nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

Review of Q3 2024

FOX IT

part of nccgroup

Executive Summary

In Q3 2024, we introduced several new research points to our reporting, including research on emerging cybersecurity trends, a ransomware spotlight and a quarterly thematic output, as produced in our Monthly Threat Pulse.

In addition, we updated our vulnerability threat landscape output, now discussing key insights identified from the CVEs we alerted on during the reporting period, via our Threat Intelligence Alerts. These updates seek to provide a more dynamic and informed report.

Our critical incidents section explores cyber events across July-September 2024. One notable incident that caught global attention was the CrowdStrike software defect resulting in disruptions and outages to global services. This event served as a reminder of the widespread impact security incidents have, and that they do not need to be orchestrated by a threat actor. Rather, that organisations can become vulnerable to threats alike if processes are erroneous.

Looking at ransomware activity, in August, we implemented the Global Industry Classification Scheme (GICS), moving away from the Refinitiv Classification Scheme we have used since 2021 to classify ransomware data. We have applied the new scheme to historical data alike and will continue to operate using this model going forward. This Quarter, we found that ransomware incidents declined by 4% from 1301 to 1252, Ransomhub were responsible for the greatest number of attacks, and Consumer Discretionary suffered the greatest number of ransomware attacks. Away from the statistics, our spotlight divers into Cicada3301 ransomware, a strain designed to target Linux/ESXi systems, and purported to be a possible rebrand of BlackCat.

Our emerging cybersecurity trend explores IoT security threats and the use of blockchains as a solution to enhance the protection of IoT devices. IoT devices have been increasingly introduced, from our offices to our homes, and can function as an entry point into networks.

Hence, we explore solutions to securing IoT, which will become increasingly important. In addition, we provide our final piece for our quarterly thematic output on misinformation, disinformation and malinformation, exploring this theme within the context of the 2024 US Presidential Elections. Our recent Threat Hunt focuses on the evolution of Quad 7 botnets.

In early September 2024, Quad7 botnet's evolution included the setting up of new staging servers, launching new botnet clusters, employing new backdoors plus reverse shells, and stepping away from open socks proxies. We provide a list of associated Tactics, Techniques and Procedures (TTPs) and indicators of compromise (IoCs) to support organisations with mitigation strategies against the threat.

Finally, we discuss the CVEs we alerted on this Quarter, with a focus on those impacting web applications and servers.

Contents

Timeline of Critical Incidents Q3 4

SECTION 1
Ransomware Key Statistics Q3 8

SECTION 2
Ransomware Spotlight: Cicada3301'S Targeted Assault on VMware ESXi Servers..... 10

SECTION 3
Emerging Cybersecurity Trend: Blockchain Innovations Enhancing Security in the IoT Landscape 12

SECTION 4
Quarterly Thematic Output: Disinformation in the 2024 U.S. Presidential Election 14

SECTION 5
Vulnerability Threat Landscape.....16

Timeline of Critical Incidents Q3

July

2nd July 2024

HealthEquity Inc reported a cyber incident in which the information of 4,300,000 people was compromised. The organisation specialises in health savings account (HSA) services as well as other consumer-directed benefits solutions, including flexible spending accounts (FSAs), health reimbursement arrangements (HRAs), and 401(k) retirement plans.

HealthEquity discovered that a vendor's account was compromised by an unauthorised third party to access the company's systems and steal protected health information. The health provider filed a report with the Securities and Exchange Commission (SEC) on 2nd July 2024, however, the investigation revealed that the breach occurred on 9th March 2024, and it was only detected on 26th June 2024 after noticing suspicious activity coming from the partner's personal device.

15 July 2024

Disney, a provider of multinational mass media and entertainment, suffered a massive leak of both employee and company data surpassing 1.1 terabytes (TB), announced on 15th July 2024.

The leaked data had been accessed via Disney's internal Slack workplace collaboration system and included discussions about ad campaigns, studio technology, personal employee information as well as the details of unannounced products including videogames.

According to the threat actors, a Trojan horse malware attack was used to breach the network. A hacktivist group known as NullBulge claimed the attack, stating that they were 'protecting artists' rights and ensuring fair compensation for their work'.

19 July 2024

The cybersecurity company CrowdStrike distributed a faulty content update to their Falcon Sensor security solution which resulted in a widespread outage causing problems with Microsoft Windows machines running the software. The issue was not related to a cybersecurity incident but rather, a defect occurring in a single content update for Windows hosts.

The disruption was first detected in Australia, before it quickly spread across Asia, Europe and the Americas, with the travel industry being one of the most affected industries.

August

10 August 2024

Orion, a global leading supplier of carbon black products, filed a report with the SEC on the discovery of a large business email compromise (BEC). The incident led to $60 million being stolen from the organisation following a series of wire transfers made to cybercriminals.

The report stated that a non-executive employee was targeted and tricked into making the transfers, likely due to impersonation tactics or other methods used by the attackers to access company funds.

Timeline of Critical Incidents Q3

August

13 August 2024

Over 50,000 confidential files belonging to Poland's anti-doping agency known as POLADA were leaked following a cyber-attack by a threat group known as Beregini. The leaked data contained thousands of confidential files including the medical and testing records of Polish athletes.

The threat group claiming accountability for the attack describes itself as a 'Ukrainian hacker group' which was previously observed working with other pro-Russian entities, also presenting themselves as hacktivists, to share fake documents and spread false information about Ukraine's war plans.

September

2 September 2024

Transport for London (TfL) announced that they had detected an ongoing cyber-attack, but no evidence suggested that customer data has been compromise, and no services were disrupted. Later, on 12th September, a further announcement was made that a 17-year-old was arrested in connection to the incident. At the time, TfL mentioned that roughly 5,000 customers' sort codes and bank account details might have been accessed by the attackers in the "ongoing cyber security incident".

Additionally, the information of an unknown number of customers who signed up to TfL email alerts, was announced as potentially exposed. The customer information includes names, home addresses and email accounts.

21 September 2024

MoneyGram, a digital payment solutions provider, posted on their X (Twitter) account an announcement about a network outage impacting connectivity to a number of their systems.

On 23rd September an additional announcement stated that a cybersecurity issue was identified as affecting their systems.

The attack impacted financial transactions, mainly in the Caribbean, Jamaica and Mexico. No threat actor has claimed responsibility for this incident yet.

23 September 2024

Fylde Coast Academy Trust (FCAT) announced that they were impacted by a ransomware attack which compromised its IT infrastructure and affected all 10 schools under the FCAT umbrella, across Blackpool and Lancashire.

The incident resulted in disrupted daily operations, with the schools being unable to rely on computers, printers and other tech for their routine tasks. All schools were forced to revert to traditional, non-IT-based processes for essential tasks. Phone lines were also reported as impacted.

Section 1

Ransomware Key Statistics

4%

1252 attacks were reported in Q3, down 4% from 1301 in Q2.

24%

Consumer Discretionary accounted for 24% of ransomware attacks in Q3.

15%

Ransomhub was responsible for 15% of attacks in Q3.

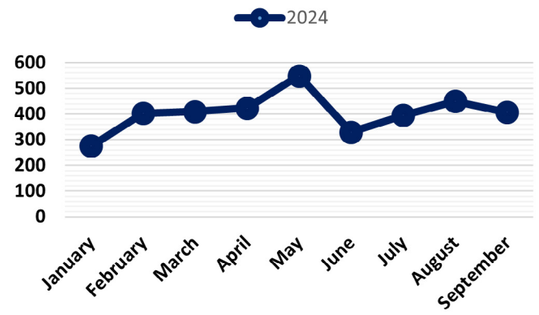


Figure 1 Number of ransomware attacks per month, 2024

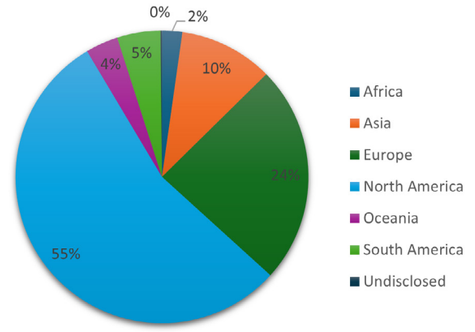


Figure 2 Number of ransomware attacks per region, Q3

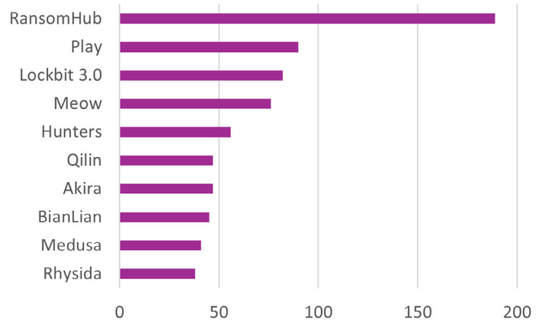


Figure 3 Top 10 threat actors in Q3

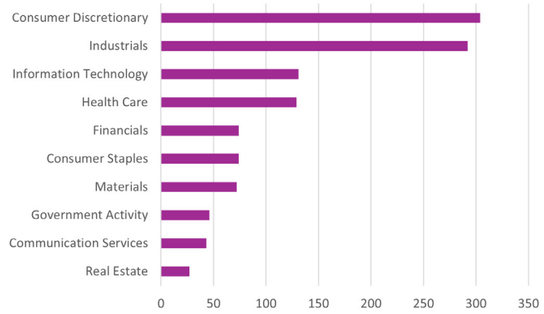


Figure 4 Top 10 sectors targeted in Q3

Key Events

July 15, 2024 - Rite Aid Pharmacy

Rite Aid reported a data breach affecting 2.2 million customers. RansomHub claimed to have stolen over 10 GB of personal data, including names, addresses, driver's license numbers, dates of birth, and Rite Aid rewards numbers.

August 08, 2024 - City of Columbus

Rhysida ransomware group leaked over three terabytes of stolen data, including Columbus employees' personal files, on the dark web after failed auctions. Cybersecurity experts confirmed the data dump.

September 5, 2024 – Kawasaki Motors EU

RansomHub attacked Kawasaki, stealing 487 GB of data, including business documents, banking records, and internal communications. After failed auctions, they threatened to leak the data on the dark web.

WazirX Hacked: $230 Million Stolen in Major Cyber Heist

A cyber-attack on July 18, 2024, saw the Indian crypto platform WazirX lose over $ 230 million in digital assets. The attack was attributed to the Advanced Persistent Threat Group (APT) Lazarus and targeted a multisignature wallet served by the firm known as Liminal. WazirX has hired the services of cyber security experts and the authorities to retrieve the lost money.

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 Cicada3301'S Targeted Assault on VMware ESXi Servers

Overview

Over the past months, the increase in cyber threats specifically aimed at virtualised environments has exposed weaknesses in organisations' essential networks. A new ransomware variant Cicada3301 was observed as targeting vulnerabilities inside VMware ESXi servers, which is crucial for organisations using virtual machines.

This research explores the ever-changing ransomware threat landscape with a focus on Cicada3301 ransomware and virtual environments that use the Linux operating system.

As more enterprises have turned to virtualisation to achieve scale and flexibility, the threat that these infrastructures pose has grown, with attackers viewing them as high value targets. The effects of ransomware attacks include the shutdown of operations, information leaks, and significant financial losses.

The following section explores Cicada 3301 ransomware, its working mechanisms, and its particular interest in the VMware ESXi servers, as well as detailing the defensive measures that organisations can take to help counter this threat.

Cicada3301 Ransomware

A new rust-based ransomware variant dubbed Cicada3301 has been identified as specifically targeting Windows and Linux/ESXi systems. The name stems from the online cryptographic puzzles from 2012-2014, but there is no link in terms of the cryptography used in the ransomware.

Notably, the strain itself bears similarities to BlackCat ransomware with rumours of this being a possible rebrand of Cicada3301's activity first became evident in June 2024, when the group advertised recruitment efforts for affiliates on the RAMP cybercrime platform.

The group operates a double-extortion model, and although identified in June, was recently flagged by the security community in reporting from late August – early September. If the group are related to BlackCat, this provides another example of ransomware actors ability to rebrand and work under new aliases, and thus the whack-a-mole nature of countering ransomware groups.

Specifically, the strain exploits weaknesses within the Linux system, enabling the malware to infiltrate and encrypt critical data stored on virtual machines.

Since June 18, 2024, Morphisec researchers have identified over 20 victims across North America and the UK. This ransomware variant has raised concerns among cybersecurity professionals due to its targeted implementation. Organisations in sectors such as finance, healthcare, and technology that utilise VMware ESXi servers are among those particularly at risk.

When the ransomware infiltrates these environments, it can freeze organisational operations by rendering crucial data unavailable, leading to significant operational and financial impacts. The implications of these risks include disruption of business activities, and financial loss due to ransom payments.

Section 3

Emerging Cybersecurity Trend: Blockchain Innovations Enhancing Security in the IoT Landscape

The Internet of Things (IoT) refers to the collective network of connected devices and technologies that facilitate communication between devices and the cloud, as well as between devices themselves. Today, more and more devices, sensors and appliances are increasingly interconnected over the internet.

How can Blockchain Improve IoT Security

IoT devices are vulnerable to cyber-attacks due to limited computational power and security features. Blockchains can address such vulnerabilities by offering secured transparent management of data and device interactions.

The integration of blockchain with IoT may support several security enhancements: first, the decentralised nature-with no single point of failure-eliminates many hacking options; second, it ensures that the data recorded on the ledger is tamper-proof and immutable, which is highly important for IoT devices gathering and further transmitting sensitive information .

It is also capable of enabling robust authentication mechanisms for IoT devices, making it harder for unauthorised devices to access the network. Its secure peer-to-peer communication reduces the risk of data interception and tampering.

Likewise, its transparency enables easy auditing and tracking of all transactions and interactions between IoT devices, hence, helping to identify and mitigate against any security breaches in record time.

There are several ways to take full advantage of the blockchain in IoT security. Investing in research and studying the best methods of integrating blockchains into devices and networks-developing lightweight blockchain protocols suitable for resource-constrained IoT devices, will be key.

Also, the development of industrial standards and protocols in blockchain-based IoT security will support interoperability and a wider diffusion of the technology. It is worth implementing pilot projects first that test and refine blockchain solutions in real-world IoT applications.

Such an approach would guarantee that potential challenges or areas for improvement were identified well in advance. This concerns a holistic security solution with close collaboration between blockchain developers, IoT manufacturers, and cybersecurity experts.

Finally, knowledge dissemination among stakeholders regarding benefits and methods of blockchain for IoT security will also function as a driver for its integration and innovation. With all the above steps considered, blockchain can greatly improve the security and dependability of IoT systems.

Section 4

Quarterly Thematic Output: Disinformation in the 2024 U.S. Presidential Election

In this final report on the theme of misinformation and disinformation, we will look at the impact of misinformation and disinformation on the 2024 U.S. Presidential elections, building on the earlier consideration of their influence on global elections this year.

Over the course of the elections in 2024, there have been reports indicating the increasing instance of disinformation in evidence. We have seen that, advances in Artificial Intelligence (AI) technologies, coupled with widespread social media usage, has helped proliferate disinformation, globally.

Such activity is of concern given its potential to assert malign influence on the voting public, manipulated by parties in such a way that democracy, as well as national security, is undermined. If voters do not trust in the democratic apparatus because of disinformation, then this will undermine confidence in democratic process.

Whilst at this point in time, the efficacy of these campaigns is not considered to be a serious threat, it does highlight the future risk, given that these are likely to become more convincing and more prolific, making it ever harder to discern the truth.

This is a period of particular importance, as the U.S. Presidential election is seen by many as a defining moment in history. With one recent poll suggesting that in the 2024 U.S.

Presidential elections, 59% of Americans believe that the very future of democracy is at stake , irrespective of the outcome, it would suggest that the stakes for the United States, and the democratic world, are very high.

The same is true, then, of its adversaries seeking to sway the result in their favour.

We will look at whether there is evidence of disinformation campaigns designed to undermine the 2024 US Presidential elections this Quarter, and whether there has been evidence of this around other 2024 elections more generally.

We will consider which parties are expected to be responsible for doing this, and their motivations and how new technologies aid them in achieving their goals.

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.

Section 6

Vulnerability Threat Landscape

In Q3 2024, multiple vulnerabilities impacted web applications and servers with Remote Code Execution (RCE) capabilities. Web applications play a vital role in business-critical systems, handling sensitive data, financial transactions, and essential communications.

CVEs affecting these systems demonstrates how web applications remain vulnerable and continue to be a potential entry point into networks. Equally, as these applications and servers often support critical business operations, this has the potential to impact wider organisational security if successfully exploited.

Web applications are vulnerable to CVEs for many reasons, from large pools of untested software as technology develops to poor security configurations. These weaknesses likely contribute to why we are observing many CVEs relating to web applications, as they are more prone to vulnerabilities.

Next Steps

Organisations should enhance their security through regular code reviews, security audits, and secure coding practices to reduce the likelihood of vulnerabilities related to improper input handling.

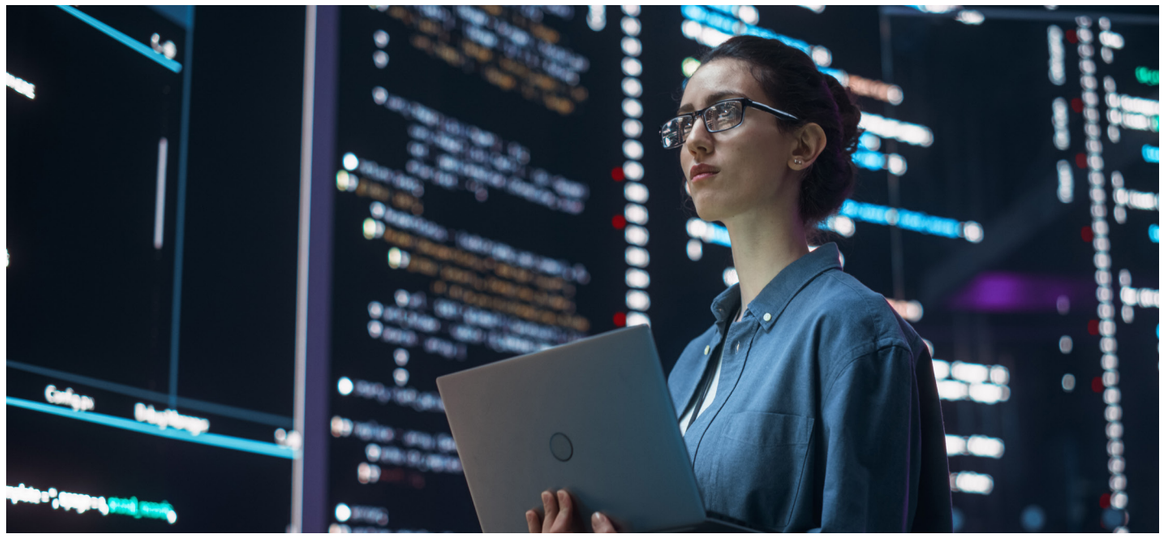
Given the severity of RCE vulnerabilities there is a clear need for patching quickly. Organisations should closely monitor vulnerabilities in their systems and prioritise immediate patch deployment to minimize exposure.

As RCE vulnerabilities are highly exploitable, organisations should also focus on their incident response plans. This includes conducting regular drills and testing their ability to respond to RCE-related incidents or breaches.

Organisations should implement continuous monitoring by deploying tools to monitor applications for vulnerabilities in real time to detect and respond to any potential attacks quickly.

Likewise, they should foster a culture of security by providing training on secure coding, input validation, and patch management to developers and IT teams where relevant. Also, collaborating and engaging in Threat Intelligence with industry peers and security groups can provide valuable insights into new vulnerabilities, enabling organisations to prepare and mitigate vulnerabilities effectively.

Given the wide spread of reliance to third-party applications, organisations must assess the security practices of their vendors and partners alike to ensure that they do not introduce new risks.



nccgroup

People powered tech-enabled cyber security

About us

NCC Group is a global cyber and software resilience business, operating across multiple sectors, geogra-phies 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

FOX IT
part of nccgroup