nccgroup

FOX IT
part of nccgroup

Insights

Pragmatic cyber security advice for senior executives

Edition

Growing Threats

The shifting sands of cyber threats

Optimising phishing and malware defences with threat intelligence

Industrial, financial and tech companies under attack. What can we learn?

GLOBAL • TRANSFORMATIVE • RESILIENT

Introduction

Cybersecurity threats are evolving. How do we adapt today, to protect ourselves tomorrow?

Welcome to the latest issue of Insights, a knowledge hub for senior leaders and executives across the globe.

Every quarter we delve into the latest cybersecurity challenges and offer actionable advice to tackle them, so we can collectively work to make the world safer and more secure. From a personal perspective, this is the first issue I have had the opportunity to work on since assuming my new role as CEO. It has been a pleasure to see our global teams come together to deliver another invaluable issue, backed by the latest threat intelligence research and analysis.

Our society is evermore online, evermore digital, evermore connected. And though it brings doubtless benefits, it creates complex risks. Coupled with complicated digital supply chains and an evolving global threat landscape, businesses are today facing some of the most pressing cybersecurity challenges of our time.

In this issue, we dive into these challenges, tracking the shifting sands of the cyber threat landscape. Our findings are clear: attacks are proliferating across the globe, with North America, Europe and Asia Q2's most targeted regions. Threat actors are weaponising new, more sophisticated, easily accessible methods - 47% of all ransomware attacks between April and June deployed off-the-shelf tools. Key industries – particularly industrials, financial services and technology – are proving to be prime targets for exploitation: industrials suffered 34% of attacks in the second quarter of the year.

And though our research shows there is promising improvement in organisations' ability to respond swiftly to attack – 84% responding within a day, a 30% increase on previous years – only a third of businesses would rate themselves as 'very resilient' against attack.

So, it is clear that there is still work to be done to educate, enhance the ability to respond to attacks and grow confidence in organisational cyber resilience. And, the focus must not only be on responding to existent attacks, but protecting against potential future threats too. We need to ask ourselves: how do we adapt today, to protect ourselves tomorrow?

Business leaders shouldn't be expected to know how to do this alone – enter Insights, where we bring together deep technical expertise and business perspectives. With evolving cyber risks an ever more critical challenge in our digitally transformed world, we want to equip you with the tools to remain resilient. In this issue, you can hear from our global specialists, keep up-to-date with the latest threat intelligence, and learn from those battling these security threats every day. You can also discover our game-changing new tool for streamlined incident response, Dissect – open source software that will ultimately keep our online and offline worlds safer and more secure.

Plus, in our upcoming virtual event, Growing Threats: Are you ready? I'll be joined by BBC journalist Geoff White, host of the incredible The Lazarus Heist podcast, and our specialist experts Matt Hull, Christo Butcher, Ade Clewlow, Chris Ulliott (NatWest), Paul Roberts (Microsoft) and Jennifer Fernick. We will delve into the ever-changing cybersecurity landscape, and the actions to take today to improve the long-term resilience of your organisation, no matter the threats you may face. I hope to see you there.

Want more insight? Join us for our free, interactive, online event.

Growing threats: Are you ready?

REGISTER HERE >

Mike Maddison
CEO, NCC Group

The shifting sands of cyber threats

How companies are fighting back against a rising tide of cyber incidents

Cyber security incidents around the world are evolving. Hackers are shifting shape, regrouping, disbanding or springing up anew. The types of attack are becoming more sophisticated or targeting new victims, increasing sharply in the first half of this year, led by a new strain of ransomware, followed closely by a continued boom in phishing, malware and denial of service attacks.

And with the geopolitical landscape in flux as the Russia-Ukraine conflict continued, many organisations were caught in the crosshairs of nation state-sponsored attacks.

Yet, as threat actors and attack types adapt, so too are organisations' ability to respond.

In this issue of Insights, we examine how cyber-security threats are changing and which industries are most at risk for potential attack. You'll hear from our experts, giving tips for how companies can identify and mitigate shifting cyber security threats.

We focus on two separate pieces of research and analysis, which provide an intriguing snapshot into the cyber security threats faced by companies and how they are prioritising their defences.

Research one was a survey commissioned by NCC Group, between December last year and January this year. It questioned nearly 1,400 cyber security decision makers in countries across the globe, including the United Kingdom, United States, China, Germany, and Singapore.

Research two was analysis by NCC Group's Threat Intelligence team, the Threat Monitor report, into critical cyber security incidents worldwide between April and June.

61%

of cyber security professionals around the world said that the number of cyber security threats their organisation had encountered had increased in the past year

Cyber security incidents around the world are evolving. Hackers are shifting shape, regrouping, disbanding or springing up anew.

Global. Transformative. Resilient.

The volume of cyber attacks are increasing

Six in ten (61%) of cyber security professionals around the world said that the number of cyber security threats their organisation had encountered had increased in the past year.

In the second quarter of 2022 ransomware attacks worldwide increased by 12%, compared to the previous quarter, according to our Threat Monitor analysis in the second quarter of this year.

Taking a regional view, in the first quarter of this year there was a noticeable rise in European-based activity, with the continent the most targeted for attack. Based on this quarter's data, it seems this was a temporary anomaly, likely as a result of the Russia-Ukraine conflict. After the initial surge in European-targeted attacks, North America returned to the 'top' target spot with 269 attacks recorded between April and June (42%), as compared to 244 in Europe (36%) and 89 in Asia (14%).

12%

increase of ransomware attacks worldwide in the second quarter of 2022 compared to the previous quarter

Types of attack

No surprise here. Ransomware continues to be the most common type of cyber attack, according to our analysis of critical cyber security incidents worldwide between April and June, responsible for 63% of all cyber security incidents.

Technology is making ransomware cheaper and more accessible.Almost half (47%) of these ransomware cases were conducted employing off-the-shelf technology tools.

63%

of all cyber security incidents worldwide between April and June continues to be ransomware

45% increase in **insider threats**

48% increase in **denial of service attacks**

49% increase in **ransomware attacks**

51% increase in **supply chain attacks**

60% increase in **phishing & malware attacks**

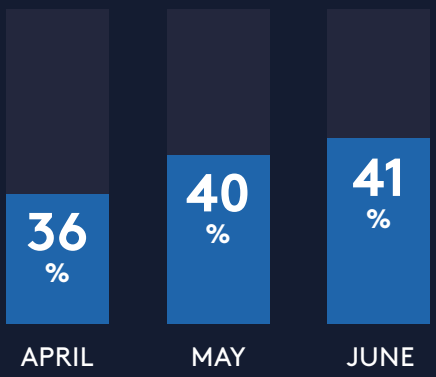
Initial access was most often achieved using vulnerable external facing servers (**37%**) followed by malicious emails with links or attachments (**32%**)

> To find out more about optimising these defences, head to page 14.

Crimewatch: The most prolific cyber-criminal groups

Corporate cyber security in the second quarter of 2022 has been dominated by three ransomware gangs: **LockBit2.0, Conti and BlackCat**.

RANSOMWARE INCIDENTS



LockBit

LockBit2.0 – a type of ransomware that targets Windows PCs and now Linux servers – remained the most prominent threat actor in the second quarter.

Over the three-month period, the number of LockBit2.0's attacks fluctuated. In April, the ransomware strain accounted for 36% of all ransomware incidents, 40% of overall ransomware or cyber security incidents in May and 41% of all incidents in June.

The decline was likely due to cyber criminals preparing a new strain – LockBit3.0.

Industrials was the most targeted sector for ransomware attacks, followed by consumer cyclicals, and technology.

Want to find out how LockBit are shifting shape?
Read our Spotlight on page 20.

16%

In April, Conti was responsible for 45 out of 289 incidents

Conti

The second most prolific ransomware group put Costa Rica under siege for several months earlier this year and, according to Wired magazine, "rewrote the rules of cybercrime".

Conti, which recently shut down its operations, accounted for around 10% of total ransomware incidents between April and June.

In April, Conti was responsible for 45 out of 289 incidents (16%). In May it accounted for 7% of all ransomware incidents, and just 1% in June. The group's activity has seen rapid decline – suggesting its members have re-grouped alongside Conti affiliates and new ransomware strains.

8%

BlackCat accounted for 8% of total ransomware incidents in the second quarter

BlackCat

The third main ransomware gang made a strong start to the year. As of March, it had breached the security of at least 60 organisations around the world, according to the Federal Bureau of Investigation (FBI).

BlackCat accounted for 8% of total ransomware incidents in the second quarter.

As with LockBit2.0 and Conti, BlackCat targeted three sectors – industrials, followed by consumer cyclicals and technology.

Spending plans and bolstering response

So, how are companies responding to changing cyber-security threats? Our research paints a mixed picture of company cyber security.

Companies said that they were able to respond faster to cyber security incidents (84% said they could respond within one day), with seven in ten reporting their ability to respond quickly and effectively had improved in the past year. However, only 34% of those questioned rated their organisation's cyber security as "very resilient".

So where do priorities lie, when it comes to cyber resilience? When cyber security professionals were asked for their spending plans for the next six months to one year, threat detection and response was top (32%), followed by cyber security reviews and assessments (25%), and jointly security awareness and training, and security testing, infrastructure and application (24%).

In the same research, we asked companies if they planned to increase spending on cyber security in the next year, and if so, what they planned to spend the biggest proportion of the increase on.

Where do priorities lie, when it comes to cyber resilience?

32 %	Threat detection and response
25 %	Cyber security reviews and assessments
24 %	Security awareness, training, security testing, infrastructure and application

82% said they planned to increase spending on cyber security. Of those that did plan to increase spending, the biggest share of any increase was expected to go on managed security services, followed by cloud integrated security products, and hardware-based third-party security products.

RESEARCH SUMMARY

The number of cyber attacks against businesses are increasing, 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.

Six in ten (61%) of cyber-security professionals around the world said that the number of cyber-security threats they had encountered had increased in the past year.

Ransomware continues to be the most common type of cyber attack worldwide, according to NCC analysis of critical cyber security incidents worldwide between April and June - responsible for **63%** of all cyber security incidents.

In the second quarter of this year, the most common cyber criminal group was the ransomware group LockBit 2.0, followed by two other groups – Conti and BlackCat. Ransomware groups form and disband quickly, sometimes within months.

Sector focus:

Cyber criminals are stepping up attacks on industrial, financial and tech companies. What can we learn?

Cyber security incidents increased rapidly in the first half of the year, but the attacks on industries were not spread evenly. Hackers have their favourites. Companies within the Critical Infrastructure, Operational Technology and Industrials sectors (which typically include Energy and Utilities, Transport, Defence and Construction amongst others) were among the most targeted by ransomware, phishing and malware attacks.

According to global data from our Incident Response statistics, in the second quarter of this year financial services, Industrials, Energy and Operational Technology continued to be the most common industry targets. By industry, technology companies recorded the highest percentage of security incidents that were escalated (38%).

38%

Technology companies recorded the highest percentage of security incidents that were escalated

So, why are these industries being targeted?

And how can companies in these industries prevent cyber attacks or minimise damage if an attack breaches their defences?

Industrials

Thoughts from Charlotte Davis, Head of Industrials, NCC Group

Until the last couple of years, companies within the industrials sector weren't necessarily considered to be prime targets for cyber criminals. This was, in part, due to the lack of connectivity of operational technology (OT), and because the architectures on which they operated were air-gapped from externally facing networks by default.

As we evolve to smart industrial environments (driven by Industry 4.0 and Society 5.0) and critical assets and networks that are connected to the Internet – the "Internet of Things" (IoT) and Industrial IoT (IIoT) – to improve efficiency, OT is becoming an increasingly viable and attractive target.

Typically ransomware has been considered almost exclusively from a traditional IT systems perspective, however as the Colonial Pipeline ransomware attack in 2021 highlighted, OT in industrial companies can be an asset of strategic and national importance.

Other recent cyber attacks to target industrials include the "parasite" malware – which targets utilities and aerospace companies, among others. It uses open-source tools to compromise infrastructure and leverages known virtual private network vulnerabilities for initial access – and a cyber crime group known as Xenotime, which is thought to have attacked oil and gas companies.

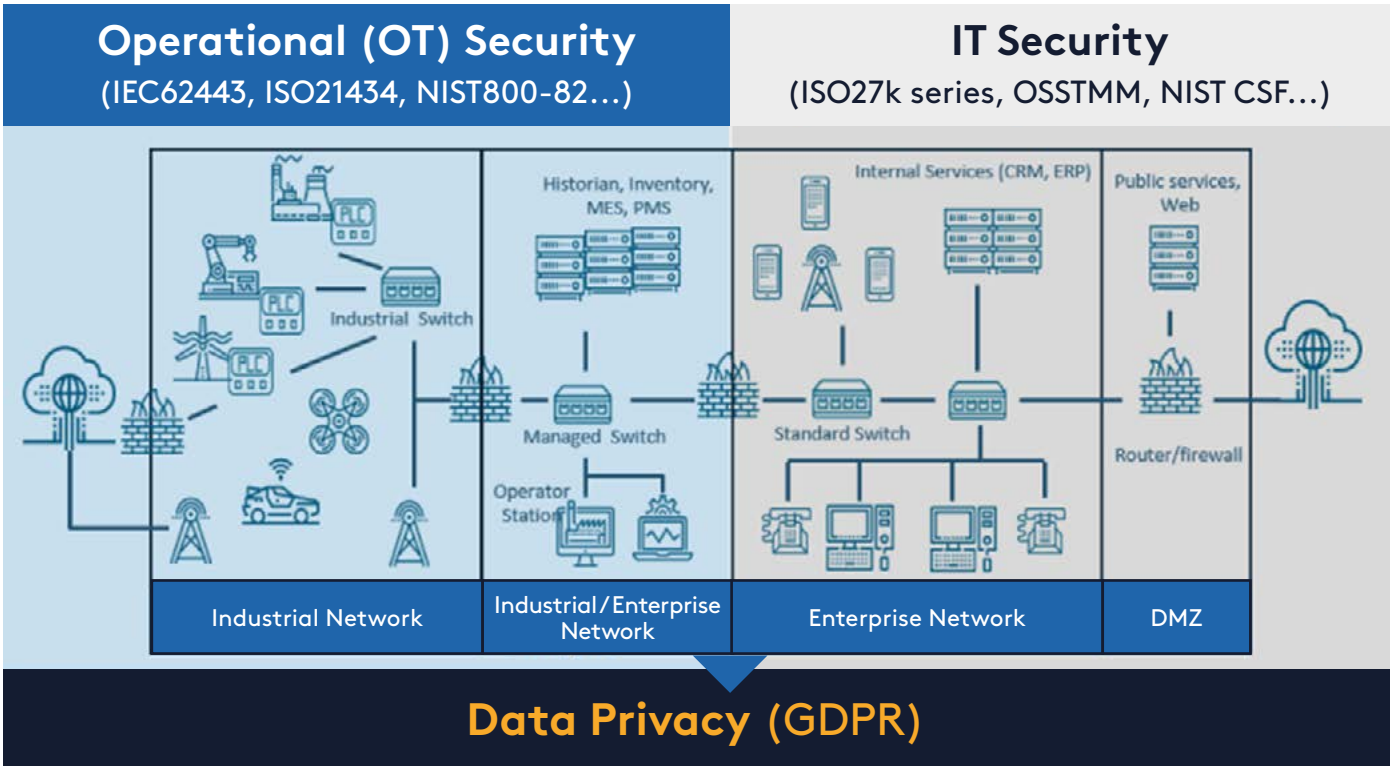
Cyber criminals have proven their ability to hold an organisation to ransom and increasingly this has impacted industrial environments and their ability to maintain operational viability. While financial gain is fundamentally the motive for cybercrime we are also identifying trends towards devastating supply chains, and regional and national infrastructure. As always, there is the danger of being caught in the crosshairs of nation state attacks either directly or indirectly and in recent months many organisations have seen Threat Intelligence advisory action as a result of this very scenario. We see increasing evidence of threat actors who target industrial and logistics businesses working within critical infrastructure to gain access to sensitive data or intellectual property (including in some instance PII) to then be weaponised for nefarious geopolitical means.

As the IT-OT convergence creates a paradigm shift for the Industrial sector, our ability to keep OT secure requires more consideration and specialist security expertise. In many instances, the connectivity of these networks is a new phenomenon, and therefore the cyber threats and their attack signatures are being explored for better understanding.

That said, basic cyber hygiene and security controls within IT and OT, and the prevention of lateral movement between parallel network architectures, are the most cost effective and efficient ways to build a strong security posture across an entire organisational or network architecture.

These measures include:

- Conducting Architectural Design reviews for network visibility to understand your organisation's critical assets, monitor them on an ongoing basis and understand if and which security controls are needed in the long term
- Ensuring your business continuity and disaster recovery plans include IoT and OT, if your organisation uses them
- Consistently monitoring environments to identify vulnerability to cyber attacks before they can be successful, using security incident and event management tools, such as Microsoft Sentinel XDR
- Creating network segmentation via process controls or technologies such as a "data diode" – hardware that allows data to travel only in one direction. By using a data diode, your business can prevent malware or ransomware from moving laterally between IT and OT environments
- Checking that your organisation follows industry best practice and international cyber-security standards, including adopting best practice NIST 800-5310 for IT and NIST 800-8211, and ISA/IEC 62443 for ICS and OT. This includes aligning security patch processes to mitigate security threats to OT.



You can work towards attaining component and asset certification to these standards or work with a partner to align your products, processes, and services to such standards (with support and guidance from an ISA/IEC 62443 specialist).

Find further advice to protect OT systems in our technical article, and explore recent attacks within the industrials sector in our **Threat Intel Report**, on page 18.

Banking, insurance and financial services

Thoughts from Sara de la Torre,
Head of Financial Services and Insurance,
NCC Group

How do financial institutions tackle the growing and most sophisticated exposure to cyber attack?

The convergence of digital transformation and globalisation will reshape the financial services' industry over the next five years. As this convergence materialises, data privacy and cybersecurity has become the top business risk and an executive board priority. With the current geopolitical instability and cyber compliance rising around the world, scrupulous end-to-end cybersecurity becomes a core focus.

As cyber attacks are increasingly becoming more frequent and sophisticated, financial institutions are using more risk driven, advanced analytical models and technology to understand and mitigate cyber threats, whilst leveraging the best advisors and practitioners with new skills and technology.

Executive boards from financial institutions are rolling out several initiatives to combat increasing cyber risks. The cyber approach in banking is looking to achieve three key objectives: security for the web, mobile applications and blockchain, risk exposure and risk quantification and the review of existing cyber resilience, on ongoing basis.

Financial institutions recognise that cybersecurity must be acknowledged as a core, strategic risk which underpins many strategic initiatives, which contribute to addressing sustainability, driving growth, protecting data privacy and maintaining business reputation. For these reasons, financial institutions are looking to improve their overall cybersecurity with a holistic approach.

In the Digital Economy and with the growing adoption of digital assets and Decentralised Finance (DeFi), cybersecurity becomes a source of competitive advantage with the right strategy, governance, and execution. Our experience helps organisations transform cyber into an opportunity and we treat cybersecurity as a business, not just a technology challenge.

Three key objectives to combat increasing cyber risks against financial services, banking and insurance:

1. Security for the web, mobile applications and blockchain end to security lifecycle solutions are being deployed with advanced analytics (machine learning), rule-based frameworks and cyber engineers' driven approaches.

2. Risk exposure and cyber risk quantification, just like any other traditional financial risk, with value at risk simulations, stress testing scenarios vs risk appetite and dashboarding following the governance, risk and compliance guidelines.

3. Review of existing cyber resilience with vulnerability assessments, attack simulation and cybersecurity frameworks which challenge the existing landscape and identify new types of attacks.

Thoughts from Pepijn Slappendel, Head of Fraud Management, Fox-IT

FOX IT
part of nccgroup

One of the many effects of the pandemic was a surge in ecommerce and online banking – and cyber criminals were quick to spot an opportunity

Fraudsters targeted two main groups: people using online banking for the first time, who were somewhat technologically naïve, and young people – the TikTok generation – who have grown up with online technologies.

Police raids on call centres

Earlier this year, Interpol made hundreds of arrests and seized millions of dollars in a crackdown on organised crime in telecommunications and financial services. The operation, codenamed, "First Light", covered 76 countries. It focused on social engineering fraud, in which criminals manipulate or trick people into giving out confidential or personal information which can then be used for criminal financial gain.

Police in participating countries raided national call centres suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, email deception, and connected financial crime.

The operation, codenamed, "First Light", covered 76 countries

Phishing for data

Currently, voice phishing or vhishing is the dominant type of fraud in most countries. The fraudster's aim is to build trust with their victim, perhaps by pretending to be from a bank helpdesk or even spoofing a customer service number.

During the scam, they will use remote access tools to gain access to devices and sensitive information, and convince customers to navigate security measures such as two-factor authentication, to deposit large sums of money into the fraudsters accounts. And many customers will do this, as they feel they are doing the right thing given the deliberate manipulations the fraudsters are subjecting them to.

It may look like a normal and perfectly legitimate transaction by a customer. However, a bank would never ask a customer to give it remote access to their accounts.

What we can see is that fraud is becoming less technological. We're seeing the rise of low-tech fraud.

Fraudsters are looking for the weakest link, and right now this could be customers themselves.

Fraud is becoming less technological.

We're seeing the rise of low-tech fraud.

So, how can you mitigate cyber threats in financial settings?

Detection

In the case of social engineering scams, it is vital to monitor the entire customer journey, including device registrations and customer log-ins, not just online transactions. Try to detect cyber attacks at an early stage and prevent them from happening.

The challenge that banks have is that customers today use many different channels. It's no longer only internet banking or using an ATM. They also use mobile and various financial apps such as PayPal. That makes it easier for fraudsters to hide their tracks between the channels and remain undetected.

Build a single point where all data is correlated and track each of your customer's journeys.

Stronger user authentication

This is the key preventive measure that can be applied. Use multiple devices to, for example, verify a customer's identity and approve banking transactions by scanning a QR code when the customer is logging in. That means a fraudster can't make a transaction on their own unless they have been able to register their own device on the victim's bank account. Multi-factor authentication makes life harder for fraudsters.

Educate your customers

When a social engineering script for fraud is seen to work it becomes widely used. The scripts change regularly. In the Netherlands, for example, one social engineering script used to be a child texting their parent saying that he or she has lost their phone and needs money to return home from holiday. That was the dominant scam until people became aware of this story. Now it's a bank helpdesk fraud – it has recently become more widely used in the UK as well.

Banks will always know which fraud story is most common and can use this knowledge to raise awareness with their customers. The stories may change but the techniques and technologies they use remain broadly similar. Fortunately, these threats can be mitigated through a methodical approach to cybersecurity and the right technology.

Optimising phishing and malware defences with threat intelligence

Christo Butcher
Global head Threat Intel managed services, Fox-IT

Phishing and malware attacks against operational technologies increased sharply in the last quarter, by 60%. With these attacks evolving rapidly, Christo Butcher, Global head Threat Intel managed services, Fox-IT, discusses how threat intelligence can optimise your defences against phishing and malware.

The rise in attacks on operational technologies – which monitor and control industrial equipment – is part of a long-term trend. Why? The bad guys are just upping their game.

How can organisations reduce the likelihood that one of these cyber attacks will be successful and cause major financial, operational and reputational damage?

Any cybersecurity policy should prioritise prevention, detection and response.

In this article, I'm going to focus on prevention, with guidance which can be applied across sectors.

60%

increase of phishing and malware attacks against operational technologies in the last quarter

Prevention

This is the most important of the three-pronged defence. As we all know, prevention is better than cure.

A great example of high-value prevention is multi-factor authentication. On the one hand, it is relatively easy to setup and doesn't cost much. On the other, it gives a high security return because it stops attackers from using stolen passwords.

If you enable multi-factor authentication, even if your credentials are stolen, the impact is much less. If you don't have multi-factor authentication and the bad guys steal your password, they have access to your account. With multi-factor authentication, hackers will struggle to log in to your account. Low-hanging fruit like this is often built into business software.

Besides multi-factor authentication, organisations should also make it difficult for phishing emails to reach their users. Implement anti-phishing and anti-email spoofing technologies. They are often built into software products, including Office 365; you just need to set it up.

Such security features analyse emails and block suspicious, phishing-like emails in which fraudsters try to trick the recipients into revealing valuable personal details such as usernames and passwords.

Another defence against phishing is thinking about your organisation's digital footprint. If you have a lot of information about your organisation and your users, you are making it easier for an attacker to collect information and write a convincing phishing attack.

And don't forget the human factor. Educate your employees and suppliers about cyber security risks, especially from phishing. Phishing emails will sneak through even the most well defended corporate networks.

Make it easy for users to do something about it. Train them so they know how to spot phishing emails.

You can train them using simulations to test users – for example using phishing emails, designed by ethical hackers, to see how they respond. This will help users spot and record phishing emails, and who to send their report to – for example your company's cyber security officer. It should be standard practice.

PREVENTION
TOP TIPS

- Set up Multi-factor authentication
- Implement Anti-phishing and anti-email spoofing technologies
- Think about your organisation's digital footprint
- Educate your employees and suppliers about cyber security risks

Let's be clear.

We're not talking about spending a lot of money on new technology. It's about using existing procedures and technologies more efficiently.

Malware threats

As well as trying to steal your user credentials, phishing emails might try to install malware on systems.

When you get a phishing email with an attachment and you open it, very often that attachment will try to deploy malware. Make sure that your endpoint, such as your laptop, is hardened so that it's more difficult for attackers to deploy malware.

That's where out-of-the-box products are often not so great, because attackers buy the standard IT tools and practice on them and try to find security flaws in the standard configuration.

Keep your security tools and procedures up-to-date, and configure them appropriately for your situation. Sticking to this best practice will make it harder for cyber criminals to infiltrate your company's network.

There are three levels of threat intelligence

Strategic

Mid-level

Base-level

Threat intelligence

This is about understanding the threats you face; how serious they are, and how you can protect your organisation against them.

There are three levels of threat intelligence – strategic (the highest level, for example, global trends in cyber security threats); mid-level ("tactics, techniques and procedures" or "TTP" in industry jargon), which has more detail on security threats, and the bottom, most basic level, which includes information about the "fingerprint" of, say, malware and other basic details.

Of these three, the middle layer is the most useful type of threat intelligence for organisations. It helps organisations prioritise cyber security risks, map them against their IT systems, pinpoint potential weaknesses and strengthen them. How could cyber criminals attack my organisation, get into my network and take it over. How can I stop them?

New technologies

Could advances in security software help stem the rising tide in phishing and malware attacks on operational technologies?

NCC Group has developed machine learning technology

FIND OUT MORE >

Machine learning, a type of artificial intelligence, is one of the most promising new technologies.

NCC Group has developed machine learning technology to detect anomalies in a network, which could be security threats. This means looking at a network to see what is normal and then when something abnormal happens flagging it. This technology is gaining a lot more traction and becoming more feasible for businesses.

Machine learning looks especially promising for OT environments due to network communications and the general behaviour of systems being more predictable than in IT environments, with a more diverse user base. That makes it easier to detect anomalies because the baseline is more stable.

Buying new technologies isn't a magic solution to evolving cyber security threats. It's often unnecessary.

Most organisations already have more than enough technologies and procedures to deal with changing security threats.

Much of the proven security technology is built into companies' existing IT systems. The key thing is to use threat intelligence to protect yourselves and configure your platforms. Your first step should be to invest time in understanding the security threats facing your organisation. After you've done that, you can update your security to fix any weaknesses – and better protect your organisation.

The key thing is to use threat intelligence to protect yourselves and configure your platforms.

The threat landscape is in flux, and OT systems are a prime target

Matt Hull, NCC Group's Global Head of Threat Intelligence, discusses the current threat landscape and the disastrous fallout of recent high profile attacks on OT systems.

Matt Hull
NCC Group's Global Head of Threat Intelligence

Once again, 2022 is shaping up to be an interesting year with regards the criminal threat landscape, particularly the use of ransomware. We continue to see Ransomware-as-a-Service (RaaS) as one of the most significant threats to organisations around the globe, despite several prominent ransomware operators disbanding and rebranding.

In the first half of this calendar year, 65% of all of our incident response cases across the globe have involved the deployment of ransomware . In most cases, this has also involved the release of sensitive corporate data on so called 'leak sites' which are used by ransomware operators as part of 'double-extortion' campaigns.

Last year there were concerns around the targeting of operational technology (OT) environments by criminal groups, something which rose to prominence following the Colonial Pipelines breach. This year, we are seeing more and more incidents involving the OT space. In 2022, the industrials sector has been the victim of 45% of all double extortion ransomware incidents. It shows that weaknesses in legacy OT environments, which may have been overlooked for many years, are an obvious and easy target for criminal groups.

65%

of all of our incident response cases across the globe have involved the deployment of ransomware

45%

of all double extortion ransomware incidents in 2022 have affected industrials sector

> Ransomware-as-a-Service (RaaS) is one of the most significant threats to organisations around the globe.

Threat Intel Report

OT systems support the critical infrastructure we depend on: electrical grids, water, transport networks, fuel and power plants, food and product manufacturing. As OT networks become increasingly connected to IT systems, attacks can be highly disruptive – a threat to not only organisations, but a country's economy and national security. We have seen that operational and production disruption is possible, with detrimental consequences for processes and safety. The stakes at play for organisations are high, with financial loss, data loss and compromised human safety at risk.

The terrifying potential of an attack against an OT environment was realised in June this year. The threat actor 'Predatory Sparrow' was able to demonstrate the true impact of a cyber-kinetic attack, which resulted in a large fire in an Iranian steel plant. Interestingly, the group claim to have deliberately launched the attack in a manner which did not cause injury to innocent people.

So, as we expect that OT environments will continue to be a priority target for a plethora of threat groups over the coming years, investment in the security of these must be a key priority for organisations and global governments alike.

As OT networks become increasingly connected to IT systems, attacks can be highly disruptive

The impact of 'Predatory Sparrow', a cyber-kinetic attack

OT environments will continue to be a priority target for a plethora of threat groups over the coming years.

Spotlight: LockBit3.0

New variant making waves on the ransomware scene

In June this year, one of the most prolific threat actors in recent years, LockBit, phased out its LockBit2.0 variant for a new strain: LockBit3.0. Released under the slogan 'Make Ransomware Great Again', the following month saw LockBit3.0 account for 52 incidents globally.

Despite fluctuations within the threat landscape as a result of its changing variants, LockBit has maintained its stronghold as one of the most prolific ransomware actors out there. NCC Group quarterly analysis shows LockBit's dominant focus on companies within industrials and technology, matching overall sector trends for Q2. In particular, professional and commercial services, construction and engineering and freight and logistics services were some of LockBit's most targeted. Given these sectors' wide customer bases and operation within complex supply chains, LockBit attempts to exploit these characteristics to pressure payment.

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

"The threat actor scene is in flux, and as one 'disappears', another strain emerges to take the top spot. It's what we saw with the disbanding of Conti earlier this year, and the emergence of LockBit3.0. Threat actors never stay still – they shift shape, evolve their attack types. For even the most cybersecurity advanced business, it can make detecting, protecting and defending against attack a complex beast.

"We are starting to see patterns in LockBit's behaviour though. For example, its clear focus on industrial operations and technology companies, often seen as lucrative targets for attack. As LockBit3.0 maintains its proliferation, our Strategic Threat Intelligence team will keep a watchful eye on its use, so that our customers can benefit from the latest updates on its activity. Arming yourself with this knowledge – on the most active threat actors, their go-to attack types, their preferred victims – means you can stay one step ahead in an evolving cybersecurity landscape."

Arm yourself with knowledge and receive our monthly threat updates conveniently in your e-mail box.

SIGN UP TODAY >

Spotlight:
Dissect: An incident response game-changer

A streamlined, easy-to-use solution, available as Open Source Software

As our online and offline worlds intertwine further, cyber incidents are having even greater impact. Whether its employee fraud or a nation state attack, they are becoming increasingly complex and sophisticated, as are the IT systems on which they take place. The main question for the good guys is this: How do you scale incident response capabilities, while both speed and accuracy of an investigation are maintained, or even improved?

Now Fox-IT, part of NCC group, has created a solution to this challenge, which we have decided to make available as open source: Dissect.

Dissect. Its modular approach means anyone with Python experience can use the concise API to adapt it to their own needs and create output to connect it to the platform of their liking. And the best part is it is now available as Open Source Software. After all, better incident response, no matter who delivers it, is a net benefit to the world – making it safer and more secure.

DISSECT

Enables the acquisition and analysis of hundreds to thousands of systems in a matter of hours – a game changer for incident response teams

> FIND OUT MORE

How could you benefit from Dissect?

Faster response times minimize the damage that any incident can cause.

How could you benefit from Dissect?

Faster response times minimize the damage that any incident can cause.

1

Respond rapidly to complex attacks

In essence, incident response still comes down to an organization experiencing pain from insiders, spies, or criminals, and calling a trusted third party to make the pain go away. This seems straightforward, but incident response is a machine with many changing parts. Attackers nowadays aim to take over a complete infrastructure, often with both on-premise and cloud systems. This requires incident response teams to investigate more systems and reconstruct longer timelines with more diverse events than in the past. With all this, plus additional time pressure, incident handling is more complex than ever. Dissect helps ease this complexity by enabling analysis of 1,000s of systems in hours, and looking for data in known or configured locations, without parsing every file on a disk. This drastically improves performance and is sufficient for most IR engagements. If during initial triage it turns out more analysis is required, you can always fall back to the more traditional toolset for individual system analysis.

2

Go beyond current capabilities

Many incident response engagements have one thing in common: a large, complex infrastructure that needs careful examination for Indicators of Compromise (IOCs), while the investigators may need to remain undetected by sophisticated threat actors. These cases often go beyond the capacities of commonly used analysis tools.

3

Keep standards high at all times

There's no shortage of parsers and tools for DFIR tasks that work fine most of the time. But whether it's missing functionalities, automation difficulties or poor performance, 'most of the time' simply isn't good enough.

4

Unlock a seamless experience

While many tools perform similar tasks, their output format, e.g. CSV, JSON or Excel, can differ wildly. Besides making it harder to collaborate, the choice of tools could lead to different findings, which is detrimental to the quality of any engagement. On top of that, the plethora of tools makes it hard to automate tasks in an analysis pipeline

5

Take control at any scale

Nowadays, there's a need for swift analysis or at least an initial impression of the state of hosts within hours from the moment of acquisition. Most current tools aren't made with this goal in mind. Dissect puts you in control of your entire analysis chain as it is easy to expand with different implementations of various parsers. This lets you reuse useful components, not limiting them to the capabilities of a single script. You can also easily add exotic systems without making changes to the rest of the framework. This flexibility enables you to easily create new and exciting capabilities with Dissect, like adding hypervisor-based data acquisition, which allows for system analysis without detection by the compromising threat actor.

6

Ready for state actors

Especially when dealing with advanced threat actors, you want to be as stealthy as possible. An example of how Dissect can help with this is by allowing data acquisition from a hypervisor, which allows for analysis of a virtual machine without the threat actor who compromised the system detecting it. Dissect can bypass any lock the hypervisor might have on a virtual disk, without running the risk of data corruption. Another example is that the Acquire data acquisition tool, when executed on live systems, reads straight from the raw disk, not using operating system APIs to copy files. This limits the possibilities for Threat Actors to tamper with the evidence collection.

Making the world safer and more secure

Dissect has pushed our own incident response practice capabilities. We want to share this with the world to make it a safer, more secure place.

With increased usage we expect valuable input into the framework from other members of the security community.

Although outstanding tools always help, we know we can only deliver effective incident response thanks to our experienced, talented team.

For more detailed information about Dissect, please go to **fox-it.com/nl-en/dissect**

Or if you need assistance in case of an incident, contact our hotline any time at **nccgroup.com** and our world-class incident responders will be happy to help.

> FIND OUT MORE

Growing Threats: Are you ready?

Virtual Event

6 October 2022, 2pm BST

Join us at our exclusive Insights event to discuss all your company needs to know about the ever-changing landscape of cyber threats. You'll hear from our global panel of experts, and learn from the real life experiences of those that are defending against attacks.

Get ready to defy today – and tomorrow's – threats and sign up now.

The event will begin with an introduction from our team live from our London studio, with BBC journalist Geoff White, host of The Lazarus Heist podcast, interviewing our newly appointed CEO, Mike Maddison

The Business Stream
Our speakers discuss how the changing nature of cyber threats are impacting different sectors across the globe.

The Technical Stream
Our experts take you through NCC Group's latest analysis on the global threat landscape.

The event will conclude with a live Q&A session with all of our speakers.

REGISTER HERE FOR VIRTUAL EVENT >

Mike Maddison
CEO, NCC Group

Geoff White
BBC journalist and presenter of The Lazarus Heist podcast

Chris Ulliott
Chief Security Officer at NatWest

Paul Roberts
OT Technical Specialist at Microsoft

Ade Clewlow
Senior Advisor, NCC Group

Jennifer Fernick
Senior Vice President and Global Head of Research, NCC Group

Christo Butcher
Global head Threat Intel managed services, Fox-IT

Matt Hull
Global Head of Threat Intelligence, NCC Group

About Insights

Insights is a program designed for sharing pragmatic cyber security insights with senior executives. You can expect a magazine and interactive online event about a trending topic each quarter. Register here for the free virtual Insights event: Growing Threats.

About NCC group

It's a new era of risk. Defy it with NCC Group's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them with strong security solutions...and with a global team of over 2,400 experts, we're ready to do the same for you.

With NCC Group, take your business to the next level. Unleash innovation without the obstacle of cyber threats.

More than a solution. **A partner.**

You're not alone on your security journey. NCC Group is your partner. Be it rolling up our sleeves with your in-house team or developing strategy with your board, we help you have control over your appropriate level of security. Yes, we deliver industry leading security solutions, but we'll also reduce stress, save your business time, and help you prepare for, or even face, a crisis together.

www.nccgroup.com

UNI106269