Monthly Threat Pulse
December 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, which sectors are being targeted this last month, and how do these insights compare to previous months?

Ransomware Tracking

Analyst Comments

In December 2022, we observed 269 attacks, a 2% increase in ransomware activity compared to November (265). Although a slight increase, this marks the first deviation from the staggered fluctuations observed since May, outlined in Figure 1. Additionally, this increase contradicts the patterns observed in 2021 in which November - December experienced a decrease, attributed to a slowing down during the holiday period. Perhaps most importantly, it appears that we are approaching the highest number of ransomware victims since the peaks reached in March and April, illustrating a major growth since the summer and autumn months, with a possible inclining trend on the horizon.

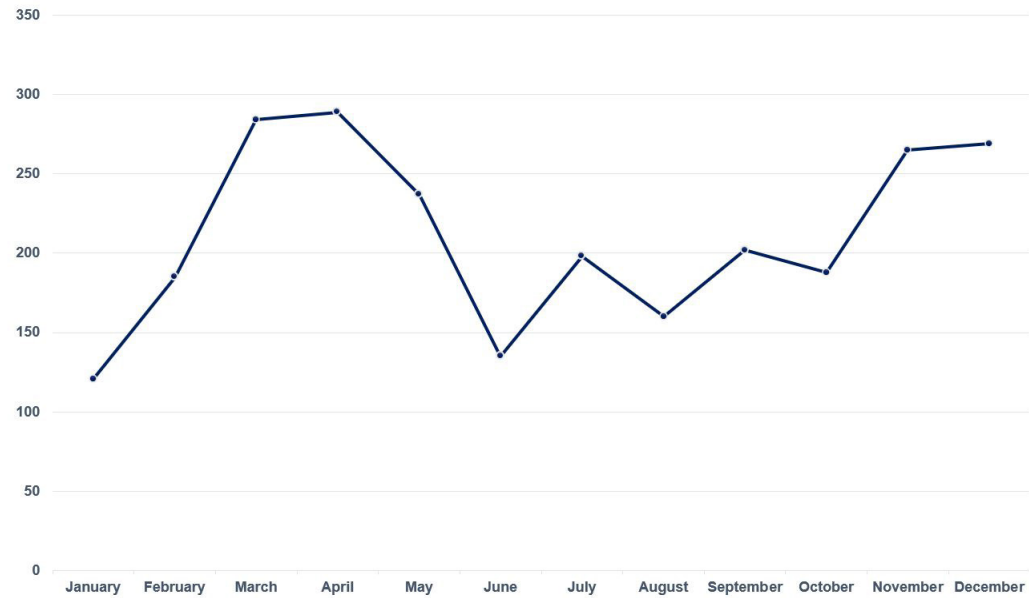

Figure 1: Global Ransomware Attacks by Month

This is particularly unusual as we might expect the holiday period to produce fewer attacks, as cybercriminals like any organisation take time to enjoy the festive season. Such change may be due to the recent shifts we have observed across ransomware players in which new and old threat actors are ranking in first, second and third place. For example, in November we reported that the new strain Royal, and familiar face Cuba, surpassed our ordinarily most prominent threat actor Lockbit 3.0.

Whilst Lockbit 3.0 reclaimed its leading position in December, threat actors such as BianLian and BlackCat have also climbed the scale to reach the top three most active groups. All of these shifts and spikes in activity may therefore contribute to the overall rise we are observing. Of course, this is a rather small incline, it is therefore uncertain how long it will remain and will require consistent monitoring.

Sectors

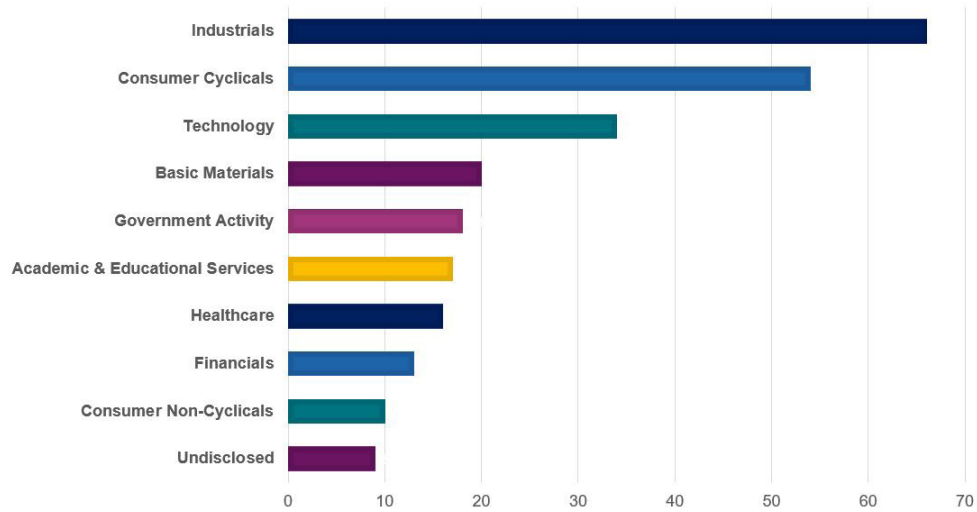

Figure 2: Top 10 Sectors Targeted December 2022

As 2022 ended, the sectors most targeted mirrored the pattern observed for the majority of the year, with Industrials, Consumer Cyclicals and Technology suffering the greatest number of ransomware attacks. The targeting of these sectors has remained consistent and therefore appears unlikely to subside into the New Year. Likewise, each sector continues to provide valuable targets, given the opportunity for widespread disruption, high value targets and cybersecurity challenges such as OT/IT convergence.

From December, we are including a new sector category labelled 'undisclosed', as illustrated in Figure 2. This references those victims' whose sectors, industries and regions are not yet identifiable due to threat actors adopting a new approach to publishing on their leak sites. Specifically, some threat actors are releasing victim names in stages, using asterisks or question marks as a censor. This may begin with the entire victim name blocked out, then slowly replacing the asterisk with letters. Alternatively, this may start with one of several words marked in asterisk or questions marks before releasing the following word, letters and so on.

We suspect that this is in a bid to prompt organisations into payment, slowly releasing their names in full where payments are not made. This censoring is a technique we have observed by two threat actors (discussed in the Threat Actor section of the report), and may become a prominent feature of the hack and leak world in 2023. As a result, once those names are released, we will record more granular data on the victims in question.

Threat actors

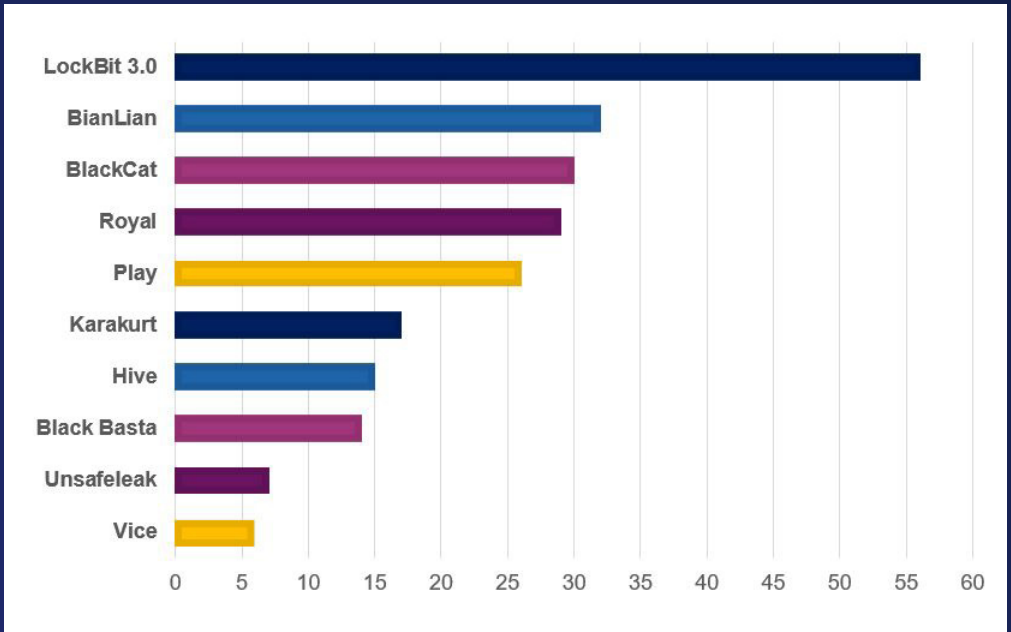

Figure 3: Top 10 Threat Actors December 2022

Firstly, the top 3 threat actors in December 2022 were LockBit 3.0, accounting for 19% (56 attacks) of all attacks, followed by BianLian in second place with 12% (32 attacks) and finally BlackCat with 11% (30 attacks). Continuing the usual trend, LockBit 3.0 was the most active threat actor in December 2022, as opposed to Royal in November, which was a deviation from the norm. Although the most prevalent threat actor has returned to the top, there are some interesting differences. For instance, BianLian have taken 2nd place, and yet another new threat actor has appeared in the top 10 to conclude 2022; Play ransomware group. Play, who were first spotted in June 2022, may be linked to the Hive and Nokayawa families.

Additionally, Royal and Cuba ransomware have exhibited diminished activity after their temporary surge to the forefront in November, with drops of 33% and 85% respectively. As mentioned, BianLian has taken the 2nd place due to their 113% increase and LockBit has returned to their usual place at the summit of the ransomware threat landscape. Based on the previous few months, we can expect 2023 to bring us similar fluctuations in the top 3, until ransomware groups that present a consistent threat dominate the landscape, as we saw in the first 2 quarters of 2022.

Regions

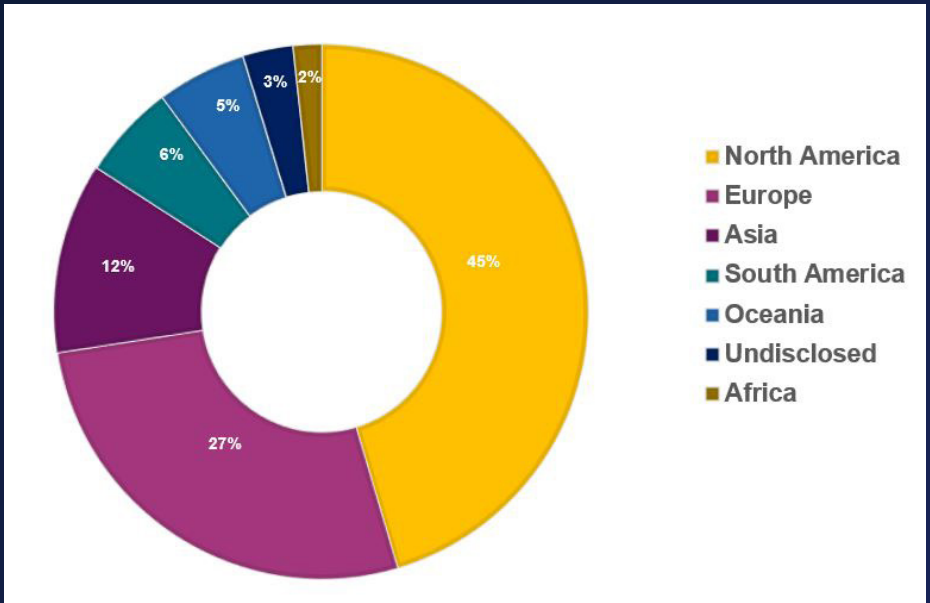

Figure 4: Regional Analysis December 2022

Finishing the year as it started, North America and Europe remained the two most targeted regions for ransomware globally. With 269 recorded global ransomware incidents in December, North America witnessed 120, or 45%, while Europe observed 72, or 27%. In real terms, this is a reduction in total attacks by 21% between November and December for North America, and an 18% increase in total attacks for Europe. Though Europe and North America have swapped between the most and second-most targeted regions throughout the year, it is likely that they will remain the top two most targeted regions for the near future.

Proportionally, Europe's share of total observed ransomware attacks increased by just over 2% while North America's share diminished by just over 12%. The rest of the world also saw some change in ransomware attacks. Asia, once again the third most targeted region, saw a real terms increase of 5 attacks from 28 to 33, 11% of November attacks, and 12% of all December attacks. Similarly, South America saw a real-terms increase in attacks from 14 in November to 17 in December, but which represents proportional stability, accounting for 5% of attacks in November and 6% in December. Proportionally, the most volatile region was Oceania, which experienced a 700% increase in attacks.

However, in real terms this is an increase of 2 total attacks in November to 14 total attacks in December.

Within Europe, the UK was the most targeted with 21 total attacks, while Germany observed 11, and France 8. December also saw the inclusion of 9 ransomware attacks with regions unidentified within the 'undisclosed' category aforementioned. These events will continue to be tracked to ascertain their relative regional identifies should the victims' name be released.

DDoS Analysis

Continuing from November's efforts to clean and refine the DDoS data on which we report, the figures for December are markedly higher than in previous months. By analysing a greater number of protocols, for instance, the available intelligence to be gained from the DDoS stats has grown significantly. It is now more stable than it was in previous months, which should enable the analysis of existing trends, and potentially the prediction of future trends too.

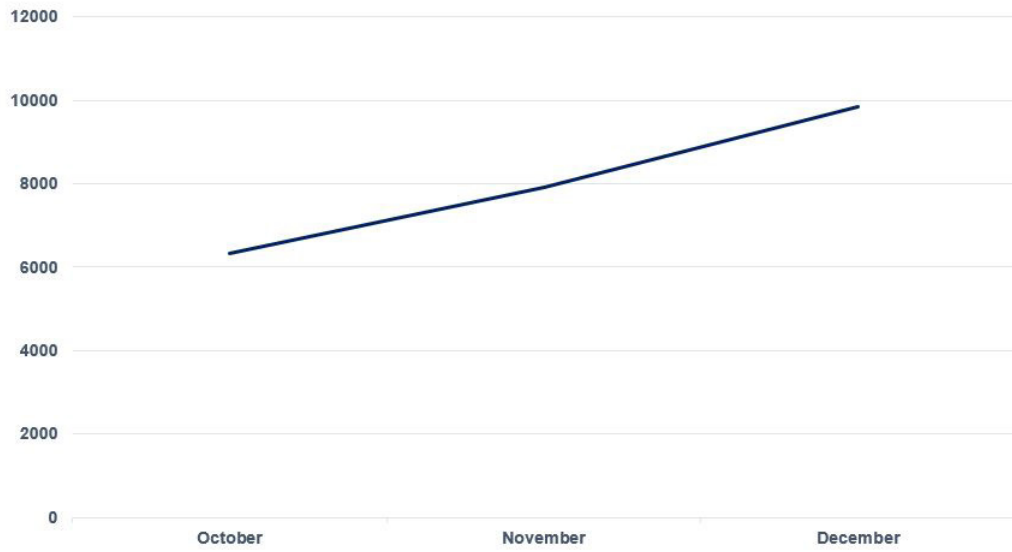

Figure 14: DDoS Attack Counts December 2022

Threat Spotlight

We have not included a threat spotlight this month, due to some very exciting research and analysis being produced for the imminent NCC Group Annual Threat Intelligence report.