nccgroup

FOX IT
part of nccgroup

Monthly Threat Pulse

Review of March 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.

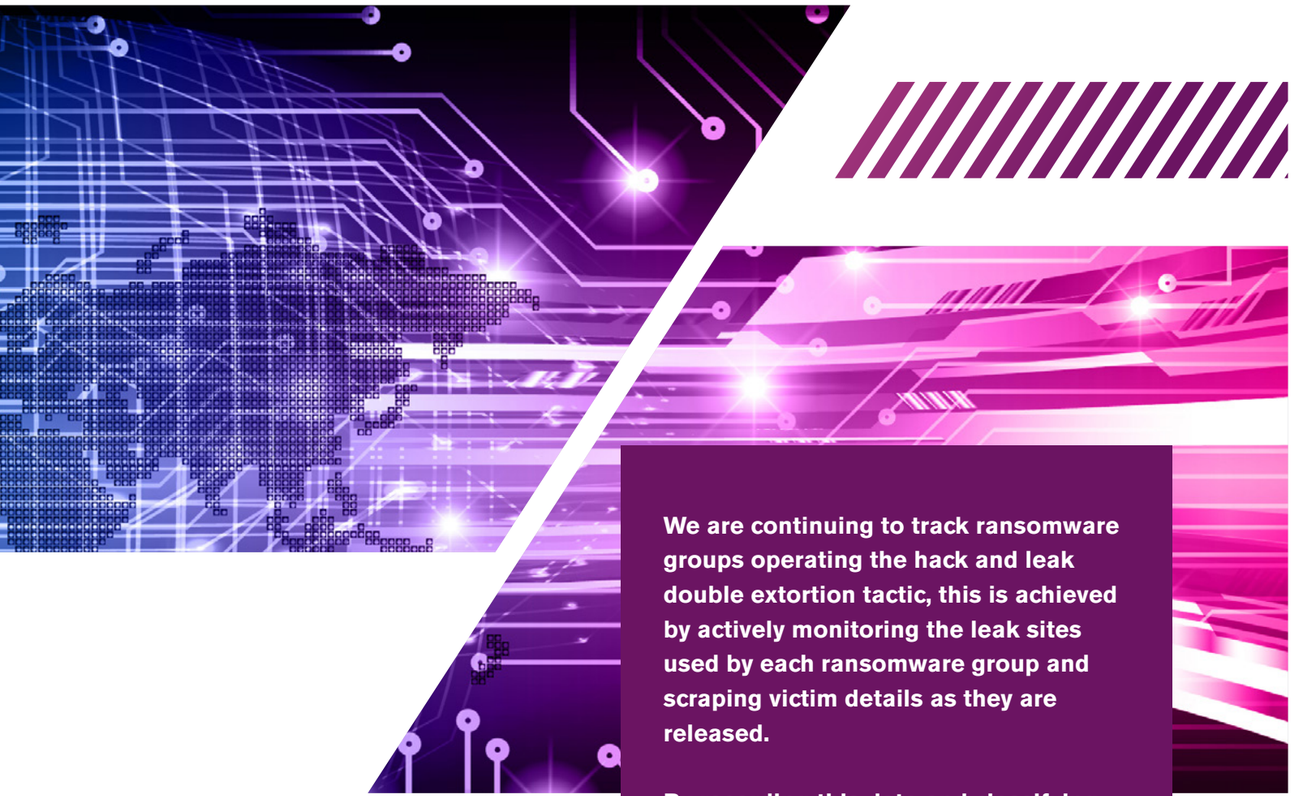
Let us keep watch over the cyber and geopolitical landscape so you don't have to.

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

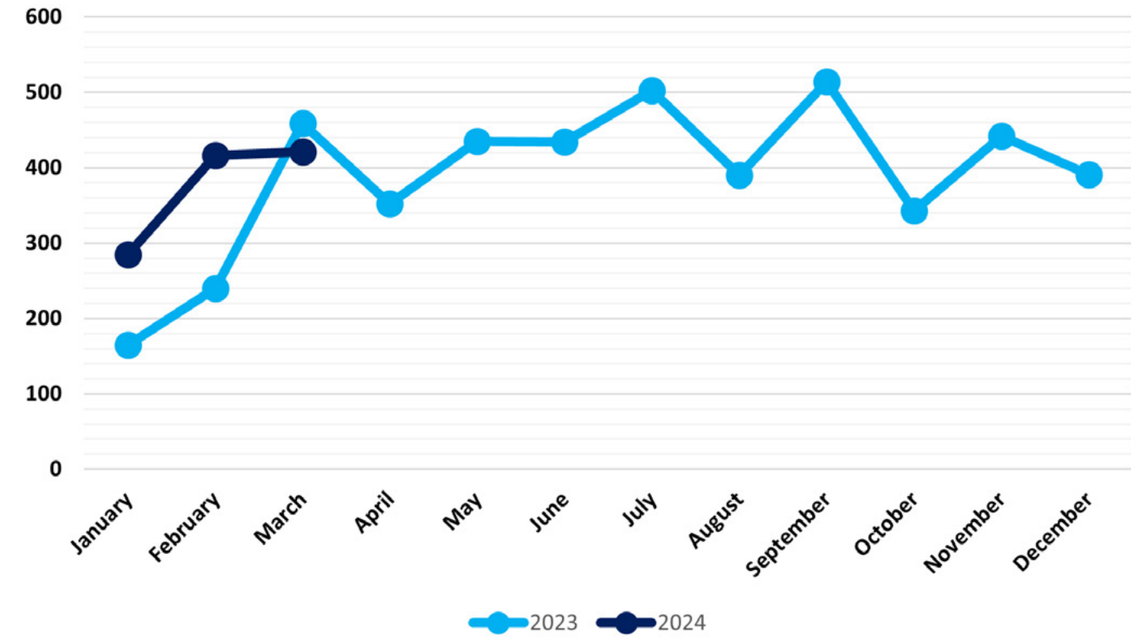


Figure 1: Global Ransomware Attacks by Month

The total number of ransomware attacks have, as is to be expected, increased but only slightly from February 2024 to March 2024 from 416 to 421 cases, or a 1% increase month-on-month. Comparing with March 2023, we observe a decrease in targeting of 8% (from 459 to 421 attacks) year-on-year (YoY).

It is important to bear in mind that March 2023's overall attack volume was highly impacted by the mass exploitation of the GoAnywhere MFT vulnerability, tracked as CVE-2023-0669.

At the time, CL0P's persistence in exploiting the vulnerability accounted for 28% of the attack volume (or 129 attacks). If we are to ignore CL0P's activity in March 2023, we would actually be seeing an increase in the attack volume of 28% (from 330) YoY.

Despite the YoY decrease in targeting, the monthly targeting increase is perhaps a good indication that we will most likely observe an activity increase in April as well as the remainder of the year.

SECTION 02

SECTORS

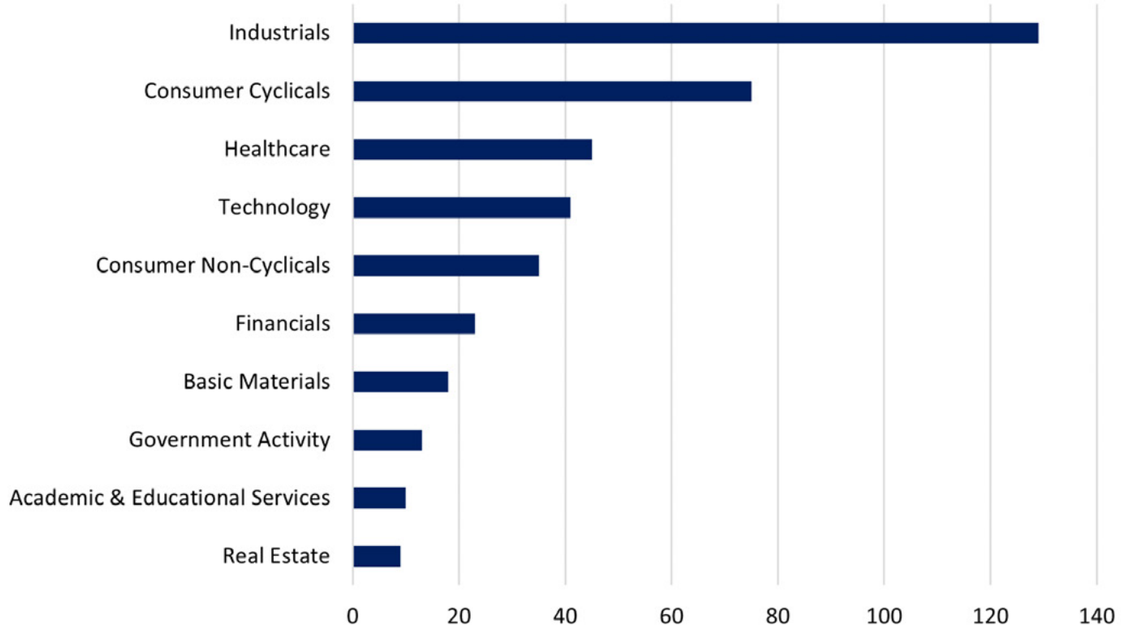


Figure 2: Top 10 Sectors Targeted March 2024

March's ransomware targeting by sector saw Industrials and Consumer Cyclicals remaining in first and second position. Industrials continued to dominate the landscape with a total of 129 ransomware attacks occurring in the sector, accounting for 31% of the output observed in March.

When compared to February, however, there was a slight decrease in targeting of 4% (from 134 to 129 attacks) for the sector. Consumer Cyclicals remained second, but, in comparison to Industrials, experienced a 14% increase in targeting from 66 to 75 attacks.

Outside of the top two sectors, we notice a lot of changes to the sectors' positioning when compared with February such as; Healthcare moved from fourth in February to third in March with an output of 11% (or 45 attacks), while Consumer Non-Cyclicals dropped from third in February to fifth in March with an output of 8% (or 35 attacks).

Consumer Non-Cyclicals' targeting, in fact, was down by 13% (from 45 attacks), while Healthcare's went up by 15% (from 39 attacks).

Next, Technology jumped from sixth position in February to fourth in March, accounting for 10% of the monthly output (or 41 attacks), which also represents a 41% increase in the sector's targeting (from 29 attacks). Due to a 64% increase in targeting (from 14 to 23 attacks), the Financials' sector moved from eight in February to sixth this month, accounting for 5% of the attack volume.

Simultaneously, a 44% decrease in targeting (from 32 to 18 attacks) resulted in the Basic Materials' sector falling from fifth in February to eighth in March.

The remaining three sectors (or Government Activity, Academic & Educational Services and Real Estate) experienced minor changes in positioning and together account for 8% (or 32 attacks) of the overall monthly output.

SECTION 03

THREAT ACTORS

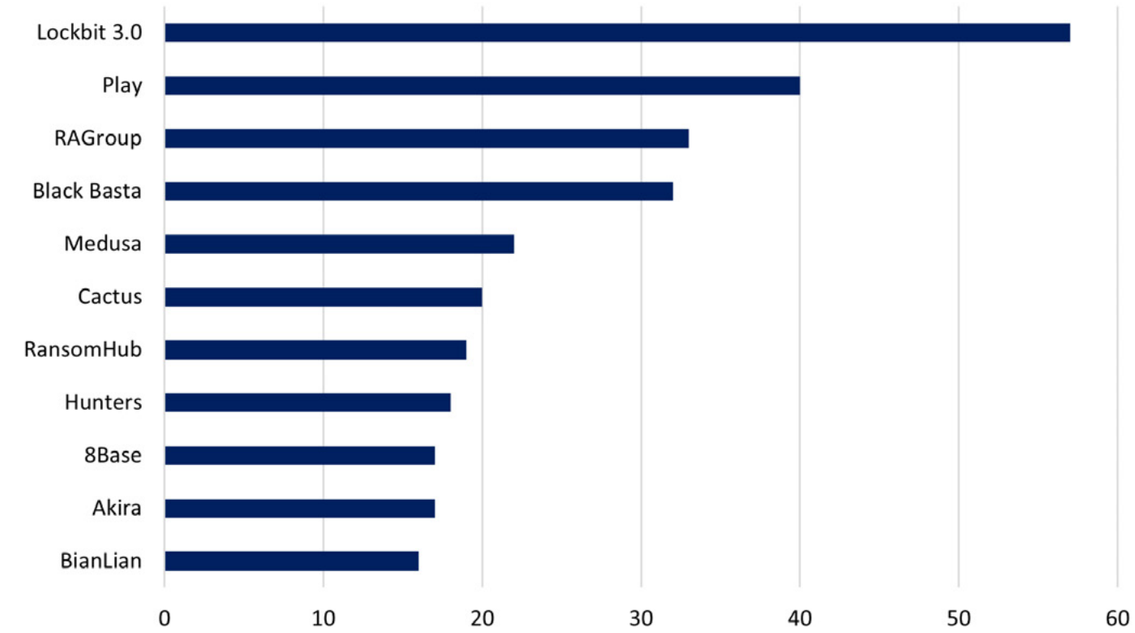


Figure 3: Top 10 Threat Actors March 2024

LockBit 3.0 are once again the most prominent ransomware threat group for the month of March 2024. Filling out the rest of the ranks though, we are starting to see some new faces.

Play, as the second most prominent actor of the month, are no strangers to the most-prominent actors list, having been joint-fourth in December 2023 alongside BlackCat. Coming in as third-most prominent for the month, are RAGroup; a ransomware group we have not seen in the top three before.

Though it is still the most prominent threat group, LockBit 3.0's observed activity in March was far lower than might have been expected given their activity levels over the last year and was in fact the lowest observed level of activity by the group since July of last year. With only 57 observed attacks to their name in March, LockBit are responsible for a comparatively paltry 14% of global attacks.

Contrary to LockBit which experienced a nearly 50% decline in activity between February and March, Play have experienced a surge in activity: going from 26 attacks in February to 40 in March, an increase of nearly 67%.

RAGroup, meanwhile, have returned to prominence with a bang after no observable activity in either January or February of 2024.

With 33 observed attacks to their name in March, they have experienced an increase in activity of over 300% from their last noted activity of 8 total attacks in December 2023. Though the group was fairly consistently active throughout 2023, for the most part they were observed conducting fewer than 10 attacks each month.

These most recent levels of activity are a massive increase over their achievements to date, with their previous highest recorded level of activity being 9 total attacks in November 2023.

SECTION 04

REGIONS

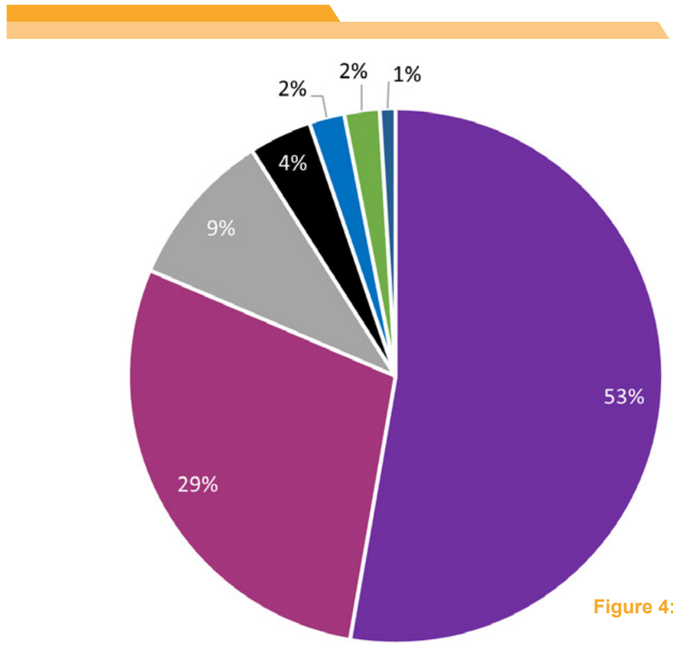


Figure 4: Regional Analysis March 2024

The picture for March 2024 looks very similar to the previous month, with 53% of all attacks for this month aimed at North American organisations, whilst in February this region accounted for 55%.

24% of North American attacks in February were driven by Lockbit (55) but of note is that in March this year, 14% (31) attacks came from Lockbit, which was matched by Play.

Play delivered the same share of attacks to this region as Lockbit up from the 8%

Play delivered the same share of attacks to this region as Lockbit, up from the 8% (18) in February, showing their relative impact has increased. This may be due to the law enforcement actions taken against Lockbit, potentially disrupting their operation, albeit not terminally.

Overall attacks were the same year on year, with March 2023 numbers at 221, showing a lower share of all attacks that month, given its representation of 48% of the monthly total.

The number of attacks in March for Europe came in at 121 (29%), showing a stable share of attacks (29%) month on month, with little variation also year on year with 126 attacks in 2023, a share of 27%. In March 2023, there were 126 attacks aimed at organisations in Europe, which meant 27% of all attacks that month, showing similar relative targeting.

Asia saw 40 attacks in March 2024, a significant decrease of 32% on the 59 seen the year before, with 13% of attacks in March 2023 versus 9% this March.

The regions of South America, Oceania, Africa and those which are not disclosed, represent the remaining 9% of all attacks in March 2024. South America saw 4% (16) share, Oceania 2% (9), Africa 2% (9) and undisclosed 1% (4).

South American aimed attacks saw the same share of attacks month on month, and the remaining regions saw very little fluctuation month on month, too.

SECTION 05

THREAT SPOTLIGHT: CONTESTS & COMPETITIONS

Criminal creativity is the backbone of all security industries. Being able to develop new strategies to evade detection and punishment, carry out illicit operations in an organized manner, and exploit technical and legal loopholes, all keep the contributors to safety & security everywhere on our toes, as understanding criminal creativity is crucial to stay ahead of evolving criminal tactics.

Unfortunately, this fascinating aspect of cybercrime tends to be somewhat de-valued in the majority of reporting in favour of focusing on the malware or group tactics, and understandably so: people and communities are fickle entities to research.

In this Spotlight we will be examining how one of the oldest and most well-known online communities of Russian origin is helping to foster this creativity.

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