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

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/.

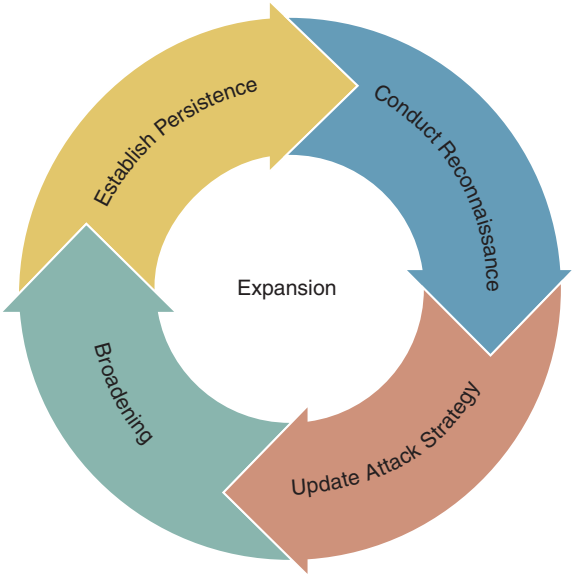

Figure 3.2 The "expansion" phase of a cyber extortion attack

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