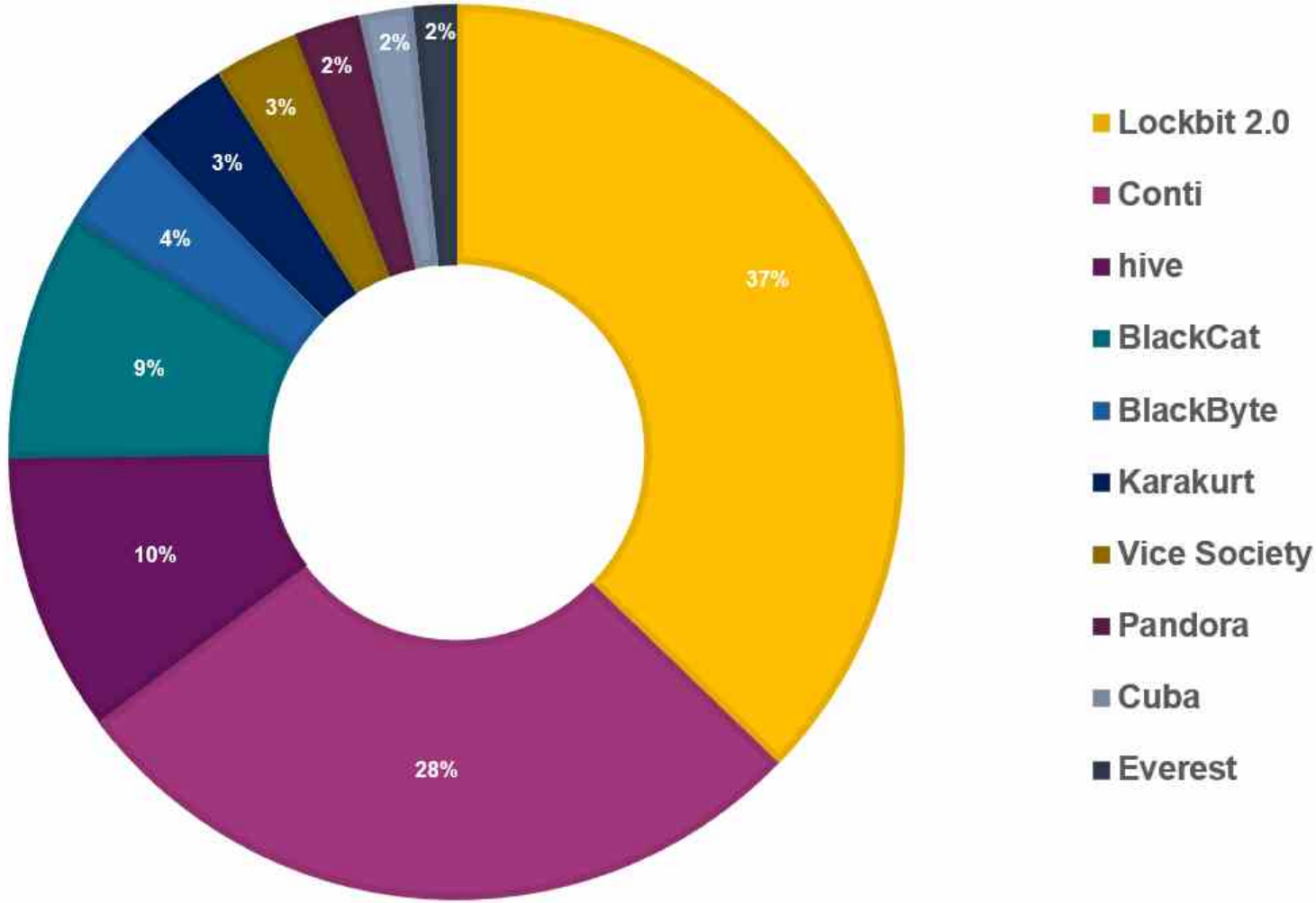
Monthly Threat Pulse
March 2022

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 last month, and how do these insights compare to previous months?

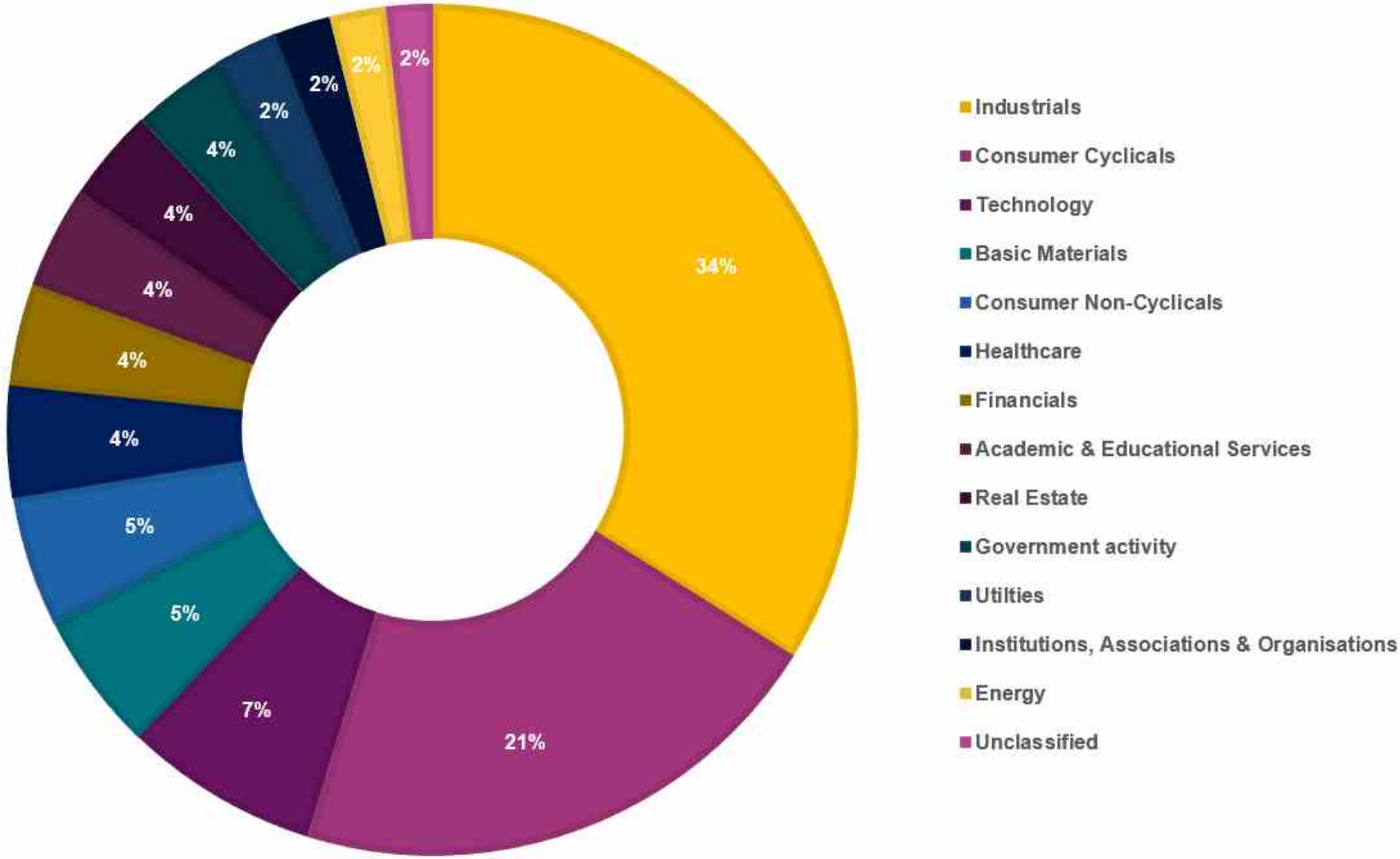
Key data

Percentage of Victims by Group in March 2022



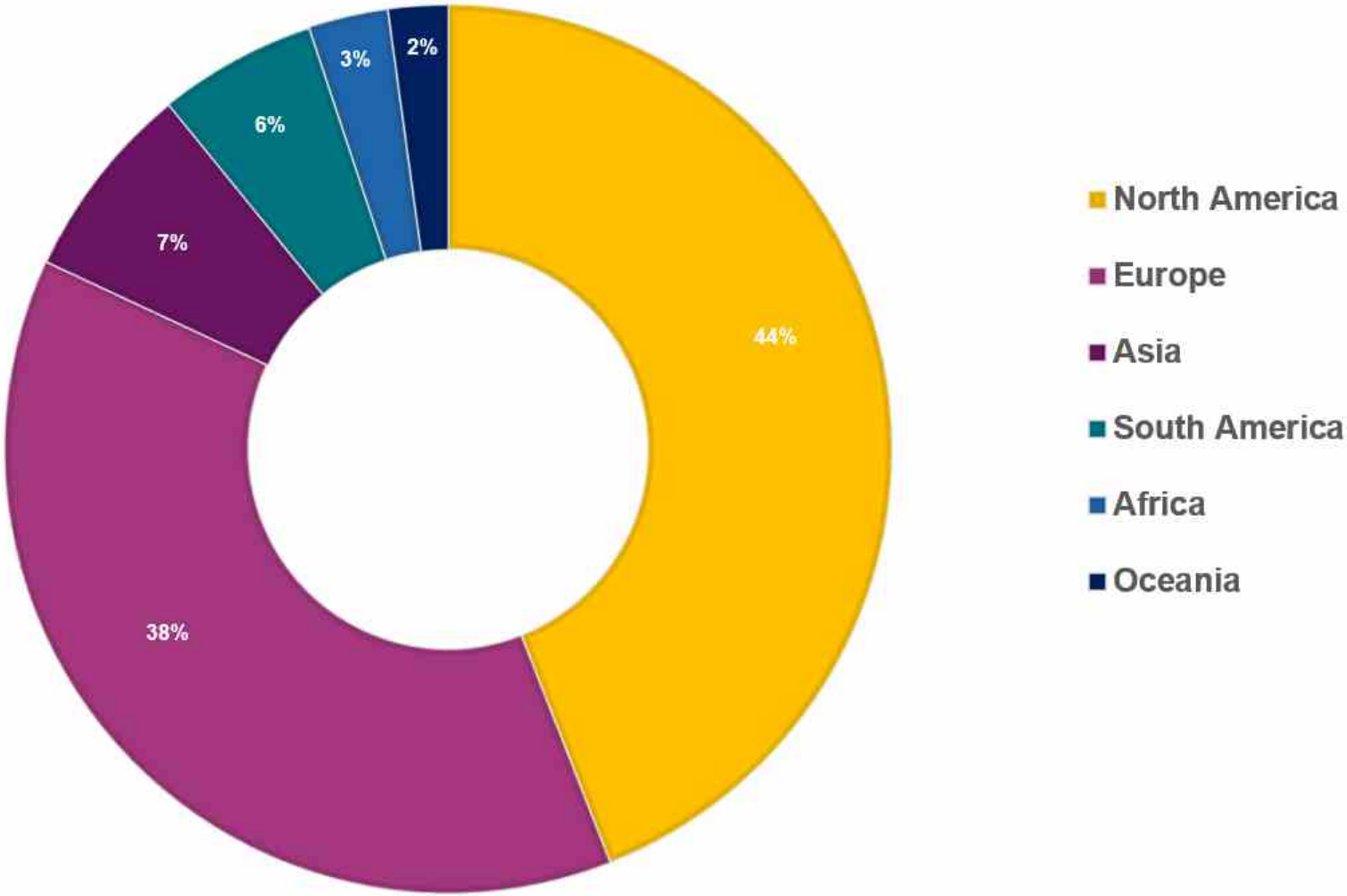
Key data

No. of Victims by Sector in March 2022



Key data

Percentage of victims per region in March



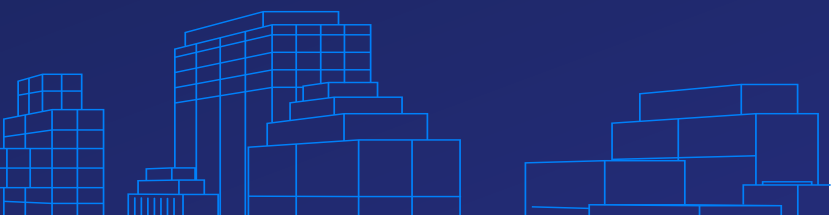
Analyst comments

In March, we observed a 52.97% increase in ransomware attacks compared to February, with the number of incidents rising from 185 in February to 283.

This increase represents a continued and substantial growth in the number of ransomware attacks, as we move out of the seasonal lull that characterised December and January.

Looking back at March 2021 in which there were 204 incidents identified within our database, this growth is thus also reflected by a new year.

As such, it remains critical to continue monitoring ransomware activity as the year unfolds, observe whether such an increase evolves, and what this means for cybersecurity.



Sectors

This March, analysis of ransomware victims once again identified Industrials (33.92%), Consumer Cyclicals (20.85%), and Technology (7.42%) as the top three most targeted sectors.

As observed in February, these sectors increased in the number of attacks perpetuated.

In March the Industrials sector demonstrated an attack growth of 66 to 96 incidents, an estimated 45.5% increase in successful attacks, whilst Consumer Cyclicals rose from 40 to 59 attacks, a 47.5% increase.

The Technology sector revealed a somewhat smaller growth from 15 to 21 (28.6%), but an increase, nonetheless.

As evoked by this analysis, these sectors continue to maintain their position at the top of our list as the most targeted. In addition, we continue to observe a pattern of fluctuating increases in other sectors that consequently changes their position in our database.

Sectors like Basic Materials experienced a decrease in February by 25%, though is noticed to have augmented by 66% this March.

This, however, is a known trend within these sectors, as it is observed that the number of attacks carried out within the last 6 months has experienced alternating increases and reductions.

Notably, a growth in attack activity within the Industrials, Consumer Cyclicals and Technology sectors continues to strengthen our observation regarding a clear trend in targeting activity.

These sectors likely continue to be attractive targets as the impact of a ransomware campaign is not restricted to the initial victim, and herein lies the benefit.

Within these sectors, products and services here are provided on a large scale, and thus the knock-on effect to both client and customer signifies a greater urgency and pressure to restore services, limit damage and cost.

Hence, threat actors exploit this weakness to elicit the desired response, payment of the ransom, which is often paid.

As such, the very make-up of the organisations within these sectors leaves them vulnerable to targeting, and emphasises the need for continued, hardened security measures to enhance the prevention, detection and mitigation capabilities of the organisations residing within.

At the same time, organisations outside of these sectors should not become complacent as changes to targeting behaviors may occur as the threat landscape evolves.

As such, robust cybersecurity should be at the heart of all organisations security posture, irrespective of their sector.

Regions

Following the equal number of attacks in North America (42.16%) and Europe (42.16%) reported in February, this March normalcy is restored as North America (44.04%) once again tops the list as the most attacked region.

In addition, Europe (37.91%) returns to its position as second most attacked. All together these regions account for 81.95% of the total attacks reported and evokes a dominant focus on, and threat to, organisations within these regions.

In addition, Asia accounted for 7.22% followed by South America 5.78%, Africa 2.89%, and Oceania 2.17%.

Furthermore, the data suggests a substantial increase in ransomware attacks in North America from 78 in February to 122, which reflects a 62.7% increase over the last month.

We also observed a rise in the number of attacks in Africa from 1 to 8, showing a 700% increase.

This is of particular interest as Africa, the region usually with the least number of attacks for the past 6 months, is reported to have an increase in ransomware attacks, moving it a level up from its position in February.

Further analysis of North America shows that the United States records an attack high of 108 from 73 reported in February, which is a 48% increase in ransomware attacks over the month and accounts for 88.5% of the total attacks reported in North America.

This consists of ransomware attacks on almost every sector with Industrials, Consumer Cyclicals and Technology as the lead sectors targeted. Africa's notable increase were successful attacks in 7 countries with South Africa accounting for 25% of the reported attacks.

Threat Actors

As noted, March revealed a continued boom in ransomware activity. Markedly, of the 283 attacks identified, Lockbit 2.0 and Conti remain the most notable players in the ransomware game, accounting for 96 and 71 attacks respectively.

As such, they were responsible for a substantial 59% of the total number of incidents reported, proving themselves to be an ongoing and critical threat to the cybersecurity of diverse organisations.

Based on the consistent level of activity we anticipate these two groups to remain at the top of the ransomware table board, there continues to be a shift in the threat actor ranking third.

Specifically, we have observed Hive take on a new position in third place, overtaking BlackCat (23) ever so slightly with 26 incidents.

Lockbit 2.0

This March Lockbit 2.0 maintained its position as the leading threat actor, responsible for the highest number of total targeted attacks, and demonstrating a continued growth in their activity from 41 campaigns in January, 78 in February, and 96 in March. Though a smaller growth from February to March, this still accounted for a 23.07% increase. The lower numbers at the offset of the year are likely representative of reduced activity around the seasonal period, with the increase marking an exit from the seasonal lull.

Like February, Industrials (34.38%), Consumer Cyclicals (20.83%) and Technology (7.29%) remain Lockbit 2.0's dominant targets. With the exception of January, where the financial sector ranked in third place, each of the sectors has placed first, second and third, as most targeted this year. A pattern of interest can thus be identified, and it would be prudent for organisations within these sectors to consider the threat from Lockbit 2.0.

Industry analysis further revealed 'Professional & Commercial Services' (16.67%), 'Construction & Engineering' (9.38%) and 'Government Activity' (6.25%), as most susceptible to Lockbit 2.0 ransomware this March. Notably, the former remains the prominent focus, and the targeting of 'Construction & Engineering' a continued interest. By contrast, Government Activity has since doubled, this may simply be reflective of behaviour this March, or an emerging trend. As such as will continue to monitor activity to verify if the threat persists.

Conti

Our second most prominent actor concerned Russian-based ransomware group Conti, and crucially for whom we have observed a considerable increase in attack quantity. In February 33 incidents were identified, however in March 71. Whilst we are observing threat actors come out of the seasonal woodworks, and a general increase in ransomware activity all round, this is a rather prominent jump in Conti activity with a percentage increase of 115%.

It will therefore be pivotal to monitor Conti's behaviour and identify whether this increase in ransomware activity will continue as we move into April.

Similarly, LockBit 2.0, the top two sectors targeted were Industrials (43.66%) and Consumer Cyclicals (26.76%), whilst Basic Materials ranked third. (9.86%). These findings continue to illustrate a trend in targeting behaviours and certainly strengthens our understanding of which sectors are most attractive (Industrials and Consumer Cyclicals), with respect to this month's top two threat actors. When analysing the industries affected, 'Professional and Commercial Services' suffered the greatest number of incidents (23.94%) followed by 'Machinery, Tools, Heavy Vehicles, Trains & Ships' (12.68%), and 'Speciality Retailers' (5.63%). Like Lockbit 2.0, there is a strong focus upon the former, and an interest alike in the latter that allows us to infer a pattern in targeting preference within our most prominent threat actors. Organisations within these industries should thus take note of the threat posed.

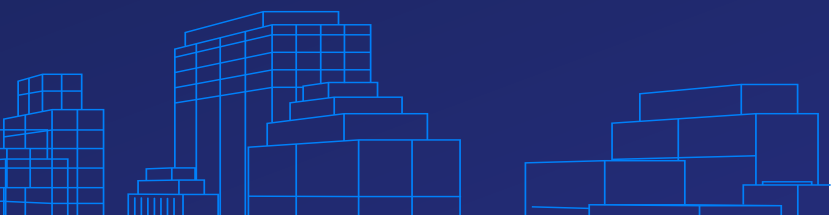
Hive

In March, Hive was our third most prominent threat actor. Responsible for 26 incidents, and therefore only 9% of total activity, this is particularly interesting as not only have they overtaken BlackCat (23 incidents), but they have also illustrated a 188% increase in targeting activity from 9 incidents in February. This is a substantial growth and the largest growth in activity across Lockbit 2.0, Conti and Hive. As such, it begs the questions as to whether we are looking at a new, dominant threat actor.

Unsurprisingly, the 'Industrials' sector remained the most prominent victim, accounting for 34.62% of attacks. 'Academic & Educational Services' (15.38%) however placed second, moving away from the usual targeting of 'Consumer Cyclicals' observed above. Third place was shared across Utilities (7.69%), Basic Materials (7.69%), Energy (7.69%) and Financials (7.69%). Whilst there is some variation, the Industrials sector takes a clear lead, however it will be interesting to observe whether a greater focus upon Consumer Cyclicals arises, if Hive are to follow in the footsteps of Lockbit 2.0 and Conti.

Analysis of the industries revealed 'Professional & Commercial Services' as the most targeted (19.23%). 'Construction and Engineering' and 'Schools, Colleges & Universities' shared joint second place with 3 incidents respectively, accounting for a total of 23.08%, whilst 'Oil & Gas' ranked third (7.69%). A common targeting of the 'Professional & Commercial Services' across the three threat actors reinforces the notion that organisations within are highly attractive targets. It is vital that those working in these industries are both aware of the threat, and take appropriate measures to harden cybersecurity.

Threat Actor Spotlight: Lapsus$ Group



Summary

Lapsus$ first appeared publicly in December 2021, however the group appears to have operated under a different name previously. Over the last 4 months, Lapsus$ has gained notoriety thanks to the multiple successful breaches of large enterprises including, Microsoft, Nvidia, Okta & Samsung.

Geographically speaking, the group has focused its efforts predominantly upon UK and South American targets, however this expands to other regions.

Like other ransomware groups their motivations are primarily financial, however, the lack of encryption methods used within their operations means that they are not classified as a traditional ransomware group.

The traditional ransomware approach focuses on business continuity by making the data unavailable via encryption. Rather, Lapsus$ should be considered an extortion group, as they use the “hack and leak” approach to target the confidentiality of their victim’s data.

The group uses its Telegram channel to announce their victims which effectively initiates the extortion procedure. For recruitment purposes, Lapsus$ uses multiple social media platforms, such as Reddit, to post recruitment messages. The communication continues either via their Telegram account or email.

Attack Example

Initial access is believed to occur via stolen authentication cookies which would grant the attacker access to a specific application.

These cookies usually are in the form of SSO applications which from there would allow the attacker to pivot into other corporate applications, bypassing controls such as MFA.

Credential Harvesting and privilege escalation is a key component of Lapsus$ breaches. The threat actors appear to elevate from a standard user account to an administrative user within a couple of days.

Techniques used by Lapsus$ include:

- Access and scraping of corporate Microsoft SharePoint sites to identify any credentials which may be stored in technical documentation.
- Searching code repositories for credentials
- Exploiting vulnerabilities in JIRA , Conflunence and Giltab
- Access to local password managers and databases to obtain further credentials and escalate privileges.
- Cloning of git repositories and extraction of sensitive API Keys.
- Using compromised credentials to access corporate VPNs.
- Disruption or destruction to victim infrastructure to hinder analysis and cause havoc.

Access to corporate VPNs is a primary focus for this group as it allows the actor to directly access key infrastructure which they require for their actions on objectives.

NCC Group has observed disruption and destruction to client environments by Lapsus$ such as shutting down virtual machines from within on-premises VMware ESXi infrastructure, to the extreme of mass deletion of virtual machines, storage, and configurations in cloud environments, making it harder for the victim to recover and for investigation teams to conduct their analysis.

About the NCC Group Monthly Threat Pulse

NCC Group's Strategic Threat Intelligence Practice has been working tirelessly to develop various software solutions for a broader, more insightful look at current threat landscapes and the way they impact businesses around the world.

Our technical team has developed a web scraper, which we use to gather data on ransomware data leaks on the dark web in real time to give us regular insights into who are the most recent ransomware victims.

By recording this data and classifying the victims by sector, we are able to derive additional insights highlighting the sectors that have been targeted, and how current ransomware threats compare to previous months.