
nccgroup
Cyber Threat Intelligence Report
December 2023

Contents

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.

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 month, and how do these insights compare to previous months?

November attacks

391

Month on month

-12%

Analyst Comments

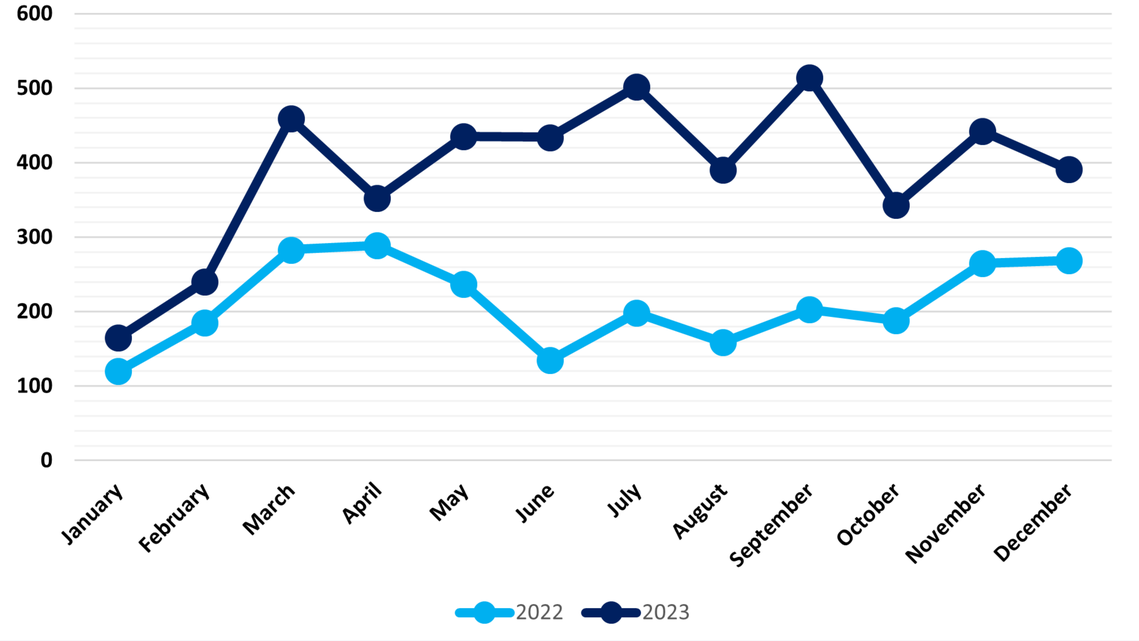

Figure 1: Global Ransomware Attacks by Month 2022 - 2023

Running in tandem with the pattern that has persisted throughout 2023, ransomware cases have once again experienced a drop from November to December, following an increase from October to November. The cases dropped from 442 to 391 which is a 12% decrease month on month but, as has been the case for the entirety of 2023, this is still an increase year on year (a 45% increase in this instance). As 2023 has presented us with some record highs in regard to total ransomware cases, it is no surprise that it has consistently surpassed 2022's figures, but as to whether 2024 will achieve the same ground-breaking feats is difficult to predict, if not hard to imagine. However, with the huge influx of new players in the ransomware threat landscape, this concept is not completely outlandish so NCC Group will continue to vigilantly observe for any shifts in the threat landscape.

The final total of ransomware cases in 2023 is 4667 which far surpassed our initial expectations for the year and is a huge increase of 84% from 2022. Should 2024 experience a similar year on year increase when compared with 2023, we can expect a mammoth total of approximately 8500 ransomware cases and, with the constant influx of new threat actors, the increase could even be exponential. At the very least, the increase from 2022 to 2023 shows that, although threats like Business Email Compromise have also been reported to be on the rise in 2023, the double extortion methodology's popularity is not going to be superseded any time soon.

Sectors

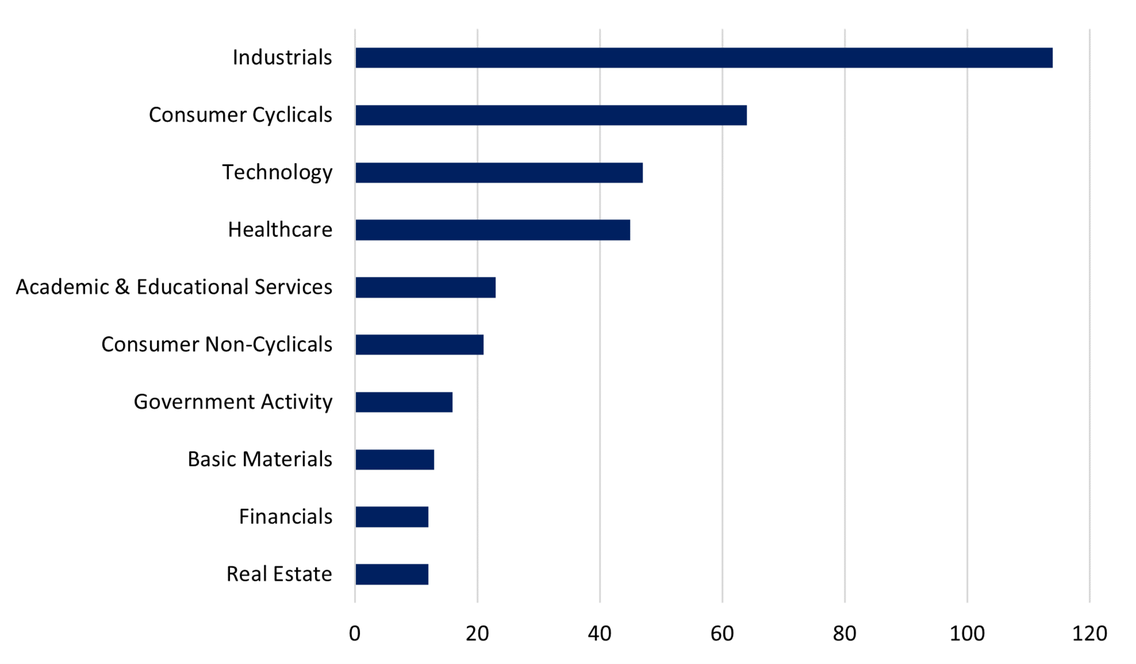

Figure 2: Top 10 Sectors Targeted in December 2023

Following two months of the Healthcare sector featuring in the top three most targeted sectors, the threat landscape has shifted back to the usual suspects with Industrials, Consumer Cyclicals, and Technology. However, there is only a difference of two hack & leak cases between the two sectors, showing that Healthcare is now more frequently targeted in general, so we can now consider this a true shift in the threat landscape. Based on the past three months, it would not be surprising so see the Technology and Healthcare sectors constantly fight for third place in 2024.

As is commonplace, the Industrials sector is in first place again in December with 114 cases (29% of the total) which is a 22% decrease from 146 in November. As we have mentioned before, the Industrials sector is a frequent target due to the breadth and diversity of organisations existing within and the nature of them, as many store vast quantities of either Personally Identifiable Information (PII) or Intellectual Property (IP).

Consumer Cyclicals is in second place once again with 64 attacks, which is 16% of the total figure for December and an 18% decrease from November's figure. Finally, Technology experienced 47 attacks in December which accounts for 12% of the total and is a rather significant 38% increase from November's figure.

Threat Actors

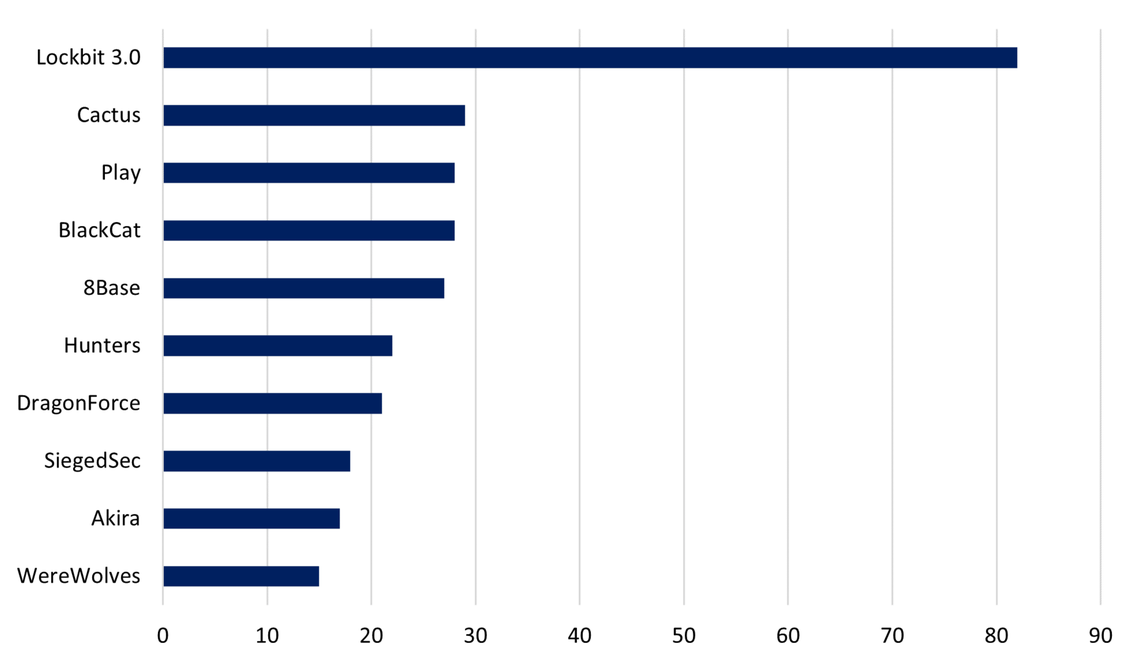

Figure 3: Top 10 Threat Actors December 2023

The month of December brings us a total output of 391 cases which represents a 12% month-on-month decrease in the attack volume. Amongst the top three we see; LockBit with 82 cases, Cactus with 29 cases and in a shared third position, Play and BlackCat with 28 cases each. Overall, the top three are responsible for 43% (167) of the monthly output, however, further details on their activity are available in the following pages.

8Base not only remains fourth for the second month in a row but also maintains the same monthly output as in November (or 27 cases), contributing 7% of the overall output in December. On the other hand, Akira drops from sixth position in November to ninth in December with a total of 17 cases, representing a decrease in activity of 11% (from 19 cases).

At fifth position, we observe a newcomer known as Hunters responsible for 22 cases that contributed 6% of the monthly total. Not a lot is known about the group, but they were initially believed to be a Hive rebrand, a ransomware group which was dismantled by Europol and FBI in 2023, due to the code overlaps and similarities found in the ransomware strings. However, members of the operation denied this 'theory' by stating they only purchased Hive's code and are in fact a newly created ransomware group with a specific focus on stealing target's data as a leverage for extortion purposes. At present, the group's top targets are Healthcare and Industrials' sectors with 36% (8) and 32% (7) respectively.

Next, we see another newcomer named DragonForce that contributed 21 cases or 5% to the monthly total. The group seems to have been around since summer 2022, operating as a hacktivist initially targeting Indian entities via exploiting vulnerabilities in Windows servers' Local Privilege Escalation (LPE) and Local Distribution Router (LDR). However, their latest activity, captured in the NCC Group database, seems to suggest that the group has evolved to a ransomware operation that currently favours targeting Industrials and Consumer Cyclicals sectors with 33% (7) and 19% (4) respectively.

Last but not least, a third newcomer known as WereWolves joins the top ten at tenth position with 15 cases, contributing 4% of the monthly total. At present, the group's top target seems to be Consumer Cyclicals with 40% (6). It is unclear when this group was established but it seems that their attacks took place between May and November 2023. There is a speculation that they are a LockBit affiliate, as some of the attacks listed on the data leak site (DLS) appear to be copy-pasted attacks that were previously carried out by LockBit.

With regards to the DLS, it contains an 'about group' section, which essentially explains the terms, conditions, and rules of the operation. Some of which include: A 5% rule meaning that 5% of the group's proceeds would go to charity, and is described as a 'law' that all group members would have to adhere to. Additionally, the group states they would not target any countries that are affected by wars and/or natural disasters as well as critical infrastructure under any circumstances. Critical infrastructure in this case would include hospitals, orphanages, etc. The statement also specifically mentions that any organisations conducting attacks against critical infrastructure entities would become a 'legitimate target for destruction' by the group and/or their partners. Finally, WereWolves states the organisation is not related nor belongs to any political system and would not be involved in any attacks with pro-government groups. Perhaps, the lack of political motivation would explain why 80% (12) of their attacks are against Russian organisations.

Regions

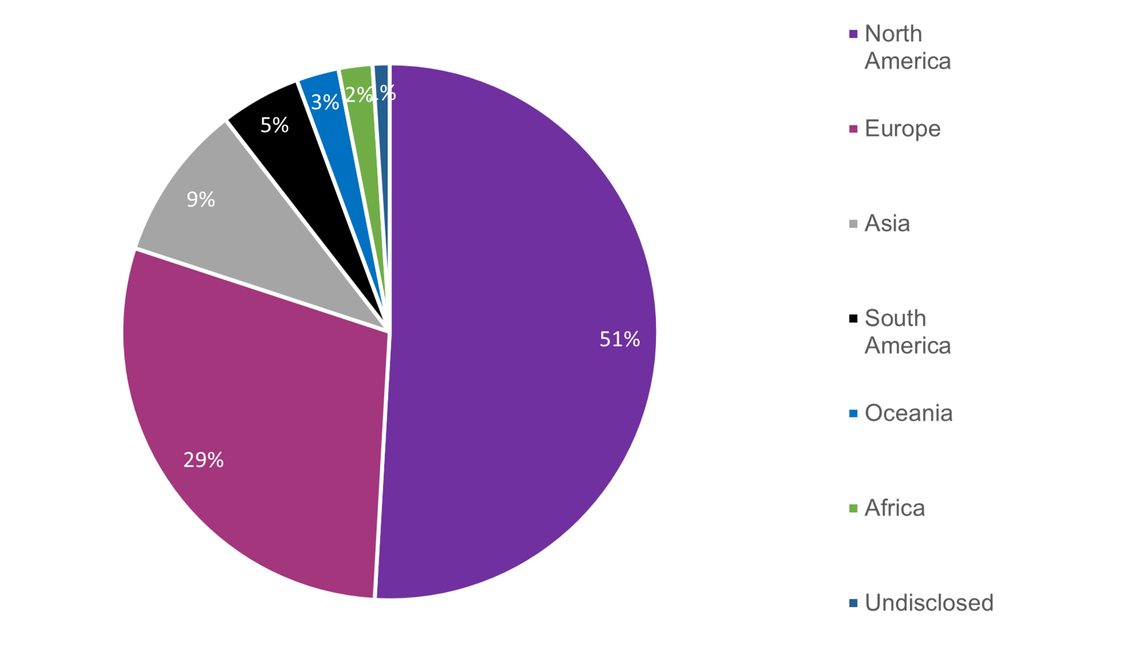

Figure 4: Regional Analysis November 2023

As has come to be expected, North America and Europe continue to be the two most targeted regions around the globe for ransomware attacks, representing 80% of total observed attacks between them. Overall attacks for December are 11.5% lower than in November, though this dip in volume is not reflected equally across all regions.

Experiencing 199 total attacks in December, North America has 51% of the total observed attacks for the month. This total is down from 219 in November, a reduction of 9%. Europe as usual comes in as second most targeted with a total of 114 attacks, or 29% of the monthly total. This is a reduction of 21 attacks from November's figure of 135, a proportional decrease of 15.5%. This is an inverse of what happened in November, when Europe saw an increase in attacks higher than the overall increase, and now experienced a decrease higher than the overall decrease. This enforces the need to accumulate several months' worth of data before making predictions of future behaviour or identifying any potential patterns.

The remaining regions are in the same positions as November: Asia with 37 total attacks, a decrease of 20%; South America with 19 total attacks, an increase of 19%; Oceania staying constant with 10 attacks in both November and December; Africa with 8 total attacks, a decrease of 11% down from the 9 total attacks observed in November; and Undisclosed with a total of 4 attacks in December, down from 7 such attacks in November.

One observation of note is the inclusion of attacks against targets in Russia this month. 12 attacks in total, 11% of all attacks levied against targets in Europe, were against victims in the Russian Federation. To put it into perspective, there were only 13 observed ransomware attacks against Russian targets in the whole of 2023. This shift in the landscape is examined in greater detail in the Analyst Comments section, and introduction to the Threat Actors section of this report.

Threat Spotlight

This month's Spotlight is twofold. December greeted us with increased activity of two malware families – Hydra mobile malware previously elaborated on in the Quarterly report publication, and the unexpected activity of Qakbot following the malware family's infrastructure take-down at the end of August. The final chapter is an overview of the Meduza Stealer. While infostealers are a cybercriminal staple that make their way into reports on a regular basis, it turns out Meduza warrants a revisit this month.

nccgroup

Our experts are here to help you every step of the way. Contact us today to learn more about cyber security.