TuxCare
We Take Care of Linux

GUIDE

How to Recover from a Ransomware Infection

www.tuxcare.com

Introduction

Ransomware.
You know it could be coming for you at any moment.

That's why you're taking every precaution you can: firewalls, patching, advanced threat protection – the works.

But, even with all these protective measures, threat actors may still get through. And what do you do when the worst happens?

In this whitepaper, we discuss the steps you need to take to recover from a ransomware attack – from identifying the initial attack, to assessing the attack strategy, to mounting a response.

This guide will help you:

- Handle the crisis confidently
- Get your data and apps up and running again, focusing on the most important stuff first
- Cut down on costs tied to recovery hiccups, fixing stuff, and getting back on track
- Make sure you've got everyone covered, from management to cybersecurity insurance through to your clients or customers

The scope of ransomware attacks varies, so this document contains generalized tips, with a focus on sysadmins and Linux users. Nonetheless, the principles are broadly applicable.

Nobody wants to be the victim of a ransomware attack, but being a victim doesn't set the outcome – how you respond sets the outcome, and we believe this guide will help you mount an effective response.

This guide is also worth reading even if you're not currently experiencing an attack. It will give you a good idea of what steps you'll need to follow – so that you're mentally prepared to act quickly should the worst happen.

Attack Identification
+ Immediate Response

Take a (brief) step back

Your company just identified a few key systems that aren't responding, and when you check to analyze the problem, you see a ransomware note.

Take a breath first and compose yourself.

It's crucial to remain calm during a potentially fast-moving ransomware attack. If you sense you're panicking: pause for a moment before you proceed. Making rash decisions will exacerbate the challenge. Instead, approach the next steps with a clear mind and thoughtful consideration.

Whatever you do, do not under any circumstances go ahead and pay the ransom. It doesn't guarantee that you'll get the key to decrypt your data and it won't instantly solve your problem.

Execute a hard stop

Stop everything. If possible, break connectivity with the outside world completely as well as between each system. Recovery could be a long process and you'll make it easier on your team if you stop the ability of ransomware to spread.

Some advice might suggest that a hard stop could tip off attackers still in your network. On balance, we believe a hard stop is better: leaving systems open simply means more data will be encrypted. Pull the plug, or use wire cutters and "cut here to activate the firewall".

Cut here to activate firewall – – – | >

You want to stop communications completely because you haven't identified all the affected systems yet and you don't know exactly where the malware is. A hard stop will help you break any command-and-control communications and prevent last-minute data exfiltration.

Key takeaways

Don't panic... but stop everything as fast as you can.

Never pay the ransom.

Steps to follow

- Pull the plug
- Alert senior management
- Initial, elementary public notification
- Alert authorities, IT partner, insurance provider
- Dash for the schematics

!

It may be a requirement in your jurisdiction to report ransomware attacks to the authorities.

Effective containment measures also prevent attackers from returning and launching new attacks later on.

Trigger an initial response

In addition to breaking connectivity, also:

- Lock compromised user accounts and change passwords
- Block inbound and outbound network traffic from external IP addresses associated with the attack
- Enforce password changes for systems administrators and others with extensive privileges

Next, start looking for your dependency schematics. You might think you know where they are but, in most cases, schematics are gathering dust somewhere. Start the process now just in case it takes you a while to find it. Slack it, email it, do what you need to do to retrieve this information.

Depending on the severity of the attack and what's affected, you need to – immediately – inform law enforcement, your cybersecurity insurance provider (if you have one), and senior management. You don't know how serious the attack is yet, so flag it right away.

Risks of paying the ransom

Paying the ransom could be your first instinct… perhaps the ransom demand isn't that much, perhaps the stakes are so high that you feel you must do it. Don't do it. The FBI, CISA and other government agencies strongly advise against paying a ransom. Here's why paying the ransom is a bad idea:

- The threat actor may ask for even more money
- The group behind the ransomware may take the Bitcoin and run
- Significant damage may already be done and the threat actor can't undo it
- The threat actor's decryptor may not work as expected
- You will be marked as a lucrative target
- You could be breaking the law
- You're supporting cybercriminals and encouraging future ransomware attacks

!

You don't know where the funds will end up, and you may be breaching embargoes and exposing your company to legal liabilities.

Assess The Situation

First: Accept that it is serious

Assume the worst case.

Thieves have no honor – don't expect sympathy and don't expect a quick get-out if you make the ransomware payment.

Don't panic, but don't be overly optimistic either. Unrealistic optimism won't serve you well in this situation. For example, if you assume that quarantining a single PC flashing a ransomware message will make you safe, you take the chance that you're just buying time for the threat actor.

Next: Accept what you don't know

Just because one system flashes a ransomware notice doesn't mean that's where the attack started, or that it's the center of the attack. You also don't know at this stage which instant in time the attack happened. You don't know if it's the backups from yesterday or from 10 days ago that are good to go (or not).

Never assume a system is not infected just because the system is not displaying a ransomware message. It takes some time before a ransomware infection on a system displays an on-screen message – intruders first need to go through data and encrypt the files, and only then will they make themselves known. They may also choose to hide.

So don't just look for that message on the screen. Try to look for last modified files and for weird extensions that alerts you to the presence of ransomware.

Determine the ransomware variant if you can

If you're lucky, the problem might not be as bad as it looks, and you could swiftly restore your systems. That's why identifying the ransomware variant should be your first actionable task.

There may be a decryptor, or there may be some widely known way to circumvent the particular strain of ransomware. Get external help if needed.

Key takeaways

You don't know what you don't know yet, so work with no assumptions.

Try and determine the ransomware variant – it could be your ticket out.

Perform a comprehensive survey of networks and systems.

Steps to follow

- Start looking for malware traces everywhere
- Thoroughly catalog what's affected
- Also focus on finding affected customer data

!

It could be just the one system, but prepare yourself that it's systemic.

After you identify the ransomware variant that infected your systems, you can learn some information about the common file extensions used in the attack – which will point you towards more infected files in systems that may not yet be displaying the ransomware notice.

Assess what's affected

As a next step, you need to find out exactly what's been affected by the ransomware. Look beyond the one machine with the flashing image – or whatever the ransomware demand contains. Identify the:

- Affected servers
- Databases that are encrypted
- File storage areas and company-wide shares that have been hit
- Cloud storage that is impacted
- Infected infrastructure including network controllers, industrial control systems, etc.

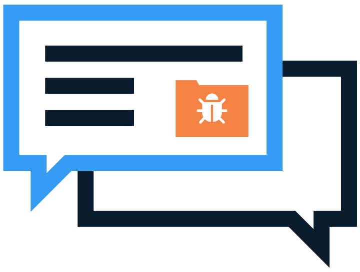
This assessment will aid you with two initial steps, knowing what you need to pull from backup, and what you need to communicate to your customers about the impact of the ransomware attack. From logs and other sources you can identify what customer data has been lost, or has been breached, or transferred outside of your organization.

Infosec matters – but do a business impact assessment too

Not everything is going to go back online at the same time. You need to assess how recovery will impact your organization. Identify priority systems to inspect for potential attack-related impacts and business needs. Classify applications into tiers based on factors such as:

- Importance to the functioning of the business
- Possible consequences for the well-being and safety of customers, employees, and the public
- Compliance with regulations and contractual commitments
- Increased expenses and revenue loss
- Effects on brand and reputation

Communicate with Stakeholders



Talk to management right away

A common “instinct” under pressure is to keep things in a closed circle

– like trying to fix the ransomware attack first, before talking to management. Yes, first drop the power cord and get the affected system off the network. But the next key action you should take: walk right into your manager's office and let them know what you did and what the suspicion is.

In other words, make sure management is the first group that knows what happened, because the next moment your colleagues will be pounding on your management’s door to try and find out why systems are offline.

Collaborate on a communications strategy

Working with your management team, consider who else needs to be informed and what they need to be told. You’ve (hopefully) already alerted key stakeholders in the first step, so now is the time to communicate more extensively about how the ransomware incident affected your organization.

Get a place for coordination: block out the meeting room, for example. Manage expectations. This will not be solved in a day or a week. Communicate with employees and other users of the enterprise’s systems to cease opening emails, and if possible, to log off and shut down their computers.

Don't exaggerate, don't overpromise

Be cautious and realistic about what you communicate. You’re under a magnifying glass – stakeholders will want to know what the consequences are. Don't promise too much because surprises could still emerge.

Key takeaways

You absolutely must communicate with external stakeholders – don’t hide away.

Be realistic and manage expectations – you’re under scrutiny.

Don't publish your own internal or external communications – get it signed off by management.

Steps to follow

- Address internal management first
- Establish the parties that need to be involved
- Communicate clearly and realistically

Publish a public message

Communicate with your IT vendors

Don’t try to be a hero - don’t try and fix everything first before communicating with stakeholders.

Message with reputation management in mind and don't send messages saying things will be fixed quickly when it probably won't be. Staggered messaging is a good idea, "We know there is a problem… and we will respond with more details shortly."

And make sure everybody involved in the recovery is on the same page and that everybody's working towards the same goal.

Set up a public message

Let your customers and partners know that you're experiencing difficulties. Publish a public facing website with a message such as "We'll be right back" or a similar message to that effect, until you have a proper assessment of how you'll recover.

A good example would be:

> "At this point, we have experienced an issue with some of our servers. We are looking into the issue."

Communicating with technology partners could be invaluable

Communicating with your technology partners matters too. Think about your cloud vendor, for example. Yes, backups go away. Snapshots go away. It might look like it's all gone… but in some instances, for a finite amount of time, there is a way to undo the backup refresh.

Loop in your technology partners if you can because if there's a feature that exists that you may not be aware of, you could be on the receiving end of good news. After all, your vendor partners know their platforms better than you do.

Vendors might also have access to logs that you don't. As a result, vendors could spot any abnormal traffic that occurred, and they might provide you with that information.

Analyze the Attack

Find out how it got in

Locating the initial point of intrusion for the ransomware attack is essential.

You must identify the infection vector and then attempt to understand how the attacker moved laterally from system to system. Things you need to think about:

- Which vulnerabilities were exploited by the attackers?
- How did they establish an initial presence in the network?
- Did they obtain additional network credentials, and how did they access other systems?
- What data, if any, was extracted from the network?
- Which files were encrypted?

If you don't have the knowledge to determine the above, you need to consult with outside contractors or law enforcement to get help.

Understanding how the intrusion happened is critical to being able to proceed with a thorough, secure response and recovery effort. Outside contractors can also help you by providing a fresh perspective on a problem that you're too close to.

Don't start reimaging immediately

Don't reimage a system too soon: you need to perform a root cause analysis first and you can't do that once the system is reimaged.

However, once you get going with restoring systems, you want to take your time to make sure that everything is cleaned or reimaged properly and that no traces are left.

Key takeaways

A detailed understanding of the nature of the attack will help you recover faster.

Narrow down the affected systems, if you can, so that you don't waste time trying to restore unaffected systems.

Steps to follow

- Find the attack entry vector
- Detect the ransomware variant
- Perform a root cause analysis
- Understand which systems are compromised
- Analyze your logs

!

Wait before you start reimaging: you don't want to erase evidence that can help you understand the attack.

Map out what’s been affected

Determine the "blast radius" of the attack, i.e., the compromised systems and the encrypted or corrupted files.

Replacing all of your organization's systems and restoring all data is a daunting task that can last days or weeks, and it helps to narrow the task down. Excessive recovery efforts can also lead to unnecessary data loss as unaffected data is reverted to previous versions.

By concentrating on a subset of systems and files, you can significantly reduce the workload involved and expedite the full recovery process.

It will also help you determine the attack's effect on crucial business systems, the cost of disrupted operations over short and long periods, the feasibility and probable timeframes for recovery based on various scenarios, and the risk to the organization's reputation and revenue if stolen data is revealed.

It’s all in the logs

Logs can help you understand what happened. It’s not necessarily a complete source of the truth, but parsing logs will provide plenty of clues, like where the attacker was and where they went to. Logs provide a sense of how things played out.

Things to watch out for include abnormal traffic on the days prior to the infection. Your logs will give you a hint if any data was exfiltrated or not before the systems got locked, so that you know if there is an additional threat that you need to deal with – and whether there are compliance implications.

Plan and Execute a Response

Don’t try to “quickly” “fix it” – don’t trust anything

Threat actors are really good at hiding things and you should proceed with that assumption.

You cannot trust a compromised installation anymore. It needs to be deleted, and you need to start over because you never know whether there's a timer in the background that just sleeps for a while and a month later the ransomware just comes back.

Work within a recovery zone

You don't want the affected systems and the refreshed systems to be in exactly the same environment. Ideally, you want to create a recovery environment completely separate from your existing systems.

That means a recovery zone with untainted servers, a reliable network, and reinstalled software tools and applications.

The recovery zone must also possess complete backup facilities. Though applications in the recovery zone will be residing there temporarily, they will generate live production data for some time. A virtual private cloud on a public cloud platform could be one way to go.

Attempt decryption

If there is a published decryptor for your specific malware infection, it’s worth giving it a try. However, do note that the decryption process takes a long time. You don't just flip a switch or execute a file and expect everything to be back to normal.

Once you start decrypting a system… you’ll be looking at hours or even days for a single system to go back to normal. It is therefore worth prioritizing systems.

Key takeaways

As we said right at the start, don’t make assumptions and don’t rush. Check everything.

Separate the recovered systems from the rest of your networks by using a recovery zone.

Steps to follow

- Establish a safe, clean recovery zone
- Try decryption if you can
- Initiate recovery starting with tier 0 and tier 1 systems
- Perform post-attack remediation

Plan carefully and considerately. If you bring all of your systems back and then a week later the attack resurfaces, you’ll be in an even worse situation.

Start the recovery

Try to bring systems up one by one. Get your team in on the process. Go over every single system and make sure that it is clean, or at the very least, try to identify the ones that are already fully encrypted. Pay attention, as you might have interrupted some systems midway through the encryption.

Recover data for Tier 0 and Tier 1 applications in the recovery zone, then restart those applications and supporting services. Use data tools for selective recovery to recover only encrypted or corrupted files. Test the applications in the recovery zone and give users access.

Clean and remediate the production environment. Transition critical services and applications back to the production environment. You can then proceed to restart Tier 2 and Tier 3 applications.

Remediation after containment and recovery

You need to try and capture knowledge about the attack, assess your response's strengths and weaknesses, and take steps to prevent similar attacks in the future:

Eradicate traces of the attack:

Identify and remove any malware or malicious software used in the attack, and reset system configurations, parameters, and registry settings that the attackers may have altered.

Document the incident and response:

Threat actors frequently reuse the same tools and techniques, so document details of the attack and your organization's response to it.

Remediate vulnerabilities and strengthen security

Now is the time to close vulnerabilities and remediate weaknesses, identify controls, and processes that can enhance security and prevent a repeat attack.

Appendix:
Prevention + Preparation

Go all-out with training

After you start getting your systems back up again and when your organization starts going back to normal again, you have the best opportunity you're ever going to get to retrain your colleagues to focus on cybersecurity.

Set up sessions to review topics around phishing, safe browsing, and not bringing outside devices onto the network. You'll get buy-in from everybody at this moment in time – from the everyday workers through to management. You'll get people's attention immediately, and you have an example that you can point back to.

Review your internal documentation

Use the notes you gathered throughout the attack and recovery to make sure you're prepared for the next attempt.

Start with things like network and systems schematics – so you know where to cut the cable, and how to limit the spread of malware as fast as you can. You never again want to scramble to try and remember how to disable a network port again. Document the commands you used.

Also work to map out your broader ecosystem and environment and develop it all into a visual schematic that explains how the different systems work together.

You do that because you need to know what is affected when one system goes down as well as where the interdependencies are between your systems: does your web server authenticate against your directory service, for example? Which databases are needed for which systems to operate? And who has access to it all?

Ensure that you have an inventory of all the servers, virtual machines and cloud servers in your cloud environment, regardless of whether they are physical or virtual. It is crucial to understand what you have, but it's also important to set up a system to monitor new additions. This includes keeping an eye out for any new MAC addresses or IP addresses that may have been assigned.

To ensure control over connectivity, it's not enough to rely solely on firewall rules and documentation. You should verify connectivity between servers. It is possible you overlooked a protocol, port or IP range in your existing rules, so testing them is essential.

If two servers are not supposed to communicate with each other, it's essential to verify that they are unable to do so. Don't simply assume that your firewall rules are accurate; confirm that all blocked connections are indeed blocked.

Backup strategy

Test your backups regularly. Keep backups on rotation too – i.e. keep more than one viable backup. It’s worth testing constantly, e.g. every week or so. Don't keep your backups on the main storage. Keep backups on a separate storage device, preferably on an air gapped device.

Even better – have a route where you perform backups and then disconnect the backups from the rest of your operations. It means that ransomware can’t touch your backups. After all, if ransomware encrypts your backups… you’re in trouble.

Patching

You should always have your systems patched and up to date. And that does mean every system: there are “no test servers” that are less important than the others – any device or service can prove to be an entry point.

So any and every server, you need to patch it. You need to keep it up to date, and it needs to be on your watch list as well as on your logging system, regardless of whether it's important or not at face value. If you struggle to patch, consider patching automation – and live patching, which removes the need to reboot servers.

Outside requirements

You need to have a clear understanding of disclosure requirements and the organization's stance on ransom payments before a crisis occurs – during the crisis is not the time to try and figure it out. Your team must prepare and record all relevant regulatory, insurance, and corporate policies that must be taken into account during a ransomware attack response.

It includes the appropriate timing and level of engagement with the organization's cybersecurity insurance provider in the response process (typically immediate and comprehensive), a suitable moment and method for involving security forensics firms and external technology vendors in analyzing and responding to the attack, as well as when to contact law enforcement agencies, such as the FBI, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and other global authorities.

You also need to predetermine the circumstances under which it is necessary to disclose information to potentially impacted parties, such as customers and business partners.