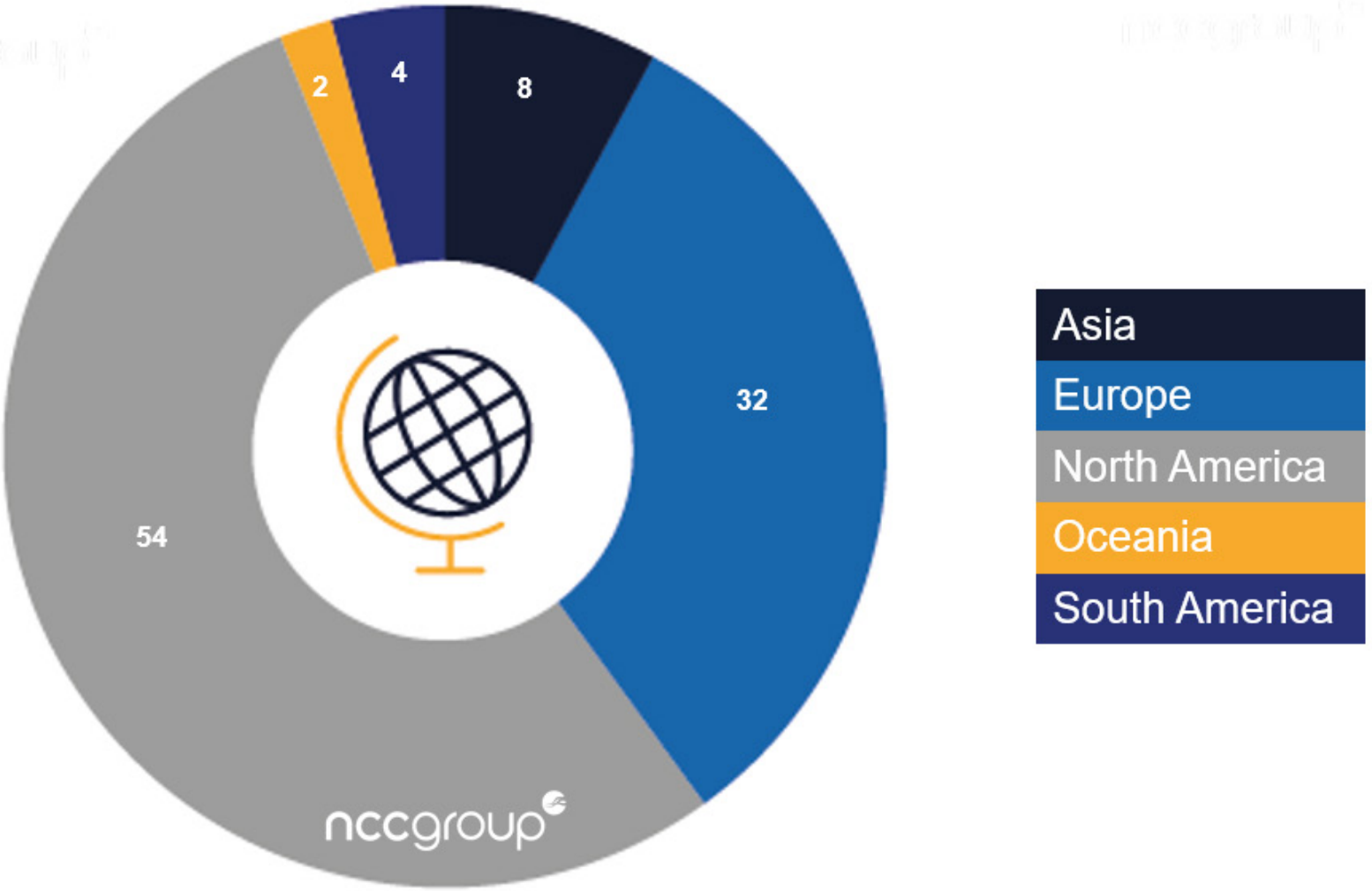
Monthly Threat Pulse
September 2021

The threat of ransomware is increasing, with the tactics, tools and techniques used by groups changing rapidly – necessitating an agile and data-informed response from businesses around the world.

In this report, NCC Group's Strategic Threat Intelligence Practice explores the ransomware landscape, providing an overview of the threats and ransomware groups that are posing a risk to businesses right now.

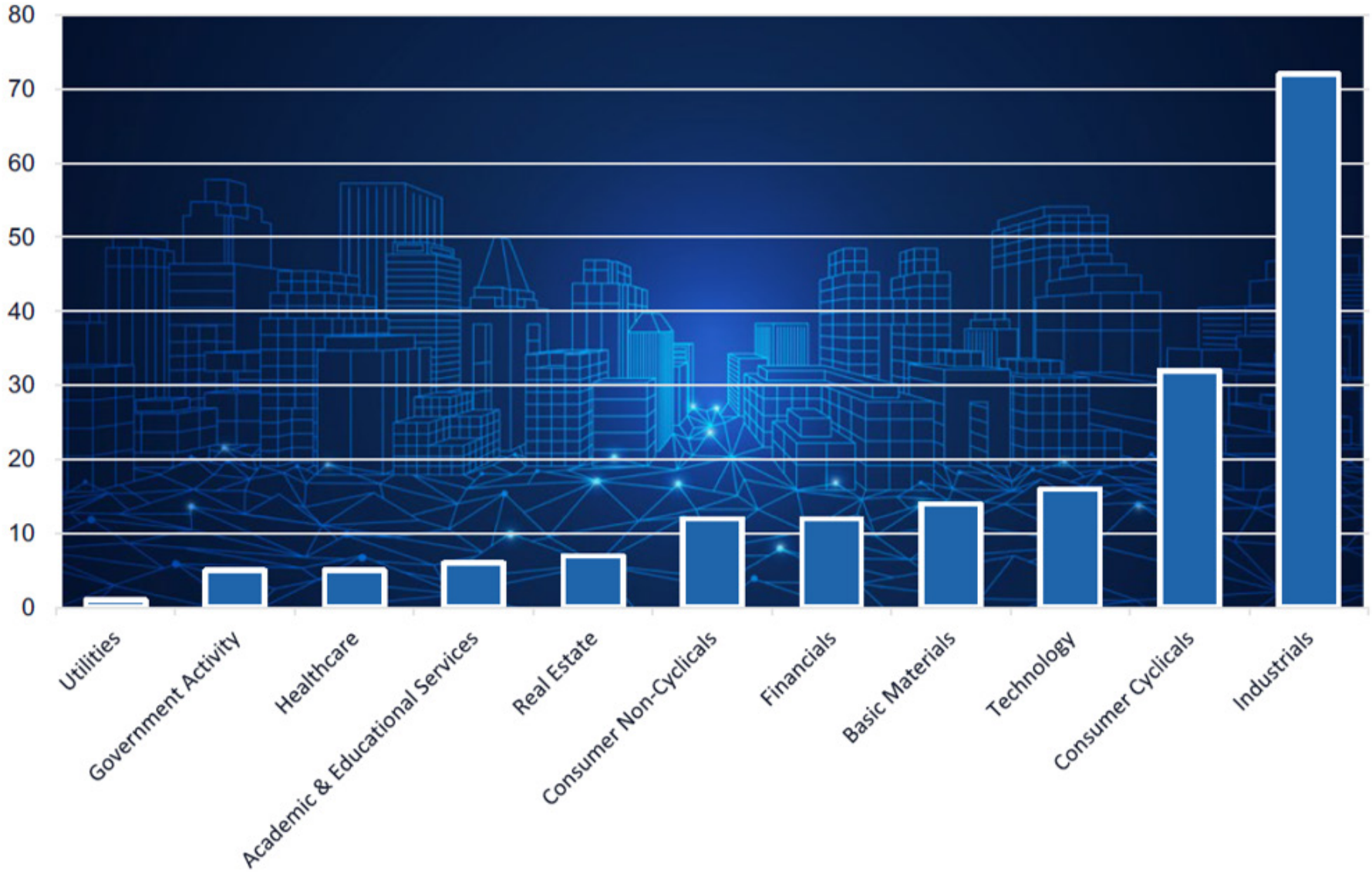
Key data

Ransomware victims' locations in September

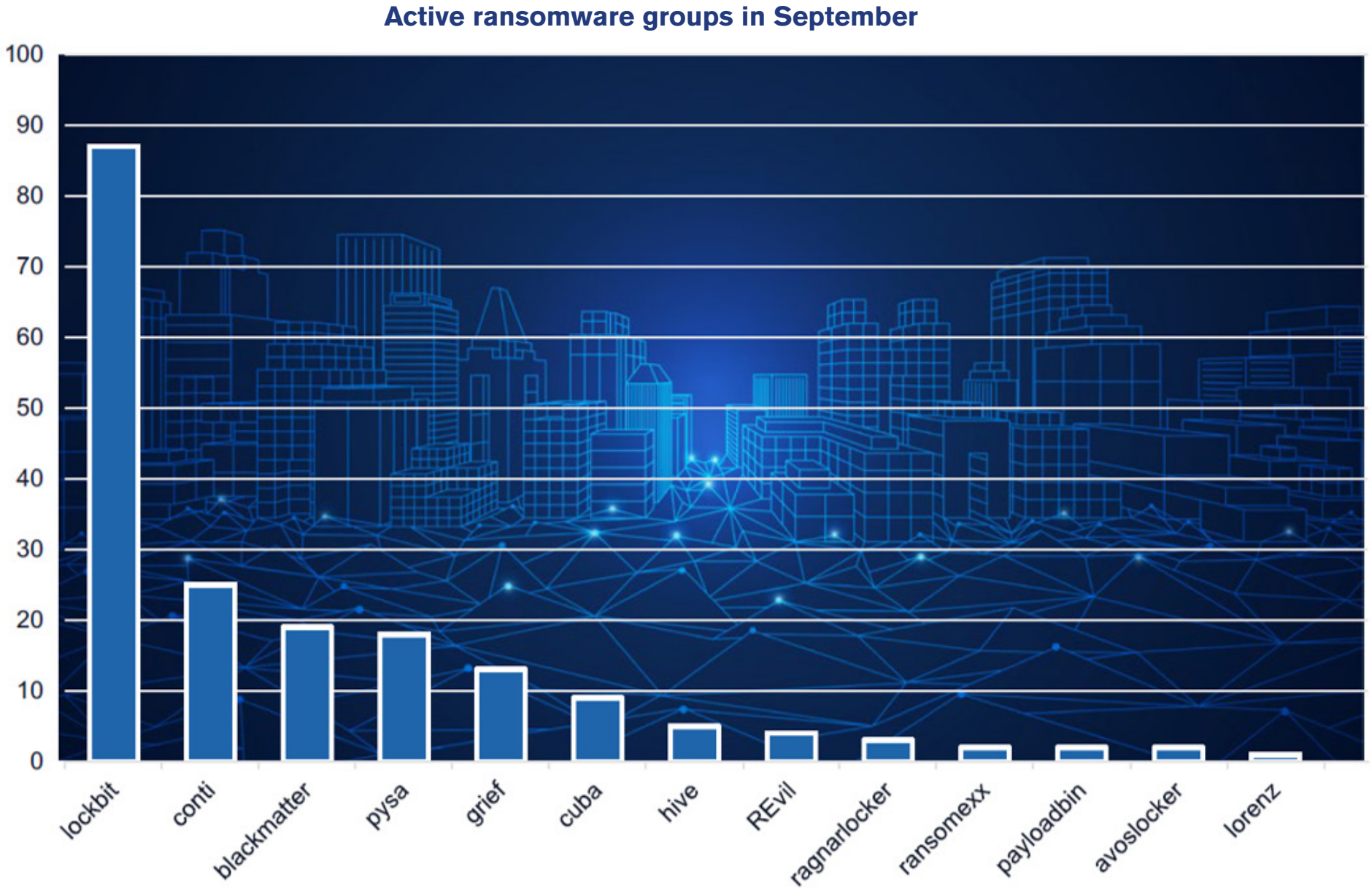


Key data

Sectors of ransomware victims in September



Key data


Active ransomware groups in September
100
90
80
70
60
50
40
30
20
10
0
lockbit
conti
blackmatter
pysa
grief
cuba
hive
REvil
ragnarlocker
ransomexx
payloadbin
avoslocker
lorenz

Analyst comments

Regions

In terms of ransomware victims by region, we can see that North America continued to be the most targeted in September, which is consistent with our observations from August. However, when compared with the total attacks that North America experienced in August, there has been a 46% decrease.

Similarly, Europe continues to follow the trend of the second most targeted location, but in contrast with North America, has a smaller percentage decrease (-23%), suggesting consistent targeting of European organisations. Due to the propensity of ransomware actors using big-game hunting tactics and the volume of high-net worth organisations in both North America and Europe, we can only expect this trend to continue.

Sectors

The Industrials sector remains the most highly targeted sector by far, followed again by the Consumer Cyclicals and Technology sectors.

When targeting these sectors, ransomware groups tend to benefit from a high probability of ransomware payment due to the level of disruption that can be generated from a ransomware incident.

Given the supply chain and energy supply issues globally, we expect to see increased targeting of organisations involved in logistics and energy production, and further disruption would have widespread societal impacts necessitating swift resolution via ransom payment.

Threat Groups

In terms of ransomware group activity, we have observed that the Conti group has had a significant drop in activity this month, while the Lockbit group has been largely consistent based on the number of victims.

One of our working theories is that that the drop in ransomware activity from the Conti Group in September is a result of their success in August. With almost half of all ransomware victims in August linked to the Conti Group (146), the administrative burden of the negotiations is likely to be substantial and could potentially impact efforts to compromise further victims.

There have also been numerous reports of the Conti Group becoming more prescriptive with how they expect negotiations to take place, with the insistence of no media communications or third-party involvement.

This observed behaviour would indicate not only a desire to expedite negotiations, but also frustration regarding outside interference, which they are attempting to counter by threatening to forgo the possible ransom and leak the data they possess as a warning to others. While this supports our theory that the group are suffering with the scale of their success, they were still active in September and were the subject of an alert pushed out by the U.S Cybersecurity & Infrastructure Security Agency.

Spotlight: Conti Ransomware Group

Recent activity

As touched on above, during August we observed a steep increase in Conti's operations as part of a global rise of ransomware attacks.

As a result, the FBI and the NSA issued a joint alert as a result of its surge of activity in recent weeks; notably, the recent attack on the Crystal Valley cooperative farm. However, there is still no information regarding the ransomware group behind the attack.

The Conti group appears to be active since 2020 and is another player in the ransomware ecosystem using the RaaS (ransomware as a service) business model.

The Conti group emerges from Russia and has affiliations with the Wizard Spider group; mainly due to the similarities of the Ryuk ransomware and especially the Trickbot malware code.

However, earlier this month, a disgruntled affiliate of the group released Conti's ransomware playbook as a revengeful response for, allegedly, being underpaid and mistreated.

The playbook, amongst other information, revealed that some affiliates of the group live in Ukraine.

In May 2021, the Conti group seemed to be behind the attack on the Irish Health Services (HSE), demanding 20 million US dollars.

The attack came against the public policy of the group against attacks on critical infrastructure and life-threatening impact attacks. A few days later, Conti group released (via their negotiator chat page) a free decryptor – however, they still threatened to sell or publish the stolen data if the $19,999,000 ransom was not paid.

The approach

The Conti group's attack operations focuses mainly on Microsoft Exchange Server exploitations and, more precisely, on ProxyShell flaws.

The attacks seem to follow a 48-72-hour cycle to reach the point of data exfiltration.

The main stages are described as follows:

- ProxyShell exploit
- Backup web shell
- Domain mapping
- Admin credentials
- Data exfiltration
- Ransomware unleashed

Analyst comments

The Conti group appeared to be prevalent in the summer period with a surge of attacks in August.

Considering the involvement of the ransomware group Wizard Spider, which uses the Conti variant for its operations, it would be interesting to explore whether there are nation state interests as well as financial gains.

Interestingly, Wizard Spider also has ties with Sidoh, an espionage malware.

That said, there is nothing to confirm at this moment the involvement of the aforementioned groups with nation state related operations.

About the NCC Group 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.