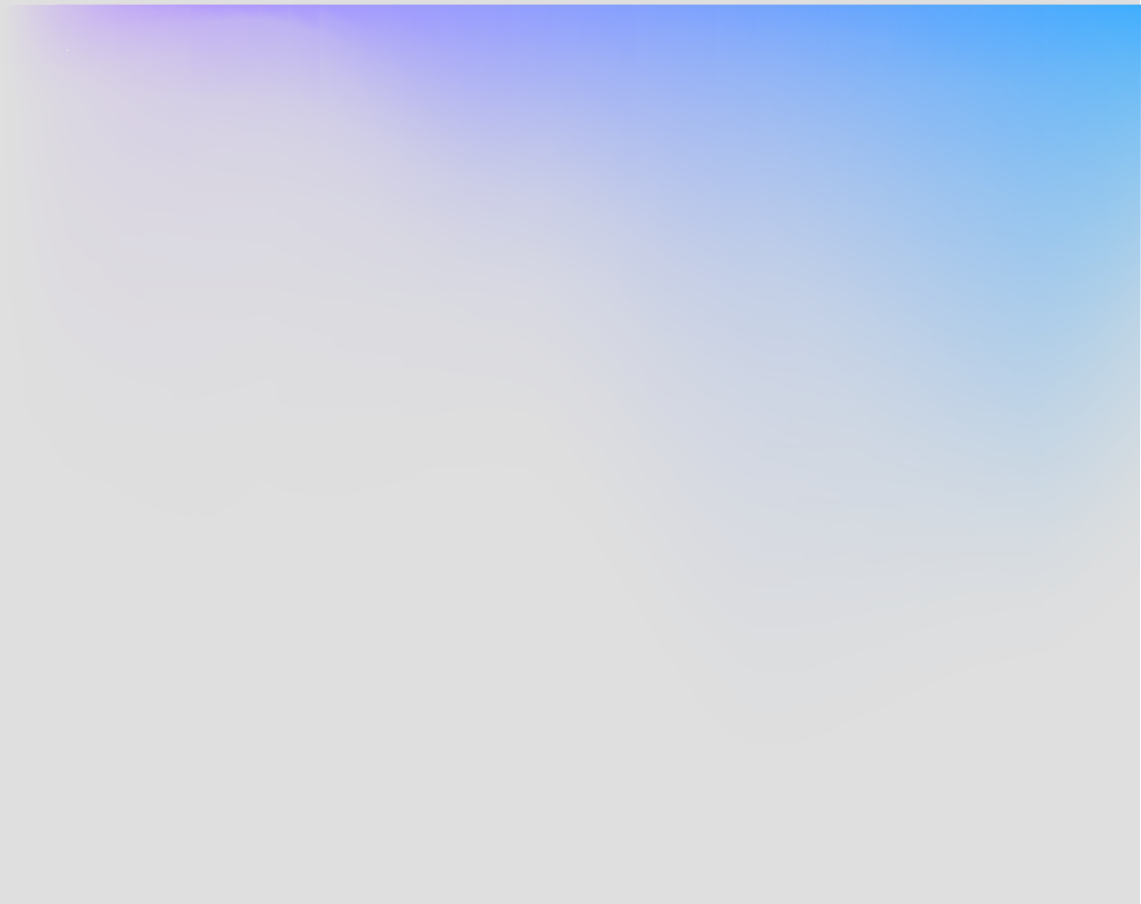
Definitive guide to ransomware 2022



IBM **Security**

Table of contents

Definitive guide to ransomware 2022

Executive summary

Ransomware is an online attack perpetrated by cybercriminals or nation state-sponsored groups who demand a monetary ransom to release their hold on encrypted or stolen data.

In the past decade, ransomware attacks have evolved from a consumer-level nuisance of fake antivirus products to sophisticated malware with advanced encryption capabilities that target primarily public and private sector organizations. While threat intelligence can help uncover what organizations may be considered primary targets at any given time, no single industry, geography, or size of business is immune.

As the footprint of ransomware keeps growing, so too does the amount of ransom demanded to release data. Ransom amounts that used to total only double digits have grown to seven-figure and eight-figure numbers.

USD 40M+

In even more extreme cases, attackers demand victimized companies pay as much as USD 40-80 million to have data released back to their control.

Ransomware has evolved along a third axis as well: the digital extortion business model. In this model, criminals escalate the attack in order to force payment from victims. If victims fail to pay within the allotted time, or opt to recover encrypted data through backups, criminals threaten to release confidential data publicly. Some attackers even auction confidential data to the highest bidder on the dark web. And in another twist, adversarial nation states sometimes blend ransomware with destructive attacks ultimately aimed at destroying and disrupting operations.

Ransomware is one of cybercrime's strongest business models today, pushing aside long-held staples like banking trojans, phishing, distributed denial-of-service (DDoS) and cryptojacking. Some criminals use those models as an initial stepping-stone to an eventual targeted attack. The ransomware crime model has harmed organizations across the globe, costing well into the billions of U.S. dollars every year. In an even darker turn, ransomware has begun reaping a toll on human life. These attacks that can impact hospitals and affect medical devices have come to be known as "killware" in the industry because of their potential to indirectly cause mortality.

As more ransomware attacks and variants rise every month, IBM Security® X-Force® believes ransomware will continue to threaten businesses in the coming years. This document provides guidance to organizations before and during a ransomware attack.

It’s designed to help organizations understand the critical steps needed to protect their business before an attack can penetrate their defenses and achieve optimal recovery if adversaries breach the perimeter.

The urgency of informed response

When a ransomware attack is discovered, the event can be jarring. Attackers still might be actively working on the attack when it’s discovered, and every second counts. As time passes, more data and files are encrypted, and more devices are infected — driving up both cost and damage. Immediate, yet methodical and informed, action must be taken.

As a first action, you should involve and allow your IT security teams to begin investigating and assessing the stage of the attack. Then, they should launch the incident response process that they’ve prepared to combat ransomware. If you have confirmed the incident and have a retainer contract with a third-party provider, it’s advisable to engage them at this point and get responders on site.

Other parties to consider contacting are federal law enforcement and regulators, depending on the local requirements for the geographies where your company operates.

About this document

This document is intended to be used as a guide to help organizations fortify knowledge and defenses against ransomware threats, or more rapidly remediate an evolving situation if an attack occurs. Distinct sections address phases both before and during an attack, with the most critical and time sensitive being in the initial response section.

If your organization is currently experiencing a ransomware incident, it's highly recommended you immediately review the Incident response: Containment section. Then, return to the remainder of this document for an overall background on ransomware attacks.

We mention several IBM Security X-Force resources in this document and include summaries of them at the end.

Definitions

Malware variants and versions
For the purpose of this guide, the terms malware "version" and "variant" have the following distinct meanings.

- The term *version* refers to the same malware program which encompasses newer or older versions of the same program with varying features.
- The term *variant* describes separate and different "families" of ransomware.

For example, there are several variants of ransomware that encrypt a user's files and then demand a ransom. These variants are commonly written by different people, known by different names by antivirus companies, and function differently but with the same overall goal. Each variant can have multiple versions, and versions are often upgraded over time to add features and capabilities.

Ransomware infections — a daily risk

IBM Security X-Force has seen a rapid increase in the number of clients who report being victims of ransomware attacks. Most cases of infection begin with unwitting employees being tricked by a well-crafted email to launch malware on devices attached to company networks.

While victims commonly receive ransomware through unsolicited email from a known or unknown sender as an attachment, there are other paths of infection. Ransomware can be injected into a user's browser session through a web browser vulnerability. Threat actors exploit these vulnerabilities using tools to compromise systems and plant "web shells" or "backdoors," or even remote access trojans.

More recent attacks also have featured a breach that started in the organization's cloud infrastructure and moved to the on-premises networks.

With an initial foothold in the compromised environment, attackers plot lateral movement, privilege escalation and the eventual deployment of ransomware on as many devices as possible.

End users: The first line of defense

End user or employee education must be a central element in any ransomware prevention effort. These individuals are often your first line of defense against attacks.

When executed, ransomware creates several telltale signs that an information system has been compromised (see the Incident response: Detection section).

> End users should know how to identify and where to report anomalies.

For example, suppose that an employee discovers a file that's been encrypted by ransomware, or the HTML or text file most leave behind to inform the user of payment instructions. It's essential that the employee not only knows how to recognize potential ransomware activity, but also who within your organization to contact for immediate assistance. Quick recognition and reporting of malicious activity can reduce the overall impact of an attack and ultimately save both time and expenses.

However, if employees are unable to recognize a security event or know how to report issues, the attack may continue uninterrupted and continue to spread throughout the network.

Not all ransomware is created equally

Like all malware, malicious codes vary in both sophistication and modularity. As such, not all ransomware codes are made the same. While some are ordinary and even obtained freely on open-source platforms and forums, others are highly sophisticated and operated exclusively by elite cybercrime syndicates.

Malware used in ransomware attacks began to evolve rapidly starting in 2013. New malware families were created, and an influx of specialized malware developers joined the ransomware arena from various threat groups. But while most modern-day ransomware uses effective and often irreversible encryption ciphers, not all ransomware is equally effective.

Much like any cybercrime operation, an individual group's technical abilities depend on the attackers' skill and sophistication. These variables translate into some attacks being impossible to break without a decryption key, while others can be reverse-engineered and overcome — potentially without having to pay the criminals. Attack effectiveness also depends on whether the attackers are able to exfiltrate critical data that they may attempt to use as leverage for ransom later.

Whether encrypted data can be freed with a decryption key or resolved through reverse engineering is an important element to understand in an attack.

Knowing this information can help defenders create an effective response and help forecast return to normal operations. It can aid decision-making efforts on all aspects of communicating with — or avoiding communicating with — the attackers.

Typical ransomware activity

While we noted earlier that not all ransomware is created equally, most codes perform a very similar list of actions when they land on a newly infected device.

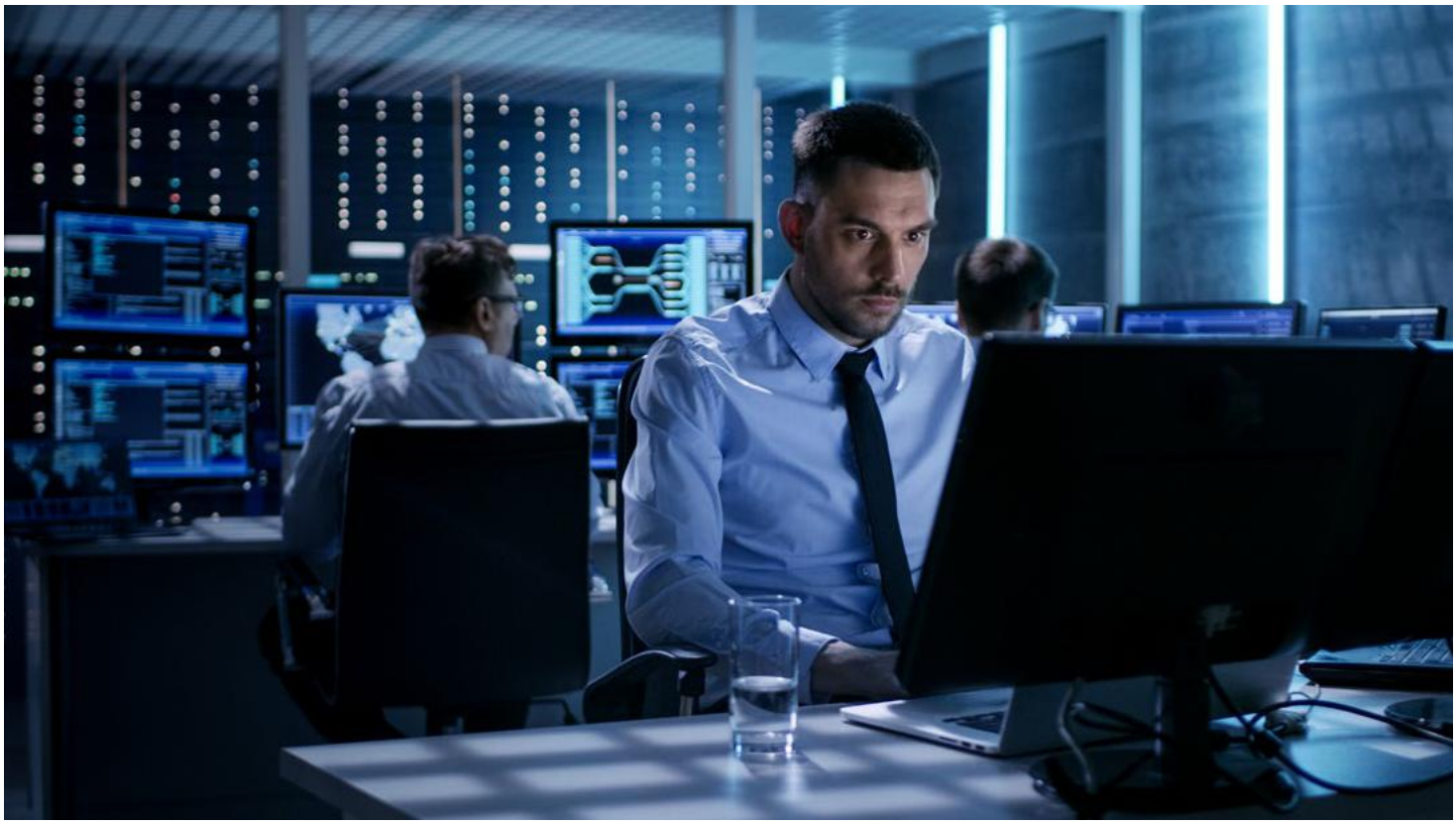
C2 communication
When a computer becomes infected with ransomware, the malware may generate network traffic by sending encrypted system information to a command-and-control (C&C) server (C2). However, communication with a C2 isn't necessary for the encryption process itself. Ransomware that must reach out to a C2 node to retrieve a key before beginning to encrypt can incur a higher likelihood of failing if it cannot connect to the C2. It can also be detected before completing its mission. Normally, ransomware contains the public key needed for encryption and uses it locally without fetching from a remote server.

Disable security and system restore, delete shadow copies
Another common action taken by most ransomware variants is terminating a list of hardcoded processes and services that may interfere with file encryption such as databases, security applications and backup services. Some variants also search for and attempt to uninstall known antivirus programs or other security applications.

Other typical activity is to prevent and disable system restore features that may be enabled by the operating system. Many variants will run commands to do one or more of the following tasks:

- Delete volume shadow copies
- Wipe free space
- Clear event logs
- Turn off services that aid in the recovery of a corrupted system

Since they often land on individual user devices, most ransomware variants are designed to encrypt files commonly created and utilized by users. The variants ignore and don't affect the types of files the operating system uses to keep the computer operational. The goal is to keep the computer functioning so the victims can opt to pay.



The file types targeted for encryption can vary within different versions of the same ransomware and across variants; however, most include the following categories of files:

1. Microsoft Office files (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf)
2. Open Office files (.odt, .ods, .odp)
3. Adobe PDF files
4. Popular image files (.JPG, .PNG, raw camera files and so on)
5. Text files (.txt, .RTF and so on)
6. Database files (.sql, .dba, .mdb, .odb,. db3, .sqlite3 and so on)
7. Compressed files (.rar, .7z and so on)
8. Mail files (.pst)
9. Key files (.pem, .crt and so on)

This list is by no means exhaustive. Some ransomware variants can target over 150 file types, and those can change over time depending on the attacker's motivation. In some attacks, ransomware will target very specific formats to capture an organization's critical files. The more critical the data encrypted, the more likely a victim is inclined to pay the demanded ransom.

Worming through — no administrative privileges needed

Ransomware is known to be very contagious. Attacks on individual machines quickly become systemic issues largely because, unlike other malware, most ransomware infections don't require administrative privileges. Instead, the malware relies on the permission level the most basic users would operate on their assigned networked device. Ransomware attacks that worm through networks are known to plant malicious code in corporate file share servers and use those folders to move to other user devices without additional effort.

Another way that ransomware gets staged throughout the network is with human intervention from the attacker's side. Often a threat actor will use offensive tools to move laterally,

abusing Cobalt Strike, for example. They may also heavily work with Windows tools such as PowerShell scripts and Windows Management Instrumentation (WMI). These actions should be hunted immediately and escalated accordingly when identified by security teams.

These factors make ransomware a viable threat to businesses where a large number of employees access networks daily.

Preventing ransomware attacks isn't easy, but it's possible to reduce and mitigate risk and to better detect and contain an attack if the network is infiltrated.

Digital extortion — the ransomware-induced data breach

Digital extortion is the most common ransomware attack model today. It's emerged over the past few years and continues to make headlines. This blended attack mode begins as a classic ransomware attack, demanding payment for encrypted files. But behind the scenes, attackers have already exfiltrated large amounts of data from the victim. If payment of the ransom is resisted, attackers threaten to expose the data or auction it online.

These ransomware attacks can quickly turn into a full-fledged data breach, with corresponding consequences on regulatory and reputational levels, encrypted data and hindered operations.

The extortive blended attacks can circumvent backup strategies because they essentially extort the victim into payment even if backups are in place. Blended attacks can put immense pressure on organizations to pay extortion fees. Still, many still opt to forego the option to pay and prefer launching response plans to recover on their own.

Ransomware — the destructive flavor

While most ransomware attacks appear to be designed for financial gain, not all attackers share these motives. In some cases, what can appear to be a ransomware attack is actually a destructive attack that's designed to destroy digital assets and data rather than eventually release them to their rightful owners.

Destructive attacks use malware to wipe system components, corrupt data and render enterprise devices inoperable. This type of malware made headlines as a tool used primarily by sophisticated nation-state actors, especially during the Russian invasion of the Ukraine in February 2022. At least two different wipers were deployed against Ukrainian organizations on that occasion.

Analysis of incident response data from IBM Security X-Force over the years has found such attacks are becoming more popular among cybercriminal attackers. Ransomware attacks including wiper elements increase the pressure on victims to pay the ransom.

The evolving trend of destructive malware attacks means that when preparing for ransomware attacks, you also should consider disaster recovery plans. Such plans should take into account the potentially disruptive impact to business continuity and critical operations.

Triple extortion — adding DDoS to the mix

A concerning ransomware extortion trend observed by X-Force in 2021 was the expansion into "triple extortion" tactics. In this type of attack, threat actors encrypt, steal data and threaten to engage in a DDoS attack against the affected organization.

This kind of attack is particularly problematic for organizations because victims can have their networks held hostage by two malicious attacks. Data is encrypted, rendering work nearly impossible, and networks are bombarded with junk traffic to impair operations. In the background, attackers add the leverage of having already exfiltrated confidential data that they threaten to expose publicly. These pressure tactics can put tremendous strain on organizations, especially as they lose data, money and goodwill with every passing hour.

The ransomware incident’s lifecycle

To describe the ransomware incident’s lifecycle, this document uses the method outlined by the National Institute of Standards and Technology (NIST). The process is further described in the NIST Computer Security Incident Handling Guide. The NIST periodically updates these documents.

Within the scope of an active attack, the following steps should be included:

- Preparation
- Detection and analysis
- Containment, eradication and recovery
- Post-incident activities

Each step is further detailed in the following sections.

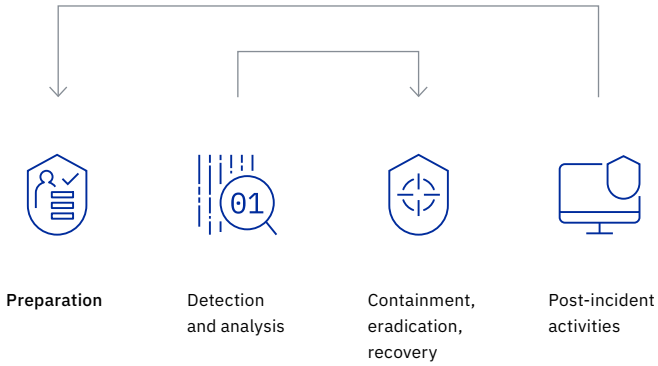


Figure 1: Incident response lifecycle (based on the NIST)

The preparation phase of the attack lifecycle involves preparing an organization for the following elements:

- The types of events and incidents they are most likely to encounter given their sector
- The systems they use
- Applicable key risk indicators (KRI) as they evolve over time

Incident response: Preparation

Detailing all aspects of the incident response process is beyond the scope of this document. But the following recommendations are provided as steps an organization can take to help prepare for and possibly prevent a ransomware incident.

Because of the rapid and continued evolution of ransomware variants and attack tactics, IBM Security X-Force notes that the preparation phase of the NIST incident response lifecycle is the most important.

When malicious ransomware files are detected, it's likely too late to prevent the attack from moving forward, since data has already been encrypted. However, there's still a chance to contain the attack and potentially even halt some parts of the attack entirely.

Success is heavily dependent on a well-rehearsed defense strategy and a preparatory plan designed specifically to thwart a ransomware attack. The following sections note some preparatory elements that should not be overlooked.

Role-based, end-user education
Proactive end-user education and training are critical in helping to prevent compromises of all types, since end users often first encounter security incidents. Training should emphasize identifying phishing, business email compromise (BEC) fraud, malicious spam (malspam) and by extension ransomware and malware incidents. Because users are the first line of defense against even the most protected environments, periodic training is recommended for end users in the following areas:

- The types of threats they are likely to encounter
- What actions they should take and avoid
- How and where to report issues

Ultimately, a security-conscious workforce is an achievable cultural asset that can serve as a cost-effective multiplier for the overall security posture of the organization.

Email as the prominent infection vector
Research shows that email continues to be a primary point of entry for ransomware attacks. According to the X-Force Threat Intelligence Index, phishing was the top attack pathway in 2021, with 41% of incidents X-Force remediated using this technique to gain initial access. Given its established use as a must-have tool for all businesses, phishing provides threat actors with a familiar and often lucrative way to reach and launch attacks on potential victims.

Educate users about email security often. Consider a campaign performing periodic, unannounced mock phishing exercises where employees receive emails or attachments that simulate malicious behavior. During such campaigns, generating metrics on the number of users clicking on suspicious attachments or links can help demonstrate both current awareness status and document improvement over time.

A successful education campaign requires generating a baseline of the number of users clicking on suspicious attachments or links, followed by educating the workforce. Thereafter, conduct a follow-up campaign to quantify the increased awareness within the organization. Test campaigns can be created in-house or contracted out to companies that specialize in these types of cybersecurity awareness campaigns.

Macros as an infection vector
Malware in general — including ransomware — is commonly distributed inside productivity files that are least likely to be blocked by email filters and security systems. Distributing malware through macros is an established but effective technique. Used by cybercriminals since at least the mid-1990s, this traditional attack method continues to pose an elevated risk to users and company networks.

In most cases, malicious code is hidden inside common work tools, such as Office suite documents or spreadsheets. To lure users into enabling the code to run, malware is concealed in macros that will launch scripts without the users' understanding of what is happening in the background. When users open the document, they're encouraged to "enable macros to see more information." The macro in turn is set to use PowerShell scripts, fetch additional payloads and use tools that can bypass security controls during transit.

While macros can be enabled in trusted workflows, they don't have to be enabled for all activities. Disabling unnecessary macros can help establish an additional layer of defense and help deter potentially risky macro enablement.

Of note, in 2022 Microsoft announced that it will block internet macros by default in Office. This change will help curb some of the potency of malicious macros, but awareness and controls will still be necessary to mitigate risk.

Misconfigurations as an entry point
The way organizations manage identities, permissions and their active directory continue to impact how they're breached. Misconfigurations discovered by security teams before attackers find them is the optimal scenario, but they're often overlooked.

Best practices include the following activities:

- Holding continual user education about the risks of macros in email attachments
- Providing stricter notification about macros to help users self-identify risky behavior
- Ensuring group policies are current
- Blocking macros from running in Word, Excel and PowerPoint documents that come from the internet

One example X-Force incident response teams encounter is setting web-based access to the Active Directory Manager and then missing the control that keeps the interface private. The interface is thereby exposed to the internet, which can allow an attacker to find and use the interface as an entry point to the organization.

Never keep a default password
Changing default passwords seems elementary, yet it's sometimes overlooked even on important assets, systems and interfaces. This little-noticed misstep can grant adversaries easy entry and the ability to take over a pivotal point of access.

Make sure all default passwords are changed and run a regular check across the infrastructure to confirm nothing was skipped or overlooked.

Deploy multifactor authentication whenever possible
Passwords are probably one of the easiest secrets to steal and are found in great abundance in breached records online. Using password-only protection isn't considered secure. Deploy multifactor authentication (MFA) across every possible login system to ensure that stolen passwords or overlooked default login credentials aren't readily usable to attackers.

X-Force analysis of attacks across different geographies shows that a more widespread use of MFA could help drive down BEC incidents and the successful use of stolen credentials.

Strip and prohibit attachments with executables from email
Most organizations configure email servers to prohibit sending or receiving emails with executable files as an attachment. This setup is one reason why attackers opt to send emails with a compressed archive attachment that conceals executable malware.

While organizations often configure their email gateways to scan inside compressed archive attachments, they don't necessarily strip or remove the executables. If an antivirus scan doesn't detect the executable as a threat, then it will eventually make it to the user's mailbox and to the endpoint. This setup enables sophisticated malware to bypass controls and allow attackers to plant an initial foothold.

It's possible to mitigate the risk of attachments getting through email controls. Do so by configuring the email server to strip any executable file, including files within archives that aren't password protected and that have an EXE, COM or SCR extension. Also, consider stripping .JS extensions before allowing delivery to the user's mailbox.

Some organizations have taken the step of automatically quarantining all Office document attachments that contain macros. Additionally, some enterprises have gone even further and quarantined all attachments, regardless of type, and then held them for approval and release to the end recipient.

One potential solution for handling Office documents is to allowlist trusted (signed) macros and block all others. In scenarios where new business document macros need to be allowlisted, this activity should be change-managed to ensure that a full audit trail exists. Taking this action can minimize the risk of misuse by malicious insiders.

Maintain current antivirus and endpoint protection
Endpoint antivirus solutions aren't the sole protection mechanism for threat detection. Still, they should be the initial mechanism and deployed to all users across the organization.

Organizations should ensure antivirus solutions are updated with the latest virus definitions to optimize their effectiveness. Ransomware is constantly evolving and changing to avoid detection. New versions appear daily and often go undetected by common corporate antivirus products for several days, which can allow attackers to elude detection and gain a foothold in the organization.

Organizations should consider using designated antivirus products for different purposes: one antivirus product for desktops, a second for servers and a third for the email gateway. This strategy can provide optimum coverage for emerging threats that may not be detected by one antivirus solution but may be detected by another.

Consider additional endpoint protection solutions that don't rely on signatures, but instead detect suspicious behavior and untrusted applications.

Restrict execution of programs from 'Temp' folders
Malware commonly uses 'Temp' folders as the initial execution point, and ransomware is no different. When possible, use Group Policy Objects (GPO) or Software Restriction Policies (SRP) to restrict the execution of any program from generic 'Temp' folders and within 'Temp' folders in a user's profile, such as **"c:\users\<user>\appdata\temp."**

For example, most ransomware initially executed tries to copy the malicious payload to the user's 'Temp' folder to continue the execution chain. If that folder were blocked, the initial malware infection could be hindered.

4 out of 5

Number of top vulnerabilities exploited in 2021 that were new [1]

A more robust solution is Windows AppLocker. This tool can disable executables from not only temporary folders, but also from other nonstandard folders such as **%AppData%** or **%LocalAppData%**, which are used by many malware and ransomware families. Conversely, most legitimate, commercial professional software doesn't use these folders to launch programs.

Hone vulnerability management
Attackers that aim to plant ransomware in IT networks often use zero-day vulnerabilities to gain a foothold within a network. Zero-day vulnerabilities can be a difficult attack vector to monitor as this activity continuously emerges with new exploitable issues — sometimes daily.

The X-Force Threat Intelligence Index revealed that the number of incidents caused by vulnerability exploitations rose 33% from 2020 to 2021. Four out of the top five vulnerabilities exploited in 2021 were new vulnerabilities.

In many instances, security teams often waste time and resources remediating vulnerabilities that pose minimal risk to their organization, while high-risk vulnerabilities go unattended. As a result, businesses are accumulating more and more "debt" in the form of unpatched vulnerabilities that can directly impact their organizations. And just as every debt expires, so can businesses lose control of their exposure to cyberattacks without proper vulnerability management.

Identifying and prioritizing the most critical vulnerabilities requires a broader, more scientific and automated approach. This approach must include correlating threat and vulnerability data from a variety of sources, identifying vulnerabilities that are actively being weaponized and ranking the most severe vulnerabilities for priority remediation.

Maintain an aggressive and current patch management policy
Threat intelligence reveals that attackers using a large variety of malware types, including ransomware, are quick to find and implement zero-day vulnerabilities as part of their overall malicious game plan.

While zero-day vulnerabilities can appear often, in most cases patches are also issued relatively promptly. Organizations should adopt an aggressive patch management policy, especially with browser vulnerabilities such as Adobe Flash and Java that are used by a large population of employees. Patches should be pushed automatically where possible and applied in a timely manner. In cases where a patch cannot be applied to a high-risk issue, measures such as segregation consideration, mitigating controls and compensating controls should be put into place to minimize potential exposure.

Increase DNS visibility, sinkhole and web filtering capabilities
In the case of ransomware, initial domain name server (DNS) resolution by the malware sometimes relies on its operator's domain generation algorithm (DGA). This setup makes identifying and blocking known bad domains more difficult, since the malware can generate and use thousands of different domain names to reach the C&C server.

Nevertheless, good visibility into the corporate DNS can be extremely helpful when working on an incident and can provide an early warning system. The ability to search and monitor DNS requests allows security teams to see patterns, such as frequent DGA-style DNS requests.

Organizations should also consider implementing a DNS sinkhole capability rather than outright blocking specified Internet Protocols (Ips) or domains at the egress gateway. Using a sinkhole allows the organization to redirect domains and IPs to a specific internal server that can provide advisories to users who attempt to go to blocked sites. The sinkhole can also provide real-time notifications when computers attempt to reach risky domains.

Another helpful control that organizations should consider implementing is a reputation-based web filtering capability. Keeping track of IPs on block lists, domains and sites in general is a never-ending job. Next-generation firewalls and proxies rely on real-time reputation feeds that crowd source intelligence information and help protect organizations by implementing known bad destinations quickly. This activity provides rapid blocking capabilities when sites are discovered as having malicious content.

IBM is a Quad9 partner. Quad9 is a free, recursive, anycast DNS platform that blocks known malicious domains, preventing computers and Internet of Things (IoT) devices from connecting to malware or phishing sites.

Enforce least privilege principles
Since ransomware targets common user files on the local system and on network shares, X-Force recommends that organizations apply least privilege methodology to file access on company networks. With least privilege principles in place, admins can grant minimal permissions necessary for each user, based on what's required for their daily work.

Since an infected computer operates with the permissions of the user currently logged on, it can only traverse and encrypt files to which it has read-and-write access. If a user doesn't require read-and-write access to various network shares, security teams should minimally consider removing write permissions from locations where access isn't required on a regular basis.

A common misstep X-Force incident response teams have seen is security teams that allow local users to run as administrators on their devices. Granting this permission level allows ransomware to perform more malicious actions on the device and what that device can connect to, augmenting potential impact. Removing local administrative privileges limits human error and malicious actors alike.

Disabling Flash
Adobe Flash has been a well-documented infection vector for ransomware. Some of the most popular internet browsers have already taken steps to block Flash by default due to mounting security flaws. Because of the risk posed by Flash, X-Force recommends that organizations consider disabling Flash by default throughout the organization.

Should a business case exist for select users to use Flash, users may benefit from additional safeguards, such as dedicated high-risk network segmented from the organization. While disabling Flash won't remove all risk from Internet activity, the change can help decrease an infection vector that attackers often use.

Flash End of Life (EOL) occurred at the end of 2020. As Flash isn't being distributed or updated by Adobe, discontinue usage to limit the risks that it can produce.

Consider disabling Windows Scripting Host
The use of JavaScript or VBScript by ransomware and other malware has increased over the last few years. Malware authors frequently use scripting because Windows Scripting Host (WSH) is enabled by default on all Windows systems. But while malware authors like this feature, most organizations don't use it, or use it sparingly in legitimate daily activity.

Scripting is a risky ability that can widen the attack surface for ransomware. That development can lead to higher chances of a malware script being successful and starting the ransomware infection cycle to its file-encryption conclusion.

Some of the malicious scripting possibilities can be centrally prevented through Group Policy. Create the following registry key and value to disable:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings\` `Enabled` and set the `Value data` of `Enabled` to `0`

This action can help limit ransomware or other malware that might attempt to use JavaScript or VBScript to run an infection routine. Instead of running the script, the user will see a WSH notification on screen warning them regarding scripting being disabled.

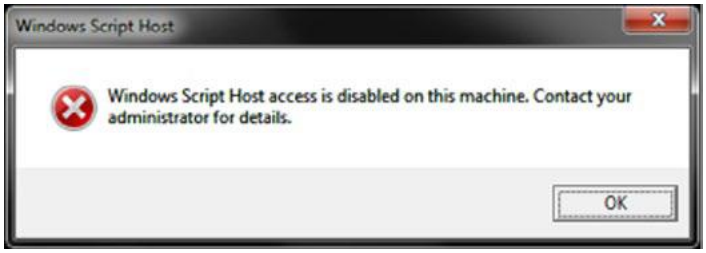


Figure 2: Windows Script Host disabled message

Note that disabling WSH will prevent users from running all scripts, including VBScript and JScript scripts, that rely on WSH. If scripts are required for daily work, other controls should be considered.

Hire a hacker
To minimize the possibilities for attackers to find ways into your networks, organizations must continually work to find and fix exploitable vulnerabilities that impact their most important applications, networks, hardware and people.

We recommend scoping and testing your environment for flaws and weaknesses that might let a criminal gain access. Include specialized testing as needed for ATMs, blockchain, IoT, automotive and cloud platforms, to name a few.

Develop and rehearse an incident response plan

An incident response plan enables companies to act quickly and effectively during a stressful situation of threats, disruption or disaster that can affect the organization's operations on all levels. Incident response plans specifically address situations that threaten digital assets and access to data.

A plan is created so that response is thorough, and when issues do arise, confusion and panic-induced decisions are minimized.

The methodology of an incident response plan should include the obvious stages of detection, containment, eradication and reestablishment of operations, but it shouldn't end there. After the incident, a root cause analysis should guide a lessons-learned phase that allows the organization to continue to mature the plan and fine-tune the future actions.

This document goes into further detail on the stages of **responding to a ransomware attack** based on the NIST framework. For details on creating your first plan, refer to the NIST guide. Alternatively, organizations can also opt for the SANS framework and handbook.

Whatever plans are in place, no matter how detailed they can seem, teams running plans must rehearse to understand how to launch and carry out response activities.

Management should also be well versed on communication. They should know the following procedures:

- How to respond to media and stakeholder questions
- What are the regulatory communication requirements and timelines
- How to employ an effective leadership style during an incident, keeping in mind that often the entire organization is affected — not just IT

Tabletop exercises (TTXs) are a good way to begin. However, to be able to validate a response plan under pressure, drills must cross into the physical realms of everyday operational activity as much as possible. A rehearsed team can function more effectively during an actual event, and rehearsals can help teams improve over time.

If your organization requires assistance at any stage of the plan creation, TTX or plan drilling, our team of experts is here to help. Contact the IBM Security X-Force Cyber Range for more information.

Incident response: Detection

The way an organization first detects a ransomware infection can vary widely. However, in most cases an employee will find it impossible to access files, see a ransom note, or notice that a certain service is no longer accessible.

The first goal is to contain the spread of the infection as soon as possible and isolate the infected systems, thereby minimizing the risk to the larger organization. This activity also helps stop any ongoing encryption processes that may still be underway. Ending these processes reduces the damage to the organization and the effort needed to restore access to data, systems and business operations.

We have uncovered common discovery scenarios through our response engagements while helping IBM Security clients deal with ransomware attacks. Those top scenarios are listed in the following sections.

As you read the scenarios, note that just because an organization identifies one host that is infected or is responsible for encrypting files doesn't mean that others haven't been affected. If just one host within an organization is found to be infected, it's highly likely that additional hosts are also infected. This possibility can occur because the same vulnerability may exist throughout hosts across the entire enterprise.

If you identify an infected host that is responsible for encrypting files, especially on a network share, monitor the shares very closely after you take the infected host offline. You should take this action because other infected hosts can continue the encryption process.

Scenario one: A network user attempts to access a file on a network share and finds it encrypted
Suppose users attempt to access a shared folder and find encrypted files in that location. This scenario presents the most potential risk to the organization. In this case, a user is accessing network shares on an infected computer somewhere on the network. Operating with the user's permission level, the ransomware goes through the network share and encrypts all the files to which the user has access as it runs through the folder.

In a larger organization, the number of files the user can access could be extensive, exposing several hundred thousand files to encryption, theft, or both. A large network share could take days for the ransomware to encrypt, but the process can nonetheless begin and run for some time before it's identified. This phase can be detrimental and harder to detect, especially since the victim computer doesn't yet display a ransom message.

To contain initial infection, it's extremely important and time sensitive to find the infected computer or computers. Narrowing down the infected user or users is most commonly achieved by looking at file ownership permissions on the files that have been encrypted.

It's also possible to examine the ownership permissions of new files that were created in each folder, notifying users that the files have been encrypted. The new files will commonly inherit the user's permissions under which the ransomware was executing, showing the file owner's name as the user account that initially became infected with the ransomware.

> Once users are identified, their devices and access should be disabled to halt the encryption process in the shared location.

Scenario two: User attempts to access a local file and finds it's encrypted

Imagine a computer becomes infected and a user finds files on the local system that are encrypted and inaccessible, but the user hasn't yet received an on-screen ransom message. Most ransomware variants leave a text file or HTML file in each folder they encrypt that informs the user the files have been encrypted and are being held for ransom.

In this scenario, it's likely that the encryption process is already in progress but hasn't yet completed its cycle. The user simply attempted to access a file and inadvertently discovered the encryption.

In this case, the victim computer should be shut off immediately. It's likely that the malicious process is active and still going through the various folders on the local and possibly network drives, rendering them inaccessible.

> Don't reboot or restart an infected system.
>
> The infected system should be hibernated and disconnected from the network immediately and IT security staff should be notified.

The system can also be turned off, but hibernating the machine may make it possible to find decryption keys that some ransomware variants keep in memory. Also, instruct employees to avoid rebooting a machine, as that action can reinitiate the ransomware's encryption process and simply run it again.

Scenario three: User received a ransom message on their computer

Here, employee devices within the organization silently become infected and begin encrypting all the user's local files and the files the user may have access to on network shares.

When the encryption process is complete, a message displays on the infected computer's screen notifying the user their files have been encrypted and providing a method to pay the ransom.

The text of a message displayed to the user varies for each ransomware family but can often look similar to the following example. The sample note is from the Ryuk ransomware gang, which was responsible for many 2019-2020 attacks on organizations across the globe.

Beyond notifying users that they're infected and helping security teams realize an incident is occurring, the message displayed can help determine which ransomware variant has been used to attack the organization.

Any displayed messages should be captured by taking a screenshot or photo with a mobile device and kept as part of the forensic information collected about the incident.

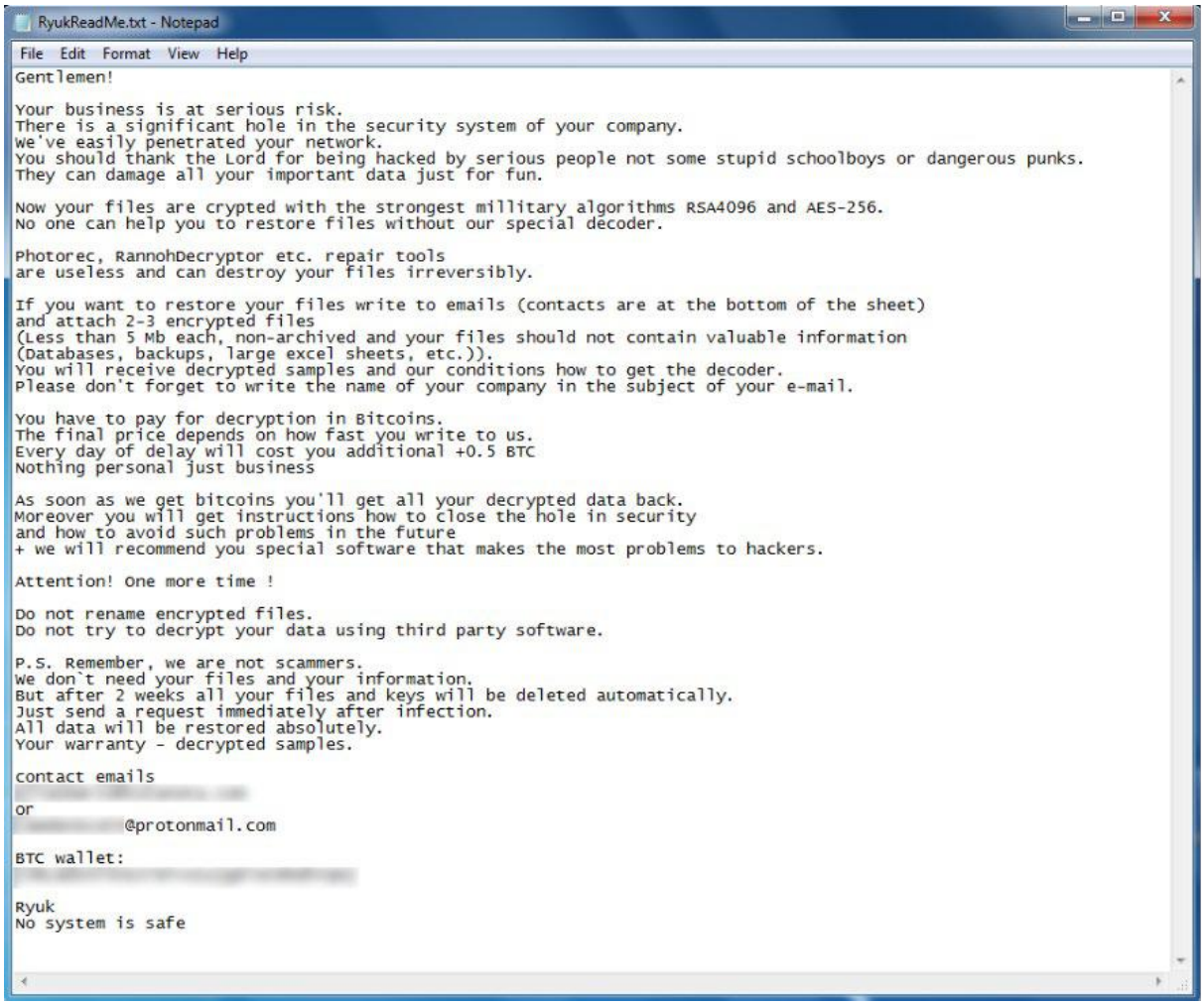


Figure 3: Sample message from ransomware attackers – in this case, Ryuk

Scenario four: massive file manipulation alert
Another way for security teams to become aware of an ongoing ransomware situation is seeing file manipulation thresholds cross significantly beyond their normal daily records. An alert of this sort would typically come from a security information and event management (SIEM) solution where corresponding rules have been set up.

The next step is the analysis phase.

Incident response: Analysis

The **Analysis** phase largely focuses on the two following areas:

1. Identifying the specific variant of ransomware in action
2. Determining how the malware entered the organization, also known as root cause analysis

Malware identification
When embarking on an analysis phase of an incident, it's essential to identify the specific variant of ransomware that compromised the environment before advancing to the containment phase.

For example, some versions of ransomware can use lateral movement features while others cannot. Knowing the capabilities of the specific ransomware code infecting an environment influences both the containment and eradication efforts.

Determining the variant can be complicated. X-Force recommends organizations consult internal subject matter experts or access external professional assistance such as a security services provider to help determine the variant and group behind a ransomware infection.

Initial root cause analysis
An abridged level of root cause analysis (RCA) should be performed to help the security team understand how the ransomware entered the digital environment.

While a formal RCA can wait until the post-incident activity phase, an abridged RCA can help the organization plan for and enter the containment phase. Without an initial RCA, the infection cycle is likely to repeat itself. It's also important to perform the initial RCA before the recovery phase. Otherwise, an organization could expend a large amount of time and effort recovering files only to see them re-encrypted again.

The following areas are some common entry points:

– Email
– Browser exploitation
– Other vulnerabilities

Email entry point
Two of ransomware's most common entry points into an organization are through unsolicited email with an attachment, or through web browser vulnerabilities that can attempt a drive-by download infection.

If an employee receives an unsolicited email containing ransomware, the organization should quickly search to identify other, possibly unopened, emails in additional employee mailboxes. These emails should be immediately extracted and purged to prevent them from being opened.

Drive-by download entry
Web browser vulnerabilities are a little more complicated to determine, but an initial RCA could rely on the organization's patch management infrastructure. A proper analysis would help identify what initial website caused the infection, allowing the organization to block access to that site from its networks.

While blocking the identified malicious site is a first step, it won't protect employees who are mobile and not blocked by the organization's firewall rules outside the local area network (LAN). Moreover, other sites could be spreading the malware at the same time or shortly thereafter.

Exploitation and manual infection
Another way that ransomware-wielding attackers get into organizations is by exploiting specific software or server vulnerabilities. These attackers plant ransomware manually in key areas on the network to infect as many devices as possible. In some cases, the malicious process can be set to start at a specific time. Criminals may set the start time on a weekend or holiday to reduce the chance of real-time discovery by employees or security staff.

X-Force recommends using internal incident response subject matter experts (SMEs) or an external third-party SME to assist in a proper root cause analysis.

Incident response: Containment

The containment phase is a critical part of the response plan. When a system is identified as potentially having ransomware, the computer should immediately be removed from your networks, including wifi connections. The computer either should be shut down, or ideally hibernated to assist in forensic and sample analysis — while minimizing the risk of the ransomware continuing the encryption process.

Failure to quickly isolate infected systems from the network may increase the impact from the incident. In this situation, you're allowing the malware to continue to encrypt more files on the local system or network shares and increase your recovery efforts.

Run endpoint detection and response (EDR)
Security automation is critical for any attack, especially for ransomware infection.

Your organization should have an endpoint detection and response (EDR) solution in place beyond basic antivirus protection for the following reasons:

- EDR can help detect an attack in its earlier stages. Sometimes that can mean detecting the virus in the first few days, allowing you to reduce the impact to the infrastructure.
- EDR can help quarantine infected devices completely, keeping them powered on but disconnected from the network. This way, infected devices retain important forensic data but can't continue to cause damage outside the local system.
- EDR can help with forensics further in the recovery cycle.

If you don't already have and regularly run a designated EDR solution, your organization needs to deploy an EDR at the onset of a ransomware attack. This activity also can be done by your external service provider, if you have incident response experts available to assist.

Last resort containment — terminate access
If you cannot quickly determine the source of the ransomware infection and where the encryption process originated, consider **taking the file share or shares offline** as a last resort. This action can help minimize risk and impact to the business.

The file servers don't need to be shut down, but all access to the file shares should be terminated — remove the share, restrict by network or host-based firewall ACL and so on.

It's not recommended that you change permissions on the files within a shared location. Depending on the number of files, permission propagation could take hours and would allow the encryption process to continue during that time.

If you use Microsoft Common Internet File System (CIFS) protocol and Server Message Block (SMB) protocol on other operating systems, including UNIX, Linux and so on, protect these as well. This action can help greatly reduce the chance of these shares being encrypted, as ransomware can exploit these protocols to move through networks and find more places with data to encrypt.

Incident response: Eradication

The eradication phase involves removing the ransomware from infected systems across the organization. Depending on the scope of the attack, this operation can be lengthy and may involve user devices and more pivotal machines and services the attackers managed to impact.

X-Force recommends that any system that has been identified as infected should be rebuilt from a trusted source. Rely on trusted templates and settings that are kept safely for cases like these infections.

Additionally, root cause analyses may reveal that the ransomware infiltrated the organization through email or mechanisms that other users can access. Those mechanisms should be examined and handled with the following steps:

- If the RCA revealed the malware initially arrived through an email message, the organization should search and purge all existing messages still pending within the mail store. Also, consider isolating any systems that received the email or opened the email until you verify that the ransomware wasn't executed on those systems.
- If the RCA revealed that the ransomware arrived through a web browser exploit, those websites should be blocked and monitored. Then you should assess the need to update or remove any vulnerable browser components.
- Passwords for all affected users should be changed as a precaution. This step should be taken carefully and strategically to avoid alerting the attackers. It's likely attackers have a number of credential sets and may attempt to use them and pivot the attack if their initial access is suddenly revoked.

Incident response: Recovery

When an organization has contained the ransomware and identified the root cause of the infection, there are several considerations to examine when beginning the recovery phase.

It's very important the organization complete the containment and identify the root cause of the infection before beginning the recovery process.

Patch vulnerabilities
If the RCA discovers that the attack was a result of vulnerable systems, those will have to be patched to prevent future attacks. If those systems cannot be patched, then segregate them, and ensure compensating controls are in place in order to minimize exposure risk.

Restoring data from backups
X-Force recommends organizations initially rely on their internal backup infrastructure to restore affected files before other options are considered.

This requires that a backup process already exists for the affected data. This process should include an analysis of the frequency and completeness of the backups to ensure complete restoration of the data.

It's important to verify the status of backups at the time of required recovery. If the attackers have been in the networks for months encrypting the backups, this status can mean that the backup option is no longer a valid choice. No backup option also applies if files have been silently encrypted and then backed up over time.

Attackers who remain silent in networks for long periods of time also can plant persistence mechanisms in the backups. This tactic ensures they can return to threaten the organization if a ransom isn't paid. A best practice for backups is using redundancy and keeping backups checked and segregated or offline. This practice can help limit the potential for tampering.

In cases where malicious encryption impacts a network share, there's still a chance that several of the most recent backups may contain partially encrypted files. For example, suppose an organization's file share is backed up daily, but an infected employee's device takes five days to encrypt everything on the file share before discovery of the attack. This situation means the last five backups are likely to contain files that have previously been encrypted.

You should have a reliable backup process in place that uses industry best practices. These methods include ensuring that local backups are kept and backups are archived to removable media, such as tapes, optical disks or removable hard disks, and to cloud-based resources.

Simply relying on local disk images, replication and other local network backups may not be sufficient. These can be encrypted by ransomware as well. Also, the backup could run after the files have been encrypted by the ransomware, rendering the backup useless for the purpose of internal recovery.

Can encryption be reversed?
Fully restoring files from backups may not be possible. In these cases, organizations may look for ways to break the encryption without paying the ransom, or perhaps locate decryption keys on infected systems. While both can happen, it's rare for either of these options to succeed.

Knowing the variant and version of the ransomware infection may help determine options. It can also aid the recovery phase and inform decisions about how to approach recovery and the consequences of each potential route.

The first way to approach encryption reversal is to work with a subject matter expert who can potentially offer insight into the malware variant and the recovery possibilities.

A cyber crisis management plan
While ransomware attacks are highly disruptive internally, the scope of attacks can vary. A whole-of-business impact requires a more robust response to a crisis-level cyberattack that escalates beyond traditional incident response and threatens your entire organization. At their worst, these attacks can impair an organization permanently.

Successful remediation of a crisis-level cyberattack requires not only adept security technical prowess but also a nimble whole-of-business response that allows an organization to respond in unison, not in silos. Advanced preparation is critical and must include planning and testing that encompasses identified members from multiple functions across the organization. This testing ensures that teams outside of the IT function learn the following duties:

Understand they have important roles to perform

Know how to accomplish their tasks

See how their participation can help the entire organization respond to and recover from a crisis-level cyberattack

Unlike a response plan that engages mostly IT and security teams, the cyber crisis management plan engages the CEO, the executive suite and stakeholders from across legal, PR, HR and multiple relevant business units. Preparation helps organizations minimize reputational damage and make better decisions under fire.

To join with a leader that can help build, deploy and execute a cyber crisis management program, contact your IBM representative or IBM Business Partner, or visit this website.

What are the requirements to notify authorities?

Most organizations understand the compliance and regulatory requirements that pertain to their company. In general, those requirements apply to all cases of a data breach and the loss of private information belonging to clients and individuals. Government entities, military and public sector organizations may have more specialized obligations to report.

In the commercial realm, depending on the industry or industries in which your organization operates, notification requirements about breaches can vary with local laws. These notifications can include regulatory requirements, international client data loss and special data such as compromised healthcare data. Specific requirements organizations may be subject to include the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and others. However, in almost all cases, breach notifications must be immediate.

In the United States, the FBI's Internet Crime Complaint Center (IC3) must be alerted as soon as a breach is confirmed. It's also recommended to advise local law enforcement.

IBM Security QRadar® SOAR can help organizations quickly understand who to notify and when.

Paying a ransom: Things to consider

Ultimately, some organizations feel compelled to decide whether to pay a ransom. They may feel rushed to make a decision so operations can resume as quickly as possible. Also, they may want to regain access to important files that cannot be recovered by other methods. The main reasons to consider payment should be the potential loss of lives or the potential for the company to collapse entirely if operations aren't restored immediately.

Paying a ransom carries consequences either way. Any decision to pay or forego paying a ransom is tightly linked with the organization's risk management, business continuity goals and downtime costs, regulatory considerations and legal implications.

Organizations must also consider the possibility that criminals won't provide the means to decrypt all files — or may attempt to extort more money — even if they're paid.

Generally, any final decision to pay a ransom must involve the relevant stakeholders from inside the company. At the same time, it's wise to seek counsel from incident response subject matter experts and understand the terms and services offered by the company's cyberinsurance provider. If ransom negotiators are part of the process, they may be able to offer insights from previous cases with the same cybercriminal group.

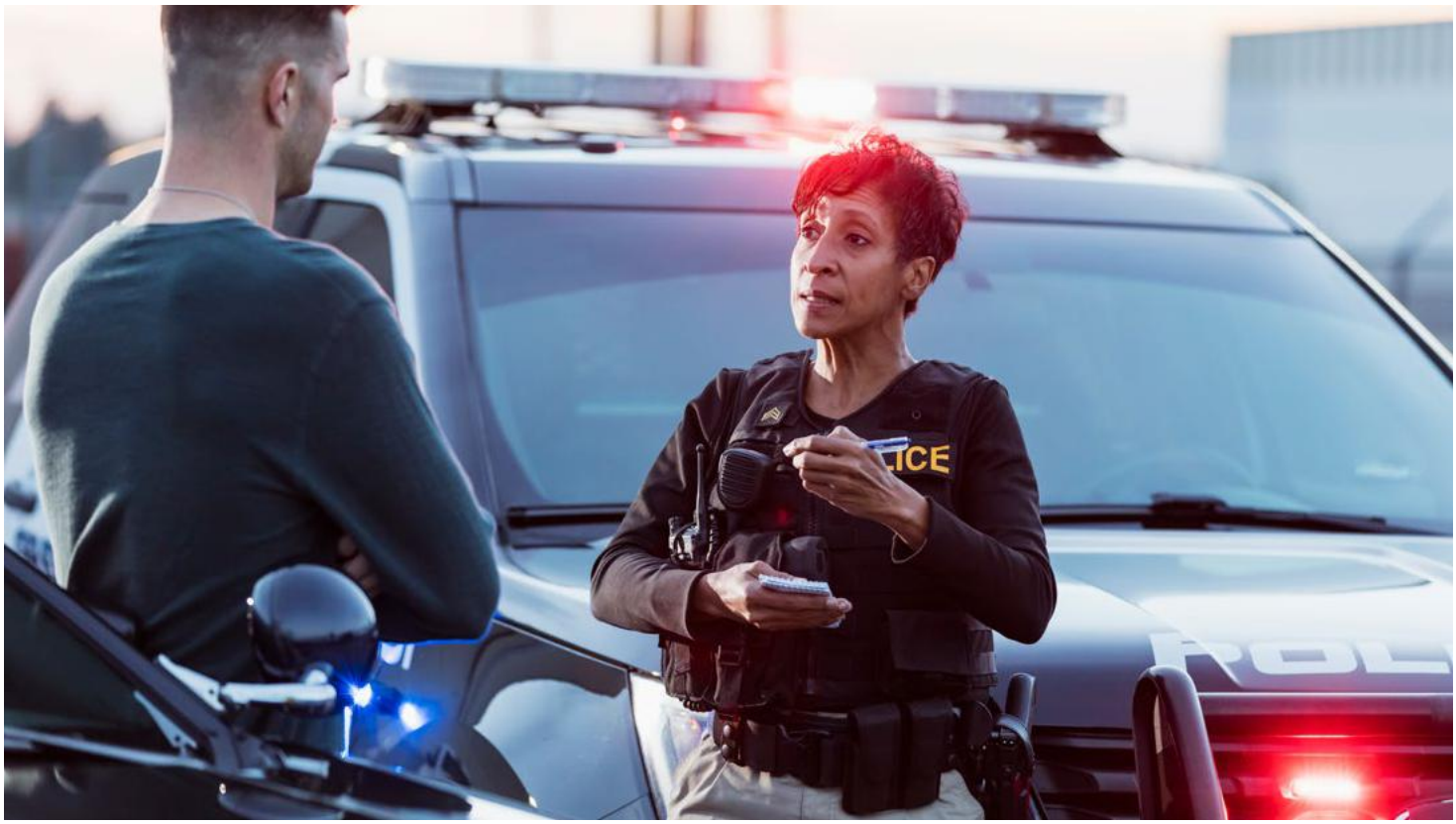
This section lists the main topics companies should consider when deciding whether to pay a ransom.

Paying a ransom doesn't guarantee recovery
Paying criminals is precisely what it sounds like — paying an untrusted party. Criminals may not fulfill their part of the deal after they have been paid, especially since they can disappear as soon as the irreversible payment is made. While not common, this does occur.

Paying a ransom doesn't equal instant recovery
Recovering with a decryption key is seldom instantaneous. Decrypting files is a manual task, and each must be decrypted individually, which can be a painstaking and time-consuming undertaking.

In most cases, even if the criminals are paid and do provide the decryption key, the recovery effort can be just as complex and strenuous as reimaging machines. That result means recovery efforts could be just as costly as if the adversaries had not been paid.

Paying a ransom can be a federal offense
The rising demand to pay ransomware attackers has given rise to a new kind of business: ransomware negotiators. Private firms in this new domain offer to help companies negotiate and pay ransoms for a fee. However, there are considerations beyond negotiating skills to examine when deciding whether to pay a ransom.



"OFAC encourages victims and those involved with addressing ransomware attacks to contact the office immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services."[2]

Instructions from OFAC

Some countries are under sanctions by the U.S. government, so paying ransom to cybercriminals from those countries can be a federal offense. In 2020, an advisory from the U.S. Treasury's Office of Foreign Assets Control (OFAC) served notice about potential fines for all those involved in aiding payments to attackers from sanctioned countries. Those countries include Russia, North Korea and Iran. Firms that offer ransomware negotiation services aren't exempt from this advisory.

While your organization may not be able to readily attribute the attack to a specific group or geography, you may still incur fines from the OFAC if you pay a ransom.

Paying cybercriminals strengthens their business model
Paying cybercriminals reinforces their business model, encourages more criminals to take part in the same activity, and continually funds both cybercrime and other crimes that are supported by that ecosystem. Keep in mind that paying a ransom ultimately serves as motivation for adversaries to increase both frequency of attacks and the price of the ransom itself.

Incident response: Post-incident activity

Post-incident activity is an important part of the response plan and shouldn't be skipped. After any incident, whether large or small, it's recommended to meet with relevant stakeholders to discuss the elements that worked well and those that didn't. This kind of "lessons learned" analysis can help your organization improve processes over time and ensure that future incidents are handled more efficiently and thereby minimize potential impact.

Your analysis also should include technological controls being used to help detect and protect the infrastructure. Analyzing effectiveness of your technology can clarify any needed architectural modifications, divestment or new investments in security technologies that can keep the security maturity model evolving.

The time to uncover and fix gaps in your incident response program is when a threat isn't active. IBM Security X-Force can help with adversary simulation exercises, through red teaming, purple teaming, control testing and tuning, and threat intelligence testing exercises.

Each organization is different, and the recommendations presented in this document are relevant, but general in nature. In all cases of a potential incident where your organization requires assistance, please contact your incident response team or service provider.

IBM Security X-Force Incident Response services resources

If you are experiencing a cybersecurity incident, contact the X-Force team to help.

North America:
24x7 Hotline: 1-888-241-9812

Global Hotline:
+00 1 (312) 212-8034

Endnotes

1. IBM Security, X-Force Threat Intelligence Index, February 2022.
2. Office of Foreign Assets Control — Sanctions Programs and Information, OFAC.

About IBM Security X-Force

IBM Security X-Force is a threat-centric team of hackers, responders, researchers and analysts. Our portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats. With X-Force as your security partner, you can affirm with confidence that the likelihood and impact of a data breach are minimal.

IBM Security X-Force Threat Intelligence combines IBM security operations telemetry, research, incident response investigations, commercial data and open sources to aid clients in understanding emerging threats and quickly making informed security decisions.

Additionally, the X-Force Incident Response team provides detection, response, remediation and preparedness services to help you minimize the impact of a data breach.

X-Force, combined with the X-Force cyber range, can train your team — from analysts to the C-suite — to be ready for the realities of today's threats. X-Force Red, a team of hackers from IBM Security, provides offensive security services, including penetration testing, vulnerability management and adversary simulation.

Schedule a consultation with one of our X-Force experts

About IBM Security
IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services. This portfolio, infused with AI and a modern approach to your security strategy using zero trust principles, can help you thrive in the face of uncertainty. We help you to manage and govern risk that supports today's hybrid cloud environments in the following ways:

- Aligning your security strategy to your business
- Integrating solutions designed to protect your digital users, assets and data
- Deploying technology to manage your defenses against growing threats

Our modern, open approach, the IBM Cloud Pak® for Security platform, is built on RedHat Open Shift and supports an extensive partner ecosystem. IBM Cloud Pak for Security is an enterprise-ready containerized software solution that enables you to manage the security of your data and applications. The solution quickly integrates your existing security tools to generate deeper insights into threats across hybrid cloud environments while leaving your data where it's located. This process allows for easy orchestration and automation of your security response.

For more information, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Authors

Limor Kessem
X-Force Cyber Crisis Management
IBM Security

Mitch Mayne
X-Force Public Information Officer
IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
May 2022