2 Types of Decryption Tools
- 9.7.3 Risks of Decryption Tools
- 9.7.4 Test the Decryptor
- 9.7.5 Decrypt!
- 9.7.6 Verify Integrity
- 9.7.7 Check for Malware
- 9.7.8 Transfer Data to the Production Network

9.8 Its Not Over

9.9 Adapt

9.10 Conclusion

9.11 Your Turn!

Table of Contents

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Chapter 10 Prevention

10.1 Running an Effective Cybersecurity Program

10.1.1 Know What Youre Trying to Protect

10.1.2 Understand Your Obligations

10.1.3 Manage Your Risk

10.1.4 Monitor Your Risk

10.2 Preventing Entry

10.2.1 Phishing Defenses

10.2.3 Secure Remote Access Solutions

10.2.2 Strong Authentication

10.2.4 Patch Management

10.3 Detecting and Blocking Threats

10.3.1 Endpoint Detection and Response

10.3.2 Network Detection and Response

10.3.3 Threat Hunting

10.3.4 Continuous Monitoring Processes

10.4 Operational Resilience

10.4.1 Business Continuity Plan

10.4.2 Disaster Recovery

10.4.3 Backups

10.5 Reducing Risk of Data Theft

10.5.1 Data Reduction

10.5.2 Data-Loss Prevention Systems

10.6 Solving the Cyber Extortion Problem

10.6.1 Get Visibility

10.6.2 Incentivize Detection and Monitoring

Table of Contents

10.6.3 Encourage Proactive Solutions

10.6.4 Reduce Adversaries Leverage

10.6.5 Increase Risk for the Adversary

10.6.6 Decrease Adversary Revenue

10.7 Conclusion

10.8 Your Turn!

Step 1: Build Your Victim

Step 2: Choose Your Incident Scenario

Step 3: Discussion Time

Afterword

Checklist A Cyber Extortion Response

Checklist B Resources to Create in Advance

Checklist C Planning Your Response

Checklist D Running an Effective Cybersecurity Program

Index