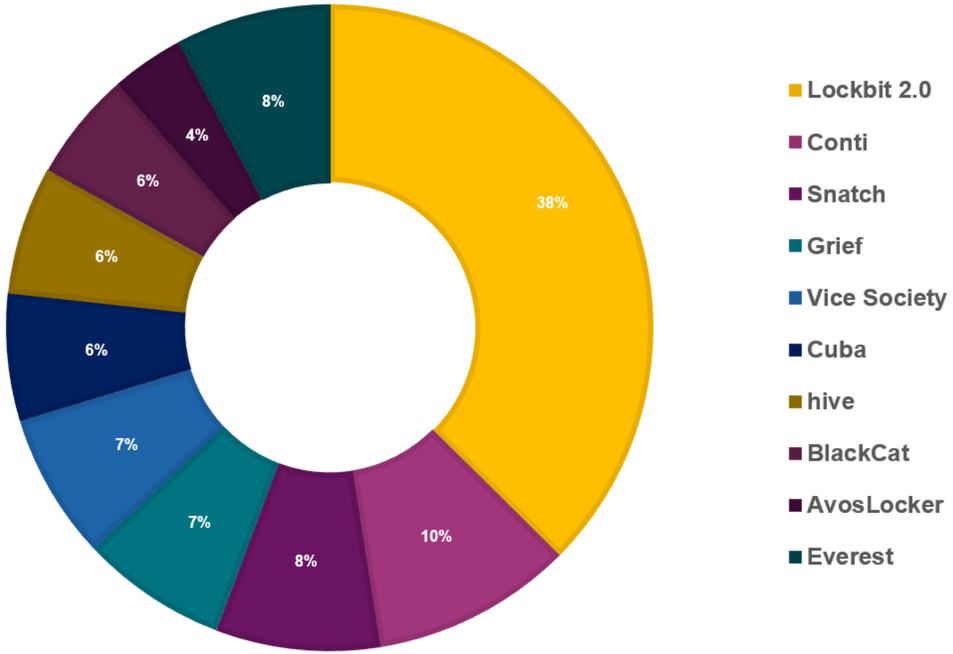
Monthly Threat Pulse
January 2022

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 what sectors are being targeted and how do these insights compare to previous months.

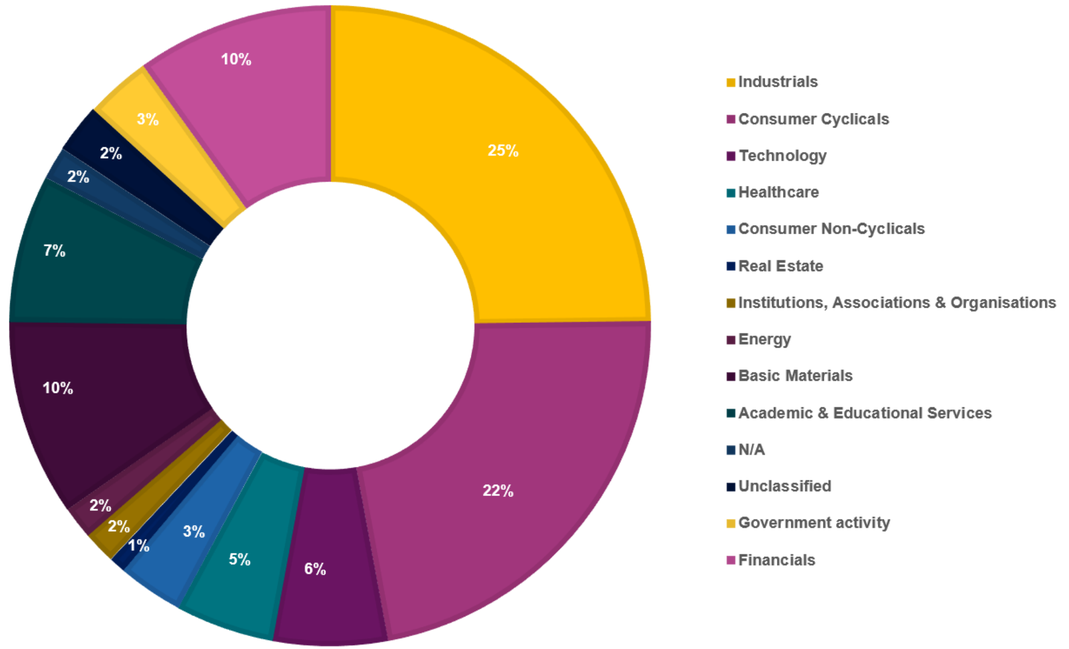
Key data

Percentage of Victims by Group in January

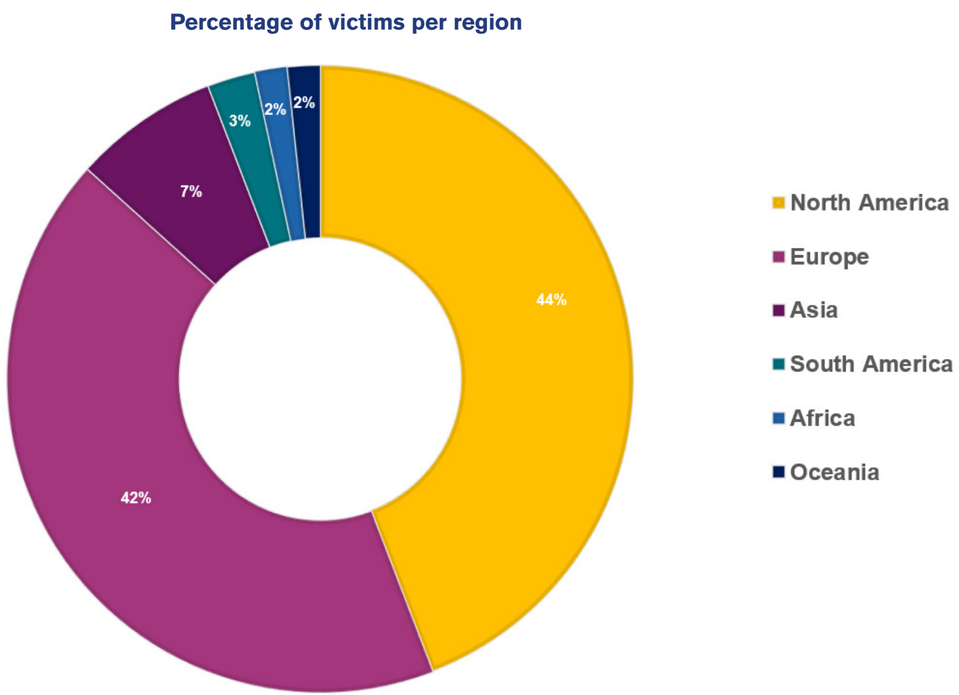


Key data

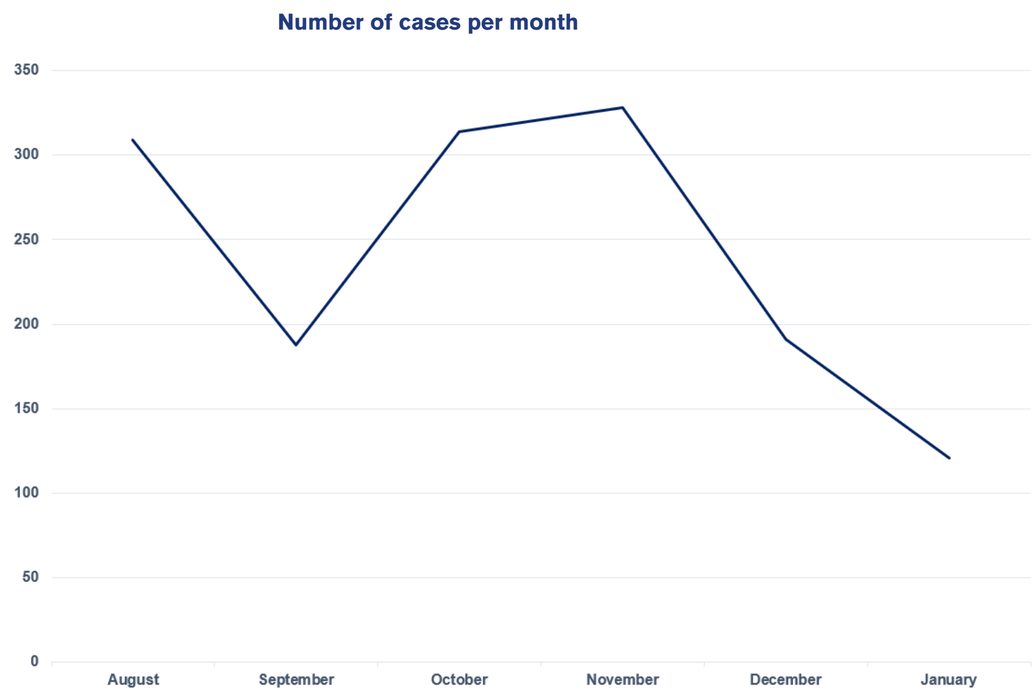
No. of Victims by Sector in January 2022



Key data



Key data



NCC Group Monthly Threat Pulse

Analyst comments

This month we observed a 36.6% decrease in ransomware attacks compared to December 2021, with the number of victims falling from 191 in December, to 121 in January. This downward trend persists from the November 2021 period and is likely consistent with a continued seasonal reduction in ransomware behaviour. Comparison against previous years reveals similar figures, with January 2021 reporting 127 ransomware attacks. As such, these changes do not present as extraordinary but a trend we can expect during this period.

Threat actors

When focusing on prevalent threat actors, Lockbit 2.0 remains a persistent contributor to the ransomware threat landscape. From December 2021 to January 2022, they only had a 12.8% decrease in hack & leak victims irrespective of the 36.6% overall decrease in cases, making them the most consistent presence in totality. Conti, on the other hand, exhibited a 65.6% decrease in victims.

Lockbit 2.0's most targeted sector was Industrials with 31.7% of their victims operating within this industry; primarily the 'Professional & Commercial Services' industry, with 19.5% of their total victims operating within this industry.

This shows that, although Lockbit 2.0 have vastly diversified campaigns, there seems to be an increased weighting of 'Professional & Commercial Services' cases.

As a result, organisations within this industry should consider their perceived attractiveness to Lockbit 2.0 and ensure that adequate ransomware mitigations are in place.

Within this industry is Business Support Services, which encompasses various contracting organisations such as legal, management and transaction & payment services. The commonality between these seemingly disparate operations is the likelihood of diverse PII due to their individual interactions with client organisations. Whether it's legal information, personal employee data, or financial documents, the data stored within these organisations is likely protected by GDPR and thus presents an attractive target to extortive ransomware groups (such as LockBit 2.0).

As for the other big player in the ransomware space, Conti's targeting focused on the Consumer Cyclicals sector in January, accounting for 45% of the group's victims, followed closely by Industrials (27%).

Although their total victims have decreased from December 2021 to January 2022, their targeting remains consistent with December as Industrials and Consumer Cyclicals were also their primary focus then, accounting for 37.5% and 31% of their victims respectively.

Their partial dip in activity should not be inferred as a decreased threat, as it is likely that their activity will increase in proportion with their peers in the coming months.

Sectors

Overall, analysis of ransomware attacks by sector revealed the industrial (24.7%), consumer cyclical (22.3%), financial (9.9%) and basic material sectors (9.9%) as the most targeted.

The findings suggest a decline in attacks within the most prominent sector industrials, when compared to December 2021 (39.7%), whilst consumer cyclicals remains at a similar level (25.65%). Their leading position overall reflect our observations from the last 6 months and thus further supports a trend in which they are still perceived as highly attractive targets.

Regions

A closer look at the targeted regions provides food for thought. North America and Europe continue to be the most targeted however this month they have suffered an almost equal number of attacks. With 53 and 51 incidents respectively, accounting for 86% of total ransomware attacks, this contrasts our usual findings in which North America is the most targeted region. This is perhaps the result of less attacks occurring overall in January, with less actors active in North America. For example, our data suggests a 46.1% decrease in Conti activity and a 62.5% decrease for AvosLocker in North America compared to December 2021. As such, we will continue to monitor if this is a pattern or a by-product of the January reduction.

The regional difference made for interesting comparison when also considering the most prominent sectors. The data shows a higher number of incidents in the industrials sector in Europe (29.4%) than in North America (19%), whilst a higher number of organisations in the consumer cyclicals sector were targeted in North America (30%) than in Europe (17.65%). Whilst the findings are representative of January and subject to change, this difference helps to better understand which sectors are likely to be targeted in which region, and therefore narrow the focus with regards prevention measures.

In Europe, the top three targeted countries remain the US, UK and France, with 47, 12, and 11 incidents respectively.

Threat Actor Spotlight: NightSky Ransomware

Overview

The start of 2022 saw a new ransomware variant enter the arena, NightSky, which targets corporate networks for financial gains. The ransomware was announced by the MalwareHunterTeam on the 1st of January 2022 and has been active ever since. It is believed that NightSky has been active since December 2021, operating in the RaaS (Ransomware as a Service) model.

The ransomware operators have adopted the popular practice of double extortion to increase likelihood of payment. Double extortion involves data encryption followed by threats to the victim of leaking the exfiltrated data. The group has already announced a small number of victims in January, located mainly in Asia (Japan and Bangladesh). In one of these cases, NightSky demanded a ransom of $800K to provide the decryptor key.

Attack example

NightSky encrypts files using AES-128-CBC algorithm and uses a combination of RSA to encrypt the file keys. During the encryption process, the ransomware appends the ".nightsky" extension to the files. Interestingly, Microsoft has issued a warning regarding a China based ransomware operator exploiting the Log4Shell vulnerability to gain access on VMware Horizon systems. Following that, the group deploys the NightSky ransomware to encrypt the victim's files and proceed with their extortion practices.

According to Microsoft, the group known as DEV-0401 seems to have used other ransomware families in the past such as Lockfile, AtomSilo and Rook.

Analyst Comments

NightSky ransomware has been used extensively at the beginning of 2022 and remains to be seen whether it will continue in such volume. At this stage, we have no conclusive information of its origin, nor its operators beyond their alleged connections with China that we have already mentioned. Regarding its techniques and practises, the ransomware uses well tested and rather effective methods that we have seen in the past which comes to show that we are still far from defending effectively these types of attacks.

European Ports and Oil Storage Facilities Targeted

January ended with a bang as largescale ransomware attacks disrupted critical infrastructure across Western Europe.

On January 29th, ransomware crippled the IT systems of 17 European oil ports affecting dozens of terminals, oil storage and global transport operations. The plethora of global victims included two major German oil suppliers that supply thousands of gas stations and retail stores; Oiltanking GmbH and Mabanaft GmbH.

Further targets included SEA-Invest in Belgium and Dutch company Evos. While no data breach is deemed to have occurred, tankers were re-routed, supply chains disrupted, and challenges to both loading and unloading refined cargo persisted.

Thus far, BlackCat has been identified as responsible for the attacks on Germany's oil suppliers by the German Federal Office for Information Security, as reported by German newspaper, Handelsblatt.

It is yet to be confirmed whether BlackCat is responsible for the attacks on wider EU countries or if the attacks are linked.

In the midst of rising geopolitical tensions, the events raise questions around possible threat actor motivations–profit vs exacerbating tensions in Western Europe.

At a time when Germany considers its position on the NordStream pipeline deal and as European leaders respond to the Russia-Ukraine conflict, possible nation-state influence comes to mind.

The Dutch National Cyber Security Center has reported a likely criminal motive and does not believe that the attacks in the Netherlands, Belgium and Germany are linked to nation-state threat actors, whilst others suspect Chinese and Russians backed APT's.

The targeting of further major critical infrastructure at Zurich Swissport has raised additional concerns around the threats to European businesses as the EU navigates Russian-Ukrainian tensions.

While at present there is not enough evidence to attribute responsibility past that of BlackCat in the instances above, the threat actors in each scenario sought to exploit the high-pressure situation Europe faces and increased threat to CNI.

Taking this into consideration, it will be all the more important for European businesses in these sectors to remain on high alert as geopolitical changes develop and CNI remains vulnerable.

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.