proofpoint.

E-BOOK

The 2022 Ransomware Survival Guide

What Every Organisation Needs to Know Before, During and After an Attack

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. With major incidents involving fuel,[1] food[2] and health infrastructure[3] in 2021 showing that no target is off limits, it's more important than ever to have a plan to mitigate risk and respond if your systems are infected with ransomware.

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- Many businesses have weak or outdated cyber defences and poor backup and recovery routines, making for a large pool of targets.
- Attackers are getting better at targeting and more sophisticated in their tactics.

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

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 opening an attachment or clicking a URL. That's why fighting ransomware requires a people-centric approach.

Consider this guide a starting point.

1 David Sanger, Clifford Krauss, Nicole Perlroth *(New York Times)* "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." May 2021.
2 Julie Creswell, Nicole Perlroth, Noam Schreiber *(New York Times)* "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business." June 2021.
3 Nicole Perlroth, Adam Satariano *(New York Times)* "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks." May 2021.

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

Update and patch

Keep operating systems, security software, applications and network hardware patched and up to date.

Invest in robust people-centric security solutions

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. These solutions also protect against other malware, typically delivered through email, that can install ransomware in targeted follow-up attacks.

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.

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 businesses 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)* "Judgement 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 getting computers, phones and networks back online and dealing with ransom demands.

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.

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.

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 defence. 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 defences

Today's fast-changing threat landscape requires security solutions that can analyse, identify and block—in real time—the malicious URLs and attachments that serve as ransomware's primary entry points.

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

Introduction

Ransomware has been around now for more than three decades, and in that time it has undergone several evolutions. When we last updated this report, ransomware numbers were trending down as businesses and security providers shut out Locky, the ransomware responsible for the threat's reemergence in 2016.

300% YOY INCREASE
in ransomware attacks as of early 2021, US government figures indicate.

That's changing. As of early 2021, US government figures indicate a new surge, with ransomware attacks increasing 300% year over year.[7]

Driving this change has been a shift in the cyber criminal ecosystem. 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.

This shift, coupled with the rising value of Bitcoin and other cryptocurrencies, has created the conditions for a ransomware epidemic.

Hitting the headlines

In the first six months of 2021, ransomware has gone from a cybersecurity headache to a crisis debated at the highest levels of government. Attacks on school districts, police departments and transport authorities demonstrated a growing willingness on the part of ransomware gangs to target public infrastructure.

Attacks on school districts, police departments and transport authorities demonstrated a growing willingness on the part of ransomware gangs to target public infrastructure.

Then in May 2021, attackers affiliated with the DarkSide ransomware group hit Colonial Pipeline, whose systems supply fuel to much of the US East Coast. The disruption led to shortages in several states as panicked consumers attempted to stockpile supplies. Eventually, Colonial Pipeline elected to pay a ransom of more than $4 million in Bitcoin to regain access to their systems.[8]

Later the same month, attackers associated with the REvil ransomware gang infected JBS Foods, a meat processor operating in several countries including the US, Brazil and Australia. Supplies of beef and other meat products were interrupted before JBS agreed to pay a ransom of $11 million.[9]

In early July, REvil was also revealed as the group behind a supply chain compromise of software company, Kaseya.[10] Since then, DarkSide and REvil have gone offline. But new ransomware operators are coming online all the time, and rebranding is not uncommon for gangs looking to evade the spotlight.

7 James Rundle and David Uberti *(The Wall Street Journal)*. "How Can Companies Cope with Ransomware?" May 2021.
8 Collin Eaton and Dustin Volz *(The Wall Street Journal)*. "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." May 2021.
9 Jacob Bunge *(The Wall Street Journal)*. "JBS Paid $11 Million to Resolve Ransomware Attack." June 2021.
10 Jonathan Vanian *(Fortune)*. "Everything to know about REvil, the group behind a big ransomware spree." July 2021.

With ransom demand amounts increasing and cyber attackers 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 situation. In the aftermath of the Colonial Pipeline incident, US President Joe Biden issued an executive order aimed at boosting the country's cyber defences. He challenged Russian President Vladimir Putin over his government's failure to prosecute ransomware gangs operating from within its borders.

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.

And in an increasing number of cases, victims are extorted multiple times: first for an encryption key to unlock their data and then to prevent the attackers from releasing or selling copies on the dark web.

The real-world costs

80%
of US businesses experienced a ransomware attack in 2020.

68%
elected to pay ransom.

Almost 80% of US businesses experienced a ransomware attack in 2020, with 68% electing to pay the ransom.[11] The financial consequences of an attack can be considerable, and ransom amounts are increasing every year.

In the first half of 2021, there have been confirmed payments of $4.4 million by Colonial Pipeline,[12] $11 million by JBS Foods[13] and a record $40 million paid by CNA Financial.[14] And these are just cases that reached the public eye. The true financial cost of ransomware is likely much higher than these figures reveal, as some businesses will inevitably look to deal with an intrusion privately.

But the business cost is not just limited to financial expense.

According to Coveware, a ransomware incident response consultancy, more than three quarters of ransomware attacks in the first half of 2021 involved a threat to leak exfiltrated data.[15] In 2020, the same company reported that 65% of victims threatened with a data leak opted to pay a ransom, highlighting the serious reputational risk attached to criminal data exfiltration.

11 Proofpoint. "State of the Phish 2021." February 2021.
12 Collin Eaton and Dustin Volz (The Wall Street Journal). "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." May 2021.
13 Jacob Bunge (The Wall Street Journal). "JBS Paid $11 Million to Resolve Ransomware Attack." June 2021.
14 Kartikay Mehrotra and William Turton (Bloomberg). "CNA Financial Paid $40 Million in Ransom After March Cyberattack. "May 2021.
15 Coveware. "Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority."

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 communications tools become inaccessible. The consequences can be even greater in critical sectors such as healthcare, as Ireland's Health Service Executive found when an attack by the Conti ransomware gang forced delays in treatment and cancellation of outpatient services such as X-ray imaging.[16]

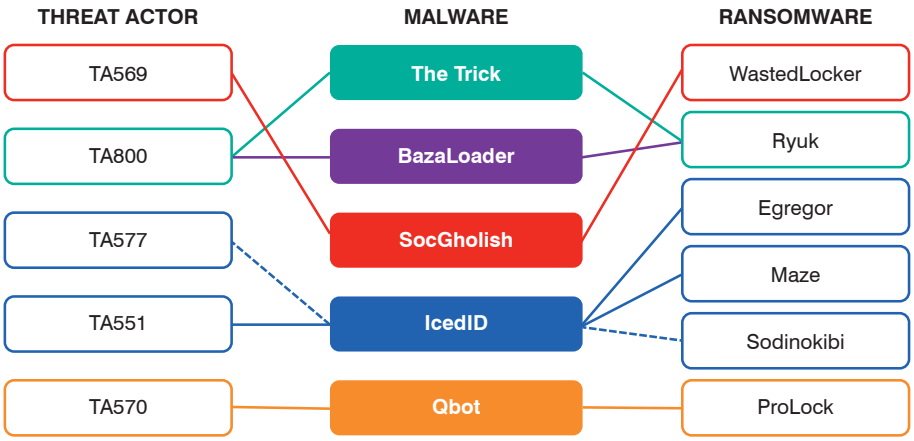
Ransomware and email

A large percentage of ransomware starts, directly or indirectly, with a phishing 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 five 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 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 isn't a simple 1:1 relationship between the initial access malware and the strain of ransomware distributed to victims. But researchers at Proofpoint and elsewhere in the industry have noted some prominent associations.



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 organisations, the first line of defence against ransomware is making sure they are protected from other kinds of malware.

In other words, block the loader and you block the ransomware.

16 Danny Palmer (ZDNet) "The human cost of ransomware: Disruption to Irish health service will continue for months." June 2021

In 2020, someone offered a Tesla employee $500,000 to install ransomware on the company's network.

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.

In August 2021, we tracked an email campaign offering employees $1 million for installing DemonWare ransomware at work. At around the same time, LockBit updated its ransom note with an offer to pay insiders millions of dollars for valid account credentials.

The DemonWare attacker made no attempt to deliver malware in their recruitment emails. Some advanced email security can detect these overtures based on other signals. Still, it's a good idea to educate employees to recognise these threats and report them promptly.

Where it comes from

Ransomware is distributed through a couple of 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
- 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.

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 can attack thousands of entities simultaneously using a variety of attack vehicles, opening the door for secondary ransomware attacks.

Conventional cyber defences 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 organisation's perimeter

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 organisations 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 other state and local governments.

For these organisations, 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.

Better targeting and more advanced tactics

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 using ransomware in the first stage of an attack, cyber criminals compromise systems with more robust, multipurpose malware.

Once they have a foothold, they deploy ransomware to devices of interest.

Bitcoin and other digital currencies

Since its debut in 2009, Bitcoin has been a boon to civil libertarians and cyber criminals alike. Payments can't be traced back to sender or recipient, providing an anonymous, friction-free way to transact private commerce.

By demanding payment in Bitcoin, cyber criminals get anonymity that makes collecting ransoms far easier than before. Earlier forms of ransomware might require a pre-purchased debit card. While this approach can bypass banks' anti-fraud measures, it's much more cumbersome on both sides of the transaction.

All major variants of ransomware require payment in Bitcoin. (See **"The Bitcoin money trail" on page 13.**)

An old and ongoing threat

To understand how insidious ransomware attacks are today —and how they can directly affect consumers— consider the attack on Garmin Ltd., a network service that distributes data to Garmin-powered smart watches and fitness trackers, among other devices.

Garmin Ltd. uses GPS technology to share data with fitness trackers such as those from FitBit and Apple. But such services were interrupted on 23 July 2020, when Garmin was the victim of a cyber attack that encrypted its online systems, including "customer support, customer-facing applications and company communications," Garmin announced in a news release.

Garmin was unable to provide many of its services because these services and those provided by their call centres were encrypted and couldn't be accessed by end users or the company. The services couldn't be decrypted until Garmin reportedly paid a ransom of $10 million to the attackers.

"A source close to the Garmin incident response and a Garmin employee confirmed … that the WastedLocker ransomware attacked Garmin," the technology news site BleepingComputer reported on 1 August.

Garmin said that after four days, it began rebooting its online services.

> "The Garmin IT department had tried to remotely shut down all computers on the network as devices were being encrypted, including home computers connected via VPN," BleepingComputer reported. "After being unable to do so, employees were told to shut down any computer on the network that they had access to."

BleepingComputer noted that the WastedLocker ransomware has been traced to a Russian-based cybercriminal group called Evil Corp. While the name might sound like a cartoon villain, Evil Corp. was sanctioned by the US Department of Justice in December of 2019 for its role in the Dridex malware incident and for using ransomware as part of other attacks, including Locky ransomware and their own ransomware strain known as BitPaymer.

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 recognised 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 at swiftly shutting down victims' accounts.

And as the value of Bitcoin has increased in recent years, peaking at almost $65,000 per Bitcoin, adding a possible extra financial upside for attackers.

In the aftermath of the Colonial Pipeline attack, the FBI revealed that they had recovered around half of the Bitcoin paid as a ransom. The agency has not been revealed how, and it's not clear whether such recoveries are repeatable.[17]

17 Katie Brenner, Nicole Perlroth *(New York Times)* "U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack." June 2021.

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. Most companies do this, but surprisingly few run backup and restore drills. Both processes are important; restore drills are the only way to know ahead of time whether your backup plan is working.

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.

Update and patch

Ensure that operating systems, security software, applications and network hardware are fully patched and updated. It sounds basic enough. But according to a recent survey, more than half of organisations say there's no easy way to track whether vulnerabilities are being patched in a timely manner. And respondents reported that updates vary wildly in terms of complexity and release schedule.[18]

But there are places to go to get a handle on patch management, such as the Center for Internet Security (CIS), a non-profit organisation 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.

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. Should you decide to pay the ransom, you'll need to map out an appropriate process that includes key executives, operational staff and legal counsel.

18 Ponemon Institute. "Today's State of Vulnerability Response: Patch Work Demands Attention." April 2018.

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 to 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 cloud security solutions

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.

Email: your most critical vector

Traditional legacy 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.

Because email is the initial infection point that leads to most ransomware, you need advanced solutions that protect this critical vector.

That means analysing embedded URLs and attachments to ensure no malicious content breaches the system. Cyber thieves 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. And email authentication based on the DMARC standard can stop attacks that rely on domain spoofing— impersonating your organisation's email domain to gain users' trust. Your email security solution should also protect against other types of identity deception, such as display-name spoofing and lookalike domains.

Protect your cloud accounts

Cloud-based email accounts are another prime vector for spreading malware. Cyber criminals can take control of users' cloud accounts to target other users within your organisation. Email accounts can be compromised in a few ways, including:

- Automated brute-force attacks, trying out countless username/password combination until something works
- Outside credential theft—knowing users often reuse passwords across accounts
- Credential-stealing malware
- Cloud controls

Securing users' cloud accounts is a critical part of protecting against ransomware attacks.

Finally, require remote users to connect to the internet through a corporate VPN so that they are protected by your cybersecurity defences wherever they are.

Make your people a strong last line of defence

Most malware infections begin with a single well-intentioned employee opening what appears to be a work-related email.

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 programme that can utilise real-world attacks and provide a feedback system to report suspicious messages will better train users to spot malicious messages and reinforce positive behaviour.

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 US 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.

These attacks play on the user's lack of awareness. They usually require people to open malicious document attachments, download and open or execute documents or scripts, or take some other action. Once users click the "Enable Content" button to turn on macros in a malicious document, for example, it can download ransomware and start the attack process.

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.

Talking tech: what US officials recommend

Beyond the top-level strategy laid out in this guide, the FBI also recommends these technical measures to head off ransomware attacks.

Audit and manage user privileges

Take a least-privilege approach to file, directory and network share permissions.

Users who don't need to edit a file, for example, should have read-only access. In many cases, users shouldn't have access at all. A cashier doesn't need access to the company's financial records. And a hospital CEO doesn't need to look at patient health records.

Give users only the level of access that they need to do their jobs.

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.

Use virtual-machine technology

Virtual-machine (VM) technology executes apps and even entire operating systems in an isolated environment.

Think of it as a software "detonation chamber." Running sensitive or unvetted code within a VM environment or VM container ensures that any security issues that arise are confined to that virtual environment—leaving other parts of the system untouched.

Keep systems and data segmented

Keep valuable data and systems separated so that a security issue on one system doesn't affect other systems. For example, sensitive research or business data should not reside on the same server and network segment as an organisation's email environment.

The US government's complete recommendations are available at **fbi.gov/ file-repository/ransomware-prevention-and-response-for-cisos.pdf.**

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.

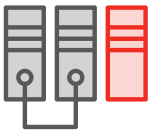
But a panicked response won't help—and may make things worse.

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. Do not be afraid to just pick up your phone and call them. They are there to help you.

You should also contact your ransomware insurer if you have coverage. They can help you coordinate your incident response and investigation.



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.

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

In those cases, what appears to be ransomware is better described as "scareware." 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 problem using threat intelligence. While all ransomware is bad, some attacks are worse than others. Your response—including whether to pay the ransom—hinges on several factors.

Ask the questions:

- **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 in 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.

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" on page 21**).

Don't count on free ransomware decryption tools. Some security vendors offer free ransomware decryption programs. In some cases, they can help you 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 ransomware.

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

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. Some businesses might not be able to afford the downtime.

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 organisation wants to be extorted, let alone fund criminal rings. Then again, many victims may 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 US 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 recently advised Congress against considering a ban on payments.[19] Even if you do pay, the agency points out, you still may not get your data back.

But in 2020, the US 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.

Another campaign to urge people to refuse to pay ransoms comes from Europol, the European Union's police agency. Its "No More Ransom" initiative, launched five years ago, is a public-private partnership intended to help cyber attack victims rebuild their data files and decrypt without paying.

The initiative has helped six million ransomware victims recover their files and avoid paying almost $1 billion in ransom. (The No More Ransom tools are available to everyone, not just those in the European Union.)

Organisations must weigh conflicting considerations when choosing the best course of action. These factors can include:

- Time and resources getting 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 organisations will answer them in the same way.

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

19 Maggie Miller *(The Hill)* "Top FBI Official Advises Congress Against Banning Ransomware Payments." July 2021.

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 defence 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 analyse and identify people-related security vulnerabilities ahead of actual attacks.

Education and training

After user awareness is analysed, 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 programme should integrate with your other cyber defences to help people not just identify attacks but promptly report them.

Invest in modern defences

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.

Focused, targeted attacks call for 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 defences 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.

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

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations 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.

0501-006-01-01 11/21