
nccgroup
People powered tech-enabled cyber security
Monthly
Threat Pulse
Review of June 2024
FOX IT
part of nccgroup

Foreword:
The Year So Far

The cyber threat landscape in the first half of 2024 has been marked by a series of significant events that have had a profound impact on global cybersecurity.

We have seen major cyber incidents that have disrupted businesses, healthcare systems, and critical infrastructure across North America, Europe, and Asia Pacific region. These incidents have ranged from data breaches to aggressive ransomware attacks, highlighting the evolving nature of cyber threats and the increasing capabilities of cyber adversaries.

One of the most notable trends in 2024 has been the continued rise in ransomware, which has persistently been one of the top cybersecurity challenges for organisations across all industries. As such, International law enforcement agencies have intensified their collaborative efforts to combat cybercrime, leading to significant operations against ransomware groups such as:

- **Operation Cronos (February 2024)** specifically targeted the LockBit ransomware group, which had gained notoriety for its global attacks. This operation, spearheaded by the UK's National Crime Agency and the US FBI, resulted in the seizure of LockBit's technical infrastructure and the arrest of key figures within the group.

- **Operation Morpheus (June 2024)**, an initiative led by EUROPOL with partners across several nations, targeted the misuse of Cobalt Strike, a tool exploited by cybercriminals for ransomware deployment. This operation successfully disrupted nearly 600 IP addresses linked to illegal copies of the tool.

In April, the UK Department for Science, Innovation and Technology and the Home Office published the latest version of the Cyber security breaches survey.

Two key take homes from this report were that phishing remains the most prevalent attack vector, affecting 84% of businesses, with 50% of these businesses and 32% of charities reporting such incidents in the last 12 months. The figures are notably higher for medium businesses (70%), large businesses (74%), and high-income charities (66%).

In terms of the geographic origin of cyber threats, research from Oxford University in 2024 has compiled a Cybercrime Index, revealing a top 10 list of countries with the highest World Cybercrime Index (WCI) scores, with Russia, Ukraine, and China leading the list.

The healthcare sector has faced significant cyber threats in 2024, with a reported 280 incidents in the United States alone, this accounts for 24% of cyber events in the US this year.

Globally, healthcare IT infrastructure has been increasingly targeted, as seen with the ransomware attack on Synnovis, a pathology laboratory serving NHS organisations in South East London.

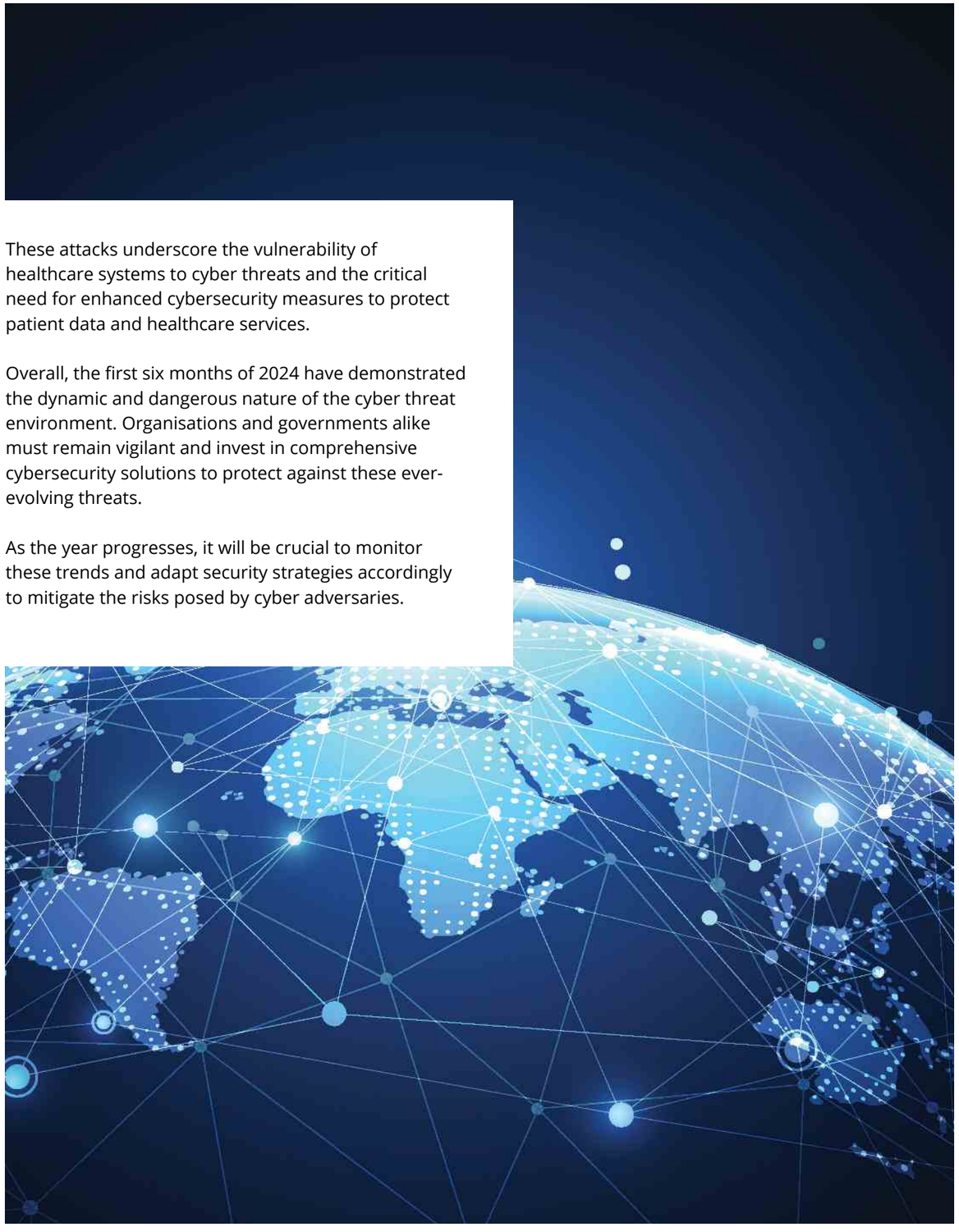
This incident led to a substantial reduction in the number of tests processed and reported back to clinical teams, causing over 800 planned operations and 700 outpatient appointments to be rearranged.

Another major IT provider for the NHS, Advanced, confirmed a ransomware attack that disrupted digital services like patient check-in and NHS 111, estimating a recovery time of three to four weeks.

These attacks underscore the vulnerability of healthcare systems to cyber threats and the critical need for enhanced cybersecurity measures to protect patient data and healthcare services.

Overall, the first six months of 2024 have demonstrated the dynamic and dangerous nature of the cyber threat environment. Organisations and governments alike must remain vigilant and invest in comprehensive cybersecurity solutions to protect against these ever-evolving threats.

As the year progresses, it will be crucial to monitor these trends and adapt security strategies accordingly to mitigate the risks posed by cyber adversaries.



Executive Summary

June's edition of the Threat Pulse produced by NCC Group's Global Threat Intelligence team explores several exciting and pertinent topics providing insights into the current threat landscape.

This month, we report on the continued threats posed by ransomware groups and a number of key changes to group activity. In addition, we discuss how AI can be used to enhance defences. We conclude our three part series on the threats posed by AI and provide details on how NCC Group's AI/ML Security Testing Offerings could be of assistance.

We also explore stealer malware focusing in on the Vidar stealer, and finish with an in-depth spotlight reviewing the threats posed by generic loaders within the threat landscape.

Analysis of ransomware attacks in June revealed that the attack method remains a severe threat to organisations globally, and that companies must continue to enforce mitigation measures. Perhaps the most interesting finding this month concerned the steep decline in LockBit 3.0 numbers, who have just 11 attacks in June. Instead, we observed Play rise to take first place, despite a relatively low victim count of 35.

Such a sharp decline in LockBit 3.0 activity could be the result of law enforcement's Operation Cronos in February finally starting to make an impact.

It remains to be seen whether we see another group step up into the dominant position or more equitable distribution of ransomware victims across the remaining active groups.

In our third instalment on AI, we discuss how advanced technologies can enhance cybersecurity defence measures, including vulnerability scanning, threat detection and threat management. Equally, we explore how NCC can support your defence with an AI-centric approach, including secure development lifecycle testing and AI/ML threat modelling.

As the world becomes increasingly technologically advanced, AI can support cyber defence efforts at a greater scale, with NCC Group offering several advanced solutions for organisations to take advantage of. Additionally, NCC Group's monthly investigations into prolific threats identified new analysis of the Vidar Stealer malware produced by CYFIRMA.

The research explains the associated tactics and techniques that characterise this malware, as well as the corresponding IoCs which can be employed for proactive detection to reinforce security efforts. NCC Group's SOC analysts assessed the risks posed by the malware to clients and identified no threat where connections to client infrastructure were identified.

Finally, this month's spotlight investigates prevalent loaders within the current threat landscape. Following Operation Endgame's success at reducing the number of larger loaders being exploited, NCC Group's Threat Intelligence analysts have investigated underground marketplaces to identify the next big thing.

Research suggests that smaller and more generic loaders alike should not be underestimated, as these can evolve into more popular payloads. We explore the anatomy of a generic loader, drawing on the Mofex loader as an example, as well as mitigation steps to ensure prevention.

Contents

Section 1

Ransomware Insights

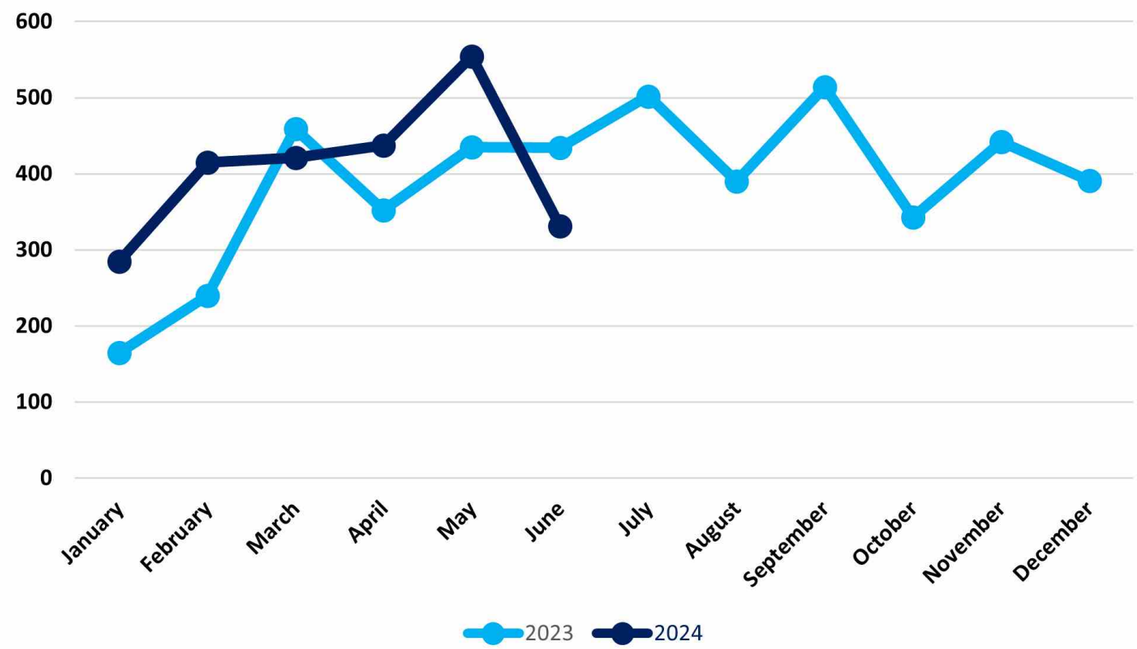


Figure 1: Ransomware Attacks Month-on-Month

In June, we observed a growth in cybercriminal activity away from the usual big players.

This could be due to several reasons including other groups seizing new opportunities, or bigger players becoming increasingly cautious due to increased international law enforcement efforts.

The dip from 554 attacks in May to 331 this month represents a significant decrease and is likely due to the steep decline in LockBit 3.0s attack numbers, who only had 11 attacks this month.

With this decline, the total number of attacks (331) sinks below the average number of attacks for the year (407) for the first time since January 2024.

In May, LockBit 3.0 was responsible for most ransomware attacks, however, in the same month the mastermind behind the group was identified as part of Operation Cronos and two members of the group were arrested.

There has been speculation that LockBit 3.0 has not actually managed to recover their full operation as a result and are reposting data from old victims to create an image of invulnerability to law enforcement efforts.

Play, on the other hand, reported the greatest number of attacks this month, rising from third place in May, which is the second time they have claimed this position this quarter, as they were also the most prominent ransomware group in April.

Their surge in activity appeared to begin in March of this year with 40 attacks, which put them in second place, so we may be beginning to witness a busy year for the group.

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

Intelligence Insights – AI: How Can We Help?

This month's Threat Pulse marks the conclusion of Q2's theme on AI for Intelligence Insights. We started off with a general introduction to the topic of AI, what it is and scratched the surface with some ways it can be used both offensively and defensively.

Last month we explored some ways defenders can mitigate the risks from AI-assisted attacks without having to rely on AI assistance themselves.

This month we'll be highlighting some of the ways which defenders can use AI to their advantage, and also look at how NCC utilises AI to help our clients, and offerings we have to assist in securing and optimising your own AI assisted tools.

There are many ways which cybersecurity professionals can use AI to assist them in their mission of defending digital estates. As highlighted in last month's Intelligence Insights, some of these methods are similar to how attackers use them with the only difference being the end goal.

One example of this is vulnerability scanning; by using AI-assisted tools to conduct vulnerability scans against your own organisation, it is possible to identify vulnerabilities which might have been targeted by an attacker, and proactively move to mitigate against the associated risk.

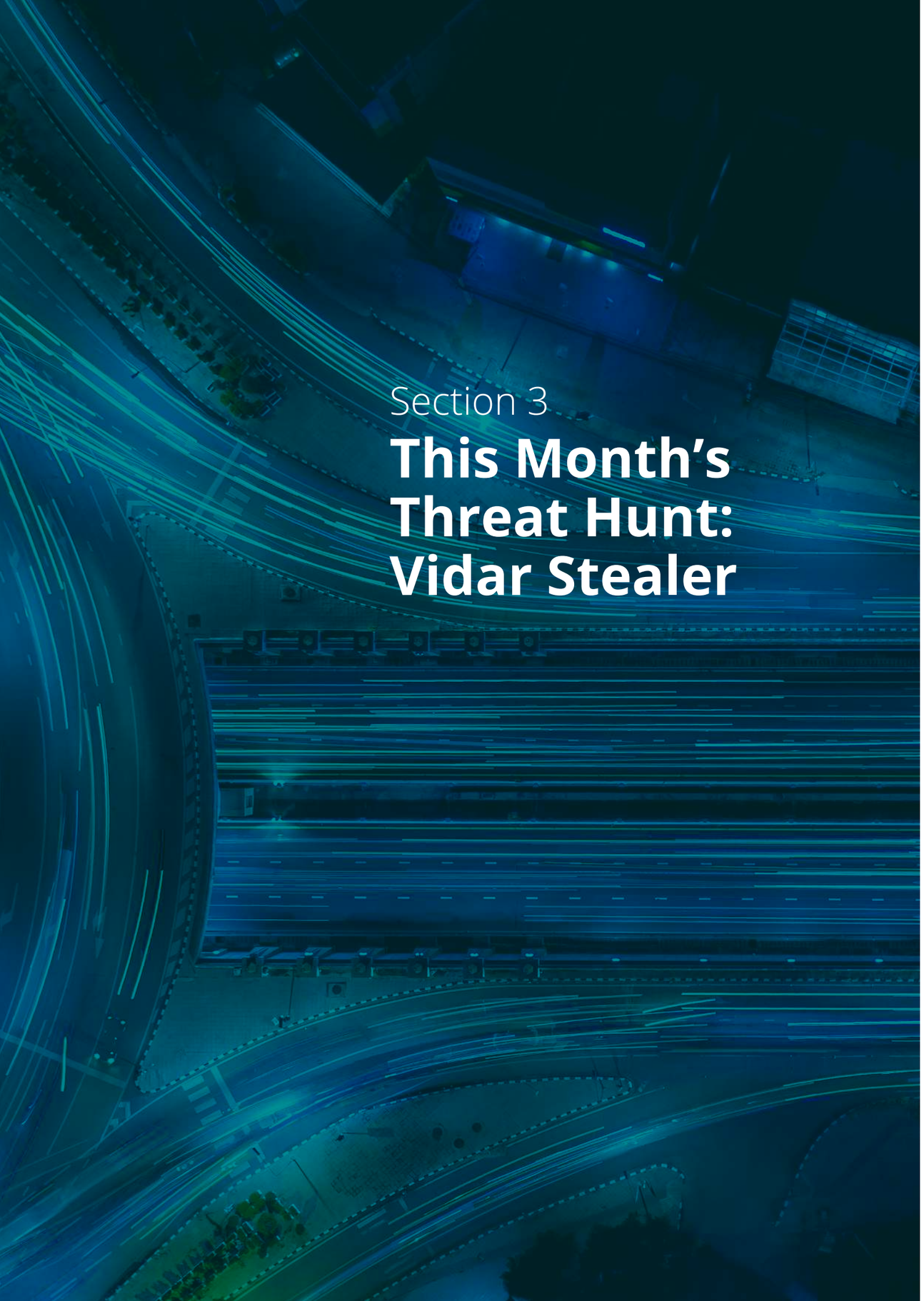
Burpgpt is a tool which helps with this, as it uses AI to "detect security vulnerabilities that traditional scanners might miss..."

NCC Group's AI/ML Security Testing Offering

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

This Month's Threat Hunt: Vidar Stealer

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 intelligence-led IoC threat hunting 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 IoC's gleaned from a new analysis of Vidar Stealer by CYFIRMA.

The Results

Our threat hunt did achieve some results for a number of IP addresses, especially for our Splunk and Defender service offerings, which were then fully investigated and raised to our clients.

However, as is commonplace with a majority of threat actors, common hosting infrastructure was used for Vidar Stealer in an effort to evade detection and increase the perception of legitimacy.

As a result, when a connection was made to any of our client's infrastructure, our SOC analysts assessed the risk of every associated domain to identify benign connections from malicious ones.

Thankfully, unlike previous threat hunts, the vast majority of these connections were concluded to be legitimate and of no threat to our clients.

Instances like this highlight the value of having in-seat analysts monitoring detailed network logs for managed cybersecurity services; reducing the frequency of false positives and increasing assurance that any true threats will be identified in a timely manner.

Organisations that are interested in replicating this threat hunt on their own estate should consult this report on Vidar Stealer produced by CYFIRMA.

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: In Droppers We Trust

As part of NCC Group's 2023 Annual Threat Monitor, we speculated and reported on the effect of Qakbot's takedown on a variety of loaders including Pikabot, Danabot, and DarkGate.

In that report we crowned Pikabot the favorite Qakbot replacement at the time, noting a considerable increase in detected IOCs relative to the other loaders included in the analysis. However, the loader landscape is vast, and the selection was non-exhaustive.

Now that Operation Endgame has dented some of the largest loader operations – including Pikabot – it's prudent to revisit the landscape now that threat actors will need to revisit their preferred underground marketplace to find the next tool to suit their needs.

Luckily for them, budding loader developers are plenty and the morale of cybercrime contributors seems to be largely unaffected by law enforcement efforts for now.

As we mentioned in NCC Group's March Threat Pulse, against the backdrop of the XSSWare competition, communities put in considerable effort to foster a collaborative and creative community.

Of course, not every project release is necessarily unique, though even small changes can be built upon which expands the menu for buyers while simultaneously lowering the barrier to entry by increasing competition.

Consequently, the secondary threat posed by the set of smaller (and often cheaper) projects should not be discounted in favor of focusing on the larger projects able to capture a significant user base.

These more generic loaders serve as a contrast against the more exclusive projects like DarkGate, Matanbuchus, or Pikabot. These loaders, often called private loaders due to their limited availability, have a different business model than more commercial loaders.

Limiting their customer base increases the chances of evading detection for longer. As part of this exclusivity, the price to be part of this small group of customers, often limited to less than 10, is much higher than those with a more commercial setup.

Let's explore the more generic formula followed by many of the more commercial offerings, followed by a case study using a recently published loader.

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