nccgroup

People powered tech-enabled cyber security

Monthly Threat Pulse

Review of August 2024

FOX IT

part of nccgroup

Executive Summary

This August, we have made a several updates to our Threat Pulse. We continue to provide you with key figures from the ransomware threat landscape, presenting ransomware activity highlights for the month including regional, sectoral, monthly and threat actor statistics, as well as key events.

In August, we observed a 14% increase in ransomware activity, RansomHub as the leading threat actor, and Industrials as the most targeted sector.

In addition, our newly incorporated ransomware spotlight discusses ransomware attacks during the August period of the 2024 Olympic Games. With over 40 ransomware attacks against organisations in the city, this raised concern regarding the security of major, global events. Equally, this raised interest as to how we best protect future events of this scale. This segment of the report will be dedicated to exploring pertinent ransomware activity from the month.

Additionally, we have introduced a new segment under 'Emerging Cybersecurity Trends'. This section is dedicated to discussing emerging cybersecurity trends, i.e. new developments and changes that could threaten the landscape.

This includes everything from technological developments in AI exploited by threat actors to growing supply chains that render organisations vulnerable.

Overall, the idea will be to support organisations to remain informed regarding the most important developments impacting cybercrime to mitigate against present and upcoming threats.

In August, we explored how AI-powered malware could be used to generate self-replicating worms, following new research by Cornell University.

Finally, we continue to explore the theme of misinformation, disinformation and malinformation as part of our theme for this quarter. This month we discuss misinformation, disinformation and cyberterrorism, following the UK Southport riots in July.

Pakistani authorities charged an individual with cyberterrorism for their role in disseminating disinformation linked to the Southport riots. Although later dropped, this raised the question of cyberterrorism and its association with disinformation and misinformation overall, as well as future considerations.

Contents

Section 1

Ransomware Key Statistics

14%

Global ransomware attacks increased by 14% in August

24%

Industrials accounted for 24% of ransomware attacks in August

16%

RansomHub was responsible for 16% of attacks in August

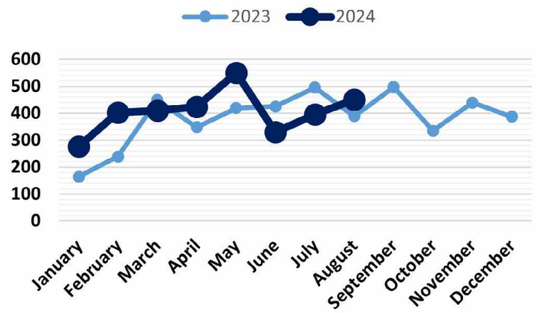

Figure 1: Global Ransomware Attacks by Month 2023 - 2024

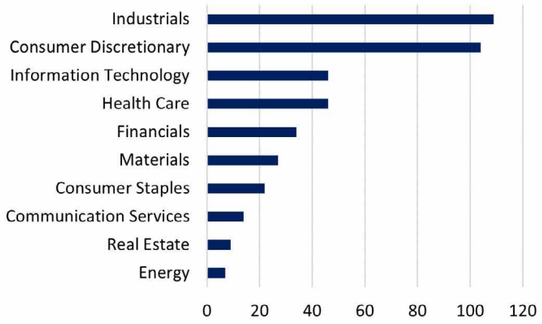

Figure 2: Ransomware Attacks by Sector July 2024

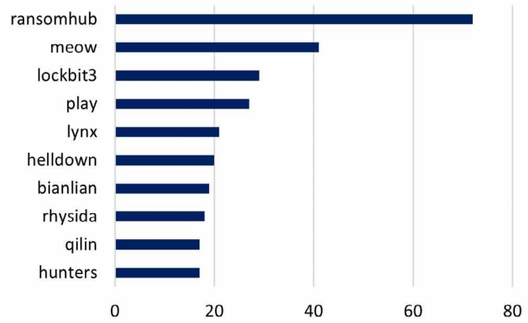

Figure 3: Ransomware Attacks by Threat Actors 2024

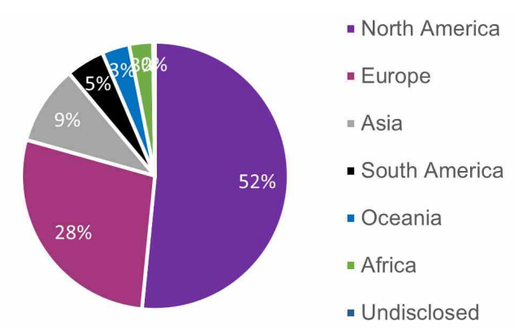

Figure 4: Ransomware Attacks by Region July 2024

Key Events

02/08/24 Immigration Firm's Customers Warned of Data Exposure

The firm was targeted by the BianLian ransomware group and directly contacted customers, warning them about potential exposure of their sensitive information. This incident raised significant concerns about data privacy and security.

05/08/2024 Ransomware Attack targets Grand Palais Paris

Threat actors target Olympic venue allegedly leaving a ransom note demanding a payment in cryptocurrency.

21/08/24 Energy Company Halliburton Targeted in Major Ransomware Attack

The attack impacted Halliburton's IT infrastructure and business activities, causing the company to shut down some systems as part of its cybersecurity response strategy. The intrusion generated concerns for the security of critical infrastructure.

Dark Angels Strike: Fortune 50 Company Pays Record $75 Million Ransom

In August 2024, a Fortune 50 company paid a record-breaking $75 million ransom to the Dark Angels ransomware organisation. This payment is the largest known ransom ever paid to a ransomware outfit, exceeding the previous record of $40 million.

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 August: Paris Olympic Games 2024

Overview

The Paris Olympics drew athletes from across the world to showcase their talents, however, it was not spared from cyber threats.

The event itself was not affected, although a largescale ransomware attack on the Grand Palais and other museums in France revealed that even with careful preparation to secure the events, risks and threats remained. This month we outline the particulars of the ransomware attack and its significance in the context of the Olympics and future events.

Ransomware hits the Grand Palais

French authorities reported that during the Paris Olympics, the Grand Palais, one of the key Olympic venues, along with approximately 40 other museums across France, fell victim to a ransomware attack in early August.

While the ransomware incident did successfully infiltrate and disrupt these cultural sites, causing them to lose access to crucial data and systems, the attack did not disrupt the Olympic Games.

This ransomware attack was part of a broader wave of cyber incidents during the Games where attackers targeted various critical infrastructures, including government entities and transport networks.

Despite the severity of ransomware, which often leads to significant operational disruptions and financial losses, Anssi, the French cybersecurity agency, managed to contain the impact and ensured that the operations crucial to the Olympics remained unaffected.

The agency's swift and effective response highlights the robustness of the cybersecurity measures in place for the Games, preventing what could have been a much more significant disruption had the attack reached the systems directly involved in the Olympics.

This incident underscores the ever-present threat of ransomware in large-scale events like the Olympics, where attackers seek to exploit high-profile targets.

However, the incident at the Grand Palais and other museums serves as a reminder of the importance of securing all connected systems, even those not directly linked to the event itself, to prevent collateral damage in the face of sophisticated cyber threats.

Section 3

Emerging Cybersecurity Trend: AI and AI-Powered Malware

Overview

This month, we are introducing a new section to the Pulse, Emerging Cybersecurity Trends (ECTs). This will explore insights from ECT topics, such as AI, IoTs or Supply Chain security.

The idea is to provide insights into critical and pertinent cybersecurity topics as they develop.

Understanding such trends will support organisations to remain abreast of the threats that are arising from increased digitalisation and the new ways in which threat actors may seek to target and/ or exploit technology.

This month we consider artificial intelligence (AI) and how it could enhance traditional malware capabilities, with a focus on the Morris Worm II.

Common manifestations of AI-assisted cybercrime include AI-generated phishing, which creates realistic but fake messages, deepfakes which produce convincing but fake audio and video content, adversarial AI/Machine Learning (ML), which manipulates machine learning models to exploit vulnerabilities, and AI-enhanced ransomware, which dynamically identifies and encrypts important data while avoiding detection.

These advanced threats significantly increase the difficulty of recognising and preventing cyberattacks.

What can AI do for Malware?

AI can increase the sophistication and effectiveness of cyberattacks attacks. Compared to traditional malware that frequently uses static code and predictable behaviour patterns, AI-powered malware uses the capabilities of machine learning techniques to improve its sophistication to continuously learn from its surroundings.

Its capacity to adapt in real-time makes it more difficult to predict and resist future attacks, since it can avoid traditional signature-based detection techniques by mimicking regular network traffic patterns or legitimate program behaviour.

AI-enhanced ransomware, for instance, can modify its code in real-time to evade detection, rendering the ransomware threat all-the-more difficult to identify and ultimately mitigate. AI algorithms can also analyse large amounts of data to identify vulnerabilities and high-value targets, customising its strategy to boost successful attacks.

Section 4

Quarterly Thematic Output: Misinformation, Disinformation & Cyberterrorism

Are we entering the Realm of Cyber Terrorism?

Continuing with our quarterly theme of misinformation, disinformation and malinformation, this month we consider this in the context of cyberterrorism.

In recent years, we have seen digital interactions intersect with the physical space more and more. Within the realm of cybersecurity, we have focused on the interaction between threat groups and operational technologies or critical national infrastructure (CNI). The interdependencies across a global supply chain have also made it possible to cause tangible disruption through digital means.

There has been increasing discourse around the impact of digital interactions on an individual basis, with a significant rise in mental health issues, phone or screen addiction, cyber bullying etc. Weaponising digital interactions to spread disinformation, misinformation and malinformation and utilising social media platforms to amplify their visibility has created the ability to cause psychological and potentially physical harm on a societal level.

When bad actors can inflict harm on such a scale, are we entering the realm of cyber terrorism?

The definition of terrorism alone has been debated for many years and is far beyond the scope of this article to examine in detail. If we take the United Nations definition an act of terrorism required 3 key elements

- The perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act
- The intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it
- When the act involves a transnational element.

Certainly, you can argue that the spread of disinformation, misinformation and malinformation aims to influence the population at large, it can be used to spread fear and its transmission via social media provides a transnational element.

It is, however, often difficult to identify the incitement of a specific criminal act, merely aiming to sow unrest and causing disruption on a large scale. We may need further legislation to tackle this growing issue.

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

People powered tech-enabled cyber security

Interested in our premium reports?

Click here