
nccgroup
Cyber Threat Intelligence Report
JULY 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?

JULY ATTACKS

502

MONTH ON MONTH

+16%

Analyst Comments

July observed new records for ransomware numbers with 502 incidents recorded. This is the highest number of hack and leak cases observed in our database and reflects a continued surge in ransomware attacks across the threat landscape. The data suggests increased interest by ransomware actors and the prevalence of the attack method at present, as such; organisations should pay particular attention to the threat and adopt the appropriate mitigations. Cl0p are largely responsible for the high victim numbers we continue to observe; their continued exploitation of the MOVEit vulnerability led to 171 out of the total 502 global attacks being attributed to the group.

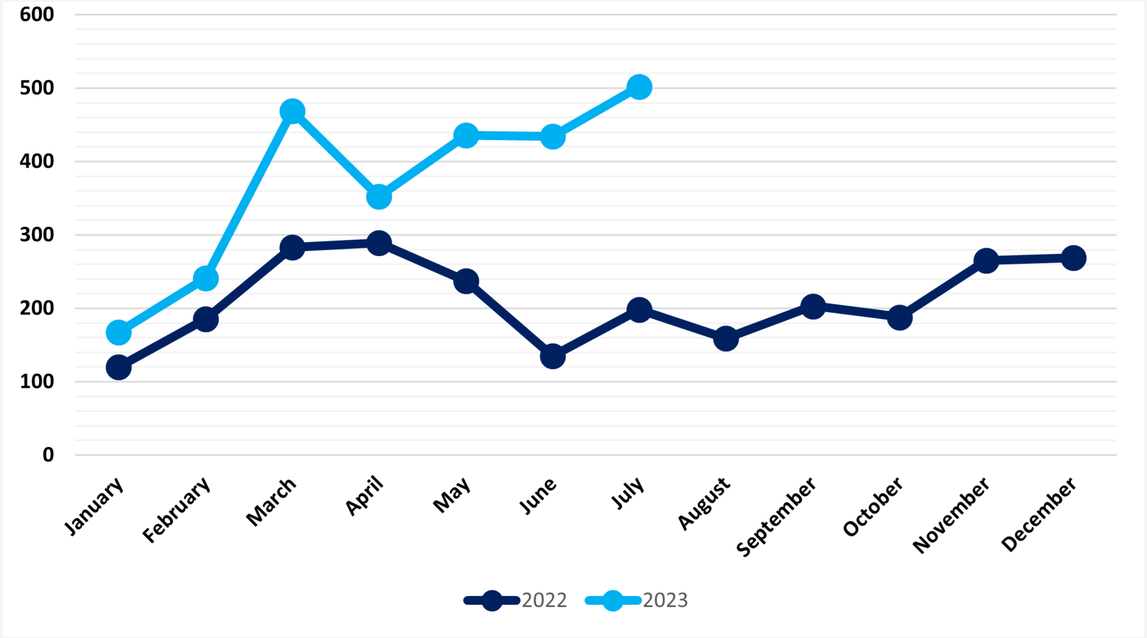

Figure 1 - Global Ransomware Attacks by Month 2022 - 2023

Sectors

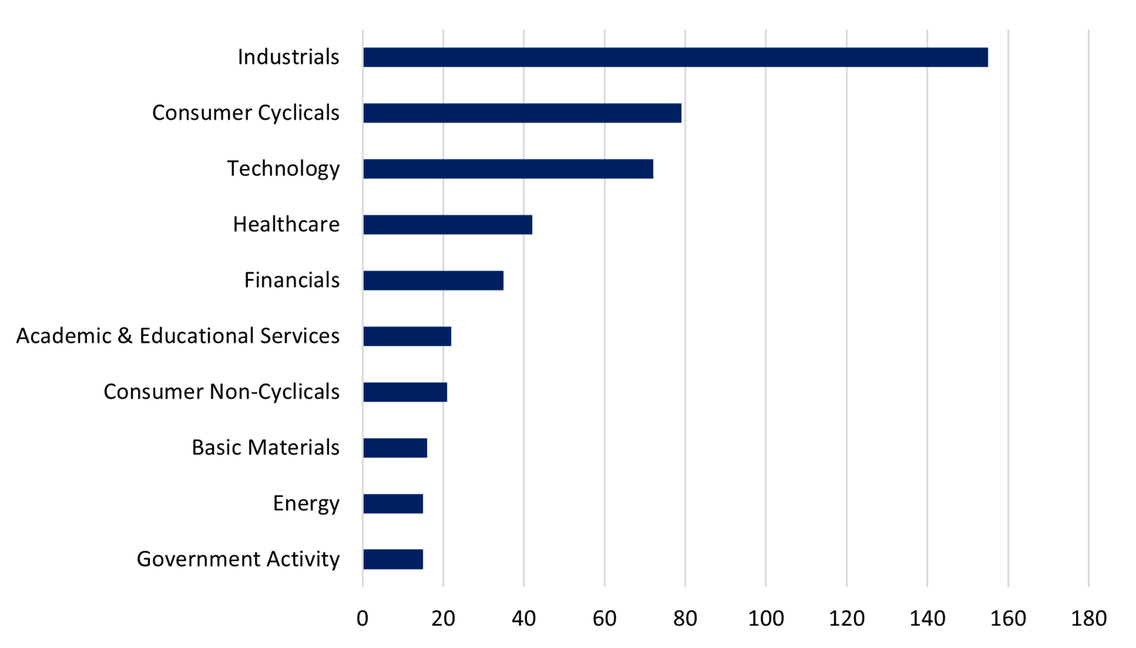

Figure 2 - Top 10 Sectors Targeted July 2023

The Industrials sector continues to be the most targeted, representing 155 (31%) of the 502 attacks. Compared with last month's figures, the sector has experienced an increase of 8% in the attack volume. July also marks the highest number of attacks against the Industrials sector in 2023, while the lowest number of attacks was observed in January (49). Bearing in mind the high number of industries that the sector has within its classification, we would expect that Industrials continue to be of a high priority for ransomware groups in 2023. As touched upon in June's Threat Pulse, businesses within the Industrials sector hold a lot of personally identifiable information (PII) and intellectual property (IP), which remain extremely lucrative targets for threat actors, alongside the potential business disruption that can be further utilized to pressure organisations into paying the ransom.

Threat Actors

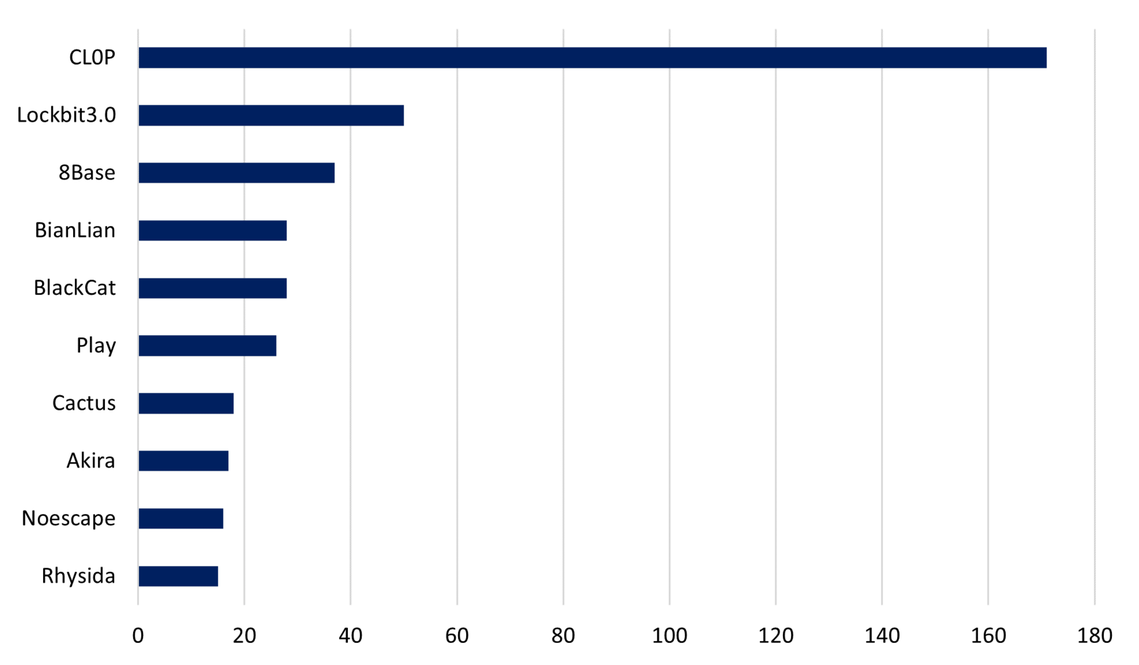

Figure 3 - Top 10 Threat Actors July 2023

With reference to Figure 3, CL0P tops the list of most active threat actors again this month, with 171 attacks, accounting for 34% of all July attacks. With 90 attacks in June, an increase of 190% month on month, Cl0p has significantly increased their activity. This steep increase is down to its successful attacks continuing to use MOVEit flaws, targeting many large, well-known brands. It is notable that this group pursues a specific vulnerability and seeks to consistently exploit it before moving on to novel exploits, differing from other threat actors whose approaches are most consistent.

Researchers believe that in these attacks, instead of relying on encryption, Cl0p is exfiltrating data from victims and then using the threat of leaking this same PII as leverage to extort money. Ransom demands are then made to victims in exchange for the data not being publicly leaked. The strategy of not deploying ransomware is pursued as it can delay detection of their presence and thereby allow them to compromise more victims before they are stopped. To add extra pressure, clearweb sites have been set up to leak this data, making it simpler to disclose the stolen information.

In second place this month is again Lockbit 3.0 with 50 attacks in July representing a decline of 17% compared with 60 attacks in June. LockBit's activity represents 10% of all attacks this month. With attention from law enforcement focused on a high-profile member of this group, it is possible we are seeing a decline in activity since April linked to pressure on the group. However, this group has rebranded and relaunched multiple times and has consistently been amongst the most active threat actors, so this pattern may be part of another reorganisation and restructure for Lockbit 3.0, with a future resurgence possible.

In third, 8Base's attack volumes remain quite stable with 37 in July, a decline of 8% compared to the 40 attributed to this group in June. 7% of this month's attacks are attributed to 8Base.

Looking at the top 10 as a whole, it is worth noting that there are some new entrants to this list. Reinvention and rebranding contribute to this changing landscape, as we have observed with Noescape. With 16 attacks attributed to them, Noescape, believed to be a rebrand of Avaddon, have moved into the top 10 most active groups this month. This accounts for 3% of the monthly 502 attacks in July and a 530% increase from the 3 attacks seen in June 2023. New details for potentially pre-existing groups such as Cactus are also now being identified. Researchers have seen this group focus their activities around VPN related vulnerabilities.

Regions

Unsurprisingly, North America is once again the most targeted region for July, experiencing 274 attacks. This is an increase of 52 attacks from June's figures, or 23%. North America experienced an increase in the proportion of overall attacks as well, with approximately 51% in June and 55% in July. As usual, in second place comes Europe which experienced 143 attacks, an increase of 27, or 23%, over June's figures. Despite this significant proportional increase of attacks, Europe only increased its share of the total global attacks by 2%; from 27%-28%. The third most-targeted region is again Asia, which witnessed a total of 36 attacks in July. This is a decrease of 4 attacks, or 10%, from June's total. Asia's share of the global total fell from 9% in June, down to 7% in July.

The rest of the regions, as is frequently the case, have moved around in the rankings since last month. Oceania experienced 15 attacks, an increase of 6 attacks or 66% over June's figures. Despite this significant proportional increase over last month's experienced attacks, it only increased its share of global attacks by 1%, from 2%-3%, due to the nearly 16% increase of total attacks since last month. Africa experienced 12 attacks, an increase of 3 attacks or 33% over what it experienced in June. Lastly comes South America with 11 total attacks, a decrease of 15, or nearly 58%. This represents only 3% of the global total, compared with 6% last month.

There were also 11 attacks against undisclosed targets, 1 fewer than the 12 we witnessed in June. This is 2% of the monthly total, 1% less than the 3% witnessed in June, and 3% less than the 5% witnessed in May.

It is too early to determine the reason for this continued reduction in undisclosed targets or even whether the trend will continue. One potential explanation could be that victim organisations are being firmer in their refusals to pay ransoms, thus undermining the power TAs attempt to hold over them during ransom negotiations by drip feeding data, and hinting at victim identities, resulting in TAs straight up naming more victims on their leak sites.

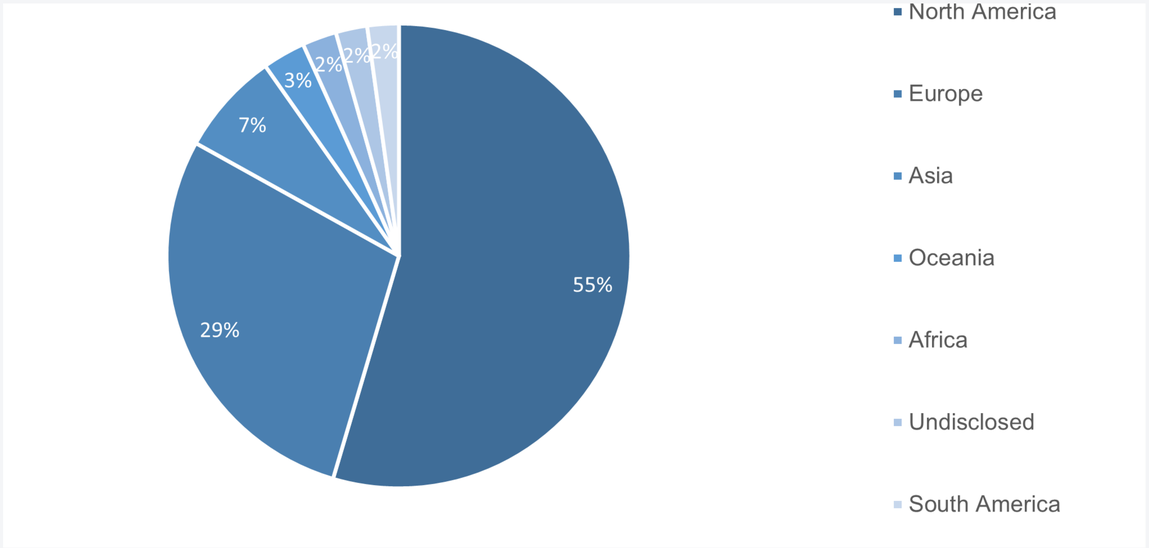

Figure 4 - Number of Ransomware Attacks by Region July 2023

Threat Spotlight

Rising Threats in the Financials Vertical Introduction

The financials vertical is, for obvious reasons, a favourite target for a variety of threat actors, especially those that are financially motivated, from state-sponsored threat groups like North Korea's Lazarus, to prolific Organised Crime Groups such as FIN7 (aka. Carbon Spider). As a result, the threats are sophisticated, dynamic and constantly evolving, making staying one step ahead of adversaries a crucial yet challenging endeavour for financial institutions. To encapsulate this point, we have developed this spotlight on emerging threats within the financials vertical, which are arguably representative of the evolution of cybercrime as a whole, due to the maturity of the Tactics, Techniques and Procedures (TTPs) used within. Therefore, this spotlight not only strives to illustrate the threats to financial institutions to promote proactive defensive action, but should also demonstrate how the wider threat landscape is developing alongside.

nccgroup

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