
nccgroup
Cyber Threat Intelligence Report
MAY 2023

Contents

nccgroup

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?

MAY ATTACKS

436

MONTH ON MONTH

+24%

Analyst Comments

This month's total victim count is 436, increasing by 24% as compared to April. Continuing the trend, May's total remains higher than its 2022 counterpart, as has been the case with every month this year. However, this month's total is boosted by a rather unusual event; the inclusion of 67 8base victims which were breached between April 2022 and May 2023. The working theory is that they have only recently begun publicizing their victim's data. It's important to note that the data used in the Threat Pulse is based on the date of victim discovery, not the date of initial publication or data breach. Even when excluding the 8base attacks, May's numbers this year are 56% higher than those in May 2022, and a small 5% higher than April 2023. For the remainder of the Threat Pulse, the 8base victims will be included in the analysed dataset.

This month saw activity from new ransomware groups like BlackSuit, MalasLocker and RAGroup, each with their own interesting characteristics. BlackSuit is thought to be Royal's – the direct successor of Conti – new encryptor, with rumours circulating about a group rebranding. MalasLocker, dubbed the Robinhood of ransomware, imposes a donation to an approved non-profit on its victims instead of a more traditional for-profit ransom. RAGroup's encryptor is based on the Babuk source code, which was leaked in full in 2021. These groups highlight the persistence of ransomware groups following infrastructure take-downs or dissolution, as well as the emergence of ransomware operations combined with activism, potentially expanding on the hacktivist term.

Nokoyawa – another Babuk spin-off - compromised only one known victim in 2023 but has jumped to 25 this month. Though not establishing themselves as a leader in absolute numbers, their victim-count skyrocketed 2400% from January. It remains to be seen if they can sustain this volume going forward, or if this month is an outlier.

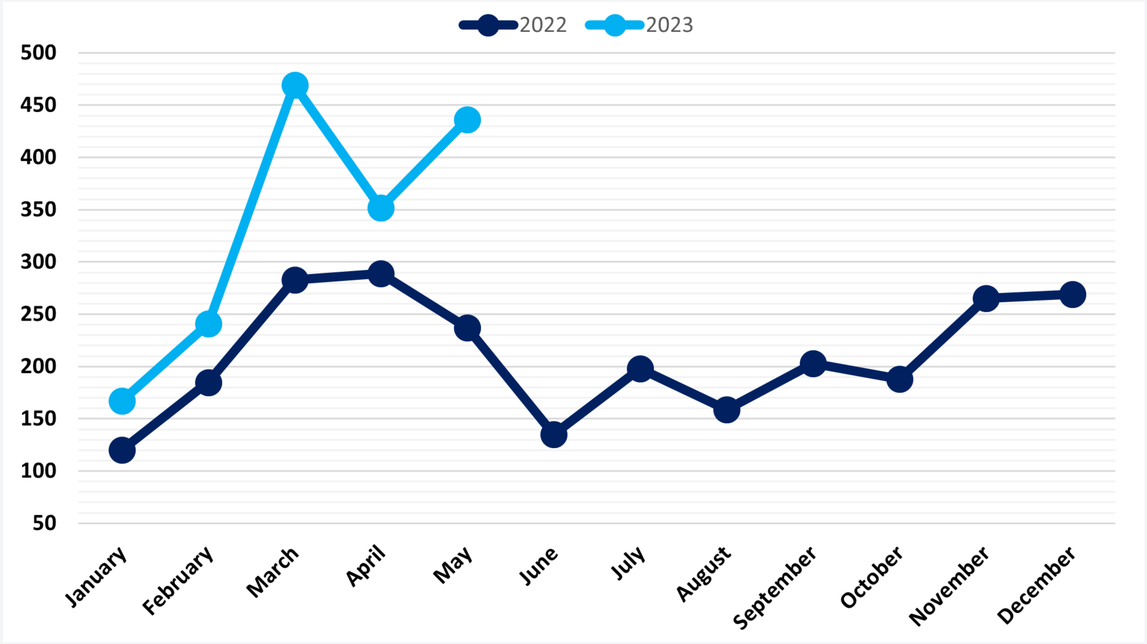

Figure 1 - Global Ransomware Attacks by Month 2022 - 2023

Sectors

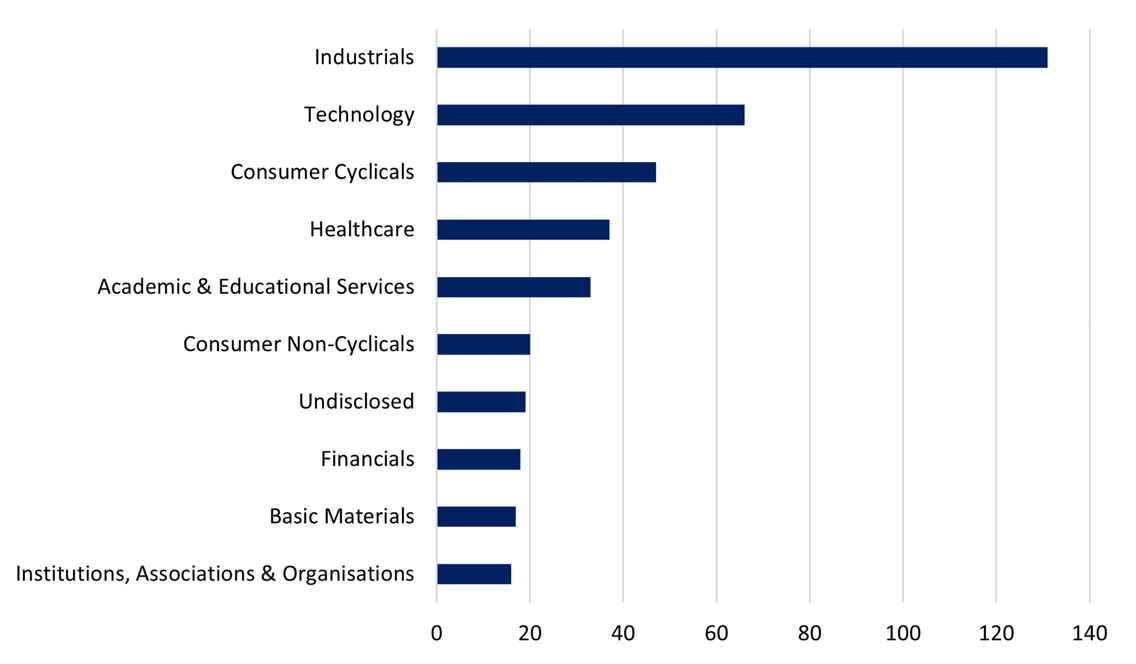

Figure 2 - Top 10 Targeted Sectors May 2023

Industrials

The Industrials sector remains the most targeted of all again this month, representing 131 or 30% of 436 attacks in May. There has been a slight increase in attack volume for this sector month on month, seeing a 14% increase from 113 in April to 131 in May. Last month's relative weighting of Industrial-focused attacks remains stable with this month's, with only a 2% proportional difference between the two. As the sector including the largest number of industries within its classification, it is likely that Industrials will remain the most popular target for ransomware attacks in future. Compared with May 2022, which saw 72 attacks, the 131 seen in May 2023 represents an increase of 82%, which supports this assertion. As the personally identifiable information (PII) and intellectual property (IP) held by businesses within this sector remain lucrative for criminal actors, the sector continues to be a popular target. Business disruption can also be used as a pressure point to encourage organizations to pay ransoms. Maintaining strong cyber defences and protections will continue to be a requirement for businesses within this sector, particularly in light of the continued focus for ransomware actors.

Figure 3 details the industries targeted in May 2023 within the Industrials sector. Most targeted continue to be businesses within Professional & Commercial Services with 72, or 55% of those attacks in May. Comparatively, the attacks in April against this same industry accounted for only 40 (or 35%) of all cases in the Industrials sector. The relative increase in weighting towards this industry in May is in part due to the reduced share of attacks against Freight & Logistics Services, with 12 in April and 4 in May, a decrease in volume of 66%. Machinery, Tools, Heavy Vehicles, Trains & Ships industries similarly saw a decrease in attacks in May, falling 20% from 36 to 29 attacks from April.

The Construction and Engineering industry is the third most active grouping targeted, with an increase of 22% in attacks month on month. There were 18 attacks in April within these industries, and 22 in May.

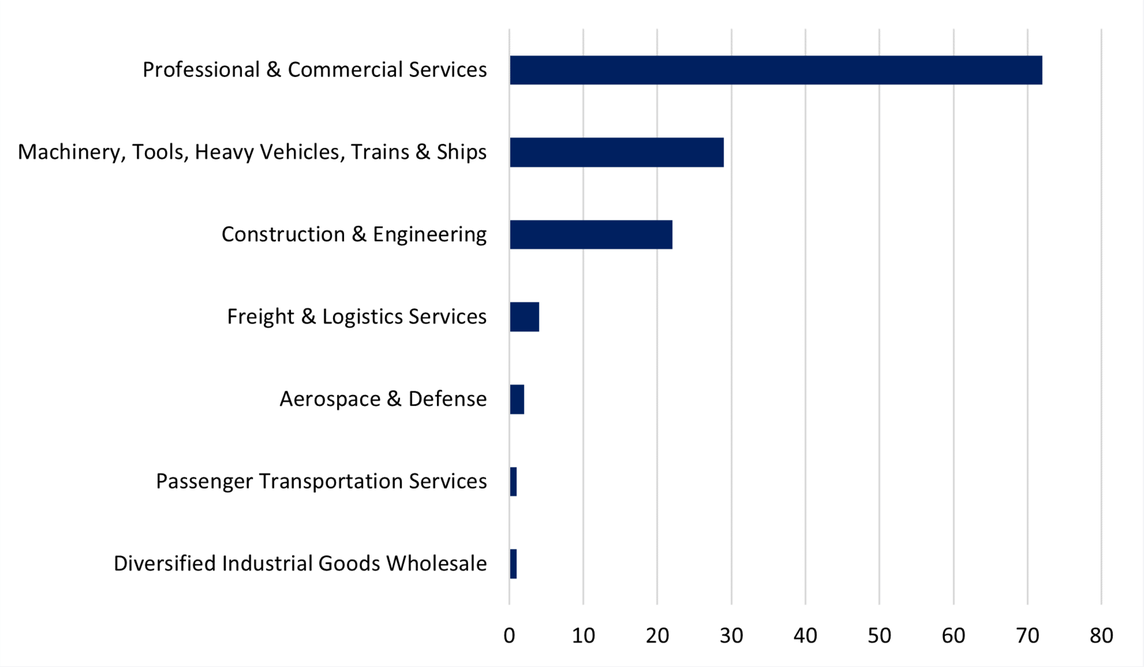

Figure 3 - Industries Targeted within the Industrials Sector May 2023

Technology

May saw the Technology sector move up in relative standing when looking at absolute numbers month on month. 15% or 66 of all attacks in May fell within the Technology sector. This is a 78% increase in attack volume for the Technology sector from April's 37 attacks.

Figure 4 shows that Software & IT Services remains the significant volume driver of attacks in this sector, with 76% or 50 of 66 attacks in May. In April, 25 attacks were attributed to Software & IT Services reflecting a 100% increase in May's 50, a significant increase coming from attacks attributed to Play. With similar volumes of attacks for all other industries within the Technology sector, Telecommunications and Communications & Networking industries saw little change month on month. There were 5 attacks within Telecommunications Services during May, which is a 150% increase on the 2 attacks seen in April. Communications & Networking saw 4 attacks in May, up from the 3 attacks seen in April.

This is a sector which continues to be a focus of attack, given not only the potential to access intellectual property, but also due to single attack vectors which allow criminals who can compromise supply chains to leverage access to multiple organisations. This therefore poses a risk of data exfiltration and extortion, making strong security protections a continued priority for businesses within the sector.

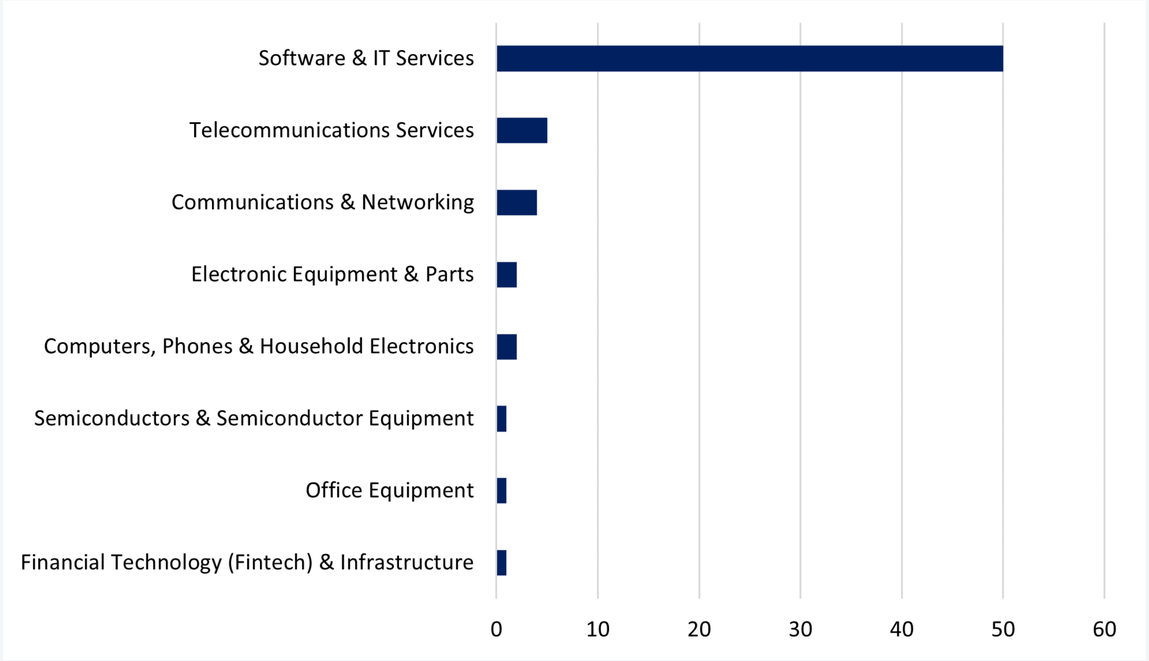

Figure 4 - Industries Targeted within the Technology Sector May 2023

Consumer Cyclicals

47 of the total attacks in May fell under the Consumer Cyclicals umbrella, representing an 11% share of all attacks that month. April 2023 saw 39 attacks of 352 that month, showing a 21% increase in attack volume month on month. As Technology sector focused attacks saw a significant uptick in May, Consumer Cyclicals moved down from 2nd to the 3rd most targeted sector.

Referencing Figure 5, Hotels & Entertainment Services moved up to the top industry category for targeting this month, with 10 attacks out of 47, representing 21% of all those within Consumer Cyclicals. In April, this category saw 3 out of 39 attacks, making this 8% of the overall total number. Speciality Retailers, which in April had attracted the most attacks – 23% or 9 out of 39 – accounted for 8% of May's number, making this a far less significant target this month.

8 attacks fell within Automobiles & Auto Parts in May – 17% of all Consumer Cyclical attacks. Compared with April, there was an increase of 33% from 6 to 8 attacks. Textiles & Apparel accounted for 15% or 7 attacks in May, which was a 40% increase from 5 attacks seen in April.

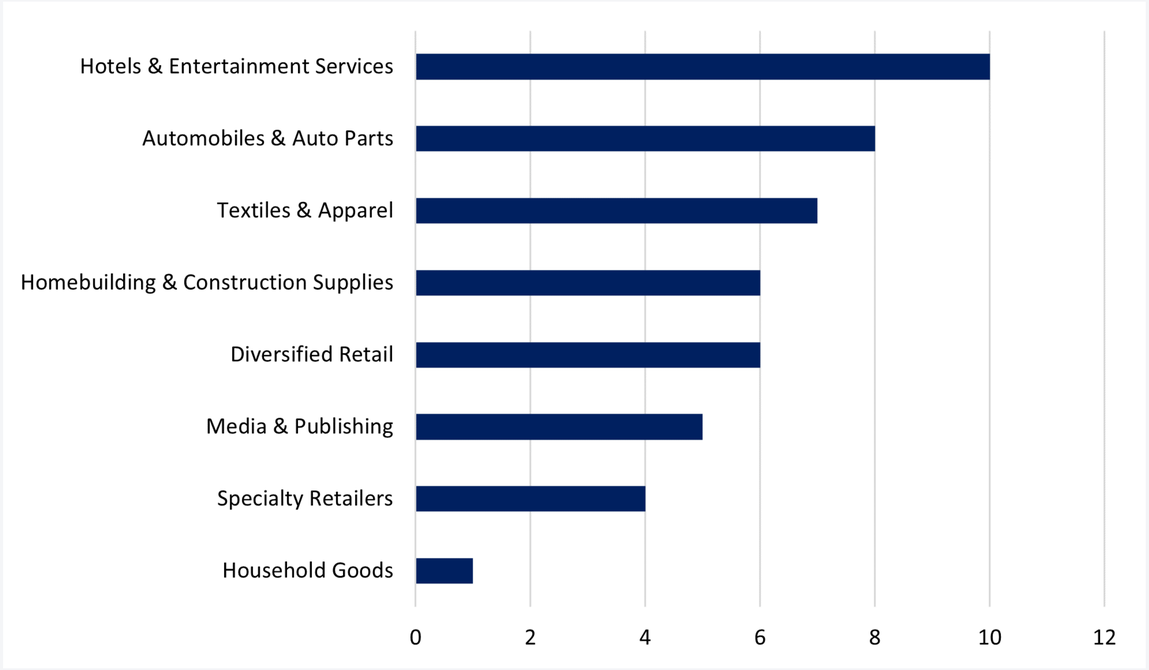

Figure 5 - Industries Targeted within the Consumer Cyclicals Sector May 2023

Threat Actors

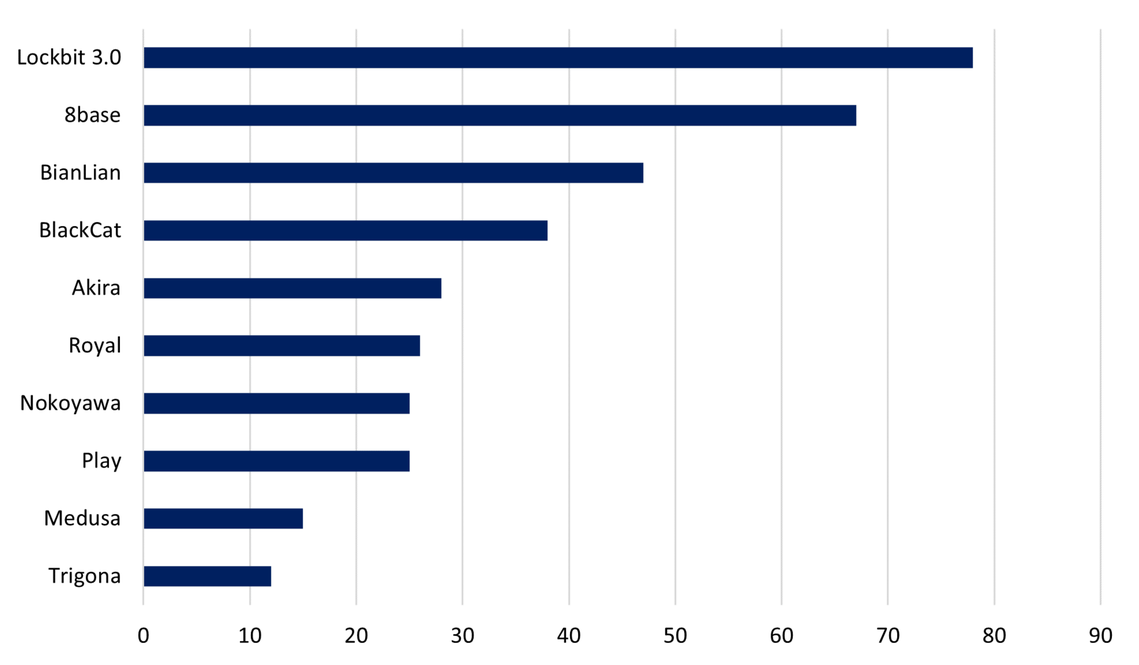

Figure 6 - Top 10 Threat Actors May 2023

The three most active threat groups in May are Lockbit 3.0, the newcomer 8base, and BianLian, the combined total of which gives 192 out of the 436 attacks recorded throughout the month, which represents a total of 44% of the overall activity across the threat landscape. The top three's activity is broken down as follows: Lockbit 3.0 maintains their position as the most active threat in May, recording 78 cases or 18% of the overall activity, followed by 8base with 67 cases or 15%, and last, but not least, BianLian with 47 cases or 11%.

Interestingly, April's second most active threat - BlackCat - has decreased their activity by 24% in May, accounting for only 9% (or 38 attacks) of the overall output. As a brief reminder, BlackCat was responsible for 50 out of 352 attacks in April (or 14% of the overall output). Such a decrease in activity means that the threat group has moved down to fourth position, which was also the position they held in March.

It is worth mentioning that April's tenth-ranked threat actor, Akira, has significantly increased their activity by 250% in May. This increase represents 6% of the overall output in May in comparison to 2% in April and has moved the threat group up to fifth position. Another interesting difference is that Akira did not seem to have a distinct industry preference in April, however the most targeted industries by them in May are Professional & Commercial Services; Schools, Colleges & Universities; and Institutions, and Associations & Organisations, accounting for 42% of their overall activity throughout the month. At this point in time, it is difficult to tell whether Akira will continue to increase their activity month on month for the remainder of the year, or if this is temporary momentum.

LockBit 3.0

Lockbit 3.0 unsurprisingly remains in their spot as the most active threat actor in May with the 78 (18%) events recorded. However, the group's overall output has decreased by 27% in comparison to April, when Lockbit 3.0 was responsible for 107 out of the 352 events, or 30% of the overall activity in that month.

It is worth mentioning that the threat group's overall output has fluctuated since the beginning of 2023 and May's total numbers represent the second lowest monthly activity for the threat actor. So far, the lowest monthly activity for the group was observed in January with 50 out of 165 attacks, while the highest monthly activity was recorded in February with 129 out of 240 attacks. Regardless of the fluctuation in overall attack numbers, the threat actor is highly likely to continue being relentless in their targeting throughout the remainder of the year.

Sectors

Consistent with the targeting pattern that has been observed since the beginning of the year, except in the month of February, Lockbit 3.0's victims were mainly spread across the usual three sectors: Industrials 36% (28), followed by Consumer Cyclicals 14% (11), and finally Technology 13% (10), as shown in Figure 7. In other words, the three most desired sectors contributed to 63% of the threat actor's activity in May. It is highly recommended that organisations within these three sectors continue to stay vigilant, enhance their awareness of the group's TTPs, and last but not least, strengthen their defensive mechanisms accordingly.

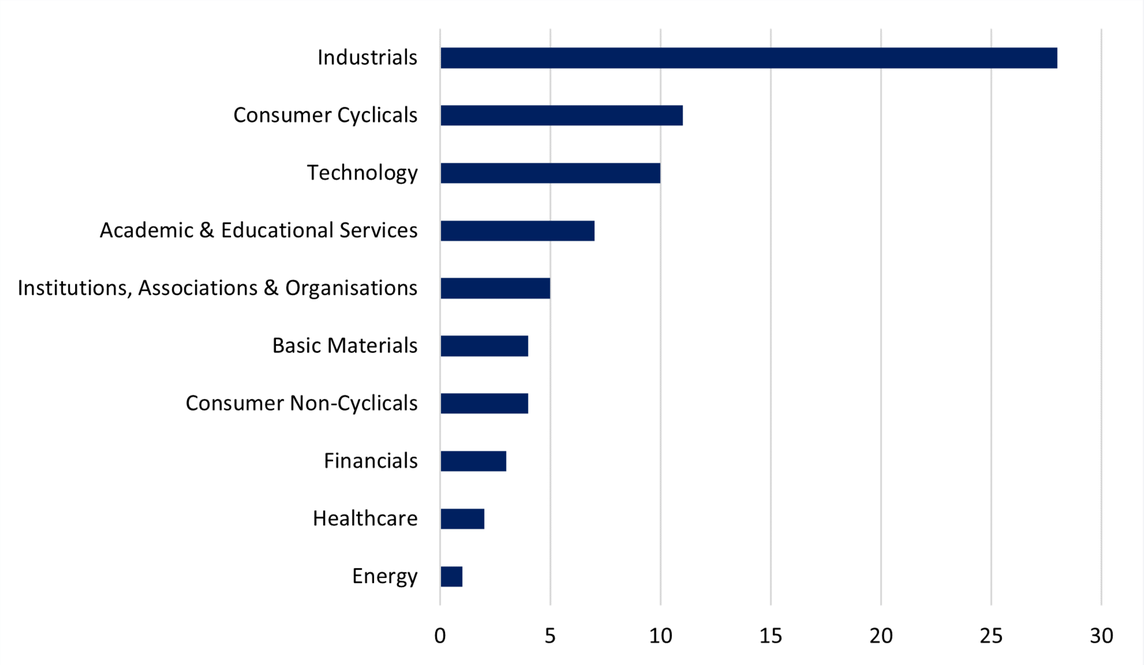

Figure 7 - Sectors Targeted by Lockbit 3.0 May 2023

Industries

From an industry perspective, the attacks are spread across a total of 26 industries in May with the most targeted one being Professional & Commercial Services 22% (17), representing a 42% increase in comparison to April's figures. Lockbit 3.0's attacks against Professional & Commercial Services also account for 4% of the overall activity in May.

The other two highly targeted industries are Schools, Colleges & Universities 9% (7) and Machinery, Tools, Heavy Vehicles, Trains & Ships 8% (6), as shown in Figure 8.

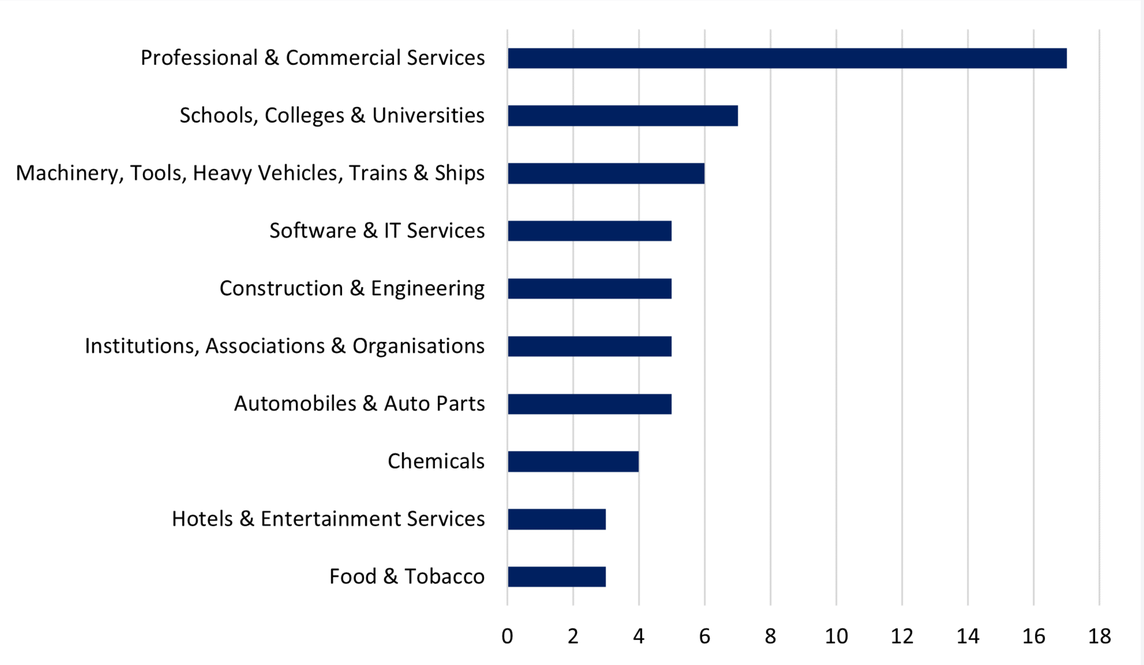

Figure 8 - Industries Targeted by Lockbit 3.0 May 2023

8base

A new ransomware player identified as 8base, not only made it into the top ten most active groups in May, but also took the second position accounting for 15% (67) of the monthly output.

The group is in favour of the double extortion strategy by stealing and encrypting victims' data. In cases where the victims refuse to comply with their demands for a ransom, the stolen data is published on the threat group's leak site. It is also interesting that 8base has very specific 'terms of service' with a section focusing on the involvement of any third parties. The terms clearly outline that the involvement of third parties is prohibited.

The victims list can also be tracked to April 2022 indicating that the threat actor has been actively operating without publicly disclosing their victims for about a year.

Geographically, the majority of the group's victims fall within the following regions - North America 39% (26), Europe 25% (17), and South America 22% (15). The three regions account for 86% of the group's output with the most targeted countries being – United States 34%, followed by Brazil 18%, and last but not least, United Kingdom and Germany with 7% each.

Sectors

As captured in Figure 9, a distinct favourite within the sectors seems to be Industrials accounting for 52% (35) of the group's overall activity.

The top five most targeted sectors also include - Consumer Cyclicals, Technology and Consumer Non-Cyclicals each adding 9% (6); and Healthcare adding 7% (5). In other words, the top five account for 87% of 8base's activity however, given that this activity has taken place between April 2022 and May 2023, it is unclear whether the threat actor will be able to reach and maintain this volume of activity in the coming months.

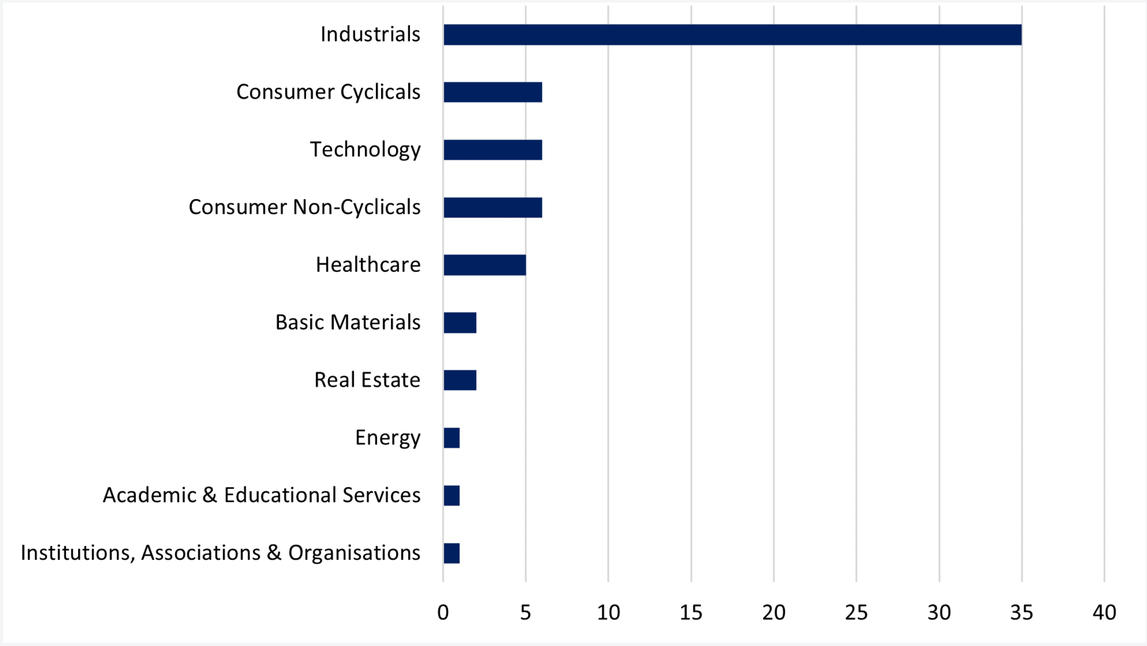

Figure 9 - Sectors Targeted by 8base

Industries

The group's activity from an industry perspective is spread across a total of 24 industries with the most targeted ones residing in the Industrials sector unsurprisingly - Professional & Commercial Services 31% (21), Machinery, Tools, Heavy Vehicles, Trains & Ships 10% (7) and Construction & Engineering 7% (5). In total, the top three industries account for 49% of the group's overall output.

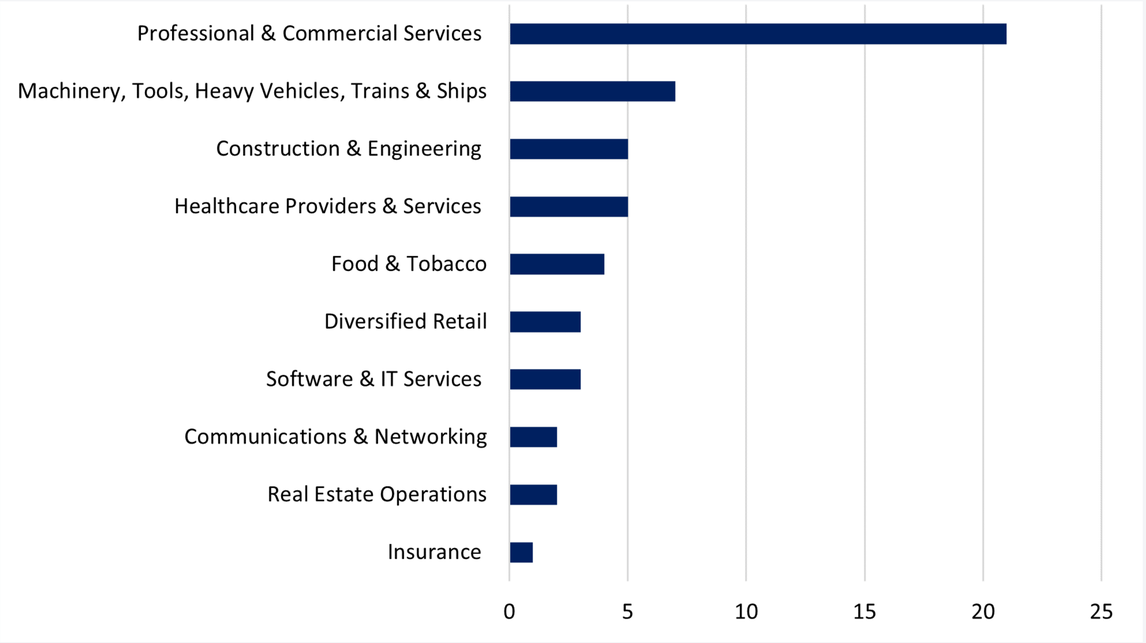

Figure 10 - Industries Targeted by 8base May 2023

BianLian

Following suit from April, BianLian is placing third, accounting for 11% (47) of the cases recorded in May, which represents a 2% increase on last month's figures. This is the first time since the beginning of the year in which the threat actor has held third position in the top ten in two consecutive months.

In 2022, BianLian's pattern of activity fluctuated, with some months placing within the top three and other months not even making it within the top ten. In 2023, the threat actor's activity has been steadily rising month on month as follows – January 5 (3%) cases, February 20 (8%) cases, March 29 (6%) cases, April 46 (13%) cases and May 47 (11%) cases. However, it is difficult to predict whether the threat actor would be able to maintain consistent threat levels in the coming months or repeat last year's pattern.

Sectors

Within the defined sectors, Healthcare is observed to be the top target accounting for 21% (10) of all of BianLian's attacks, which represents a 400% (from 2) increase since April. Industrials targeting accounts for 11% (5) of the attacks this month, representing a 55% (11) decrease compared to last month's figures.

It is notable that 40% (19) of BianLian's attacks in May were focused on the 'Undisclosed' sectors, a category defined by NCC Group which represents how the threat actor conducts their targeting. The group tends to hide their victims' names when an announcement is posted on their extortion site, and offers them approximately ten days to comply with the required ransom.

There seem to be cases in which the threat actor has made references to specific legislation applicable to the victim's region, highly likely to apply further pressure on the victim to cooperate with the demands.

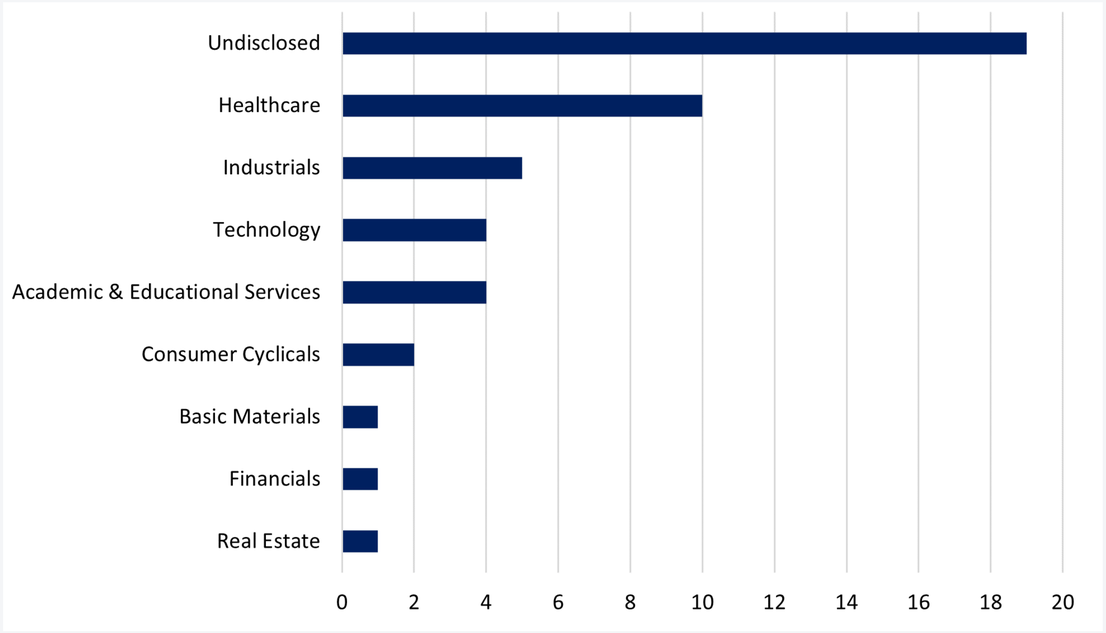

Figure 11 - Sectors Targeted by BianLian May 2023

Industries

Unsurprisingly, BianLian's May activity mainly falls within the 'Undisclosed' category with 40% (19). It is possible that more will be understood about the victim profiles of this group with retrospective analysis, if full details are leaked.

Of the remaining 28 attacks with identifiable victims, the most targeted industries by the group are Healthcare Providers & Services with 15% (7), representing a 600% (1) increase on April's figures; and Software & IT Services with 9% (4), representing a 300% (1) increase on April's figures.

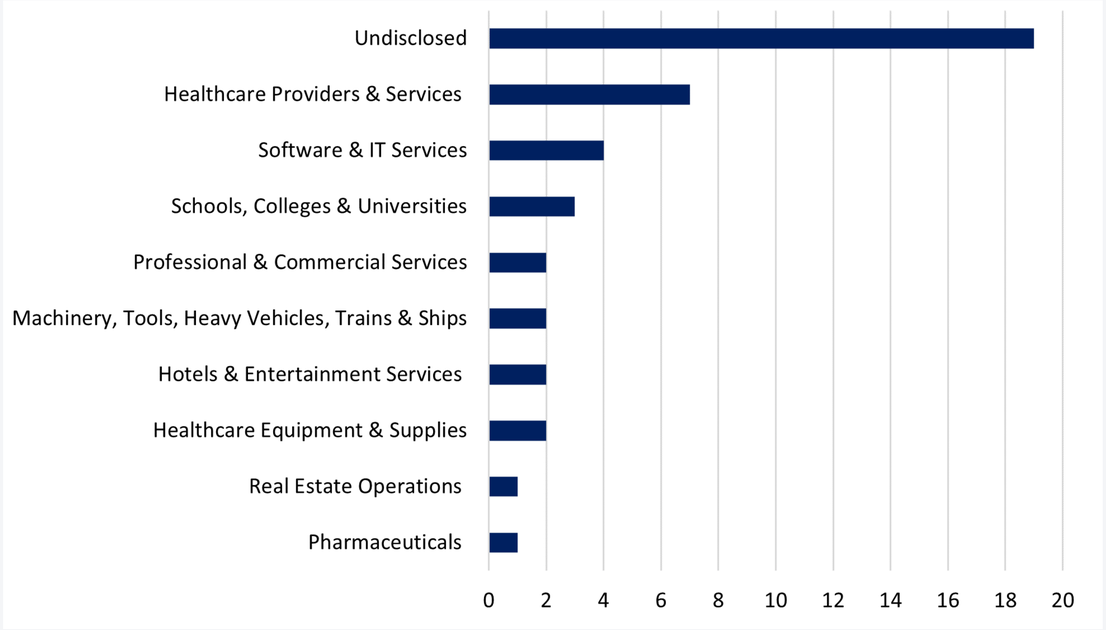

Figure 12 - Industries Targeted by BianLian May 2023

Regions

North America and Europe remain the top two most targeted regions, and their relative victim count is similar to that of April. North America experienced a small increase from April, rising to represent 51% (222) and Europe remained at 24% (106) of the total attacks (436).

Looking past the top two, some significant changes may be observed. First, South America has seen a notable increase in victims, coming in as the third-most targeted region with 8% (34) of the total, compared to 5% (18) in April, an 89% increase of total victims. However, this increase is almost entirely due to 8base publishing 15 South American victims in May.

In absolute numbers, Asia has remained quite stable, with 33 attacks in May compared to 34 in April. Given the higher number of total attacks, this represents 2% less than last month with 8% of the total attacks in May.

There was more clarity into the regions attacked due to there being fewer Undisclosed victims. In both April and May, the main contributor to the number of Undisclosed victims was BianLian, where in April 56% (26) of their victims couldn't be classified. In May, 38% (18) of the victims weren't classified and therefore marked as Undisclosed, representing a 31% reduction.

Finally, Oceania and Africa each saw 2% of the victims in May, with 11 and 10 attacks each. Though Africa has remained stable, with only 1 fewer attack when compared to April, Oceania has seen a significant increase from April's 5 attacks. This marks a 120% increase in victims for countries in Oceania.

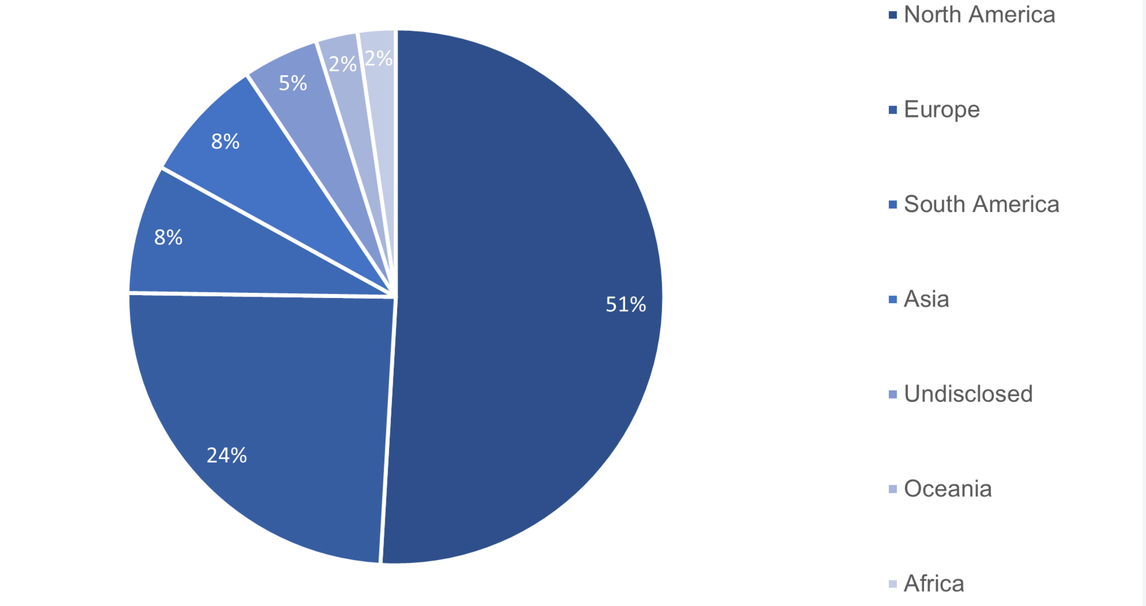

Figure 13 - Ransomware Cases by Region May 2023

Threat Spotlight

From ERMAC to Hook: Investigating the Technical Differences between Two Android Malware Variants

Hook and ERMAC are Android based malware families that are advertised by the same actor who goes by the nickname "DukeEugene". Hook was first announced at the start of 2023, with the actor claiming that it was written from scratch. ThreatFabric researchers have stated that the majority of the code base in Hook is the same as in ERMAC. In our research, we have analysed two samples of Hook and two samples of ERMAC in an effort to further examine the technical differences between these malware families.

After our investigation, we concluded that the ERMAC source code was used as a base for Hook. All of the commands (30 in total) that the malware operator can send to a device infected with ERMAC malware, also exist in Hook. The code implementation for these commands is nearly identical. The main features in ERMAC are related to sending SMS messages, updating and starting injections (to display a phishing window on top of a legitimate app), extracting a list of applications, SMS messages and accounts, and automated stealing of recovery seed phrases for multiple cryptocurrency wallets.

Hook has introduced a lot of new features however, with a total of 38 additional commands when comparing the latest version of Hook to ERMAC.

The most interesting new features in Hook are: streaming the victim's screen and interacting with the interface to gain complete control over an infected device, the ability to take a photo of the victim using their front facing camera, stealing of cookies related to Google login sessions, and the added support for stealing recovery seeds from additional cryptocurrency wallets.

Hook had a relatively short run. It was first announced on the 12th of January 2023, and the closing of the project was announced on April 19th, 2023 due to "leaving for special military operation". On May 11th, 2023, the actors claimed that the source code of Hook was sold at a price of $70,000. If these announcements are true, it could mean that we will see interesting new versions of Hook in the future.

nccgroup

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