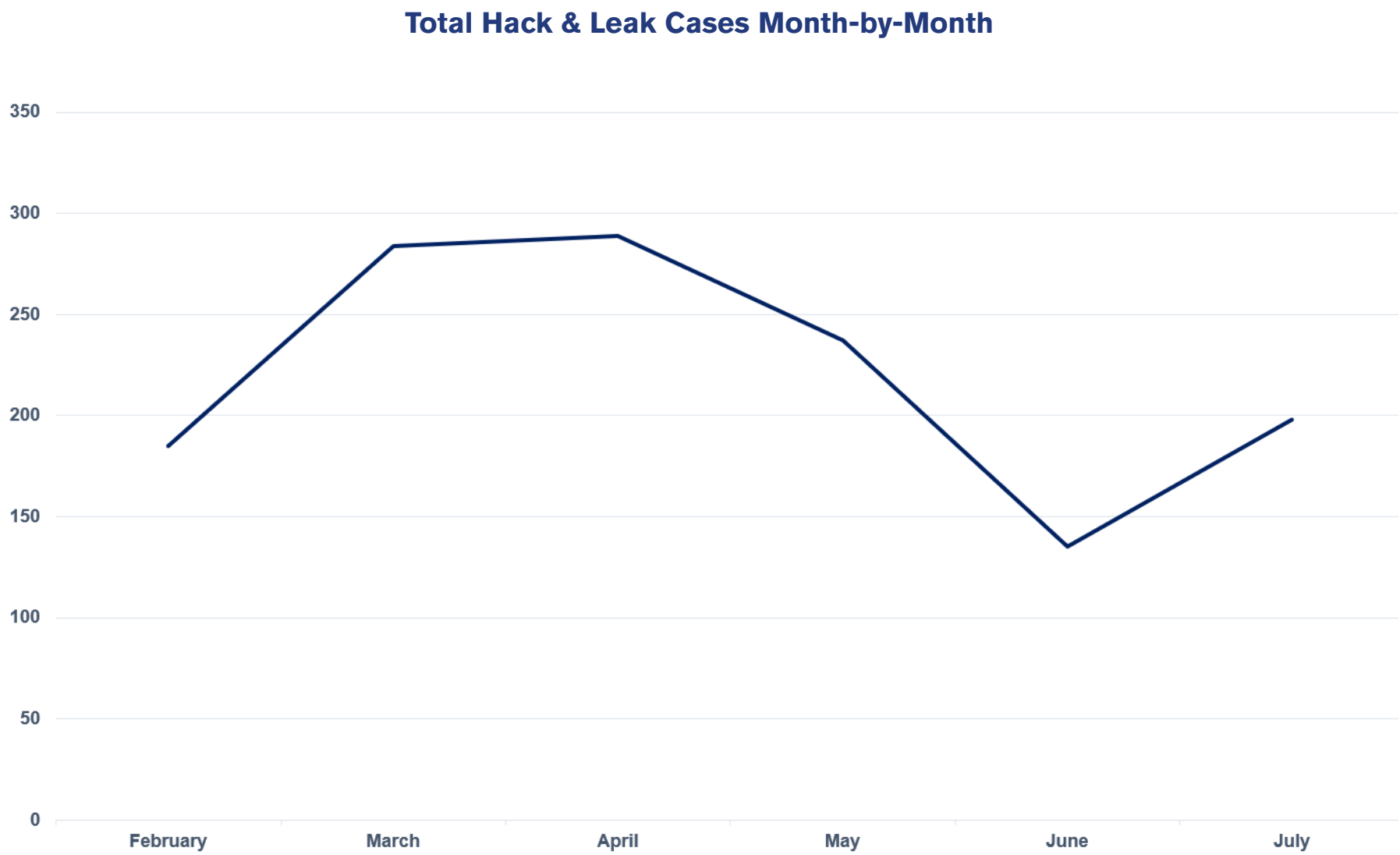
Monthly Threat Pulse
July 2022

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.

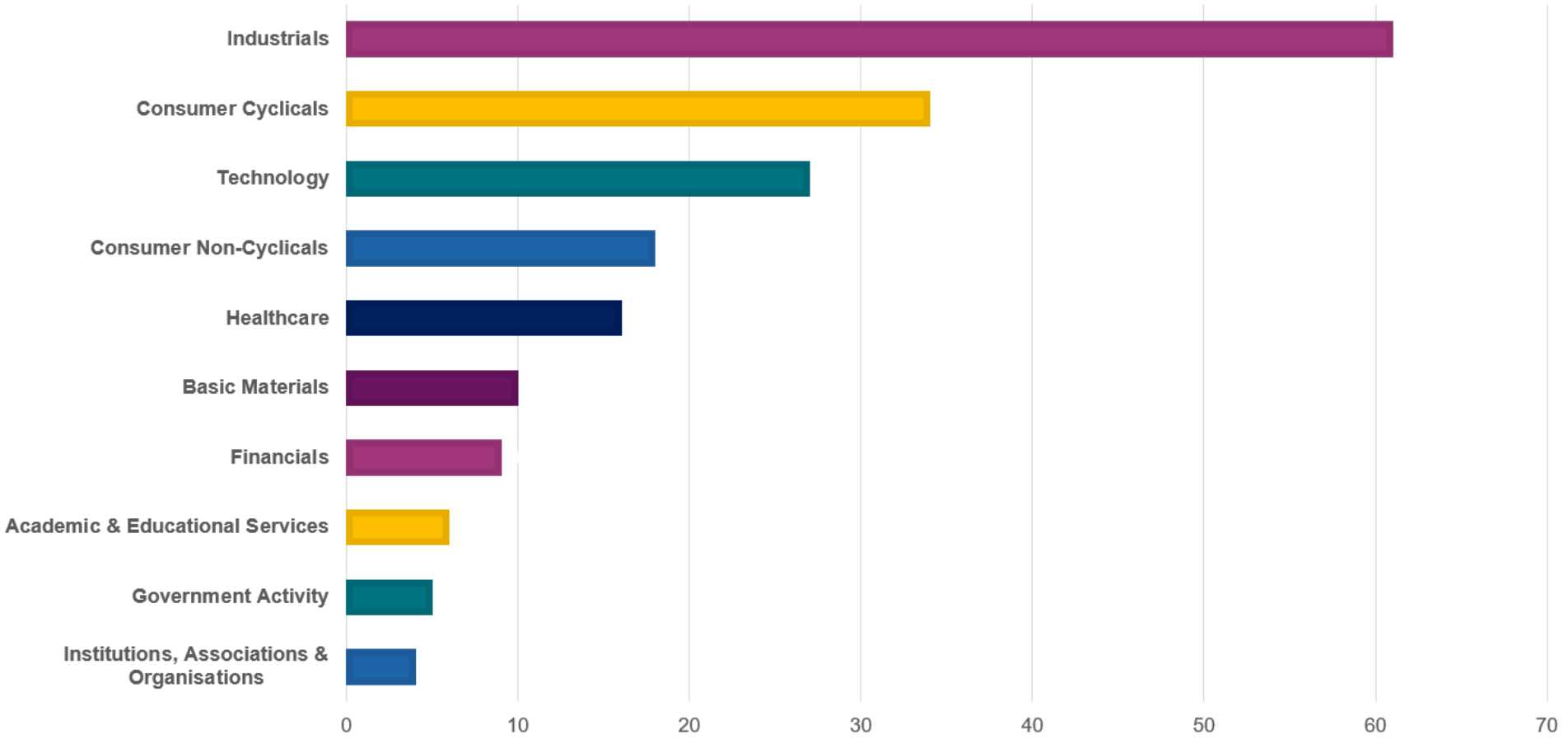
By recording this data and classifying the victims by sector, we are able to derive additional insights such as, which sectors are being targeted this last month, and how do these insights compare to previous months?

Key data

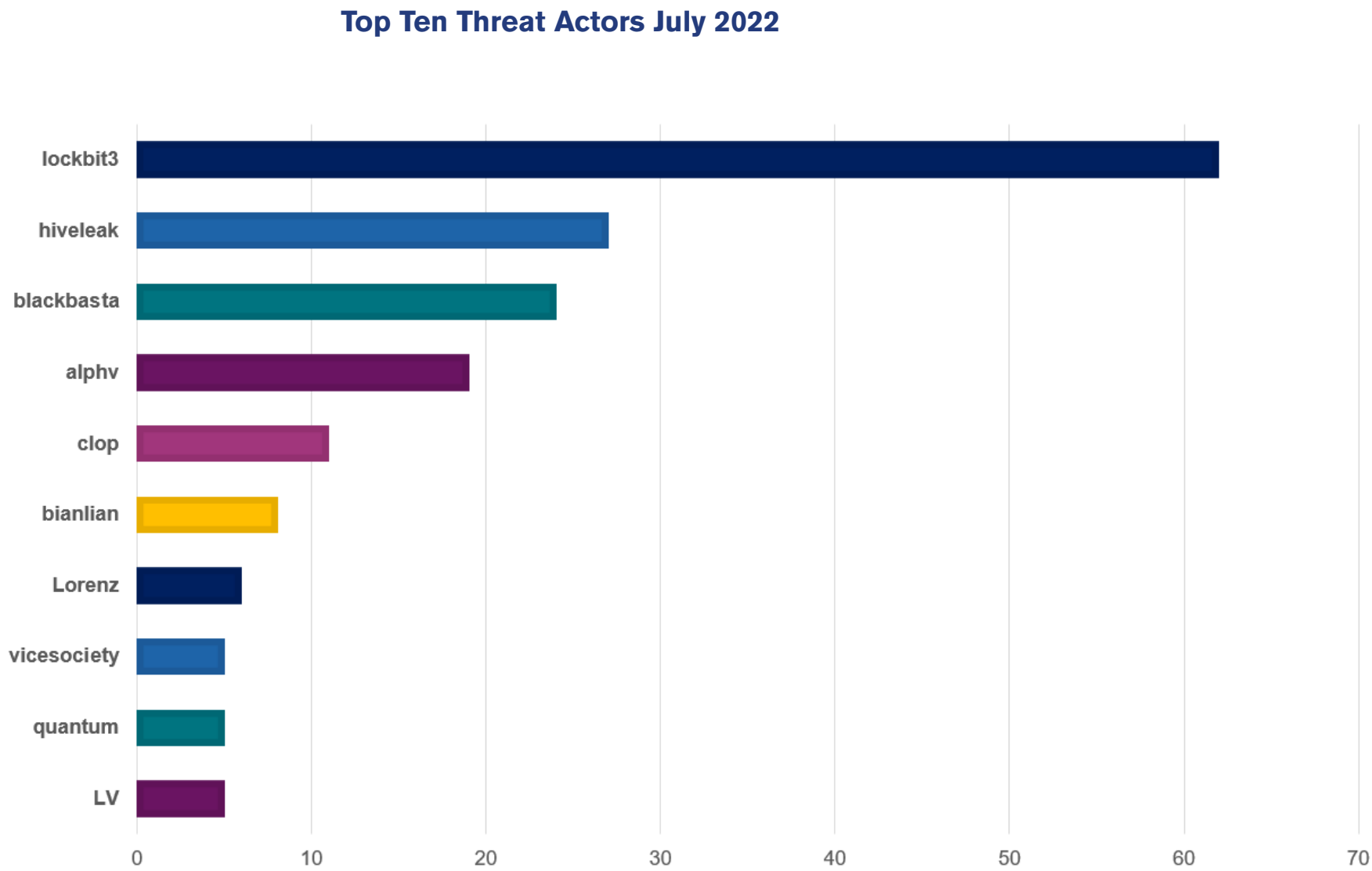

Total Hack & Leak Cases Month-by-Month
350
300
250
200
150
100
50
0
February
March
April
May
June
July

Key data

Number of Hack & Leak Cases by Sector in July 2022

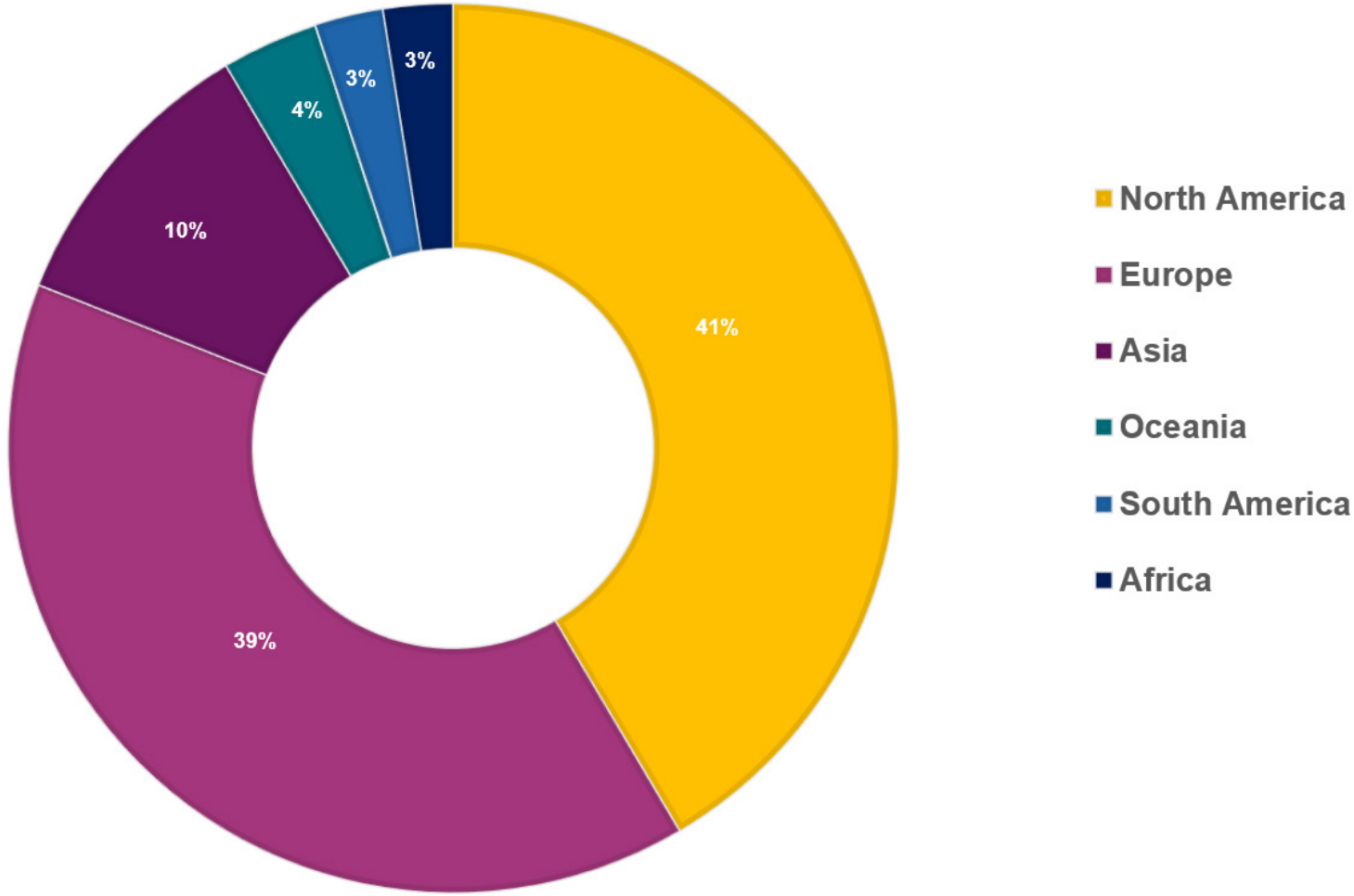


Key data


Top Ten Threat Actors July 2022
lockbit3
hiveleak
blackbasta
alphv
clop
bianlian
Lorenz
vicesociety
quantum
LV
0
10
20
30
40
50
60
70

Key data

Percentage of Hack & Leak Victims by Region July 2022



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

Analyst Comments

In July, we observed a 47% increase in ransomware attacks compared to June, with the number of incidents rising from 135 to 198.

Following the considerable decrease from May to June (from 236 to 135), it is likely that the threat actors that were undergoing structural changes, such as the Conti operators and Lockbit, and have begun settling into their new modes of operating, resulting in their total compromises increasing in conjunction.

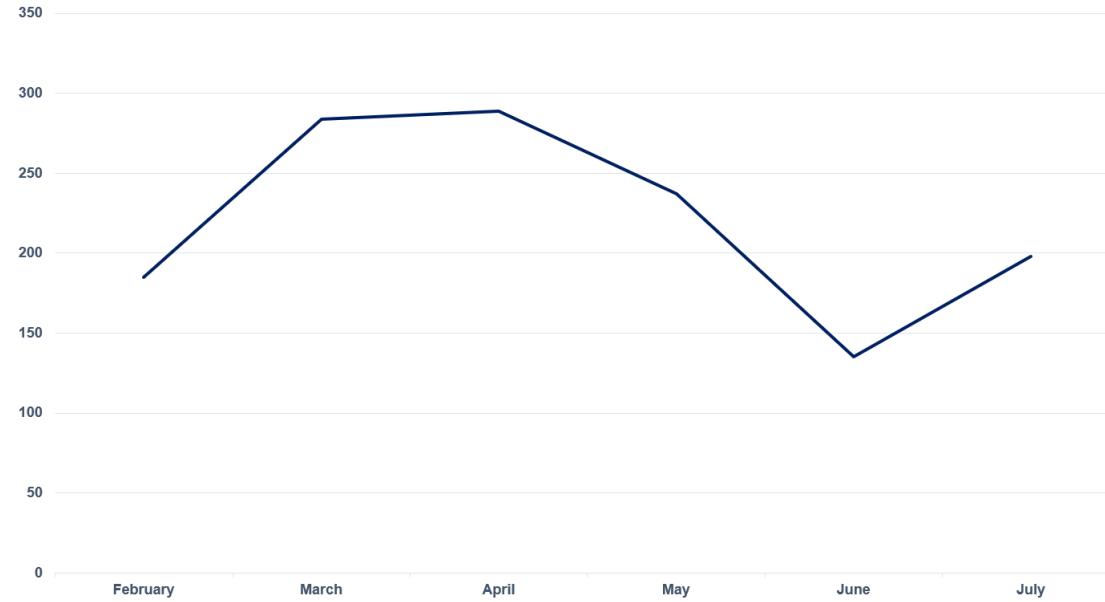


Figure 1: Total Hack & Leak Cases Month-by-Month

Consequently, it would not be surprising to see these figures further increase as we move into August.Interestingly, when we compare this observation to June and July of 2021, we find the inverse taking place; a 27% decrease from 219 in June to 159 in July.

As July's increase takes place just after Conti's integration into alternative ransomware groups (such as BlackBasta) and LockBit's third metamorphosis, it is likely that this year-on-year disparity is as a result of this.

No such activity was taking place in 2021, and as a result, June – July of 2021's figures were possibly representative of general seasonal changes in activity. Going forward, we expect to see more similarities between 2021 and 2022 as the ransomware threat landscape becomes less volatile.

Sectors

In line with our findings in June's threat pulse, the top most targeted sectors in July 2022 were Industrials with 63 incidents (32%), Consumer Cyclicals with 34 (17%), and Technology with 27 (14%). As is to be expected with the overall increase of hack & leak cases in July, the individual figures of each of these sectors have increased proportionally as well.

Based on previous months and emerging patterns, these sectors are likely to remain as the top targets throughout the second quarter, due to the attractive organisations residing within them and due to the breadth of different activities taking place in each sector.

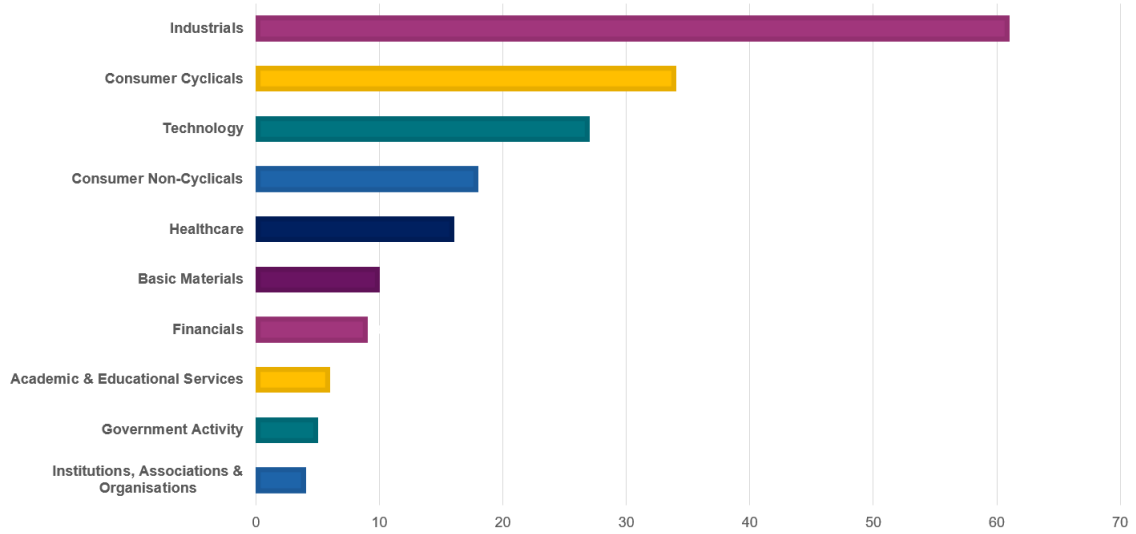


Figure 2: No. of Hack & Leak Cases by Sector in July 2022

Industrials

As we have stated previously in our Threat Pulses, industrials is a sector that continues to be heavily targeted and successfully compromised due to its broad range of industries within, the costliness of operational disruption, and its vast distribution of Operational Technology (OT) and legacy systems. The distribution of targeting across the entire industrials sector is identical to that of June's targeting, with slightly larger figures for some due to the total increase in hack & leak cases in July 2022.

Professional & Commercial services were the most targeted once more, with 28 cases (22% increase from June), Construction & Engineering were second with 15 attacks (50% increase) and finally, Freight & Logistics Services were third with 6 cases (25% decrease).

NCC Group expect this pattern to continue going forward, as the identical ordering of these industries from June – July accurately represents the attractiveness of each respective industry to threat actors.

Consumer cyclicals

As previously assessed by NCC Group, Consumer Cyclicals will likely continue to be present within the top most targeted sectors due to their integration with services that are present within day-to-day life, and therefore the amount of customer data that they likely hold as a whole.

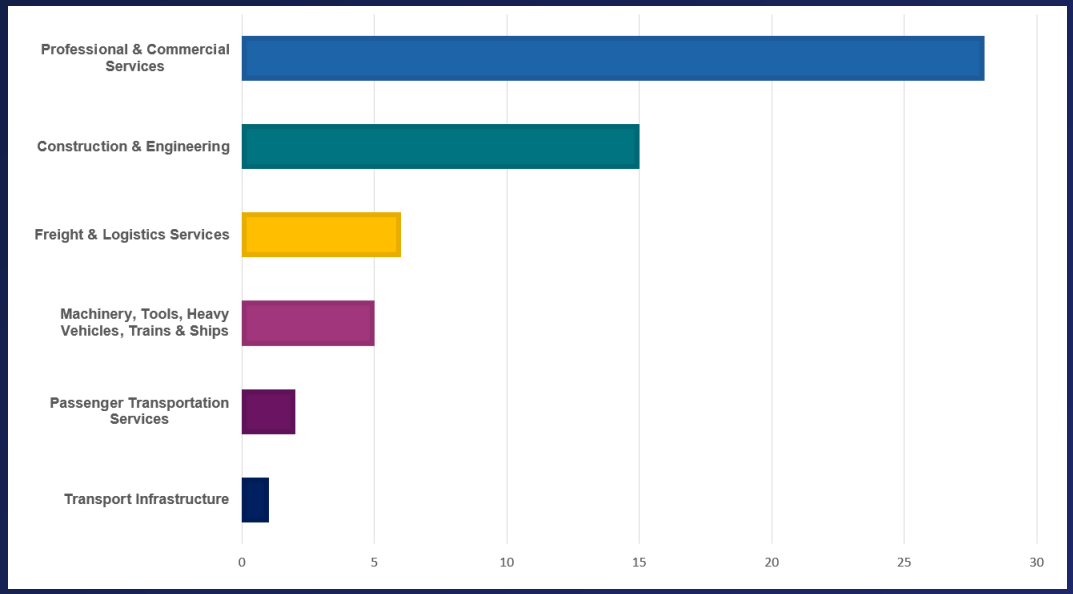


Figure 3: No. of Hack & Leak Victims for the Industrials Industries July 2022

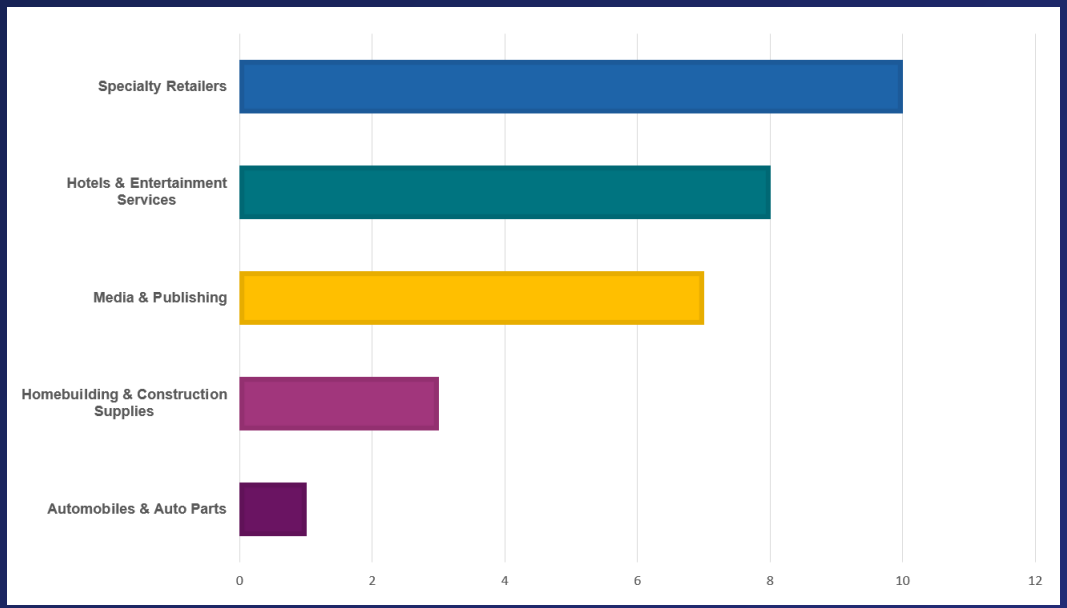


Figure 4: No. of Hack & Leak Victims for the Consumer Cyclicals Industries July 2022

July's distribution of Consumer Cyclicals victims by Industry differs slightly from June, with Specialty Retailers as the most targeted with 10 cases (2nd place in June), Hotels & Entertainment Services in second with 8 cases (4th place in June) and finally Media & Publishing in third with 7 cases (the same as in June).

It is surprising to see such a sizeable decline in the interest of Homebuilding & Construction supplies (57% decrease from June to July) alongside a sizeable increase in the targeting of Hotels & Entertainment Services (60%) and Specialty Retailers (100%).

NCC Group suggest that threat actors are increasingly concentrating on the industries with vast quantities of customer Personally Identifiable Information (PII), as opposed to those industries that would be more effected by operational disruption.

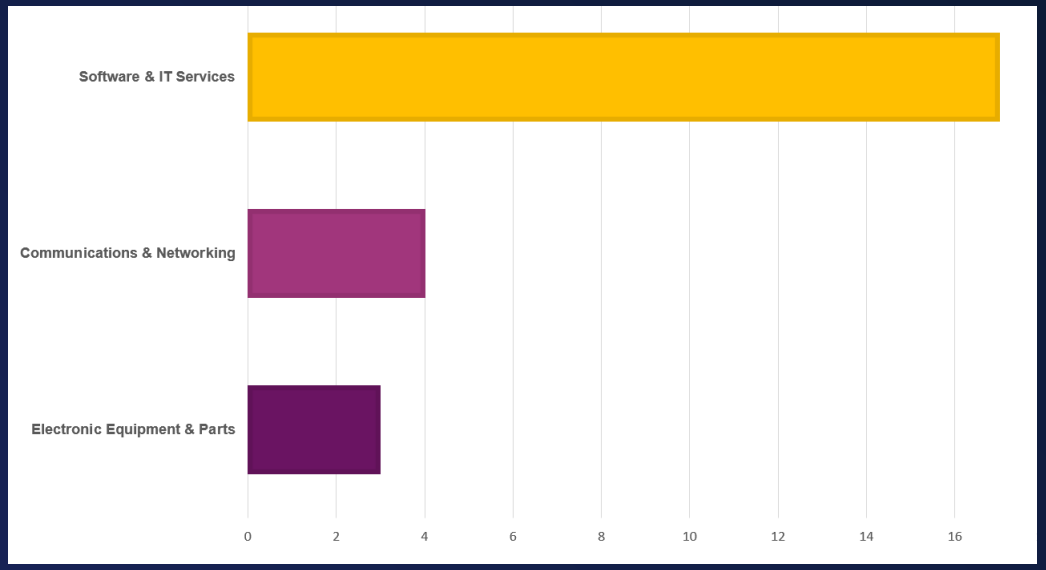


Figure 5: No. of Hack & Leak Victims for the Technology Industries July 2022

Technology

Finally, the Technology sector is the third most targeted sector in July of 2022, with the industry primarily targeted being Software & IT Services.

NCC Group assess that the focus on this sector is for a number of reasons; the first being the fact that some IT Services can be exploited for supply chain attacks (e.g. via widely distributed software), as well as the valuable Intellectual Property (IP) that is frequently present within organisations residing within these industries.

July highlights some interesting developments in the targeting of the industries within the Technology sector.

Firstly, two industries are missing from July's data; Computers, Phones & Household Electronics and Semiconductors & Semiconductor Equipment, implying that the threat actor interest within these industries has all-but disappeared in July.

Additionally, there has been an increased interest in Communications & Networking and Electronic Equipment & Parts, particularly the former (400%).

NCC Group will continue to monitor the Hack & Leak cases present within the Technology sector to see if this is an anomaly or an emerging trend.

Threat actors

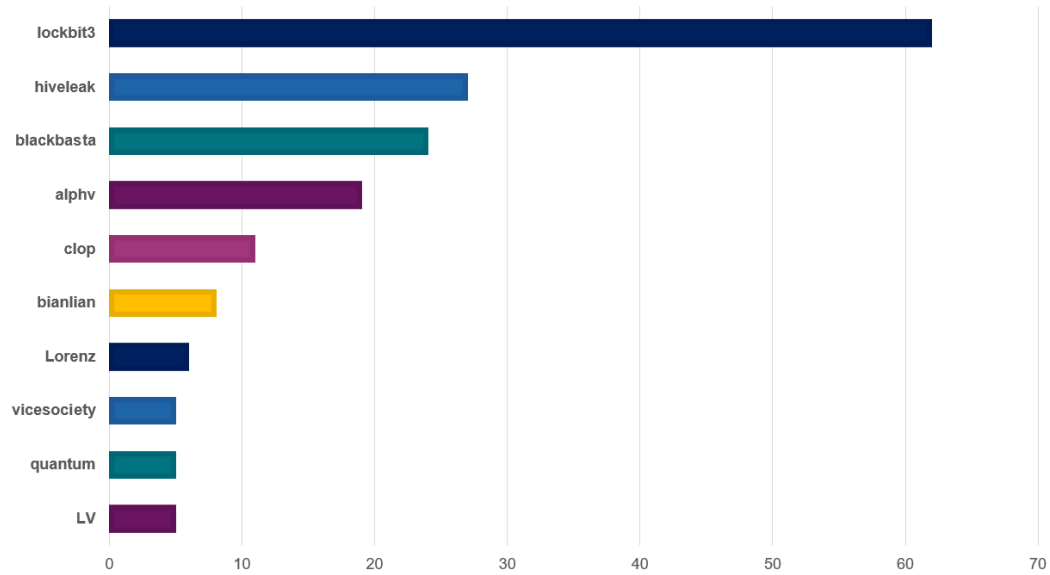


Figure 6: Top 10 Threat Actors July

In July, our top three threat actors were Lockbit 3.0, Hiveleaks and BlackBasta. Lockbit 3.0 maintains its top position, as the new variant of the Lockbit strain evolves and bounty bug programs are encouraged.

Hiveleaks and BlackBasta, both associated with Conti as either affiliates (the former) or a replacement strain (the latter), account for second and third position.

If, as we suspect, these groups are working alongside ex-Conti members and/or employing their TTPs, we would expect the number of incidents for which they are responsible to place highly, sitting just behind Lockbit 3.0, as is the case here.

As such, it appears that it has not taken long for Conti's presence to filter back into the threat landscape, albeit under a new identity. In July, our top three threat actors were Lockbit 3.0, Hiveleaks and BlackBasta.

Lockbit 3.0 maintains its top position, as the new variant of the Lockbit strain evolves and bounty bug programs are encouraged. Hiveleaks and BlackBasta, both associated with Conti as either affiliates (the former) or a replacement strain (the latter), account for second and third position.

If, as we suspect, these groups are working alongside ex-Conti members and/or employing their TTPs, we would expect the number of incidents for which they are responsible to place highly, sitting just behind Lockbit 3.0, as is the case here. As such, it appears that it has not taken long for Conti's presence to filter back into the threat landscape, albeit under a new identity.

LockBit 3.0

Lockbit 3.0 were responsible for 62 ransomware attacks in July, a 19.2% percentage increase from June (52 incidents). Activity therefore remains largely similar to that of the previous month, with no major change.

Reasons for this may concern continued changes/edits made under the new ransomware variant and/or a quieter summer period. That said, Lockbit 3.0 maintain their foothold as the most threatening ransomware group, and one with which all organisations should aim to be aware of.

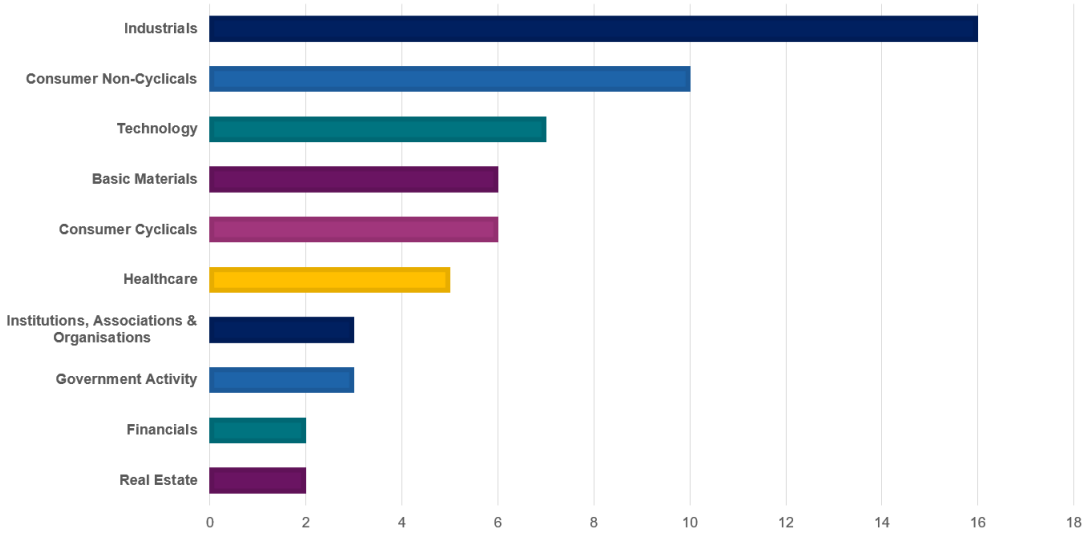


Figure 7: Top 10 Sectors Targeted by Lockbit 3.0

Sectoral Targeting:

- Industrials remains the prime target accounting for 26% of attacks, followed by Consumer Non-Cyclicals (16%), and Technology (11%).

Industry Targets

- Professional & Commercial Services lead representing 18% of incidents, followed by Food & Tobacco (10%), Software & IT Services and Construction & Engineering

As no changes to sector preference continue to be observed, we predict that this will remain the same in the coming months.

Professional & Commercial Services remains the most targeted industry as they encompass a wide variety of organisations, whilst all other industries continue to vary.

We therefore expect fluctuations in industry targeting outside of Professional & Commercial Services moving forward, meaning no organisation is immune.

Hiveleaks

Hiveleaks moved up from seventh place in June with 5 attacks, to second place in July with 27 incidents identified, representing 13% of total activity in July.

This reflects a rather substantial activity growth at a 440% increase, and raises the question as to whether this group will place as a top 3 threat actor in the coming months.

As identified in our last monthly reports the threat landscape has since changed due to Conti's disbanding, and noting Hiveleaks' affiliation with Conti, their prominent growth may reflect a possible grouping of the two.

If so, the group will certainly remain one to watch, as we would expect their capability and reach to grow accordingly.

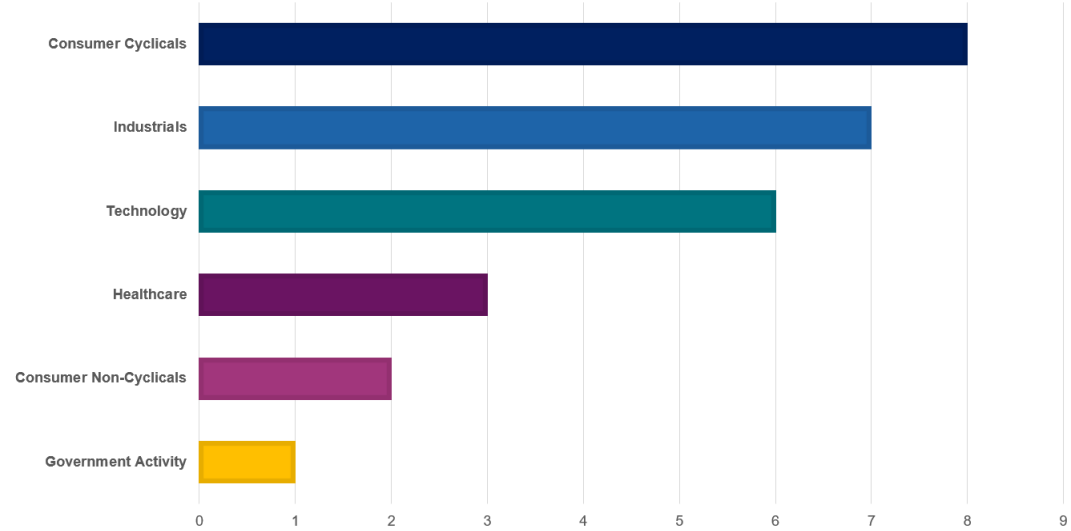


Figure 8: Top 10 Sectors Targeted by Hiveleaks

Sectoral Targeting:

- Consumer Cyclicals accounted for most of the targeted incidents (30%), followed by Industrials (26%) and Technology (23%).

Industry Targets

- Software and IT Services (19%), Professional & Commercial Services (11%), Media & Publishing (11%), and Healthcare Providers & Services (11%).

Although the orders are reversed, again the focal point of sectoral targeting remains around Consumer Cyclicals, Industrials and Technology.

This continues to reinforce the notion that these three sectors are attractive targets and we are likely to observe this trend over the coming months.

Industry targeting paints a different picture to that of Lockbit 3.0, but echoes the idea that industry targeting is highly varied and therefore all organisations should continue to promote strong cyber hygiene.

BlackBasta

In July, BlackBasta moved down from second to third most prominent threat actor although there is an increase in the number of total attacks from 16 in June to 24 this July, and accounts for 12% of total targeting activity.

As we continue to move into the second half of 2022 and BlackBasta establishes themselves further, we are likely to observe a growth in ransomware numbers.

Sectoral Targeting:

- Consumer Cyclicals accounted for the majority of ransomware attacks with 46%, followed by Industrials (33%) and Technology (13%).

Industry Targets

- The most targeted industries were Speciality Retailers (13%), followed by Professional & Commercial Services (8.33%), Household Goods (8.33%), Homebuilding & Construction Supplies (8.33%), Software and IT Services (8.33%), Aerospace & Defense (8.33%).

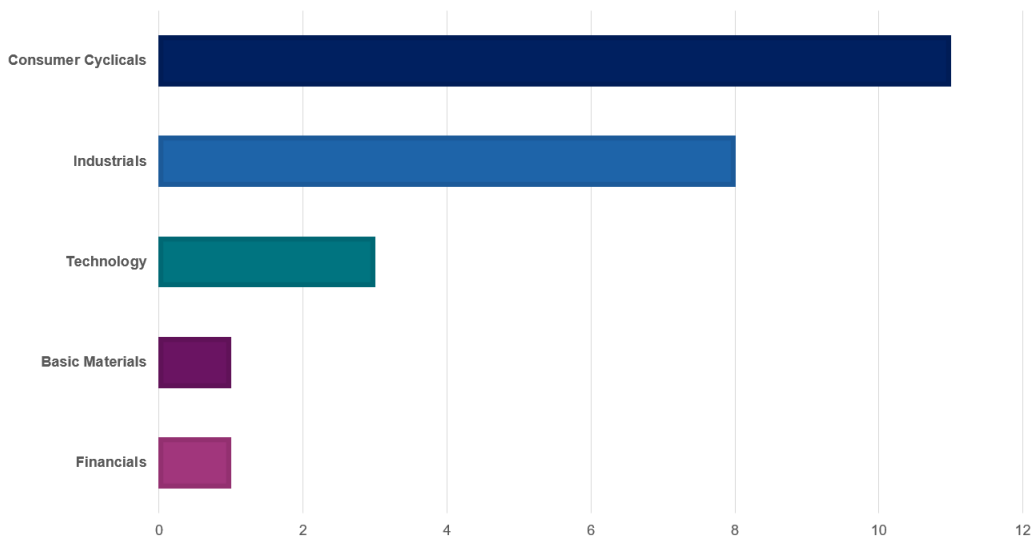


Figure 9: Top 10 Sectors Targeted by BlackBasta

A trend in ransomware targeting is further observed as BlackBasta demonstrates the same interest in the top three targeted sectors as Lockbit 3.0 and Hiveleaks, reiterating their prominence.

It is worth noting that BlackBasta's overall sectoral focus is much narrower than that of the abovementioned groups and therefore demonstrates a more specific targeting approach.

The industries identified, however, remain highly varied and illustrates how it is much harder to identify key industries within that may be vulnerable.

Best practice would therefore concern organisations identifying whether they sit within the main sectors of interest, and familiarising themselves with BlackBasta's TTP's in order to adopt a proactive over reactive approach to ransomware protection.

Regions

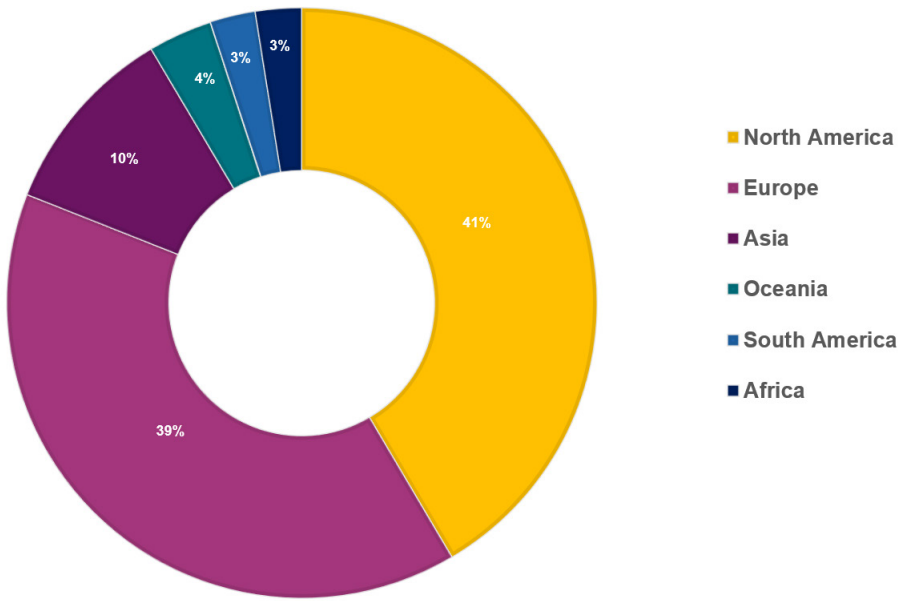


Figure 10: Percentage of Hack & Leak Victims by Region

This month, North America tops the list of regions with the most ransomware attacks with 83 incidents (42%) and Europe closely behind with 79 incidents (40%).

This is a deviation from the reports in May and June where Europe had the most attacks with 93 (39%) and 56 (41%) incidents; and North America with 86 (37%) and 49 (36%) incidents respectively.

This indicates a refocus on North American organisations, and with Europe closely behind it is important that organisations within these regions continue implementing preventive security controls to ensure the security of their assets.

Irrespective of the deviation in positions held by North America and Europe in the past three months, Asia has remained the third most attacked region.

This month Asia has 21 incidents (11%) reported, followed by Oceania with 7 (4%) incidents, South America with 5 (3%) incidents and Africa with 3 (2%) incidents. July reflects a total of 198 incidents showing an increase of 63 (47%) incidents.

Although the number of incident reports this month does not reflect a major increase, it does indicate that threat actors remain active in attacking organisations across regions and continuous vigilance is essential to stay protected against their exploits, tactics, and techniques.

Threat actor spotlight:

North Korean cyber operations

The North Korea-backed APT Group Lazarus have been making serious ripples in the cyber threat landscape in the first half of 2022. Historically, Lazarus Group have long been associated with committing financial cybercrime to facilitate the states agenda, in fact, according to a report released by Chainanalysis in February, the greatest share of North Korea's 2021 GNP was illegal revenues (10%).

This activity has continued in 2022 with enormous cryptocurrency thefts and even the suspected adoption of ransomware, likely as a method for generating more revenue. In this spotlight we will take a deep-dive into Lazarus Group's recent campaigns and modes of operating.

Before we look deeper into their recent operations, we should ask; why has there been a noticeable prominence of North Korean threat actor campaigns in 2022? There are many possible influences, one being the current state of their economy, which shrank for the second year running in 2021, possibly forcing North Korea to lean more heavily on illegal methods of revenue generation to compensate for their continued economic hardships.

Furthermore, many of their targets are either in the West or in the APAC region, both of which have seriously strained geopolitical relations with North Korea. North Korea have accused United States, Japan and South Korea of being in danger of forming an 'Asian version of NATO.'

Considering these associations and the existing economic sanctions already imposed by the European Union, paired with North Korea's struggling economy, it is possible to see why they would turn to offensive cyber operations as a source of income and why their targets would lie within the West or APAC (as they so frequently do). As a result of their ramping activity, the US has responded by offering $10 Million to any individual who can provide valuable intelligence on any of the operators within Lazarus Group; Bluenoroff, Andariel, APT38, Guardians of Peace, or Kimsuky. Going forward, as North Korea evidently see the advantages of crypto-theft, and possibly even ransomware operations, we may see their financial cybercrime presence increase in pursuit of financial security.

$600 million cryptocurrency heist on Axie Infinity

On the 23rd March 2022, the second-most costly cryptocurrency theft of all time occurred on the Ronin network, which is an Ethereum-linked sidechain used for the NFT blockchain game Axie Infinity, and was undertaken by North Korea's Lazarus Group.

The heist was achievable through delivering a fake job offer for a fictitious organization in the form of a pdf to an Axie Infinity senior engineer, who subsequently applied for the position. This attack resulted in the loss of at least $540 million in cryptocurrency, with estimates as high as $625 million.

The fake job offer was delivered to the victim via LinkedIn, and the malicious pdf document allowed spyware to be deployed on Ronin's systems. Following this initial access, Lazarus Group gained control of four of the total nine validator nodes on the Ronin network; just one validator short of complete control of the network. As stated by Radix, a validator node is "a special type of full node that participates in 'consensus.' By participating in consensus, validator nodes become responsible for verifying, voting on, and maintaining a record of transactions."

On the Ronin network, the validators facilitate a 'proof of authority' system for signing transactions, where five of the nine validators must approve a transaction before it is carried out. As Lazarus at the time only had four of the five validators within their control, they went on to compromise the Axie Decentralised Autonomous System (DAO), a group set up to support the Axie Infinity game, in order to finalise their operation. Consequently, Lazarus were able to verify and vote on their own transactions, allowing them to exfiltrate such a large quantity of cryptocurrency.

In a blog post by the games developers, Sky Mavis said "The Axie DAO allowlisted Sky Mavis to sign various transactions on its behalf. This was discontinued in December 2021, but the allowlist access was not revoked". "Once the attacker got access to Sky Mavis systems they were able to get the signature from the Axie DAO validator."

$100 million crypto heist on Harmony's Horizon Bridge

On the 23rd June 2022, Harmony were alerted of a cyberattack on their proprietary Horizon Ethereum Bridge, wherein eleven separate transactions took place and $100 million in crypto assets were transferred from the bridge. The assets stolen included Ethereum, Binance Coin, Tether, USD Coin, EOS, and Dai. Similarly to the Ronin network attack and many previous cryptocurrency thefts, the hack was performed by compromising the cryptographic keys of a multi-signature wallet (a digital wallet that requires more than one private key to sign and authorise a crypto transaction), a tactic which indicated Lazarus Group as the perpetrator.

Furthermore, the Tornado Cash mixer was utilised to 'launder' the money, which is another behavior closely associated with Lazarus Group. Tornado Cash is a mixer that is often used to reroute illegitimately obtained cryptocurrency funds, in an effort to disguise the origin of the digital assets. Finally, North Korea's Lazarus Group have exhibited a recent transition into the targeting of Decentralised Finance (DeFi) networks, such as blockchain bridges.

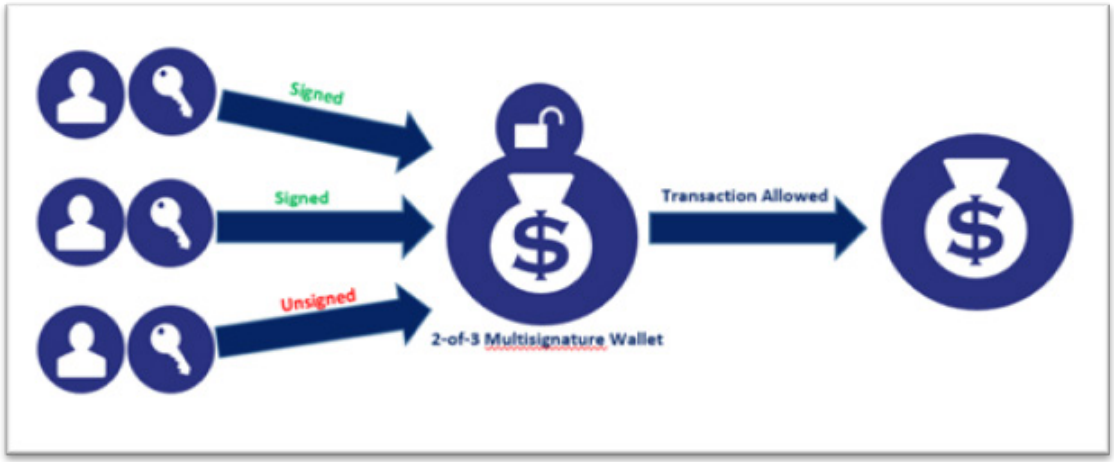


Figure 11: How a Multisignature Wallet Works

Lazarus Group associated with VHD, Maui and H0lyGh0st ransomware strains

Following an analysis conducted and published by Trellix on the 3rd May 2022, it is likely that the ransomware family 'VHD' (which was initially observed in March of 2020) can be attributed to Lazarus Group, due to the similarity in function blocks within the code and the generic distribution of targets.

Given that ransomware strains are frequently associated with financially motivated Organised Crime Groups, it is interesting to see a state-sponsored and highly capable threat actor possibly adopt this approach to revenue generation.

One might ask if we will see more nation-states pursue this method of attack in the future? Alternatively, will North Korea's strain (or a future iteration) develop into one with previously unseen capability, given the technical knowledge and aptitude that they have at their disposal?

As touched upon, the parallels were drawn after reviewing the VHD source code and spotting similarities between it and other ransomware strains; implying re-usage of existing code.

Trellix, upon identifying these blocks searched for similar ransomware families that contain these same functionalities within their source code, identifying the following:

- BEAF ransomware
- PXJ ransomware
- ZZZZ ransomware
- CHiCHi ransomware

Following the discovery of these individual families, Trellix conducted comparison analysis within the code blocks, as opposed to generic functions, which could easily have been coincidental. They found that BEAF and ZZZZ were almost clones of one another, both of which shared a substantial amount of code with VHD, as shown in the below visualization. Comparatively, as Tflower and CHiCHi only shared very generic functional similarities with the other families, they were not correlated.

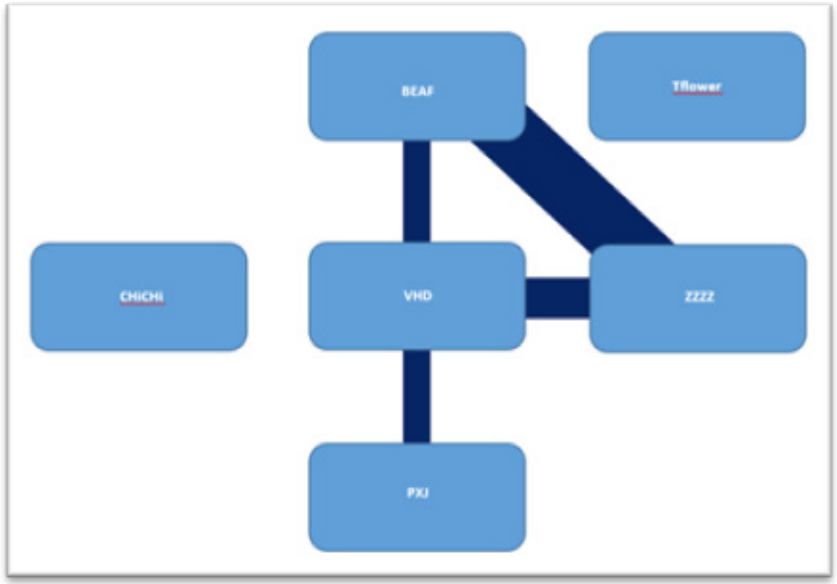


Figure 12: Code Similarity Based on Code Blocks and Functions

Trellix were able to visualize the code similarities and differences between the families by using Hilbert curve mapping, which again shows definite similarities between the BEAF, ZZZZ, PXJ and VHD strains:

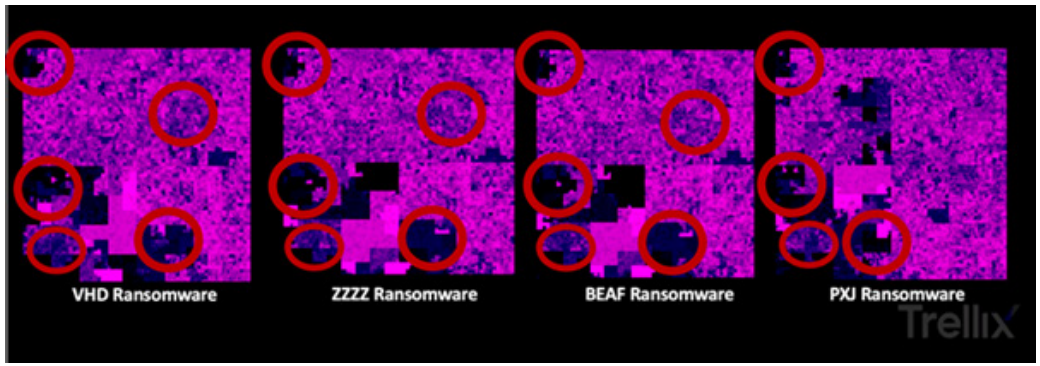


Figure 13: Hilbert Curve Similarities (Trellix)

So how does any of this indicate, with any amount of confidence, that the VHD ransomware family is associated with North Korea or specifically, Lazarus? Independently it does not, however, if we consider the geography of the attacks carried out by these ransomware families, we can see a very narrow distribution of specifically targeted victims; typically around the APAC region; a region strongly considered to be a primary target of North Korea. Trellix suggest that "these attacks might have been executed to discover if ransomware is a valuable way of gaining income," and attribute these ransomware families to DPRK-sponsored threat actors.

Lazarus Group targets crypto experts with fake Coinbase job offers

At the time of writing, security researcher Hossein Jazi posted a tweet regarding a new social engineering campaign being conducted by Lazarus Group. The campaign, targeted at individuals who work within the FinTech industry, involved distributing fake job offers that were supposedly from Coinbase.

The advertised role was that of "Engineering Manager, Product Security", given Coinbase is one of the most well-known and successful cryptocurrency exchange platforms globally, the job offer was inevitably an enticing opportunity for the victims. Lazarus Group are well known for their highly sophisticated social engineering campaigns, with this instance being reminiscent the Axie Infinity attack mentioned above, resulting in losses of over of $600 million in crypto assets.

Similarly to the Axie Infinity social engineering attack, this recent campaign features what appears to be a pdf file (purporting to be a career opportunity), that was actually a malicious executable with a pdf icon named 'Coinbase_ online_careers_2022_07.exe'.

When opened, the executable would display the below fake document while simultaneously loading a malicious DLL:

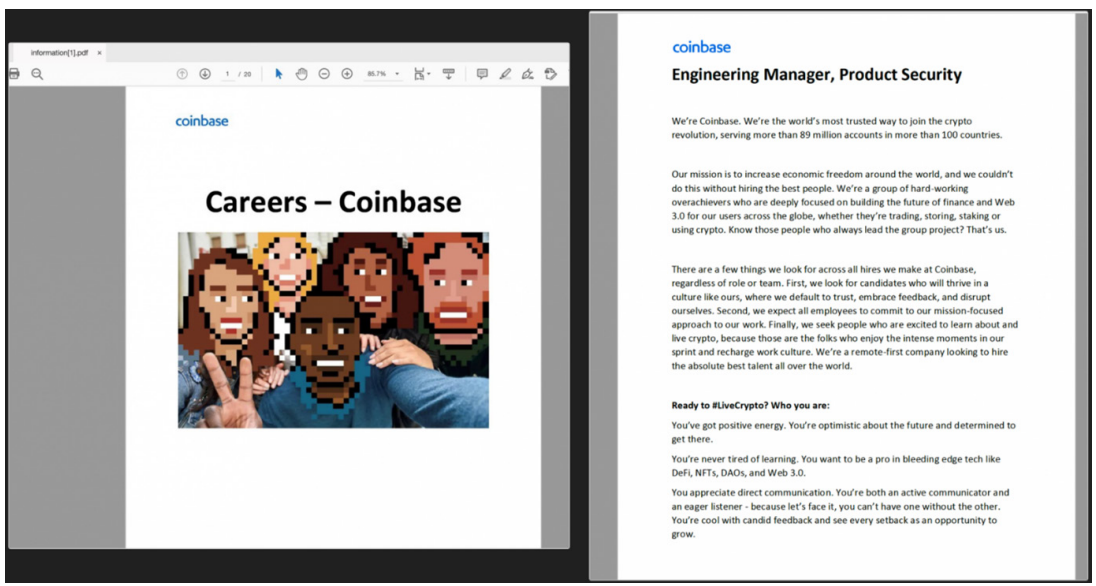


Figure 14: Decoy PDF Displayed When Running Fake PDF Executable

Upon execution, the malware communicates with a C2 server via GitHub to run commands on the compromised system. Jazi has stated that the infrastructure used in these phishing campaigns overlaps with previous ones carried out by the threat group, thus indicating their involvement.

This is yet another, very recent example of North Korea's involvement in offensive cyber operations targeted at the Financials sector in the West.

Lazarus' evolving modus operandi, and next steps

It would seem that North Korea is indeed beginning to see the advantage of ransomware, as there have been yet more reports of strains linked to them in July.

Firstly, the Cybersecurity & Infrastructure Security Agency (CISA) released an alert on the 6th of July regarding the Maui ransomware strain (thought to have first been observed as early as May 2021), primarily targeting the healthcare sector (reportedly, solely for operational disruption).

Additionally, multiple articles surfaced around mid-July regarding yet another suspected North Korean ransomware operation dubbed H0lyGh0st, attacking a variety of small businesses in a wide distribution of countries.

Interestingly, this operation does employ a double extortion methodology and features a leak site where exfiltrated data is posted, unlike VHD and Maui.

At the time of writing, the leak site used by the group was found to be down.

Figure 15: H0lyGh0st Leak Site

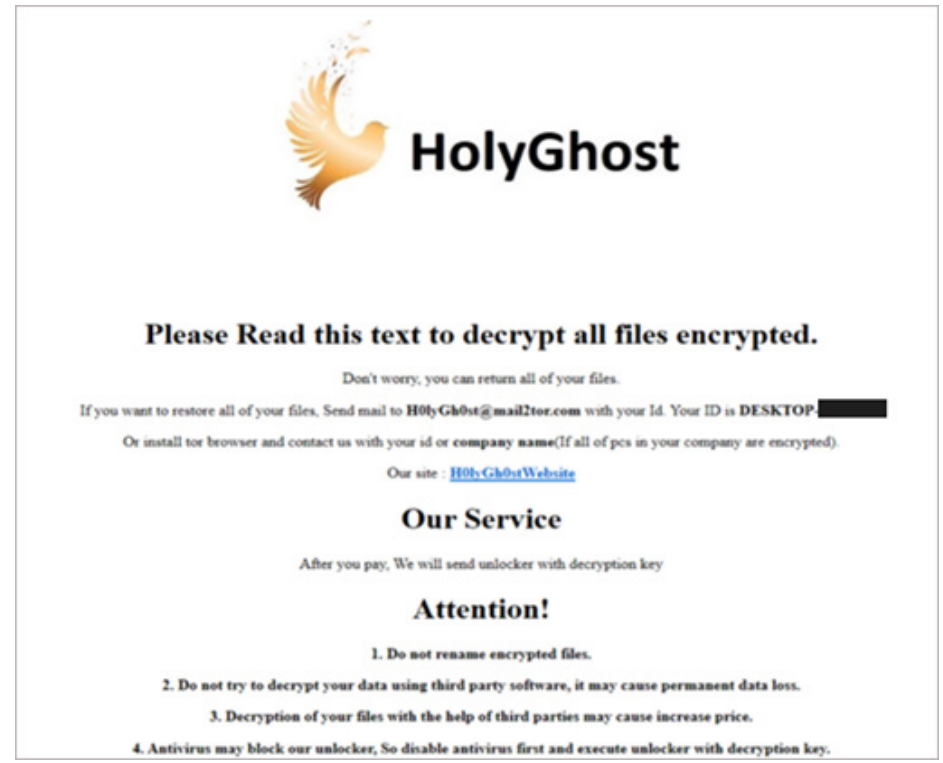


Figure 16: H0lyGh0st Ransom Note

H0lyGh0st is less easy to attribute to the North Korean government given the random victim distribution, lack of frequency of the attacks, and the transition to data exfiltration. It has been suggested that H0lyGh0st is perhaps an independent project performed outside of the government's input, for the personal financial gain of the threat groups typically associated with state-sponsored operations.

About the NCC Group Monthly Threat Pulse

NCC Group's Strategic Threat Intelligence Practice gathers data on ransomware data leaks on the dark web in real time to get regular insights into who are the most recent ransomware victims.

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