proofpoint.

EBOOK

2023

Ransomware Survival Guide

Preventing, managing and recovering from threats at every stage of the attack chain

Table of Contents

Executive Summary

Ransomware is an old threat that persists as a modern-day problem.

This type of malware—which gets its name from the payment it demands after locking away victims' files—is a major issue for modern businesses. It's one of today's most disruptive types of cyber attack. In 2022, ransomware incidents targeted school districts,[1] local and national governments[2] and healthcare organizations,[3] proving that cyber criminals will go after any organization they might be able to extort. Given the severity of this threat, it's more important than ever to have a plan to mitigate risk and respond if your systems are infected with ransomware and your data is stolen.

Like most cyber attacks, ransomware usually requires someone to have acted on the attacker's behalf, such as by opening an attachment or clicking a URL.

Why ransomware is still around

Ransomware has persisted because of four primary drivers:

- Ransom payments are easier to collect than other types of fraud, thanks to Bitcoin and other digital currencies.
- Attackers have many distribution channels—including existing compromises of an environment—boosting the chances of success.
- Many businesses have weak or outdated cyber defenses and poor backup and recovery routines, making for a large pool of targets.
- Attackers are getting better at targeting and becoming more sophisticated in their tactics.

Surviving ransomware

Ransomware compromises systems and data, but the attacks that lead up to it target people. Like most cyber attacks, ransomware usually requires someone to act on the attacker's behalf, such as by opening an attachment or clicking a URL. That's why fighting ransomware requires a people-centric approach. It's also important to keep internet-facing devices patched (such as file-transfer and VPN appliances) and lock down remote administration tools and protocols (such as RDP).

Consider this guide a starting point.

1 Howard Blume, Alejandra Reyes-Velarde (Los Angeles Times) "Student information remains at risk after massive cyberattack on Los Angeles Unified." September 2022.
2 Kate Conger, David Bolaños (New York Times) "Russian Hacking Cartel Attacks Costa Rican Government Agencies." May 2022.
3 Naomi Diaz (Becker's Hospital Review) "289 healthcare organizations were impacted by ransomware attacks in 2022." January 2023.

Before the attack

The best security strategy is to avoid ransomware altogether. This requires planning and work—before the crisis hits.

Back up and restore

One of the most important parts of any ransomware security strategy is regular, immutable data backups. Because many ransomware strains target network-connected backups, maintain those backups on a separate network or in the cloud. And be sure to disable file-system access to those backups.[4]

Surprisingly few organizations run backup and restore drills. Both halves are important; restore drills are the only way to know ahead of time whether your backup plan is working.

Keep in mind that backups, while necessary, are not always sufficient. In many cases, ransomware attacks also involve data theft—backups won't stop attackers from leaking, selling or misusing that data.

Update and patch

Keep operating systems, security software, applications and network hardware patched and up to date to prevent easily accessed vulnerabilities—particularly on internet-facing devices favored by attackers, such as VPNs and file-transfer appliances.

Invest in robust people-centric security solutions

Many types of people-centric attacks—including malicious attachments, URLs and phishing emails—lead to ransomware. Recently, threat actors have even started using callback phishing, also known as telephone-oriented attack delivery (TOAD). In these attacks, the only malicious part of the email is a phone number. The most advanced email security solutions can protect against all of these attacks as well as any other malware that's delivered through email.

Employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware and how to report it. If employees receive a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own.

Harden your identity infrastructure

Most ransomware attackers must obtain privileged access to install their malware across enough devices to disrupt their victims. In most cases, they do this through Microsoft Active Directory. Their tactic is to use a host of easily obtainable tools, like BloodHound, PingCastle, Impacket and Cobalt Strike. These tools run Microsoft utilities—not malware—to turn the attacker's initial, low-level access into what is known as a Tier-0 entitlement, such as domain administrator.

By using an identity threat defense solution—or even those same open-source tools—you can see which paths can be used by an attacker. Finding these paths is a critical step; it helps you to understand how you can prevent a single compromise from becoming a full-blown, enterprise-wide ransomware incident.

Plan your response

Being locked out of business-critical systems is stressful, and stress affects decision-making.[5] Know in advance how you are going to respond so that you can focus on containment and recovery in the event of an attack.

There is no one-size-fits-all response plan to a ransomware attack. Hospitals and other essential infrastructure must weigh the cost of disruption very differently than a consumer business would. Running a full tabletop exercise is a good way to plan each stage of your response.

4 W. Curtis Preston (Network World) "How to protect backups from ransomware." February 2021.
5 Kathleen M. Kowalski, Charles Vaught (International Journal of Emergency Management) "Judgment and Decision-Making Under Stress: An Overview for Emergency Managers." June 2003.

During the attack

While the best ransomware strategy is to avoid it in the first place, increasingly sophisticated attacks against the software supply chain have shown that even the best-prepared companies can be caught.[6] Ransomware may not even be the first payload to infect your system. Many ransomware gangs now prefer to buy access to targets already infected with Trojans or loader malware.

During the attack, you have urgent problems to resolve, such as getting computers, phones and networks back online and dealing with ransom demands.

Disconnect from the network

The moment employees see the ransomware demand or notice something odd they should disconnect from the network and take the infected machine to the IT department. Only the IT security team should attempt a reboot, and even that will only work in the event it is fake scareware or run-of-the-mill malware.

If the ransomware has already made its way to a server, the security team should isolate it as quickly as possible and map out a response.

Be aware: as is the case with household pests, a single infected device is usually a sign of a larger issue. Proactively search your environment for other infected systems.

Call law enforcement

Ransomware—like any form of theft and extortion—is a crime. Notifying the proper authorities is a necessary first step.

You should also contact your ransomware insurer if you have coverage.

Implement your planned response

Your planned response should be flexible enough to accommodate a variety of factors:

- The type of attack, specifically the ransomware strain used and the attacker behind it
- The presence of earlier malware payloads that may have been used for reconnaissance or loading the ransomware
- Who in your network is compromised
- What network permissions compromised accounts have

Ransomware infections are often secondary infections on already-compromised networks. That means each of these factors are critical in assessing the scope of the problem and preventing further infections and data loss.

Don't count on free ransomware decryption tools

Most free tools work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your ransomware.

Restore from backup

The only way to completely recover from a ransomware infection is restoring everything from backup. But even with recent backups, paying the ransom might make more financial and operational sense.

6 Kellen Browning (New York Times) "Hundreds of Businesses, from Sweden to U.S., Affected by Cyberattack." July 2021.

After the attack

While the immediate crisis may be over, there's still plenty of work ahead.

Review and reinforce

We recommend a top-to-bottom security assessment to find threats that may still linger in your environment. Take a hard look at your security tools and procedures—and where they fell short.

Cleanup

Some ransomware is delivered through other threats or backdoor Trojans that can lead to future attacks. Often, the victim's environment was already compromised, opening a door for the ransomware.

Look closer for hidden threats that you may have overlooked in the chaos, especially if there is a risk that backups may also have been compromised.

Post-mortem review

Review your threat preparedness, the chain of events that led to the infection and your response. Without figuring out how the ransomware got through, you have no way of stopping the next attack.

Assess user awareness

A well-informed employee is your last line of defense. Make sure employees, staff and faculty are up to the task. Regular assessments and phishing simulations can help pinpoint who is most vulnerable and to which email lures and other tactics.

Education and training

Develop a curriculum to address employee vulnerability to cyber attacks. It should be based on real-world attack campaigns and tactics. Create a crisis communications plan in the event of a future attack, and follow up with drills and penetration testing.

Reinforce your technology defenses

Today's fast-changing threat landscape requires security solutions that can analyze, identify and block—in real time—the malicious URLs and attachments that serve as ransomware's primary entry points. During your incident response, you should also have the tools to find evidence of how an attacker gained privileged access in your environment, which is usually through Active Directory. This ensures you can prevent lateral movement and privilege escalation in future incidents.

Seek out security solutions that can adapt to new and emerging threats and help you respond to them faster.

SECTION 1

Introduction

Ransomware has been around now for more than three decades. And in that time it has undergone several evolutions. Over the past year, the amount of money being paid to ransomware criminals has trended down. This decrease has been attributed to the disruption of major ransomware gangs—including some arrests—and to declines in cryptocurrency values.[7]

However, keep in mind that the decrease in ransomware payments came on the heels of an enormous surge. 2021 saw attack volumes—and payment amounts—spike to new all-time highs.[8] Typically, after ransomware gangs' activities are interrupted by law enforcement, these same criminals resurface elsewhere with new names and new strategies. So we anticipate that a surge may follow the current decline. The pace of ransomware attacks carried out by Russian criminals against U.S. targets may also have slowed due to the war in Ukraine, but this lull is likely to be only temporary.

Amidst ongoing efforts by governments and law enforcement to stop cyber crime, criminals are shifting their tactics. Attackers no longer rely on broad distribution and small ransom amounts. Instead, ransomware gangs now often collaborate with other malware distributors who provide access to systems already infected with Trojans and loaders for prospecting, reconnaissance and attack. This approach allows criminals to identify high-value targets with more to lose from disruption and more capacity to pay.

Ransomware gangs are creative and inventive. They're experimenting with new tactics, which means that defenders cannot let their guard down even for a second.

7 Robert McMillan, Dustin Volz, Aruna Viswanatha (Wall Street Journal) "Hackers Extort Less Money, Are Laid Off as New Tactics Thwart More Ransomware Attacks." February 2023.
8 James Rundle, David Uberti, Catherine Stupp (Wall Street Journal) "Cyber Defense Confidence Ebbs as Ransomware Attacks Multiply." May 2022.

Hitting the headlines

With ransomware attacks coming frequently and criminals getting ever closer to causing serious harm to national infrastructure—whether intentional or not—governments around the world are waking up to the seriousness of the ransomware threat.

During the first months of 2022, regulators and government officials stepped up their efforts to combat ransomware attacks. In March, the U.S. Securities and Exchange Commission (SEC) published new proposed cybersecurity rules for listed companies.[9] The proposed rules would mandate reporting of ransomware attacks and data breaches. And they would also require companies to disclose their policies for identifying and managing cybersecurity risks.

Later that month, the Biden administration signed a bill into law that requires critical infrastructure operators to report cyberattacks and ransomware incidents within 72 hours to the Cybersecurity and Infrastructure Security Agency (CISA).[10] The goal of this new legislation is to promote information sharing across the public and private sectors to help prevent similar attacks elsewhere.

U.S. officials' efforts to stem the ransomware tide didn't seem to slow down the prominent Russian Conti ransomware group. A month later, in April 2022, the group successfully attacked the government of Costa Rica—one of Conti's last actions before shutting down in the face of unprecedented scrutiny. Nearly 30 government departments were compromised. And medical appointments, tax payments and essential citizen services were disrupted.[11] In response, newly elected president Rodrigo Chaves declared a national state of emergency. Chavez stated that his country was "at war" with the cyber criminals, who allegedly called for his overthrow in a blog posted to the dark web.[12]

September 2022 saw more major ransomware attacks targeting public sector organizations. The Los Angeles Unified School District was impacted by a high-profile ransomware incident just in time for back-to-school. District officials refused to pay the ransom demanded. So the criminals—who stole roughly 500 gigabytes of data—published files on the dark web, including Social Security numbers, contracts, tax forms and student records from the nation's second-largest school district.[13] A few days later, attackers targeted Suffolk County, New York State's most populous county outside of the five boroughs of New York City. The ransomware attack triggered a full digital shutdown of the municipal government.[14]

9 Paul Kiernan (Wall Street Journal) "SEC Proposes Requiring Firms to Report Cyberattacks Within Four Days." March 2022.
10 David Uberti (Wall Street Journal) "Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches." March 2022.
11 Dustin Volz (Wall Street Journal) "U.S. Saw Signs of Decline in Russian Ransomware Strikes at Start of Ukraine War." May 2022.
12 Carly Page (TechCrunch) "Fears grow for smaller nations after ransomware attack on Costa Rica escalates." May 2022.
13 Howard Blume (Los Angeles Times) "L.A. Unified data breach last year includes at least 2,000 student records, officials say." February 2023.
14 James Rundle (Wall Street Journal) "Suffolk County, N.Y., Hack Shows Ransomware Threat to Municipalities." November 2022.

Soon afterwards, the ride-sharing platform Uber became the latest victim of the infamous cyber attack group Lapsus$, joining the ranks of Microsoft, Nvidia, Okta, Samsung and other major technology firms.[15] Lapsus$ attacks typically involve social engineering to get login credentials and gain access employee user accounts. While the group often attempts to extort money from its victims, it usually does so without installing malware on their computers.

A ransomware attack on cloud services provider Rackspace in December 2022 rounded out the year. The attack led to an outage in the company's Microsoft Exchange hosting platform, which shut down its customers' email access. Rackspace later confirmed that a threat actor group known as Play was responsible for the incident.[16]

How ransomware works

Ransomware works by blocking access to a computer system or data, usually by encrypting files with specific extensions (JPG, DOC, PPT and so on). Files remain out of reach until the victim pays the attacker for an encryption key code to unlock the files. In many cases, the payment demand comes with a deadline. If not met, that ransom can double, or the data can be lost forever, leaked or even destroyed.

In many cases, victims are extorted multiple times: first for an encryption key to unlock their data and then again to prevent the attackers from releasing or selling copies on the dark web. Today, nearly 100% of ransomware incidents involve data theft. Many groups now focus solely on data theft, no longer attempting to install ransomware, encrypt data or destroy information.

In many cases, victims are extorted multiple times: first for an encryption key to unlock their data and then again to prevent the attackers from releasing or selling copies on the dark web.

This makes attacks more problematic for their victims. Once data has been stolen, there's no guarantee it'll ever be recovered. Even if it is, there's no way to know if it has already been sold or if it'll be exposed in the future. This makes the decision of whether to pay even more difficult.

What's worse, cyber criminals are increasingly "triple dipping." In other words, they're extorting one ransom to return or unlock stolen data, a second to destroy that stolen data and yet a third to reveal any modifications that were made to the returned data.

15 Robert McMillan (Wall Street Journal) "Uber Says Breach Was by Lapsus$, a Teenage Hacking Group Motivated by Fame Over Money." September 2022.
16 Eric J. Savitz (Barron's) "Rackspace Ransomware Attack Reveals the Cloud's Vulnerability." December 2022.

64%
of organizations were infected by ransomware in 2022.

64%
elected to pay the ransom.

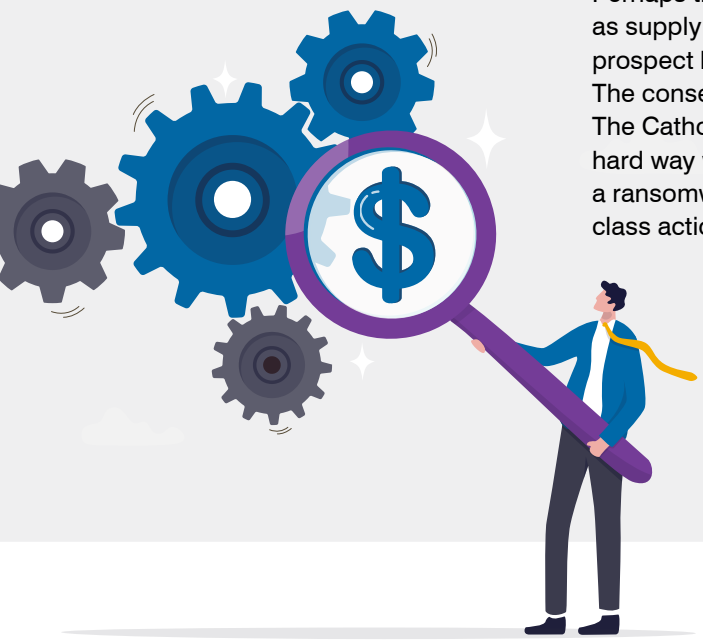
The real-world costs

Nearly two-thirds of global organizations experienced at least one ransomware attack in 2022, with 64% of victims electing to pay the ransom.[17] The financial consequences of an attack can be considerable, with average ransom payments exceeding $400,000 per incident.[18]

Cybersecurity industry analysts report that payments to ransomware groups dropped by 40% in 2022, though they still totaled $457 million.[19] The average ransom demand is down as well, from an average of $5.7 million in 2021 to $4.1 million in 2022.[20] Experts suspect that more victims are refusing to pay, especially since the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) made it clear that organizations can face penalties if they make payments to groups that are on the sanctions list.[21] However, many ransom payments remain undisclosed. And the threat of consequences may push more of them out of the public eye. The true financial cost of ransomware to businesses is very difficult to ascertain since some will inevitably attempt to deal with an intrusion privately.

But the business cost is not just limited to financial expense. The vast majority of ransomware attacks now include a threat to leak exfiltrated data. This means all ransomware incidents have the same consequences as a data breach. These range from harm to the company's reputation, to disclosure requirements and potential fines.

Perhaps the hardest cost of all to anticipate is the price of business disruption, as supply chains grind to a halt, sales teams are unable to access customer and prospect lists and even the most basic communication tools become inaccessible. The consequences can be even greater in critical sectors such as healthcare. The Catholic nonprofit healthcare system CommonSpirit Health found this out the hard way when it experienced downed networks and IT systems for weeks after a ransomware attack. In the incident's aftermath, the organization was hit with a class action lawsuit that alleged it had failed to adequately protect patient data.[22]



17 Proofpoint. 2023 State of the Phish. February 2023.
18 Coveware. "Improved Security and Backups Result in Record Low Number of Ransomware Payments." January 2023.
19 Robert McMillan, Dustin Volz, Aruna Viswanatha (Wall Street Journal) "Hackers Extort Less Money, Are Laid Off as New Tactics Thwart More Ransomware Attacks." February 2023.
20 Ibid.
21 Department of the Treasury. "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." October 2022.
22 Annie Burky (Fierce Healthcare) "Class action accuses CommonSpirit Health of negligence following major ransomware attack and data breach." January 2023.

Where it comes from

Ransomware is distributed through several main attack vectors:

- Email, including ransomware attachments and URLs that lead to malicious files
- Compromised remote desktop protocol (RDP) and virtual private network (VPN) access
- Compromised cloud accounts that lead to malware uploads
- Vulnerabilities in enterprise networking equipment
- Infected websites/links through social media and malware-infected advertising (malvertising)
- Other malware (such as loaders and stealers) that can infect already-compromised systems with ransomware

Even when the ransomware stems from other malware, an email is often the initial vector.

These emails look legitimate and can fool unsuspecting employees. Often, the messages masquerade as official software updates, unpaid invoices or even a note from the boss targeted to a direct report.

How it's evolving

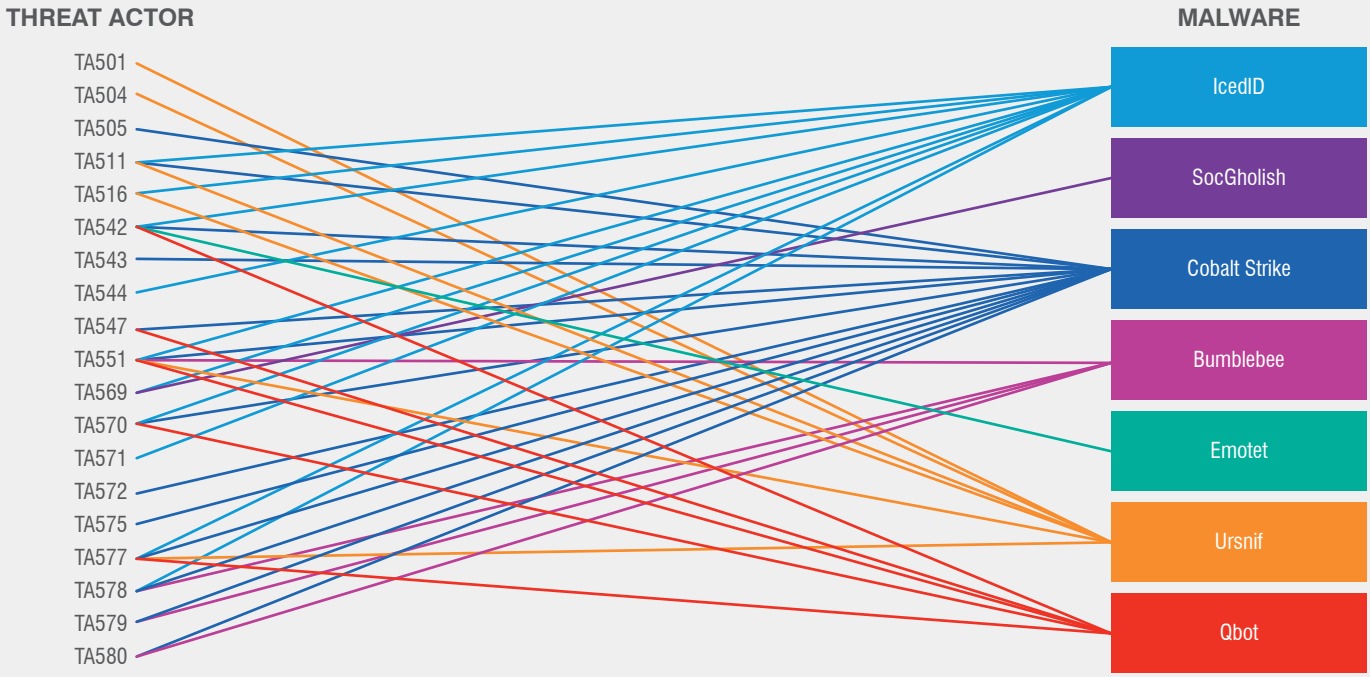
As attackers adapt to new defenses, adopt new tactics and embrace new tools, the ransomware game is evolving. Here are some ways the threat landscape is changing.

Ransomware and email

A large percentage of ransomware starts, directly or indirectly, with a phishing email. These emails trick users into opening a malicious attachment or clicking a malicious URL.

But things have changed in the seven years since Locky appeared in millions of inboxes. More recently, ransomware has been delivered as a secondary infection after a system is already infected with a Trojan or loader. The groups responsible for distributing these kinds of malware, known as initial access brokers, then sell access to ransomware gangs, who prospect among infected networks, looking for the most valuable targets. The brokers or facilitators either earn a flat fee or a percentage of the ransom in return for providing an entry point to the network.

There are several strains of malware known to be used for this initial access, and several different cyber criminal groups known to distribute them. Since 2022, researchers at Proofpoint have seen potential initial access malware featuring in campaigns by these groups:



It's important to note that we have not directly observed these criminal groups distributing ransomware themselves. Nor is it possible to draw a simple one-to-one relationship between malware and ransomware strains. But all of the malware on this list can lead to ransomware infection. And all of it is regularly delivered by some of the world's most prolific attackers.

For most organizations, the first line of defense against ransomware remains protecting users from downloading remote access Trojans (RATs), botnets and other kinds of malware. Block the loader, and you block the ransomware.

The network of relationships between cyber criminal groups is complicated, but the sequence of events in a typical email-instigated ransomware attack is not: infection by a Trojan or loader leaves a network vulnerable to ransomware gangs looking for high-value targets. So for most organizations, the first line of defense against ransomware is making sure they are protected from other kinds of malware.

The insider threat

Beyond email lures and tech exploits, attackers have opened another front in the ransomware war: willing collaborators. In a small but alarming number of cases, threat actors are trying to recruit employees of targeted companies to install ransomware at their workplace in return for payment.

In 2020, someone offered a Tesla employee $500,000 to install ransomware on the company's network. The employee reported the attempt, and the culprit was arrested and pleaded guilty—but not before bragging about succeeding elsewhere.

Since then, the LockBit ransomware family has risen to prominence with a series of high-profile attacks targeting large enterprises and government agencies.[23] LockBit's operators are actively recruiting insiders to help them deploy malware on their victims' networks. In return, insiders are promised million-dollar payments. LockBit also offers large payments to insiders who provide them with access to networks or valid account credentials.

Attempts to recruit insiders are usually made via email, but the messages don't contain malware attachments. As a result, only advanced email security solutions can detect the risky messages. It's a good idea to educate employees to recognize these threats and report them promptly.

Double (and triple) extortion

The days of simple system lockdowns and encryption after a ransomware attack are over. Threat actors are now focused on increasing their payouts. This means they're asking for multiple payouts, carrying out multiple data breaches, publicly shaming their victims on leak sites and blackmailing consumers in double- and triple-extortion schemes.

Recently, Proofpoint observed that 64% of organizations infected by ransomware agreed to pay the ransom.[24] Of that group, 41% were forced to pay more than once. And a small and unlucky percentage of this group never got back access to their data; unfortunately, this situation is not uncommon.

In the last few years, we've seen ransomware attackers employing double extortion more frequently. This entails exporting customer data and using it for leverage instead of simply halting company operations. Sometimes, these threat actors skip encryption and go straight to extortion tactics.

The number of malicious actors that favor data theft and extortion attacks—and don't use ransomware—are growing. This group grew by 20% in 2022.[25] Extortion techniques have also progressed, giving rise to triple extortion. In this case, ransomware gangs bypass organizations and go directly to consumers with their stolen data to alert them of a breach.

23 Aaron Sandeen (Dark Reading). "Everything You Need to Know About LockBit." November 2022.
24 Proofpoint. State of the Phish Report. 2023.
25 Crowdstrike. Global Threat Report. 2023.

The goal of triple extortion is to convince customers to apply additional pressure on the victim company and, rarely, to extort the customers themselves. An example of this criminal technique occurred in the United States in December 2022 at Knox College in Illinois.[26] The recently disrupted ransomware group known as Hive gained access to sensitive student information and contacted students directly, saying, "For us, this is a normal business day. For you, it's a sad day," before listing their demands.

Conventional cyber defenses are overwhelmed with threats from all sides.

Why it's still around

Ransomware is a decades-old exploit. But it has become a bigger threat because of four primary drivers.

More distribution channels

Cyber criminals have the ability to attack thousands of entities simultaneously using a variety of attack vehicles, opening the door for secondary ransomware attacks.

Conventional cyber defenses are overwhelmed with threats from all sides:

- Massive botnet-driven email campaigns
- Exploitable vulnerabilities in networking hardware and software
- Polymorphic malware that outpaces security vendors' ability to build new malware signatures
- Malvertising and compromised websites outside of the organization's perimeter
- The ubiquity of Active Directory, making it easy for attackers to "rinse and repeat" their lateral movement and privilege escalation tactics

Together, these factors make compromises more likely, giving ransomware more opportunities to gain a foothold.

More lucrative targets

Instead of broad-ranging attacks, cyber criminals are increasingly turning their sights to organizations with sensitive data, thinly stretched IT departments and a high incentive to quickly settle the matter.

Adding fuel to the fire are the security challenges common in hospitals, police departments, schools and state and local government agencies.

For these organizations, network downtime is not a viable option. It's no wonder that many make the quick calculation that forking over a ransom is the best business move.

26 Kevin Collier (NBC). "Ransomware hackers take demands directly to college students: 'For you, it's a sad day'." December 2022.

Better targeting and a more developed ecosystem

Ransomware used to be a numbers game: attack hundreds of thousands of recipients in high-volume, low-ransom email campaigns and hope enough victims take the bait.

Today, attackers are getting choosier about their targets. They seek out vulnerable business- and mission-critical data and systems that victims desperately need access to in hopes of a bigger payout.

At the same time, ransomware attacks are growing more sophisticated. Instead of simply deploying malware in the first stage of an attack, cyber criminal groups have grown more specialized, with some focused on obtaining access to corporate networks, others making their ransomware available for rent and still others setting their sights primarily on data exfiltration and extortion.

On the one hand, the ransomware tools used in these attacks has grown more robust, and some criminals are even paying “bug bounties” for new zero-day exploits. On the other, attack sequences focused solely on stealing data and asking victims to pay for it not to be sold or leaked—sometimes involving no malware at all—have grown more common.

$13M

Karakurt, an extortion-only group, has demanded ransoms as high as $13 million.

Ransomware without the "ware"

Traditionally, ransomware has worked by blocking victims' access to business-critical files and systems. For organizations with operations that depend on digital technology—which is nearly everyone today—an attack not only leads to downtime and high per-minute costs but can have devastating consequences.

In healthcare, for instance, downtime can compromise patient care and access to life saving procedures. An attack can also result in negligence claims. This was the case for one hospital in Alabama where a baby was born with a severe brain injury and eventually died because the hospital was struggling in the aftermath of a ransomware attack, according to a lawsuit filed by the baby's mother.[27] It's no wonder that ransomware victims are motivated to pay up quickly to minimize an attack's impact and severe potential consequences like this one.

As mentioned earlier in this guide, ransomware gangs are adding other layers to their attacks, incorporating data theft in so-called double- and triple-extortion attacks. In these attacks, criminals demand money even from companies that have robust backups of the encrypted data. Additional payments are supposed to stop sensitive data from being published. The potential release of data belonging to customers, third-party partners and vendors could put the victim at risk of lawsuits or fines. These threats are often just as effective as locking victims out of their networks.

Today, a growing number of cyber criminal gangs are embracing data theft and extortion-only attacks. Increasingly, they're not even bothering to install file-encrypting malware. Instead, they're simply exfiltrating data and threatening to publish it on the dark web or use it to publicly humiliate victims in other ways. This attack strategy is faster. Plus, it doesn't depend on file-encrypting malware, which can be difficult to spread across a network or can fail midway through an attack.

LockBit, one of the most active ransomware gangs in 2022, focuses heavily on data exfiltration. Its latest ransomware-as-a-service offering was LockBit 3.0 (also known as LockBit Black). With its release, the group published a set of "Affiliate Rules." One rule explicitly bans affiliates from using encryption in their attacks on critical infrastructure.[28]

Additionally, Karakurt, an extortion-only group, has demanded ransoms as high as $13 million. In mid-2022, the FBI and CISA published a joint statement that warned about the danger posed by Karakurt,[29] which has subsequently been linked to the now-defunct Russian group Conti.

Conti appeared to cease operations after an insider leaked the group's internal chats, which enabled threat researchers to compromise Conti's servers. Later, it became apparent that Karakurt was developed as a side business to monetize data stolen during Conti's encryption-based attacks.[30]

27 Kevin Collier (NBC News) "Baby died because of ransomware attack on hospital, suit says." September 2021.
28 Lawrence Abrams (Bleeping Computer) "LockBit 3.0 introduces the first ransomware bug bounty program." June 2022.
29 The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury) and the Financial Crimes Enforcement Network (FinCEN). Joint Cybersecurity Advisory: Karakurt Data Extortion Group. June 2022.
30 Ionut Ilascu (Bleeping Computer) "Karakurt revealed as data extortion arm of Conti cybercrime syndicate." April 2022.

The Bitcoin money trail

In traditional kidnapping for ransom, the biggest challenge has always been collecting and getting away with the money. Unfortunately, ransomware cyber criminals have a much easier path.

The most popular form of payment involves untraceable cryptocurrencies, the most well-known of which is Bitcoin. Bitcoin enables person-to-person payment via the internet and does not involve a bank or government.

A simple way of thinking about cryptocurrencies is to imagine them as the electronic equivalent of a casino chip. The tokens have no intrinsic value in the real world, but users can purchase tokens in their local currency and use them within the establishment—in this case the internet—then trade them in for currency upon exiting.

Similarly, cryptocurrencies can be purchased online using a credit card or bank account, from legitimate sources. In the case of ransomware, a victim might convert their local currency into Bitcoin, then send the Bitcoins to an anonymous cryptocurrency wallet address provided by the attacker.

The coins don't always go directly to the attacker. Typically, the tokens will land at a "tumbler," an electronic service that mixes the Bitcoins in with others, then dispenses coins out to the attacker (differently numbered, but the same value minus commission).

Much like money laundering in the physical world, the attackers can end up with untraceable payment. That payment then converts back into their local physical currency by trading in their Bitcoins for cash.

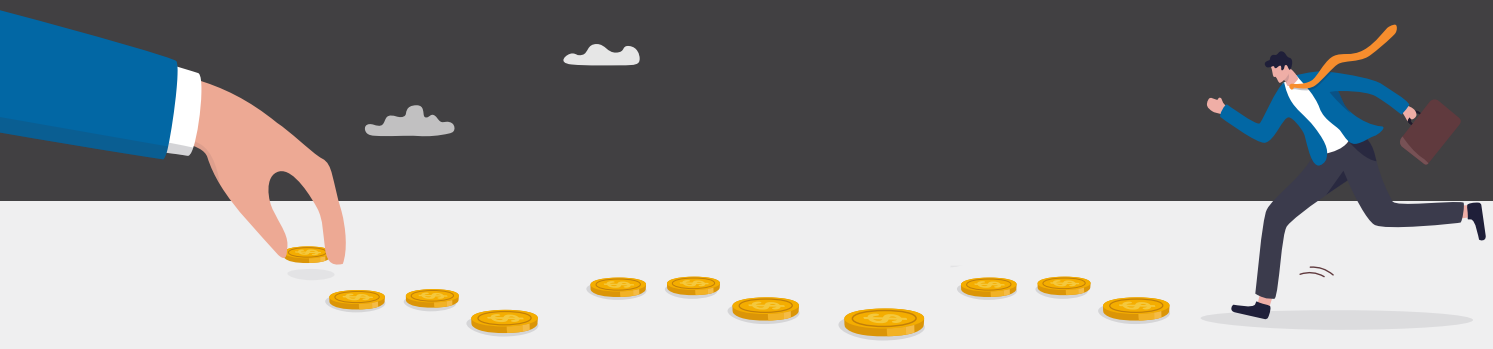
Unlike government-backed currency, cryptocurrencies are not widely recognized as money. They are instead regarded as something equivalent to poker chips or gaming tokens. Therefore, the transmission system and tumblers are neither regulated nor considered money laundering—though the effect is arguably the same.

The appeal of Bitcoin is obvious. It gives attackers a hard-to-trace, globally available cyber currency that converts directly to local hard currency, in other words, "unmarked bills."

Such an approach has clear benefits over the use of stolen credit cards, whose value plummets by the day as financial institutions have become more adept as swiftly shutting down victims' accounts.

The value of Bitcoin—along with those of other cryptocurrencies—plunged in 2022 as investors pulled back from these risky assets. In mid-May, the price of many cryptocurrencies collapsed, wiping out more than $300 billion in digital assets.[31] This had a significant impact on cyber criminals as well as the perpetrators of other financial crimes. Ransomware payments—and criminal profits—are still depressed.

At the same time, law enforcement has stepped up efforts to trace and recover cryptocurrency payments. The FBI was able to recover $2.3 million of the ransom paid in the 2021 attack on the Colonial Pipeline, which shut down fuel supplies to much of the U.S. east coast.[32] The FBI was also able to disrupt $130 million in ransomware profits when it gained access to servers run by the Hive ransomware gang.[33]



31 David Yaffe-Bellany, Erin Griffith, Ephrat Livni (New York Times) "Cryptocurrencies Melt Down in a 'Perfect Storm' of Fear and Panic." May 2022.
32 Dustin Volz, Sadie Gurman, David Uberti (Wall Street Journal) "U.S. Retrieves Millions in Ransom Paid to Colonial Pipeline Hackers." June 2021.
33 Aruna Viswanatha, Dustin Volz (Wall Street Journal) "FBI Disrupts 'Hive' Ransomware Group." January 2023.

SECTION 2

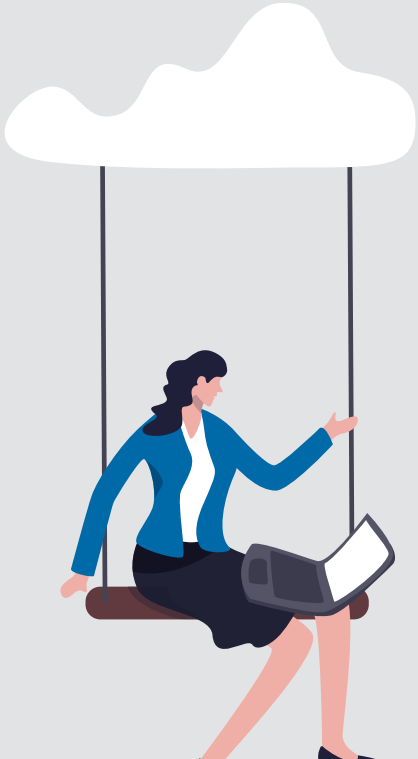
Before the Attack

The best security strategy is to avoid this extortion altogether. This is well within the power of most companies, but it requires planning and work—before the crisis hits.

Backup and restore

The most important part of any ransomware security strategy is regular data backups. Backups should be external and immutable. Most companies do this, but surprisingly few run both backup and restore drills. Restore drills are the only way to know ahead of time whether your backup plan will work. When planning and executing backup restoration, be sure backups can be restored to an isolated recovery environment. This can identify and help prevent any lingering consequent malware infections.

You may have some kinks to work through before a crisis hits. If backup-and-restore testing is done regularly, a ransomware infection won't have a devastating impact—you'll have a safe, recent restore point. But don't forget that there's caveat here. Attackers are increasingly threatening to leak data if victims don't pay. So while you may be able to prevent the worst, in terms of data losses, you probably won't be able to control any other fallout, like brand damage, lawsuits or fines.



70%

of security stakeholders say that their organization's vulnerability management program is only somewhat effective—or worse.

In the past, IT and security teams often assumed that cloud storage would be more resilient to ransomware attacks than endpoints or network drives. Recent research has suggested otherwise. Proofpoint threat researchers have discovered a potentially dangerous functionality in Microsoft 365 that allows ransomware to encrypt files stored on SharePoint and OneDrive in a way that makes them unrecoverable without dedicated backups or a decryption key from the attackers.[34] This means that ransomware attacks can now target organizations' data in the cloud, especially if they're able to gain access to SharePoint Online or OneDrive accounts using compromised credentials.

Keep in mind that backups are not a cure-all against ransomware attacks. In many cases, the price of restoring data from backups—including business downtime, IT labor and opportunity costs—will exceed the ransom. And many ransomware attacks involve data theft—even the most complete backups won't stop attackers from leaking or misusing it.

Update and patch

Ensure that operating systems, security software, applications and network hardware are fully patched and updated. It sounds basic enough. However, many organizations struggle to update software promptly. This trend is concerning because the number of vulnerabilities considered "critical" has skyrocketed in recent years. According to one recent survey, 70% of security stakeholders say that their organization's vulnerability management program is only somewhat effective—or worse. Only 18% are able to patch critical vulnerabilities within 24 hours of learning about them.[35]

But there are places to go to get a handle on patch management, such as the Center for Internet Security (CIS), a nonprofit organization that shares and promotes best practices for IT security management, including the threat of ransomware.

Overcoming "patch fatigue" is necessary—and essential to maintaining a safe environment. Closing remote desktop protocols and patching VPNs can be key to preventing easy access points for threat actors to launch ransomware attacks.

34 Proofpoint. "Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive." June 2022.
35 Cyentia Institute. "The State of Vulnerability Management." 2022.

Plan your response

Know in advance how you are going to respond so that you can focus on containment and recovery in the event of an attack. Dealing with a ransomware breach in the moment is a stressful experience, and every second counts as attackers try to reach further into the network to do more damage.

Critical questions such as: who needs to be informed, how to maintain communications and how much are you willing to pay (if you're willing to pay at all) are harder to answer in real time. This pressure creates potential bottlenecks in decision-making and leads to costly delays. These decisions will involve many stakeholders, including operational staff, legal counsel, financial decision makers and the board of directors, as necessary. Involve these players in the planning process before an attack happens to ensure a smooth and timely response after the fact.

There is no one-size-fits-all response plan to a ransomware attack. Hospitals and other essential infrastructure will weigh the cost of disruption very differently from consumer businesses. Running a full tabletop exercise is a good way to plan each stage of your response.

Invest in robust, people-centric email, web and identity threat defense solutions

Ransomware doesn't exist in a vacuum. Rather, it's one in a sequence of events that take place when cyber criminals attack an organization's IT environment. This "cyber attack chain" is a model that can help researchers understand, conceptualize and communicate how attacks unfold.

When security teams understand how attacks work, they can select technology that stops threats anywhere in the IT ecosystem.

Steps in the cyber attack chain

While cyber criminals don't follow the same steps every time, the basic phases of an attack are pretty much always the same:

- During the **initial compromise**, a user may be tricked by a malicious email, click a malware link or accidentally give away their credentials.
- Once attackers get in, they use **privilege escalation** and move laterally across the network.
- In the **impact phase**, attackers abuse privileges to steal, corrupt or destroy data, make changes to the network, and more.

The most effective strategy is to invest in technology that stops cyber criminals at every phase of the attack chain.

Email: your most critical vector

Traditional mail gateways, web filters and antivirus software should be updated and running on all networks. But they alone cannot counter the ransomware threat. An effective email security solution must go deeper.

Today's phishing email is sophisticated and highly targeted. Attackers carefully research their targets to create email that looks legitimate and preys on human nature to get them to click.

Malicious emails are sent during the initial compromise phase of an attack, and they lead to most ransomware infections. That's why you need advanced technology to protect this critical vector.

This means you need an email solution that can analyze embedded URLs and attachments to ensure no malicious content breaches the system. Cyber criminals are always one step ahead, and typical email security configurations rely too heavily on outdated signatures.

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. They also employ advanced machine learning and behavioral AI to identify hard to detect social engineering and phishing emails that lead to initial malware infections. And email authentication based on the DMARC standard can stop attacks that rely on domain spoofing—impersonating your organization's email domain to gain users' trust. Finally, your email security solution should protect against other types of identity deception, such as display-name spoofing and lookalike domains.

Remove common attack paths in your identity infrastructure

Ransomware actors need leverage, and there's no faster way to get it than compromising as many endpoints and as much data as possible. In a typical organization, the path to that sort of access goes through Active Directory or an insecurely managed privileged account.

An identity threat defense solution can automatically identify attack paths and remove them, including:

- Cached credentials
- Improperly protected local admin accounts
- Other weaknesses that attackers' tools will find from other compromised endpoints

Many organizations struggle to achieve this task because they may have thousands of Active Directory or Azure AD accounts. This is made even more difficult because many Active Directory accounts may connect to each other—often across numerous domains that trust each other.

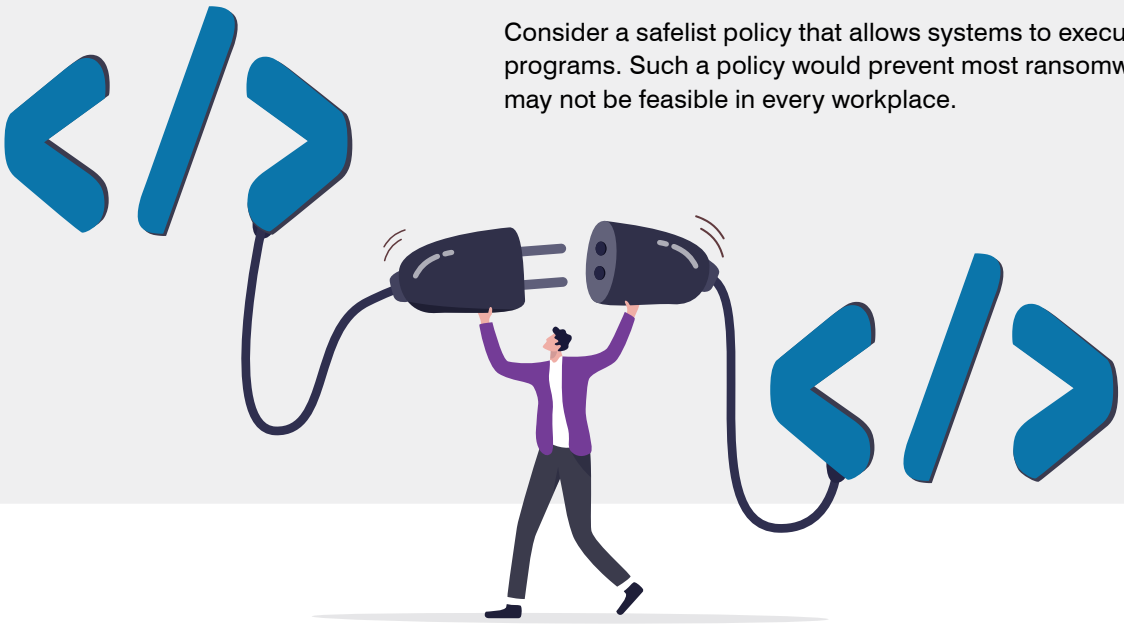
But the payoff of protecting identities is worth it. When you can identify and remediate at-risk user identities, you can stop attackers from moving laterally across the network and prevent them from accessing privileged accounts that they may not been able to access otherwise.

Stop code from running in certain locations

Deploy software controls to stop code from executing in common ransomware locations. These include temporary folders created by web browsers and compressed file directories in Windows' AppData/LocalAppData folder.

Restrict unknown software

Consider a safelist policy that allows systems to execute only known and vetted programs. Such a policy would prevent most ransomware from running, though it may not be feasible in every workplace.



Make your people a strong layer of defense

Most malware infections begin with a single well-intentioned employee opening what appears to be a work-related email. These attacks play on the user's lack of awareness. They usually require someone to open malicious attachments, download and execute documents or scripts, or take some other action. For example, once a user clicks the "Enable Content" button to turn on macros in a malicious document ransomware can be downloaded and the attack process begins.

That's why employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware and how to report it. A training program that can utilize real-world attacks and provide a feedback system to report suspicious messages will better train users to spot malicious messages and reinforce positive behavior.

If anyone receives a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own. Payment may carry serious brand reputation and security ramifications and, in some cases, could involve breaching U.S. government sanctions. This decision should be weighed carefully by upper-level management with advice of legal counsel.

Our research shows that cyber criminals actively exploit human error and curiosity. It's part of a larger cyber crime trend—fooling humans into becoming unwitting accomplices in the quest to lock information and demand payment.

The most effective training teaches users about real-world attack techniques and campaigns. And it incorporates the latest threat intelligence to make users aware of the threats they're most likely to face. Phishing simulations can identify users who are especially prone to falling for ransomware and other attack tactics.

SECTION 3

During the Attack

You've been hit with ransomware. Now what?

While the best ransomware strategy is to avoid it in the first place, increasingly sophisticated attacks against the software supply chain have shown that even the best-prepared companies can be caught out. Ransomware may not even be the first malware payload to infect your system, as many ransomware gangs now prefer to buy access to targets already infected with Trojans or loader malware.

During an attack, you have short-term problems to resolve, like getting computers, phones and networks back online and dealing with ransom demands.

But a panicked response won't help—and may make things worse.

Isolate infected systems

The second employees see the ransomware demand or notice something's odd—such as suddenly losing access to their own files—they should disconnect from the network and take the infected machine to the IT department.

To prepare for this scenario, we recommend that you keep valuable data and systems separated so that a security issue on one system doesn't affect other systems. For example, your sensitive research or business data should not reside on the same server and network segment as your email environment.

We advise against having employees reboot their system. Only the IT security team should attempt a reboot, and even that will work only in the event that it is "scareware," or fake ransomware.

"Scareware" is malware that appears to be ransomware but isn't. It may lock the user's screen with a ransom demand and payment instructions, but the data is not actually encrypted. In those scenarios, standard anti-malware tools can help.

Knowing the difference isn't always easy. Determine the scope of the problem using threat intelligence and external incident responders or forensic analysts when necessary. While all ransomware is bad, some attacks are worse than others. Your response—including whether to pay the ransom—hinges on several factors.

Call law enforcement

Ransomware—like other forms of theft and extortion—is a crime. Nobody has the right to seize devices, networks or data, let alone demand a ransom in exchange for it. Notifying the proper authorities is a necessary first step.

Contact local or federal law enforcement right away. Special departments exist specifically to aid cyber crime victims, so do not be afraid to pick up your phone and call them. They are there to help you and may have access to decryption keys or information on payment recovery after the fact.

You should also contact your cyber insurance provider to see if you have ransomware coverage and under what conditions. They can help you coordinate your incident response and investigation.

Questions to answer during an attack

- What type of attack is it? Is this attack a secondary infection? Did it come from downloaders, remote access Trojans (RATs) or other malware installed on the infected machine or others on the network?
- Who in your network is compromised? How widespread are the infections? Is a threat actor actively scouting your network, exfiltrating data or ready to drop ransomware on other devices?
- What network permissions do compromised accounts or devices have? Ransomware may have been installed only after attackers had already moved laterally within the network or stolen credentials and other data.

Your answers should help network administrators scope the problem, devise an action plan and possibly curtail the spread.

Keep in mind that ransomware spreads quickly and often is a byproduct of other threats. If you see one infection, there are probably others that you don't see. Proactively look for other issues within your environment.

Restore from backup

The only way to completely recover from a ransomware infection is restoring everything from backup—backups that should be happening every day. This might come last in terms of steps to take once infected but should be first in terms of prevention.

Even with recent backups, though, paying the ransom might make more financial and operational sense. Restoring backups takes time and effort. And some businesses might not be able to afford the downtime.

Deploy your response plan

Depending on network configuration, containing the spread to a single workstation might be possible.

Best case scenario: a new computer is swapped out for the infected machine and a restore from backup is completed. Worst case: every network machine is infected. This will require a cost-benefit calculation that weighs the time and resources needed to restore the data versus simply paying the ransom.

If the ransomware has already reached your servers, isolate affected systems—that's where your network segmentation efforts can help contain the threat.

A big part of your response is deciding whether to pay the ransom. The answer is complicated and may require you to consult law enforcement and your legal counsel. For some victims, paying may be unavoidable (see "To pay or not to pay: ransomware's moral and legal dilemma").

Don't count on free ransomware decryption tools. Some security vendors offer free ransomware decryption programs. In some cases, they can help you to retrieve your data without paying the ransom. But most work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your strain of ransomware.

You may get lucky with a free decryption tool. Just don't make it part of your incident response plan.

To pay or not to pay: ransomware's moral and legal dilemma

Ransomware is bad enough in itself. But one of its especially loathsome aspects is that it forces victims to make a necessary but morally problematic choice. When you're under the gun of a ransomware threat, you don't often have the luxury of time to carefully weigh the moral nuances of paying up. The attack is here—now.

Paying up isn't just a repugnant but necessary evil. It actively funds the attacker who has just broken into your network and stolen your data. It marks you as someone with a vulnerable network and incentive to pay. And it enables the cyber criminal to bankroll future attacks.

But recent attacks highlight an uncomfortable fact: there isn't always a clear-cut answer on whether to pay.

No organization wants to be extorted, let alone fund criminal rings. Then again, many victims feel they have no choice. In some ways, it's the price to pay for having underfunded IT departments running unpatched or outdated software. There are still hospitals in the U.S. running Microsoft Windows XP on legacy devices. And the ransom demand is often a relatively small price to pay when lives are on the line.

At times, even the FBI has advised victims to "just pay the ransom." The agency officially discourages paying, but in 2021 advised Congress against considering a ban on payments.[36] Even if you do pay, the agency points out, you still may not get your data back. Or, worse yet, you may be forced to pay a second time in a double extortion scheme. This is not uncommon, as shown by the 41% of victims who paid additional ransom demands after their first ransom payment.[37]

36 Maggie Miller (The Hill) "Top FBI Official Advises Congress Against Banning Ransomware Payments." July 2021.
37 Proofpoint. "2023 State of the Phish." February 2023.

In 2020, the U.S. Department of the Treasury issued an advisory reminding American citizens and businesses that paying a ransom could involve violating sanctions or other financial regulations. The ramifications of this advice are still being worked out by insurers and incident response negotiators, but possible legal risk adds another layer of complexity to decision-making.

Since then, government agencies have added stronger incentives not to pay ransoms. In 2022, the U.S. Securities and Exchange Commission (SEC) proposed a new rule mandating that listed companies report data breaches and ransomware attacks within a specified time frame.[38] Shortly afterwards, the president signed a bill into law that also requires critical infrastructure operators to report ransom payments.[39] Additionally, the Transportation Security Administration (TSA)[40] and Federal Communications Commission (FCC)[41] recently published disclosure requirements. These new rules signal an effort to reverse the underreporting of ransomware attacks, which has become all too common. With more knowledge about current threats, organizations will be able to make better decisions about how to keep their employees, systems and data safe.

Meanwhile, the United Nations is discussing an international treaty aimed at strengthening cyber resilience.[42] And Europol has continued its "No More Ransom" initiative, a public-private partnership intended to help cyber attack victims rebuild their data files and decrypt without paying. More than 30 countries have banded together to attempt to disrupt the payment networks that cyber criminals use to launder money.[43] And some countries have proposed banning ransomware payments altogether.

Among the most notable proposed bans comes from Australia, where it was announced that the government is considering making it illegal to pay ransoms.[44]

Organizations must consider many factors when they're choosing the best course of action, including:

- Time and resources to get back online
- Responsibilities to shareholders to keep the business up and running
- Safety of customers and employees
- What criminal activity the payment will potentially fund
- Any regulatory liability that might ensue from providing money to a sanctioned individual or state

As with most complicated questions, no two organizations will answer them in the same way.

38 Paul Kiernan (Wall Street Journal) "SEC Proposes Requiring Firms to Report Cyberattacks Within Four Days." March 2022.
39 David Uberti (Wall Street Journal) "Fearing More Cyberattacks, Congress Requires Key Businesses to Report Digital Breaches." March 2022.
40 United States Department of Homeland Security. "DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators." December 2021.
41 Federal Communications Commission. "Chair Rosenworcel Circulates New Data Breach Reporting Requirements." January 2022.
42 United Nations. "A UN treaty on cybercrime is en route." April 2022.
43 Jonathan Greig (ZDNet) "More than 30 countries outline efforts to stop ransomware after White House virtual summit." October 2021.
44 Reuters. "Australia to consider banning paying ransoms to cybercriminals." November 2022..

SECTION 4

After the Attack

Regardless of the damage caused by ransomware, an attack reveals a security failure resulted in a device or network compromise. Now that things are back to normal, you have an opportunity to learn from the security breach and avoid future attacks.

We recommend a top-to-bottom security assessment, perhaps by an outside services firm, to find threats that may still linger in your environment. Now is also the time to take a hard look at your security tools and procedures—and where they fell short.

Cleanup

Some ransomware contains other threats or backdoor Trojans that can lead to future attacks. In other cases, a preexisting compromise opened the door to a ransomware infection. That's why wiping every device and restoring from a clean backup is a must. Look closer for hidden threats that you may have overlooked in the chaos.

Post-mortem review

Review your threat preparedness and response. How was the crisis plan executed? Can we improve networking configurations to contain future attacks? Can we implement a more robust email security solution? Should we take a whole new approach to cybersecurity in general?

Audit current security measures and ask if this is enough to combat today's threats. Turn this into a learning experience—because it very well might happen again.

Without figuring out how the ransomware got through, you have no way of stopping the next attack.

Assess user awareness

Many strains of ransomware rely on human interaction to deploy payloads, whether as a direct infection or later delivery by another kind of malware. Should current security measures fail and a fake "unpaid invoice" makes it onto the email server, a well-informed user is the last line of defense between a company, hospital or school staying online or becoming another ransomware statistic. Ensure your employees, staff or faculty are up to the task.

It might also be worthwhile to invest in phishing simulation tools to drive employee awareness, identify users who are especially vulnerable, and improve overall security. By mirroring real-world attacks and the latest social engineering techniques and attack methods, phishing simulations can help analyze and identify people-related security vulnerabilities ahead of actual attacks.

Education and training

After user awareness is analyzed, develop a curriculum to address employee vulnerability to cyber attacks, including lessons learned from previous encounters. Include regular follow-up training for people who are more vulnerable, heavily targeted or have elevated privileges to sensitive data, systems and other resources.

And your training program should integrate with your other cyber defenses to help people not just identify attacks but promptly report them.

Invest in modern defenses

Today's cyber attacks target people, not infrastructure. Seek out security solutions that take a people-centric approach to keeping them protected.

Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

At the same time, keep risky web content out of your environment. Web isolation technology can render web pages from suspicious and unverified URLs in a protected container within a user's normal web browser. Web isolation can be a critical safeguard for shared email accounts, which are difficult to secure with multifactor authentication. The same technology can isolate users' personal web browsing and web-based email services, giving them freedom and privacy without compromising the enterprise.

Identity is the next front for almost all ransomware attacks, especially Active Directory. If your team has the expertise, open-source tools can give you a view of the attack paths in your environment. But if you make changes in AD to cut off the attack pathways that you've identified, it's often difficult to model the impact on business applications. An identity threat defense solution can remove nearly all of those exposures and provide detection for those that you cannot address by reconfiguring AD due to the business impact.

Being proactive also helps. When you're looking to stop today's targeted attacks, you need advanced threat intelligence. Seek out a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them.

Next steps

As long as cyber criminals can find a way to make money from it, ransomware will exist in one form or another. The recommendations in this guide can start you on the path to dealing with ransomware before, during and after an attack.

Of course, the easiest way to combat ransomware is to stop it at the gates. That requires cyber defenses built for today's threats.

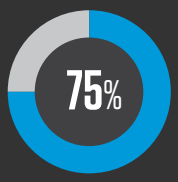
Robust cybersecurity is people-centric cybersecurity. It makes users more resilient through awareness training based on real-world attack techniques. It identifies and kills ransomware targeting your people. And it contains threats and helps you respond quickly and effectively when something goes wrong.

Why Proofpoint

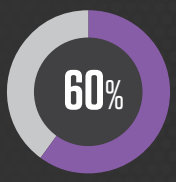
Every day, we analyze more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

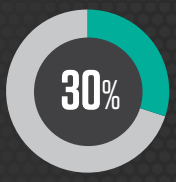
We are trusted by more than:



OF THE FORTUNE 100



OF THE FORTUNE 1000



OF THE FORTUNE GLOBAL 2000

8,000 ENTERPRISES

200,000 SMALL BUSINESSES

LEARN MORE

To learn more about how you can stop ransomware attacks, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0501-006-01-02 8/23