
nccgroup
Cyber Threat Intelligence Report
APRIL 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?

APRIL ATTACKS

352

MONTH ON MONTH

-23%

Analyst Comments

The amount of successful ransomware attacks this month has decreased to 352 from last month's record-breaking number, 459. This does not come as a surprise, given the massive 91% jump in ransomware incidents from February to March. As mentioned in the previous report, the main contributor to March's numbers was the prolific exploitation of the GoAnywhere MFT vulnerability, hence, a decline was anticipated in line with patches being applied, reducing the possibility for further exploitation and attacks.

Looking at the first 4 months of 2023, it is clear that ransomware numbers are trending much higher than in 2022. Although the results this month have declined, the number of victims is the second highest ever recorded in our database (beginning 2021). This is a result of both BianLian and BlackCat recording their highest victim count in a given month since the start of NCC Group's ransomware tracking in 2021. In addition, Lockbit 3.0's victim count is the second highest ever recorded for the group, in part due to their exploitation of the critical PaperCut vulnerability in the second half of this month. More information regarding the PaperCut vulnerability may be found in the Spotlight at the end of this report.

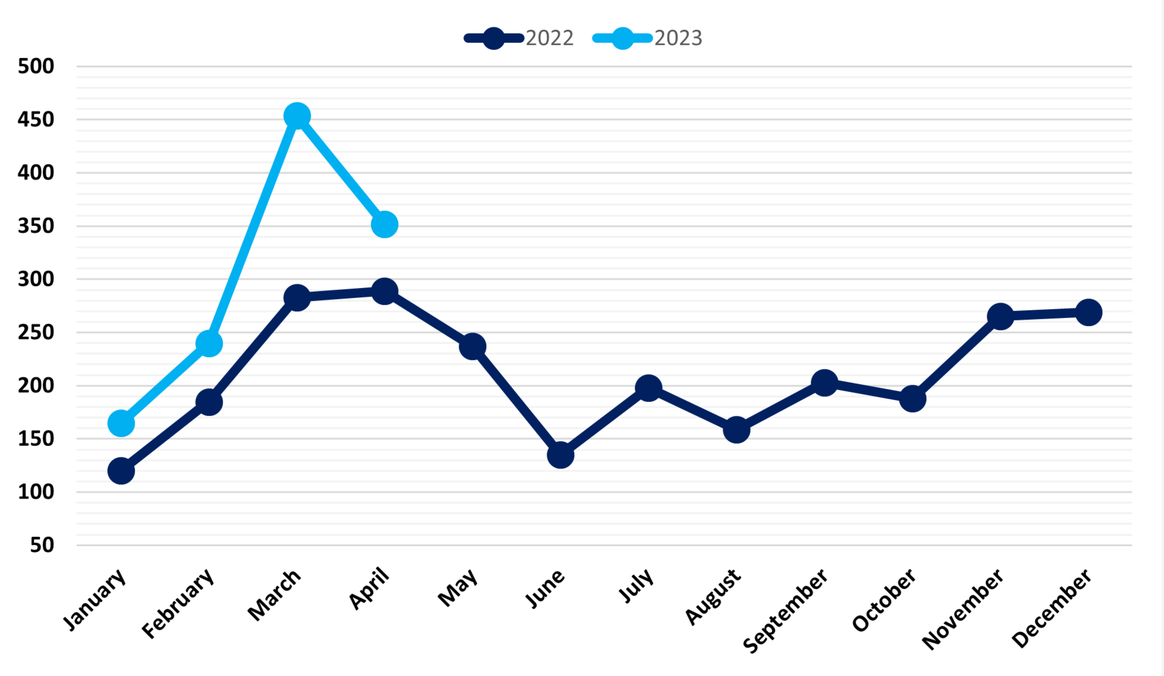

Figure 1 - Global Ransomware Attacks by Month 2022 - 2023

Sectors

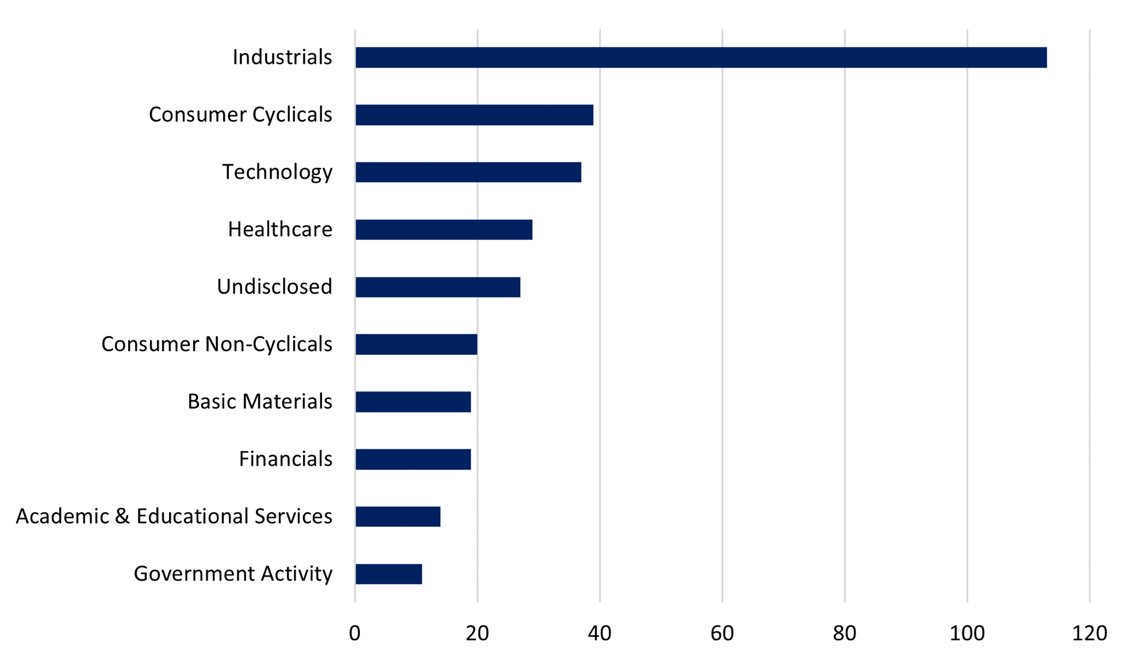

Figure 2 - Top 10 Targeted Sectors April 2023

The most targeted sector in April concerned Industrials with 113 attacks, although this declined by 23% from 147 in March, in line with the wider threat landscape. Industrials nevertheless remains the most targeted sector for ransomware attacks, representing 32% of all such attacks this month, a static percentage month on month. As the Industrials sector remains the largest sector classification, it is expected that this will remain the most targeted for 2023. The personally identifiable information (PII) and intellectual property (IP) of businesses within the Industrials sector remain lucrative targets for ransomware driven threat actors, alongside potential business disruption, which can be exploited to pressure organisations into payment. Organisations within should continue to reinforce strong cyber security hygiene against ransomware.

Threat Actors

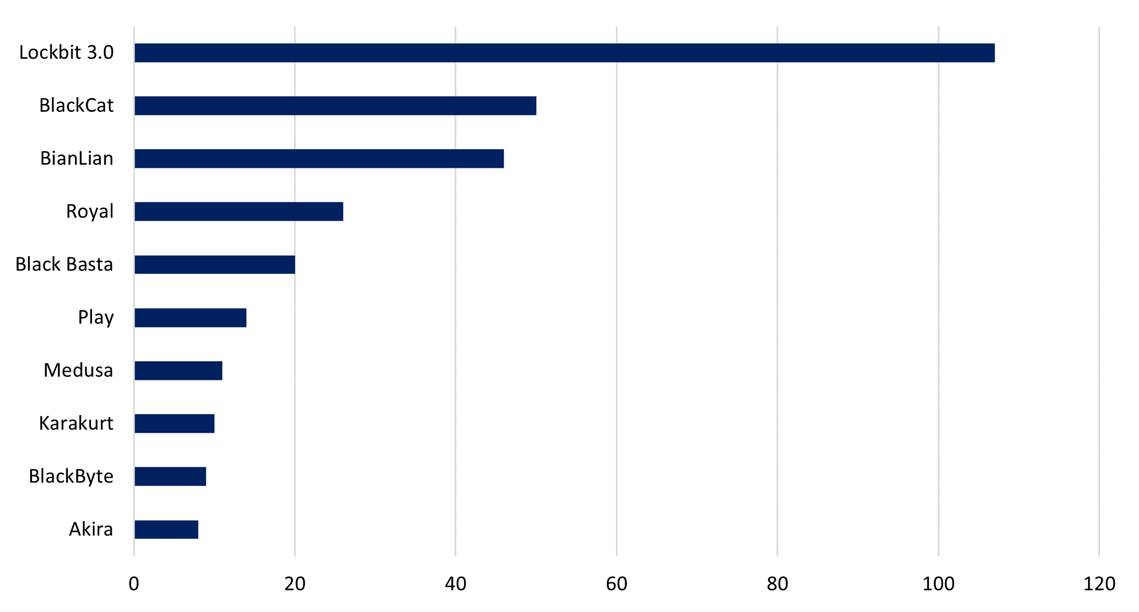

Figure 3 - Top 10 Threat Actors April 2023

After a slight shuffle of the most active threat actors in March, the top three most-active groups are Lockbit 3.0, BlackCat, and BianLian, as observed in February. These top three are responsible for carrying out 203 out of 352 attacks recorded in the month of April, representing 58% of the overall activity across the threat landscape.

For comparison, their activity in February was as follows: Lockbit 3.0 recorded 129 cases, followed by BlackCat with 31 cases, and finally BianLian with 20 cases representing 180 (75%) out of 240 cases that month. Interestingly in April, BlackCat and BianLian significantly increased their activity over February's output (by 38% and 56% respectively), whereas Lockbit's has fluctuated up and down since the start of the year. March's most prominent threat group Cl0p has fallen out of the leadership board and only accounts for 3 attacks last month, representing a 98% decrease in activity.

In addition, a new ransomware player called Akira made it into the top ten most active groups in April, contributing 2% of overall activity. The threat group is believed to be independent from other well-known ransomware groups but operates in a similar way and is mainly interested in targeting enterprises. At present, there does not seem to be a distinct favourite industry for this group. The list of current victims is spread evenly across the following industries, with one attack each: Construction & Engineering, Leisure Products, Containers & Packaging, Investment Holding Companies, Personal & Household Products & Services, Professional & Commercial Services, Real Estate Operations, Schools, and Colleges & Universities.

Regions

The relative distribution of attacks across the globe remains largely unchanged, with only minor shifts. North America experienced an increase of 1% from 48% of all attacks in March (221 attacks) to 50% of all attacks in April (172 attacks). Europe witnessed a decrease of 3% from receiving 27% (126 attacks) of attacks in March to 24% (85 attacks) in April. Asia experienced a similar decrease from 13% (59 attacks) in March to 10% (34 attacks) in April.

South America recorded a proportional increase of 1% from 4% (20 attacks) in March to 5% (18 attacks) in April. Africa likewise observed a 1% increase, from 2% (7 attacks) in March to 3% (11 attacks) in April. Oceania remained at 1% of total attacks from March (6 attacks) to April (5 attacks).

Undisclosed attacks however, doubled as a proportion of the total from 4% (19 attacks) in March to 8% (27 attacks) in April.

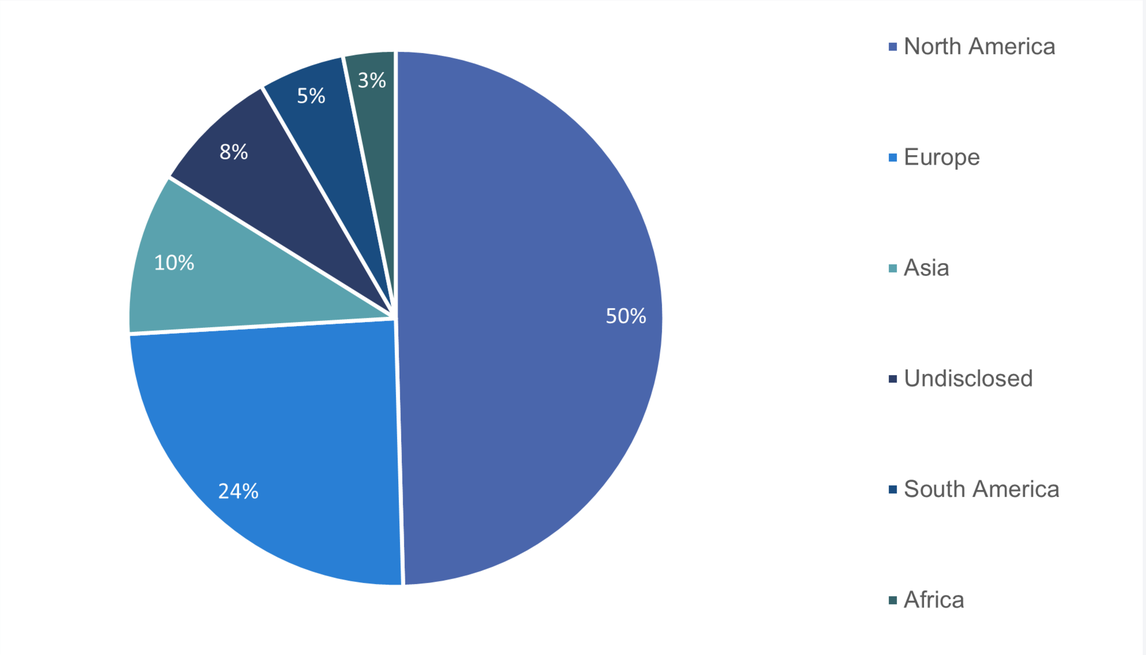

Figure 4 - Ransomware Cases by Region April 2023

Threat Spotlight: PaperCut Printer Software

CVE-2023-27350 and CVE-2023-27351 are two critical software vulnerabilities affecting PaperCut's printer software. These vulnerabilities are critical not only due to the potential impact should they be exploited, but also due to the scale of potentially impacted users. PaperCut states that they have more than 100 million users in over 70,000 organisations. The company's products are used by a variety of industries including local government, healthcare, and education institutions. Shortly after the announcement of the vulnerabilities, Shodan indicated roughly 1,700 instances of software exposed to the internet. These vulnerabilities were patched in March, but are now being actively exploited at organisations which are yet to update their software versions.

nccgroup

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