Monthly Threat Pulse

Review of February 2024

nccgroup.com

INTRODUCTION

Welcome to NCC Group's monthly Threat Pulse Review, bringing you exclusive insight into the latest Threat Intelligence, updates on recent and emerging advances in the threat landscape and a deep understanding of the latest Tactics, Techniques and Procedures (TTPs) of threat actors.

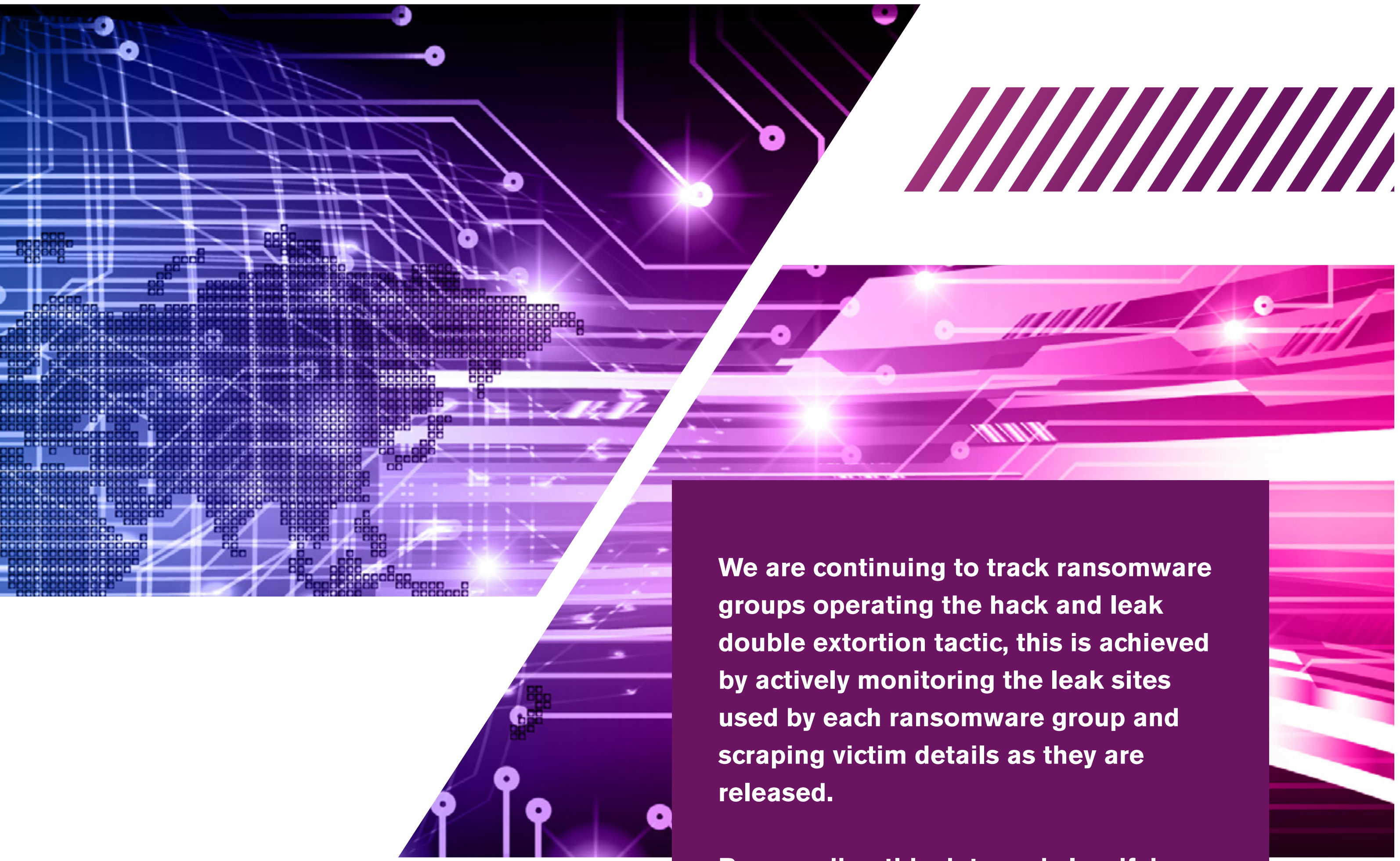
Let us keep watch over the cyber and geopolitical landscape so you don't have to.

Take a look at our Cyber Threat Intelligence webpage to view all our previous reports and subscribe to our monthly highlights webinar.

CONTENTS

SECTION 01

RANSOMWARE TRACKING



We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

By recording this data and classifying the victims by sector, we are able to derive additional insights such as, which sectors are being targeted this last month, and how do these insights compare to previous months?

Analyst Comments

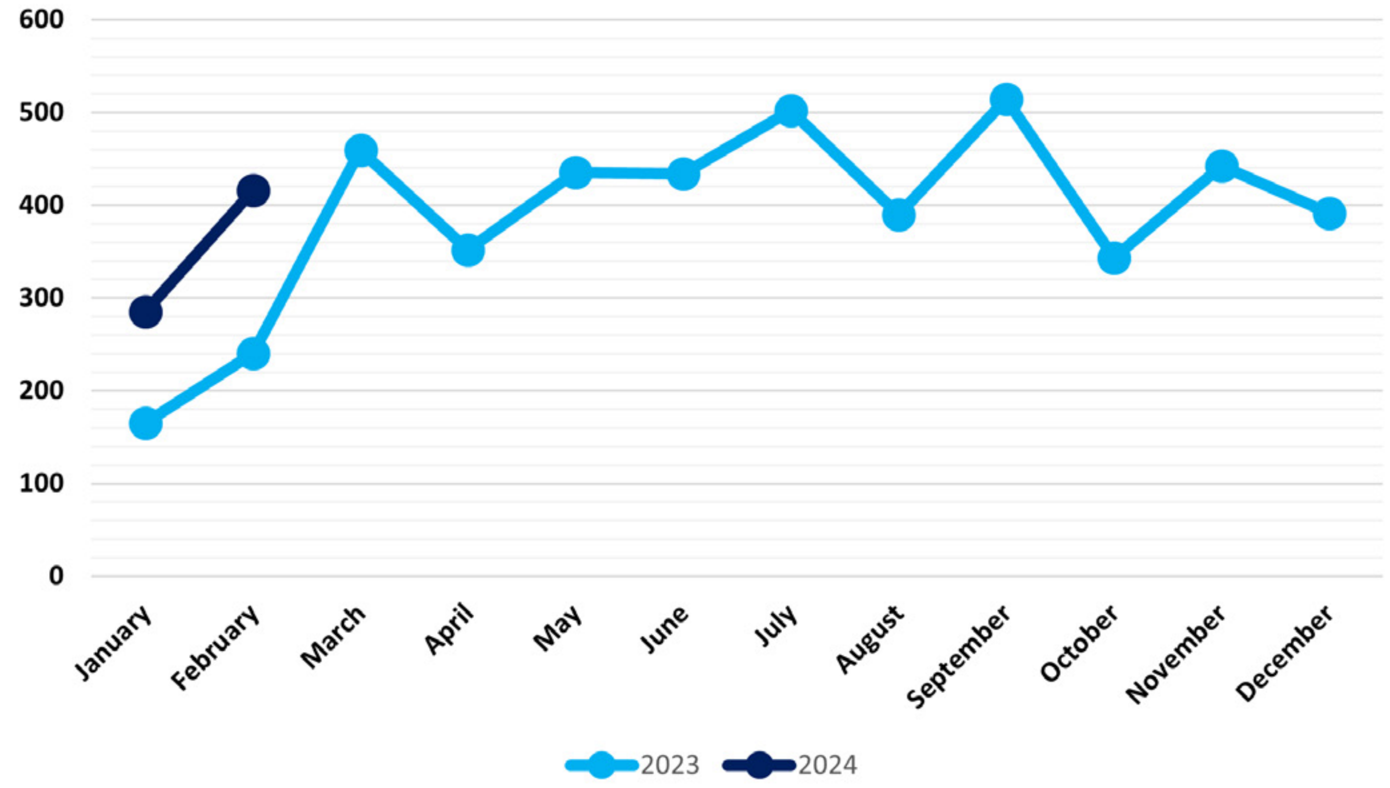


Figure 1: Global Ransomware Attacks by Month

Observed ransomware attacks have, as is to be expected, increased significantly from January 2024 to February 2024 from 285 to 416 cases, marking a 46% increase month on month which is once again the highest figure that we have witnessed in February (73% higher than February 2023).

This pattern has persisted for as long as NCC Group has been tracking hack & leak ransomware groups, so it is not expected to change in the near future; threat groups exhibit a seasonal lull around Christmas and the New Year, and subsequently return to their normal operations in February.

If 2024 is to follow the same pattern as 2023, we can expect a further increase going into March as we start to reach the baseline for 2024's ransomware activity, which will likely consistently surpass that of 2023 based on previous trends.

Something of note that will be explored in the Threat Actors section of this report is that we have quite a mix of top threat actors this month (excluding the usual LockBit 3.0) with Hunters and Qilin pushing their way into the top 3.

Perhaps this implies a change in the most active threat actors for 2024? Either way, NCC Group will continue to track the activity of hack & leak ransomware groups.

SECTION 02

SECTORS

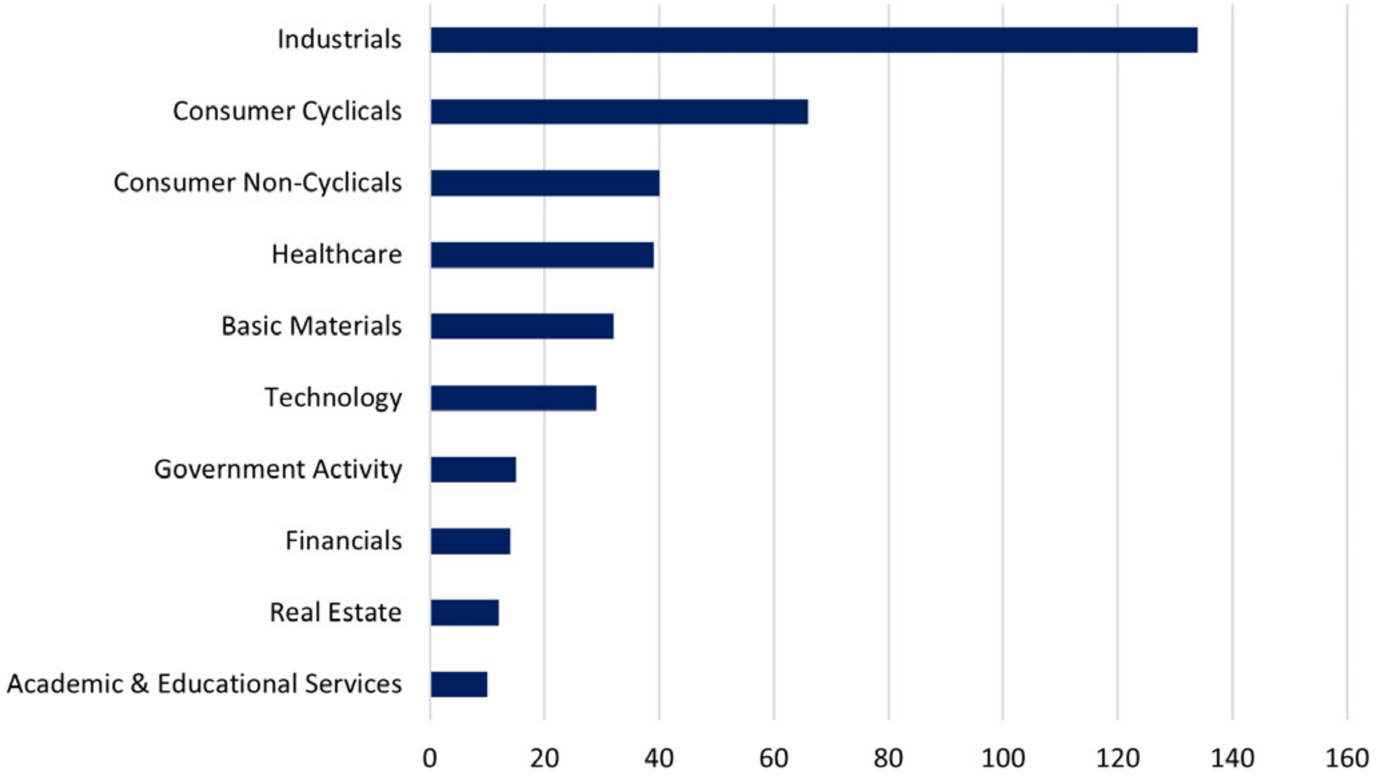


Figure 2: Top 10 Sectors Targeted February 2024

February's ransomware targeting by sector continued to see Industrials domineer the landscape with 134 ransomware attacks occurring in the sector, accounting for 32% of the attacks observed in February.

When compared to January there was a significant increase from 96 by 40% which replicates the increasing trend seen in 2023. The trend in 2023 saw January have a seasonal dip and a revival in the proceeding February increasing by 63%.

This trend has been observed again in 2024 but down proportionally 23% year on year (YoY). Whilst the month on month percentage increase was less than last year; the YoY for February saw an additional 54 attacks meaning an increase of 68%.

Although, February saw the Technology sector drop out of the top 3 and move three positions to number 6, it wasn't due to a decrease in ransomware attacks. In fact, the Technology sector saw a total of 29 attacks in February, a nearly 4% (+1) increase compared with a month earlier (28).

The Technology Sector accounted for 7% observed in the month of February. The largest decrease in attacks came in the Academic & Educational Services sector where they saw a decline month on month by 41% from 17 attacks in January to 10 in February (-7).

This sector also saw their position in the list drop three positions to 10 and accounted for 2% of observed attacks in the month.

Government Activity enters the top 10 at position 7 in the list for the first time in 2024, accounting for nearly 4% (15) of the total ransomware attacks observed. This is an increase month on month by 400% (+12) when compared with 3 attacks in January 2024.

Government Activity replaces Institutions, Associations & Organisations in the list who saw the activity in their sector decrease by just under 29% month on month to 10 ransomware attacks in February 2024 causing them to lose their position in NCC Group's top 10 only accounting for 2% of attacks.

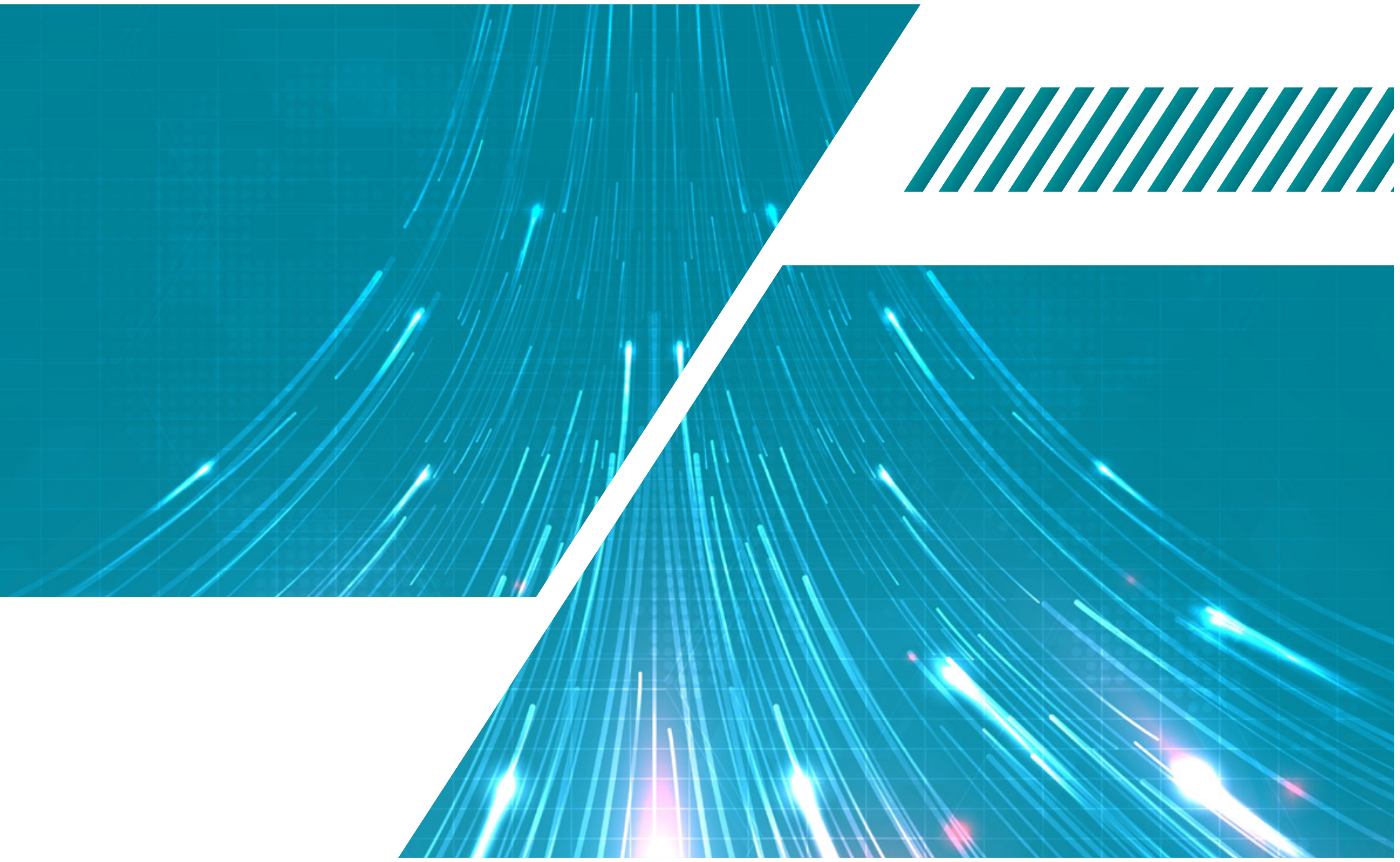
It is noteworthy that Consumer Non-Cyclicals are up two positions in February attributed to their increase in attacks by 135% (40) and account for 10% of the total activity observed in the month.

Additionally, Basic Materials, Financials, and Real Estate all saw their position change to move up the list by one position each respectively.

Month on month Basic Materials saw an increase of 88% to 32 attacks, Financials an increase of 27% to 14 and Real Estate an increase of 50% to 12 attacks. The three sectors accounted for a combined 14% of observed attacks.

SECTION 03

THREAT ACTORS



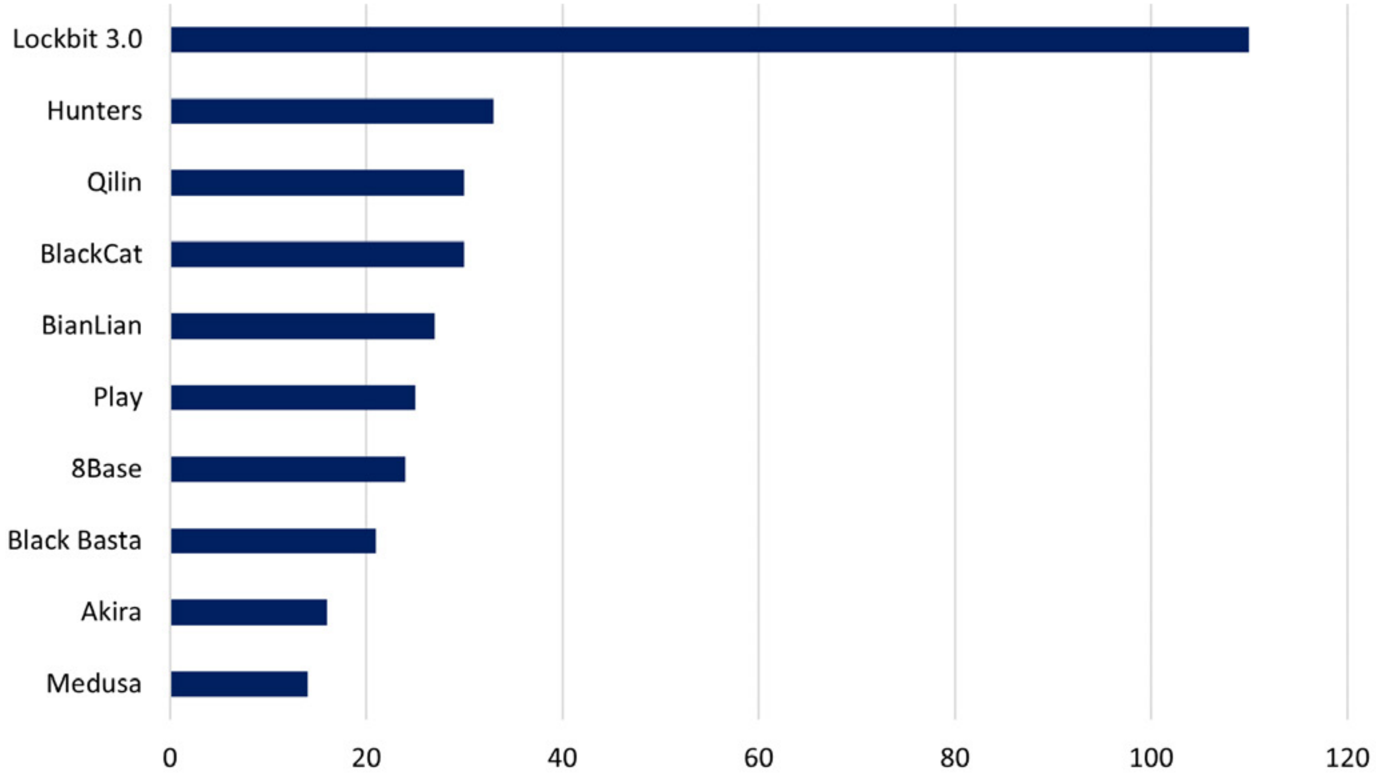


Figure 3: Top 10 Threat Actors February 2024

February was quite the standout month for ransomware. Not only because of the scale of activity, 46% higher than January 2024 and 73% higher than February 2023, but also because of the shift in Threat Actor activity levels as well as multiple notable events which have the potential to significantly shake up the ransomware threat landscape.

Continuing their 7-month reign, LockBit 3.0 is once again the most active group for February with 110 credited attacks to their name.

This is nearly double the 64 attacks they were credited with in January, and significantly higher than the total month on month percentage increase from January, at a 72% increase.

Dwarfed by LockBit's activity, and yet the second most active threat group for the month, comes Hunters, with 33 attacks to their name.

Though Hunters have appeared in the list of ten most-active monthly threat groups before, this is the first time they have been in the top three.

Next, as joint 4th most-active groups, come Qilin and BlackCat with 30 attacks apiece. Though BlackCat is accustomed to being included in the most active monthly threat groups, Qilin, like Hunters, is relatively new to these levels of activity.

It is perhaps a bit early in the year to predict what levels of activity we are likely to see from them in the future, it is worth noting a shift in the usual actors we see following behind LockBit.

As we have analysed BlackCat's activity on numerous prior occasions when they were amongst the most active ransomware threat groups, we will not include an analysis of their activity in this report but rather will focus on Qilin instead.

In addition to shaping the ransomware landscape through their overwhelming presence and activity levels, LockBit also promises to impact the ransomware scene through its losses as well as its wins.

The UK's National Crime Agency (NCA) alongside the US' FBI and supported by law enforcement agencies from 9 other nations succeeded in taking down LockBit's primary administration environment and seizing their site on 20 February as part of Operation Cronos.

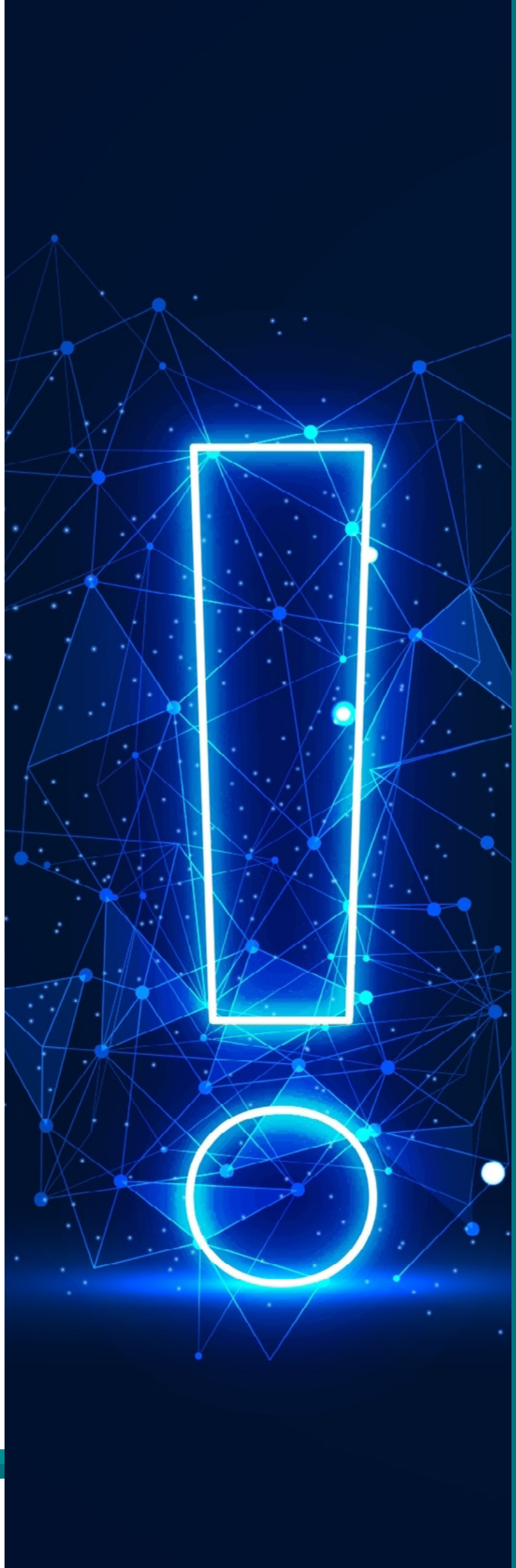
The NCA also claimed to have accessed LockBit's source code, though the group themselves have disputed this. Despite this set back, LockBit were back up and running on new infrastructure less than one week later.

However, once tarred with the brush of law enforcement intervention, it is hard for a cyber threat group to operate as before as they are, naturally, treated with suspicion by other players in the game.

Though law enforcement intervention is not uncommon, a group the size and notoriety of LockBit being impacted has a knock-on effect on the rest of the landscape.

The level of attention which LockBit has brought to ransomware operators in general through their prolific activity, and now more specifically through this law enforcement intervention, may have served to put the wind up some of LockBit's peers.

It is entirely possible that the near future will witness a schism amongst ransomware operators and other malicious threat actors and the forums on which they're active, and affiliates of LockBit's may move to other providers in an attempt to distance themselves from the potential of being caught up in whatever law enforcement does next in retaliation to LockBit's establishing of new infrastructure.



SECTION 05

REGIONS

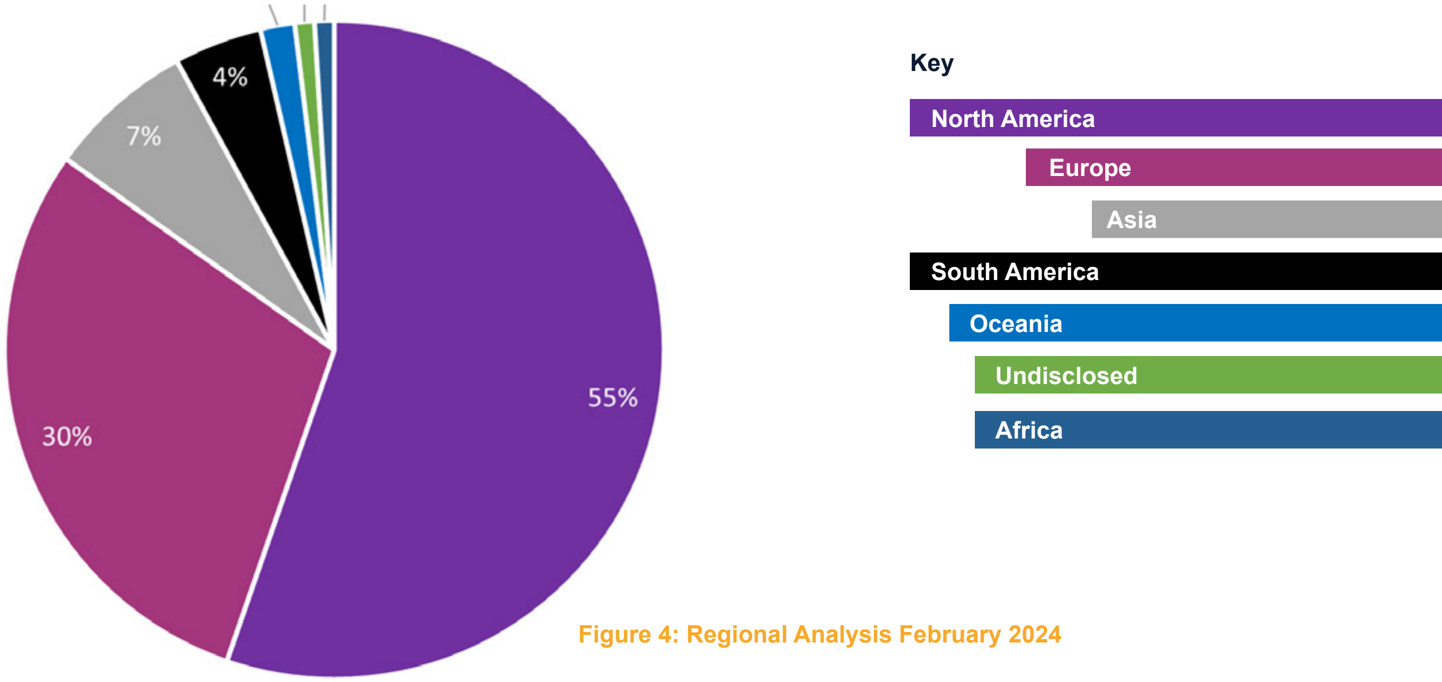


Figure 4: Regional Analysis February 2024

In February 2024 North America continues to contribute a vast majority to the total ransomware cases with 230 of the 416, and is already the second time in 2024 where it has accounted for more than 50% of all attacks, which was only the case 4 times in 2023 and only to a narrow degree.

Europe accounted for 123 attacks in total for February 2024

Europe accounted for 123 attacks in total for February 2024 which is still a 64% increase on January's total of 75, as well as a 4% proportional increase.

This means that as a unit Europe and North America accounted for 85% of all attacks in February 2024, which is identical to January where they also accounted for 85%; a feat that wasn't achieved once in 2023.

For the remaining 15% we have Asia with 30 attacks, South America with 18, Oceania with 7, and finally Africa and Undisclosed with just 4 victims each.

This is mostly consistent with last month with just 1% differences between some of the regions, showing that this particular focus on North America and Europe is possibly a shift in the threat landscape for 2024.

Further corroborating this statement, when compared with February 2023, North America and Europe exhibited huge 102% and 120% increases respectively, while the remaining regions all experienced decreases (excluding South America which saw a 38% increase).

Based on the data presented to us in the past two months, NCC Group expect North America and Europe to maintain their positions of most popular ransomware targets in March.

SECTION 06

THREAT SPOTLIGHT: RAASCYCLING

The end of February was taken by storm by Operation Cronos, the recent valiant addition to law enforcement efforts in combatting global digitally enabled crime that attempted to interfere with the operations of Lockbit group.

Following suit, the last day of February flowing into beginning of March was marked by another ransomware group, ALPHV (also known as Blackcat), who has exited the scene with the grace of a runaway bus after pulling off an exit scam under the guise of being disrupted by the FBI.

Despite the big ransomware game hunting, smaller threat actors within the same cybercriminal space seem undeterred and, on the contrary – motivated.

Although we are only two months into the year 2024, we have already been dubiously blessed by seeing more than 10 new groups and providers of different flavors forming.

Out of these, 6 have been advertised on a primarily Russian forum that specifically markets itself as a safe haven for all ransomware related activities, including networking between initial access brokers who support the ransom business.

This month's Spotlight will delve into the politics and culture of ransomware groups.
Of course, keep in mind that in the world of malware, most new things are not truly new.

Like criminal methods and techniques, reworked versions of old software with a new twist circulate underground due to leaks or sharing and will inevitably be picked up by a more (or less) creative group or individual actor.

Most infostealers can trace their lineage to specific families. Even platforms for networking and forum teams are subject to the same change.

These often bring some sort of fresh breath of activity to the previously developed solutions or use them as building blocks for something new.

The dynamic of these developments is an important tool for research, and so old groups re-assembling, new groups building on top of older malware versions, or old groups re-grouping – these all would still qualify as new developments.

FOX IT
part of nccgroup

nccgroup

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