Insight Space

cyber insights programme

nccgroup

ISSUE 06

SUPPLY CHAIN RISK

A back door for hackers?

The rise of cyber security risks in company supply chains

How to detect, prevent and respond to supply chain attacks

How to reduce supply chain risk

February Threat Pulse Report

Global. Transformative. Resilient.

UK ◆ North America ◆ Europe ◆ Australia ◆ Singapore ◆ Japan ◆ China

Introduction

Working with suppliers can deliver a range of benefits for organisations, enabling them to reduce costs, increase efficiencies and strengthen operations. As a result, modern supply chains often involve thousands of third parties that are connected to companies' systems and networks.

These integrations enable suppliers to access the data they need to carry out their roles, but they can also increase organisations' cyber risk by widening their potential attack surfaces.

Our latest global research of cyber security decision makers suggests that hackers are increasingly targeting organisations through their suppliers: attacks on supply chains have increased by 51% in the last six months. Encouragingly, respondents acknowledged third-party and supplier risk as one of their top three challenges for the next 6-12 months and plan to increase their security budgets this year. However, our findings uncovered specific areas for improvement concerning third-party risk management. These include a lack of clarity around responsibility for preventing, detecting and resolving attacks, and minimal controls around supplier assurance, so it's important that any investment addresses these areas.

With that in mind, this global edition of Insight Space explains how organisations can reduce supply chain risk and detect and respond to an attack. We summarise the results of our research, including insights into organisations' security postures and budget plans, and outline the latest threat actor behaviours and trends in our threat intel report.

And, for even more insight into supply chain risk, sign up to our forthcoming virtual event with Ade Clewlow, Rick Tahesh, Vincent de Vries and Ishan Gridhar. We'll be asking 'The Big Three' questions around third-party risk, giving you the knowledge you need to realise the benefits of supply chains without worrying about its impact on your security posture.

Sign up to our upcoming virtual event on 'The Big Three'

REGISTER HERE FOR VIRTUAL EVENT >

Ollie Whitehouse
CTO, NCC Group

Supply Chain Risk

A back door for hackers?
The rise of cyber security risks in company supply chains.

Cyber security attacks on company supply chains have increased sharply in the past year, but there is confusion about whether companies or their suppliers are responsible for keeping supply lines secure

Introduction

Supply chains around the world have been under severe strain in the past two years during the pandemic. Some experts have warned that shortages in global supply chains for things ranging from computer chips to alcohol and brown sugar could last for another two years.

For companies, the prolonged disruption to supply chains is creating cyber security problems as well as logistical ones. Last year, a security vulnerability known as Log4j in widely used open-source software vulnerability, highlighted the difficulty of keeping track of and fixing security problems in convoluted global supply chains.

Our latest research suggests that Log4j is far from an isolated incident. Cyber security attacks on company supply chains have increased by 51% in the past six months, according to our global survey of approximately 1,400 cyber-security decision makers at large companies in 11 countries including the UK, United States, China, Germany and Singapore.

Encouragingly, our respondents recognised third-party and supplier risk as one of their top three challenges for the next 6-12 months and plan to increase their security budgets this year. However, our research uncovered some glaring security issues around third-party risk, so it's crucial that organisations address these issues alongside any investment in security products and services.

Encouragingly, our respondents recognised third-party and supplier risk as one of their top three challenges for the next 6-12 months

51%

Cyber security attacks on company supply chains have increased by 51% in the past six months according to our global survey

> "Supply chains around the world have been under severe strain in the past two years during the pandemic. "

Supply chain confusion

Despite the severity of security risks to supply chains, there is confusion among companies about whether a company or its suppliers are responsible for keeping them secure.

Around one in three (36%) of respondents in our research said that they are more responsible for preventing, detecting and resolving supply chain attacks than their suppliers. Just over half (53%) said that their company and its suppliers are equally responsible for the security of supply chains.

This ambiguity could increase organisations' third-party risk if it means that they are not conducting the appropriate due diligence on their suppliers, and could expose them to regulatory penalties. The EU's Digital Operational Resilience Act (DORA) mandates that financial entities include key security requirements in their contracts with third parties, indicating that regulators across the globe are increasingly emphasising the organisation's role in supplier risk management.

Our research also highlighted room for improvement here: half (49%) of the organisations we surveyed said that they did not stipulate security standards that their suppliers must adhere to as part of their contracts. One in three (34%) said that they do not regularly monitor and risk assess their suppliers' cyber security arrangements, so there is a big opportunity for organisations to get ahead of the curve and tighten their supplier risk management now.

36%

of respondents said that they are more responsible for preventing, detecting and resolving supply chain attacks than their suppliers

A growing threat?

Supply chain attacks were one of the top three types of cyber attack to increase in the last 6 months, behind phishing and malware and attacks of operational technology. Concerningly, only one in three (32%) respondents were "very confident" that they could respond quickly and effectively to a supply chain attack.

Despite this gap between the rate of attacks and organisations' ability to deal with them, just one in four (24%) named third-party and supplier risk as a major cyber security challenge for the next six to 12 months. Many plan to invest in new third-party software, hardware and SaaS security products in 2022, which could further complicate organisations' supply chains and increase their attack surfaces.

32%

of respondents were "very confident" that they could respond quickly and effectively to a supply chain attack

Security challenges

The top challenges for organisations over the next 6–12 months are:

- Data privacy
- Understanding the threat landscape post Covid-19
- Finding a way to measure/report the effectiveness of cyber security and
- Third-party and supplier risk

When we asked decision-makers about their organisation's resilience against such threats, they presented a mixed picture. Six in ten (57%) said that they were "quite resilient" while one in three (34%) said that they were "very resilient."

34%

of decision-makers said their organisation's resilience was "very resilient."

33%

of decision-makers said that they could respond to a cyber attack within four hours.

Speed of response

Thirty-three per cent of decision-makers said that they could respond to a cyber attack within four hours, followed by 28% (one day), and one hour and one week (jointly at 14%). However, only one in three (34%) said that they were "very confident" that they could quickly identify the root cause of the breach, with the same percentage reporting that they were "very confident" they could fix the root cause to prevent it from happening again.

There is uncertainty about whether some companies would be able to meet regulatory requirements for information security and report a cyber breach to the relevant authorities, too. Forty-five per cent of respondents said they were "fairly confident" that they could report a data breach to authorities according to any local legal or regulatory obligations.

> "There is uncertainty about whether some companies would be able to meet regulatory requirements for information security and report a cyber breach to the relevant authorities."

Spending increases

After freezes and cuts to company IT security budgets during the last couple of years, budgets are set to rise again this year – by an average of 10%, according to our research.

Threat detection and response (32%), cyber security reviews and assessments (25%), security awareness and training (14%), training and testing (infrastructures and application) represent the top priority spend areas for our respondents in the next 6-12 months.

Meanwhile, managed security services (54%), off-premise cloud integrated security products (44%) and hardware-based third-party security products (42%) will see the largest proportional increases in budget.

10%

IT security budgets are set to rise again this year – by an average of 10%, according to our research.

RESEARCH SUMMARY

Cyber security attacks on company supply chains have increased by **51%** in the past six months, according to an NCC Group survey of approximately 1,400 cyber security decision makers at large companies in 11 countries, including the UK, United States, China, Germany and Singapore. The survey was conducted in December 2021 and January 2022.

Respondents said that they planned to increase their cyber security budgets by an average of **10%** in 2022.

One in three (**34%**) of companies surveyed said that they do not regularly monitor and risk assess their suppliers' cyber security arrangements.

Despite the severity of security risks to supply chains, there seems to be confusion among companies about whom – a company or its suppliers – is responsible for keeping them secure.

Priorities for cyber security investment this year include threat detection and response, cyber security reviews, security training and security testing.

TECHNICAL VIEWPOINT

How to prevent, detect and respond to a supply chain attack

Rick Tahesh
Associate Director, NCC Group

Supply chains at large organisations often include thousands of enterprises, partners, service providers, contractors and other suppliers. Managing risk across these complex networks is difficult, so there is a huge dependency on trust across global supply chains. However, recent cyber attacks have targeted organisations through their third parties, so relying on trust to provide strong business assurance without strong measures and controls is simply an illusion.

Threat actors can exploit supply chains in various ways, including:

1. **Open-source software**
   Attackers introduce code into builds that get installed or leveraged by organisations' systems.
2. **Third-party software**
   Attackers target third-party systems and compromise them by introducing malware or trojan-ware.
3. **Software development tools**
   Attackers compromise legitimate websites through website builders and other methods.
4. **Service provider data stores**
   Attackers target outsourcing partners and service providers to exploit organisations' data and assets.
5. **Stolen certificates**
   Attackers introduce malicious code under the guise of trusted organisations' certificates.
6. **Firmware attack**
   Attackers target access to firmware and introduce malware to enable them to gain access to organisations' data and systems.

The following example illustrates a supply chain attack using open-source software

A banking organisation partners with an open-source software developer's party.

Threat actors receive intelligence of the banking organisation partnership.

The banking organisation uses the open-source software in one of its applications.

Threat actors compromise one of the developer's GitHub accounts through a phishing attack.

Using the compromised GitHub account, the threat actors insert malicious code into the open-source software library with a trojan horse.

The software library is packaged, along with the trojan horse, for release.

The banking organisation installs the latest release of the open-source software and with it the trojan horse.

Threat actors now have full access to the banking application.

The nature and complexity of supply chains and the tactics, techniques and procedures that threat actors use to exploit them require a broad set of governance and technical cyber security controls to mitigate against such attacks. In this paper, we highlight some of the key requirements that CISOs need to consider to prevent, detect and respond to supply chain threats and attacks.

Prevention

Building resilience against supply chain attacks requires a multi-layered prevention strategy that includes a number of key components.

Awareness

Firstly, it's crucial that you know which entities make up your supply chain pool by conducting a comprehensive discovery exercise involving your procurement, finance, legal, BCM, IT, cyber and other teams from across the business. Then, you can better understand your supply chain risks by gaining clarity on the services and products that your suppliers provide you with, as well as the access they have to your environment and data assets. Finally, you can use this intel to prioritise assurance for those services and products based on their value, criticality and priority to your organisation and the risk attached to the suppliers that support them.

Help you better understand your supply chain risks by gaining clarity on the services and products that your suppliers provide you with

1 in 4

cyber security decision makers do not rigorously audit the results of their suppliers' risk assessments

Assurance

To maintain ongoing assurance around your supply chain, develop a supply chain risk management framework that is supported by supplier assurance policy, processes and controls. This could include roles and responsibilities for key business functions that interact with third parties, and working with your procurement team to integrate their supplier onboarding process with cyber security, BCM, technology, risk and compliance processes.

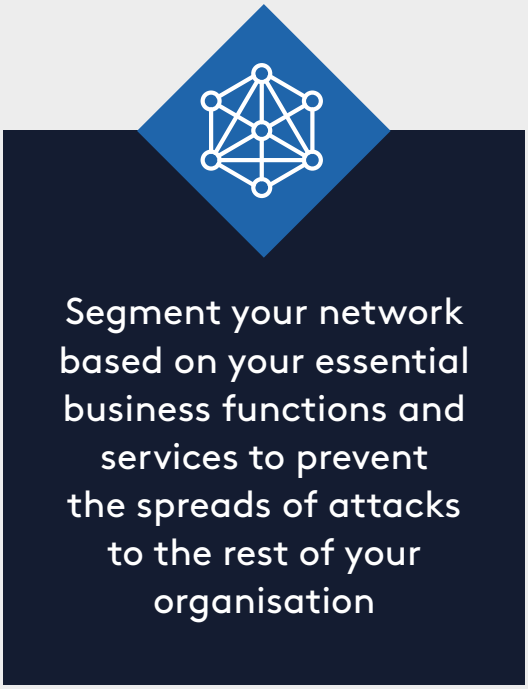
According to our global survey of 1,400 cyber security decision makers, one in four do not rigorously audit the results of their suppliers' risk assessments. This should be a non-negotiable, so ensure that the right to audit and appropriate security reporting measures are included in any RFIs, RFPs and contracts, alongside security requirements and clauses.

Finally, you should assess your vendors and suppliers regularly with a focus on high-risk providers. Adopt different approaches to assessments that commensurate with the risk profile of suppliers, such as tailored security control questionnaires supported by evidence gathering, pen testing, input from vulnerability scanning tooling, certification and other assurance reporting measures.

Isolation and segmentation

Threat actors can infiltrate a supplier before moving through the chain until they reach their target. Excessive privileges and permissions make supply chain attacks much easier, so adopt least privilege access controls, always assigning least privilege to your suppliers, software processes and employees. You should also segment your network based on your essential business functions and services to prevent the spreads of attacks to the rest of your organisation.

Implementing security-by-design by ensuring secure and safe software and application development practices at the supplier end as well as your own should also fix known software vulnerabilities and support the operation of secure applications.



Detection

Timely detection of supply chain attacks rely on comprehensive coverage of suppliers' connections and activities across your networks, systems and applications. Consider monitoring through a Security Operations Centre (SOC), which can detect and respond to incidents in real time. You should also introduce automated security controls to break off suppliers' connections in case of access violation or attempted breach. For ongoing detection, test your software applications and network using pen testing and vulnerability scanning regularly, and frequently apply integrity checks on new, updated or patched software to detect any changes to software code that could indicate a malicious attack.

Respond

Responses to incidents and breaches in your supply chain should be built into your organisation's incident response plan. This plan should ensure that security incident reporting clauses are part of your suppliers' legal and contractual agreement with your business. Similarly, ensure you have an agreed media and stakeholders' communication plan with your suppliers, to effectively manage public and stakeholders' relations following any major security breaches.

Finally, develop appropriate incident response play and run books, based on up-to-date real-world scenarios, to handle and respond to incidents from within the supply chain. Regularly test those plans and scenarios with your key suppliers and partners to keep everyone updated and well-practiced for incidents.

Conclusion

Our research shows that supply chain attacks have increased by 51% in the past six months. Despite this, many of the organisations that we spoke to planned to invest in new third-party software, hardware and SaaS security products in 2022, which could increase the third-party threat vector for malicious actors. All of this makes it crucial for technical decision makers to act now to prevent, detect and respond to this growing threat.

Top five actions to prevent, detect and respond to supply chain attacks

1. Be aware of your critical assets, the suppliers that support them and the risks to the business if they were compromised.
2. Maintain ongoing supplier assurance with policy, processes and controls including security requirements in RFI, RFP and contracts and ongoing security assessments.
3. Adopt least privilege access controls for third parties, segment your network and implement security-by-design.
4. Implement a Security Operations Centre (SOC) to continually monitor, detect and respond to indicators of supply chain attacks.
5. Integrate supplier management into your incident response plan, including real-world scenarios and communication plans following an incident.

Global. Transformative. Resilient.

Could you respond to a cyber attack on your supply chain?

28 April at 12:00pm – 12:45pm (GMT)

Join our free upcoming webinar, **'The Big Three,'** where we'll explore third-party risk in more detail and answer three key questions:

1. How do you even start to identify / define your digital supply chain?
2. Do service providers or suppliers hold all the power in a customer supplier relationship?
3. Are we right to focus on supply chain security risks rather than developing resilient, responsible and sustainable supply chains?

Ade Clewlow
Senior Advisor, NCC Group

Rick Tahesh
Associate Director, NCC Group

Vincent de Vries
Chief Information Officer, Fox-IT, part of NCC Group

Ishan Gridhar
Founder and CEO at Privva

REGISTER HERE FOR VIRTUAL EVENT >

How to reduce supply chain risk

Sam Thornton
Associate Director, NCC Group

Working with suppliers is business-as-usual for most large organisations around the world.

According to our recent global survey of 1,400 cyber security decision makers, many plan to invest in new third-party software, hardware and SaaS products this year. These solutions can strengthen operations and increase efficiencies, but they can also increase organisations' cyber risk by providing new avenues for hackers to infiltrate their networks and systems.

Left unchecked, this risk can result in data loss, regulatory fines and reputational damage. Attacks on supply chains have increased by 51% in the last six months, so it's vital that organisations act to reduce their third-party risk now. In this article, we explain how businesses can combat these threats by adopting a risk-based approach to supplier management, and outline the questions that decision makers should ask of their suppliers to reduce third-party risk.

51%

increase of attacks on supply chains in the last six months

Applying a risk-based approach

A risk-based approach requires organisations to understand the assets that are critical to their goals and objectives, where those assets are located across their people, process and technology, and the risks to the business if they were compromised.

As a result, decision makers can identify, manage and monitor the suppliers that support critical assets more effectively, and understand the potential threats and impacts on the business in the event of a supply chain attack.

For example, organisations can identify early warning signs for potential contractual failures by continually monitoring key suppliers and the levels of access they have to the network and applications. By doing so, they can identify any unusual behaviour that could indicate an attack on the supply chain, such as misconfiguration of access credentials, and respond accordingly.

Ultimately, a risk-based approach to supplier management forces organisations to pay attention to the data involved in supplier contracts and services. Armed with this knowledge, decision makers can develop a comprehensive supplier assurance program to protect that data as part of a wider risk management program.

Identify

Manage

Monitor

Asking the right questions

Taking responsibility for third-party cyber security is a key aspect of any supplier assurance program.

However, 53% of cyber security decision makers believe that they and their suppliers are equally responsible for the security of supply chains according to our research. Regulators are increasingly emphasizing the organisation's responsibility for supplier risk management, making it impossible for decision makers to outsource responsibility for a cyber attack.

53%

of cyber security decision makers believe they and their suppliers are equally responsible for the security of supply chains

Do we know who our suppliers are?

This should include any sub-contractors involved, their approach to risk management and their commitment to following the organization's cyber security controls.

Do we know what our suppliers are doing?

Ask whether your organisation knows which assets are supported by third-party suppliers, how critical they are to the business, and the impacts if exploited.

How are we assessing and monitoring our suppliers?

One in three respondents told us that they do not regularly monitor and risk assess their suppliers' cyber security arrangements, putting them at increased risk of a third-party cyber attack. Ensure that you know when a supplier isn't compliant with a contract or service agreement, or isn't following defined security controls. Ask how often you assess and monitor suppliers, and confirm that contracts and service agreements include key performance indicators.

If an incident does occur, can we detect it and recover from it?

Are your incident response and business resiliency plans up to date? Have they been tested, are they looking at the right things (people, process, technology) and are they fit for purpose? If not, these should be addressed as priorities to mitigate supply chain risk.

Modern supply chains are complex and wide-reaching, so managing third-party risk can feel like a difficult task. In fact, only 32% of respondents to our survey were 'very confident' that they could respond quickly and effectively to a supply chain attack. However, by adopting a risk-based approach to supply chains, organisations can begin to reduce their third-party risk and work with suppliers in confidence.

Five actions to reduce supply chain risk

1. Understand what your business objectives and critical assets are, and which assets are supported by third parties.
2. Fully understand the services provided by suppliers and the value of any data, infrastructure, or platforms that they have access to.
3. Apply a risk-based approach to selecting and assessing suppliers, and ensure contracts include confidentiality clauses, appliable security and regulatory controls and key performance indicators.
4. Continually monitor supplier performance and adherence to contractual obligations, including their handling of any associated data.
5. Ensure business incident identity, response and resiliency plans are fit for purpose and regularly tested.

February 2022 Threat Pulse

NCC Group's Strategic Threat Intelligence Practice has been working tirelessly to develop various software solutions for a broader, more insightful look at current threat landscapes and the way they impact businesses around the world.

Our technical team has developed a web scraper, which we use to gather data on ransomware data leaks on the dark web in real time to give us regular insights into who are the most recent ransomware victims. By recording this data and classifying the victims by sector, we are able to derive additional insights highlighting the sectors that have been targeted, and how current ransomware threats compare to previous months.

In this edition, we share a summary of our findings in February 2022.

Analyst comments

The number of victims of double extortion ransomware attacks increased 52.89% between January and February. This increase represents a marked exit from the seasonal reduction in ransomware behaviour observed by the team across December and January.

This pattern also echoes NCC Group's 2021 findings, where a 55.1% increase was observed between January and February. The team assesses that the volume of ransomware incidents will continue to increase as the year unfolds and threat actors get back to 'work'.

52.89%

increase in the number of victims of double extortion ransomware attacks between January and February

Analyst comments

In terms of key threat actors, the top players remained consistent in February. Lockbit 2.0 remains the most persistent contributor with 42.2% of all attacks. The sector most targeted by Lockbit 2.0 was industrials, accounting for a sizeable 30.77% of their total attacks in February. This remains consistent with attacks in January, when businesses in the industrials sector accounted for 31.7% of their victims.

Conti remains the second largest player with 17.8% of attacks. However, the third largest contributor in February was BlackCat, as opposed to Snatch in January. BlackCat accounted for 11.4% of all attacks – a significant rise on the 5% that they exhibited in January, showing a steady increase in their activity.

Consistent with the team's findings in January, Industrials was the most targeted sector - making up 35.68% of attacks – whilst consumer cyclicals was the second most targeted sector with 21.62% of attacks. NCC Group analysis suggests that the increase in number of attacks in these sectors compared with January was responsible for the overall growth observed by the team this month.

The leading positions of these two sectors reflects wider observations from the last 7 months, suggesting they continue to be seen as highly attractive targets.

As in January, an equal number of attacks were observed in North America and Europe. Last month, this was an abnormal finding, as up until then, North America had adopted a clear leading position. This month, however, the team again observed an equal number of ransomware incidents in the two continents, with both suffering 78 incidents respectively.

42.2%

Lockbit 2.0 remains the most persistent contributor with 42.2% of all attacks

35.68%

Industrials was the most targeted sector - making up 35.68% of attacks

Spotlight: Conti Group

There was significant activity across the security community in relation to Conti Group in February.

The group posted a 'warning' message on its public facing blog site, officially announcing its full support of the Russian government. This was later amended to state that they are not allied with a government, however they also stated that they will retaliate against any targeting of Russian critical infrastructure, suggesting they are sympathetic to the Russian government.

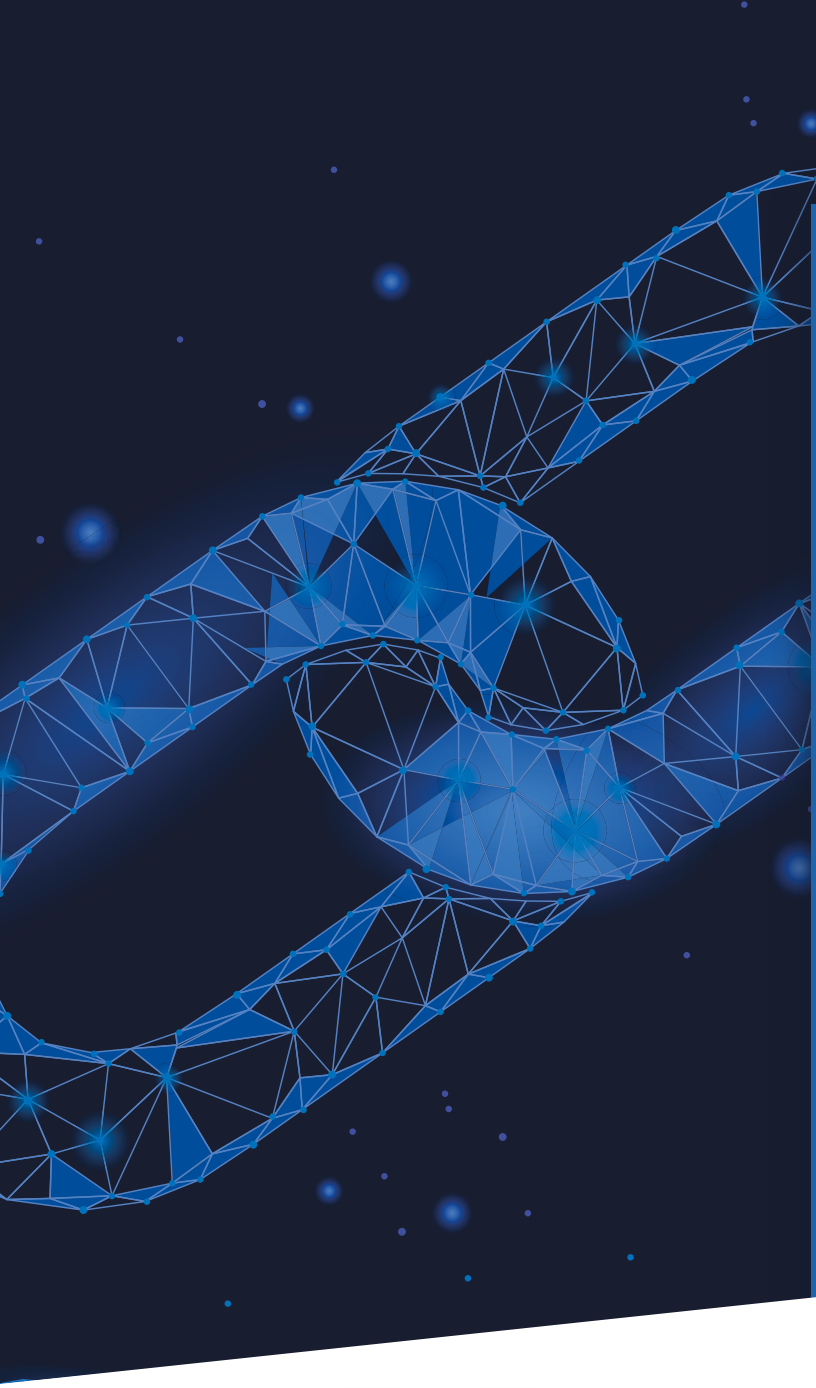
In response to the incident, an anonymous member of the group released a significant amount of internal communications, screenshots and tactics used by the gang.

Matt Hull, cyber threat intelligence manager at NCC Group, said:

"With ransomware attacks increasing – as would be expected after the seasonal reduction in January – it is vital that organisations continue to ensure they apply appropriate security measures. This is especially important for the Industrials sector, which continues to be the most frequent victim of ransomware."

"It's interesting to see a regional trend emerging in Europe and North America, with both regions seeing the same number of victims of double extortion ransomware attacks. By continuing to closely monitor if this pattern persists, we will be able to determine what this means for the wider European threat landscape."

"The disruption in Conti activities comes as a welcome change, but with clients continuing to come under new attacks, it is clear that this ransomware variant is still very much in use. Our Strategic Threat Intelligence team continues to keep an eye on the use of Conti, and as always will provide updates to our customers to help them manage the risk to their organisations."



Key takeaways

- Ransomware attacks increased by 52.89% compared to January, with the number of incidents rising from 121 in January to 185 in February.
- The most targeted sectors were industrials (35.68%), consumer cyclicals (21.62%), and technology (8.11%).
- The most targeted regions were North America (42.16%), Europe (42.16%), and Asia (10.27%).
- Lockbit 2.0 remains the most consistent threat actor, accounting for 42.2% of all attacks.

Keep up to date with our latest insights

Never miss a threat intelligence update - sign up to receive our monthly insights into the emerging advances in threat landscape and for our next quarterly Threat Monitor webinar here.

SIGN UP FOR THEAT MONITOR WEBINAR >

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 3,000 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 we can help you address legacy security issues to build your organisation's cyber resilience, speak to our team today.

www.nccgroup.com

UNI104675