Monthly Threat Pulse

Review of April 2024

What's inside:

Ransomware Insights | Intelligence Insights: Introduction to AI | This Month's Threat Hunt - CVE-2024-3400 | Threat Spotlight

nccgroup.com

EXECUTIVE SUMMARY

This April edition of NCC Group's Threat Intelligence Team's monthly Threat Pulse report contains a summary of observed ransomware attacks around the globe, an introduction to Artificial Intelligence (AI) and the types of threats it can present as well as how it can be used to bolster security teams' defences, a threat hunt done in collaboration with NCC's Security Operations Centre (SOC), and finally a threat spotlight on a recently discovered and constantly evolving mobile malware written by the Strategic Intelligence Team.

The ransomware scene has managed to both match expected behaviours but also to buck expected trends. The scale of activity we have observed follows the pattern we saw in 2023; a slow start to the year in January, monthly increases for the rest of Q1, followed by a dip in activity in April.

Beyond that though, the scale of activity is still, in general, greater than it was last year as we expected to see, and which realistically we expect to see again next year. The Industrials and Consumer Cyclicals sectors were once again the first and second-most targeted sectors, while North America and Europe were, as expected, the two most targeted regions around the globe.

In a surprising turn of events however, LockBit 3.0 was not the most prominent threat group for the month and had fewer than half of the observed attacks they did in March. Instead, Play was the most active threat group, followed shortly after by Hunters.

Artificial Intelligence is an emerging set of technologies which has gripped the imagination of many. It has the ability to be used by cybercriminals and security teams alike and can either be responsible for a paradigm shift in the cyber threat landscape or be used simply as just another tool in the arsenal of malicious threat actors and defenders alike.

We have outlined some of the ways it can be used both for good and ill, and will be expanding on these in the next two issues of the monthly Threat Pulse; treating AI as a theme for Q2.

The threat hunt this month, in collaboration with NCC's SOC, focused on the exploitation of a CVSS 10.0 critical vulnerability (CVE-2024-3400), affecting the PAN-OS software found in Palo Alto Network Firewalls.

The malicious C2 IP identified by Palo Alto themselves was found to be the Indicator of Compromise (IoC) responsible for most hits against our EDR, SIEM, and Network Monitoring clients.

This IP address was first reported on the 9th of July 2023, and as recently as the 5th of May 2024, with activity picking up significantly in March which is when the exploitation of CVE-2024-3400 was first reported.

This implies that, not only was this IP first utilised for malicious activities within the last year, but that abuse is still taking place at the present.

The Threat Spotlight is research about Vultur Android malware conducted by our Tactical Intelligence Team. First spotted in March 2021, it was one of the first Android banking malware families to include screen recording capabilities and contains features such as keylogging and interacting with a victim's device screen.

Vultur mainly targets banking apps for keylogging and remote control. A more comprehensive look, including: an overview of the infection chain; execution flow; and an assessment of new features including obfuscation capabilities, can be found in the blog post.

CONTENTS

SECTION 01

RANSOMWARE INSIGHTS

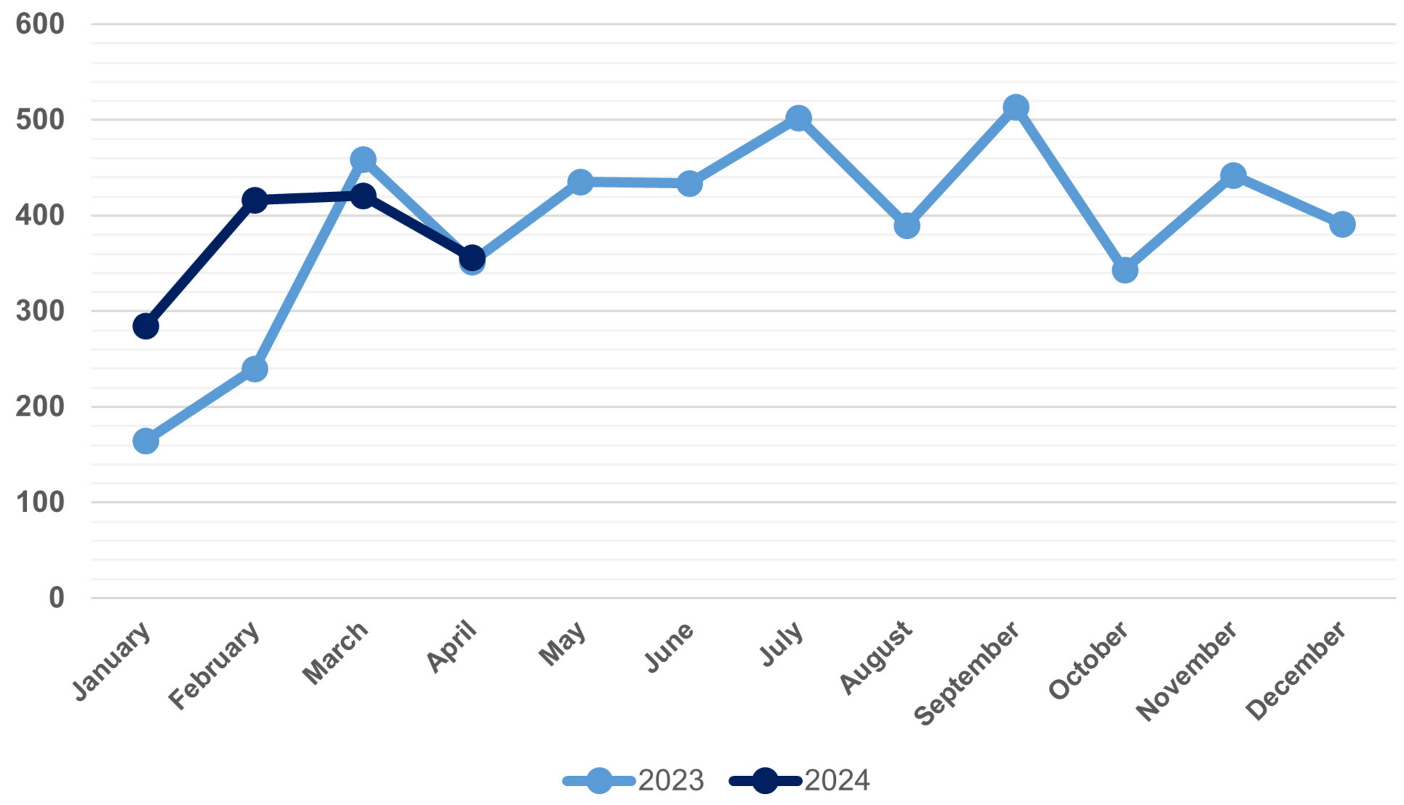

Figure 1: Global Ransomware Attacks by Month

As we can see from Figure 1 above, the ransomware scene is following roughly the same pattern in the first four months of 2024 as it did last year in 2023 with the notable difference being the scale of activity from threat groups being, in general, higher this year.

To demonstrate this point, looking at April specifically, observed attack numbers have grown from 229 when we first started tracking attacks in 2021, to 289 in 2022, then quite a massive increase of 22% up to 352 attacks in 2023, and now to 356 in April 2024.

Though March 2023 experienced more attacks than March 2024; 459 compared to 421, April 2023 experienced fewer than April 2024; 352 compared to 356. We expected higher numbers in April 2024 though these expectations have been dashed by the surprise “fall from grace” of the, up until now, most prominent ransomware threat group; LockBit 3.0. Their activity is examined in more detail in the Threat Actors section below. This is a trend we have noticed and expect to see continued, unless a more lucrative opportunity presents itself to OCG’s; each year, ransomware activity will be, on the whole, greater than in the year before.

As we continue into Q2 we can see a familiar pattern emerge; most established ransomware threat groups will commence the year with a relatively low level of activity. Part of the reason for this is that ransomware actors are human like the rest of us; they experience burnout, they have families, and crucially, they enjoy downtime during festive periods.

Additionally, as many cyber threat actors are located either in Russia or CIS nations, Orthodox Christmas is celebrated in January and not in December as it is in the West. After the frankly understandable, low levels of activity in January, most threat groups will increase their levels of activity throughout the year with most months being higher than the preceding one.

This is the rough pattern we expect to see for the rest of the year ahead, though obviously there can be fluctuations around this theme. By comparing ransomware activity month on month and year on year as in Figure 1 above, we are able to gain a holistic understanding of how the ransomware threat landscape continues to evolve.

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 Enhanced 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 02

INTELLIGENCE INSIGHTS: INTRODUCTION TO AI

Introduction

Artificial Intelligence has been the flavour of the month for quite a while now, and understandably so. Any time a new technology is developed or introduced; people wonder what it could be capable of, and AI is no different. It has the potential to be a paradigm shifting technology or simply another tool in the arsenal of both good and bad actors.

AI has been around in various forms for years now, though has exploded into the public consciousness through the introduction of generative tools like Chat GPT and CoPilot. Due to this public interest, uncertainty around what exactly AI is, and queries from our client base, NCC is using AI as a handy topic to introduce a new feature to our monthly Threat Pulse; the Theme.

AI will be examined in various details across the quarter, with this first edition being used as an introduction to the topic.

We will be examining:

- **What is AI?**
- **How can it be used by security teams to facilitate defensive measures?**
- **How can it be used by bad actors?**
- **Should you be worried about it?**

What is AI?

In its broadest sense, Artificial Intelligence is a form of computer science which develops methods for computers to execute tasks which are commonly associated with human intelligence such as analysing data, identifying patterns and behaviours, or making recommendations.

It is not a specific technology itself, but rather a set of technologies implemented within a system to enable it to display these behaviours.

security posture?

The great thing about AI, from a defender's perspective, is that as outlined above it isn't one specific technology which only does one specific thing.

Rather, it should be seen as a tool which can be used in a number of different ways to facilitate its wielder in achieving whatever their specific goals are.

How can AI be used maliciously?

Just as security teams and other benevolent actors can use AI to facilitate working at a faster pace than humans are capable of, or as a tool to greatly increase the available resources to a team with limited resources of skilled human workers, malicious actors can also use AI in such a way.

It can be used in a "fire and forget" manner for the management of bots, for example. Management of the botnet can be relegated to the AI tool, freeing up the human threat actor to dedicate their time to other activities such as engaging in social engineering.

Should you be worried about AI?

AI is a tool much like any other; it can be used both for good or maliciously depending on the motives of who wields it.

Just as a tool such as search engines or network/vulnerability scanners can be used by security researchers to help find resources to enable them to strengthen their defences but also by threat actors looking to find exposed documents or unsecure networks, AI can be used to facilitate securing defences, helping customers find an answer or resolution to an issue, or help a threat actor craft a more convincing phishing email, facilitate writing malware packages and enable malicious network scanning, or almost anything else that can be thought of.

Figure 2: An AI's visualisation of AI defending a network

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 03

THIS MONTH'S THREAT HUNT - CVE-2024-3400

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 customers' infrastructure.

This allows us to leverage both behavioural and IoC-driven threat hunting techniques 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 the exploitation of a CVSS 10.0 critical vulnerability (CVE-2024-3400), affecting the PAN-OS software found in Palo Alto Network Firewalls.

The Results

Across all of our services, our hunt produced hits for 22% of our clients, the vast majority of which were triggered for the malicious IP address 66[.]235[.]168[.]222 which was labelled as command & control (C2) infrastructure by Palo Alto themselves.

Our Network Monitoring services saw results for 18% of the client base, for the same IP address, highlighting its prolific use by the threat actor.

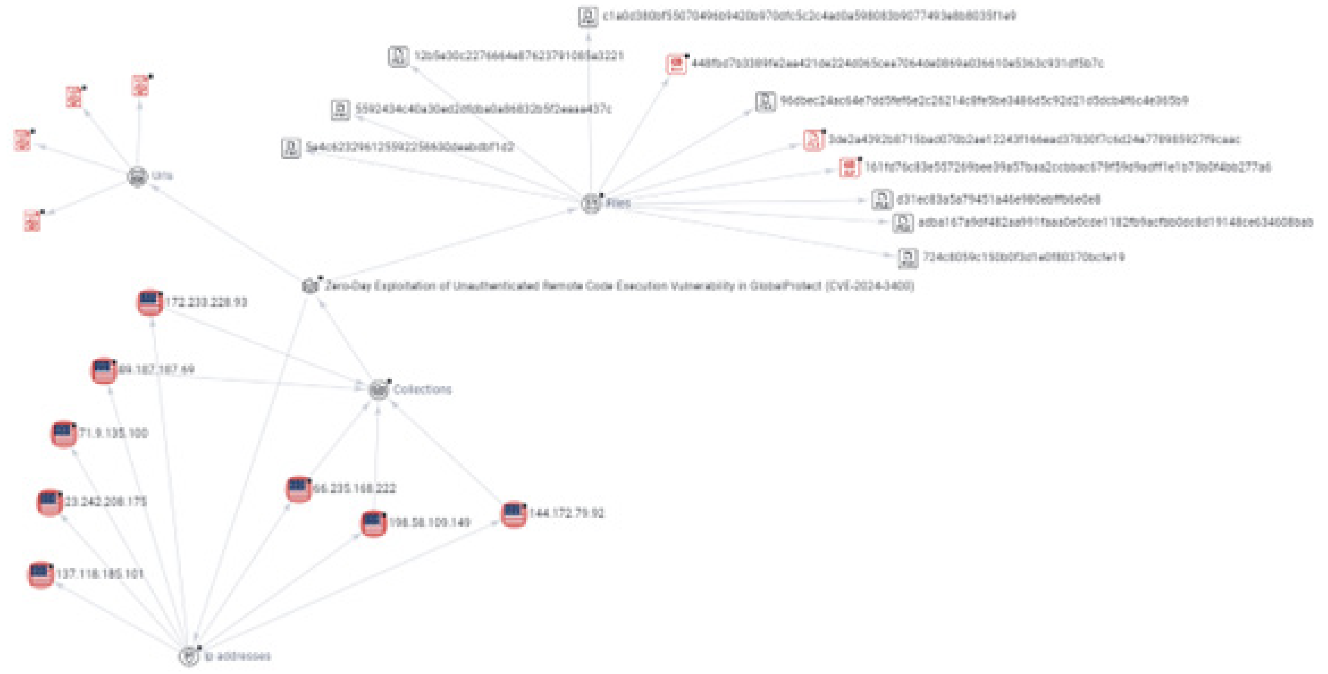

Figure 3: Plotted Graph of findings

MDR and XDR services

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 04

THREAT SPOTLIGHT

Our Tactical Threat Intelligence Team at Fox-IT, part of NCC Group, has released an in-depth breakdown of some newly found technical features inside Vultur- a nefarious Android banking malware.

It was one of the first Android banking malware families to include screen recording capabilities and contains features such as keylogging and interacting with a victim's device screen.

Vultur mainly targets banking apps for keylogging and remote control. ThreatFabric first discovered Vultur in late March 2021.

The authors behind Vultur have now been spotted adding new technical features, which allow the malware operator to further interact with the victim's mobile device remotely.

Vultur has also started masquerading more of its malicious activity by encrypting its Command-and-Control server (C2) communication, using multiple encrypted payloads that are then decrypted on the fly, and using the guise of legitimate applications to carry out its malicious actions.

Back in 2021, Vultur (ab)used legitimate software products, AlphaVNC and ngrok, to provide remote access to the VNC server running on the victim's device. Vultur was distributed through a dropper framework called Brunhilda, responsible for hosting malicious applications on the Google Play Store.

In a recent campaign, the Brunhilda dropper was spread in a hybrid attack using both SMS and phone calls.

The first SMS message guides the victim to a phone call. When the victim calls the number, the fraudster provides the victim with a second SMS that includes the link to the dropper: a modified version of the McAfee Security app.

The dropper deploys an updated version of Vultur banking malware through three payloads, where the final two Vultur payloads effectively work together by invoking each other's functionality. The payloads are installed when the infected device has successfully registered with the Brunhilda C2 server.

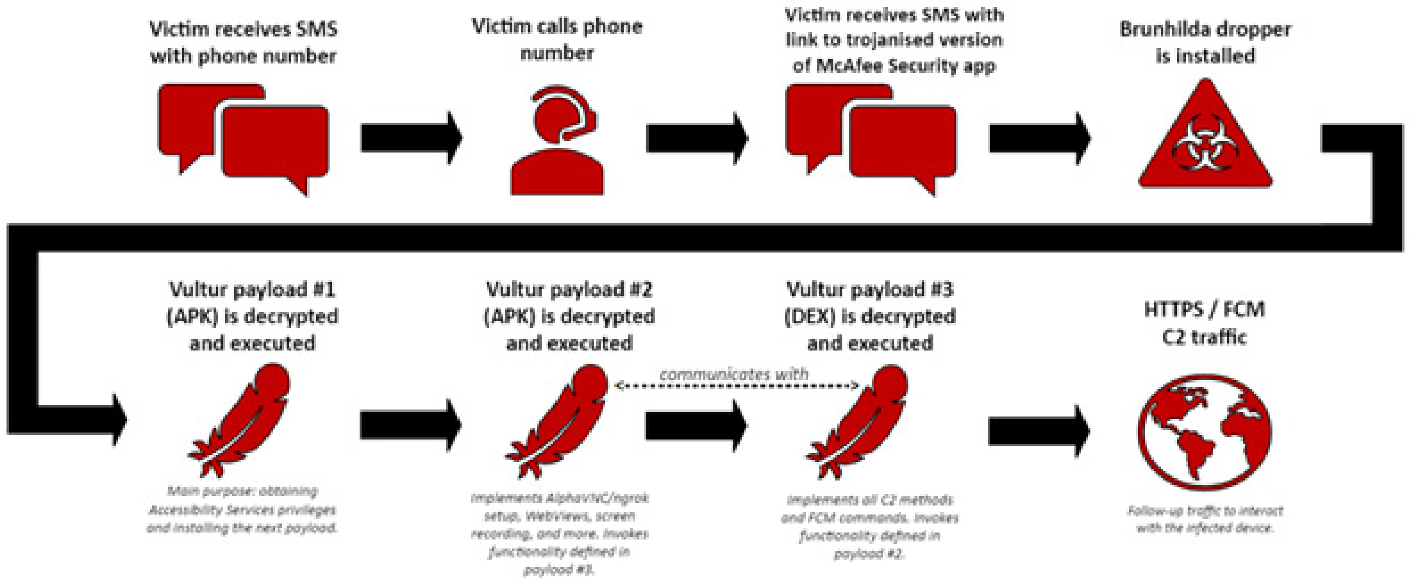
Victim receives SMS with phone number
Victim calls phone number
Victim receives SMS with link to trojanised version of McAfee Security app
Brunhilda dropper is installed
Vultur payload #1 (APK) is decrypted and executed
Vultur payload #2 (APK) is decrypted and executed
Vultur payload #3 (DEX) is decrypted and executed
HTTPS / FCM C2 traffic
communicates with
Main purpose: obtaining Accessibility Services privileges and installing the next payload.
Implements AlphaVNC/ngrok setup, WebViews, screen recording, and more. Invokes functionality defined in payload #3.
Implements all C2 methods and FCM commands. Invokes functionality defined in payload #2.
Follow-up traffic to interact with the infected device.

Figure 4: Visualisation of the complete infection chain. Note: communication with the C2 server occurs during every malware stage

In the latest version of Vultur, the threat actors have added seven new C2 methods and forty-one new Firebase Cloud Messaging (FCM) commands.

Most of the added commands are related to remote access functionality using Android's Accessibility Services, allowing the malware operator to remotely interact with the victim's screen in a way that is more flexible compared to the use of AlphaVNC and ngrok.

Consult the full blog post for a comprehensive analysis of Vultur, beginning with an overview of its infection chain, followed by a deep dive into its new features, uncovering its obfuscation techniques and evasion methods, and examining its execution flow.

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
response@nccgroup.com
www.nccgroup.com

Interested in our premium reports? Click here