
nccgroup
Cyber Threat Intelligence Report
September 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?

SEPTEMBER ATTACKS

514

MONTH ON MONTH

+32%

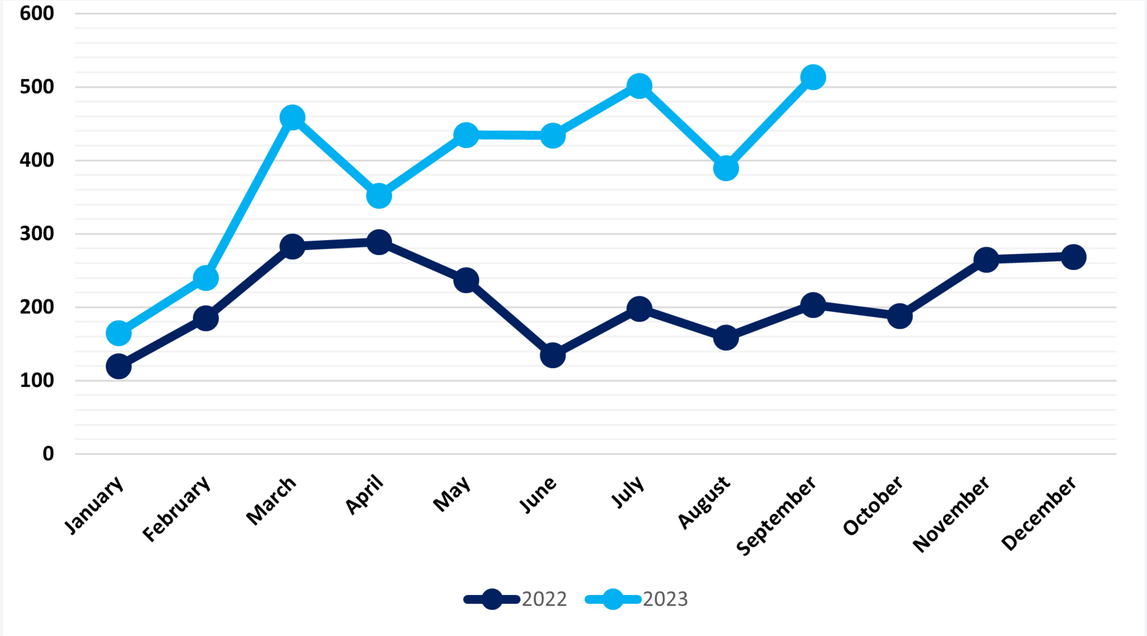

Figure 1: Global Ransomware Attacks by Month 2022 - 2023

Analyst Comments

After August's 22% decline from 502 attacks to 390, the figures have spiked once again to July's heights with 514, which is in fact a miniscule increase on the former's figure and, once again, marks the highest number of hack & leak attacks recorded in one month within NCC Group's dataset. This is in part due to the inclusion of yet another host of new double extortion ransomware groups but can also be attributed to the arguably more proportional efforts of groups across the board, when usually big players like LockBit 3.0 and/or CL0P contribute a vast majority to the total figure. In our previous Threat Pulse reports we projected that with this year's figures constantly surpassing those of 2022, we could see 4000 by the end of 2023 and, with the total already reaching just short of 3500 attacks, this is highly likely to be reached and even substantially surpassed by the end of the year.

Another observation worth mentioning is the continued year-on-year increase, with there being a 153% rise from September 2022 and September 2023. This, paired with the fact that there has been a 76% increase in the quantity of double extortion ransomware groups between these time periods, suggests that the interest in ransomware for profit is by no means dwindling. NCC Group predicts that it is highly probable that this pattern will continue and repeat itself in another year's time, as we are yet to observe evidence to the contrary.

Some of this month's new groups of note include LostTrust and RansomedVC both of which contributed 9% and 10% to the total number of attacks this month respectively, as well as featured in the top 5 most active TA's, indicating that they are starting off with a bang. The targeting of some of these groups will be expanded upon in the Threat Actors sections, and our Spotlight piece this month will be a deep dive into RansomedVC following their alleged compromise of the world famous technology giant, Sony.

As mentioned, CL0P would typically feature in at least the top 3 threat actors for activity in the month, however, as we alluded to in the August Threat Pulse, CL0P kept a significantly lower profile with just 3 victims that month and have now completely vanished from our dataset in September. Following this hiatus, which is characteristic of the threat group, it would be wise to expect and prepare for a highly targeted mass-exploitation campaign soon.

Sectors

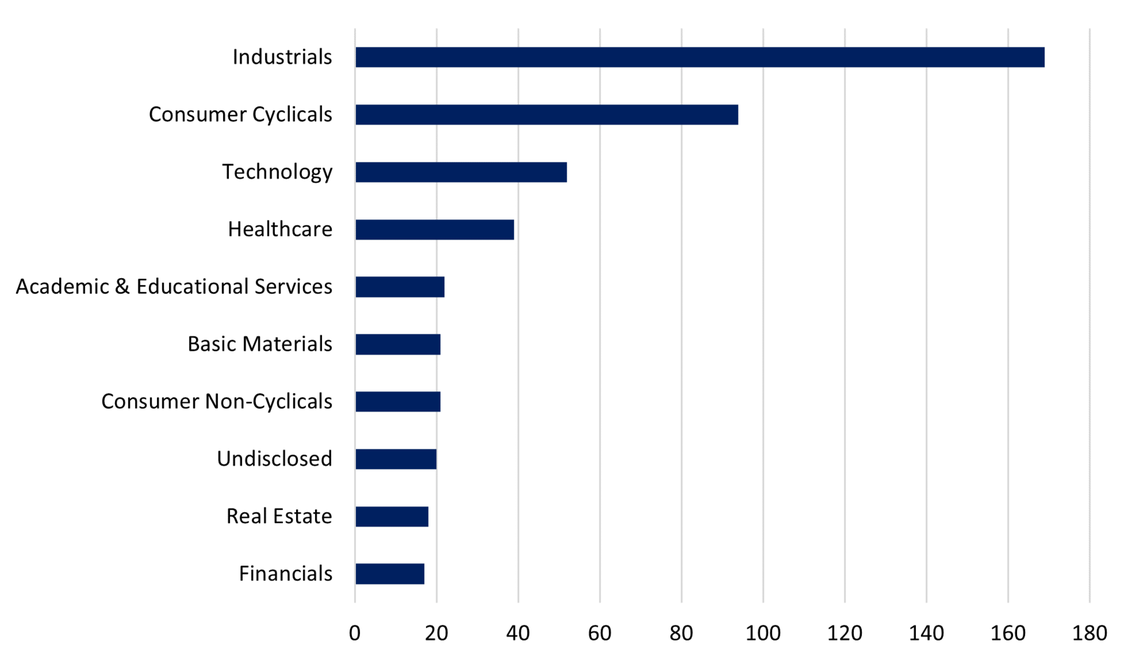

Figure 2: Top 10 Sectors Targeted September 2023

There has been no deviation from the norm in September of 2023, with Industrials leading once again in terms of attack volume with 169 attacks or 33% of the total, which is a 40% increase in attacks when looking at the absolute figures. In terms of relative weighting however, this is an increase of just 2% which shows that despite peaks and troughs in the total number of attacks in the sector, it continues to represent roughly a third of all hack and leak instances month-on-month. The typical motivations to target this sector remain the same, especially where the theft of Personally Identifiable Information (PII) and Intellectual Property (IP) are concerned. Additionally however, a consideration needs to be made for the issue of Operational Technology (OT) and Information Technology (IT) convergence. While OT environments may be targeted to cause operational disruption and thus incentivise ransom payments, their use with IT environments also simultaneously expands the attack surface and increases the number of attack vectors, providing lucrative opportunities for financially-motivated threat actors.

The following two most targeted sectors this month also remain consistent with what we usually see; Consumer Cyclicals and Technology which, as we have mentioned in previous reports, have held the top positions since March 2023. In September, Consumer Cyclicals saw 94 attacks (or 18% of the total)

which is an increase of 28 in terms of absolute figures and a 1% proportional increase. Technology experienced 52 attacks this month (or 10% of the total), which is an increase of 18 attacks, and equally a proportional increase of 1%. Although August saw some notable contrasts in terms of the relative weighting of attacks when compared to July, the difference in the targeting of the top sectors between August and September is much less significant, perhaps implying a more permanent shift.

One other observation of note is the noticeable increase of ransomware attacks in the Healthcare sector. The sector has experienced a rise of 18 attacks, which is a huge 86% increase month-on-month, bringing its targeting back to the levels we have seen for the majority of 2023, likely making August an outlier. One way we could explain the interest in Healthcare is the combined wealth of the sector, especially in Pharmaceuticals which, according to an article published by Goldman Sachs, is sitting on US$700 Billion for acquisitions and investments. This would make the sector an extremely attractive prospect for financially-motivated threat actors that employ a big game hunting methodology to their targeting.

Threat Actors

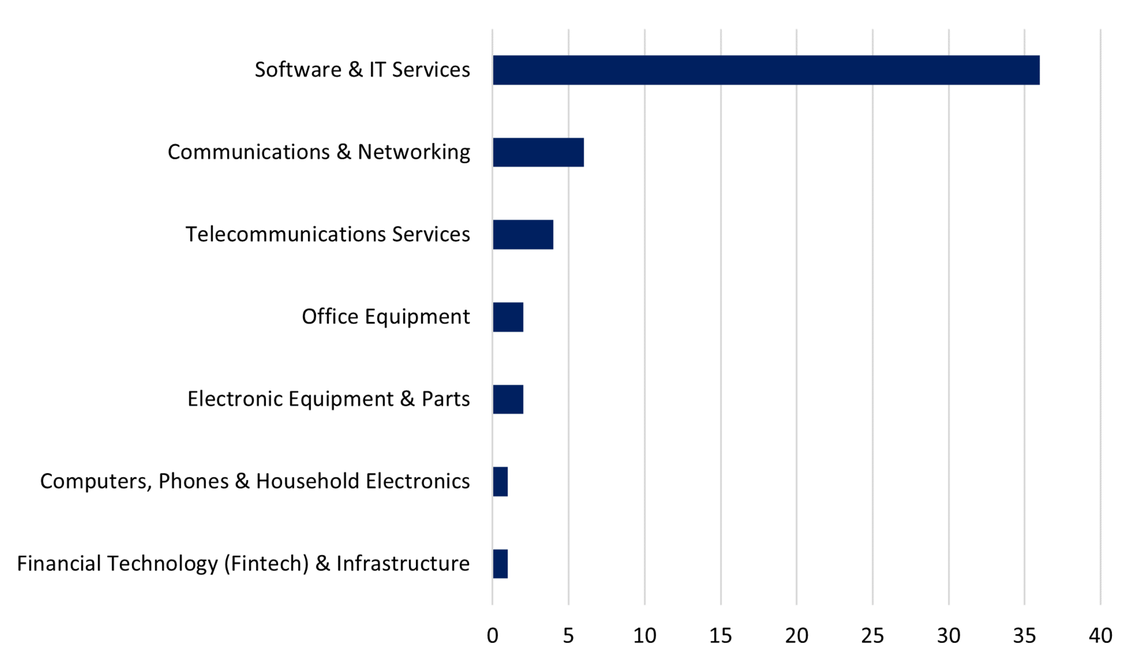

Figure 6: Top 10 Threat Actors September 2023

The month of September brings not only the highest activity, with a total of 514 attacks, across the threat landscape recorded in 2023 so far, but also a number of new threat groups emerging to contribute to that peak activity, representing a 31% month-on-month increase when compared with last month. Figure 6 captures the top 10 threat groups in September and what we can immediately observe is a much more even split in the attack volume amongst the groups as opposed to what we have seen in previous months. For example, Lockbit dominated with 32% (125 out of 392 cases) in August whereas the majority of groups within the top ten would have only accounted for 10%, or less of the monthly total. This month, the top ten are jointly accountable for a total of 362 cases representing 70% of the monthly output, which also represents 93% of the output recorded in the month of August, when we saw a total of 392 cases.

We are noticing newcomers LostTrust in second position with 10% (53) and RansomedVC in fourth position with 9% (44) of the monthly output. The newcomers' activity account for a total of 19% (97) of the September's figure. More information about these two threat groups is available in the top three overview as well as the Spotlight.

This month saw ramped-up activity from two other recently discovered threat groups; Cactus and Trigona. In the case of Cactus, the group's activity was initially picked up in July with a total of 13 cases, followed by 0 cases recorded in August. Cactus' activity so far sits at 51 cases in total although this number is significantly boosted by their activity this month, which is a total of 33 cases. The group was identified around March and is known to target high-profile commercial entities via exploiting known vulnerabilities in VPN appliances to gain initial access.

On the other hand, Trigona's activity has become known in April with a total of 5 cases, but the group has only been active in certain months with their total activity so far coming to a total of 32 cases. Trigona seems to have been around since at least June 2022 and what is currently known is that the group tend to target compromised MSSQL servers via brute force methods. Trigona has also been spotted exploiting the ManageEngine vulnerability, tracked as CVE-2021-40539. The group is believed to be linked to another ransomware group; knows as CryLock due to the similarities found in the Tactics, Techniques and Procedures (TTPs) used by both.

Outside of the top ten, we can also observe the following newcomers – Threeam and CiphBit; jointly responsible for 4% (19) of the monthly output. CiphBit was first spotted in April and operates in favour of the double extortion tactic where the target's stolen data is encrypted followed by a ransom demand to decrypt it. In the case of a failure to comply with the request, the victim's data is leaked on the group's data leak site. When encrypting the files, the group seems to add titles containing a unique ID which is assigned to each victim, the group's contact email address and finally, an extension containing four randomly selected characters.

In the case of Threeam or 3AM, it is believed to have been around since February, written in Rust and does not appear to be currently associated with any other known ransomware families . The group also favours the double extortion tactic, and it has initially been spotted in the wild when an affiliate failed to deploy LockBit's ransomware on a targeted network. This seems to be a novel approach not only indicating the independence of affiliates from operators but perhaps also paving the way for a new trend in ransomware attacks.

Regions

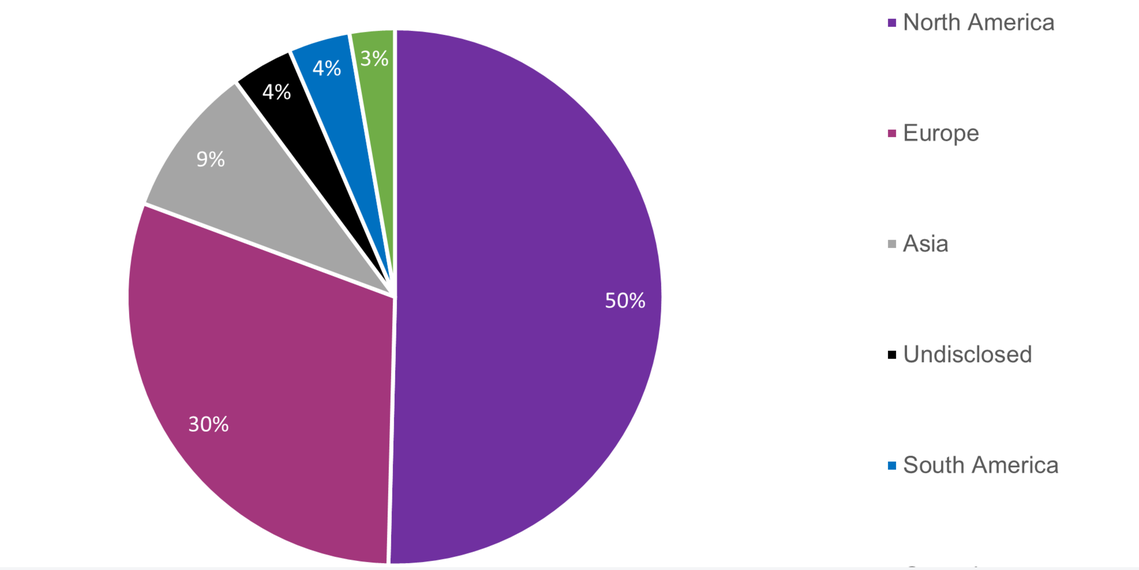

Figure 10: Regional Analysis September 2023

Running parallel with the rest of the year, the top three most targeted regions remain static, with North America coming in at the top with 258 attacks, then Europe with 155, and finally Asia with 47.

It is interesting that in relative terms, North America's targeting has increased by 3% and Europe's by 2%, while Asia has experienced a considerable 6% decrease, which highlights a shift in the threat landscape away from Asia towards Western nations, bringing levels back towards baseline behaviour. Asia's baseline for hack and leak instances usually hovers around 10% but this deviated in February 2023 and August 2023 to 15%. Therefore, when compared to August, the threat landscape is trending away from Asia towards Western nations bringing levels back to baseline behaviour.

The remaining regions feature the undisclosed category which has the equivalent percentage of attacks (19 in absolute figures) as August 2023. This category is characterised by BianLian's tendency to redact company names before they pay the ransom to further pressurise them into paying. Then we have South America equally with 19 attacks and Africa with just 2.

Like the distribution of total attacks for threat actors, where regions are concerned it is similarly a similarly even spread, with the highest contribution being LockBit 3.0's 42 attacks accounting for 22% of North America's total figure and is expected behaviour. The predominant conclusion to be drawn from September's activity, it is that the vast total of ransomware attacks in the month cannot be attributed to just one or two threat actors, but the independent efforts of many.

Threat Spotlight: Ransomed

Overview

A newly identified ransomware group going by the name of RansomedVC (or ransomed[.]vc, Ransomed), whose activity started coming to light in late August 2023, has stirred up a media storm after claiming that they successfully compromised Sony on Sunday 24th September. In this month's spotlight we are going to investigate the group's background and dissect their activity as well as discuss their legitimacy.

Who are Ransomed?

RansomedVC is a newly established ransomware actor that describes themselves as 'penetration testers', similar to another recently identified ransomware group known as 8Base. However, in comparison, Ransomed has also added a slight twist to their extortion method by stating that any vulnerabilities found in their targets' networks would be reported under Europe's General Data Protection Regulation (GDPR). According to the Regulation, two tiers of penalties exist in the case of a breach of GDPR, depending on the severity, with the maximum fine being either up to €20 million or 4% of annual global turnover – whichever is greater. Additionally, the data subjects would also be able to seek compensation for damages. With regards to Ransomed, such threats are intended to apply further pressure on victims to comply with the requested ransom.

There is limited information available for this group at the moment, however, what is currently known is that the group was initially formed as an underground forum in early August. The main focuses were data leaks, access brokerage, and other common cybercrime areas/topics. At the time, the forum was managed by two administrators under the aliases of 'Admin' and 'Yuna'. A credit system was introduced, similar to other underground forums, to encourage members to leak valuable yet undisclosed data; an important requirement to be a member of the forum. It is speculated that the idea behind the forum was to create a community specializing in unauthorized access.

The rest of the spotlight will delve into group's activity, targeting, and the conspiracies surrounding them following their alleged cyberattack on Sony.

nccgroup

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