



Threat Intelligence Report

January 2024




INTRODUCTION



Welcome to NCC Group's monthly Cyber Threat Intelligence Report, 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 1
Ransomware Tracking.....4



SECTION 2
Sectors.....6



SECTION 3
Threat Actors.....10



SECTION 4
Regions.....12



SECTION 5
Threat Spotlight: Hydradynamics.....14

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

Observed ransomware attacks have fallen from 391 in December 2023 to 285 in January 2024.

This is a pattern we have come to expect as it was observed previously from December 2021 to January 2022, and also from 2022 to 2023.

Despite this month-to-month reduction, attack numbers this January are higher than they have ever been seen before; a full 73% higher than the 165 witnessed in January 2023, and 138% higher than January 2022.

2023 was an explosion in ransomware activity, both with regards to raw numbers of attacks as well as by introducing new threat actor groups.

Though the January-to-January increase in attack numbers is slightly lower than the 2022-to-2023 numbers, they are still the highest yet witnessed and a likely indication that the ransomware threat landscape will only continue to expand in scale and develop in maturity as 2024 continues.

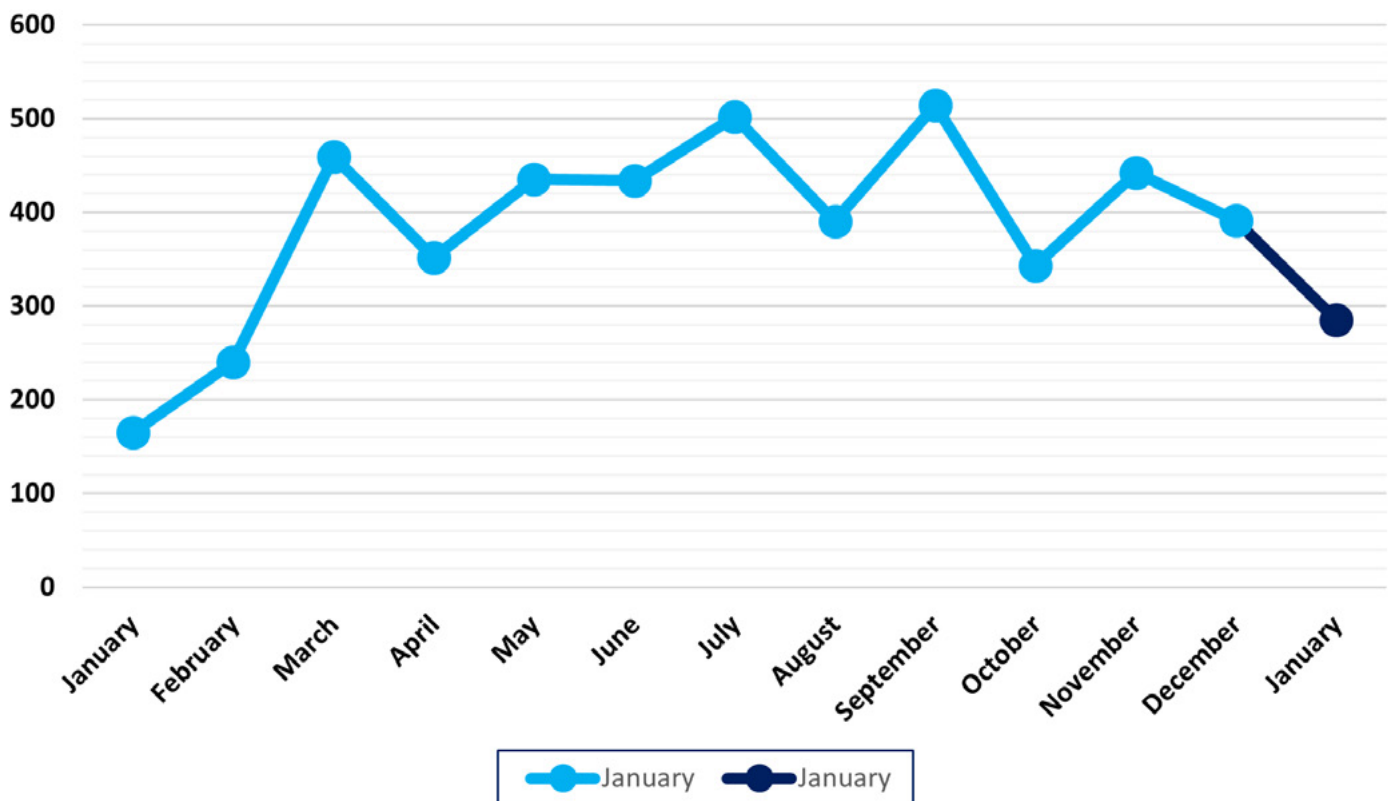


Figure 1: Global Ransomware Attacks by Month

SECTION 02

SECTORS



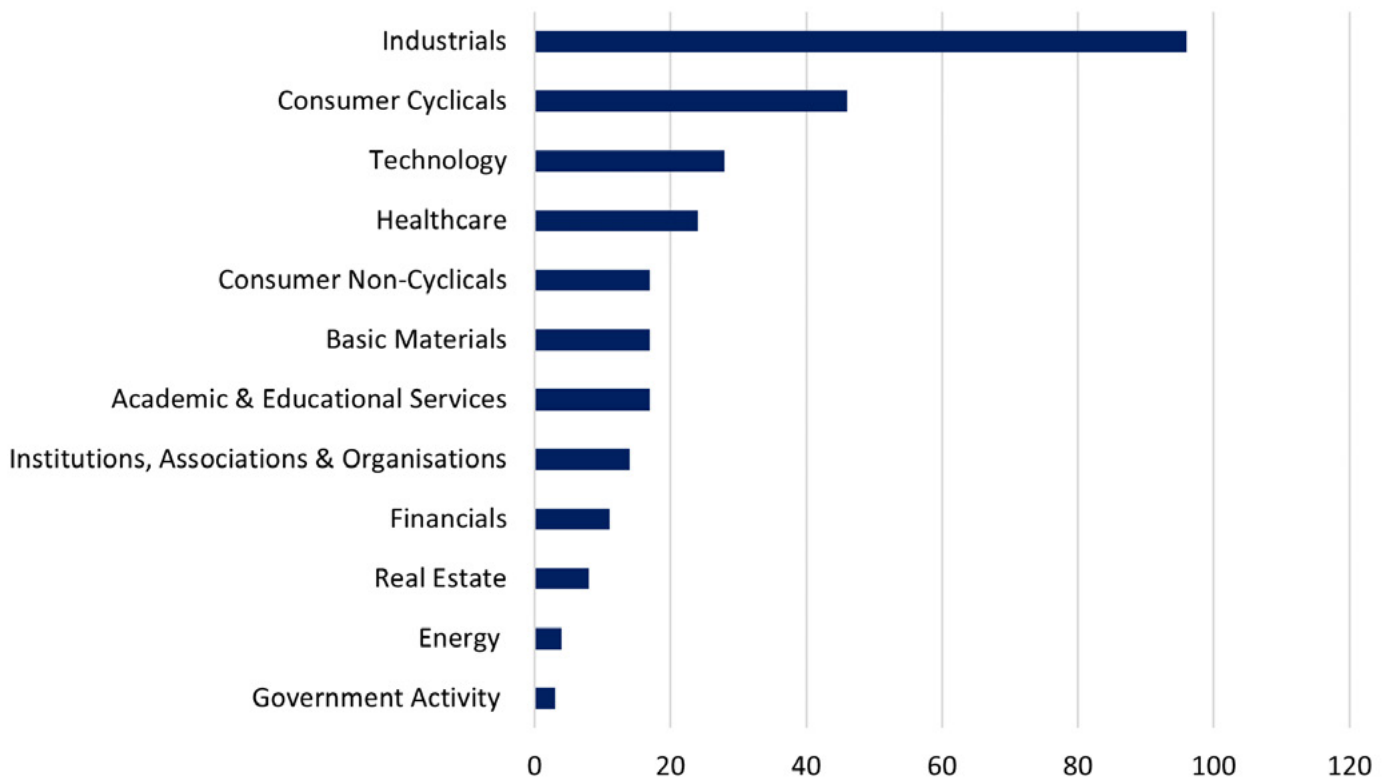


Figure 2: Top 10 Sectors Targeted January 2024

January’s top 4 sectors attracting ransomware attacks replicate those from December 2023, with Industrials dominating the landscape. Industrials account for 34% (96) of the 285 attacks seen this month.

This is a fall in numbers of 16% from the 114 attacks noted in December, a seasonal dip at the start of the year which replicates the findings from December 2022 to January 2023.

Of note is that compared with January 2023, attack numbers (49) against the Industrials sector, this year has started with a significantly higher volume of attacks (96), representing a 96% uplift year on year.

Consumer Cyclical came in significantly lower in the second spot, with 16% (46) of the total this month, and a decrease of 28% by December’s figure of 64.

As with other sectors, whilst remaining in the same relative 2nd position, the year-on-year figure has seen a significant rise, with an 84% increase on the 25 attacks seen in January 2023.

The Technology sector accounted for 10% (28) of those attacks counted in January and was down 40% compared to December’s 47.

In January 2023, the Technology sector ranked in 4th position, after Academic & Educational Services, with 9% (15) of all attacks that month, therefore maintaining its relative share this month, although in total numbers there is an increase of 87% compared with January 2024.

Whilst the Healthcare sector retains its position as 4th in the top 10, there is a significant fall of 47%, with 24 attacks compared with the 45 attacks attributed to the Healthcare sector in December 2023.

Having said that, this sector remains an important target and attack numbers are very close to those for the Technology sector.

The shape of the top 10 sectors outside of the top 4 has seen some changes in their relative position, although it is worth noting that Institutions, Associations & Organisations has moved into 6th place, after falling outside the 10 in December 2023.

Government Activity related attacks have fallen by 81%, from 16 in December to 3 in January, representing 4% and 1% of all attacks in respectively.

These top 10 encompass all sectors, which goes to highlight that all sectors are vulnerable and attractive targets, and that organisations of all types should make strengthening their cyber defences a priority.





SECTION 03

THREAT ACTORS



In January, we observe a total of 285 attacks representing a decrease of 27% when compared with December's figure (391).

However, looking back to January 2023, we actually observe an increase of 73% from 165 attacks recorded at the time, which signifies the growth of the threat landscape year-on-year.

We have a very different top three this month compared to the previous months with the exception of LockBit maintaining their prime spot as the most prominent threat actor. In second and third positions, however, we observe 8Base and Akira who were in fourth and eight positions in December respectively.

It is worth noting that out of all newcomers in 2023, these two groups regularly appeared within the top ten and might be the ones to watch closely in 2024. The top three are responsible for 41% (118) of the monthly output and further details regarding their activity are available on the following pages.

Next, we notice that BlackCat dropped from third in December to fourth in January with 8% (22) while Hunters dropped from fifth to seventh with 5% (14) of the monthly output.

We also observe the following decrease in these groups' activity; BlackCat shows a decrease of 21% (from 28) while Hunters' activity is down by 36% (from 22) likely due to the overall decrease in the attack volume this month.

Black Basta, BianLian and Medusa are in fifth, sixth and eighth positions with 7% (19), 6% (17) and 5% (13) respectively, however, none of these groups were part of the top ten in December.

Qilin, INC Ransom and Trigona share the ninth position with 3% (9) each and finally, BlackSuit is tenth with 1% (4).

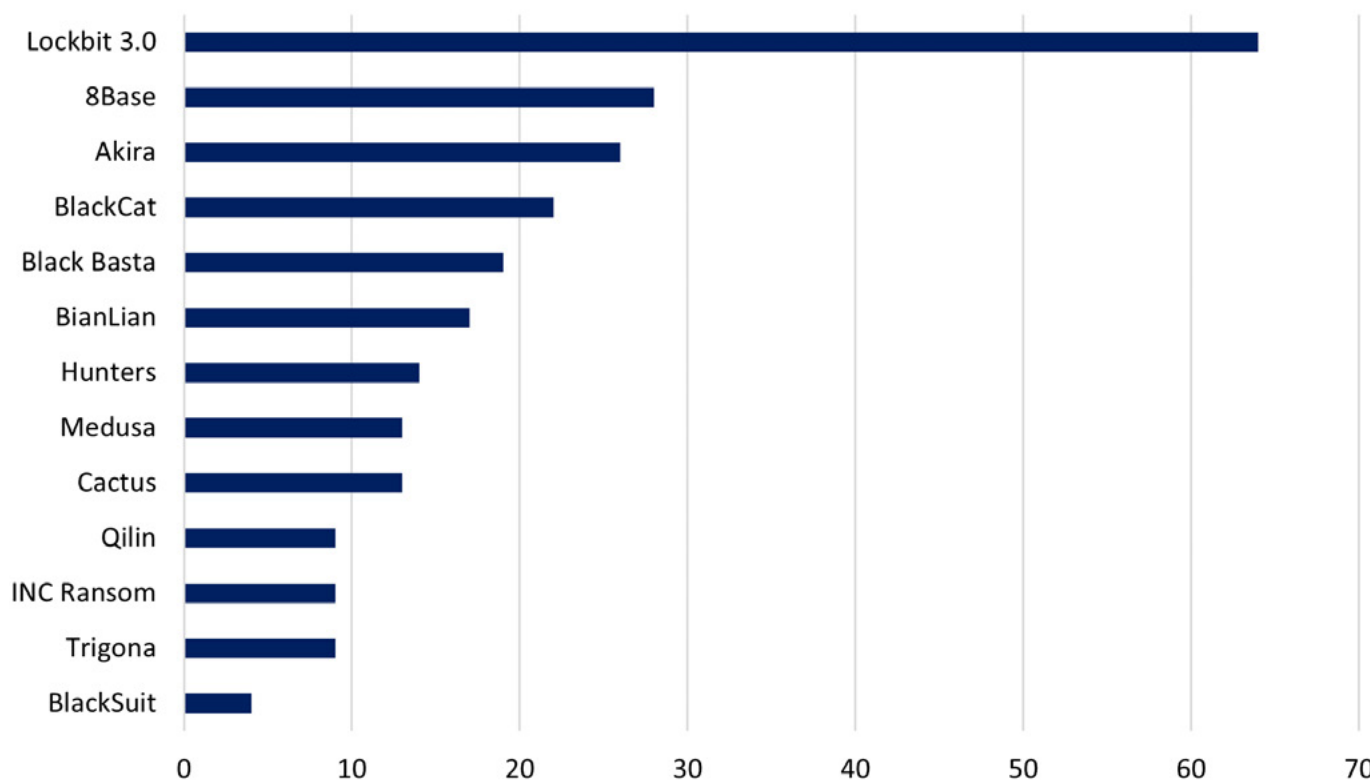
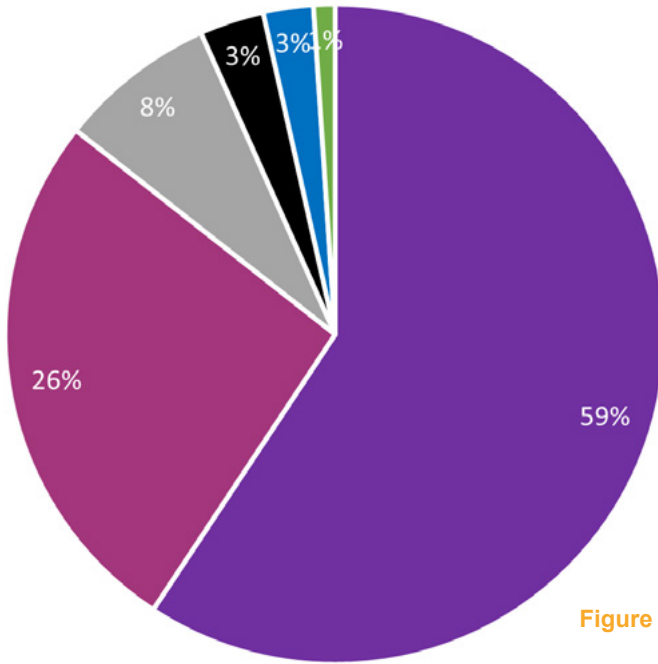


Figure 3: Top 10 Threat Actors January 2024

SECTION 05

REGIONS





Key

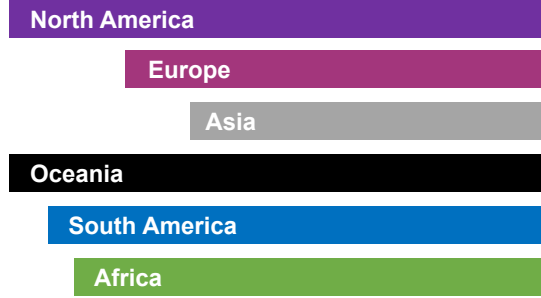


Figure 4: Regional Analysis January 2024

2024 kicks off as 2023 ended, and as we expect it to continue, with North America and Europe as the two most targeted regions around the globe for ransomware in January.

Between them, they represent nearly 86% of all observed ransomware incidents for the month, up from 80% in December. Attack numbers have continued to fall since November and, contrary to what was witnessed in December, this is represented for every region around the globe.

Additionally, January has not seen any Undisclosed ransomware attacks, allowing us to geographically place all observed victims.

North America witnessed 169 total attacks in January, or 59% of the global total.

North America witnessed 169 total attacks in January, or 59% of the global total. This is a reduction of 15% down from the 199 total attacks the region experienced in December 2023, however it is 8% higher than the 51% of the global total which the region experienced in December.

It is a nearly 250% increase over the 68 attacks the region witnessed in January 2023, highlighting the extent to which the ransomware scene has grown in the last 12 months.

Europe witnessed 75 total attacks in January, down 34% from the 114 it witnessed in December. These 75 attacks represent 26% of the global total for the month, down from 29% last month. As was the case for 11 months in 2023, Asia is the third most targeted region for ransomware in January.

The scale of the attacks the region observes, however, pale in comparison to Europe and North America. With only 22 total attacks, down 41% from December's 47 attacks, this represents slightly less than 8% of the global total.

Bringing up the rear are Oceania, South America, and Africa, having recorded 9, 7, and 3 attacks respectively. These, combined, amount to not even 7% of the total observed attacks around the globe for the month.

SECTION 06

THREAT SPOTLIGHT: HYDRADYNAMICS





For subscription customers, this month's Spotlight focussed on a small walkthrough of how we identify campaign threats.

In our continued efforts to stay atop of the currently active threats, NCC Group's analysts could not help but pull the tail of mobile banking malware once again, namely Hydra, in another instalment to our three-part spotlight piece.





FOX IT
part of 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