nccgroup

People powered tech-enabled cyber security

Monthly Threat Pulse

Review of July 2024

FOX IT

part of nccgroup

Executive Summary

July 2024 represented a busy month across the cyber security threat landscape, from ongoing ransomware attacks to misinformation and disinformation activity.

Analysis of ransomware attacks throughout June identified RansomHub, LockBit 3.0 and Akira as the leading threat actors.

Where targets were concerned, the Industrials, Consumer Cyclicals and Technology sectors held the greatest number of victims. Notably, the exploitation of a critical VMware ESXi vulnerability was exploited by ransomware actors. This demonstrated that the exploitation of vulnerabilities remains a key tactic for ransomware actors, and that organisations should continue to prioritise patch management, as part of their wider threat mitigation efforts.

This month, we kickstart our focus on an exciting new theme for Q3, misinformation, disinformation and malinformation. In recent years we have observed increasing efforts by threat actors to conduct misinformation, disinformation and malinformation campaigns, often aligned with strategic geopolitical interests.

This year, there are several global events which have been targeted, such as the global elections and the Olympic Games. The events stress the pressures society operates under to preserve and protect the truth, as threat actors seek to manipulate public opinion for their own strategic advantages.

NCC Groups monthly investigation into new prolific threats investigated the DarkGate Remote Access Trojan (RAT) and associated campaign, which ran from March 2024.

This campaign was primarily observed as most active in the United States, although also impacting Europe and Australia alike. Sectors of interest included Healthcare and Telecommunications, alongside several others.

No detections were made by NCC Group's MXDR team for DarkGate malware across any of our clients SIEM, network detection, and EDR solutions.

Finally, our spotlight this month provides exciting insights into the evolving tactics, techniques and procedures (TTPs) of ransomware actors. Specifically, we look at the ever-increasing use of information stealer malware by ransomware actors.

The research underscores how threat actors are continuously identifying new methods to bolster the sophistication of their attacks and seek to gain profit via illicit means.

Likewise, it serves as a reminder that effective cybersecurity demands multiple solutions, regularly updated and informed by actionable threat intelligence.

Contents

Section 1

Ransomware Insights

From June to July 2024, the ransomware landscape observed a 20% increase in attacks from 329 in June to 395 in July.

This increase could be attributed to the summer holiday period, during which time threat actors may seek to exploit the decrease in employees present at work, including in IT security and support departments.

Attacks during the holiday period can catch companies off guard, which may result in longer investigation times, damage, and recovery times.

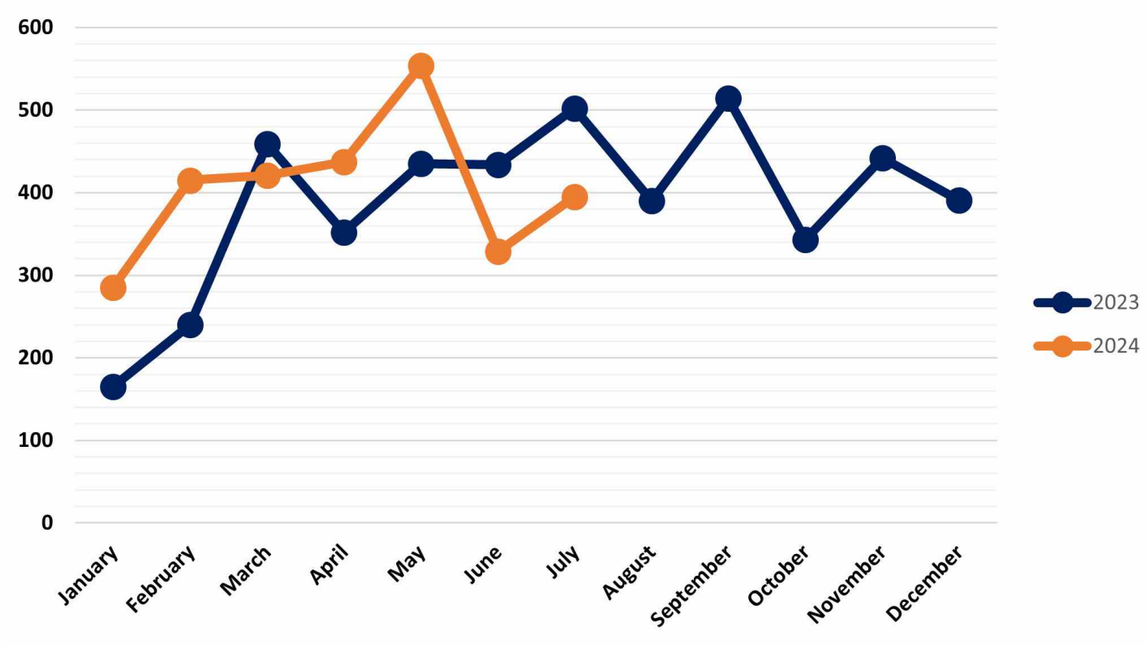


Figure 1: Global Ransomware Attacks by Month 2023 - 2024

The July numbers overall however remain much lower than observed between February – May, the most active period of 2024 thus far, and suggests an overall decline in ransomware activity at present. Whether this increase reflects the start of an upward trend remains to be seen, and we will continue to monitor such activity.

The Industrials sector saw the greatest number of attacks, 125, up from 105 in June, and reflects a continued interest by threat actors in targeting critical national infrastructure (CNI). Organisations within CNI provide critical services to society making them valuable targets, and ransomware actors pressure these targets into payment, exploiting their need to remain operational.

RansomHub emerged as the most active threat actor this month with 43 attacks, up from 27 in June. This accounted for 11% of all activity for the month and reflects a continued hold on the threat landscape by the group. RansomHub operates a ransomware-as-a-service model (RaaS), which will contribute to the higher numbers we observe, with wider affiliates also employing the ransomware strain to conduct attacks.

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 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 2

Misinformation, Disinformation and Malinformation: 2024 Global Elections and the Olympic Games

Misinformation, Disinformation and Malinformation

In Q3, we will be covering the themes of misinformation, disinformation and malinformation. Misinformation, disinformation, and malinformation are three types of false or misleading information that can have harmful effects on individuals, groups, organisations, and countries.

This month, we consider how campaigns can impact large scale events, such as the 2024 Olympics and global elections.

Recent events, including the attempted assassination of Presidential candidate Donald Trump, and the controversy surrounding Olympic athlete Imane Khalif, have brought to the forefront the impact of disinformation on discourse.

Developments in artificial intelligence (AI) have helped drive improvements in the output of malicious actors, increasing the plausibility and persuasiveness of misinformation and disinformation.

Information manipulation is not new however, with the advent and proliferation of social media, messages are easily amplified and disseminated at scale.

In addition, social media is increasingly consumed by a diverse audience of all ages, with information reaching a much broader cross section of the population. Combining large scale reach through digital channels with the advances in AI, lowers the barrier to entry for making credible content and can have increased influence.

As such, threat actors have the potential to create and disseminate false information to audiences more easily. For those wishing to influence current large-scale events, such as elections and the 2024 Paris Olympics, this provides ample opportunity.

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 3

July's Threat Hunt: DarkGate Remote Access Trojan

Summary

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

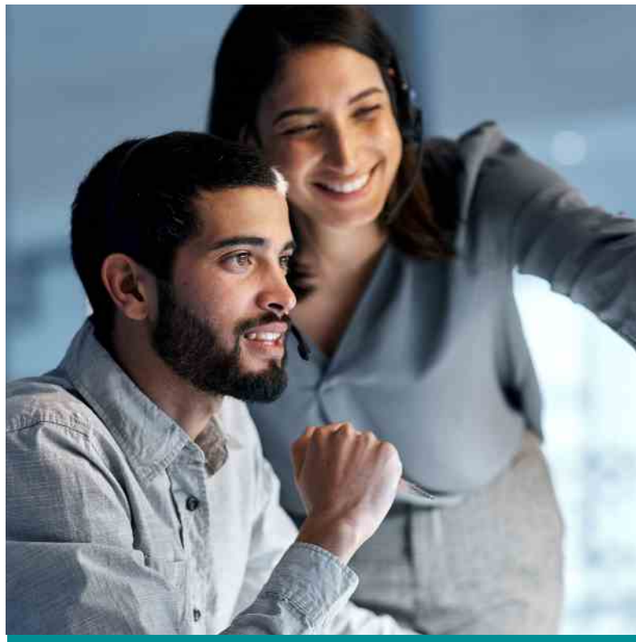
This allows us to leverage IoC-driven threat intelligence to fuel proactive detection on our customer's environments and subsequently remediate the threat.

These IoC's are queried against our Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM) and Network Monitoring clients, and in July, our focus was a DarkGate Remote Access Trojan (RAT) targeting multiple sectors around the globe

The Results

No detections were made by NCC Group's SOC team for DarkGate malware across any of our SIEMs, network, or EDR solutions. Ongoing monitoring of our clients' estates is a key part of helping to maintain strong security postures and ensure a swift response to any emerging threat.

For any queries about how our SOC, Threat Intelligence, or Online exposure Monitoring (OXM) services can help you, please contact your Account Manager/Service Delivery Manager who can assist you.



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 4

Threat Spotlight: Infostealer and Ransomware Blog

Is the apparent rise in infostealer malware usage among cybercriminals reflected in the ransomware landscape too?

Infostealers have been making headlines due to their role in harvesting valid corporate credentials, leading to significant data breaches.

The recent CrowdStrike incident, involving a content configuration update for the Falcon Sensor in Windows, which led to global IT outages, was exploited by threat actors using a false recovery repair manual to lure victims to install information stealing malware.

The use of infostealers has increased recently, this is unsurprising given that they reduce the burden on criminals wishing to gain access to organisations and their networks.

It is far easier, faster, and often cheaper, to use stolen valid credentials to access a network, than it is to find usable exploits and leverage these for initial access.

With the threat of ransomware continuing to dominate the cyber threat landscape, has the rise in the use of infostealers impacted how ransomware groups operate?

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.

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