nccgroup

Cyber Threat Intelligence Report

June 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?

JUNE ATTACKS

434

MONTH ON MONTH

>0.5%

Analyst Comments

The total number of ransomware cases for June 2023 is 434, which is a negligible decrease of less than 1% from the 436 recorded in May 2023. Although these figures are almost identical, June's activity is contrastingly a huge increase of 221% from June 2022, thereby continuing the trend of large year-on-year increases in 2023. Interestingly, 8base ransomware group has managed to maintain its inclusion in the top 3 most prevalent threat actors again in June, and although with a month-on-month decrease of 40%, May's figure included compromises going back as far as April 2022; thereby reducing the significance of this decrease. This therefore perhaps solidifies 8base as a prominent threat actor of note.

Like last month, there have been some new additions to NCC Group's list of ransomware threat actors, though they haven't made it into the top 3. These include Darkrace, Rhysida, and NoEscape, all of which were first spotted in May of 2023. The Darkrace variant is written in C/C++, solely targets Windows machines and, according to some sources, shares similarities with the LockBit 3.0 variant. Rhysida has fewer technical analyses on it, but has experienced considerable media coverage following their leakage of 30% of the documents that they stole from the Chilean Army (360,000 so far). Finally, NoEscape is written in C++ like Darkrace, though it was reportedly built from scratch, and leverages the triple extortion ransomware methodology. This triple extortion mode of operation stems from a special DDoS/Spam service that they offer to affiliates who are imposing a ransom north of USD $500,000 to further pressurise victims into paying.

Perhaps the most significant event that occurred in June was Clop's mass exploitation of the MOVEit vulnerability, which made them the most active threat actor for June and will be touched on in this Threat Pulse's Spotlight.

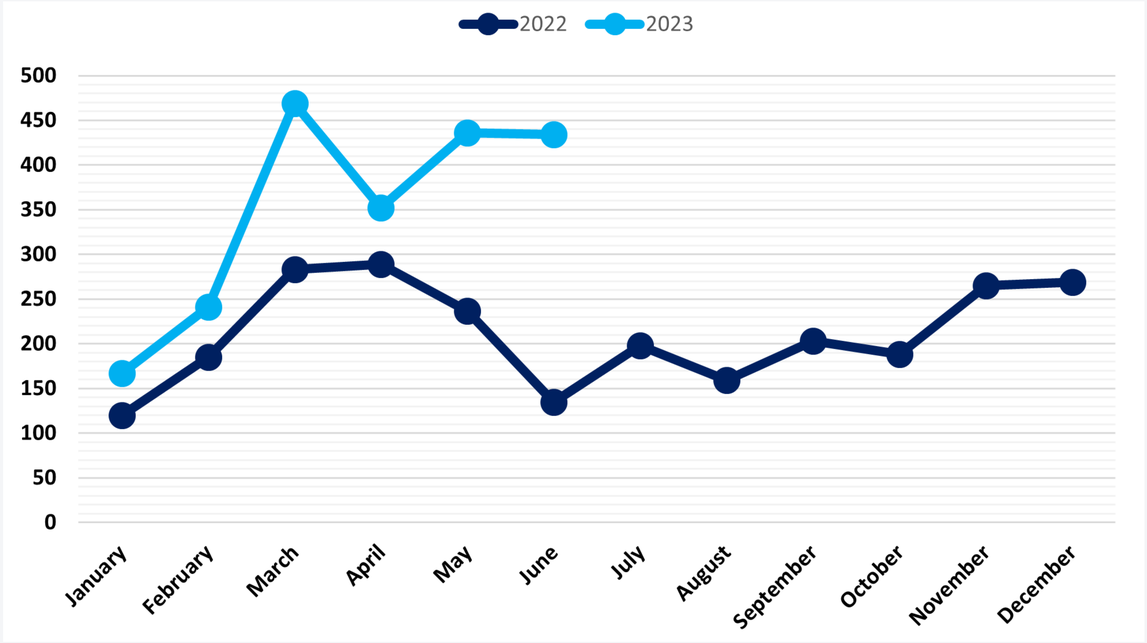

Figure 1 - Global Ransomware Attacks by Month 2022 - 2023

Sectors

The Industrials sector maintains its position as the most targeted sector again in June, representing 143 (33%) of 434 attacks. Comparing with May figures, the sector has seen a slight increase of 9% in the attack volume this month. Given the many varied industries that the sector includes within its classification, it is highly likely that Industrials will remain to be a top priority for ransomware groups for the remainder of the year.

The personally identifiable information (PII) and intellectual property (IP) which businesses within the Industrials sector hold still remain very lucrative targets for threat actors, alongside with the potential business disruption that can be further exploited in order to pressure organisations to comply with the ransom request.

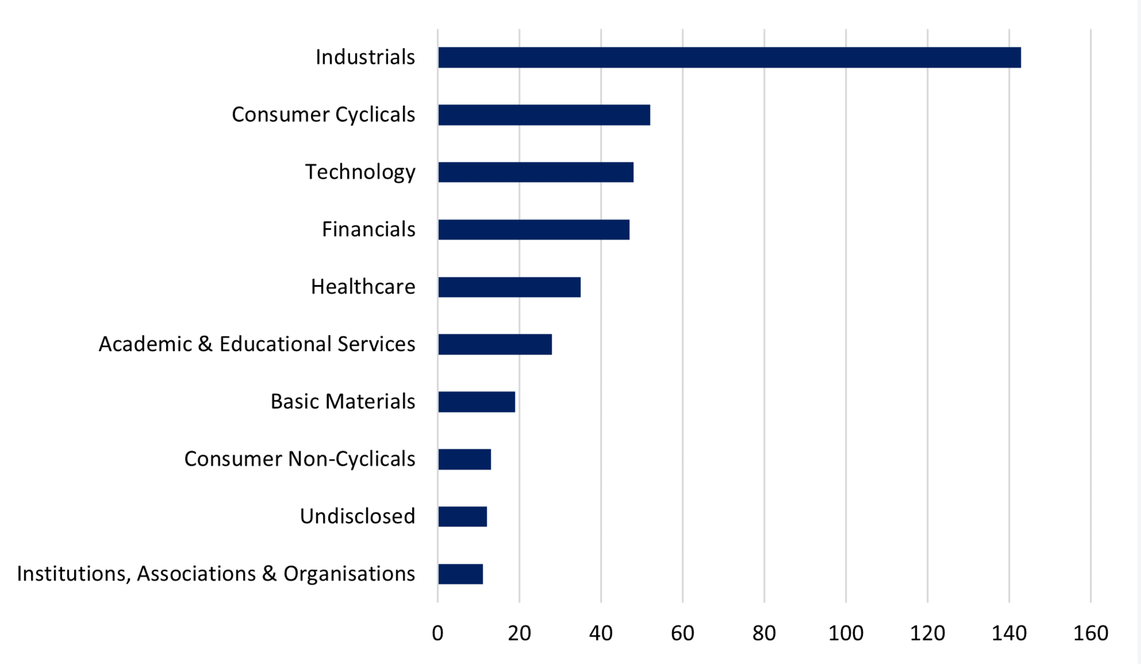

Figure 2 - Top 10 Targeted Sectors June 2023

Threat Actors

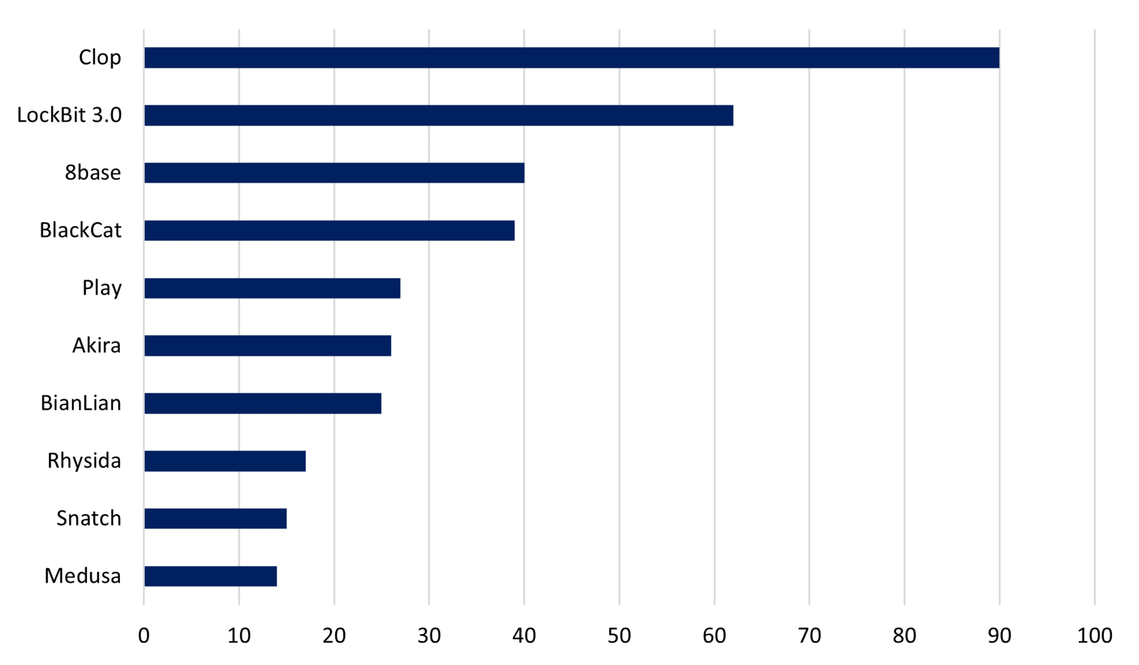

Figure 3 - Top 10 Threat Actors June 2023

Referencing Figure 6, June has seen activity by the group Clop increase significantly, which has shifted LockBit 3.0 into second position for this month. With 2 attacks in May and 90 attributed to this group in June, this is an increase of 4400% month-on-month, accounting for 21% of all attacks this month. This is not, however, as prolific a month for this group as March 2023, where 129 attacks were attributed to this group due to their extensive exploitation of the GoAnywhere MFT vulnerability.

LockBit 3.0 was responsible for 62 recorded attacks this month, a fall of 21% from 78 attacks in May. This has moved LockBit 3.0 from the most active group in May, to second behind Clop. 14% of all attacks recorded in June came from this group.

8base maintained its presence amongst the 3 most active ransomware groups in June, with 40 attacks (9%) this month. With the significant increase in Clop activity, 8base has moved into 3rd most active group. Month-on-month comparison here reveals little, as the count for May 2023 (67) includes attacks from 12 months prior. However, whilst we cannot compare accurately, it is clear this group is significantly increasing its activity.

As mentioned earlier in the report, a new entrant into the top 10 list of most active threat actors this month is newcomer Rhysida, who provide Ransomware-as-a-Service (RaaS), and falling just outside the top 10 threat actor list is Darkrace, responsible for 9 recorded attacks in June.

Nokoyawa had a busy month in May, with 25 attacks (6%) out of 436. In June, however, there were no attacks attributed to this group, perhaps hinting at them focusing on existing ransom negotiations this month, as opposed to amassing further victims.

Regions

North America continues to be the most targeted region to a large extent with 222 (51%) victims operating within that region, which is remarkably the exact same total as May, highlighting the consistent interest displayed by threat actors. In second place is Europe with 116 victims (27%) which is a 3% proportional increase from May and 10 additional victims (9% increase). Although Europe's popularity with threat actors is always moderately volatile, they persist in being second place month-on-month.

There have been slight changes in the remaining regions, with Asia once again taking third position after being overtaken by South America in May, with a total of 40 victims operating within this region (9% of the total). South America has therefore moved back down to 4th place with 26 victims (6%) and, based on previous months, it would be unsurprising to see them remain there for the foreseeable future, leaving May as an anomaly.

There were fewer undisclosed victims in June with 12 (3%) which is a 2% proportional decrease from May. The majority of these victims were attacked by BianLian who use the redaction of their victims' names to further pressure victims into paying the ransom through the looming threat of reputational damage, with one being attributed to an unnamed ransomware group who have only amassed 5 victims in 2023 thus far.

Finally, in joint sixth place is Oceania and Africa with 9 victims (2%) each, which is largely similar for both regions when compared to May's total figures (11 and 10 respectively).

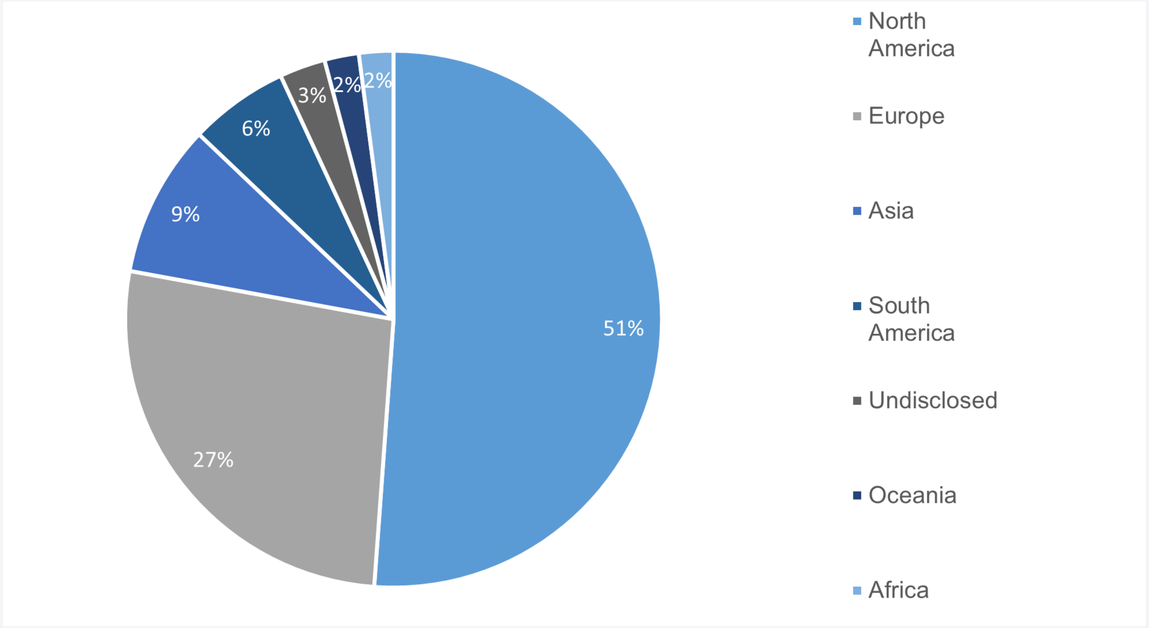

Figure 4 - Ransomware Cases by Region June 2023

Threat Spotlight

Clop and the MOVEit Vulnerability

Over the last years, Clop has built a reputation to still be one of the original cybercrime groups to be active under their trusty name. Even through interruptions by International Law Enforcement, Clop have shown that they are still in the game, and continue to be a big threat for many organisations out there; without needing to deploy ransomware.

Clop have shown that they are able to adapt to the changing Cyber Threat Landscape and make the exploitation of managed file transfer (MFT) software packages/appliances their new modus operandi. Over the last two years, Clop has abused four vulnerabilities in appliances that would either lead to the deployment of Clop ransomware or the exfiltration of victim organisation's data.

MOVEit exploitation

On the 31st of May 2023, the company Progress released a security advisory about a vulnerability in the MOVEit Managed File Transfer (MFT) software package. This vulnerability, at the time of the publication a 0-day, has been abused to compromise MOVEit MFT servers and exfiltrate data. The vulnerability is currently tracked as CVE-2023-34362.

nccgroup

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