nccgroup

Monthly Threat Intelligence Report

Media Edition

MARCH 2023

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?

MARCH ATTACKS

459

MONTH ON MONTH

+91%

Analyst Comments

In our previous Threat Pulse, NCC Group touched upon the fact that we had seen the highest number of ransomware hack & leak cases for both January and February in the past 3 years, and this observation has continued into March. In fact, March's ransomware victim numbers are the highest of any month in the past three years, highlighting an enormous surge as visualised in Figure 1. February to March 2023 exhibited a 91% increase from 240 attacks to 459; this also illustrates a 62% increase, year-on-year, when compared to March 2022.

NCC Group have assessed that the cause of this dramatic incline is likely associated with the highly publicised GoAnywhere MFT vulnerability being exploited across the threat landscape. CL0P, who were the most active threat actor in March, are known to have widely exploited this vulnerability, resulting in a huge soar in their victim numbers. CL0Ps' recent surge in activity and their modus operandi will be discussed in depth in the Threat Spotlight of this report.

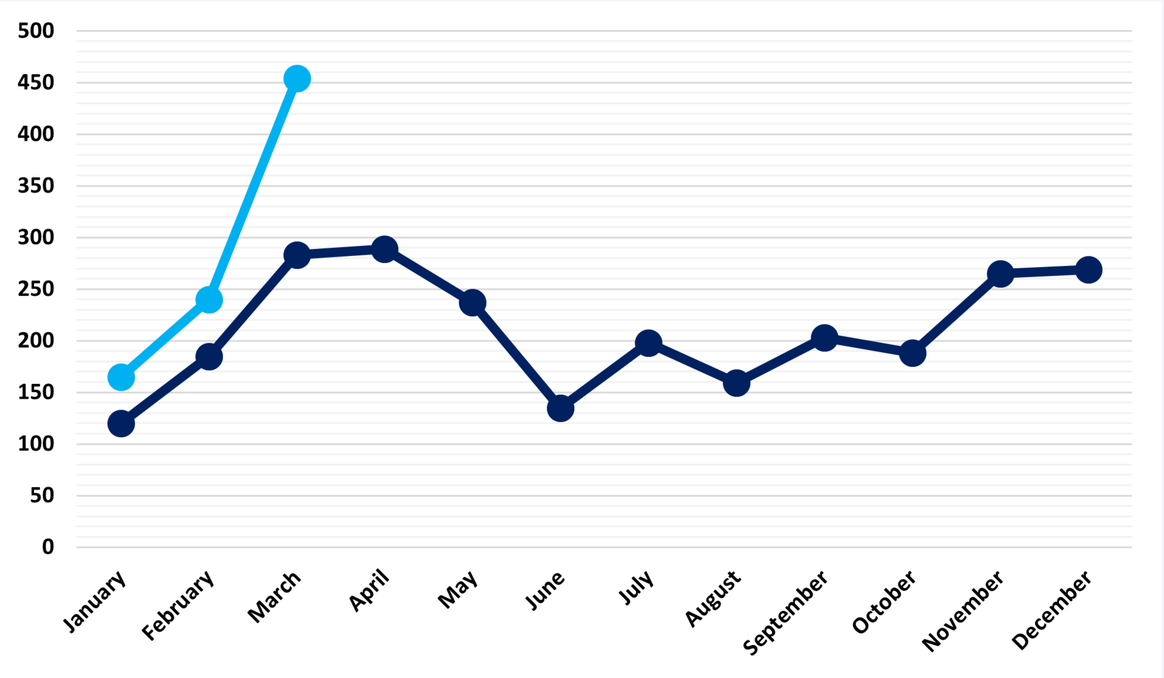

Figure 1 - Global Ransomware Attacks by Month

Sectors

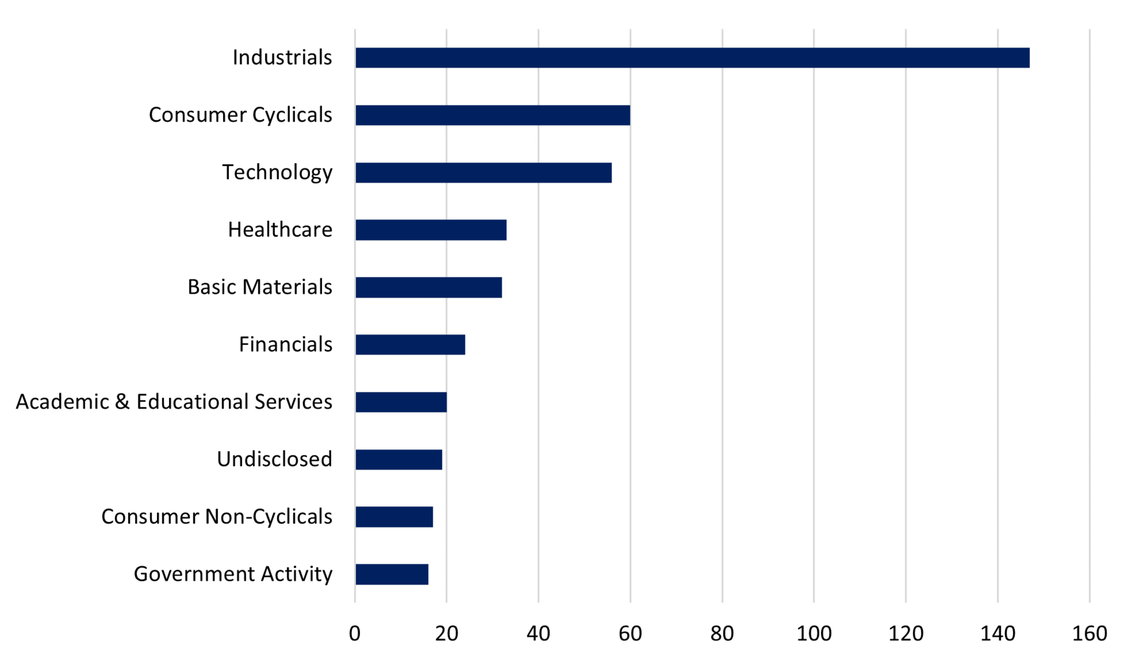

Figure 2 - Top 10 targeted sectors March 2023

Industrials

The most targeted sector in March 2023 was Industrials with a significant 147 attacks out of 459, accounting for 32% of the total. In terms of total figures, this is an increase of 67 attacks (84% increase) but a miniscule proportional decrease of 1%, showing that irrespective of the dramatic increase of victims this month, the relative targeting remains largely similar. This will likely continue to be the case for the majority of 2023 for the same reasons that we have mentioned previously; Industrials contains possibly the widest variety of industries that provide threat actors with opportunities to extort PII/IP, and cause operational disruption to incentivise ransom payments.

As illustrated in Figure 3, Industrial's most targeted industry was Professional and Commercial Services with 66 of the total cases (45%), followed by Machinery, Tools, Heavy Vehicles, Trains and Ships with 34 (23%), and finally Construction and Engineering with 22 cases (15%). When compared to February's figures, victims in Professional and Commercial Services have increased by 36 in total figures (120%), Machinery, Tools, Heavy Vehicles, Trains and Ships by 19 (127%), and Construction and Engineering by 3 (16%).

This is highly similar to February, during which the most targeted industry was Professional and Commercial Services, followed by Construction & Engineering, and Machinery, Tools, Heavy Vehicles, Trains and Ships. The targeting of industries within this sector is therefore mostly consistent, with minor fluctuations between the top 3 most targeted industries. Although, the most targeted usually is, and will likely continue to be, Professional and Commercial Services. In conclusion, organisations residing within this sector should consider their attack surface in relation to common ransomware group TTPs.

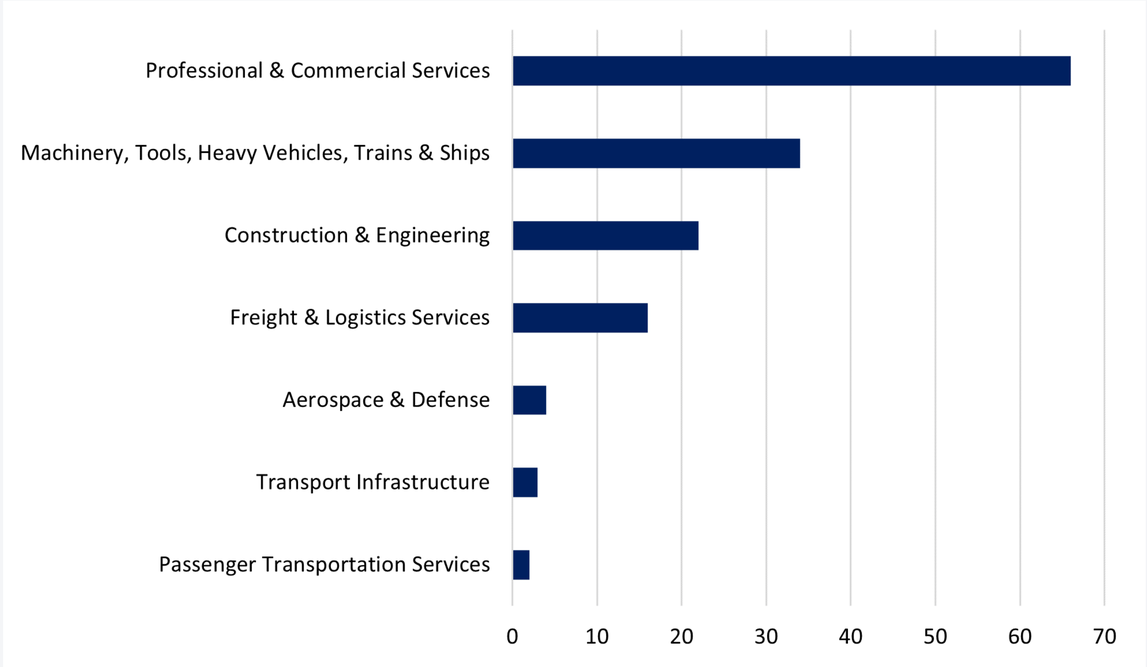

Figure 3 - Industries Targeted within the Industrials Sector March 2023

Consumer Cyclicals

Consumer Cyclicals was the second-most targeted sector in March 2023 with 60 of the total 459 attacks (13%). When compared to February's figures, this is an increase of 25 attacks month-on-month (71% increase) and a proportional decrease of 2%. Again, this shows that March's targeting of Consumer Cyclicals is mostly consistent with February's, irrespective of the increases in absolute figures. Consumer Cyclicals is often a key target for extortive threat actors due to the storage of client PII and the increased incentive to cause operational disruption due to the need for consistent uptime, contributing to its consistent spot amongst the top 3 sectors.

Highlighted in Figure 4, the most targeted industries within Consumer Cyclicals were Homebuilding and Construction Supplies, Specialty Retailers, and Hotels and Entertainment Services in joint first place, with 12 attacks each out of the total 60 (20%). The second most targeted industry was Automobiles and Auto Parts with 10 attacks (17%), and finally the third most targeted was Media and Publishing with 5 cases (8%). As aforementioned, the most targeted industries within Consumer Cyclicals often fluctuates due to the similarity of the extortive opportunities available to each of them, as has been the case again in March when compared to February.

In February, the top 3 most targeted industries within Consumer Cyclicals were Hotels & Entertainment Services in first, Specialty Retailers and Automobiles and Auto Parts in joint second, and Textiles & Apparel in third. Contrastingly, in March Homebuilding and Construction Supplies has soared to the top with an increase of 9 attacks from just 3 in February (300% increase), highlighting the volatility of this sector. Thus, organisations operating within any of these industries should consider the threat from the ransomware threat landscape.

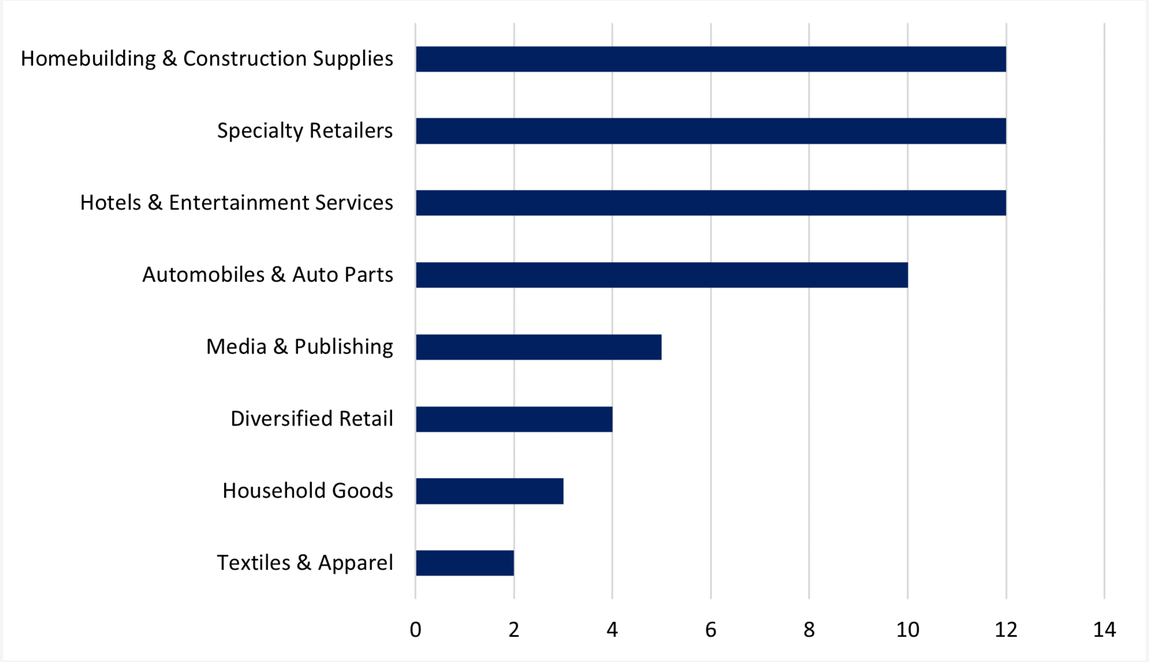

Figure 4 - Industries Targeted within the Consumer Cyclicals Sector March 2023

Technology

Returning to the norm following a minor shift in February, (Consumer Non-Cyclicals replaced Technology), Technology was the third most targeted sector again, just narrowly behind Consumer Cyclicals, with 56 out of 459 attacks (12%). This is a notable month-on-month increase from just 16 attacks in February, representing an increase of 40 cases (250% increase) and the biggest proportional increase so far of 6%; the overall interest in the Technology sector has returned to its prior height. The technology sector has unique characteristics that extortive threat actors are attracted to, such as the opportunities for supply chain compromises, which likely contributes to a heavy targeting of the Software and IT Services industry.

For the reasons outlined just above, Software and IT Services was the most targeted industry in Technology, accounting for a substantial 33 of the total 56 attacks (59%), this was then followed by Communications and Networking with 7 cases (13%), and finally Telecommunications Services with 5 (9%). A common feature of these industries is that they frequently contain managed service providers; ideal targets for threat actors looking to do the least work for the largest compromise. To illustrate this point, Software and IT services, Telecommunications Services, and Communications and Networking were also among Technology's most targeted industries in February 2023.

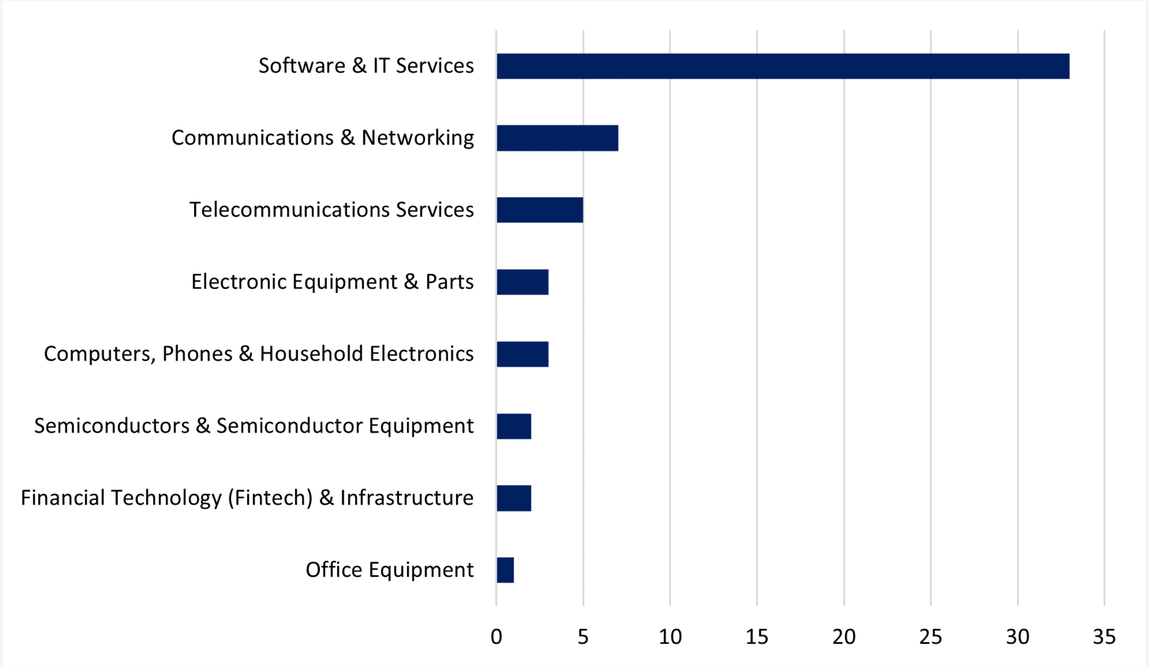

Figure 5 - Industries Targeted within the Technology Sector March 2023

Threat Actors

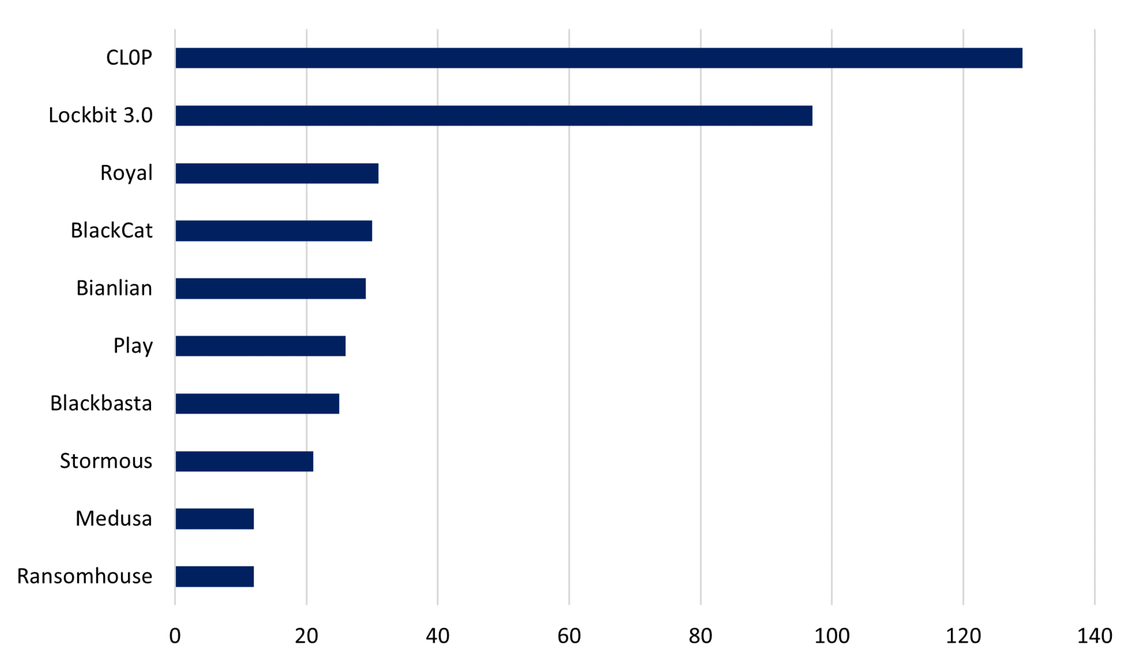

Figure 6 - Top 10 Threat Actors March 2023

Cl0p's successful exploitation of the GoAnywhere vulnerability saw the threat group rise to first place on the leader board, a position they have never held. This shift saw Lockbit displaced to second most prominent threat actor, a decline we have not observed since Lockbit was surpassed by the Royal and Cuba ransomware strains in November 2022. Given Lockbit's persistent success as a highly relentless ransomware group, supported by an affiliate model that affords them global reach, Clop's position could be considered a rather insurmountable feat. That said, we suspect that their rise in attacks will see results manifest only in the short-term, as organisations adopt patches against GoAnywhere and Lockbit 3.0 reclaims their place. The group's success nonetheless provides a critical reminder of threat actor exploitation of zero-day vulnerabilities at pace, their associated risks, and the importance of patching ASAP.

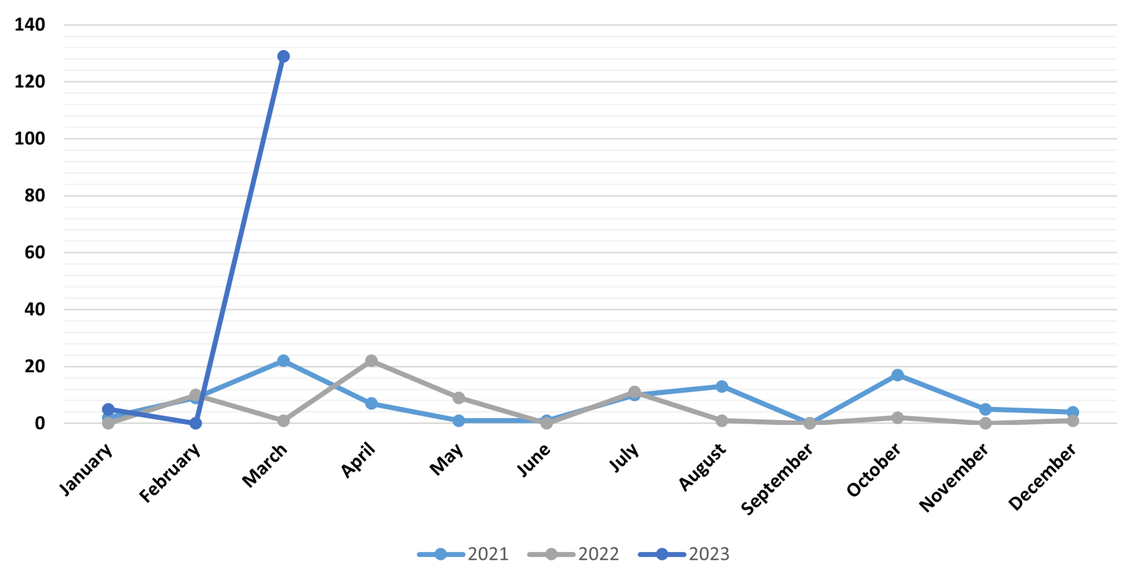

Figure 8 - Number of Hack and Leak Victims for Cl0p across, 2021, 2022 and 2023

Whether Cl0p will maintain momentum is a separate issue. Given that these attacks are directly linked to the exploitation of the GoAnywhere vulnerability, as patches and mitigations are adopted, this will likely result in a reduction of successful attacks. Organisations will need to act swiftly however as other threat actors will be quick to capitalise on this opportunity. Furthermore, whilst Cl0p has remained a relatively quiet threat actor, not maintaining a consistent Top 10 category position, this may drive the group to identify novel opportunities for vulnerability exploitation following their widespread success.

It is therefore important to understand who the threat actors are, their respective TTPs as well as victimology, to reinforce prevention across the board.

Sectors

Of Clop's 129 attacks, sectoral analysis identified 36 attacks pertained to the Industrials sector (28%), 23 in Technology (18%) and 19 in Consumer Cyclicals (15%). Focus therefore still remained within the top three targeted sectors we observe each month, meaning that the vulnerability did not result in any major change to the most targeted sectors. Naturally, these sectors incorporate more organisations and potential targets, which will likely contribute to their higher numbers; however, we might have expected to see some changes to the sectoral rankings as Cl0p's targeting was driven by a specific vulnerability. This may suggest a number of considerations including, the software and its vulnerability being widespread across these three sectors, as well as a general, continued interest in these sectors given their value as ransomware victims. Whatever the reason, it remains clear that these sectors are highly susceptible to ransomware attacks and should ensure both patching against the vulnerability as well as broader prevention measures.

Industries

Within the abovementioned sectors, the following industries were of greatest interest to Cl0p; Professional and Commercial Services (21 attacks), Software and IT Service (15 attacks) and Specialty Retailers (5 attacks).

LockBit 3.0

Second to Cl0p, LockBit were responsible for 97 ransomware attacks in March, accounting for 21% of attacks that month. As aforementioned, this is the second time LockBit has been displaced from its leading position, which it has held since September 2021. Interestingly, despite numbers increasing across the wider threat landscape, LockBit observed a decline of 25% from the 129 attacks observed in February. A number of variables may contribute to this such as changes to threat actor targeting procedures, however, what is important to note is that even with this decline, the group still maintains a clear foothold on the threat landscape. The threat actor remains highly relentless in their targeting and we anticipate that this is unlikely to change at present.

Sectors

Lockbit's targeting pattern mirrored that of Cl0p with the majority of their victims in the Industrials sector with 32 attacks (33%), followed by Technology with 13 attacks (13%) and Consumer Cyclicals with 12 attacks (12%). This reiterates the importance for organisations within these sectors to heighten knowledge around Lockbit's TTPs and the corresponding prevention measures.

Industries

Closer analysis of the industries within Lockbit's top 3 targeted sectors identified Professional and Commercial Services (12 victims), Software and IT Services (10 victims) and Homebuilding and Construction Supplies (5 victims) as most susceptible. As we know, industry selection often fluctuates but Professional and Commercial Services certainly remains central to Industrial targeting.

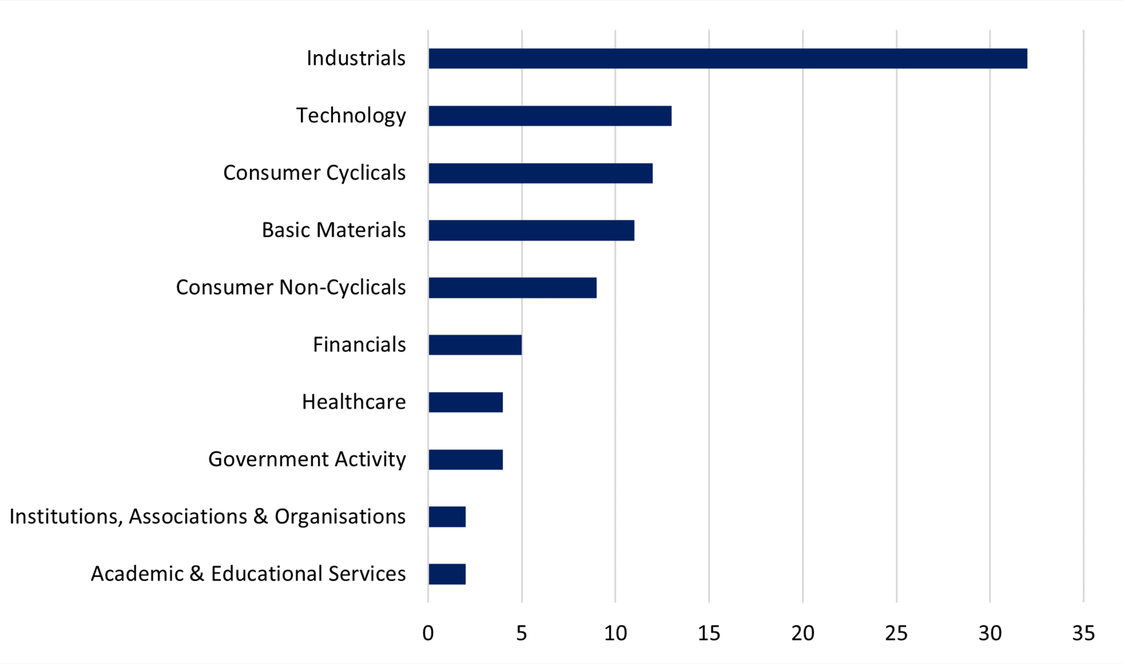

Figure 9 - Sectors Targeted by LockBit 3.0 March 2023

Sectors

Royal's top three targeted sectors concerned the Industrials sector with 15 attacks (48%), Consumer Cyclicals with 5 attacks (16%) and 3 incidents in Healthcare (10%). As with Cl0p and Lockbit, the majority of Royal's targeting centred on the Industrial sector, and has remained their most important target this year. We can certainly anticipate that the group will target organisations within this sector in the coming months.

Industries

Within these sectors the most targeted industries concerned Machinery, Tools, Heavy Vehicles, Trains & Ships (7 attacks), followed Healthcare Providers and Services (2 attacks) and Consumer Cyclicals saw an even amount of attacks (1) across their five industries; Specialty Retailers, Automobiles and Auto Parts, Textiles &Apparel, Diversified Retail, Homebuilding and Construction Supplies.

As we know, industry targeting often varies and this is reflected in CISAs acknowledgement of the many sectors Royal has breached within critical infrastructure, and therefore, their respective industries. In this respect, prevention efforts should concern all organisations within the wider critical infrastructure sectors, not only the top three aforementioned, to ensure for greater coverage

Regions

Alongside the overall rise in cases in March, the weighting of targeting within each region has remained mostly consistent with some minor differences. North America was the most targeted region with 221 cases out of the total 459 (48%), this was followed by Europe with 126 (28%), and Asia with 59 (13%). The remaining regions have remained mostly consistent with their positions in February with just slight 1% decreases in proportional targeting across the board. Note that one of these incidents falls under “TA Dispute” which has been mentioned in the Threat Actors section just prior.

In terms of total figures, cases in North America have increased by 108 (96%) from February to March 2023, which is a proportional increase of just 1%, again highlighting the targeting consistency. Europe’s total figures have increased by 70 cases (125%), which is a more noticeable proportional increase of 5%, perhaps implying an increased focus on European countries in March. Finally, Asia’s attack numbers have increased by 24 cases (69%) which is a proportional decrease of 2%. Therefore, NCC Group as always suggest that organisations residing all regions monitor and strengthen their cyber defences where possible, but this is particularly pertinent for North America and Europe.

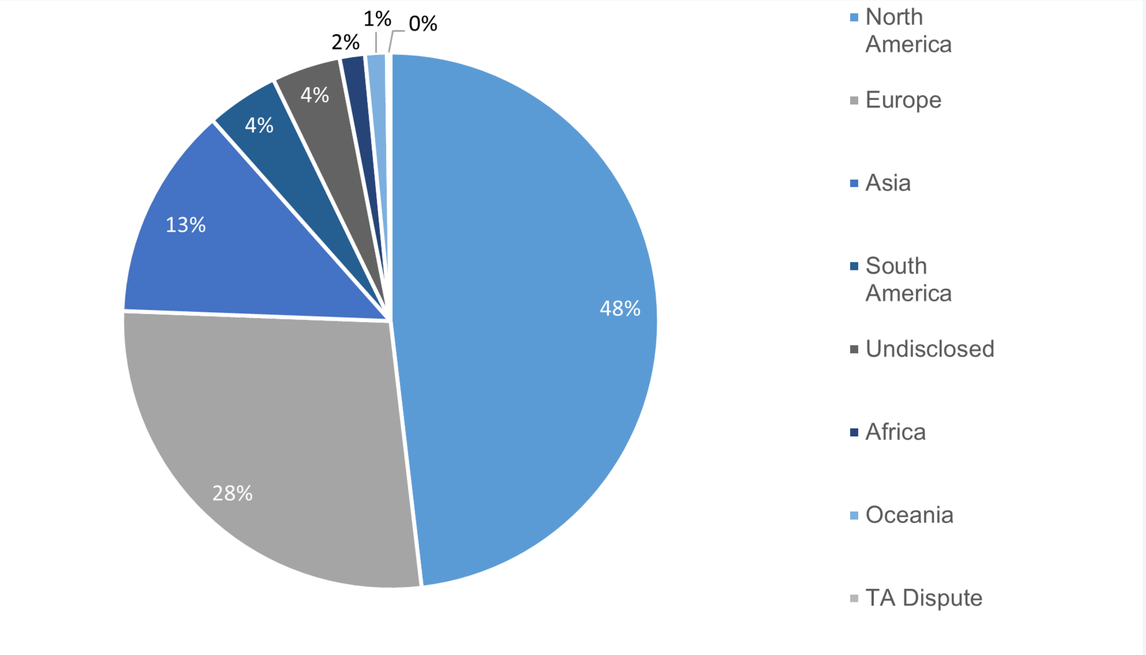

Figure 12 - Regional Analysis March 2023

February 3rd

- Story picked up by cyber news outlets and vendors
- Fortra advises the Web Client interface is not exploitable
- Fortra advisory for customers to review admin users and monitor for suspicious ones
    - Especially if users are created by system indicating follow-on attacker behaviour

February 6th

- Proof of exploit released

February 7th

- CVE-2023-0669 assigned
- Patch 7.1.2 released

February 9th

- Fortra announces some MFTaaS instances were also compromised
    - “We have determined that an unauthorized party accessed the systems via a previously unknown exploit and created unauthorized user account.”
- Shodan shows 1K+ GoAnywhere instances exposed online, but only 135 on ports 8000 and 8001 used by the vulnerable admin console

February 10th

- Cl0p contacted BleepingComputer stating they’d stolen data from 130+ organisations over a ten-day period
    - They claimed they had the ability to move laterally within victim networks yet decided not to deploy ransomware, instead limiting themselves to stealing data directly from MFT servers
    - They did not provide any proof of these claims

March 10th

- Cl0p add 7 new companies to their leak site
    - Allegedly some of these victims have received ransom demands; contra to what Cl0p stated in their communiques with BleepingComputer

March 29th

- Shodan indicates 94 instances on port 8000 and 8001 are still open

Importantly, this is not the first time Cl0p has mass-hacked a vast number of large organisations by exploiting a vulnerability in a third-party product. The Accellion attacks outlined above, occurring in late 2020 and early 2021, are a great example of this. Using similar tactics to attack Accellion's legacy File Transfer Appliance (FTA) with a combination of new web shells and zero-day vulnerabilities to exploit, they managed to amass more than 100 victims. This time, it was Fortra's GoAnywhere MFT tool and CVE-2023-0669, which were exploited. The targeting of multiple organisations and the announcement of multiple victims in quick succession is something of an identifier for Cl0p, which distinguishes them from other ransomware operators.

Notably, as Cl0p is a RaaS provider, a number of affiliates also exploit the ransomware strain in their attacks. Cl0p have been linked to other actors before, most notably TA505 and FIN11, and this recent campaign against the GoAnywhere MFT has been attributed to actors other than Cl0p themselves. Additionally, Huntress linked the use of the malware family Truebot which has been previously associated with another Russian-speaking threat group, Silence. Silence have also been linked in the past with TA505, who are also being discussed as responsible for this latest spate of attacks.

Securing Your Systems: How do I Protect Myself?

Some simple mitigations organisations can adopt to prevent against this threat include:

- Limit exposure on ports 8000 and 8001; these are the ports where the GoAnywhere MFT admin panel is situated.
- Login to your account and follow the steps outlined in the GoAnywhere security advisory.
- Install patch 7.1.2
- Review admin user accounts for suspicious activity, with a special focus on accounts created by system, suspicious or atypical timing of account creation, or disabled super users creating multiple accounts.
- Contact GoAnywhere MFT support directly via portal, email, or phone to receive additional assistance.

Further advice on mitigating ransomware specifically, as well as new emerging threats more generally includes:

- Know your estate: knowing what systems are in use and how they are configured makes the task of knowing whether a recently announced vulnerability has the ability to impact your organisation or not.
- Patch! Patch! Patch: New vulnerabilities are exposed regularly and it can be difficult to keep up. However, a years-old vulnerability on a system which has not been patched serves only to make an attacker's life easier.
- Block common forms of entry: Create a plan for how to quickly disable at-risk systems like VPNs or RDP, or look into endpoint security packages to detect exploits and malware before they are utilised by attackers.
- Create backups: backup's stored offline and offsite are beyond the reach of attackers and can serve to get an organisation back on its feet with minimal downtime in the event of falling victim to a ransomware attack.

Do not get attacked twice: Attackers can target organisations more than once. If they see that a vulnerability remains unpatched, or that a security flaw which previously assisted their attacks has not yet been remedied, they may return to the same victim for follow-up attacks. Once the outbreak is isolated and the first attack is successfully stopped, every trace of their intrusion, malware, tools, methods of entry, must be removed, assessed, and acted upon to avoid being attacked again.

nccgroup

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