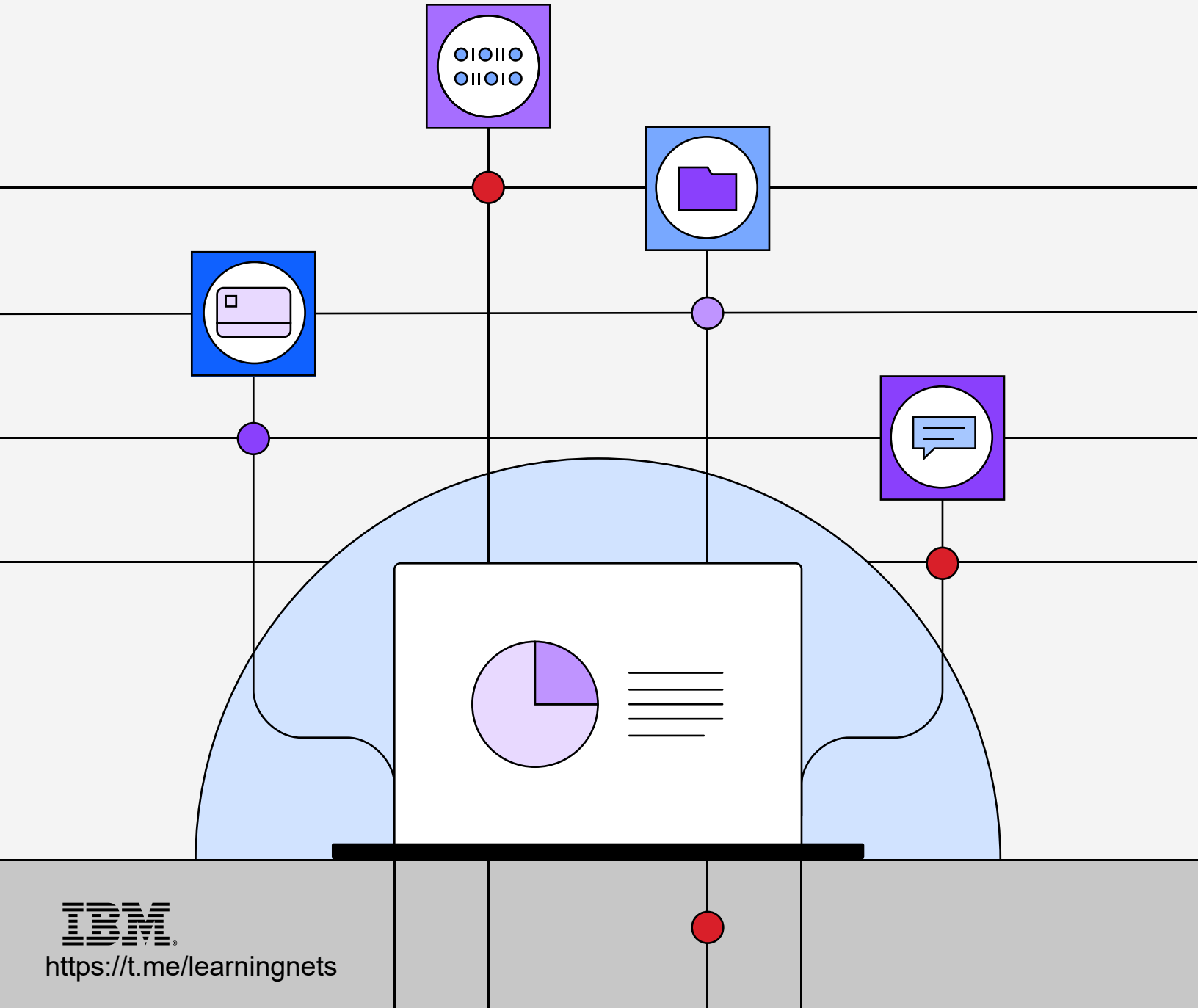
IBM **Security**

Definitive guide to ransomware 2023



https://t.me/learningnets

Table of contents

https://t.me/learningnets

Definitive guide to ransomware 2023

Executive summary

Ransomware is an online attack perpetrated by cybercriminals or nation state-sponsored groups who demand a monetary ransom to release a hold on encrypted or stolen data. Increasingly, ransomware attacks result in crisis-level operational impact to critical infrastructure and commercial organizations, while criminals threaten to publicly release or destroy data if prompt payment isn't made.

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 now primarily target public and private-sector organizations. Robustly applied threat intelligence can help identify industries and geographies considered a primary target at any given time, but no individual or organization is immune to attack.

Ransomware is now one of cybercrime's most profitable and popular business models, pushing aside long-held staples such as banking Trojans, phishing, distributed denial of service (DDoS) and cryptojacking. The ransomware crime model is based on the urgency to restore operations to prevent revenue loss. This model has crippled organizations across the globe, carrying with it a price tag well into the billions of US dollars every year. In an even darker twist, ransomware has begun reaping a toll on human life itself. Attacks that impact hospitals can delay emergency care, leading to potential deaths. Ransomware attacks can also affect medical devices and modify their functions in a subcategory dubbed killware.

As the footprint of ransomware has increased, so has the price of the ransom itself. Ransom amounts that once totaled only double digits have grown to 7 and 8 figures.

USD 80M+

In some extreme cases, attackers demanded that victims pay as much as USD 80 million to have data released.

https://t.me/learningnets

However, ransomware criminals are also keenly aware of economic cycles, often shifting their price tag to map to economic trends. In 2022, the global economy slowed, and ransomware demands decreased.

The IBM Security® X-Force® Threat Intelligence Index 2023 found that ransomware's share of incidents declined very slightly—4 percentage points—from 2021 to 2022, likely because defenders were more successful detecting and preventing ransomware attacks. That encouraging finding is eclipsed by a massive 94% increase in the attack timeline. A separate X-Force report found the average time to complete a ransomware attack diminished from 2 months to fewer than 4 days—giving organizations very little time to detect and thwart potential attacks.

Extortion schemes are also evolving, as threat actors continue to explore new ways to pressure victims into paying. In some cases, cybercriminals silently exfiltrate victim data before they launch the attack itself. Once data is encrypted, threat actors threaten to publicly expose the stolen data unless ransom demands are met, using yet another mechanism to apply pressure for payment. If victims fail to pay for a decryption key within the allotted time, or opt to recover encrypted data through backups, criminals release confidential data publicly, or even auction it off to the highest bidder in dark web markets.

And in yet another twist, ransomware is sometimes blended with destructive or DDoS attacks, causing major disruptions to pressure organizations to pay.

As more ransomware attacks and variants emerge every month, IBM Security X-Force experts believe 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 to protect their business before an attack can penetrate defenses, and how to plan for optimal recovery should adversaries successfully make it through the extended perimeter.

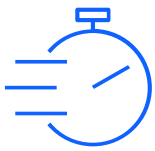
The urgency of informed response

Discovering a ransomware attack can be jarring. Attackers might still be actively working on the attack, and at that stage every second counts. Uninterrupted, time is the ally of the attacker. 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.

You should first involve your IT security teams to investigate and assess the attack and launch the incident response process that they've prepared to combat ransomware. If you've confirmed the incident and have a retainer contract with a third-party provider, then you should engage them as early as possible and get responders onsite.

Other parties to consider contacting are federal law enforcement and regulators, depending on your local and state requirements.

Organizations that have a cyber crisis management plan in place, or executive ransomware response playbooks, should activate the response process. Many ransomware attacks quickly evolve into cross-organizational cyber crisis events. Such crises require leadership and support from executive management, so your teams should be alerted, informed and prepared for this possibility.



https://t.me/learningnets

About this document

This document isn't a ransomware response playbook, nor is it personalized for any one organization's needs. It's intended to be used as a guide to help organizations boost their knowledge, planning and rethinking of adequate defenses against ransomware threats to gain the ability to remediate an evolving ransomware situation more rapidly. This document has distinct sections that address phases both before and during an attack, with the most critical and time-sensitive phases in the initial response section.

If your organization is currently experiencing a ransomware incident and you require immediate assistance, contact the X-Force 24x7 hotline:
(US) 1-888-241-9812
(WW) +1 312 212 8034

It's also highly recommended you immediately review the Incident response: Containment section and return to the remainder of this document for an overall background on ransomware attacks.

Although we mention several IBM Security X-Force resources throughout the document, we also include them at the end to summarize all resources in one place.

Definitions

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

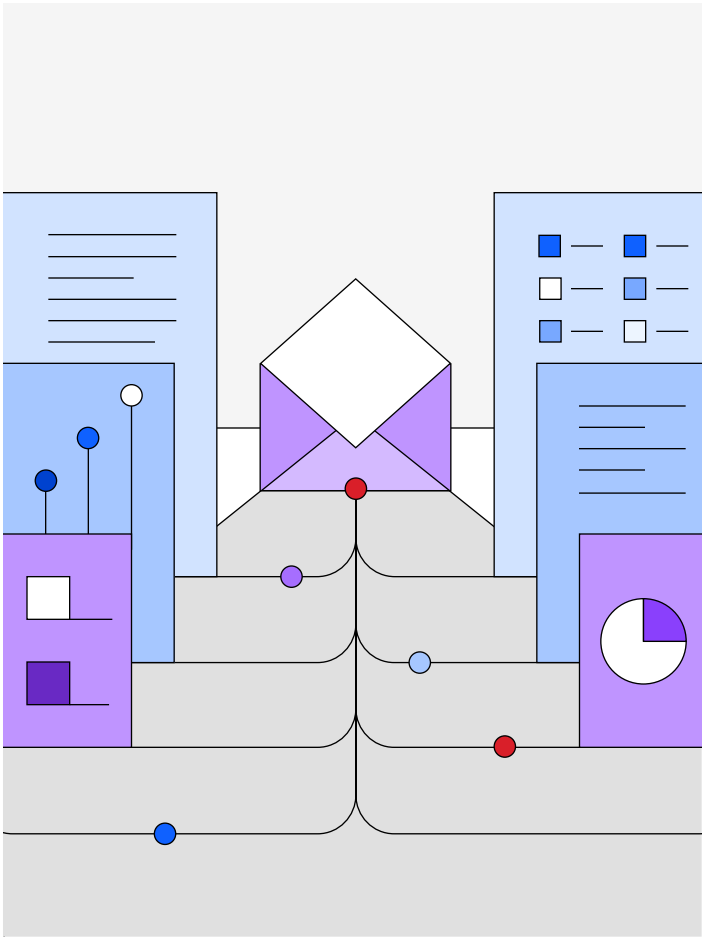
The term *variant* is used to describe separate and distinct programs or families of ransomware.

The term *version* refers to the same malware program or family and encompasses evolving versions of that program, each with varying features.

For example, several variants of ransomware 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 share the same overall goal. Each variant can have multiple versions, and versions are often upgraded over time to add features and capabilities.

https://t.me/learningnets

Ransomware: An enduring adversary



Over time, the IBM Security X-Force team has seen an increase in the number of clients who report being victims of ransomware attacks. Falling victim to ransomware is unfortunately all too easy. Most infections begin with unwitting employees who get tricked by a well-crafted email designed to launch malware on devices attached to company networks.

Though ransomware is commonly deployed on a victim's system as an attachment on an unsolicited email from a known or unknown sender, there are other paths of infection. These include thread hijacking campaigns, which are identified as among the most prominent methods attackers used to deploy ransomware in 2022.

Thread hijacking campaigns use legitimate emails that have been stolen from previous victims through an *infostealer* or email-stealing module. These emails are then distributed in tremendous volumes to the others in the email chain, making the final email look like a reply to the stolen email, thereby hijacking the email thread and increasing its perceived legitimacy.

Another frequently used method is exploitation of public-facing applications, or vulnerability exploitation, which is then used to deploy backdoors on systems. Backdoors often go undiscovered for months and can eventually lead to further compromise.

According to X-Force data, a large portion of backdoor deployments in 2022 led to ransomware attempts. In many cases, these deployments involved older vulnerabilities for which patches exist—underscoring the need to identify and prioritize patches for existing systems.

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.

https://t.me/learningnets

The 5 stages of a ransomware attack

The X-Force team has observed that most ransomware attacks occur in a predictable pattern that can be parsed into the following 5 stages.

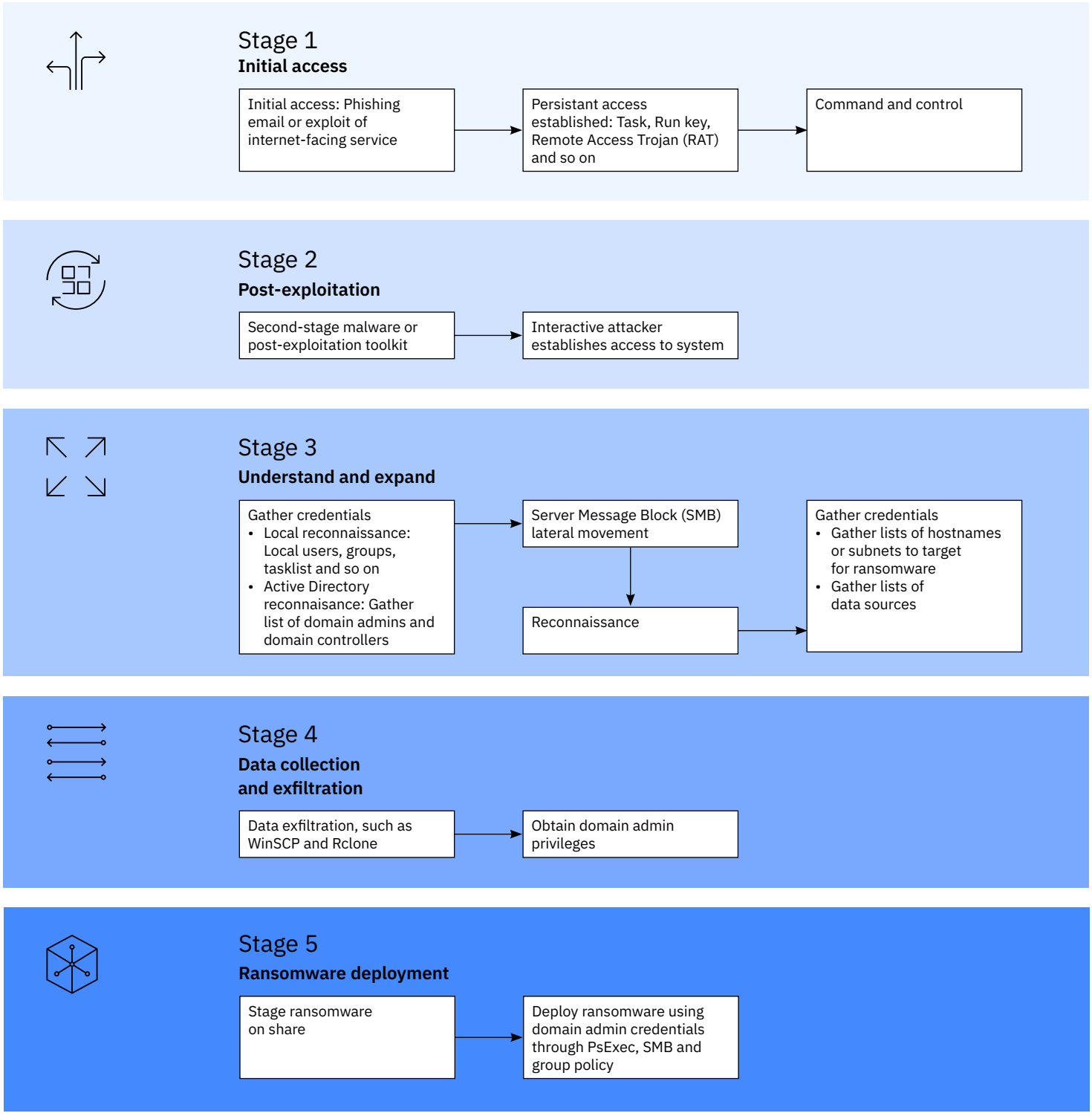


Figure 1: Activities that occur during each of the 5 stages of a ransomware attack

https://t.me/learningnets

Stage 1: Initial access
The most common access vectors for ransomware attacks continue to be phishing, such as MITRE ATT&CK T1566; vulnerability exploitation, including exploitation of a public-facing application T1190; and external remote services T1133, such as exploiting Remote Desktop Protocol (RDP).

Stage 2: Post-exploitation
Depending on the initial access vector, the second stage may involve an intermediary remote access tool (RAT) or malware prior to establishing interactive access with an offensive security tool such as Cobalt Strike or Metasploit.

Stage 3: Understand and expand
During the third stage, attackers consistently focus on understanding the local system and domain to which they currently have access and acquiring credentials to enable lateral movement.

Stage 4: Data collection and exfiltration
Almost every ransomware incident to which the IBM Security X-Force Incident Response (IR) team has responded because 2019 has involved the *double extortion* tactic of data theft and ransomware. During Stage 4 of the attack, the focus of the ransomware operators switches primarily to identifying and exfiltrating valuable data.

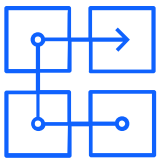
Ransomware operators usually move laterally to additional systems during Stage 4 through SMB, RPC and RDP to identify data for exfiltration. X-Force experts have observed ransomware operators using one or two staging systems to collect data prior to exfiltration, which they continually access through a tunneled RDP connection. Although certain ransomware operators access and exfiltrate data from databases, the majority of data collection occurs over SMB.

Data exfiltration is an area of the attack lifecycle where the X-Force team has observed moderate variance across ransomware operators. Tools such as WinSCP and Rclone continue to be the most common. However, the X-Force team has responded to several ransomware incidents where the adversaries used custom data exfiltration tools or existing tools such as bitsadmin.

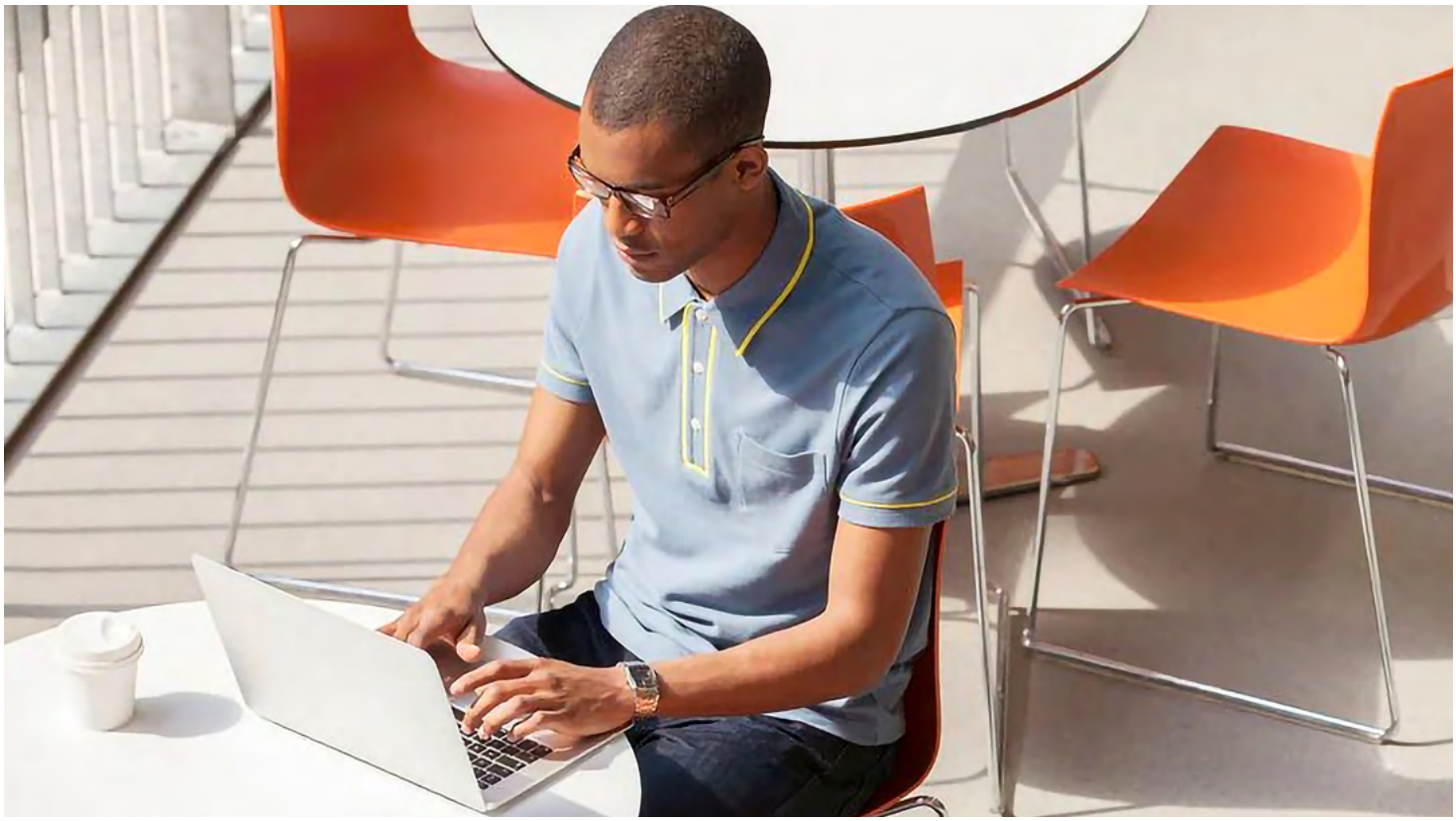
Stage 5: Ransomware deployment
Although innovation within ransomware developers continues to create new variants of malware, distribution of the ransomware payload to the target systems remains fairly common across ransomware operators.

In almost all ransomware incidents to which the X-Force team has responded, the ransomware operators targeted a domain controller as the distribution point for the ransomware payload.

No two ransomware incidents are identical. However, analyzing the adversaries' behaviors across various engagements, operators and geolocations has allowed us to create this 5-stage model that can identify logical control and detection opportunities to help organizations recognize ransomware attacks.



https://t.me/learningnets



Users: The first line of defense

Employee education must be a central element in any ransomware prevention effort. With employees often being the first line of defense against cyberattacks, the more they understand the signs of ransomware, the better the chances are that they will recognize and report them early on.

For example, a trained employee may discover a file that has been encrypted by ransomware or notice an HTML or text file that most ransomware variants leave behind to inform the user of payment instructions. It's essential that the employee not only know how to recognize potential ransomware activity but also know the first action to take to hibernate the device and disconnect it from the network.

> Users should know how to identify and where to report anomalies.

The employee also should know whom within your organization to contact for immediate assistance. Quick and astute recognition and reporting of malicious activity can reduce the overall impact of an attack and ultimately save both time and money.

However, if employees are unable to recognize early signs and know how to report issues through effective channels, the attack may continue uninterrupted and spread throughout the network.

https://t.me/learningnets

Can ransomware be decrypted without paying?

Virtually every victim of a ransomware attack asks this question: Can we decrypt without paying? In most cases, ransomware cannot be decrypted without a key, which is often promised but not always delivered when the ransom is paid.

Whether an organization chooses to pay is often a difficult choice and something the executive and technical teams should decide. Business impact and tolerance for downtime should be weighed when developing a recovery strategy.

> It's wise for organizations to decide whether and under what circumstances they will pay a ransom before an attack happens.

Whichever choice you make, you need a proper plan and playbook designed specifically to address ransomware attacks.

It's important to understand whether encrypted data can be freed with a decryption key or resolved through reverse engineering. Knowing this information in the early stages of an attack helps defenders create an effective response and better forecast the return to normal operations. It can also inform the overall business impact analysis, helping you decide whether to pay the attackers and how much to pay them.

When your security team is attempting to recover from an attack without buying a decryption key, it should consider the following factors:

- Data impact
- Data corruption
- Amount of data lost when recovering from backup
- The time it will take to decrypt files

Again, if these decisions are made in advance, more time can be saved during an active incident.

In a small percentage of cases, the ransomware or its encryption mechanism are technically flawed or a decryptor already exists freely from ethical sources. Those situations are rare, and either approach must be validated by a security professional with the required knowledge.

Detections that help identify ransomware

The X-Force IR team has analyzed hundreds of ransomware cases and identified common activities that span geographies, industries and affiliations. This research has helped uncover common tools, techniques and procedures that can often be detected through the default Microsoft Windows event logs.

Detection opportunities in the Windows event logs
The following event log entries have been present in most ransomware incidents to which X-Force IR has responded and were all logged on systems with the default audit policy. Although all these detections have been useful during X-Force IR engagements, some may have been false positives. Defenders should evaluate their data sets to identify possible false positives and tuning opportunities before adding to a production system.

- System log event ID 7045
- Security log event ID 4624
- Security log event ID 4662
- PrintService Admin log event ID 808
- Security log event ID 4648
- Windows Remote Management (WinRM) event ID 91

Get the details on common detection techniques that can help reduce and mitigate risks to your critical assets and backups, and more quickly detect and contain an attack if your network is infiltrated.

https://t.me/learningnets

Types of ransomware attacks

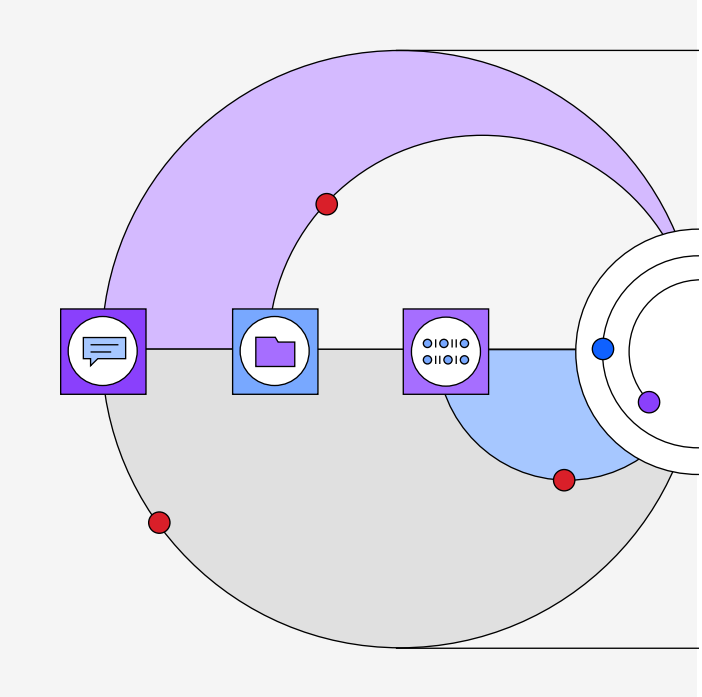
Ransomware groups continue to innovate technically to improve their odds of completing a successful attack. At the same time, the models they use against victims have also evolved to support this goal. Although this section doesn't contain all models used by ransomware threat actors, it does provide an overview of some of the latest and likely more harmful attack types we've seen emerge.

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 or auction it off online.

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

These extortive, blended attacks can circumvent backup strategies because they essentially extort the victim into payment even if clean backups can be used to resume operations. Blended attacks can put immense pressure on organizations to pay extortion fees, but many still opt to forego the option to pay and prefer launching response plans to recover on their own.



https://t.me/learningnets

The destructive flavor

Although most ransomware attacks appear to be designed for financial gain, not all attackers share these motives. In some cases, what initially appears to be a financially motivated ransomware attack can actually be a destructive attack that's designed to destroy digital assets and data and cause disruption and loss.

Destructive attacks use malware to wipe system components, corrupt data and render enterprise devices inoperable. This type of malware typically makes headlines as a tool used primarily by adversarial nation-state actors, especially during the Russian invasion of Ukraine that began in February 2022. In fact, during the first year of the war, Ukraine suffered more data wiper attacks than ever in recorded history.

That said, analysis from IBM Security X-Force Incident Response data over the years has found that destructive attacks are also becoming more popular among financially motivated attackers. The latter have been using data wiper capabilities to increase the pressure on victims to pay the ransom.

The evolving trend of destructive malware attacks means that when preparing for ransomware attacks, organizations must also consider the integration with business continuity and disaster recovery plans. Crisis-level disruption to the business should be handled by more specific planning and the preparation of executive leadership to drive decisions, communications and support throughout a major attack.

Triple extortion: Adding DDoS to the mix

A concerning ransomware extortion trend the X-Force team observed in the past few years was the expansion to *triple extortion* tactics. In this type of attack, threat actors encrypt, steal data and then 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 2 malicious attacks simultaneously. Data is encrypted, rendering work nearly impossible, and networks are bombarded with junk traffic to cripple operations.

In the background, attackers add the advantage 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.

Triple extortion tactics are, however, less commonly seen in ransomware attacks. They require additional expertise to implement as well as add costly layers to an attack, both of which can reduce the overall profit a threat actor could achieve when deploying a ransomware attack.

https://t.me/learningnets

The ransomware incident’s lifecycle

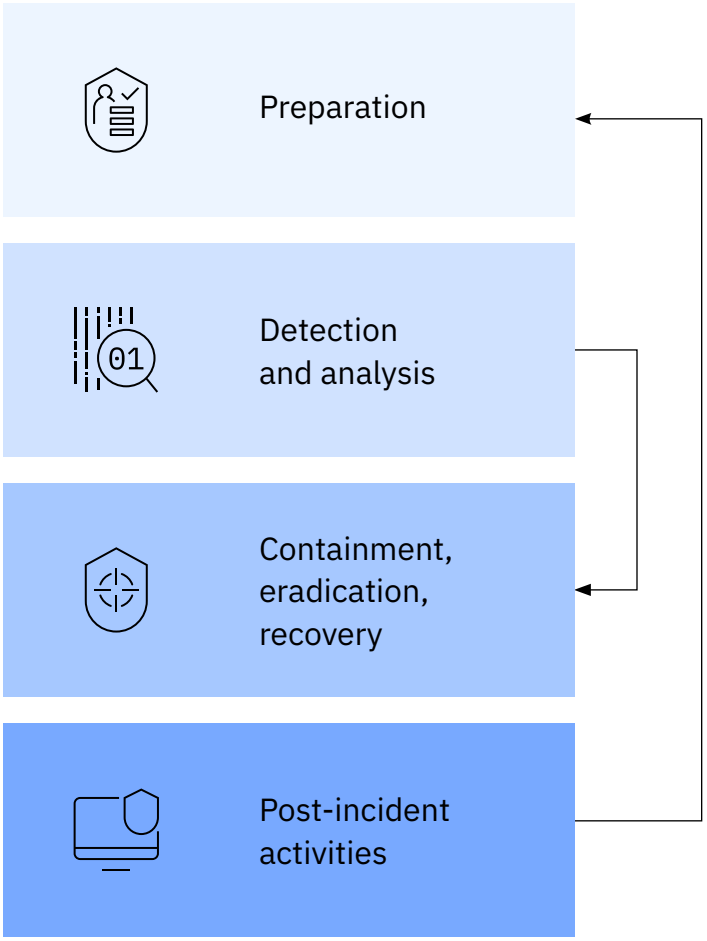


Figure 2: IR lifecycle based on the NIST framework

To describe the ransomware incident’s lifecycle, this document uses the structure outlined by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 1800-25.

Within the scope of an active ransomware attack, steps to undertake include:

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

Each step is further detailed in the following sections.

Incident response: Preparation

The preparation phase of the attack lifecycle involves readying organizations for the types of events and incidents they’re most likely to encounter given the sector in which they operate, the systems they use and applicable key risk indicators (KRIs) as they evolve over time.

https://t.me/learningnets

USD 1M

Having plans in place and a staff trained on the response plan can help reduce the time to recover and save an average of USD 1 million of the total cost of attacks.

Though detailing all aspects of the IR process is beyond the scope of this document, 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, preventing all attacks isn't possible. The X-Force team, therefore, notes that the *preparation phase* of the NIST IR lifecycle is the most important step.

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

Success will heavily depend on a well-rehearsed defense-in-depth strategy and a thought-out preparatory plan designed specifically to thwart a ransomware attack. The following sections note some preparatory elements that shouldn't be overlooked.

Role-based user education

Proactive user education and training continue to be critical in helping prevent compromises of all types because it's often users who first encounter security incidents. Training should emphasize the ability to identify phishing, business email compromise (BEC) fraud, malicious spam (malspam), and by extension, ransomware and malware incidents in general.

Because users are the first line of defense against even the most protected environments, periodic training is recommended for users in the following areas:

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

Security teams should rehearse their ransomware response plans alongside executive teams to ensure that they can respond in unison if ever a cyber crisis-level ransomware incident escalates beyond traditional response capabilities.

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

https://t.me/learningnets

Phishing
Phishing received through email continues to be a top vector leading to ransomware attacks. According to the IBM Security X-Force Threat Intelligence Index 2023, phishing was identified in 41% of incidents in 2022. Across incidents, spear phishing attachments were used in 62% of those attacks, spear phishing links in 33% and spear phishing through service in 5%. The X-Force team also witnessed threat actors use attachments alongside Phishing as a service (PhaaS) or links in some instances.

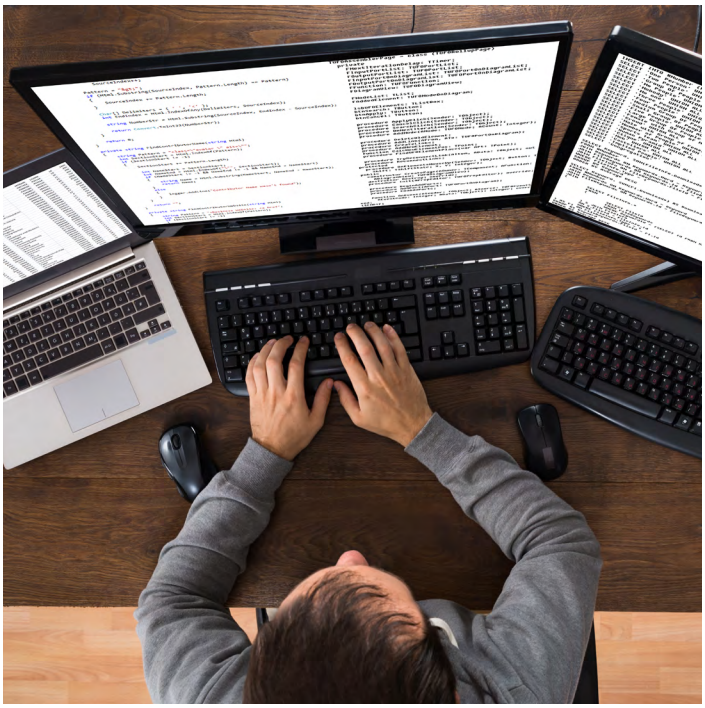
Email thread hijacking
Email thread hijacking saw a significant rise in 2022, with attackers, posing as the original participant, using compromised email accounts to reply within ongoing conversations. The X-Force team observed that the rate of monthly attempts increased by 100% compared to 2021 data.

It's important to educate users about phishing and email security often. Also educate them about password hygiene, and layer email security controls to help block most malicious emails from ever getting to users.

To measure controls effectivity, 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 helps estimate current awareness status, provides the knowledge and ability to report phishing, and results in 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, and then 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 cybersecurity awareness campaigns.

Hone vulnerability management
Attackers that aim to plant ransomware in IT networks often use zero-day vulnerabilities to gain a foothold within a network. This attack vector can be difficult to monitor because it continuously emerges with new exploitable issues—sometimes daily. But new vulnerabilities aren't the most prominent culprit. Frequently, it's existing vulnerabilities that attackers use, which are often unpatched due to R&D and other constraints.



https://t.me/learningnets

Case in point: In 2022, the X-Force team uncovered an 800% increase in infections resulting from exploits of the 2017 WannaCry vulnerability. This increase reinforces the need for organizations to refine their vulnerability management programs and prioritize critical patches.

In many instances, security teams can 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 an increasing amount of "debt" in the form of unpatched vulnerabilities that can directly impact them. And just as debt builds over time, businesses can similarly expand their exposure to attacks if an informed and prioritized vulnerability management plan isn't in place.

Identifying and prioritizing the most critical vulnerabilities requires a broader, more scientific approach that's specific to each organization's most critical assets and data troves. This approach must include correlating threat and vulnerability data from a variety of sources including cloud assets, identifying vulnerabilities that are actively being weaponized and ranking the most severe vulnerabilities for priority remediation.

Deploy MFA whenever possible
Passwords are probably one of the easiest secrets to steal and 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 help ensure that stolen passwords or overlooked default login credentials aren't readily usable to attackers.

The X-Force team's analysis of attacks across different geographies shows that a more widespread use of MFA can drive down the successful use of stolen credentials and the plethora of attack opportunities they can engender.

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.

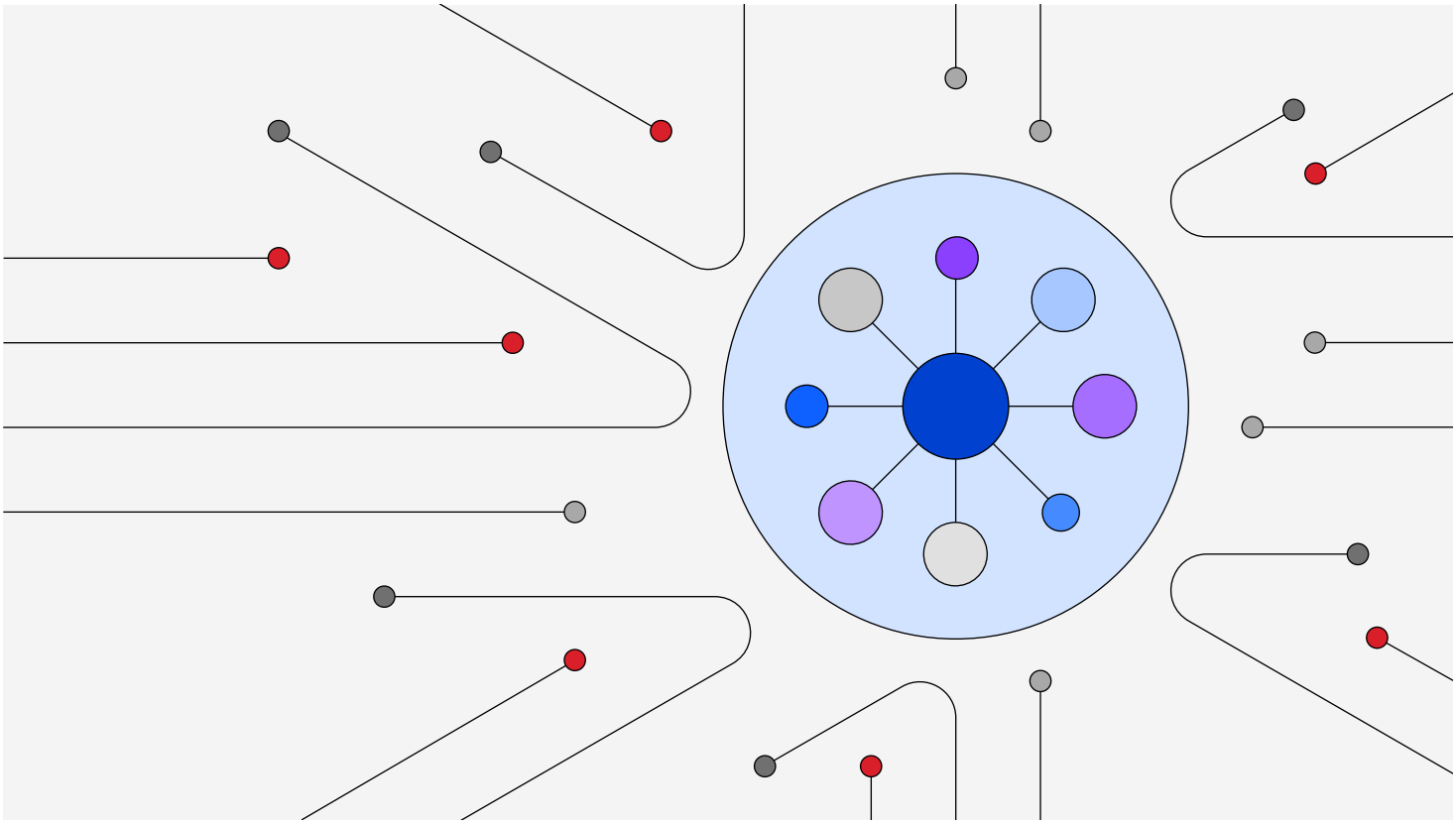
Although zero-day vulnerabilities can appear often, in most cases, patches are also issued relatively promptly. Organizations should adopt an aggressive patch management policy, especially with browser vulnerabilities that expose a large population of employees. Patches should be pushed automatically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

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

Nevertheless, good visibility into the corporate DNSs 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 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 crowdsource intelligence information and help protect organizations by implementing known bad destinations quickly. These reputation feeds provide rapid blocking capabilities when sites have been discovered as having malicious content.

https://t.me/learningnets



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

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

An infected computer operates with the permissions of the user currently logged on, so 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 multiple network shares, security teams should at least consider removing write permissions from the locations where access isn't required on a regular basis.

A common misstep the X-Force IR team has seen is security teams that allow local users to run as administrators on their devices. When this permission level is granted, it provides ransomware the ability to perform more malicious actions on the device and what that device can connect to, augmenting potential impact. Removing local administrator privileges limits human error and malicious actors alike.

https://t.me/learningnets

Spot misconfigurations as an entry point
The way organizations manage identities, permissions and their Active Directory continue to impact the way they're breached. Security teams discovering misconfigurations before attackers find them is, of course, the optimal scenario—but they're often overlooked. One example that the X-Force IR team encounters is setting web-based access to the Active Directory manager and then missing the control that keeps it private. The interface is thereby exposed to the internet, which can allow an attacker to find it and use it as an entry point into the organization.

There are many other types of misconfigurations applicable to both on-premises and cloud environments, but the one thing they all have in common is that, if overlooked, they can lead to a serious compromise—in most cases, a ransomware attack.

Organizations should also consider a robust attack surface management (ASM) solution. ASM is conducted entirely from a hacker's perspective rather than the perspective of the defender. It identifies targets and assesses risks based on the opportunities they present to a malicious attacker. ASM relies on many of the same methods and resources that hackers use. Many ASM tasks and technologies are devised and performed by hackers who are familiar with the behaviors of cybercriminals and skilled at duplicating their actions.

Never keep a default password
Changing default passwords seems elementary, yet it's sometimes overlooked even on important assets, systems and interfaces. This misstep shouldn't be underrated because it 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 make sure nothing was skipped or overlooked.

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. For this reason, attackers often opt to send emails with a compressed attachment that conceals executable malware.

Although organizations often configure their email gateways to scan inside compressed attachments, they don't necessarily strip and 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. The executable then enables sophisticated malware to bypass controls and allow attackers to plant an initial foothold.

International Organization for Standardization (ISO) files, PDF files and Microsoft Office documents are still the most common attachments used in phishing attacks. However, it's possible to mitigate some risk of malware-laden attachments getting through email controls by configuring the email server to strip any executable file. Configuration should include files within archives that aren't password protected and have an .EXE, .COM or .SCR extension. Also, consider stripping .JS extensions before allowing delivery to the user's mailbox.

Some organizations automatically quarantine all email attachments—regardless of type—and then hold them for approval before releasing them to the intended recipient.

https://t.me/learningnets

Maintain current antivirus and endpoint protection
Endpoint antivirus solutions aren't the sole means for threat detection and protection, but they should be a baseline 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 can 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 maximum coverage for emerging threats that may not be detected by one of the antivirus solutions but may be detected by one of the others.

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

Consider disabling Windows Script Host
The use of JavaScript or VBScript by ransomware and other malware has been increasing. Scripting is frequently used by malware authors because Windows Script Host (WSH) is enabled by default on all Windows systems. But although malware authors are fond of 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, leading 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 set the 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 onscreen, warning them that scripting is being disabled.

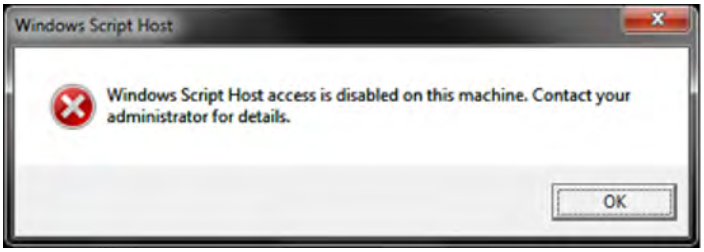


Figure 3: Windows Script Host disabled message

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

https://t.me/learningnets

Hire a hacker
To minimize the possibilities for attackers to find ways into their 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, and include specialized testing as needed for ATMs, blockchain, IoT, automotive and cloud platforms.

Developing and rehearsing an IR plan

An IR plan enables companies to act quickly and effectively during a stressful situation of threats, disruption or disaster that can affect operations on all levels. The plan should specifically address incidents that threaten digital assets and access to data.

A plan should be created so that response is methodical and thought out in advance, so when issues do arise, confusion and panic-induced decisions are minimized.

The methodology of an IR 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 phase on lessons learned to allow the organization to mature the plan and fine-tune actions for future incidents.

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 directly to the NIST Computer Security Incident Handling Guide. Alternatively, organizations can also opt for the SANS Institute framework and handbook.

Whichever plan is in place—and no matter how detailed it seems on paper—plans must be rehearsed so that the team running them understands how to launch and carry out response activities.

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

- How to respond to media and stakeholder questions
- 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 testing response plans, but 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 will function more effectively during an actual event, and rehearsals will 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 IBM Security X-Force Cyber Range for more information.

https://t.me/learningnets

Incident response: Detection

The way by which an organization first detects a ransomware infection can vary widely, but in most cases an employee will find it impossible to access files or notice that a certain service is no longer accessible. Or they may receive a ransom note on-screen. The most time-sensitive issue at the onset of the attack is to identify all infected systems and those in imminent danger of becoming infected.

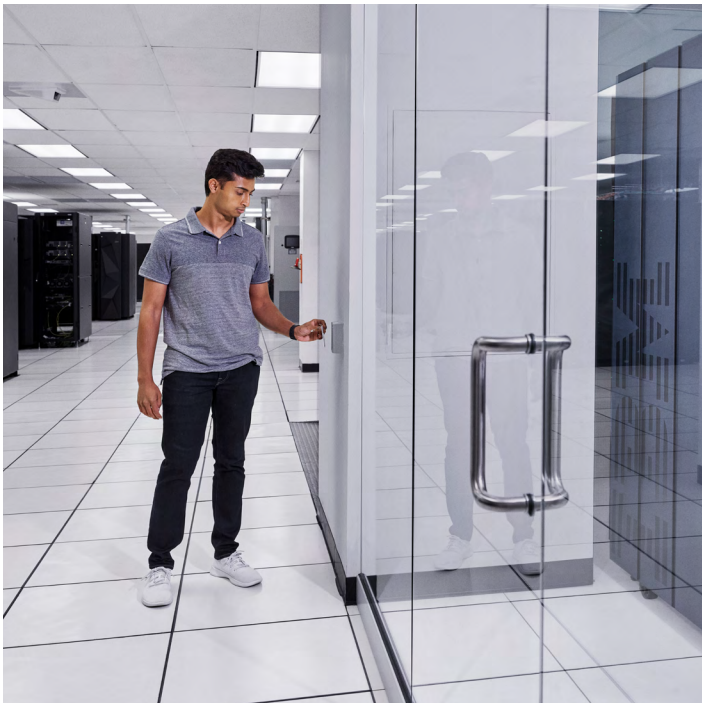
The first goal is to contain the spread of the infection as soon as possible and isolate the infected systems, thereby minimizing the risk to the larger organization. This activity also helps stop any ongoing encryption processes that may still be underway. Ending these processes reduces the damage to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

Keep in mind as you read the scenarios that just because an organization identifies one infected host that's responsible for encrypting files, it doesn't mean that others haven't been affected. If just one host is found to be infected, there's a high likelihood that multiple hosts are also infected because the same vulnerability may exist throughout hosts across the entire enterprise.

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

Scenario 1: 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, there's an infected computer somewhere on the network, and the infected user is using it to access network shares. The ransomware, operating with the user's permission level at this point, goes through the network share and all the files to which the user has access, encrypting them as it runs through the folder.



https://t.me/learningnets

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 because 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 through which the ransomware encryption activity is taking place. 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 2: User attempts to access a local file and finds it 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 ransom.

But 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.

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 because that can reinitiate the ransomware's encryption process and simply run it again.

Scenario 3: User receives a ransom message
Here, one or more employee devices within the organization will silently become infected and begin encrypting all the user's local files as well as the files the user may have access to on network shares.

When the encryption process is complete, a message will display 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 it will often look similar to the example shown in Figure 4. The sample note is from the Ryuk ransomware gang, which was responsible for many 2019–2020 attacks on organizations across the globe.

https://t.me/learningnets

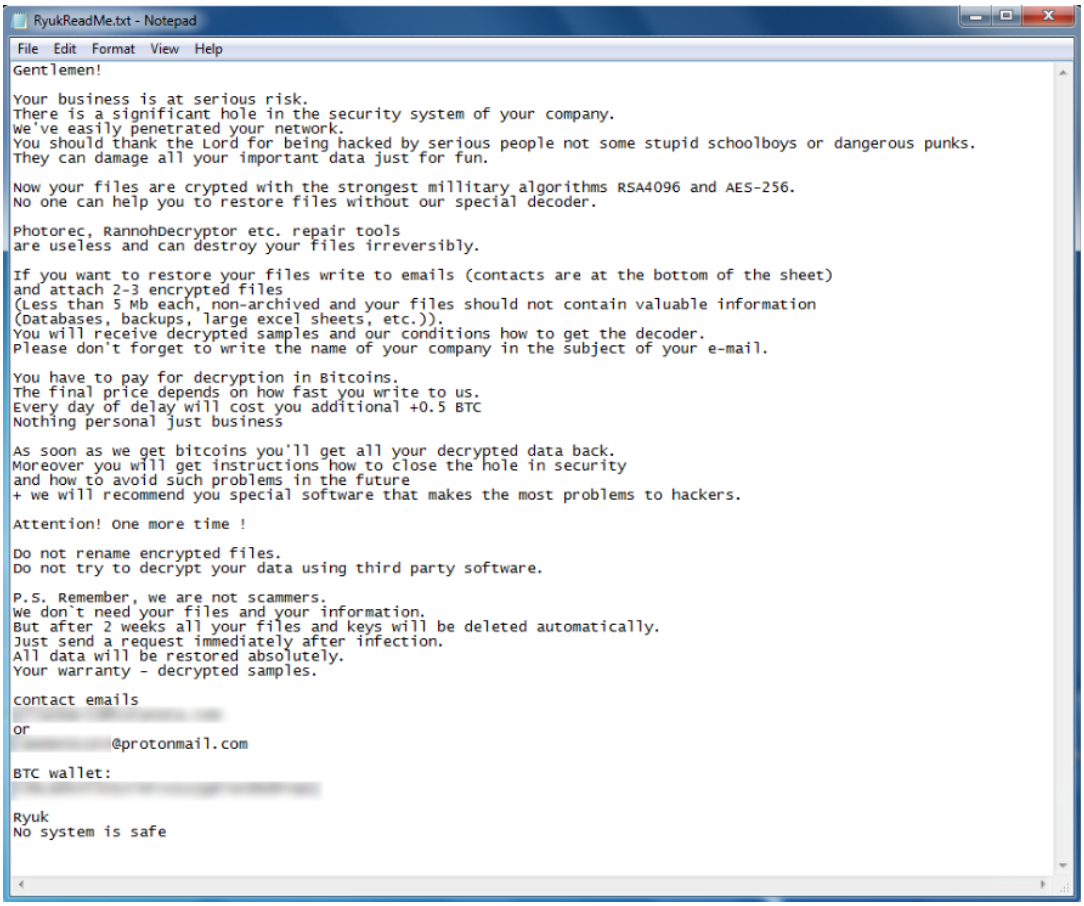


Figure 4: Sample message from ransomware attackers—in this case, Ryuk

Beyond notifying the user that they're infected and helping security teams realize an incident is taking place, the message displayed on the infected computer 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.

Scenario 4: 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.

https://t.me/learningnets

Incident response: 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 may not have this ability. Knowing the capabilities of the specific ransomware code infecting an environment greatly influences both the *containment* and eradication efforts.

Determining the variant can be complicated. The X-Force team recommends organizations consult internal subject matter experts (SMEs) 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 was introduced into the digital environment.

Although a formal RCA can wait until the *post-incident activity* phase, an abridged RCA will aid the organization in planning for and entering 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, because an organization could expend a large amount of time and effort recovering files only to see them re-encrypted shortly thereafter.

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

If an employee received an unsolicited email that contained ransomware, a search across the organization's email store should be quickly conducted to identify other—possibly unopened—emails in additional employee mailboxes. These emails should be immediately extracted and purged to prevent them from being opened.

The *analysis* phase largely focuses on two areas:

- Identifying the specific variant of ransomware in action
- Determining how the malware entered the organization, also known as root cause analysis (RCA)

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

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

Exploitation and manual infection
Another way that ransomware-wielding attackers get into organizations is by exploiting specific software or server vulnerabilities and planting ransomware manually in key areas on the network, aiming 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.

The X-Force team recommends using internal IR SMEs or an external third-party SME to assist in a proper RCA.

https://t.me/learningnets

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
Security automation is critical in cases of any attack, and especially so in cases of ransomware infection.

Your organization should have an endpoint detection and response (EDR) solution in place beyond basic antivirus protection for the following 3 reasons:

- EDR helps detect an attack in its earlier stages. Sometimes that response can mean detecting the attack in the first few days, allowing you to avoid more expansive impact to the infrastructure.
- EDR helps 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 helps 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 one at the onset of a ransomware attack. This activity can also be done by your external service provider if you have IR experts available to assist.

Last resort containment: Terminate access
If you can't 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 access control list (ACL) and so on.

It's not recommended to 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 or SMB protocol on other operating systems, including UNIX, Linux® and so on, protect these protocols as well. This action helps greatly reduce the chance of these shares being encrypted because ransomware can exploit these protocols to move through networks and find more places with data to encrypt.

https://t.me/learningnets

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 experts recommend that any system that has been identified as infected be rebuilt from a trusted source, relying on trusted templates and settings kept safely for cases such as these.

Additionally, RCA may reveal that the ransomware infiltrated the organization through email or mechanisms that other users can access.

These mechanisms should be examined and handled with the following steps:

1. 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 it until it's verified that the ransomware wasn't executed on those systems.

2. If the RCA revealed that the ransomware arrived through a web browser exploit, those sites should be blocked and monitored. The organization should then assess the need to update and remove any vulnerable browser components.

3. 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 an attacker has several 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 it should examine when beginning the *recovery* phase. It's essential that the organization completes the containment and identifies the root cause of the infection before beginning the *recovery* process.

Patch vulnerabilities
If the RCA uncovers that the attack was made possible by vulnerable systems, those systems will have to be patched to prevent them from being re-exploited in the future. If those systems can't be patched, separate them and ensure compensating controls are in place to minimize exposure risk.

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

This step requires that a backup process already exist for the affected data. The process should include an analysis of the frequency and completeness of the backups to ensure that the data will be completely restored.

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. The no backup option also applies if files have been silently encrypted and then backed up over time.

https://t.me/learningnets

Attackers who remain silent in networks for long periods of time can also 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 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 5 days to encrypt everything on the file share before discovery of the attack. This situation means the last 5 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 methods 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.

Don't trust breaking the encryption

Fully restoring files from backups may not be possible. In these cases, organizations may seek ways to break the encryption without paying the ransom or, perhaps, locate decryption keys on infected systems. Although both cases 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 as well as the consequences of each potential route.

The first way to approach the question of encryption reversal is to work with a SME that can potentially offer insight into the malware variant and explore the recovery possibilities.

https://t.me/learningnets

A cyber crisis management plan
Ransomware attacks are already known as highly disruptive events, but the scope of attacks can easily get to the point of a full-blown cyber crisis. At their worst, these attacks can cripple an organization permanently.

Response to all the aspects of a ransomware crisis will require activating support from the entire organization and the command of executive leadership. Successful remediation of a crisis-level cyberattack, therefore, requires not only adept security technical prowess but 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 encompass identified members from multiple functions across the organization. This preparation ensures that teams outside of the IT function understand they have important roles to perform and know how to accomplish them and 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 timely decisions under fire.

To learn how IBM Security X-Force Cyber Crisis Management Services can help you build, deploy and execute a cyber crisis management program, contact your IBM representative or IBM Business Partner®, or visit www.ibm.com/security/services/incidentresponse-services.

What are the requirements to notify authorities?

Most organizations know the compliance and regulatory requirements that pertain to their company or can obtain the information from their compliance and data privacy officers. In general, those requirements apply to all cases of a data breach and the loss of private information belonging to employees, customers and other individuals. Government entities, the military and public-sector organizations may have more specialized obligations to report and should be prepared to do so within the allotted time for each entity.

In the commercial realm, depending on the geography, industry or industries in which your organization operates, breach notification requirements can vary with regional and local laws. These rules can include regulatory requirements, international customer 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 or within 72 hours of finding out about a breach.

In some cases, regulators require using their templates, and certain analyses to be provided—data impact analysis, for example. These requirements should be readily available in advance to save time during an active incident.

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

IBM Security QRadar® SOAR helps organizations quickly understand whom to notify and the applicable deadlines in each case.

https://t.me/learningnets

Paying a ransom: What to consider

When a high-stress situation such as extortion arises, many organizations feel compelled to decide whether to pay a ransom. Factors that may force this rapid decision include a need to resume operations as quickly as possible or regain access to important files that can't 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 SMEs and understand the terms and services offered by the company's cyberinsurance provider. If a ransom negotiator is 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 if the decision to pay a ransom is being discussed.

Paying a ransom doesn't guarantee recovery
Paying criminals is precisely what it sounds like—paying an untrusted party. Criminals may or may not fulfill their part of the deal after they've been paid, especially because they can disappear as soon as the irreversible payment is made. Though not common, it 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 file 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. It means recovery efforts could be just as costly as if the adversaries hadn't been paid.

> "OFAC [Office of Foreign Assets Control] 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."[1]

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, but there are considerations beyond negotiating skills to examine when deciding whether to pay a ransom.

Some countries are under sanctions by the US government and, as a result, paying a ransom to cybercriminals from those countries can be a federal offense. On 1 October 2020, an advisory from the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) served notice about potential fines for all those involved in aiding payments to attackers from sanctioned countries, which include Russia, North Korea and Iran. Firms that offer ransomware negotiation services aren't exempt from this advisory.

https://t.me/learningnets

Although your organization may not be able to readily attribute the attack to a specific group or geography, you may still incur fines from OFAC if you decide to 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 the frequency of attacks and the price of the ransom itself.

Incident response: Post-incident activity

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

Your security team's analysis should also include technological controls being used to help detect and protect the infrastructure. Analyzing the 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. Your executive team should also conduct its own lessons learned session to identify gaps and improvement opportunities.

The time to uncover and fix gaps in your incident response program is when a threat isn't active. The X-Force team 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, contact your incident response team or service provider.

IBM 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:
+1 312 212 8034

https://t.me/learningnets

About us

About IBM Security X-Force

IBM Security X-Force services comprises 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 the X-Force team 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 how to quickly make informed security decisions.

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

The X-Force team, 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. IBM 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 your security strategy using zero trust principles, can help you thrive in the face of uncertainty. We help you 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 the Red Hat® Open Shift® Platform 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.

https://t.me/learningnets

Authors

Chris Caridi

John Dwyer

Limor Kessem

Mitch Mayne

Camille Singleton

Ole Villadsen

Endnotes

1. Office of Foreign Assets Control — Sanctions Programs and Country Information, OFAC.

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
May 2023

IBM, the IBM logo, IBM Business Partner, IBM Cloud Pak, IBM Security, QRadar, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

Java and all Java-based trademarks are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.

https://t.me/learningnets