Monthly Threat Pulse
May 2022

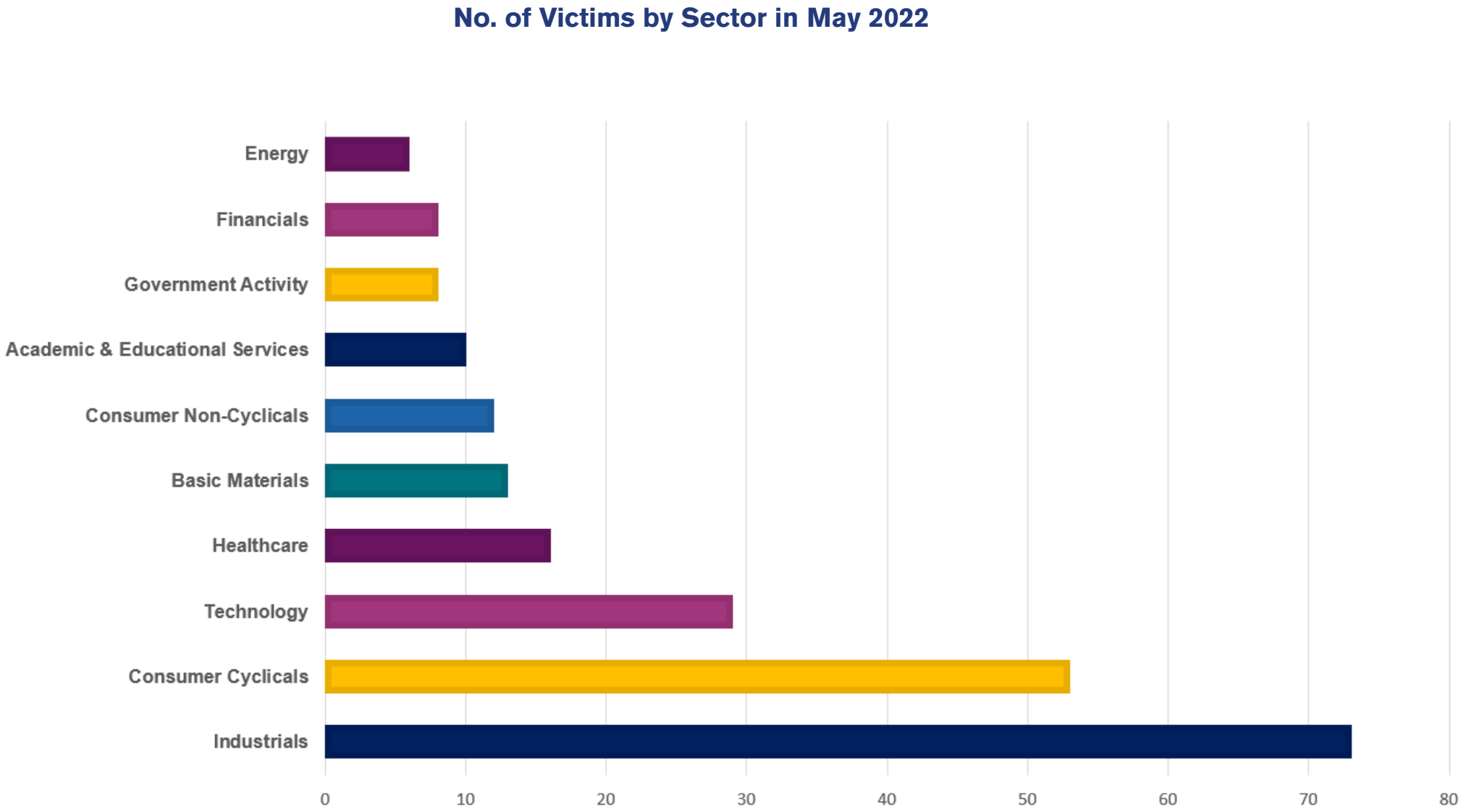
We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

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

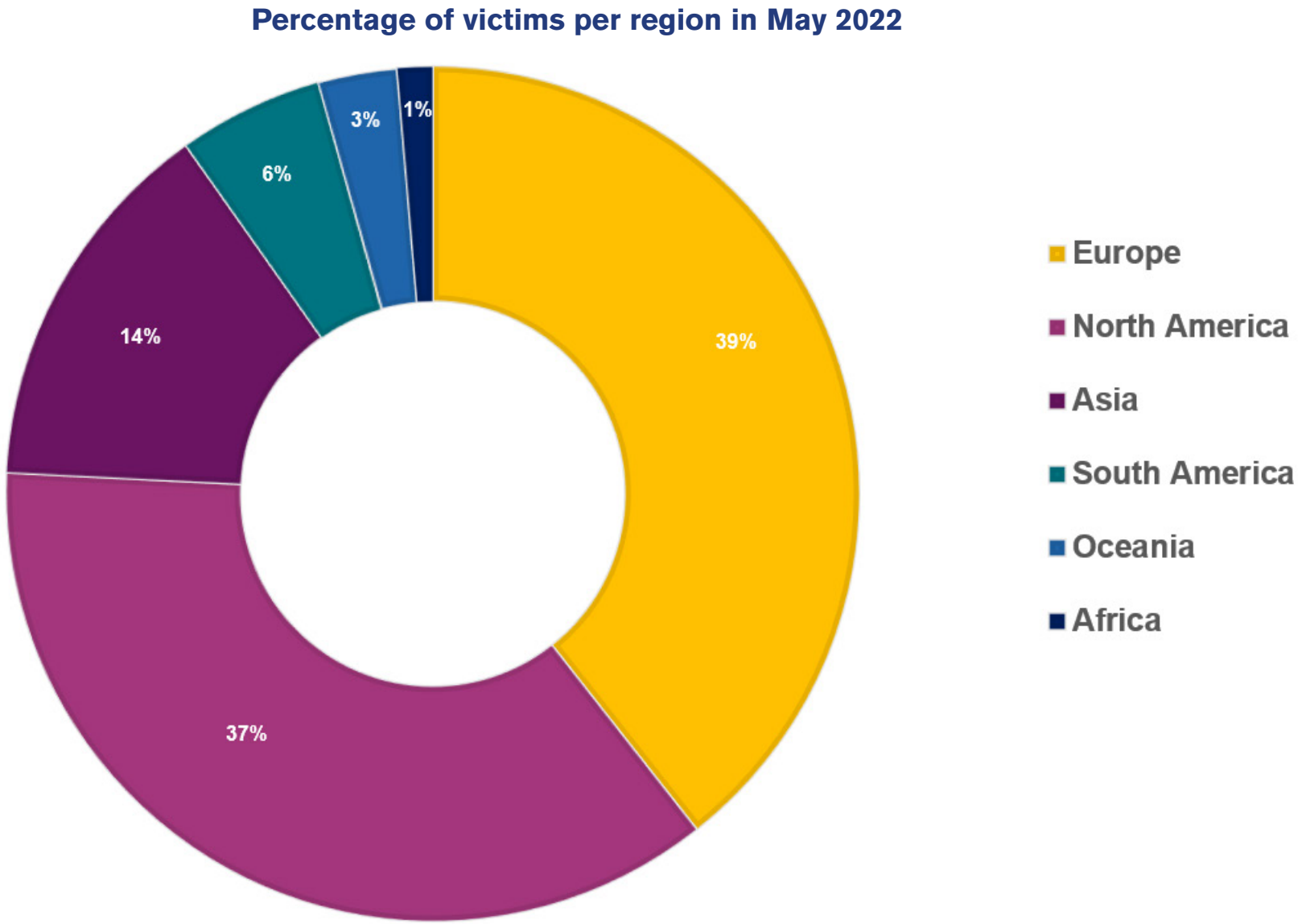
Key data


Number of Victims by Group in May 2022
Lockbit 2.0
Conti
blackbasta
hive
BlackCat
mindware
Vice Society
CL0P
BlackByte
kelvinsecurity
0
10
20
30
40
50
60
70
80
90
100

Key data


No. of Victims by Sector in May 2022
Energy
Financials
Government Activity
Academic & Educational Services
Consumer Non-Cyclicals
Basic Materials
Healthcare
Technology
Consumer Cyclicals
Industrials
0
10
20
30
40
50
60
70
80

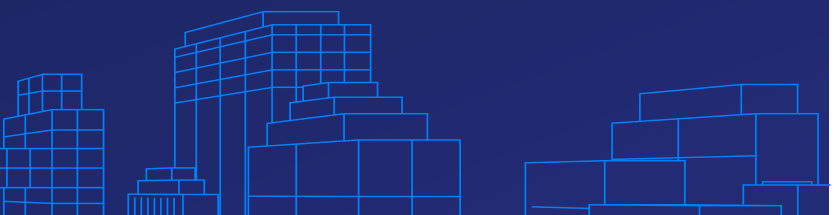
Key data


Percentage of victims per region in May 2022
39%
37%
14%
6%
3%
1%
Europe
North America
Asia
South America
Oceania
Africa

Analyst comments

In May we observed an 18% decrease in ransomware attacks compared to April with the number of incidents decreasing from 289 in April to 236 in May.

This decrease represents the first decline in ransomware hack & leak cases since December 2021 – January 2022, which may have several contributing factors; including Conti's step back and collaboration/ rebranding with 'smaller ransomware groups.



Sectors

Although there has been an 18% decrease in the total hack & leak ransomware cases in May, the top 3 most targeted sectors remain to be Industrials with 73 incidents (31%), Consumer Cyclicals with 53 (22%) and finally Technology with 29 (12%).

Aside from the Industrials sector which accounted for 100 incidents (48%) in April, the targeting in these two months is similar with 54 incidents in Consumer Cyclicals (19%) and 29 in Technology (10%).

As Conti is usually one of the biggest contributors to attacks within the Industrials sector (16 attacks or 16% in April and as high as 31 attacks or 32% in March), we can partially attribute this decline to them as they only had 8 Industrials victims in May (11%).

As we have touched upon in previous threat pulses, these three sectors are likely to remain as the top three most targeted, with minor fluctuations between second and third. This is mostly due to the diverse nature and vast number of different organisations operating within these sectors (particularly Industrials).

This is also likely a result of the personally identifiable information (PII) and intellectual property (IP) that organisations within these sectors store, which are attractive targets for extortive ransomware gangs.

Industry analysis within the Industrials sector revealed some disparity between April and May. In April, Professional & Commercial Services held the most targets with 47 attacks (47%), Construction & Engineering followed with 22 (22%) and Machinery, Tools, Heavy Vehicles, Trains and Ships with 16 (16%).

Professional & Commercial Services are the most targeted in May with 28 incidents (38%), however, 3 industries shared second place. Accounting for 12 attacks individually (16% each), these concerned; Construction & Engineering, Freight & Logistics, Machinery, Tools, Heavy Vehicles, Trains & Ships. The third most targeted industry was Passenger Transportation Services with 5 incidents (7% each).

Fluctuations in industry targeting shows the importance for a cross-industry cybersecurity response to account for uncertainty and ensure protection across the board.

Threat Actors

Lockbit 2.0

Lockbit 2.0 remained the dominant threat actor accounting for 95 of the reported 236 incidents (40%).

Whilst their top position is not new, the major discrepancy between the number of attacks conducted and the remaining threat actors makes their dominant position more prominent.

This sizeable gap is unusual as we normally observe a greater number of attacks by those groups in second or third place, albeit secondary to Lockbit 2.0. For example, in April, Lockbit 2.0 were responsible for 103 out of 289 attacks (36%), Conti 45 (16%) and BlackCat 24 (8%). In May the pattern sits as follows: Lockbit 2.0 95 (40%), Black Basta 17 (7%), Conti, 17 (7%), Hive 17 (7%).

Many reasons may explain this difference, such as changes to the targeting behaviour of other ransomware groups. However, despite this, and even considering fluctuations in Lockbit 2.0s own targeting, the group remains highly prominent and continues to cement their place as 2022's most prolific threat actor.

Consequently, it is crucial for organisations to be familiar with the tactics, techniques, and procedures (TTPs) associated with the group, and the organisations victimised, to gain a stronger understanding of targeting risks and relevant security measures to implement.

These can be identified within our Conti research blog: Conti-nuation: methods and techniques observed in operations post the leaks – NCC Group Research

In May, Lockbit 2.0 focused predominantly on the following sectors, Industrials with 29 incidents (31%), Consumer Cyclicals with 25 (26%), Technology, 8 (8%) and Consumer Non-Cyclicals, 8 (8%). The group continues to follow the same pattern where the Industrials, Consumer Cyclicals and Technology industries are the main focus, now with the addition of Consumer Non-Cyclicals.

The substantial risk of major operational disruption within each of these industries likely motivates ransomware attacks as the need to resume activity hopes to pressure organisations into payment. Organisations within these sectors should anticipate targeting and ensure strong cyber security hygiene to minimise risk.

Industry analysis also revealed the targeting of Professional and Commercial Services with 12 incidents (13%), Speciality Retailers, 9 incidents (9%), and Hotels and Entertainment Services, 7 incidents (7%).

Professional and Commercial Services has remained in first place since January 2022, companies within should take note of this persistent threat to protect against as the targeting pattern anticipates future attacks. Both second and third places fluctuate, stressing the importance for all industries to equally adopt a rigorous approach.

Conti discontinued?

In May, second place was shared amongst three threat actors, the recently discovered ransomware gang Black Basta, Hive and Conti, with 17 incidents respectively.

Notably, security researchers suspect Black Basta and Hive to be working alongside Conti and/or, functioning as a possible replacement for Conti themselves, following Conti's rumoured shutdown.

The internal politics identified in April and early Spring were followed by the shutdown of Conti News on May 19th (the ransomware group's official website), negotiations service, as well as certain infrastructure, including chat rooms, messengers, servers and proxy hosts undergoing a major reset, alluding to the possibility that Conti 'can no longer sufficiently support and **obtain extortion**.

Whilst the public-facing Conti News site remains online and accessible, Bleeping Computer reported that 'the Tor admin panels used by members to perform negotiations and publish "news" on **their data leak site are now offline**.'

Advintel's research blog marks this as the 'end of Conti's Brand' and one that will lead to a new chapter for the threat landscape, and **has been echoed by other cybersecurity experts.**

What might this look like? Conti are anticipated to make use of existing subsidiaries operating under different names such as KaraKurt, BlackByte and BlackBasta. This rebrand is anticipated to be a division into smaller groups, in which Conti's leaders are dispersing into Conti-loyal groups such as Hive, BlackCat and AvosLocker, rather than creating another major ransomware **organisation that dominates the threat landscape**.

In addition, the following partitions disclosed in Advintel's research are believed to have been created prior to the shutdown process:

Type 1: Fully autonomous groups:

- Karakurt
- Black Basta
- Black Byte

Type 2: Semi-autonomous groups:

- AlphV/BlackCat
- HelloKitty/FiveHands
- AvosLocker

Type 3: Independent affiliates with other collectives in order.

Type 4: Mergers & Acquisitions:

Conti leadership infiltrates an already existing small-brand and consumes it entirely, keeping the small brand name. The small group's leaders lose their independence however receives a massive influx of manpower, while Conti receives a new subsidiary group.

This rebrand is also a possible repercussion of Conti's announced allegiance with Russia in the Russia-Ukraine war, now suffering lost payments as a consequence.

Solidarity with the Kremlin is proposed to have made financial extortion all the more challenging, leaving them unable to receive ransom payments as companies are advised that any pay-outs violate U.S economic sanctions on **Russia**.

Ultimately, Conti appear to have lost the once strong foothold they maintained in the cybercrime landscape, at least under their name.

Conti Activity in May

In line with the rumors of retirement our ransomware database demonstrates that the group, whilst still active in May, illustrates a marked decline in activity. These variations in Conti's activity have continued since April, in which we observed a decline from 71 incidents in March to 45 in April, (37% decrease), and now a 62% decrease from 45 incidents in April to 17 in May.

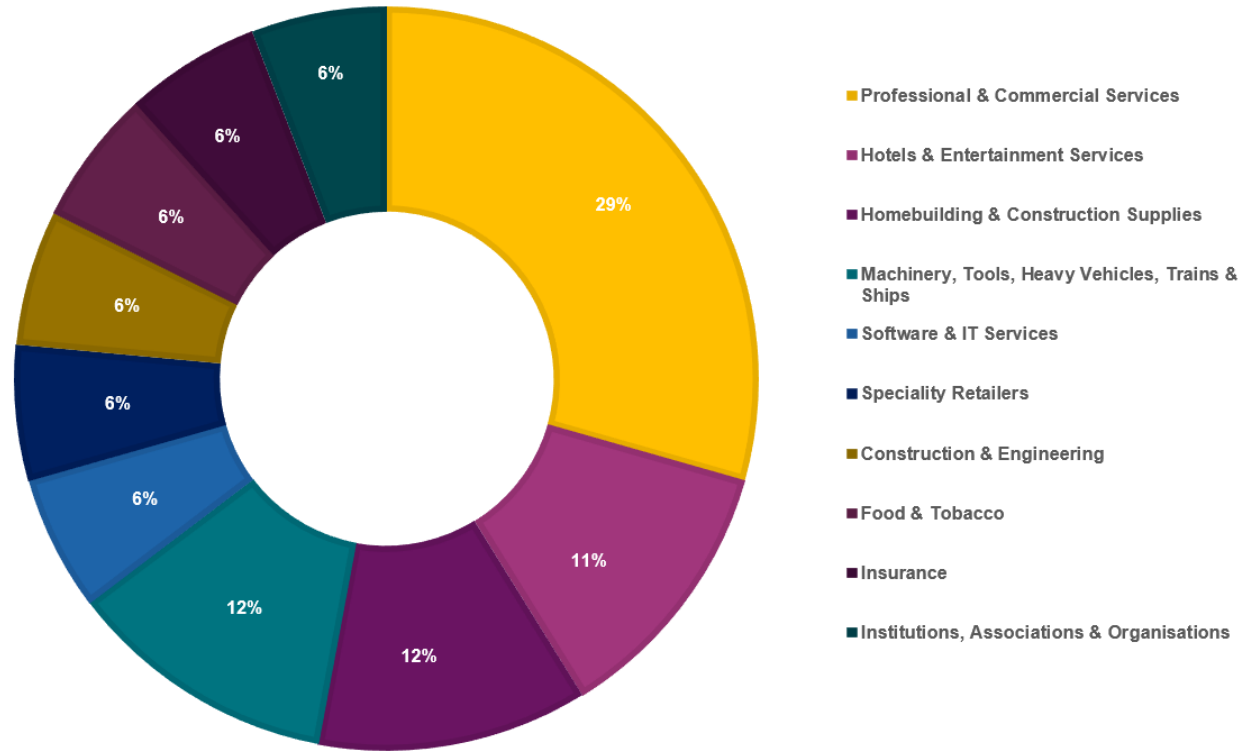
Within this, Conti's top two targeted sectors were the Industrials with 8 incidents (47%), Consumer Cyclicals with 5 incidents (29%), and Financials, Consumer Non-Cyclicals, Institutions, Associations and Organisations and Technology, sharing third place with 1 incident respectively (5.88% each). Whilst the Industrials and Consumer Cyclicals remain at the forefront, victims by sector are more dispersed when compared to previous months; in April, there were three clear dominant sectors Industrials, Consumer Cyclicals and Technology.

This should signal to organisations that Conti's targeting behaviour at present is not fixed and that variations may arise, even where numbers are limited.

Likewise, since January, there has been much disparity in Conti's third most targeted sectors. As such, any organisation currently not identified in the group of sectors above should not take this as a sign of being in the clear, but must continue to be vigilant and implement strong cyber security measures nonetheless.

Industries within revealed Professionals & Commercial Services as the most targeted, accounting for 5 incidents (29%). Second and third place were shared across 9 other industries, with 2 or less incidents. Similarly to the sectoral analysis, we observed a variety of victims revealing a limited targeting structure at present.

Aside from a continued interest in the Professionals & Commercial Services, this signals a more random attack pattern. From a prevention standpoint, organisations across all industries should maintain a rigorous cyber security posture.



Rebranding and/or Support for Conti

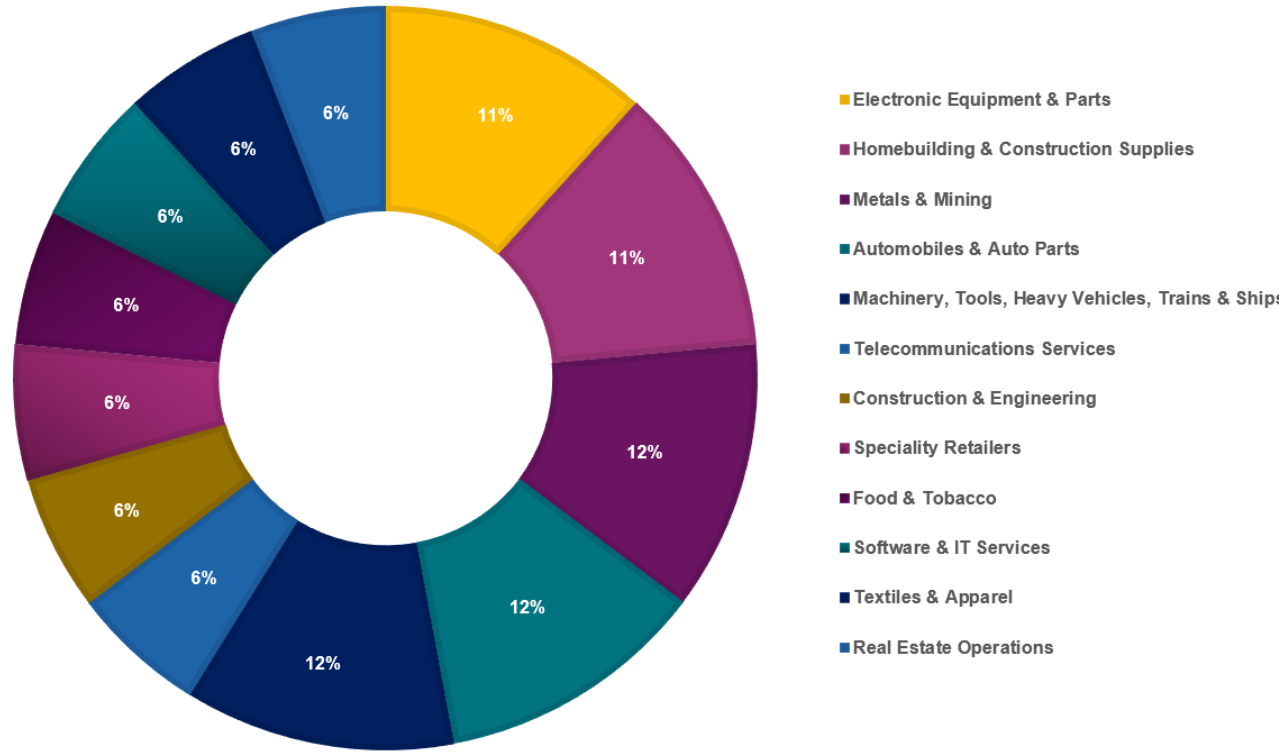
Black Basta

Two ransomware groups prominently discussed by security researchers as supporting the rebrand of Conti are Black Basta and Hive. Research by Trend Micro and Cyble pinpoint similarities between Black Basta and Conti, including the ransomware data leak site, victim recovery portals, support systems and negotiation style. This familiarity was further noted in online Twitter discussions by the MalwareHunterTeam and Arkbird . At the same, this has been refuted by researchers, although they do not deny the possibility that members may be affiliated from previous experiences and therefore working together.

In May, we observed 17 incidents from the new ransomware gang Black Basta who were quickly identified following breaches to multiple organisations in a short time frame. The sectors most prominent within our database were: Consumer Cyclicals, 6 incidents (35%), Technology, 4 incidents (24%), and Industrials 3 incidents (18%).

Notably, their interest is aligned with the top three targeted sectors of Lockbit 2.0, and share two with Conti, further stressing their importance when it comes to sector targeting. Whilst the sectors remain clear, industry analysis was widely dispersed across 12 categories, with no more than a maximum of 2 incidents in each.

This shows a more brute-force style than a selective approach, similar to that of Conti, and as such, emphasises the importance for prevention measures to be widespread across industries as aforementioned, as we observe this trend across the different threat actors.



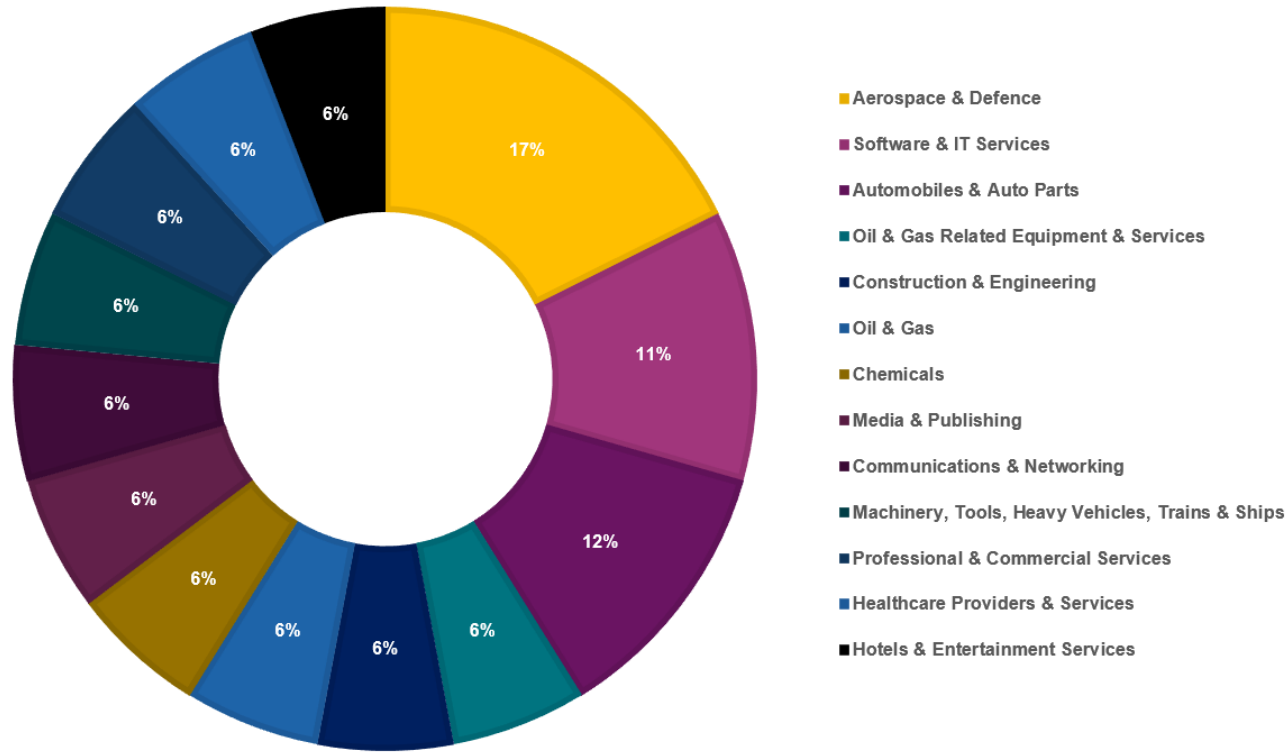
Hive

In addition to Black Basta, Hive are suspected to be supporting Conti following the high-level breaches of the Costa Rican government. Costa Rica's public health service, the Costa Rican Social Security Fund (CCSS), were forced to shut down systems subsequent to an attack by Hive ransomware. This came one week after the country declared a state of emergency as a result of cyberattacks by Conti on May 16th. It has been questioned whether Conti's attack on Costa Rica was an attempt to go out with a final bang, with Advintel reporting this to be a 'last-ditch' effort to maintain their publicity. By bringing the group into the spotlight in this way, this allowed for re-brand preparations to get underway.

Cybersecurity experts have advocated that Hive may be working with Conti to support the group with a rebrand and to evade international sanctions concerning extortion pay-outs to cybercriminals operating in Russia. It is therefore possible that cross-group working relationships have been established to work in Conti's favour.

This May, Hive were responsible for 6 incidents in the Industrials (35%), 4 in Consumer Cyclicals (24%) and 3 in Technology 3 (18%). Once again, a pattern continues to emerge with regards the favoured sectors hence organisations within should continue to be wary of future threats.

Industry analysis identified Aerospace and Defence as most targeted, Software and IT services and Automobiles and Auto Parts in joint second, with third place shared across 10 further industries with 1 incident respectively, listed below.



Regions

Organisations were predominantly targeted in Europe this May with 93 incidents (39%) but closely followed by North America with 86 attacks (37%). Asia accounted for 33 victims (14%), South America 13 (6%), Oceania 7 (3%), and Africa 4 (2%).

An interesting point to note is that for the first time in the last 6 months Europe tops the list as the region with the most attacks. Consequently, North America was displaced to second place, reflecting a shift in attack concentration from North American to European organisations.

The threat actor group with the most attacks on European organisations was Lockbit 2.0 with 48 victims (51.6%). Targeting was predominantly directed the Consumer Cyclicals (31.25%) and Industrials sectors with 15 incidents respectively (31.25% each). As observed, the Consumer Cyclicals and Industrials were prime industries of target in this region.

Therefore, it is considerable for European organisations within these sectors to implement tighter security measures to ensure they are well protected against ransomware attacks.

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.