nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

Review of November 2024

FOX IT

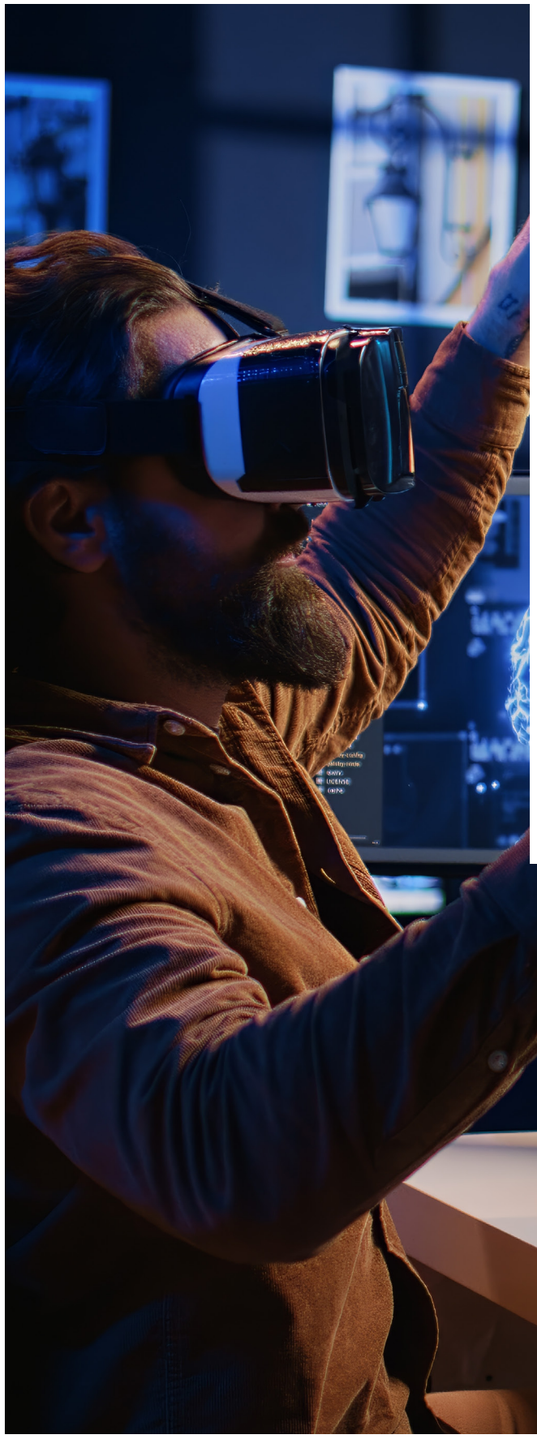
part of nccgroup

Executive Summary

This November, we continue to provide you with insights from the cyber threat landscape. The figures from our ransomware database suggest a 16% increase in ransomware activity, with Akira overtaking as the leading threat actor and Industrials as the most targeted sector. Away from the statistics, our ransomware spotlight discusses the identification of a new ransomware strain, Ymir, its application in a recent attack, and ongoing collaboration between ransomware actors and different cybercriminals. As ever, the lines continue to be blurred between cybercriminals and their traditional roles.

In November, we continue with our theme of nation-state activity, flagged as part of the current and emerging threats by Microsoft in the recent Microsoft Digital Defense Report 2024. This month, we provide a high-level overview of Sandworm, the Russian nation-state actor, and the potential threat to the Energy Sector. This follows a recent warning within the security community of a potential uptick in activity over the winter period, and thus the importance of securing infrastructure in the sector.

Finally our Emerging Cyber Security Trend explores Quantum Computing, as although this is a threat that will be more prominent in the long-term, reports suggest that we must consider and prepare for this now. A particular emphasis on its ability to reduce the effects of cryptography is explored.



Contents

Section 1

Ransomware Key Statistics

16%

Global ransomware attacks increased by 16% in November

32%

Industrials accounted for 32% of ransomware attacks in November

15%

Akira was responsible for 15% of attacks in November

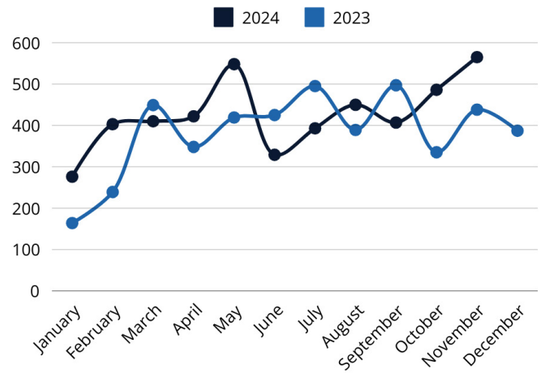


Figure 1 Ransomware Attacks 2023-2024

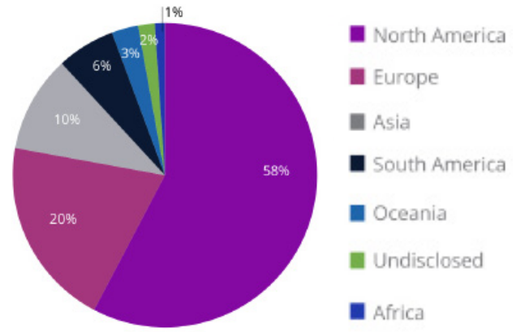


Figure 2 Ransomware Attacks by Region November

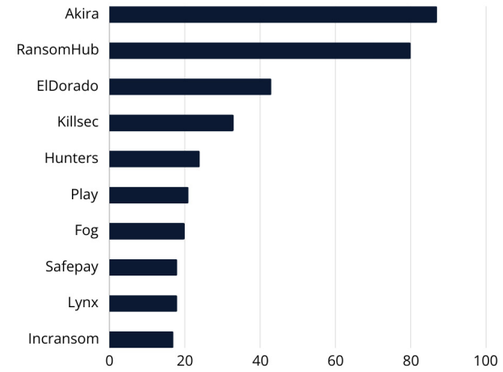


Figure 3 Top 10 Threat Actors November 2024

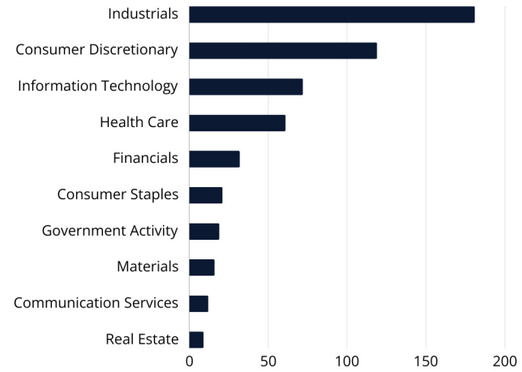


Figure 4 Top 10 Sectors November

Key Events

07/11/24
Howell Electric

Medusa ransomware stole 189.9 GB of data from Howell Electric. The company is now assessing the impact and securing its systems.

08/11/24
MedElite

Everest ransomware attacked MedElite Group, threatening to release data of 119,000 patients unless demands are met within 13-14 days. They posted sample data on the dark web, highlighting the need for better cyber security in healthcare.

25/11/24
Mexican Government

RansomHub breached Mexico's gob.mx, stealing 313 GB of data. They demanded a ransom within 10 days, threatening to release sensitive government information.

Starbucks Back To Pen & Paper

The recent ransomware attack on Blue Yonder, a supply chain management software provider, has significantly impacted Starbucks. The attack, which began on November 21, 2024, has disrupted Starbucks' ability to track employee hours and manage payroll systems. As a result, Starbucks has had to revert to manual processes to ensure employees are compensated accurately.

NCC Group Services

NCC Group can support you to mitigate against the ransomware threat. Please see our contact details at the end of this report should you require assistance.

Section 2

Ransomware Spotlight:

Ymir Ransomware and Collaboration between Ransomware Operators

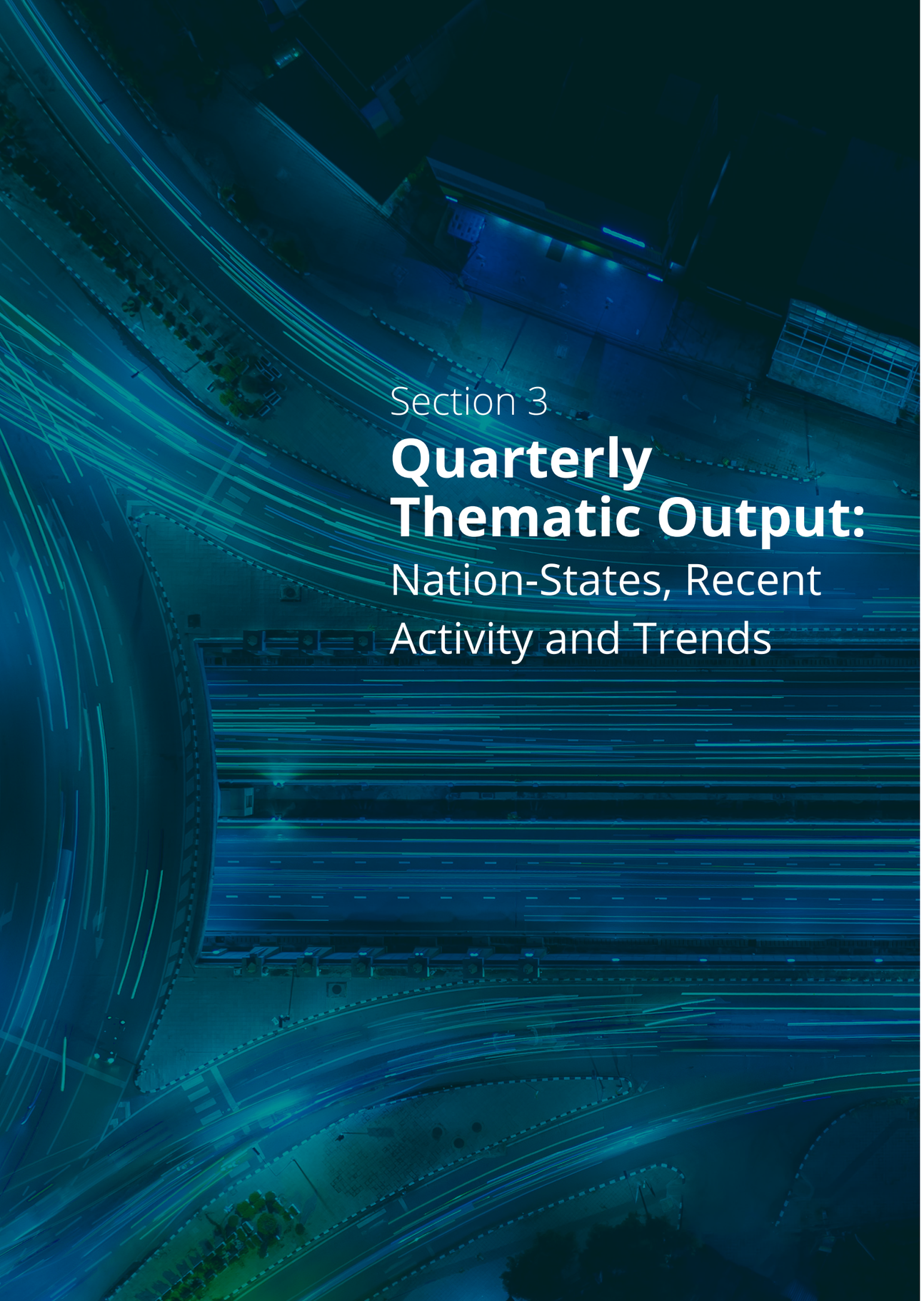
The Ransomware Spotlight piece for November introduces a new ransomware strain, Ymir. Ymir has only recently been documented for the first time, in July 2024, and was recently discussed in the context of their attack against a target in Colombia.[1]

This attack relied upon gaining initial access using a credential compromised by the RustyStealer malware, which then allowed Ymir to deliver their ransomware in a targeted way thanks to the specific configuration options within, allowing them to bypass unwanted files and avoid discovery. This, combined with the atypical execution flow utilised by Ymir, using the “malloc”, “memmove”, and “memcmp” memory management functions, allowed the group to operate stealthily and avoid discovery until their malware had been successfully deployed.

The strain has divided security commentators over whether the group acted entirely independently, or whether they collaborated with one another to provide initial access. This speaks to a wider conversation on collaboration between ransomware operators and other types of malicious cyber actors, which we also explore below. 2024 has also seen a variety of cybercriminals deploy ransomware, including nation-state-sponsored groups and hacktivists.

There are many factors influencing the adoption of ransomware tooling and methodology by these groups, including the ability to use ransomware tools as a means of destruction, i.e. by encrypting a victim’s data, as well as the increasingly political nature of hacktivism in the wake of Russia’s invasion of Ukraine.

This proliferation of ransomware from a wider range of actors than we have previously seen is likely to continue into 2025. Ransomware has been growing, evolving, and becoming steadily more sophisticated in the last few years and other actors have certainly taken notice.



Section 3

Quarterly Thematic Output:

Nation-States, Recent Activity and Trends

In November, we continue with our quarterly theme reviewing nation-state activity and trends, with a specific focus on Russia, one of the most notable nation-state threats. A recent warning of the potential targeting of the Energy sector by the notorious Sandworm during this coming winter has flagged new interest and concern.

Below, we will discuss the possible motivations for such an attack, as well as insights into the group's typical targeting pattern, capabilities and motivations. Additionally, we provide a brief overview of the Energy sector and why it might be of interest to nation-state groups.

A recent warning for Sandworm Activity

On 22 November 2024, a Threat Intelligence Analyst from Google Mandiant warned of a potential spike in Sandworm's activity, specifically targeting the Energy sector across Europe during this winter period.

This concern was also initially raised by Google Mandiant's Head of Threat Intelligence during the Tallinn Digital Summit, which took place on the 19th and 20th November 2024.

The warnings were flagged due to observed activity against the sector by Google.[2] Additionally, physical attacks are already active, with Russia targeting the Energy infrastructure in Ukraine with missiles and drones end of November 2024.[3] Considering potential for a cyber-attack, we review Sandworm's targeting pattern, capabilities, motivations and any notable recent activity, to support organisations within the Energy sector with their defence.

Sandworm is an operationally mature threat associated with Russia's General Staff Main Intelligence Directorate (GRU), Main Center for Special Technologies (GTsST) military unit 74455.

The Russian Intelligence services are split into the Federal Security Service (FSB), Foreign Intelligence Service (SVR) and Main Intelligence Directorate (GRU). Each service has with their own remit.

For example, the SVR focusses on intelligence and espionage activities outside of Russia, while the GRU handles military intelligence. The two services are known to work alongside each other, whereas the FSB has a domestic focus and is mainly tasked with counterterrorism, counter espionage, and Russian information security.[4]

Sandworm has actively engaged in a full spectrum of operations including influence operations and cyber espionage attacks, placing the group in a unique position to support Russia's cyber warfare goals and objectives.

Sandworm is suspected to have been active since at least 2009 and typical targets include government, energy, transportation, and defence sectors globally.

Recent activity has however focused heavily on targeting Ukraine to assist the Russian military with intelligence gathering to gain an advantage in the ongoing war. Even with the ongoing war, Sandworm has been observed to sustain espionage activity across the following regions: North America, Europe, the Middle East, Central Asia, and Latin America.[5]

This is not the first time in which Sandworm have been observed to target Energy to advance Russia's strategic goals, as targeting this sector can prove highly disruptive and destructive, and a method to support kinetic warfare efforts. Whilst specific targets are currently not specified, we recommend that organisations operating in the European Energy sector, and more broadly, familiarise themselves with Sandworms TTPs to tailor defence measures, helping to prevent attacks.

Section 4

Emerging Cyber Security Trend:

Quantum Computing

The advent of quantum computing will constitute a seismic shift in computing power. Using quantum mechanics, this will be able to solve far more complex problems, far more quickly than is possible with our digital computers, bringing incredible advancements and opportunities.

In addition to quantum computing, other quantum technologies such as sensing and imaging, as well as quantum clocks and communications, will transform the way in which we live.[6]

The UK's Information Commissioner's Office (ICO) has explored the issue of quantum computing and its impact on personal data, considering the implications such changes will have on privacy and data protection.

The World Economic Forum has stated that investment currently has reached US$35.5 billion and notes that the power of this technology must be used responsibly, pointing to the requirement for industry-specific frameworks and best practices-based guidelines.[7]

Exactly when quantum computing will have widespread uptake is unclear, but estimates suggest we are 5-10 years away. Organisations preparing for the advent of quantum computing will be dealing with long lead times and potentially considerable expense, so allowing time to do this is crucial.

The risks associated with quantum computing relates predominantly to cryptography and its implications for data security. Whilst these are forecast to be a future problem, there is the possibility that threat actors will hold on to data which they exfiltrate at this time and wait for future opportunities to decrypt the stolen data.

It may appear that these risks are sufficiently far ahead that organisations can wait to monitor and react to changes later, however, it is an important conversation to raise for consideration now.

There is notable risk to organisations whose lead times can be significant and may well have large amounts of data and systems to protect. As such, having sufficient time to consider, review, and implement protections can be of significant value and the reason for highlighting the impact quantum computing might have in the near-term future.

The full versions of our spotlight, quarterly thematic output, and emerging cyber security trend research 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 on the current threat and geopolitical landscape, look no further than our research insights.

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

Sign up here

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
reponse@nccgroup.com
www.nccgroup.com

People powered tech-enabled cyber security

FOX IT
part of nccgroup