nccgroup

FOX IT
part of nccgroup

Monthly Threat Pulse

Review of May 2024

What's inside:

EXECUTIVE SUMMARY

This month's edition of the Threat Pulse from NCC Group's Threat Intelligence Team contains a summary of observed ransomware attacks around the globe, a continuation of last month's inaugural theme of AI with an examination of how to defend against AI-assisted attacks, an insight to some of the great work being carried out by the TI team in the form of an exploration of the emerging issue of brute force attacks against VPNs, a Spotlight piece by the Tactical Threat Intelligence team on the evolution of criminality with regards to AI's emergence, a threat hunt done in collaboration with NCC's Security Operations Centre (SOC).

The ransomware scene has evolved significantly from last month's reporting. Not only have we seen the introduction of several new and interesting actors, but also the reemergence of LockBit 3.0 to their previously well-established position at top of the pack of most prominent actors. This, however, is not to be taken at face value; though their activity levels have returned to what we would ordinarily expect, there is speculation within the cybercriminal and security commentator communities that they are artificially inflating their attack count in order to appear unperturbed by their recent interactions with law enforcement. We have also observed a continuation of attacks levied against organisations in South America and Africa which last month we linked to a potential new trend of sophisticated actors using the region as a proving ground for new malware before deploying it against targets in Europe and North America.

This month's Spotlight piece on AI and the continuation of last month's theme are similar in scope. The Spotlight discusses the criminality element of the cybercrime landscape after the advent of AI; it is being increasingly utilised in a similar manner to how we're seeing in the non-criminal landscape i.e. through the use of chatbots on forums which use LLMs to assist users in finding answers to their questions. It also can be used to assist in actively malicious use cases such as to assist and speed up network scanning, or to write better phishing emails.

The Intelligence Insights piece pivots from this angle and focuses on how to defend against AI-assisted attack methodologies. Though AI can indeed be a tool to help malicious actors carry out their nefarious campaigns, it can also be used by defenders to protect their digital estates. Beyond that though, traditional defensive measures such as; proactive network and vulnerability scanning, updating and patching software and firmware in a timely manner, and, most importantly, training staff to identify common security threats, can and do go a long way to mitigate the threat caused by cybercriminals of all types whether they are using AI assisted tools or not.

The Intelligence Insights section was expanded this month to include an examination of the rise of brute force attacks against VPN services. Brute force attacks are when attackers utilise every possible combination of characters, words, or phrases in order to get hold of encrypted information or gain valid credentials. Though typically not thought of as a sophisticated attack methodology, they can require immense levels of computational power to conduct and so could be carried out by actors with large botnets at their disposal. Further, despite a lack of perceived sophistication, this does not mean that they are not capable of achieving the desired ends of an attacker. Since March 2024 there has been an increase in brute force attacks against a range of VPN services and originating from both the TOR browser as well as a range of proxy services. These attacks do not currently appear to be targeting a specific industry or region, but IP addresses released by CISCO which were included in observed attacks have been linked to the activity of APT 29, a Russian state-sponsored threat group, in the past.

This month's threat hunt examined a phishing campaign that, although after being spotted in August 2023, was first reported on the 29th of April 2024. Our Global SOC did see a number of detections on the back of some of the IoCs we provided, and we were able to uncover further IoCs as a result. This month we dig into some additional potentially malicious IP addresses that were discovered by pivoting from suspicious domains.

CONTENTS

SECTION 01

RANSOMWARE INSIGHTS

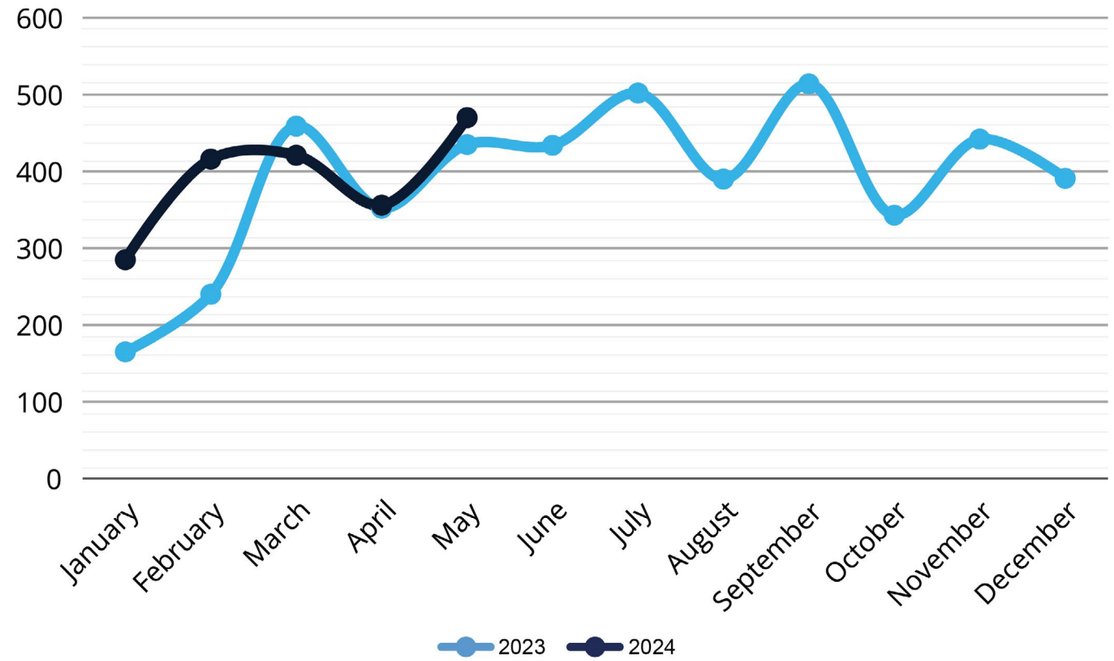


Figure 1: Global Ransomware Attacks by Month

As we continue into Q2, the pattern which was established in last month's Threat Pulse – generally speaking ransomware activity will increase each year until a more lucrative opportunity presents itself to Organised Crime Groups (OCGs) – can continue to be observed.

Despite the dip in March of this year when activity levels were lower than in March 2023, 421 observed attacks compared to 459, every month in 2024 has observed higher levels of ransomware activity than in 2023.

In April's edition, one reason we attributed to the lower-than-expected levels of ransomware activity was the massive drop-in activity from LockBit 3.0.

This was likely due to their targeting by law enforcement agencies in February. Although they are once again the most active group for May, with nearly 100 more attacks than was recorded in May 2023, there is still some consternation amongst the cybercriminal community as to whether or not to get involved with the group.

Any threat actor touched by the long arm of law enforcement is treated with suspicion after the fact, and sometimes their reputation never recovers.

There is some speculation that LockBit has not actually managed to recover their operations fully but is instead reposting old victims in an attempt to put forth an image of imperturbability.

Until the status of LockBit, their activity, and their affiliates is more clearly understood, we will be taking their claims at face value and reporting on what victims are found on their leak site.

For those organisations that feel they could benefit from in-depth ransomware insights, which is a threat that has only continued to significantly rise in prevalence and sophistication over the past few years, we point you towards our Enhanced Threat Intelligence Subscription Service.

This package gives clients access to our Premium Threat Pulses, Threat Monitor Reports, and Threat Intelligence Alerts – reported within 24 hours - for significant vulnerabilities and cyber campaigns.

For Ransomware Insights specifically, we elaborate on the most targeted sectors and regions, as well as the most active ransomware groups so organisations can proactively enhance their security posture based on the threat to their specific areas of operation.

SECTION 02

INTELLIGENCE INSIGHTS: MALICIOUS USE CASES OF AI

In last month's Threat Pulse, we introduced the topic of AI as the inaugural theme for the Intelligence Insights section of the report; an umbrella topic we will explore various aspects of throughout the quarter.

We introduced the topic and scraped the surface on some issues surrounding malicious uses of AI, as well as how it can be used as a legitimate tool to assist defensive measures.

In this month's Threat Pulse, we will be examining how some specific malicious use cases of AI can be defended against. The criminological angle, as well as some more detail on the malicious use cases themselves, will be examined in the Spotlight section prepared by the Tactical Intelligence team.

As alluded to in April's Threat Pulse, one way which AI can be used to assist bad actors is through vulnerability scanners. Attackers use port and network scanners to try and identify any weak points or vulnerabilities in an organisation's network.

By querying a port, attackers can determine if it is open or closed and use this information to determine if there are any known weaknesses which can be exploited.

One freely available tool for this, though not one designed with explicitly malicious purposes in mind, is burpgpt.

Burpgpt is a tool which uses AI to "detect security vulnerabilities that traditional scanners might miss," and lists some potential use cases as:

- **Analysing request and response data for potential vulnerabilities specific to a Single-Page Application (SPA) framework**
- **Analysing request and response data exchanged between serverless functions for potential security vulnerabilities**

One way which security researchers can get ahead of malicious uses of AI is by*

The full version of Intelligence Insights is covered in our Premium Threat Pulse. This is available to Managed Service clients and those that purchase our Intelligence Subscription Service.

NCC Group offer Threat Intelligence services including that of bespoke reporting on topics surrounding your organisation. Why not speak to a member of the team to see how we can support your business with the ever-evolving threat landscape.

SECTION 03

VPN BRUTE-FORCE ATTACKS

In a continuation of this month's Insights section, we are taking a closer look into a recent increase in brute force attacks specifically targeting virtual private networks (or VPNs). We will explore the nature of a brute force attack, the different types of attacks, what recent waves of activity have been spotted in the wild as well as any mitigation advice that clients/ organisations can implement.

Brute Force Attack/s

First and foremost, it is important to determine what a brute force attack is; A brute force attack is a widely used method by threat actors in which they utilise every possible combination of characters, words, or phrases in order to get hold of encrypted information or gain valid credentials (i.e. a threat actor would typically send GET and POST requests to a server).

In other words, a threat actor essentially relies on a trial and error approach in order to guess the information they are seeking which could include the following:

- Obtain passwords / credential details
- Access systems, networks and /or infrastructure

The full version of Intelligence Insights is covered in our Premium Threat Pulse. This is available to Managed Service clients and those that purchase our Intelligence Subscription Service.

NCC Group offer Threat Intelligence services including that of bespoke reporting on topics surrounding your organisation. Why not speak to a member of the team to see how we can support your business with the ever-evolving threat landscape.

Key Steps of A Brute Force Attack

Figure 2: Basic Brute Force Attack

According to the MITRE ATT&CK framework, brute force is a technique mainly associated with the credential access tactic and can be further broken down into the following sub-techniques.

SECTION 04

THIS MONTH'S THREAT HUNT – ICEDID & DAGON LOCKER

Summary

On a monthly basis, NCC Group's Threat Intelligence Team researches and identifies prolific threats in the landscape, from new infostealer malware to widespread campaigns conducted by nation states or Organised Crime Groups (OCGs) for threat hunts on our SOC customer's infrastructure.

This allows us to leverage IoC-driven threat intelligence to fuel proactive detection on our customer's environments and subsequently remediate the threat.

These IoC's are queried against our EDR, SIEM and Network Monitoring clients, and this past month our focus was a phishing campaign which resulted in the deployment of IcedID and, eventually, Dagon Locker.

This allows us to leverage IoC-driven threat intelligence to fuel proactive detection on our customer's environments and subsequently remediate the threat.

These IoC's are queried against our EDR, SIEM and Network Monitoring clients, and this past month our focus was a phishing campaign which resulted in the deployment of IcedID and, eventually, Dagon Locker.

The Results

On a monthly basis, NCC Group's Threat Intelligence Team researches and identifies prolific threats in the landscape, from new infostealer malware to widespread campaigns conducted by nation states or Organised Crime Groups (OCGs) for threat hunts on our SOC customer's infrastructure.

The full insights provided by our Threat Hunt are covered in our Premium Threat Pulse. This is available to Managed Service clients and those that purchase our Intelligence Subscription Service.

Our Threat Hunt capabilities are available through our Managed Services offerings including MDR, MXDR and XDR SOC services. Get in touch with our teams to give your organisation the reassurance and insights provided by our proactive intelligence-led security services.

SECTION 04

THREAT SPOTLIGHT

RenAIssance

AI and its exploitation by anyone with a modicum of malicious intent is a topic on par with the current top 10 pop radio singles – ubiquitous, and somehow on everyone's mind. Automated attacks, sophisticated phishing schemes, adaptive malware, supercharging the threat actors' capabilities, the transformative potential of AI have been listed as the next disruptive novelty in the cybercrime news.

The intriguing aspect of AI in cybercrime, however, lies less in the realm of disruption, and almost entirely in the same realm that all of us exist in physically, including the cybercriminals themselves: the human reality we all share.

The core application of AI is enhancing existing human ability to process tasks, and its implementation in our daily lives is still largely dependent on higher levels of skill and resource investment on the side or end users who would like to experience the transformative tech beyond shaping phishing prompts or drafting legitimate emails to their doctor.

In this report, we will be mainly focusing on the support uses of AI in the cybercriminal world.

The full Threat Spotlight can be viewed in our Premium Threat Pulse. This is available to Managed Service clients and those that purchase our Intelligence Subscription Service. If you are interested in key insights and explorations of the current threat and geopolitical landscape, look no further than our monthly Threat Spotlights.

These will provide you with an in-depth view of current pertinent topics from AI, rising malware, emerging threat actors, nation-state activities and more.

Advised defensive strategies remain unchanged as AI has an augmentative role in existing TTPs (Tactics, Techniques & Procedures), though heightened awareness of the landscape may aid in future decision making.

Part 1: Attack tools

A large portion of the underground chatter concerning AI seems to be heavily focused on pure learning efforts. Participants discuss GPT prompts, potential implementation of AI and other hypotheticals, and periodically inquire about the service providers within the area that could construct something resembling the said hypotheticals.

Straddling the line between attack and support tools, one area of obvious AI augmentation is in that of reconnaissance. In its current state AI's role within these tools is more supportive than offensive, though with the rapid rate of development this could change very quickly. If AI can be harnessed to facilitate increased automation this gap will get smaller and smaller.

Once access is acquired a threat actor's next goal is often to gather additional privileges or move laterally throughout the network.

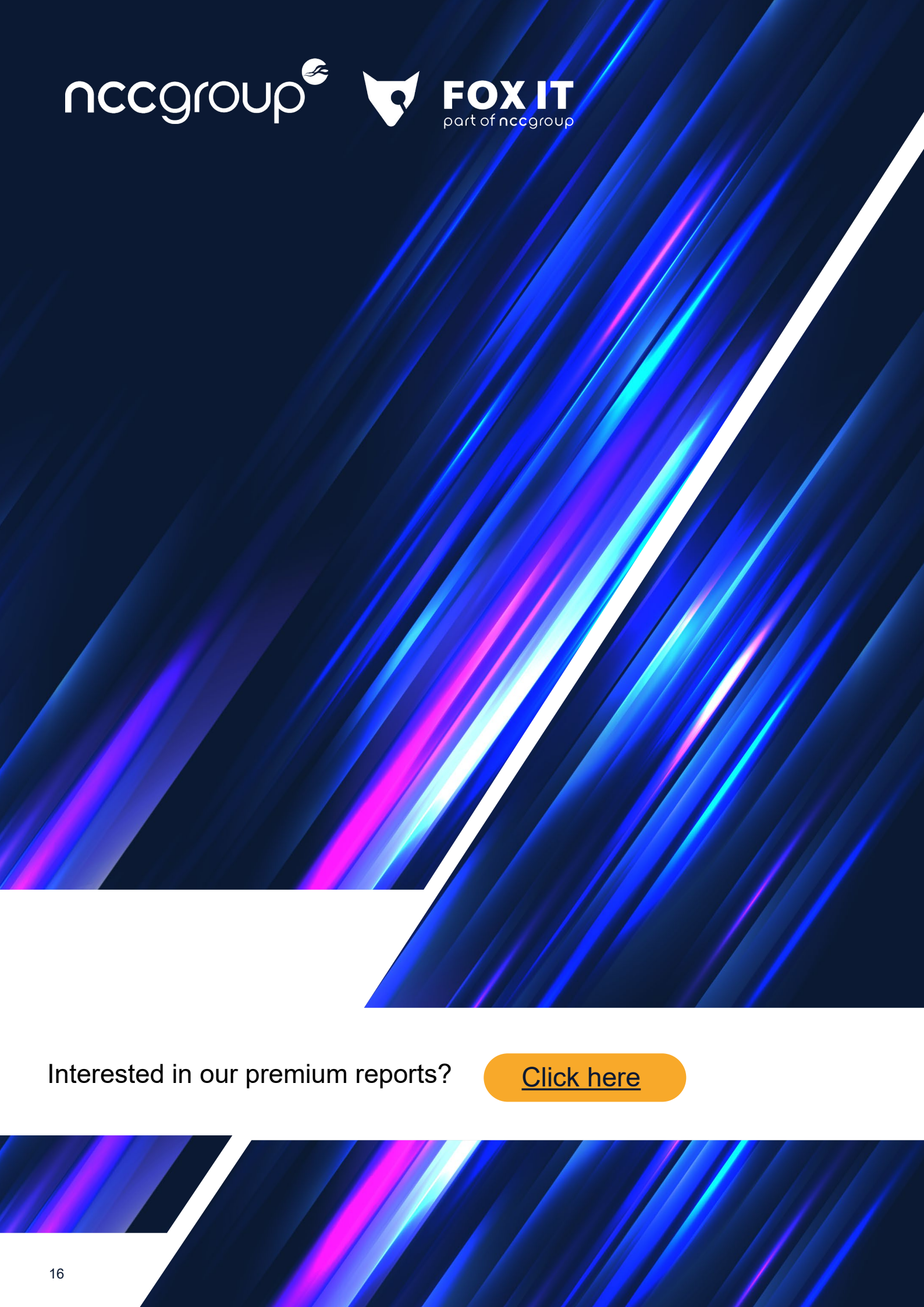
About us

NCC Group is a global cyber and software resilience business, operating across multiple sectors, geographies and technologies.

As society's dependence on the connected environment and associated technologies increases, we use our global expertise to enable organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With circa 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com



Interested in our premium reports? Click here