Insight Space

cyber insights programme

Executive Analysis

How to effectively respond to a ransomware attack in four key steps

Lloyd Brough,
Technical Director at
NCC Group

Introduction

Ransomware attacks can be incredibly stressful. Unlike previous strains that were opportunistic and relatively small in scope, modern ransomware targets entire organisations and uses sophisticated tactics to encrypt, destroy and steal data with little chance of recovery.

Prevention is the best form of defence, but no organisation can achieve total security against ransomware, so it’s important that you understand how to respond to an incident as effectively as possible.

With that in mind, here are four key steps that you should take following a ransomware attack:

- Ensure backups are resilient and restore them
- Investigate the root cause
- Implement detection and response
- Create a security improvement plan

Ensure backups are resilient and restore them

If a ransomware threat actor has deployed a payload within your organisation, there are three ways that you can recover your data: decrypt your files, pay the ransom or restore your backups. However, decryption tools are not widely available for modern strains and paying the ransom can expose you to future extortion with no guarantee that you'll get your files back.

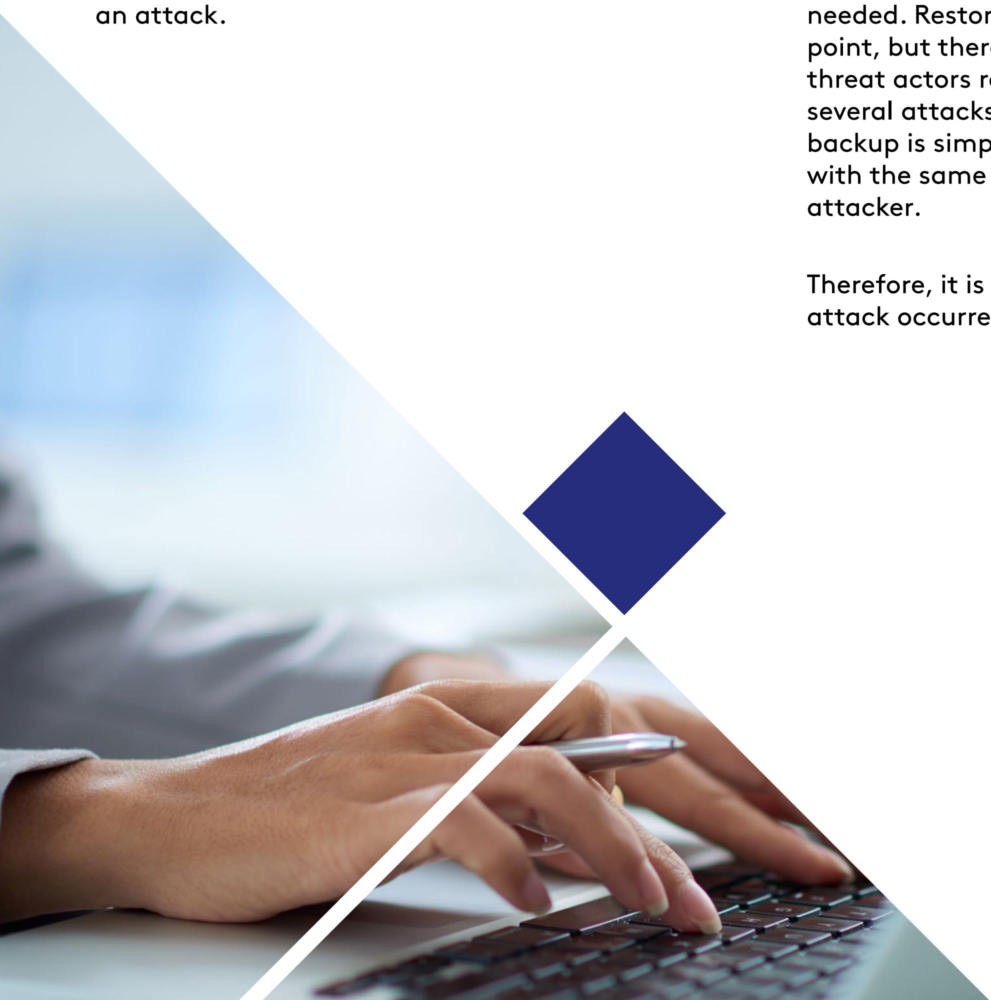
Restoring backups is often the only way to recover your assets. You should back up and test the retrieval of all your applications, systems and data regularly so that you can restore their latest versions and resume normal operations as quickly as possible.

This process should include supporting IT infrastructure that you wouldn't always include in a backup, such as directory services like Active Directory that enable you to authenticate systems. Without completing a full and exhaustive test of your backup programme you have no guarantee that you'll be able to resume operations following an attack.

Threat actors often target backups to cause as much devastation as possible, so mandate additional out-of-band authentication before granting access to them. You should also consider creating immutable backups that cannot be changed and storing them offsite or away from your main network. Essentially, if a threat actor can destroy backup solutions with just an administrator username and password then the backup protections are not appropriate to protect them.

If you have a fully tested and comprehensive backup strategy, you will be able to give priority to key systems and fully understand the dependencies needed. Restoration will be fairly simple at this point, but there is more to consider. We have seen threat actors return at this point and redeploy during several attacks recently. Essentially, returning to a backup is simply standing up the same infrastructure with the same weakness that was used by the attacker.

Therefore, it is critical that you understand how the attack occurred.



Investigate the root cause

When an incident occurs, having immediate support on hand can be the difference between a minor pause in operations or a costly breach and reputation damage.

Therefore, it is critical that you have appropriate logging available to perform quick investigations or call in the services of a Cyber Incident Response Team (CIRT) which you should have on retainer.

Logging the correct things to investigate cyber incidents is a complex topic, but even the basics can get you a long way. Many organisations have no logging available.

Implement detection and response

After you've activated your backups, you should implement a thorough logging mechanism and services like Managed Detection & Response (MDR) to help you monitor for further suspicious activity across your network.

Any key indicator of compromise (IOC) from the previous attack should be actioned for mitigation or for monitoring. A key example here would be to sink hole the communication channels used by the threat actor and to block egress at the firewall as appropriate.

You should also be prepared to perform some drastic actions: an attacker likely had full access to your user account passwords from your domain. A complete password change is a simple thing to say, but not that simple in reality.

Remember that antivirus (AV) alerts and incident logs that seem harmless could be signs that the threat actors behind the original attack are searching for other vulnerabilities that they can exploit to deploy their ransomware. As such, it's important that you detect these incidents at an early stage and investigate them thoroughly.

By using MDR to detect ransomware attacks early on, you can implement an incident response plan to prevent them from deploying their payloads and harming your organisation. This plan should involve more root cause analysis to establish how the ransomware infiltrated your organisation in the first place, so that you can take action to prevent threat actors from exploiting that vulnerability again during or after the initial attack.

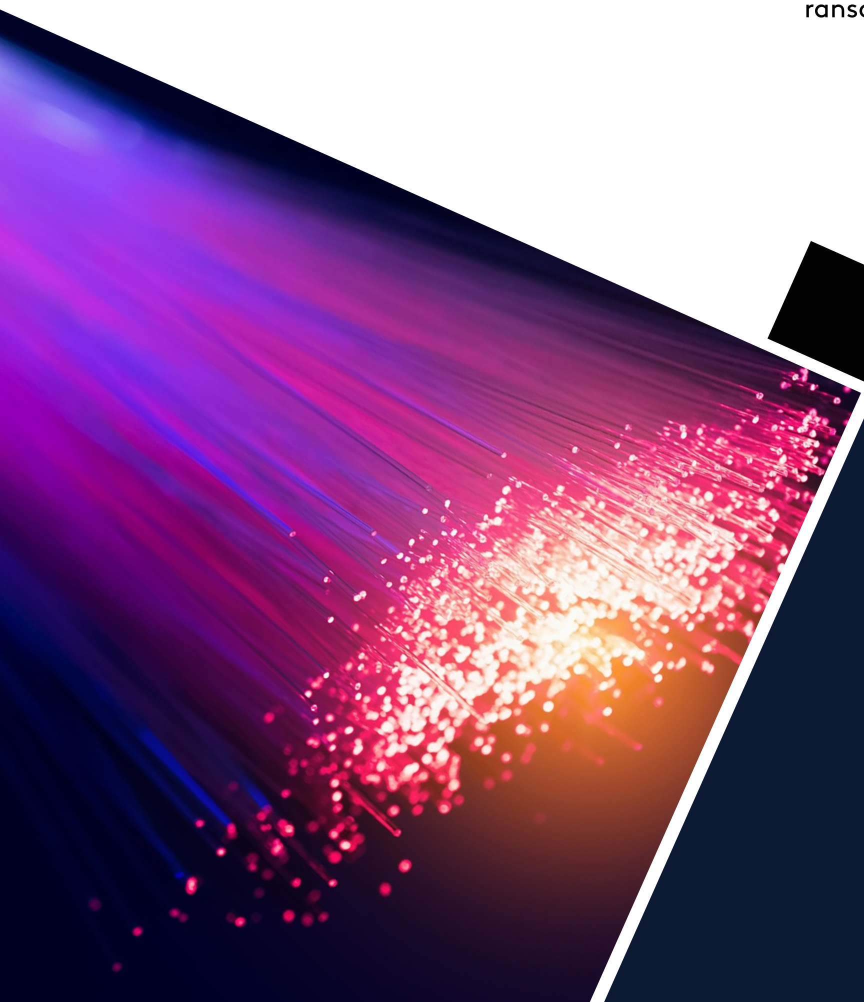
When you've dealt with the initial ransomware and any subsequent attacks, MDR can provide ongoing protection against ransomware across your network. Instant Endpoint Detection and Response (EDR) can also help you keep track of malicious activity across devices that are being used remotely or in less secure environments.

Create a security improvement plan

The measures that you put in place to prevent future attacks are a critical part of your response to a ransomware incident. Mitigating ransomware risk over time requires a multi-layered cyber resilience strategy, but translating the lessons learned from an attack into a rapid and sustainable security improvement plan is an effective starting point. This involves prioritising and resolving your security weaknesses at pace to rapidly reduce your risk without disrupting your usual operations.

To create an effective security improvement plan, start by triaging your risks across your people, processes and technology. This should be based on your existing strategy, challenges and risk position, as well as any insights from the ransomware attack and recent security assessments. Once you've established your risks, you can prioritise countermeasures based on your risk appetite, the value they offer to your organisation and the cost and scale of implementation.

After you've prioritised your risks, you can create a structured improvement plan that focuses on urgent fixes to your most dangerous vulnerabilities, enhances and secures your organisation over the mid-term and implements more strategic mitigations to reduce risk in the long-term. Agile project delivery methods are particularly useful when implementing a security improvement plan, enabling you to break activity into sprints, give stakeholders an ongoing view of the status of each action and ensure measurable improvement of your organisation's resilience against ransomware.



Insight Space

cyber insights
programme

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how you can reduce your ransomware risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com