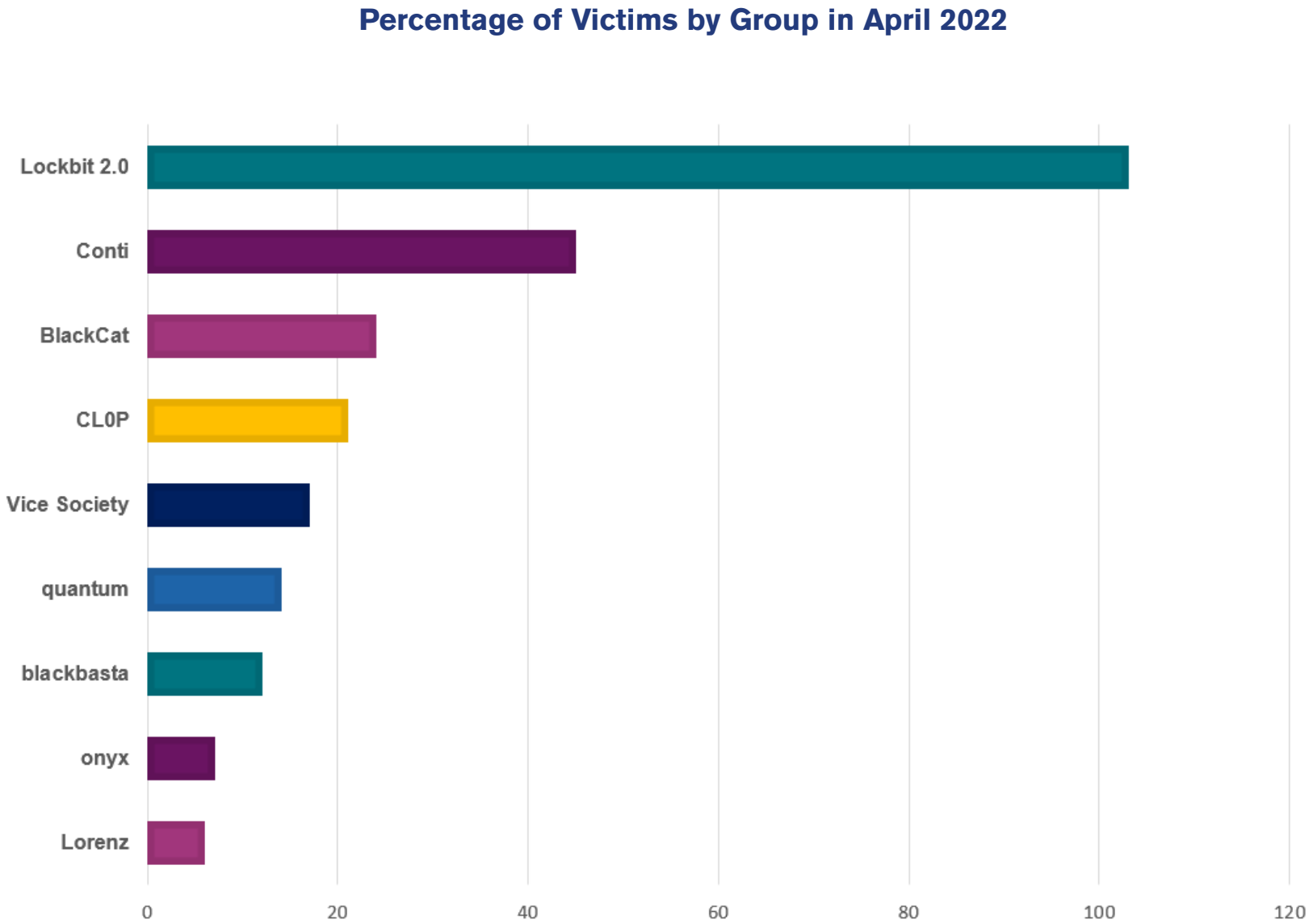
Monthly Threat Pulse
April 2022

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.

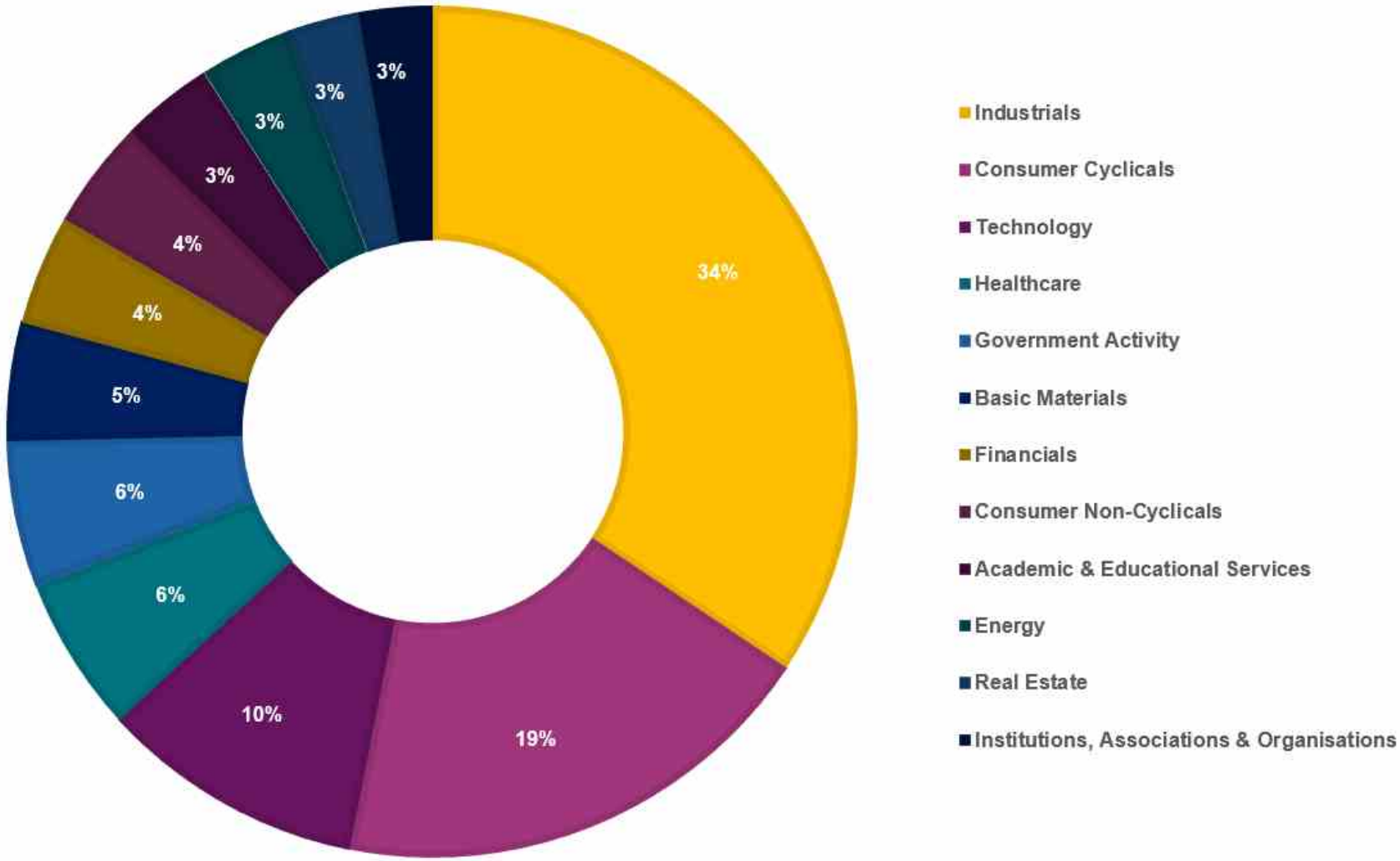
By recording this data and classifying the victims by sector, we can derive additional insights such as, which sectors are being targeted this last month, and how do these insights compare to previous months?

Key data


Percentage of Victims by Group in April 2022
Lockbit 2.0
Conti
BlackCat
CL0P
Vice Society
quantum
blackbasta
onyx
Lorenz
0
20
40
60
80
100
120

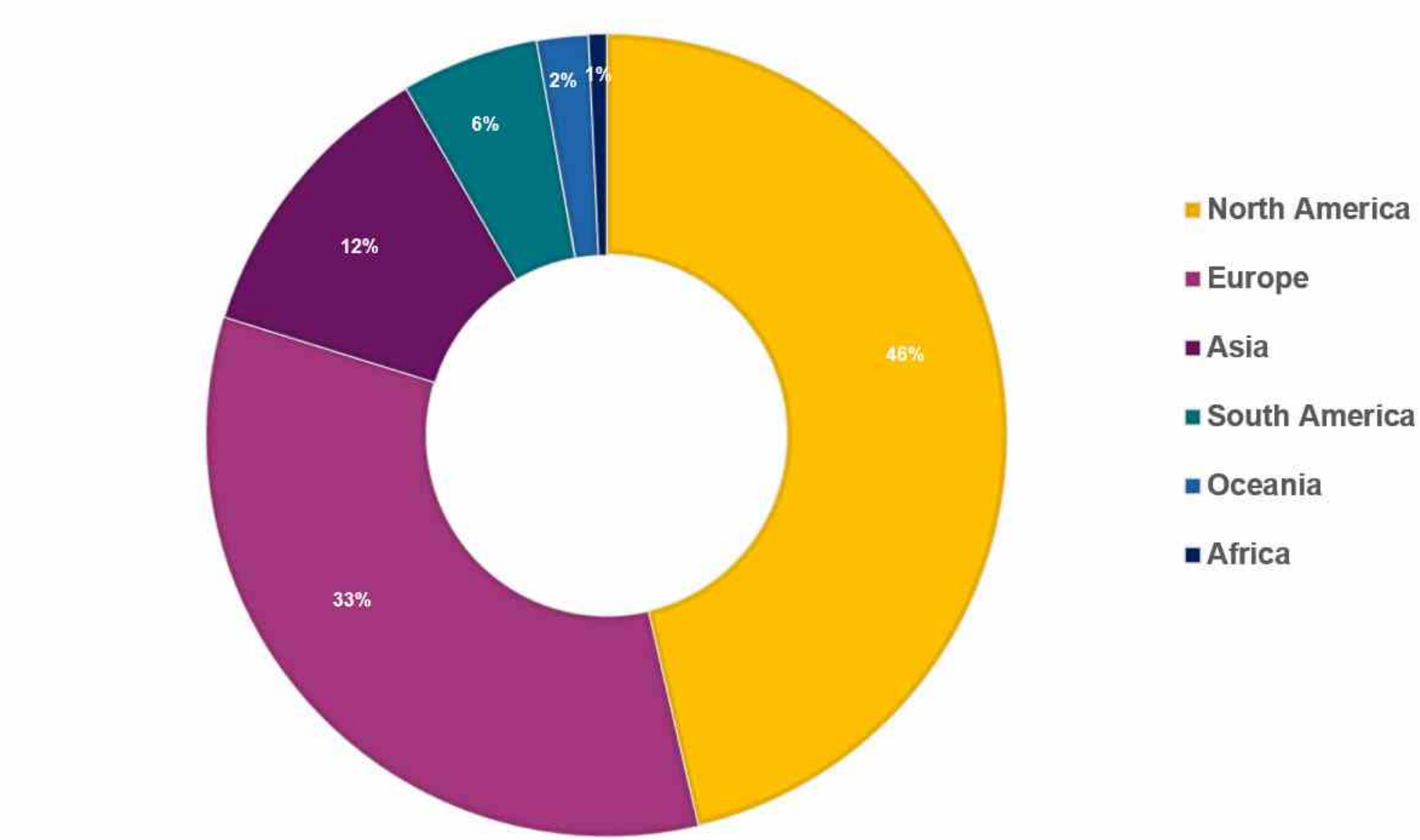
Key data

No. of Victims by Sector in April 2022



Key data

Percentage of victims per region in April



Analyst comments

In April we observed 288 attacks, a small increase in the number of ransomware incidents from 283 in March. As the number of attacks appears to stabilise, this raises the question as to whether ransomware groups may have reached their optimum level of activity already.

Looking back to 2021, 288 and 283 already far surpasses the number of attacks reported for March (204) and April (230) of last year. Likewise, the average number of attacks for the first four months of 2022 is now substantially higher, with 219 incidents vs 189 for the Jan-April period 2021.

In addition, the average number of incidents in 2021 was 224, and with 288 attacks in April 2022, we are already ahead of the average.

With this in mind, it appears we are already observing higher numbers of ransomware incidents than in 2021 and may suggest that we will be looking at a higher number of incidents overall in 2022. At the same time, last year was characterised by many ups and downs in the number of attacks, April and March's higher figures this year may therefore reflect a similar pattern of peaks and troughs, when compared to January (121) and February (197).

Following this we may observe a decline, which would be in line with 2021's targeting behaviour. Nevertheless, we cannot discount the possibility of an increase, certainly as the number of incidents continues to remain at the higher end. We will continue to monitor ransomware hack and leak data to understand how the pattern evolves.

Regions

Regional analysis identified North America as most targeted (46%), followed by Europe (33%), Asia (12%), South America (6%) Oceania (2%) and Africa (1%). When compared to last month, these figures present similar results: North America (44%) Europe (38%), Asia (7%), South America 6%, Africa 3%, and Oceania 2%.

Together, North America and Europe continue to account for the majority of ransomware attacks, reflecting the ever-present threat to organisations situated within these regions. Notably however, European businesses experienced a small decline in targeting, with 105 incidents recorded in March, and 96 in April. This is of course only a minor fluctuation and unlikely to represent a major decline in the targeting of European businesses as the region has remained within the top 2 most targeted since at least 2021, and into 2022.

As such, organisations within Europe should remain both aware of, and on alert to the risk of ransomware campaigns. Interestingly, whilst North American and European organisations remain at the forefront of threat actor interest, incidents in Asia rose from 20 to 34 in April, resulting in a 70% percentage increase.

Notably, Lockbit 2.0 were responsible for 17 incidents in Asia during April (50%), a similar percentage to that of March (60%). Within this market, their greatest interest lay in the Industrials (35%) and Consumer Non-Cyclicals (24%) sectors, it would thus be prudent for organisations in Asia and within these sectors to remain informed around Lockbit 2.0's TTPs, in effort to strengthen prevention. As the second quarter unfolds, we will continue to observe the targeting behavior in Asia.

Sectors

Overall, our sectoral analysis of April's ransomware campaigns revealed similar results to those of March. Notably, Industrials, Consumer Cyclicals and Technology continue to trump any other sector, with Industrials accounting for 101 incidents (35%), Consumer Cyclicals 54 (19%) and Technology 29 (10%). As such, there has been little shift in the number of overall targeted campaigns when compared to March: Industrials 96 (34%), Consumer Cyclicals 59 (21%), and Technology 21 (7%).

In April, what remains evident is an unrelenting interest for these sectors that demonstrates a consistent trend. Of course, as each of these sectors incorporates numerous, diverse organisations, this naturally increases the number of attacks likely attributed to the Industrials, Consumer Cyclicals and Technology sectors.

However, as noted last month, the characteristics of the organisations that structure these sectors should be considered where working to understand this trend in targeting, and this is worth re-stressing.

Specifically, the Industrials, Consumer Cyclicals and Technology sectors offer a surplus of products and services that are widely distributed, thus working with a vast and diverse clientele. The impact of a ransomware campaign on the targeted organisation's ability to support countless clients and customers ultimately increases the pressure on the victim to restore service. Likewise, with a foothold into multiple organisations there is scope to accumulate or destroy extensive sensitive data that organisations wish to protect. The pressure to restore and safeguard on such a large scale are both exploited by threat actors to prompt payment.

Moving away from our top 3 sectors, some minor yet notable increases were identified in Healthcare and Government Activity. In April, Healthcare ransomware incidents totalled 17 incidents (6%), vs 12 in March (4%). Likewise, 16 (6%) attacks were attributed to Government Activity in April, vs 11 (4%) in March. Whilst this presents only a slight increase and the percentages remain small, the possible consequences that can stem from ransomware attacks within these sectors can be particularly detrimental.

The value of sensitive information stemming from medical or government data, alongside the ability to disrupt operations, healthcare and day-to-day government activity risks major social and economic impact, an attractive exploit to any threat actor. Additionally, both sectors are classified as Critical National Infrastructure (CNI), for which the NCSC has recently warned of an increase in CNI ransomware-related threats. Healthcare and Government sectors should remain vigilant and continue to strengthen security measures in an effort to prevent and protect.

It is worth noting that Lockbit 2.0 (25%) and Conti (25%) were responsible for the majority of Government-related activity. Likewise, Lockbit accounted for 41% of healthcare-related targeting.

An understanding of both threat actors TTPs would support Government and Healthcare organisations to minimise risk. We will continue to monitor the data and assess whether this increase in targeting within both sectors will progress throughout the second quarter and advise accordingly.

Threat Actors

As the number of attacks in April was largely similar to that of March, fluctuations in threat actor targeting are more noticeable. In line with last month, the most active threat actor in April was Lockbit 2.0, whose activity increased by 6% (from 96 to 103 victims).

Just behind Lockbit sits Conti, maintaining the same position as in March, with a decrease of 36.6% (from 71 to 45 victims). Transitioning from fourth place in March to third in April is BlackCat with a minimal 4% increase (23 to 24 victims).

Critically, CL0P increased by a mammoth 2,100% (from 1 to 22 victims), soaring from the least active threat actor in March to the fourth most prominent in April. As predicted in March's monthly report, Lockbit 2.0 and Conti have sustained their ranking in first and second place, however CL0P's sudden surge in activity is highly unprecedented.

We will look to analyse why this has become the case.

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.