

Insight Space

cyber insights
programme

Issue 04: Ransomware

Welcome to the NCC Group Insight Space

Ransomware is one of the most common types of cyber attacks for organisations around the world: according to our research, the number of ransomware attacks on organisations of all sizes across every sector has increased in the last 12-18 months by 45%.

Unlike historic attacks that were relatively small in scope, modern ransomware attacks are designed to devastate entire organisations by encrypting, stealing and destroying data at will.

At NCC Group, we've worked closely with clients from multiple sectors to help them prevent and recover from ransomware attacks. However, the threat is constantly evolving, so it's vital that cyber security decision makers remain informed on best practice to ensure ongoing resilience against this exponential threat.

In this edition of Insight Space, we analyse the ransomware landscape, including recent trends like the growth of ransomware-as-a-service attacks, and explain what that means for your organisation. We also explore how ransomware tactics, techniques and procedures have evolved, providing practical advice on how you can prevent ransomware from infecting your organisation. Finally, we summarise four steps that you should take if you do fall victim to a ransomware attack, helping to ensure that you can recover as effectively as possible.



"Ransomware is an exponential threat to societies around the world, so cyber security decision makers should consider a ransomware attack on their organisation as an inevitable event and prepare accordingly. In practice, this means applying good cyber security hygiene as part of a multi-layered strategy of resilience.


"Ransomware attacks are a symptom of broader cyber security issues, so we're working closely with our clients to implement security improvement plans that prioritise and remediate those issues to have the greatest impact on their resilience."

- Ian Thomas,
Managing Director at NCC Group

Contents

	Tim Rawlins Senior Adviser	Executive Viewpoint Defending your organisation from ransomware	P 4
---	--------------------------------------	--	------------

	Lloyd Brough Technical Director	Executive Analysis How to effectively respond to a ransomware attack in four key steps	P 10
---	--	---	-------------

	Lloyd Brough Technical Director	Technical Viewpoint EternalGlue revisited: reflecting on lessons from a self-propagating worm in the context of a modern ransomware attack	P 16
---	--	---	-------------

Additional insights

Case Study: Charity Response, rapid remediation and solution implementation for a charity organisation	P 22
--	-------------

Case Study: University Delivering essential assurance, monitoring and detection services for a university	P 25
---	-------------

Insight Space

cyber insights
programme

nccgroup[®]

Executive Viewpoint

Defending your organisation from ransomware

Tim Rawlins,
Senior Adviser at
NCC Group



The ransomware threat landscape is becoming increasingly complex. Changing ways of working and the increasing commoditisation of ransomware mean that ransomware is more of a threat to business resilience than ever before.

One factor contributing to this increasing threat is the way that working life has changed. At the beginning of the pandemic, many organisations quickly transformed their operating model to allow employees to work from home, often onboarding new solutions and ways of working without taking the time to consider any security gaps that would open up as a result.

The adoption of new technology has meant that we've increasingly seen criminals taking advantage of unsecured solutions. It's common for ransomware groups to take advantage of business web applications with vulnerabilities and remote access solutions such as Virtual Private Networks (VPN) and Remote Desktop Protocols (RDP), to gain a foothold on a corporate network.

Social engineering attacks are another common route for criminals. While email phishing attacks remain at the top of the list, LinkedIn, WhatsApp, and text messages are increasingly used as ways to reach unwitting employees. Highly targeted and well-crafted phishing attacks are more likely to be successful if employees are working away from the office, and are therefore less likely to question any requests that are even slightly out-of-character.



The threat of ransomware spans borders and sectors, with the targets of ransomware gangs ranging from IT suppliers and software companies to critical national infrastructure providers, local and national governments and financial institutions, where stakes and potential rewards for hackers are high.

In the past few months alone, the world has seen several large-scale ransomware attacks. These include the attack on Kaseya, an IT solutions company, which leveraged vulnerabilities in its VSA product for managed service providers (MSPs) to impact between 800-1,500 businesses in July 2021.

Another particularly notable example was a ransomware attack that targeted the [Colonial Pipeline](#), a 5,500 mile fuel pipeline covering the US East Coast in May 2021, severely disrupting fuel supplies across the country. The impact of the attack quickly became apparent as increased fuel demand and shortages led to panic buying and fuel price increases. When added to the \$4.4 million (£3.1 million) ransom paid by the Colonial Pipeline Company to Eastern-European based ransomware gang, Darkside, the true cost quickly becomes apparent.

The lucrative nature of ransomware attacks means that businesses are experiencing ever-more aggressive and highly targeted approaches from criminals. This is particularly true for the financial sector, which is frequently targeted by a banking malware family known as Gozi, characterised by an aim to cause financial losses through transactional fraud or targeted ransomware activity. NCC Group's Research and Intelligence Fusion Team (RIFT) [found](#) that 136 financial institutions had been targeted by threat groups using RM3, an advanced variant of the Gozi ransomware family, since 2017 - just one small aspect of a vast threat landscape.



The evolution of ransomware

As well as an increase in targeted ransomware attacks, the last year has led to a rise in ransomware-as-a-service attacks, in which ransomware variants are sold to criminals in a subscription model.

This means that many criminals target victims simply by scanning for vulnerable applications or remote access ports. Often, these gangs seek to go after irreplaceable business assets as well as devices connected to a business network, which could include file servers, database services, virtual machines and cloud environments. The theft of data is also a common element of today's ransomware attacks, with criminals often using the threat of publication as leverage.

The determination of today's criminals makes it much harder for organisations to recover from ransomware attacks. In many cases, attacks go undetected until the damage is done. The timeline of attacks can often span weeks from the initial breach to full control of the victim's corporate network.



Building a security strategy fit for the new normal

Prevention is better than a cure, which is why it's vital for organisations to build a proactive security strategy. As organisations step back and review their processes, people and technology for the post-COVID world, it's crucial for them to also consider the security measures they have in place.



Creating a security-aware team

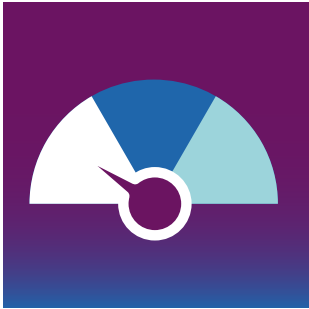
People are a critical line of defence for businesses, and the way that colleagues respond to security challenges can be the difference between ongoing resilience and a damaging cyber attack.

It's therefore crucial for organisations to provide regular security awareness training to staff members, covering best practice when it comes to dealing with phishing and scam attempts. This training should also cover reporting to regulatory bodies, strong password security and how to store sensitive credentials.

In addition to this, individuals can play a key role in helping a business recover quickly after an incident – it's important for organisations to have individuals that are given the authority to make decisions during an incident as part of a robust incident management policy.



Building a security strategy fit for the new normal



Minimising risk

Having robust controls in place and limiting access to business networks wherever possible can help to reduce an attacker's chances of breaching corporate systems.

This includes only providing privileges that employees require for business functions, such as only having access to specific folders on a shared drive or server. This means that if a user's account is compromised, the attacker would be able to access a smaller amount of information, and data is less likely to be deleted or modified.

Ensuring that a process is in place for regularly updating software and solutions in line with the release of security patches or improvements is also important. This minimises the risk of vulnerabilities appearing in your system from out-of-date solutions.



Maintaining visibility over your IT estate

To ensure that any ransomware attacks can be managed and swiftly resolved, it's crucial to keep logs and backups of critical services, files and networks. This includes logging events into a Security Information and Event Management (SIEM) system, and storing this information for at least 90 days.

As well as increasing the chances of continued access to business-critical systems, this will also make investigating, tracking and remediating the damage caused by an attacker a far more streamlined process.

In today's complex and ever-shifting ransomware landscape, taking positive steps to secure your infrastructure can make a tangible difference.

To find out more about how we can strengthen your organisation's defences against the threat of ransomware, speak to our team.

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com

Insight Space

cyber insights
programme

nccgroup[®]

Executive Analysis

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

Lloyd Brough,
Technical Director at
NCC Group



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 reputational 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.

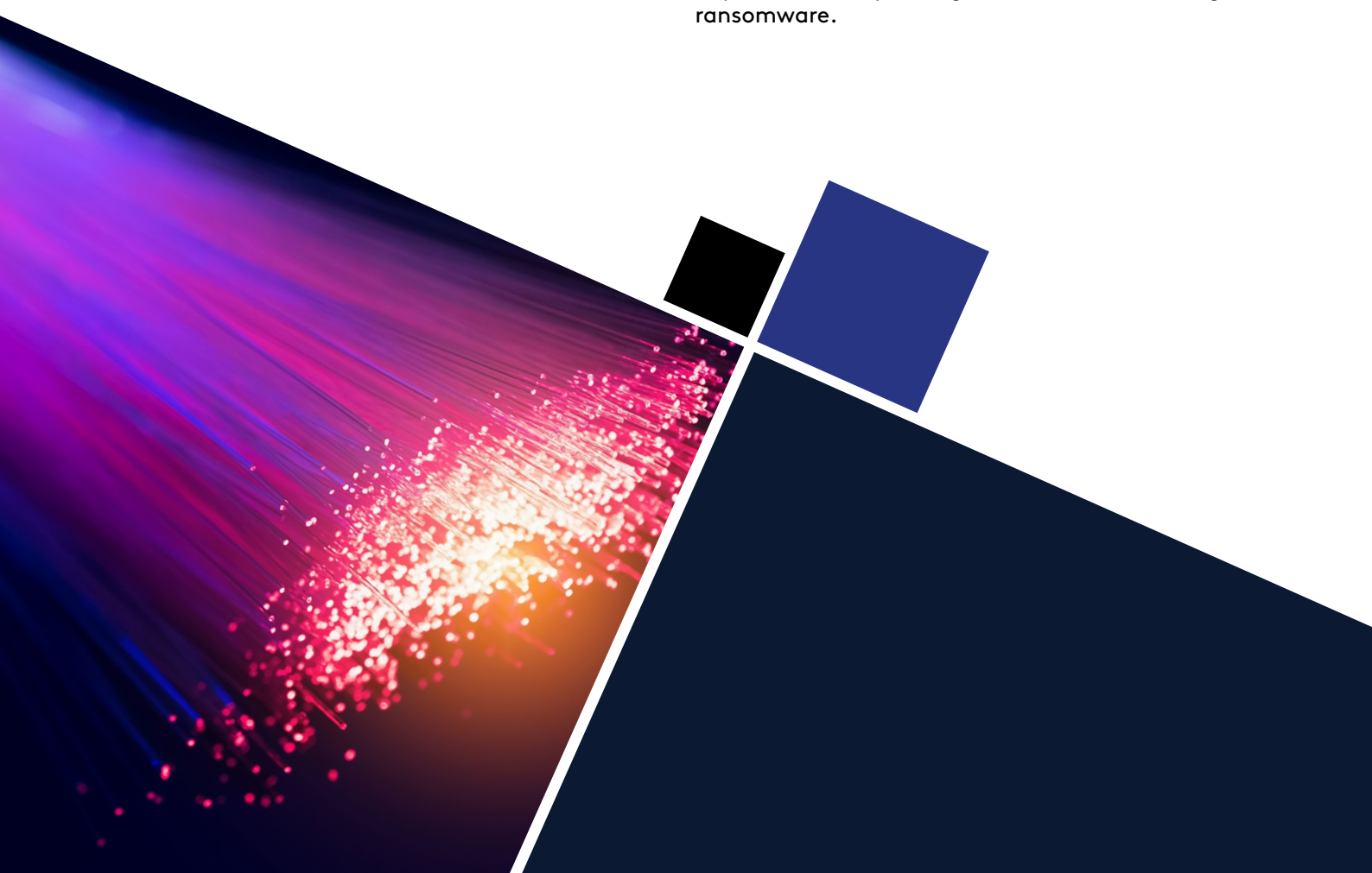


Create a security improvement plan

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.

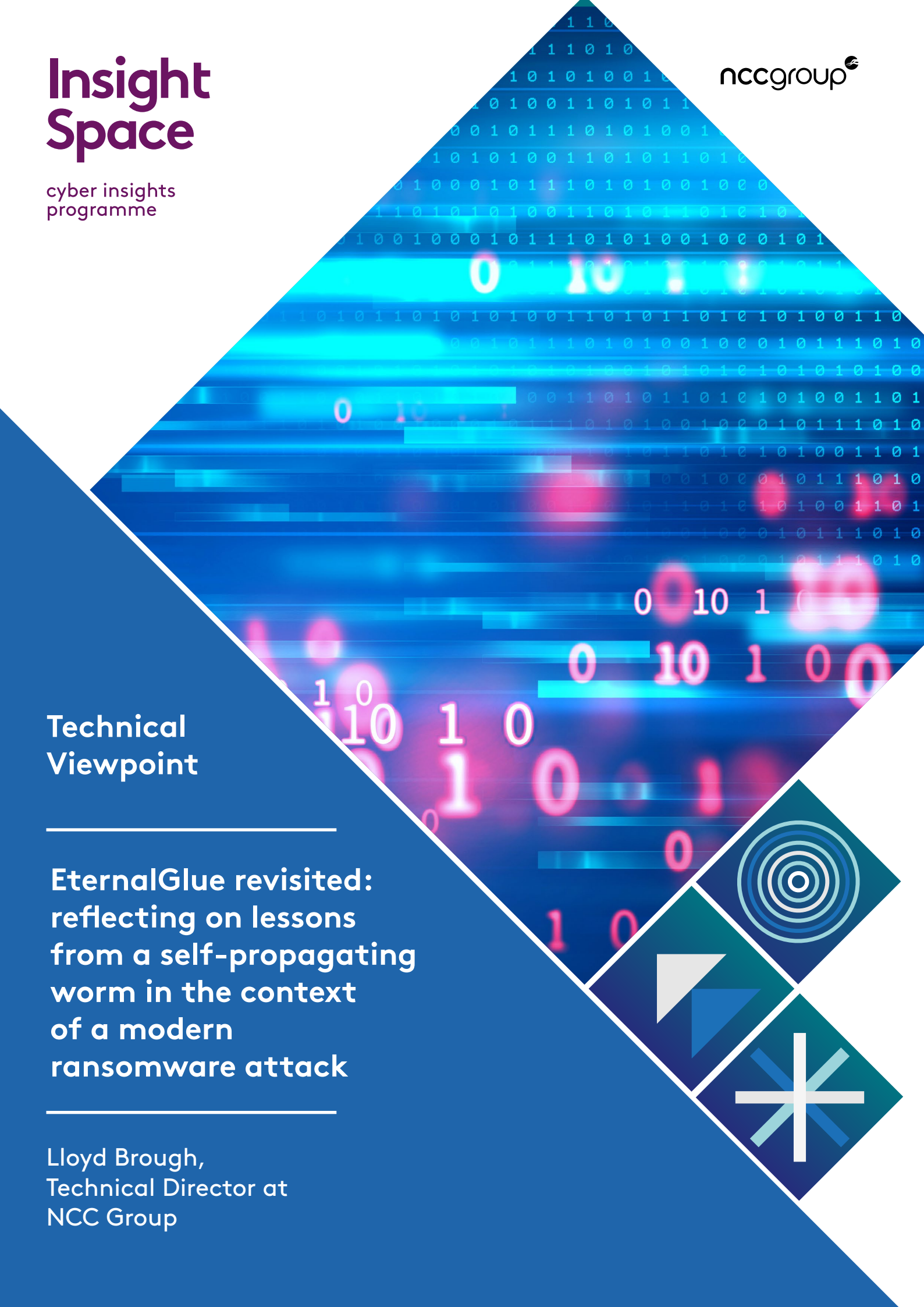
After you've prioritised your risks, you can create a structured improvement plan that focuses on urgent fixes to your most dangerous vulnerabilities, enhances and secures your organisation over the mid-term and implements more strategic mitigations to reduce risk in the long-term. Agile project delivery 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.



Technical Viewpoint

EternalGlue revisited: reflecting on lessons from a self-propagating worm in the context of a modern ransomware attack

Lloyd Brough,
Technical Director at
NCC Group

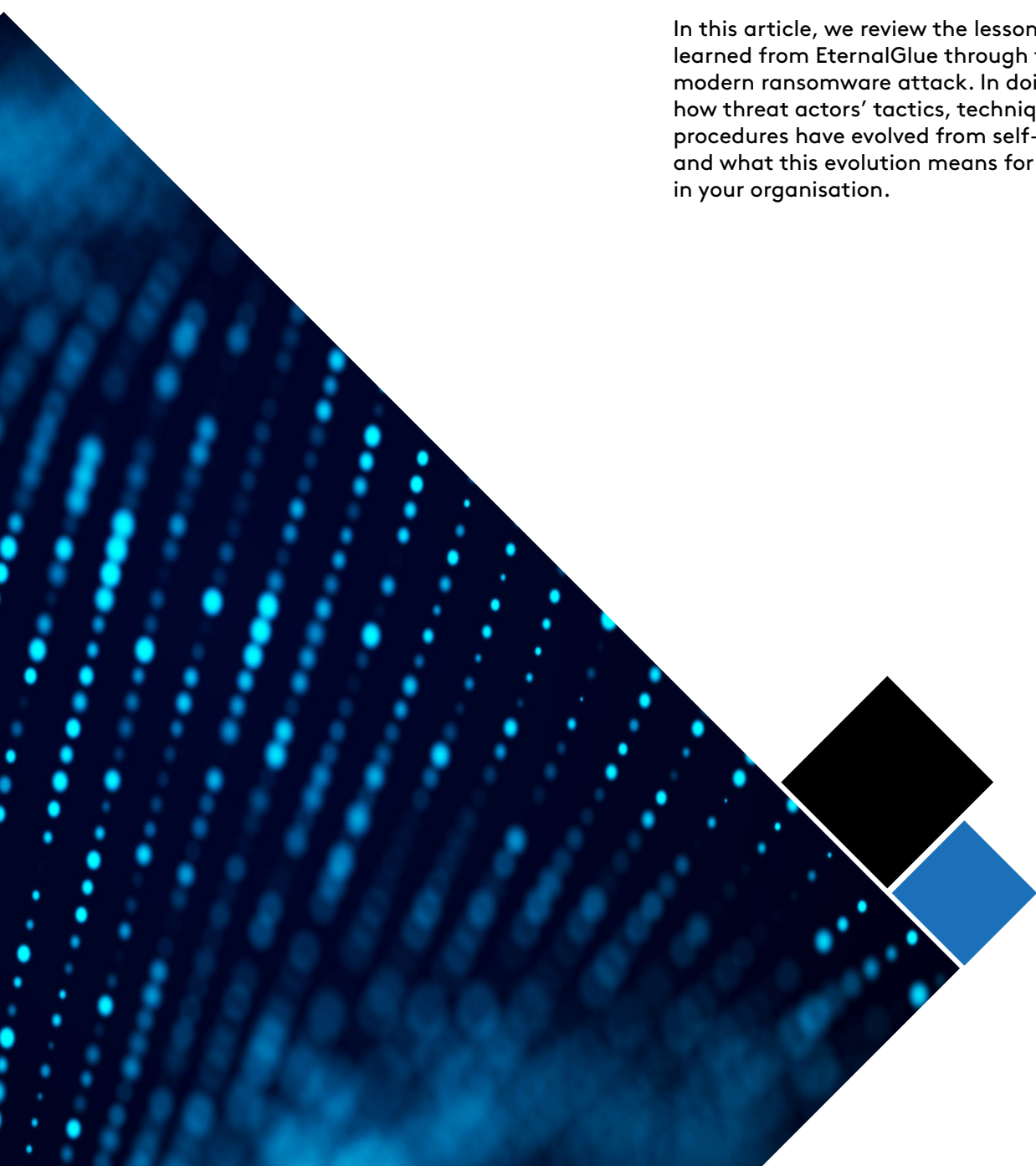


In June 2017, the NotPetya worm alerted boards, technical staff and the general public around the world to the threat of ransomware.

Unlike previous strains that encrypted data which could be recovered if paid for, NotPetya destroyed any of the hosts it was able to infect. It also propagated itself from one unpatched machine to another without relying on human or technical errors, enabling it to rapidly spread across entire networks and causing more than \$10 billion in estimated damages around the world.

Following NotPetya, boards and technical staff began to question how resilient their organisation was against such an attack. With that in mind, one client asked if we could create a simulation of NotPetya and deploy it within its network so that it could quantify its risk against this new threat. The result was EternalGlue, a safe and controllable self-propagating malware worm.

In this article, we review the lessons that we learned from EternalGlue through the lens of a modern ransomware attack. In doing so, we outline how threat actors' tactics, techniques and procedures have evolved from self-propagation, and what this evolution means for ransomware risk in your organisation.

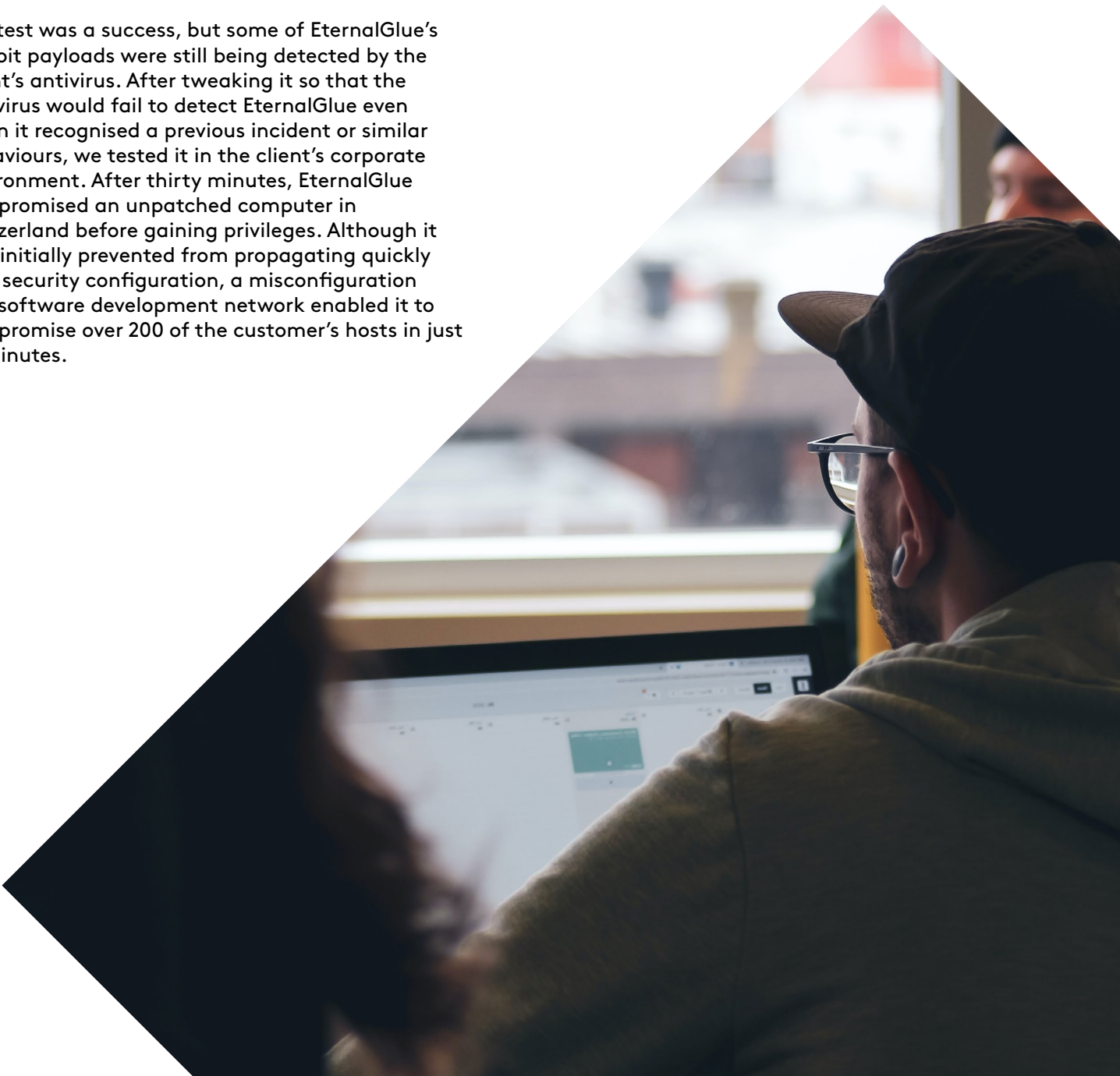


Launching EternalGlue in a live environment

The first live test of EternalGlue took place on a section of the customer's engineering network that was isolated from its corporate systems. After being deployed on a single machine with low privileges, EternalGlue found three unpatched machines and obtained system level access.

Within ten minutes, it spread itself through the entire departmental network using recovered or stolen credentials. Two minutes later, the domain controller was infected. When the client initiated the kill switch after 45 minutes, EternalGlue had compromised all 107 hosts on the isolated network.

The test was a success, but some of EternalGlue's exploit payloads were still being detected by the client's antivirus. After tweaking it so that the antivirus would fail to detect EternalGlue even when it recognised a previous incident or similar behaviours, we tested it in the client's corporate environment. After thirty minutes, EternalGlue compromised an unpatched computer in Switzerland before gaining privileges. Although it was initially prevented from propagating quickly by a security configuration, a misconfiguration in a software development network enabled it to compromise over 200 of the customer's hosts in just 15 minutes.



Self-propagation vs enhanced hybrid evolution

Since EternalGlue, ransomware has evolved beyond self-propagation. Many of the attacks that we've seen in recent years have been manually deployed by a human and used bespoke tactics to encrypt, destroy and steal data from entire organisations.

However, recent developments including exploits of 0days, the compromise of managed service providers (MSPs) and automation for lateral movement and privilege escalation indicate that threat actors are continuing to evolve their methods of attack.

Although the tactics, techniques and procedures have evolved since EternalGlue, the consequences of a successful ransomware attack remain the same: catastrophic damage and highly visible disruption. As such, the prevention of access to your network remains the best and only defence against modern ransomware attacks. With that in mind, here are the three key steps that you should take to reduce your risk:

PATCH

Patching is the first line of defence against ransomware. EternalGlue and almost every major ransomware attack started by infecting an unpatched device before spreading laterally across a network, so it's crucial that you include regular patching as part of a good cyber hygiene programme.

Creating an inventory of every device and system on your network and monitoring its status can help you to patch promptly as part of everyday operations and prevent threat actors from gaining an initial access vector in your organisation.

HARDEN AND SECURE

Next, you should reduce your susceptibility to ransomware by mandating that access to all of your externally facing systems requires multi-factor authentication. Then, apply least privilege concepts to lock down permissions across your network and segment it where appropriate.

Among other actions, you should also apply hardened build guides, including settings like the Attack Surface Reduction (ASR) Microsoft configuration. Hardening your endpoints and servers is critical. This includes application control, credential guard and exploit protection. Even simple steps like preventing servers from routing to the internet can help to derail an attacker.



Self-propagation vs enhanced hybrid evolution

CREATE A CULTURE OF RESILIENCE

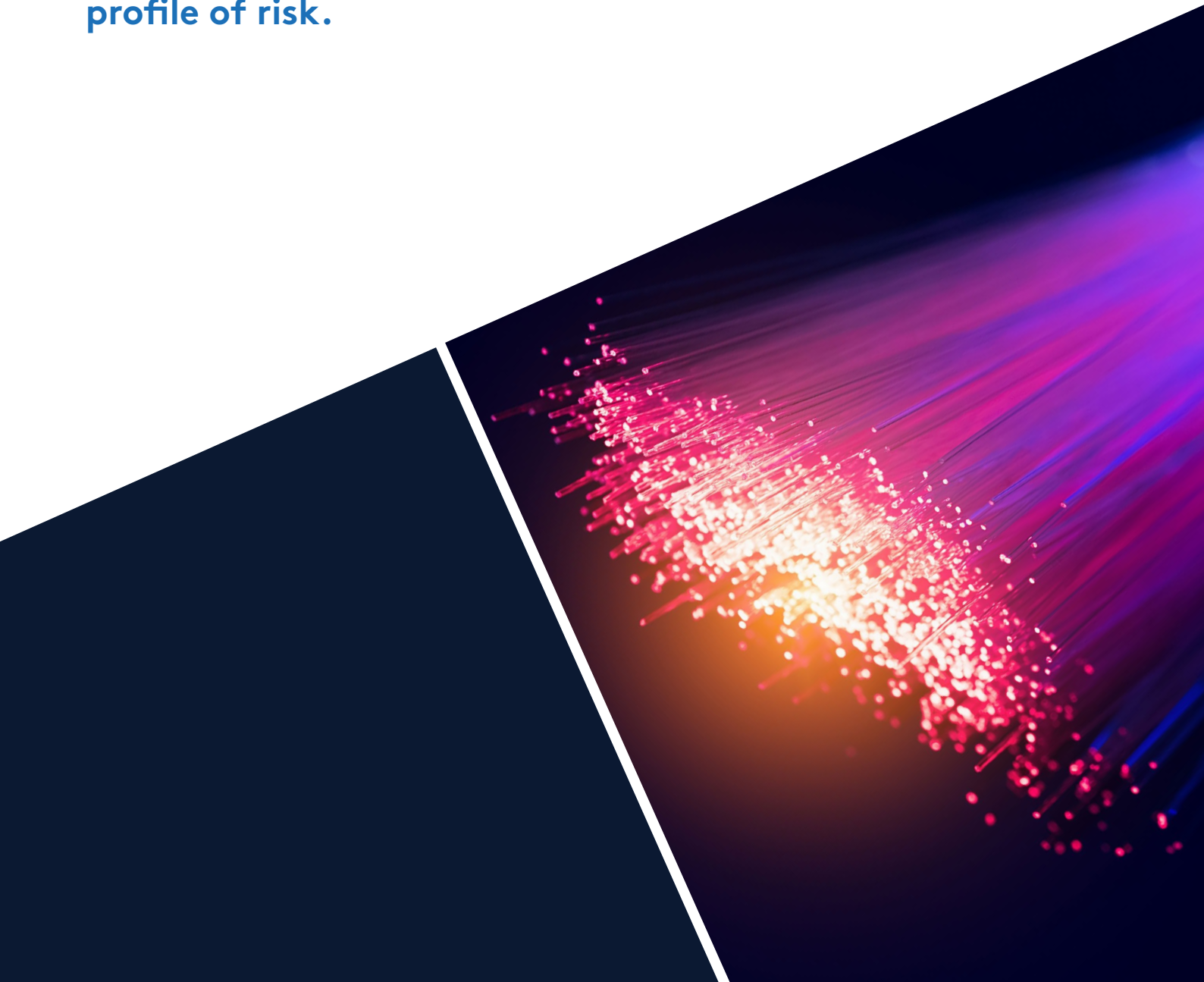
To create ongoing resilience against an attack, ensure that you have a tested continuity and disaster recovery plan. You should also create an incident management policy and supporting procedures that consider the operational impact of lost data and systems and empowers people to make decisions like calling in external help in the event of an attack.

Finally, ensure good cyber hygiene across your organisation by training your employees to identify modern phishing emails and enable them to flag suspicious activity with your IT team.



Preparing for the next big ransomware attack

Ransomware is a profitable crime, so threat actors will continue to develop new ways of infecting organisations with it. As such, it's highly likely that even more devastating attacks will occur in the future using a combination of new and existing techniques, potentially including a self-propagating strain like EternalGlue and human deployment. Prevention is the best form of defence, so it's essential that you act on the steps outlined in this article to maintain a low profile of risk.



Insight Space

cyber insights
programme

nccgroup[®]

Case Study

Response, rapid
remediation
and solution
implementation for a
charity organisation



NCC Group provided extensive support to a charity organisation after it fell victim to a ransomware attack.

The support consisted of a full investigation into the root cause of the attack and remediation of the organisation's vulnerabilities to protect the organisation against attacks in the future. NCC Group's support, guidance and expertise enabled the organisation to strengthen its security posture and save valuable time and resources in the process.

AT A GLANCE

Industry/Sector
Charity

Challenge
Providing support for a charity after it fell victim to a ransomware attack

Solution
The extent of the attack was ascertained, with key information identified and systems rebuilt to ensure services could be resumed

Results
Vulnerabilities were rectified, saving the organisation resources and time in the process



CHALLENGE

After falling victim to the ransomware attack, the charity enlisted NCC Group to investigate the incident, assist it in reasserting control of its estate and restore its critical services. The organisation also wanted to strengthen its security capabilities to protect itself against similar attacks going forward.

The organisation severely lacked resources that it could allocate to cyber security, and its small IT team was primarily focused on patching vulnerabilities as and when they occurred. This shortage, combined with an ongoing move to the cloud, meant that the charity did not have the time or the opportunity to perform or invest in necessary security upgrades and protections.

RESULTS

In addition to the ransomware attack being fully investigated and handled by NCC Group's CIRT, the Remediate team was able to rectify many of the vulnerabilities that were illuminated by the attack in the first place.

The project also saved the organisation a considerable amount of expenditure in both resources and time. This was particularly notable as the charity was initially considering outsourcing to one of its suppliers. It transpired that this supplier would have continued to use SFA as a security measure, which would have exacerbated one of the major vulnerabilities which led to the ransomware attack in the first place.

NCC Group has become a trusted advisor to the organisation and continues to work with it, having recently rolled out an Endpoint Detection and Response (EDR) capability across its estate.

SOLUTION

NCC Group performed two workstreams in parallel, with its Cyber Incident Response Team (CIRT) establishing the extent of the attack. Meanwhile, its Remediate team liaised with key stakeholders at the organisation to identify the information that was held on its estate, what systems were currently in place and which assets were mission-critical.

The team used this information to rebuild the charity's security infrastructure, enabling it to resume operations and ensuring that it could handle any potential breaches in the future. During the scoping exercise, NCC Group identified that the organisation was using single-factor authentication (SFA) for external services.

By collaborating with the CIRT team's investigation, it identified that the successful attack vector originated from credential stuffing from public breach data. As such, the team rapidly rebuilt the charity's finance system onto a cloud-based platform based in Microsoft Azure and secured it with multi-factor authentication and conditional access.

The team also helped the charity to rebuild its on-premise domain controllers to operate wider services and implement group policy server hardening to further bolster its security controls. This was combined with a full password reset programme with proactive auditing and filtering against known breached accounts.

Finally, the NCC Group Remediate team assisted the charity with setting its network up to operate via a cloud-based platform and through ExpressRoute, allowing its users to seamlessly access their internal networks.

Insight Space

cyber insights
programme

nccgroup[®]

Case Study

**Delivering essential
assurance,
monitoring and
detection services
for a university**



A leading university enlisted NCC Group to validate its cyber security posture.

After NCC Group identified multiple improvements that needed to be made to bring the organisation's security to the required standard, it was enlisted to design a comprehensive security package that included a Managed Detection and Response (MDR) solution.

The university was supporting essential research into COVID-19 and required assurance that its solution was fully secure, so the engagement was time-critical.

AT A GLANCE

Organisation
University

Industry/Sector
Higher education

Challenge
Providing assurance, monitoring and detection services for a university with 30,000 students

Solution
NCC Group consultants designed a multi-layered solution, including MDR, Security Information Event Management (SIEM) and 24/7 Security Operations Centre (SOC) monitoring

Results
The organisation's security has improved, and its research endeavours are much better protected by NCC Group's monitoring and detection services



CHALLENGE

With around 30,000 students across six faculties, the challenge was considerable. From previous experience in the higher education sector, NCC Group has learnt that securing universities from cyber threats can be more complicated than in other sectors. Student bodies' liberal expectations of information sharing need to be balanced with the requirement to protect the university's extremely valuable intellectual property. A nuanced and segmented approach to risk is required.

As is often the case with large organisations that have a user base with high turnovers, one of the most fundamental security requirements was an accurate understanding of the enterprise deployment in a way that could be digested by security teams. Once baselined, the next priority was to implement a solution that could identify malicious activity at the earliest possible stage and accurately report incidents so that effective remediation could be conducted. A solution that worked equally well for on-prem and cloud architectures was also required, as the customer operates an enterprise that draws on both designs.

SOLUTION

NCC Group consultants designed a multi-layered solution, including an MDR suite incorporating SIEM, endpoint detection and network detection with a unifying service wrap centred on a SOC facility. Under NCC Group's project management, the full service was deployed progressively.

The specific requirement to deploy a full network discovery and access control solution had not been delivered in the managed service model previously. However, NCC Group developed the service at pace, implementing a working solution in tandem with the other elements of MDR.

COVID-19 CHALLENGE

A further challenge was presented at short notice during the deployment. The customer was involved in research supporting a World Health Organisation (WHO) trial and needed to establish dedicated infrastructure to contribute to the global megatrial of the four most promising coronavirus treatments. They urgently required assurance that their solution was secure and fit for purpose. The request was time-critical, and NCC Group worked around the clock to ensure that the infrastructure was penetration tested, remediated and added to its 24/7 monitoring within three days.

RESULTS

Following NCC Group's engagement, the customer has a comprehensive managed service in place that informs its in-house security team quickly, and only when they need to be informed, allowing them to focus exclusively on what matters.

The result is an organisation that is more informed and more secure, enabling the university to continue to conduct its research with greater peace of mind that it is equipped to handle any potential security incidents.

Insight Space

cyber insights
programme

nccgroup

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