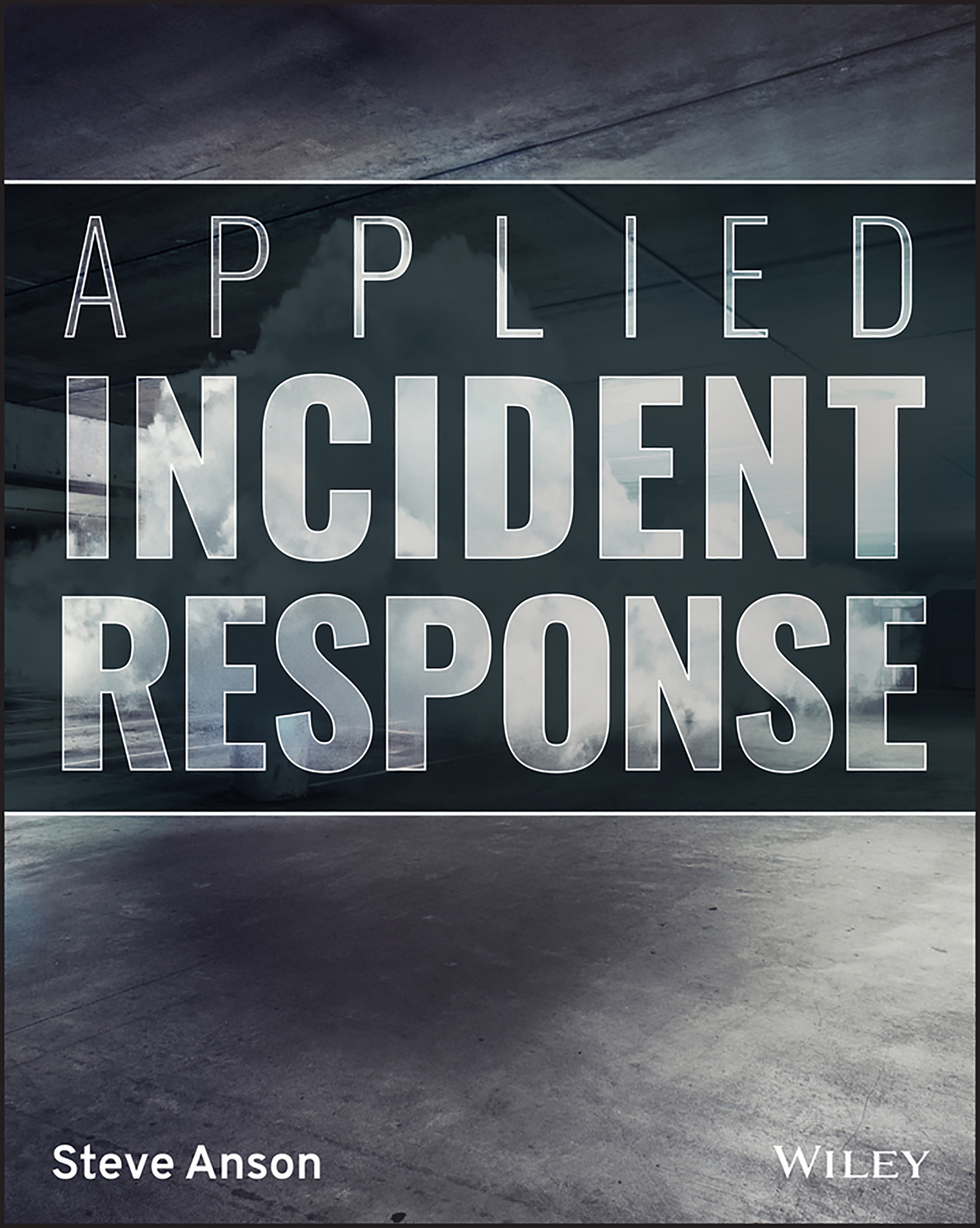

# APPLIED INCIDENT RESPONSE

Steve Anson

WILEY

# Applied Incident Response

# Applied Incident Response

Steve Anson

WILEY

Published simultaneously in Canada

ISBN: 978-1-119-56026-5
ISBN: 978-1-119-56028-9 (ebk)
ISBN: 978-1-119-56031-9 (ebk)

Manufactured in the United States of America

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at `http://booksupport.wiley.com`. For more information about Wiley products, visit `www.wiley.com`.

**Library of Congress Control Number:** 2019954524

# Contents at a Glance

# Contents

*This book is dedicated to the community of IT security professionals who innovate, create, and inform through blogs, open-source software, and social media. The techniques outlined in this book are only possible due to your tireless efforts.*

# Preface

Incident response requires a working knowledge of many different specialties. A good incident handler needs to be proficient in log analysis, memory forensics, disk forensics, malware analysis, network security monitoring, scripting, and command-line kung fu. It is an amazingly difficult task and one that requires constant training across a range of disciplines. That's where this book comes in. In between these covers (or in this digital file), you will find the distilled essence of each of these specialized areas. Whether you are an IT professional looking to broaden your understanding of incident response, a student learning the ropes for the first time, or a hardened veteran of the cyber trenches in search of a quick reference guide, this book has you covered.

This work is not focused on high-level theory, management approaches, or global policy challenges. It is written by and for hands-on practitioners who need to detect, deter, and respond to adversarial actions within their networks on a daily basis. Drawing on experience performing intrusion investigations for the Federal Bureau of Investigation (FBI) and U.S. Department of Defense, consulting for global clients, developing digital forensics and cyber investigative capabilities for dozens of national police forces, and working with students in hundreds of courses delivered for the U.S. State Department, the FBI Academy, and SANS, I have attempted to provide the most effective and actionable techniques possible for addressing modern cyber adversaries. I have also sought out the opinions, guidance, reviews, and input of many experts (who are far smarter than I am) in the various specialties presented in this book to ensure that the most current and relevant techniques are accurately presented. The end result may bear the name of a single author, but it is truly a collective work. As a result, I will use the plural "we" for first-person interjections to bear witness to the many practitioners and editors who helped make this work possible.

This book is in many ways a follow-up to *Mastering Windows Network Forensics and Investigation*, 2nd Edition (Sybex, 2012). While that book still contains many useful techniques for dealing with incidents more than 10 years since the release of its first edition, a great deal has changed since it was initially conceived. Threat actors are more advanced; breaches occur at a faster pace; the tactics, techniques, and procedures (TTPs) used by organized criminals and nation-state actors have merged; and code from each attack campaign is routinely reused by other threat actors. The days of pulling massive numbers of hard drives for static imaging and performing full forensic analysis of each have given way to performing targeted forensic examinations, searching live RAM across thousands of systems for injected malware, interrogating systems through scripts for indicators of compromise, and using data visualization techniques to detect malicious lateral movement among seemingly countless legitimate events. Modern threats require a different and more dynamic approach, and that is what you will find here: effective techniques for incident response that you can immediately apply in your environment.

## What We Will Cover

This book approaches incident response as a cycle rather than a stand-alone process. While we will cover several different incident response models, to achieve cyber resiliency, incident handling must feed into an overall cycle of prevention, detection, and response. Networks can no longer rely solely on preventive security defenses, viewing incident handling as an isolated and discreet activity. Instead, incident response must be an ongoing part of active defensive operations, feeding intelligence and information to network defenders to not only respond to current threats but to help mitigate future ones. We will cover a range of technical skills needed to achieve this objective over the following chapters:

Part I: Prepare

Chapter 1—"The Threat Landscape": Over the last decade, offensive cyber operations have become a leading source of revenue for organized crime, a key method of nation-state espionage, and an emerging weapon of war. Understanding modern adversaries and their attack vectors is a key step to effectively defending a network.

Chapter 2—"Incident Readiness": If you are not prepared for battle, the war is over before it even begins. This chapter provides you with the tools necessary to prepare your network, your team, and your process for effective incident response.

Part II: Respond

Chapter 3—"Remote Triage": Incidents can rapidly evolve from a single beachhead system to total domain domination. In order to properly scope and respond to an incident, you need the ability to triage systems, assess the impact of the incident, and identify impacted systems throughout the enterprise. This chapter arms you with the knowledge necessary to seek out evil in your environment.

Chapter 4—"Remote Triage Tools": Building on the knowledge gained in Chapter 3, this chapter provides you with specific techniques and tools to interrogate systems throughout the network, identify those that may be compromised, and initiate containment and mitigation steps.

Chapter 5—"Acquiring Memory": Once a system is identified as potentially compromised, the next logical step for an incident handler is to capture the contents of volatile memory from the system. This chapter explores various methods and tools to capture memory from local or remote systems in a forensically sound manner.

Chapter 6—"Disk Imaging": In addition to volatile data, forensic imaging of nonvolatile storage devices such as hard disks and solid-state disks may be necessary to preserve evidence and facilitate analysis of a compromised system. This chapter provides tools and techniques to obtain a forensic image from local and remote systems.

Chapter 7—"Network Security Monitoring": Monitoring and analyzing network communications provides critical visibility and information to incident responders. This chapter looks at telemetry gathered from the network to aid in the incident response process and ways to fuse that information with endpoint data to achieve a more complete picture of network activity.

Chapter 8—"Event Log Analysis": Windows event logs record granular details of system activity throughout a Windows environment. By aggregating and analyzing these logs, incident responders can reconstruct attacker activity. This chapter teaches you the skills necessary to understand and interpret this vital piece of evidence.

Chapter 9—"Memory Analysis": Modern attackers increasingly avoid making changes to disk as a mechanism of evading detection, making volatile memory an important battlefield. Whether analyzing a previously collected RAM dump or the volatile memory from a running system, being able to parse data structures in RAM to understand the details of system activity is a key skill for any incident handler.

Chapter 10—"Malware Analysis": Even with the rise of "living off the land" techniques, malware remains an important tool in the attacker's toolbox. This chapter gives you practical skills you can use to analyze suspected malware with both static and dynamic approaches.

Chapter 11—"Disk Forensics": Analysis of nonvolatile storage from impacted systems can identify indicators of compromise, uncover TTPs of your adversary, and document the impact of the intrusion. This chapter provides you with the skills needed to do a deep-dive analysis of an impacted system in a forensically sound manner.

Chapter 12—"Lateral Movement Analysis": Many intrusions begin with a client-side attack followed by lateral movement. We combine the skills learned in previous chapters and apply them to identifying lateral movement within your environment. This chapter explains the techniques used by adversaries to spread throughout an environment and the steps you can take as an incident handler to counter them.

Part III: Refine

Chapter 13—"Continuous Improvement": Once a suspected incident is effectively mitigated, the information gained during the incident response needs to feed back into the overall organizational defensive posture. Understanding controls, telemetry, procedures, and training that can help mitigate future incidents helps harden your environment for the next attack.

Chapter 14—"Proactive Activities": Incident response should not be purely reactive. Your team should actively engage in threat hunting, purple team exercises, and adversary emulation to identify potential intruders, blind spots, and gaps in your defensive posture. This chapter discusses ways to ensure that your team continuously strives to outwit the adversary.

## How to Use This Book

The best way to approach this book depends on your current skill level. We assume a basic knowledge in networking, so if you are not yet familiar with core networking concepts such as ports, protocols, and IP addresses, this may not be the best place to start your journey into incident response.

If you are a student looking to build on foundational IT knowledge and embark on the next leg of your journey into IT security, then welcome! Working through each section either as part of a course or on your own will provide you with a detailed overview of the field and give you the opportunity to identify the facets of incident response that most appeal to you for further study.

IT administrators seeking to better defend their networks are also part of the intended audience. Network defense requirements have shifted away from purely preventive approaches to a combination of prevention, detection, and response. Today's adversaries are dedicated and capable, and with enough effort, they can breach any network. Administrators need to know how to recognize, contain, and respond to incidents that may occur within their environment. Learning core incident response skills will help IT practitioners better secure and defend their networks to protect operations. Skim the whole book and focus on the areas of greatest interest to you, knowing that the rest of it will be there to help you deepen your understanding when you are ready.

If you are already an incident response professional, you know the challenge of trying to keep track of all the various skills needed to do your job. For you, we offer the ability to catch up on the latest techniques, hone your skills in areas where you may not be as comfortable, and provide a valuable reference to quickly look up the event ID, registry key, PowerShell cmdlet, or other technical detail needed to address your current challenge. You will likely pick up several useful tips and tricks along the way to make you a more efficient and effective incident handler.

Regardless of your starting point, you will find additional online references located at `www.AppliedIncidentResponse.com`, this book's official website. We will continue to update the site with new techniques and updates related to the topics covered here to ensure that you have access to current information.

We use several different formatting conventions throughout the book:

- Commands are set in `monospace` font.
- Commands that are to be typed by the user (as opposed to prompts or output) are in **`bold monospace`**.
- Context-variable command input (such as IP addresses) are in *`monospace italics`* or `<monospace in angle brackets>`.
- If a command is too long to fit a on a single line in print, we will use a ↵ to show that the line continues.

## Building a Test Lab

One of the best ways to learn any IT-related subject is to build a test environment and practice, and incident response is no exception. We will provide you with a wide range of commands, tools, and techniques as we proceed, and having a test lab where you can experiment in a hands-on fashion is invaluable for being able to apply these skills in your production environment. To facilitate this, we will provide some tips (and a script) to help you quickly get a test domain up and running.

First, you will need to pick your virtualization platform. VMWare is a popular and reliable choice. If you need to run your test environment on top of an existing host OS, then the free VMWare Workstation Player (`www.vmware.com/products/workstation-player.html`) may be an option for you. If you can spare a separate partition or separate bare-metal system, then VMWare ESXi (`www.vmware.com/products/esxi-and-esx.html`) provides a free platform and the benefit of working with a product that is implemented in many production environments. Of course, if you prefer HyperV or other (perhaps open-source) virtualization products, those will also work perfectly well.

The next step is to identify the operating systems that you would like to include in your test environment. Microsoft offers free trial licenses of many of its products with a EULA that permits evaluation for testing. For server products, you will find the licenses and downloads at `www.microsoft.com/en-us/evalcenter/evaluate-windows-server`, and for the client systems, you can find downloads available at `developer.microsoft.com/en-us/microsoft-edge/tools/vms`. You can also find a wide range of Linux/UNIX (referred to as "*nix" throughout this book) distributions freely available. Many of these such as Security Onion, the SANS Investigative Forensics Toolkit (SIFT), and Sumuri's Paladin are focused on providing security and forensics capabilities that rival or exceed those of commercial products. We will explore each of these in the coming chapters.

After you obtain your virtualization software and test operating systems, you will need to configure them into a suitable test domain. We provide a PowerShell script on the `www.AppliedIncidentResponse.com` website to help you create the same environment that we use throughout this book, complete with user accounts and groups.

# About the Author

**Steve Anson** is a former U.S. federal agent with experience working all manners of cyber-related cases for an FBI Cybercrime Task Force and the U.S. Department of Defense Criminal Investigative Service. Steve taught computer intrusion investigation at the FBI Academy and works with national police agencies around the globe as a contractor with the U.S. Department of State's Antiterrorism Assistance Program, where he helps develop sustainable organizational capabilities in digital forensics and cyber investigations. As co-founder of leading IT security company Forward Defense (`www.forwarddefense.com`), he provides security consulting services to government and private sector clients around the world. Steve is a Certified Instructor with the SANS Institute, teaching courses on securing and defending network environments.

## About Other Contributors

Several other contributors have reviewed and provided advice to make this book possible. At the top of that list is **Technical Editor Mick Douglas**. Mick is the founder of Infosec Innovations and a SANS Certified Instructor who generously provided in-depth technical editing of every page. He spent countless hours working with the author to refine the technical information presented in this book, ensure its accuracy, and suggest topics for inclusion in the final work. Mick's contributions can be felt in every chapter as he suggested tools and techniques to enhance the information provided every step of the way.

**Mary Ellen Schutz**, **Jeff Parker**, and the rest of the Wiley editing team did a great job of ensuring that the final product met the high standards set by Wiley. **Nicole Zoeller** likewise lent her quality management skills to the project, reviewing each chapter before it went to print. In addition to the core team, individual chapters were also reviewed by some of the foremost authorities in the various specialties covered. These experts took the time to review and suggest changes to chapters in their specialties to ensure that the book contains the most current and applicable topics.

Chapter 2 was reviewed by **Michael Murr**, an experienced incident handler, researcher, and developer who has worked in a variety of sensitive environments. The co-author of the SANS "SEC504: Hacker Techniques, Exploits, and Incident Handling" class, Mike provided valuable insight into this chapter on preparing for an incident.

**Alissa Torres**, the lead author of the SANS "FOR526: Memory Forensics In-Depth" course, and **Anurag Khanna** (@khannaanurag) both provided suggestions for topics and tips to include in the memory forensics chapters (Chapters 5 and 9).

Chapter 7 on network security monitoring was reviewed and improved by **John Hubbard**. John is a former SOC Lead for GlaxoSmithKline, with years of experience defending networks against advanced adversaries. He is the author of the SANS "SEC450: Blue Team Fundamentals" and the "SEC455: SIEM Design and Implementation" courses.

Chapter 11 on disk forensics benefited greatly from review and suggestions from **Eric Zimmerman**. Eric is a former special agent with the FBI who now serves as senior director for Kroll's cybersecurity and investigations practice. Eric teaches several SANS forensics courses as a Certified Instructor and is the co-author of the SANS "FOR498: Battlefield Forensics & Data Acquisition" course.

Chapter 12 on lateral movements techniques was reviewed by **Tim Medin**, the founder of Red Siege (`www.redsiege.com`), the man who discovered Kerberoasting, and the lead author of the SANS "SEC560: Network Penetration Testing and Ethical Hacking" course. Tim's extensive experience in offensive cybersecurity helped ensure that the techniques discussed were those you will most likely see should an intrusion occur in your environment.

Chapter 13 was reviewed by **Erik Van Buggenhout**, the lead author of the SANS "SEC599: Defeating Advanced Adversaries" course. Erik also suggested many other topics that are covered throughout the book on preventing, detecting, and defeating cyber adversaries.

Each of these contributors made significant improvements to this book, and leveraging their individual areas of expertise ensured that the final product provides you with the most valuable topics and technical details. We hope that it will help you improve the defensive stance of your network now and into the future.

Finally, the author would like to thank his parents, for providing the opportunities and assistance that made everything that followed possible.

# Part I

# Prepare

## In This Part

CHAPTER 1

# The Threat Landscape

Before we delve into the details of incident response, it is worth understanding the motivations and methods of various threat actors. Gone are the days when organizations could hope to live in obscurity on the Internet, believing that the data they held was not worth the time and resources for an attacker to exploit. The unfortunate reality is that all organizations are subject to being swept up in the large number of organized, wide-scale attack campaigns. Nation-states seek to acquire intelligence, position themselves within supply chains, or maintain target profiles for future activity. Organized crime groups seek to make money through fraud, ransom, extortion, or other means. So no system is too small to be a viable target. Understanding the motivations and methods of attackers helps network defenders prepare for and respond to the inevitable IT security incident.

## Attacker Motivations

Attackers may be motivated by many factors, and as an incident responder you'll rarely know the motivation at the beginning of an incident and possibly never determine the true motivation behind an attack. Attribution of an attack is difficult at best and often impossible. Although threat intelligence provides vital clues by cataloging tactics, techniques, procedures and tools of various threat actor groups, the very fact that these pieces of intelligence exist creates the real possibility of false flags, counterintelligence, and disinformation being used by attackers to obscure their origins and point blame in another direction. Attributing each attack to a specific group may not be possible, but understanding the general motivations of attackers can help incident responders predict attacker behavior, counter offensive operations, and lead to a more successful incident response.

Broadly speaking, the most common motivations for an attacker are intelligence (espionage), financial gain, or disruption. Attackers try to access information to benefit from that information financially or otherwise, or they seek to do damage to information systems and the people or facilities that rely on those systems. We'll explore various motives for cyberattacks in order to better understand the mindset of your potential adversaries.

## Intellectual Property Theft

Most organizations rely on some information to differentiate them from their competitors. This information can take many forms, including secret recipes, proprietary technologies, or any other knowledge that provides an advantage to the organization. Whenever information is of value, it makes an excellent target for cyberattacks. Theft of intellectual property can be an end unto itself if the attacker, such as a nation-state or industry competitor, is able to directly apply this knowledge to its benefit. Alternatively, the attacker may sell this information or extort money from the victim to refrain from distributing the information once it is in their possession.

## Supply Chain Attack

Most organizations rely on a network of partners, including suppliers and customers, to achieve their stated objectives. With so much interconnectivity, attackers have found that is often easier to go after the supply chain of the ultimate target rather than attack the target systems head on. For example, attacking a software company to embed malicious code into products that are then used by other organizations provides an effective mechanism to embed the attacker's malware in a way that it appears to come from a trusted source. The NotPetya attack compromised a legitimate accounting software company, used the software's update feature to push data-destroying malware to customer systems, and reportedly caused more than $10 billion in damages. Another way to attack the supply chain is to attack operations technology systems of manufacturing facilities that could result in the creation of parts that are out of specification. When those parts are then shipped to military or other sensitive industries, they can cause catastrophic failures.

## Financial Fraud

One of the earliest motivations for organized cyberattacks, financial fraud is still a common motivator of threat actors today, and many different approaches can be taken to achieve direct financial gain. Theft of credit card information, phishing of online banking credentials, and compromise of banking systems, including ATM and SWIFT consoles, are all examples of methods that continue to be used successfully to line the pockets of attackers. Although user awareness and increased bank responsiveness have made these types of attacks more difficult than in previous years, financial fraud continues to be a common motivation of threat actors.

## Extortion

We briefly mentioned extortion in our discussion of intellectual property theft, but the category of extortion is much broader. Any information that can be harmful or embarrassing to a potential victim is a suitable candidate for an extortion scheme. Common examples include use of personal or intimate pictures, often obtained through remote access Trojans or duplicitous online interactions, to extort money from victims in schemes frequently referred to as "sextortion." Additionally, damage or the threat of damage to information systems can be used to extort money from victims, as is done in ransomware attacks and with distributed denial-of-service (DDoS) attacks against online businesses. When faced with the catastrophic financial loss associated with being taken off line or being denied access to business-critical information, many victims choose to pay the attackers rather than suffer the effects of the attack.

## Espionage

Whether done to benefit a nation or a company, espionage is an increasingly common motivation for cyberattacks. The information targeted may be intellectual property as previously discussed, or it may be broader types of information, which can provide a competitive or strategic advantage to the attacker. Nation-states routinely engage in cyber-espionage against one another, maintaining target profiles of critical systems around the globe that can be leveraged for information or potentially attacked to cause disruption if needed. Companies, with or without the support of nation-state actors, continue to use cyber-exploitation as a mechanism to obtain details related to proprietary technologies, manufacturing methods, customer data, or other information that allows them to more effectively compete within the marketplace. Insider threats, such as disgruntled employees, often steal internal information with the intent of selling it to competitors or using it to give them an advantage when seeking new employment.

## Power

As militaries increasingly move into the cyber domain, the ability to leverage cyber power in conjunction with kinetic or physical warfare is an important strategy for nation-states. The ability to disrupt communications and other critical infrastructure through cyber network attacks rather than prolonged bombing or other military activity has the advantages of being more efficient and reducing collateral damage. Additionally, the threat of being able to cause catastrophic damage to critical infrastructure, such as electric grids, that would cause civil unrest and economic harm to a nation is seen as having the potential to act as a deterrent to overt hostilities. As more countries stand up military cyber units, the risk of these attacks becomes increasingly present. As Estonia, Ukraine, and others can attest, these types of attacks are not theoretical and can be very damaging.

### Hacktivism

Many groups view attacks on information systems as a legitimate means of protest, similar to marches or sit-ins. Defacement of websites to express political views, DDoS attacks to take organizations off line, and cyberattacks designed to locate and publicize information to incriminate those perceived to have committed objectionable acts are all methods used by individuals or groups seeking to draw attention to specific causes. Whether or not an individual agrees with the right to use cyberattacks as a means of protest, the impact of these types of attacks is undeniable and continues to be a threat against which organizations must defend.

### Revenge

Sometimes an attacker's motivation is as simple as wishing to do harm to an individual or organization. Disgruntled employees, former employees, dissatisfied customers, citizens of other nations, or former acquaintances all have the potential to feel as if they have been wronged by a group and seek retribution through cyberattacks. Many times, the attacker will have inside knowledge of processes or systems used by the victim organization that can be used to increase the effectiveness of such an attack. Open source information will often be available through social media or other outlets where the attacker has expressed his or her dissatisfaction with the organization in advance of or after an attack, with some attackers publicly claiming responsibility so that the victim will know the reason and source of the attack.

## Attack Methods

Cyber attackers employ a multitude of methods, and we'll cover some of the general categories here and discuss specific techniques throughout the remaining chapters. Many of these categories overlap, but having a basic understanding of these methods will help incident responders recognize and deter attacks.