Monthly Threat Pulse
January 2023

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?

Ransomware Tracking

Analyst Comments

As we entered a new year, ransomware continued to threaten organisations globally with January recording 165 attacks, a 38% decrease from December 2022. Although a notable drop in the figures when compared to November and December 2022, lower figures in January were anticipated. This reflects previous trends in which 2021 and 2022 recorded lower attack numbers, 127 and 120 respectively. Seasonal fluctuations around the festive period as cybercriminals enjoy some respite is a likely variable influencing such change.

Figure 1: Global Ransomware Attacks by Month

The data suggests that ransomware attacks may be on the rise, with 165 representing the highest number of attacks recorded in January over the last three years. A 39% decrease from December 2022 to January 2023 reflects a similar proportional decline from December 2021 to January 2022, in which we observed a 37% reduction. As such, we would have expected a greater decline in both the raw numbers and proportionally, however overall numbers remain much higher than anticipated.

Furthermore, an unexpected change to sectoral targeting revealed the Academic sector to be the third most targeted, outranking Technology which has held third place for all of 2022, with the exception of January and October. Likewise, Vice Society adopted a more prominent position, moving into our second most active ransomware operator and holding a Top 3 ranking position for the first time in our analysis. As such, January has already proved interesting, with shifts and changes across the threat landscape.

Sectors

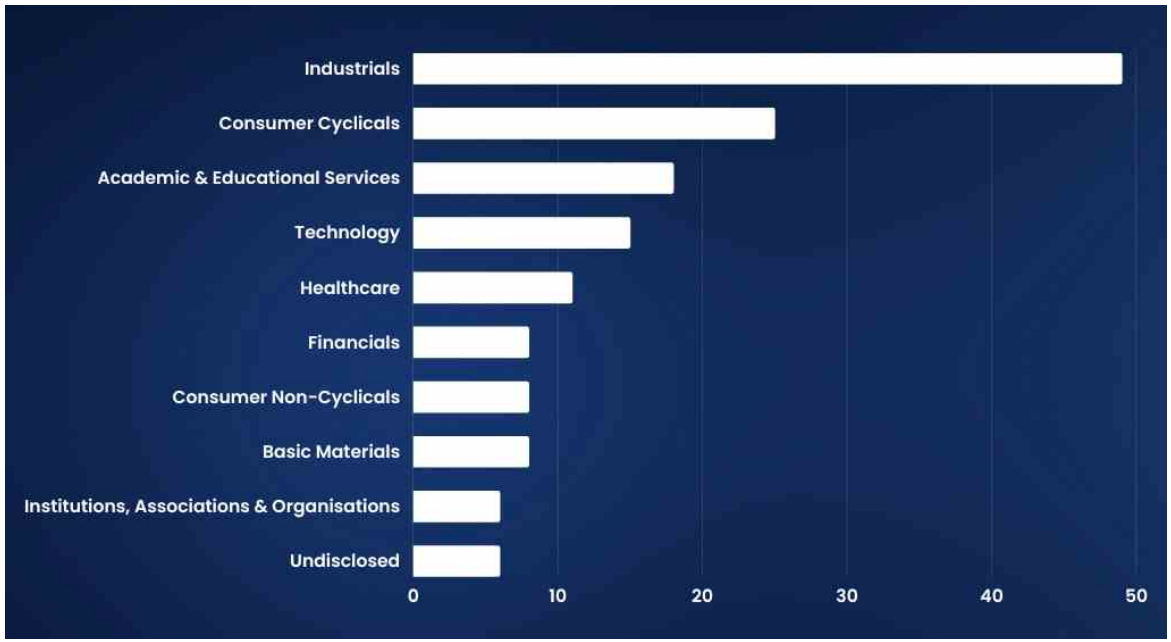

Figure 2: Top 10 Sectors Targeted January 2023

In January, the most targeted sector was Industrials with 49 attacks representing 30% of all observed ransomware events for the month. This is a decline in real-terms of 17 attacks from December, though a proportional increase of 5%, up from 25% of all attacks in December.

The Industrials sector is vast and contains many industries of high value to potential attackers such as Professional & Commercial Services. Industries like this which contain a large number of organisations of course expand the attack surface of the sector overall, contributing to its perennial position amongst the most targeted sectors for ransomware every month.

Threat actors

Firstly, the top 3 threat actors in January 2023 were LockBit 3.0, accounting for 50 of the 165 total attacks (30%), followed by Vice Society in second place with 22 (13%), and finally BlackCat in third place with 20 attacks (12%). As has been the case for months prior, LockBit are the most active threat actor in the ransomware threat landscape, which is unlikely to change throughout 2023 providing there are no major adjustments to the landscape, such as law enforcement crackdowns.

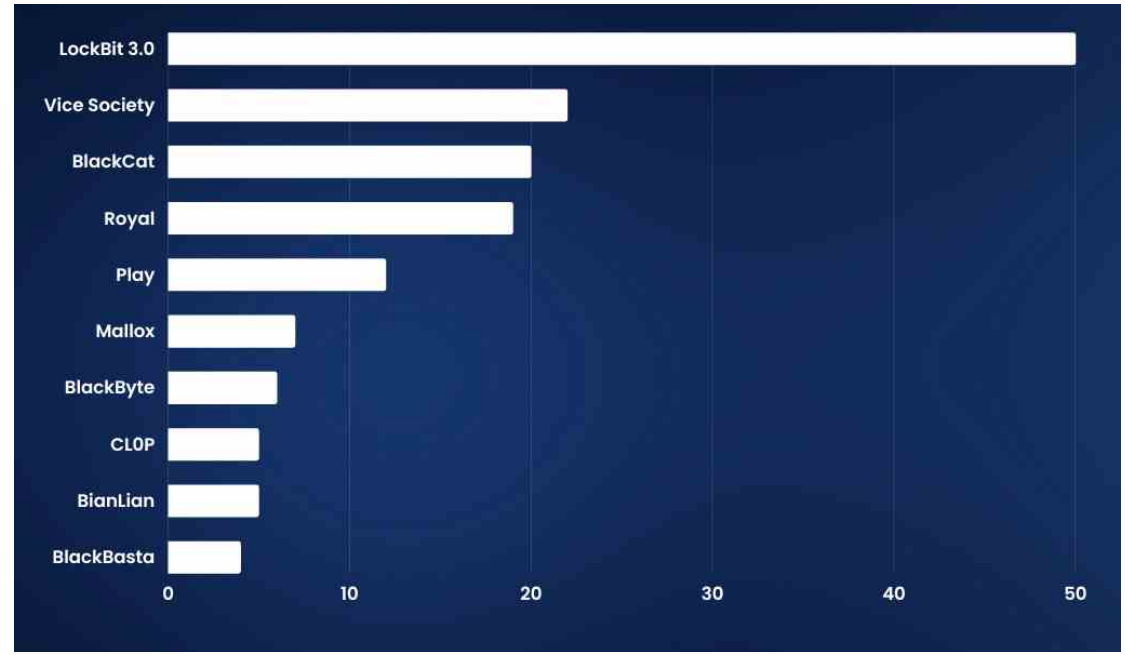

Figure 3: Top 10 Threat Actors January 2023

Vice Society in second place is an interesting development, as they were in 10th place in December, meaning that they may be ramping up their activity for 2023. Additionally, this is the largest number of attacks that NCC Group have recorded for Vice Society in one month (as far back as January 2021), so what does this sudden increase mean and who does it affect? We will attempt to answer this question later on in this report.

It is unsurprising to see BlackCat in the top 3, as has been the case intermittently throughout 2022 (October and December being two examples in the latter half of the year). Interestingly, Royal has remained in 4th place, continuing from December 2022, demonstrating that their activity is showing no signs of slowing. In fact, the Linux version of their ransomware strain has been identified in campaigns targeting a two-year-old VMware ESXi vulnerability in early February, implying that they indeed won't be easing off this month either.

Regions

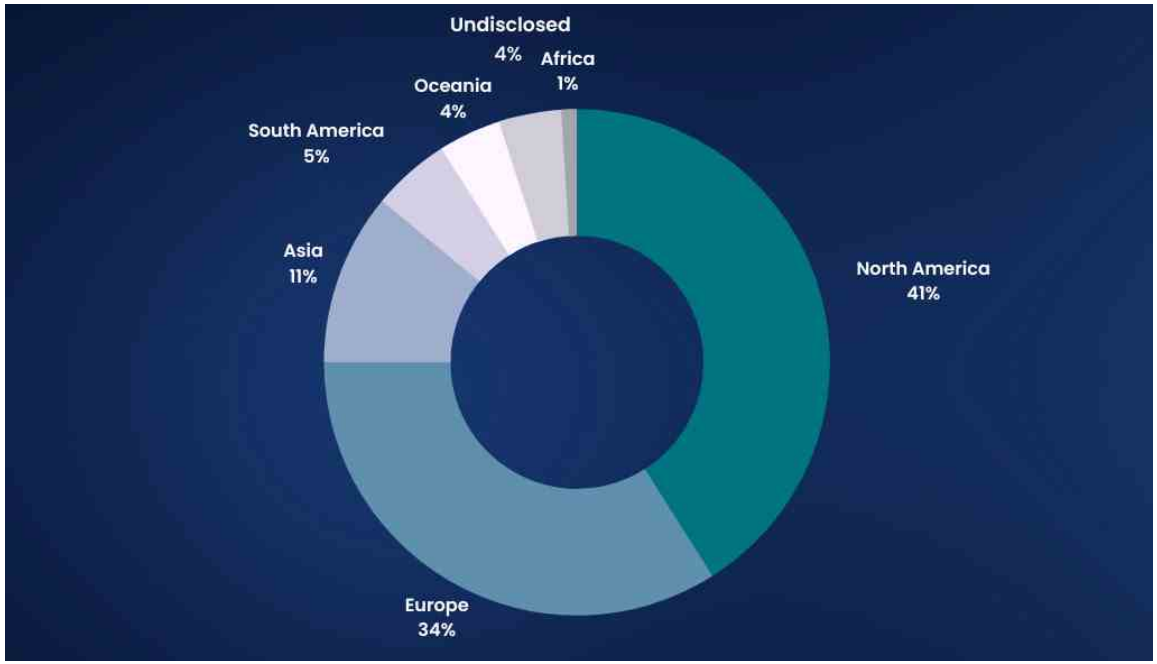

Figure 4: Regional Analysis January 2023

This year started off as previously forecasted with North America and Europe remaining as the two most targeted regions for ransomware globally, with North America experiencing 68 out of 165 attacks (41%), and Europe observing 56 (34%). Notably, the 33% decrease in total attacks from December to January plays out as a 44% decrease in North America (from 121 attacks in December) and a 21% decrease in Europe (from 71 attacks in December).

As we progress further into the New Year, it is likely the two will remain the most targeted regions globally as they have in the past. The proportion of total attacks occurring in North America decreased since December by 4% (from 45% to 41%), while Europe's share increased by 8% (from 26% to 34%).

Asia remained the third most targeted region with 19 attacks (11%), which, while is a 42% decrease from the 33 attacks (12%) in December, shows proportional stability. South America, once again fourth-most targeted, this time saw 8 attacks (5%), or a 53% decrease from 17 (6%) in December. Oceania, once again fifth-most targeted, saw 6 attacks (4%), representing a 57% decrease from 14 (5%) in December. Finally, Africa saw a 50% decrease in attacks, from 4 (1%) in December to 2 (1%) this month. This month showed low region-based volatility, with only relatively moderate decreases in attack volumes across all regions except Europe, for which its comparatively low decrease in attacks led to its increase in proportion of total attacks.

The 'Undisclosed' category, representing attacks with unidentified victims and thus unidentified regions, has remained proportional since December despite a decrease in actual numbers, from 9 (3%) in December to 6 (4%) in January. These events will be continually monitored to identify the relevant region in the event that the victims' names are released, as well as to monitor for changes in the prevalence of this new trend of ransomware disclosure.

Threat Spotlight: AcridRain Infostealer

Summary

AcridRain is a resurfacing threat actor in the infostealer tribe. Debuting in 2018 as a run of the mill C++ password, cookie and credit card data grabber that did not get a lot of traction, the new iteration of malware rebrands itself to fit the current 'market' standard functionality of infostealers and refocuses on targeting cryptocurrency and crypto wallets specifically.

The main advertised feature is collecting as many fingerprints on the target as possible, specifically for building profiles bypassing anti-fraud mechanisms, rather than catch-all collecting system logs. The modus operandi is rigged towards working directly with anti-detection browsers, allowing the infostealer user to directly load the victim profiles in tools such as Octobrowser and Che Browser, for accessing compromised accounts. This integration would make cash-out and account takeover attacks more seamless for potential users.

Going forward

AcridRain's current enterprise became active in the beginning of October 2022 and is still undergoing development.

The primary advertiser for AcridRain is believed to be a Russian speaking entity. In addition to renting out stealer software, the threat actor leads a team of programmers with several different sub-specialisations that are leased for malware development projects, and possesses a sizable business deposit on the underground platforms. This indicates a medium sized planned and funded operation.

We expect AcridRain to evolve further and develop its operations, capability, and reach. NCC Group will continue monitoring this actor and stealer variant over the coming months.