Surviving Ransomware—What You Need to Know

Ransomware attacks have dominated recent headlines in a seemingly endless parade of compromises in numerous sectors. From Trojan.Gpcoder, the first modern ransomware exploit to use a spam email attachment, to high-profile hits on Colonial Pipeline (one of the largest US pipeline operators) and JBS Foods (the world's largest meat processing company), it's becoming clear that security practitioners are up against formidable foes.

Ransomware was first recognized around 2005, primarily because online payment systems weren't so readily available before then. Early victim targets were sent ransom demand messages via SMS (short message service) as nascent attack methodologies leveraging telecommunications began to evolve. It wasn't until 2008 when Bitcoin arrived on the scene—officially launching in January 2009—with the ability to (largely) anonymize transactions, making them hard to trace.

Table 1: Ransomware: Then & Now

	Infiltration	Post-Exploit Activity	Impacted Entities	Ransoms
Then	• Remote Desktop Protocol (RDP) • Phishing emails	• Short dwell times • Unsophisticated recon and privilege escalation	• Individuals • Smaller organizations <100 endpoints • Lots of healthcare orgs • Small practitioner shops	• Small, often less than a couple of bitcoins (1 bitcoin = $13,620.00 US)
Now	Still RDP and phishing CVE points of entry: • Recent load balancer vulnerabilities • General web framework vulnerabilities	Still see some of the older TTPs, but also: • PowerShell-based framework • RATs • Bloodhound • Dridex, Emotet, Trickbot • Deletion of backups	• Companies of all sizes • No company or org is immune	• Hundreds of thousands, sometimes millions of dollars • The average ransomware payment climbed 82% since 2020 to a record $570,000 US in the first half of 2021[1] • Prices often set based on recon by the threat actors into suspected business worth

Ransomware 101: The Basics

Ransomware is a criminal business model that uses malicious software to cryptographically hold data hostage, locking and encrypting a system while demanding a ransom payment in exchange for restoring access. While an increasingly urgent challenge, ransomware can be prevented—or at least damage can be minimized—through proper training, specific tunings in your current IT environment, and deploying advanced endpoint technology, including adding solutions such as extended detection and response (XDR) to your security stack.

Ransomware can be divided into two basic types: *crypto-ransomware*, the most common, which encrypts files and data, and *locker ransomware*, which locks the computer or other device, preventing the victims from using it.

Locker ransomware only locks the device, while the data stored on the device is typically untouched. As a result, if the malware is removed, the data is untouched. Even if the malware cannot be easily removed, the data can often be recovered by moving the storage device, typically a hard drive, to another functioning computer.

Crypto-ransomware, on the other hand, encrypts the data, so even if the malware is removed from the device or the storage media is moved to another device, the data is not accessible. Typically, crypto-ransomware does not target critical system files, enabling the device to continue to function despite being infected—after all, the device could be needed to pay the ransom.[2]

Most ransomware attacks consist of the following steps unless the attack is mitigated, or the victim refuses to pay the ransom:

1. **Compromise and take control of the system.** Most attacks begin with spear-phishing, tricking a user with a fraudulent email to open an infected attachment that compromises the system. This may impact a single host, such as a computer or mobile device. Then the compromised host will establish communications to a command-and-control server. The attacker might, at that point, move laterally from the initial host to other systems in the organization to maximize the impact of the ransomware attack.
2. **Prevent access to the system.** Once the system is infected, an attacker either identifies and encrypts certain file types likely to be of value to the victim, such as business documents like .doc, .xls and .pdf, or totally denies access to the entire system through lockout screens or scare tactics.

[1] Tao Yan et al., *Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228)*, Unit 42, December 28, 2021, https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/.

[2] Ronny Richardson and Max M. North, *Ransomware: Evolution, Mitigation and Prevention*, Kennesaw State University, January 1, 2017, https://digitalcommons.kennesaw.edu/facpubs/4276.

3. **Alert the owner of the device about the compromise, ransom amount, and steps to be taken.** The attacker must notify victims of the ransomware attack, often by providing a ransom note with payment instructions and additional steps to unlock their devices.
4. **Accept ransom payment.** An attacker must have a way to receive ransom payments while evading law enforcement, which explains the use of anonymous cryptocurrencies such as bitcoin for these transactions.
5. **Promise to return full access upon payment receipt.** Failure to restore compromised systems will destroy the scheme's effectiveness, as no one pays a ransom without confidence that their valuables will be returned.

Common Attack Methods

In order to better prevent ransomware, it is critical to understand the tactics attackers use to deliver this threat. There are multiple ransomware variants in use across multiple attack vectors, including through the network, SaaS-based applications and directly to the endpoint. This information will enable you to focus your security controls on the areas most likely to be leveraged and reduce the risk of infection.

Malicious Email Attachments

Historically, with malicious email attachments, the attacker would craft an email, likely from a believable source, such as human resources or IT, and attach a malicious file, such as a portable executable (PE) file, a Word document, or a .JS file. The recipient opens the attachment thinking the email has been sent from a trusted source. Once the file is opened, the ransomware payload is unknowingly downloaded, the system is infected, and the files are held for ransom. Today, malware infections give access to attackers who later deploy ransomware.

Malicious Email Links

Similar to malicious email attachments, malicious email links are URLs in the body of the email. Likewise, these emails are sent from someone or some organization that you believe to be a trusted source. When clicked, these URLs download malicious files over the web, the system is infected, and the files are held for ransom.

Vulnerable Credentials

Ransomware operators may also buy credentials from Initial Access Brokers (IABs) to avoid the whole process of actually compromising the victim. IABs are individuals who gather and collect credentials, selling them to the highest bidder. While IABs are not exclusively for ransomware, the system is definitely leveraged by ransomware operators, typically at the beginning of the intrusion lifecycle, by conducting reconnaissance to identify networks with vulnerable applications or devices such as VPNs, open Remote Desktop Protocol (RDP), or servers with exposed software vulnerabilities. With solid best practices such as two-factor authentication (2FA) and additional identification mechanisms, this vector can be avoided.

Are You at Risk?

One might assume only large corporations are the targets of ransomware. That said, small business is not immune to compromise, making up over half of the attacks according to a Senate Judiciary Hearing in July 2021, "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks."

Ransomware attacks can have a very public impact, as victim organization operations may be severely degraded or shut down entirely, illustrated by recent attacks on hospitals across the United States. Personally identifiable information (PII) can be a veritable goldmine of data for cyber thieves who can sell or auction it off on the dark web.

Criminals have realized that this is a lucrative business with low barriers to entry; case-in-point, the ransomware-as-a-service model where affiliates use already-developed ransomware tools to execute ransomware attacks. Consequently, ransomware

> **"Ransomware does not just affect the deeper pockets of large companies like Colonial Pipeline and JBS. Small businesses already operate on thin margins, and many have been pushed to the brink by the pandemic."**
>
> — Chuck Grassley,
> Senate Judiciary Ranking
> Minority Member

is displacing other cybercrime business models. Moreover, attackers are becoming increasingly sophisticated in their ability to determine the value of compromised information, assess the victim organization's willingness to pay, and demand higher ransoms.

More Platforms Are Vulnerable

While attackers focused almost exclusively on Microsoft Windows® systems in the past, the emergence of ransomware for Android® and macOS® X and now Linux demonstrates that no one operating system is immune from these attacks. Nearly all computers or devices with an internet connection are potential victims of ransomware, which is a valid concern with the proliferation of IoT devices, and most recently, an expanded attack surface due to a surge in remote workers driven by work-from-home mandates.

Supply Chains in the Crosshairs

In 2021, Kaseya VSA, a global IT management software company, became the unwitting poster child for supply chain attacks when they were breached with a particularly nasty variant of Sodinokibi ransomware. Dubbed REvil, it's ransomware as a service (RaaS) that uses affiliates to distribute malware infections, giving them a percentage of the ransoms paid after developers of the ransomware receive their cut.

By exploiting a software vulnerability, attackers gained access to Kaseya software, leveraging this access to install ransomware on customers' infrastructure. The attack targeted Kaseya's customers' data and financial resources through ransom demands.

As a global scourge, organizations such as the European Union Agency for Cybersecurity (ENISA) research and report on mapping and studying supply chain attacks, among others. In their recent report, *ENISA Threat Landscape for Supply Chain Attacks, 2021*,[3] they highlight serval findings, including:

- Around 50% of the attacks were attributed to well-known APT groups by the security community.
- Around 42% of the analyzed attacks have not yet been attributed to a particular group.
- Around 62% of the attacks on customers took advantage of their trust in their supplier.
- In 62% of the cases, malware was the attack technique employed.
- When considering targeted assets, in 66% of the incidents, attackers focused on the suppliers' code to further compromise targeted customers.
- Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.

Supply chain attacks can be attributed to the rise of DevOps and agile practices, which can speed up development cycles due to often aggressive release timelines for new features and capabilities and the resultant reliance on third-party code in vendor applications.

Double, Triple and Even *Quadruple* Extortion Are on the Rise

In a case of double extortion, ransomware operators encrypt and steal data to further coerce a victim into paying a ransom. If the victim doesn't pay the ransom, the ransomware operators then leak the data on a leak site or dark web domain, with most leak sites hosted on the dark web. These hosting locations are created and managed by the ransomware operators. At least 16 different ransomware variants are now threatening to expose data or utilize leak sites, and more variants will likely continue this trend.[4]

In October 2020, the first case of triple extortion was reported when the internal systems of Vastaamo, a Finnish psychotherapy clinic with 400 employees and approximately 40,000 patients, were breached. After attempting to extort a 40-bitcoin (£403,000; over $500K) ransom, the attackers began to target payments from individual victims, including children.

[3] *ENISA Threat Landscape for Supply Chain Attacks*, European Union Agency for Cybersecurity, July 29, 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[4] *Unit 42 Ransomware Threat Report*, Palo Alto Networks, April 20, 2021, https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.

Extortion Payments Hit New Records as Ransomware Crisis Intensifies

The average ransomware payment climbed 82% since 2020 to a record $570,000 in the first half of 2021!
Ransomware operators now commonly use as many as four techniques for pressuring victims into paying.

Encryption
Victims pay to regain access to encrypted data

Data Theft
Hackers threaten to release stolen data if ransom is unpaid

Denial of Service
DoS attacks shut down victims' public websites

Harassment
Customers, business partners, employees and media contacted

Figure 1: Quadruple extortion is on the rise

The rise of "quadruple extortion" (figure 1) is one disturbing trend identified by Unit 42 (Palo Alto Networks threat intelligence and consulting arm). Ransomware operators now commonly use as many as four techniques for pressuring victims into paying:

1. **Encryption**: Victims pay to regain access to scrambled data and compromised computer systems that stop working because key files are encrypted.
2. **Data Theft**: Hackers release sensitive information if a ransom is not paid. (This trend really took off in 2020.)
3. **Denial of Service (DoS)**: Ransomware gangs launch denial of service attacks that shut down a victim's public websites.
4. **Harassment**: Cybercriminals contact customers, business partners, employees and media to tell them the organization was hacked.

While it's rare for one organization to be the victim of all four techniques, 2021 showed an increase in ransomware gangs engaging in additional approaches when victims don't pay up after encryption and data theft. The 2021 Unit 42 Ransomware Threat Report, which covered 2020 trends, flagged double extortion as an emerging practice—and the latest observations show attackers again doubling the number of extortion techniques they use.

As they've adopted these new extortion approaches, ransomware gangs have gotten greedier. Among the dozens of cases that Unit 42 consultants reviewed in the first half of 2021, the average ransom demand was $5.3 million. That's up 518% from the 2020 average of $847,000.

The ransomware crisis will continue to gain momentum over the coming months as cybercrime groups further hone tactics for coercing victims into paying and developing new approaches for making attacks more disruptive.

Prepare and Prevent

Ransomware acts quickly—sometimes within minutes of infection—so it is critical to take action and deploy controls that either mitigate or prevent ransomware attacks. The next two sections summarize the top recommendations to do both.

Recommendations to Mitigate the Impact of a Ransomware Attack

Develop and execute a plan for an end-user awareness program.

- It can be difficult to get approval to send regular company-wide security reminders, but smarter end users who are more aware of cybersecurity risks will surely experience fewer ransomware incidents.

Review/Validate server backup processes.

- Backups that are configured improperly or in a location that can allow for further compromise can result in further losses, both monetary and otherwise.
- Review critical file servers that host network shares for critical departments and plan for regular review of the recovery process for these servers.

Conduct end-user privilege reviews.

- Assign a trusted delegate to develop and organize a process to evaluate permissions that users have on mapped network drives. Whenever possible, implement the principle of least privilege to minimize the impact that any single user can have.
- Start the review process by looking at end-user privileges for critical resources and departments.
- Require strong, unique, and complex passwords for all accounts.
- Review network drive permissions to minimize the impact a single user can have.

Define administrator user privilege reviews.

- Audit privileged roles used by the server, backup, and network teams to validate appropriate access.
- Ensure administrators are assigned normal, restricted accounts, separate from their highly privileged accounts.
- Require administrators to use their highly privileged accounts only when they need them.
- Remove automatic network drive mappings from administrative accounts, where possible.
- Restrict administrative accounts from receiving email.
- Require multi-factor authentication for all users, including administrative accounts, and monitor for abnormal use.
- Require strong, unique and complex passwords for all accounts.

Document your incident response plan for ransomware.

- Ensure ransomware response processes are included in your incident response plan. Ransomware requires a unique process to recover and should stand out on its own.
- Cases where all the files on an entire department drive are encrypted can become quite complex as multiple teams need to be engaged—backup team, file-server team, endpoint, directory team, and others. The more you plan now, the quicker your response time will be.

Top Recommendations to Prevent Ransomware Infections

Promptly apply software patches.

- Review your patching processes and risk acceptance and look for opportunities to remove roadblocks.
- Ensure VPN and file-sharing services are up to date.

Protect against email-based threats.

- Configure protections for inbound mail and block files most likely to present a higher risk.
- Prevent users from enabling macros by blocking macros from running in MS applications.
- Inspect emails for malicious URLs.
- Train end users on phishing and social engineering techniques.

Deploy a next-generation firewall.

- Ensure your firewall automatically blocks known threats based on a trusted threat feed that constantly updates.
- Ensure your firewall provides sandboxing capabilities so you can stop unknown threats (URLs and executables) before they reach the endpoint.
- Configure your firewall/proxy to require user interaction for end users communicating with websites labeled as “uncategorized” (e.g., click a “Proceed” button). Many uncategorized websites are used in targeted phishing campaigns to distribute malware. This two-step process prevents certain types of ransomware from making that external call to the command-and-control server. If that doesn’t happen, your files may not be encrypted.
- Ensure signatures are up to date regarding remote desktop vulnerabilities.
- Ensure your next-generation firewall includes advanced URL filtering capabilities to detect unknown threats.

Deploy advanced endpoint protection.

- Ensure that your endpoint protection measures can detect and prevent known and unknown malware, as well as known and unknown exploits, including zero-day exploits.
- Add behavior-based malware detection on top of allow listing.
- Ensure your endpoint protection systems are armed with real-time threat intelligence gained from internal and external sources that cross organizational boundaries, geographies, and industries.

Restrict and manage external network access.

- Direct external remote desktop access should be disabled by default. If external access is necessary, ensure all administrative connections are conducted through an enterprise-grade, multi-factor authentication VPN.
- Limit user privileges wherever possible, including users of BYOD initiatives.

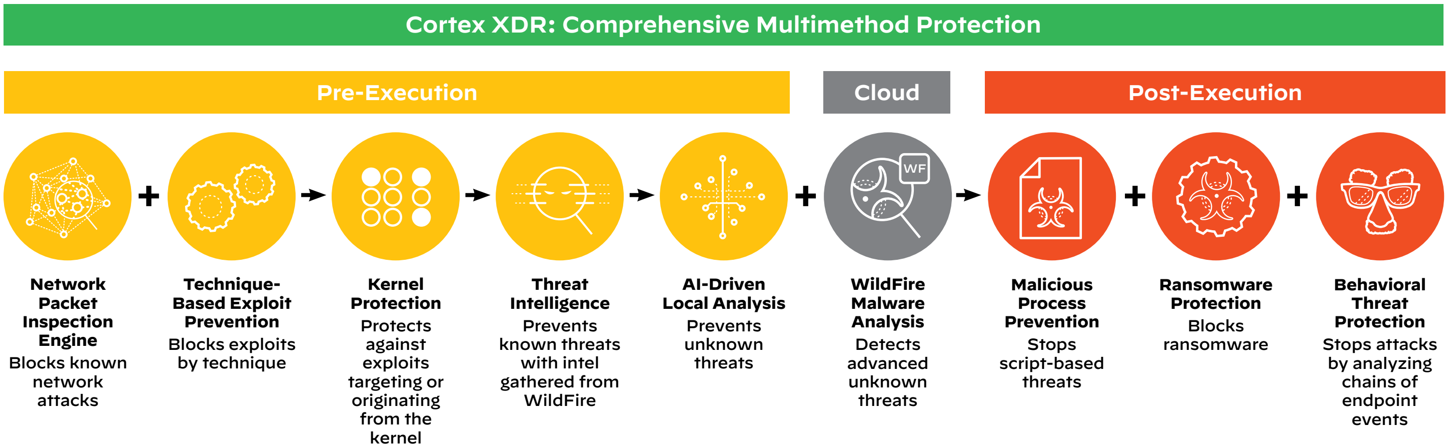
Know your environment.

- Maintain an up-to-date inventory of all assets. Routinely validate inventory and accounts associated with each device.
- Establish a network norm and set alerts for activity occurring outside of normal operations globally.
- Identify all traffic on the network and block all high-risk traffic.
- Review and inspect protections on all internet-exposed services.

How Cortex XDR Helps Prevent, Detect, and Stop Ransomware Attacks

Cortex® XDR™ is an integrated platform for cross-data prevention, detection, and response (figure 2). It lets your security team instantly contain network, endpoint, and cloud threats from one console. Analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists like bad domains through tight integration with enforcement points. Cortex XDR also allows you to:

- Block ransomware attacks at every step in the attack lifecycle, from the initial exploit to file analysis and behavioral protection.
- Find stealthy attacks with AI and cross-data analytics.
- Quickly investigate with root cause analysis.
- Contain any threat with a coordinated response.



Cortex XDR: Comprehensive Multimethod Protection

Pre-Execution

Network Packet Inspection Engine
Blocks known network attacks

+

Technique-Based Exploit Prevention
Blocks exploits by technique

→

Kernel Protection
Protects against exploits targeting or originating from the kernel

→

Threat Intelligence
Prevents known threats with intel gathered from WildFire

→

AI-Driven Local Analysis
Prevents unknown threats

+

Cloud

WildFire Malware Analysis
Detects advanced unknown threats

→

Post-Execution

Malicious Process Prevention
Stops script-based threats

+

Ransomware Protection
Blocks ransomware

+

Behavioral Threat Protection
Stops attacks by analyzing chains of endpoint events

Figure 2: Cortex XDR includes XQL search, grouping alerts into incidents, revealing the root cause of any alert from any source, and more

Response Options in Cortex XDR

- **Live Terminal** for direct endpoint access includes a graphical task manager and file manager to view and terminate process, delete files, download files, run commands, and much more.
- **Script Execution** from our management console to execute virtually any Python script on one endpoint, a group of endpoints, or all endpoints.
- **Search and Destroy** indexes all the files on your endpoints to find and delete malicious files anywhere in your organization in real time.
- **Host Restore** to recover a compromised endpoint.

With our remediation suggestions, you can delete malware, restore files using Windows shadow copy, and remove registry key changes. These features are in addition to more traditional response options like quarantine, network isolation, blocking files, and integrating with Cortex XSOAR for an automated response.

Traditional Endpoint Protection, Detection and Response Aren't Enough

- Cannot identify and block advanced endpoint attacks.
- Requires too many manual processes.
- Provides a limited, endpoint-only view into your environment.
- Depends on experienced analysts to manually investigate alerts.
- Weak at identifying new and advanced threats.

5 Musts if You've Been Attacked

1. **Network isolation.** Disable your virtual NICs.
2. **Carefully consider the location of your attack info before rebooting.** Sometimes the encryption key and other attack info can be found in the memory.
3. **Verify adequate data backups** and determine the overall risk to the organization if the ransom is not paid.
4. **See if a decryption tool exists using** https://www.nomoreransom.org/en/index.html.
5. **Execute an IR plan or call an IR team such as Palo Alto Networks Unit 42.** Unit 42 brings together an elite group of cyber researchers and incident responders with a deeply rooted reputation for delivering industry-leading threat intelligence. If you think you may have been breached or have an urgent matter, get in touch with the Unit 42 Incident Response team by emailing unit42-investigations@paloaltonetworks.com or calling:
    - **North America Toll-Free**: +1.866.486.4842 (+1.866.4.UNIT42)
    - **EMEA**: +31.20.299.3130
    - **APAC**: +65.6983.8730
    - **Japan**: +81.50.1790.0200

For more information on how Palo Alto Networks can help prevent ransomware attacks and/or minimize damage if a breach has occurred, view our on-demand webinar, Best Practices for Stopping Ransomware and download our 2021 Unit 42 Ransomware Threat Report.

Defending against ransomware attacks starts with having a plan. Organizations can jump-start that process with our Ransomware Readiness Assessment.

For More Information on Cortex XDR

Visit our webpage.

Download our XDR For Dummies Guide.

Download The Essential Guide to XDR.

Watch our video How Cortex XDR Works.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com