Monthly Threat Pulse
October 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 October, ransomware incidents were down 7% from September with 188 attacks recorded vs 202. Interestingly, this is half the amount of ransomware events recorded in October 2021, in which we observed 314. Last year revealed a substantial increase from 188 in September to 314 in October, and continued growth into November (348). This year, the data suggests that there are lower levels of ransomware targeting and unlikely to reach the same heights as in 2021.

This would suggest some improvements where ransomware levels have reduced in comparison, and will be due to a number of factors. For example, highly prominent threat actors present last year such as Conti and REvil are no longer active (at least under these names), likely due to the vast amount of attention they drew following major attacks. Changes therefore to those threat actors once most active on the scene has likely resulted in the reduction of attack numbers we are now observing.

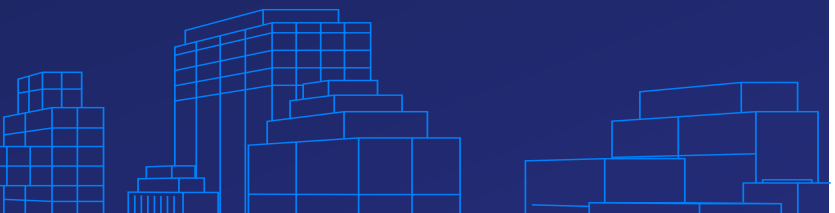

Figure 1: Month-by-Month Count of Ransomware Attacks for 2022

Additionally, following the mass global impact ransomware had in 2020 and 2021, organisations are likely to have ramped up their defenses improving overall protection as a result. Interest in other attack types may also see a shift away from ransomware, such as the returned interest to DDoS.

Whilst October's numbers are near to those observed in the summer months of this year, we are yet to observe consistency in targeting levels. Given the instability observed since May, November may go either way.

Having said this, it is unlikely that the numbers will shift by much in either direction given the changes observed over the last couple of months. Overall, this half of the year is much quieter than earlier on, particularly in comparison to Q1, and will likely continue to be the case as we head into the winter months.

Sectors

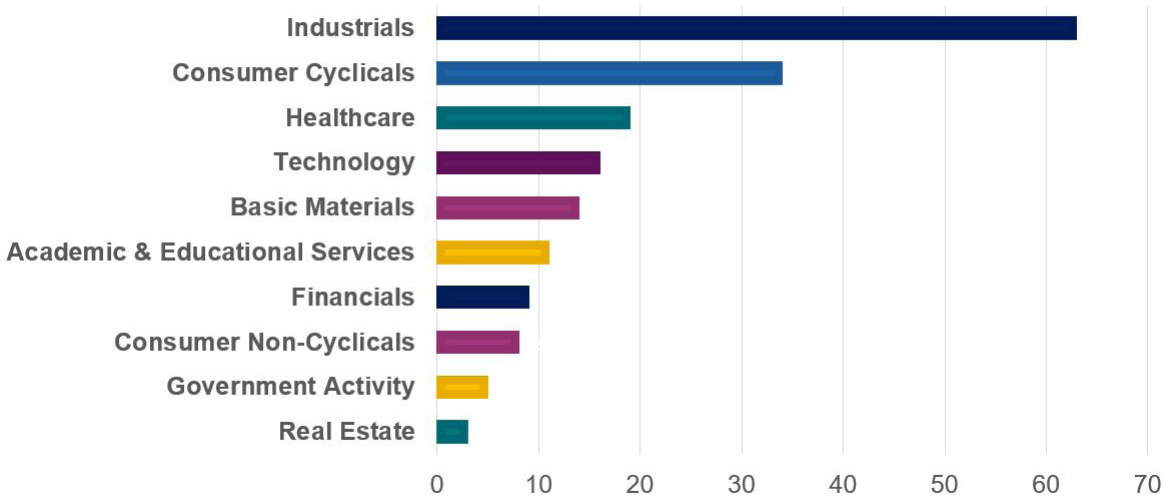

Figure 2: Top 10 Sectors Targeted in October

This month we return our focus to our top three most targeted sectors as certain changes have drawn our attention. The Industrials and Consumer Cyclicals sectors have maintained their top two positions and have managed to increase in numbers, albeit small, despite the decrease in overall ransomware statistics observed.

Additionally, for the first time since January, the Technology sector did not rank in the top three but moved to the fourth spot, having been replaced by the Healthcare sector. Whether this is an anomaly or a shift in which the Healthcare sector will see greater targeting remains to be seen, and one which we will continue to monitor.

Threat actors

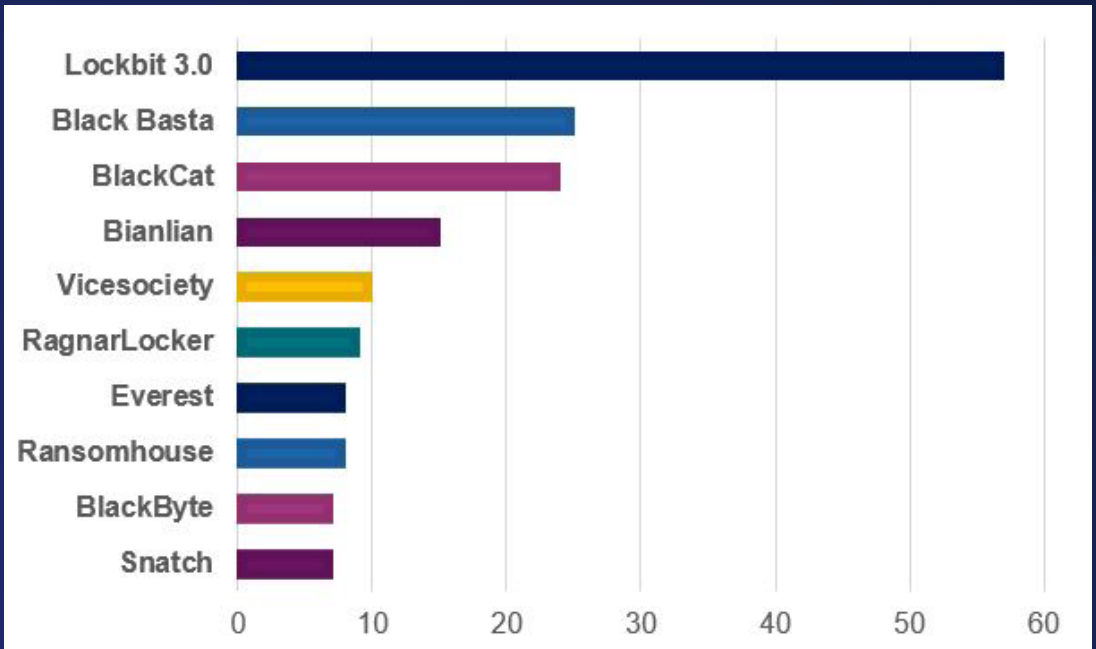

Figure 3: Top 10 Threat Actors in October

Repeating what was seen in September, the top three most active ransomware groups of October are; Lockbit 3.0, Black Basta, and BlackCat. This marks the tenth month in a row, in which a variant of Lockbit (Lockbit 2.0/Lockbit 3.0) has been the most active threat actor, and the sixth month in a row in which Black Basta has placed in the top three. This prevalence of just a few actors is relevant as, if circumstances change for any one of them, it will cause a significant impact on the overall ransomware landscape beyond that which smaller actors could have. Such circumstances include law enforcement-based disruption, evolution of TTPs, and a shift in direction of industries targeted.

October, however, did not see a repeat appearance of neither Sparta, nor IceFire; groups seen for the first time in the last two months respectively. The presence of smaller groups, in addition to the behemoths Lockbit 3.0, Black Basta and Black Cat, is a bit of a wildcard element to accurately analysing the landscape. With just a couple of attacks here and there, followed by periods of prolonged inactivity, it is difficult to predict trends or know which industries or regions might be targeted next. NCC Group will maintain active monitoring of the landscape to see if either of these two groups emerge again, and if so, to assess what level of impact they could have or if they were “one hit wonders”.

Regions

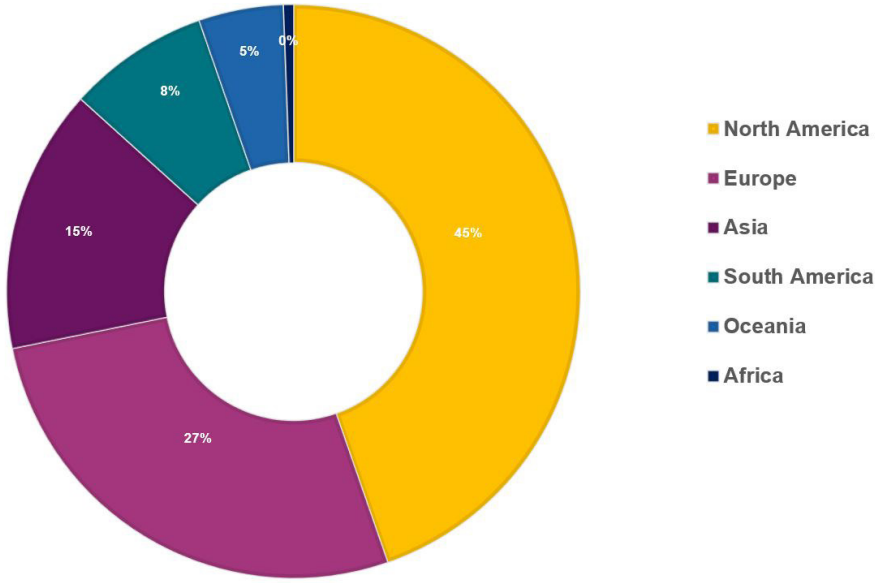

Figure 4: Regions Targeted in October 2022

In October, North America suffered 84 attacks (45%) whilst Europe experienced 51 (27%). These regions have once again swapped positions, with North America taking the lead as the most attacked region. Similar to patterns previously observed, these two regions continue to remain the top two targeted globally and will likely remain the case moving forward. As we know, Europe and the US are home to a vast number of organisations, vastly broadening the attack surface.

In addition, numbers in October have fallen to 188 total attacks compared to September's 202. However, there has been an increase in attacks in North America by 16% (9 more) and in Asia by 22% (5 more). Similarly, we have seen an increase of 300% in Oceania (6 more) and 7% in South America (1 more). Although there is an overarching lower number of total attacks, with some regions decreasing in attack numbers, it is important to remain vigilant and continue to monitor new vulnerabilities and recommended mitigations to maintain a proactive and robust position in protecting organisations and businesses.

DDoS Analysis

This October, we are excited to introduce a new analytical segment covering DDoS data. The feature comes following growing concerns regarding a rise in the number of DDoS attacks, and as such, the numbers suggest this to be the case. By including the data, we aim to unearth any trends and patterns to better support organisations in anticipating DDoS risk and putting the appropriate protection measures in place. The sources used include a combination of NCC observed data alongside open-source reporting.

This month, the database identified the highest number of DDoS attacks observed this year, 2090. This is a 14% increase from September in which 1832 DDoS events were recorded. Please note, the September figures are much larger than those in our Quarterly report as we have included new protocols targeted in DDoS events to analyse, consequently increasing the number of overall attacks observed. Despite this, it is clear that September and October illustrate a monumental growth when compared to the rest of 2022, supporting the notion that DDoS is in fact on the rise.

NCC Group TI team continue to identify new data sources for both retrospective and ongoing DDoS analysis. The data captured has, at the time of writing, not unearthed data for May 2022. While this is likely to be an anomaly, and as with all other areas of intelligence collection, the TI team will continue to identify sources that can fill this intelligence gap.

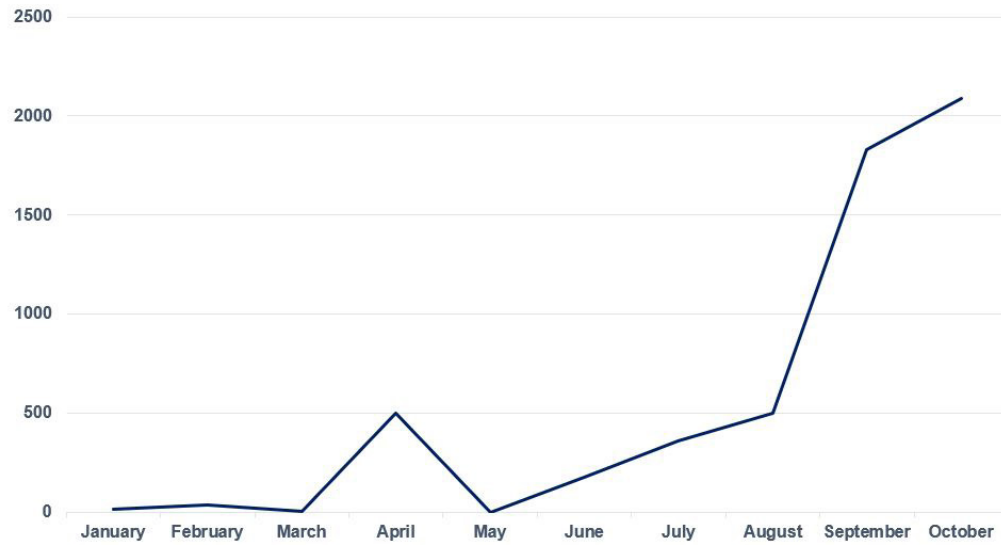

Figure 5: DDoS Attacks by Month 2022

Threat Spotlight: SocGholish

SocGholish is a framework linked to the Russian cybercrime group Evil Corp and used to gain access to networks. It has been active since at least the end of 2017 and is known for its stepwise infections in which an infection consists of multiple stages. Over the past year, SocGholish has been particularly active, showing changes in its traditional Tactics, Techniques & Procedures (TTPs), such as its final payload or how it is being distributed, and having been hosted on new servers each month.

The lack of significant changes within the framework itself shows its effectiveness and hints that it will not cease to exist any time soon. The recent reporting of fake updates from SocGholish having been dropped by Raspberry Robin infections, however, is an interesting turn of events. This may signify that in the future, SocGholish fake updates will not only be distributed via infected websites, but also through other means. NCC Group will continue to monitor this malware strain.

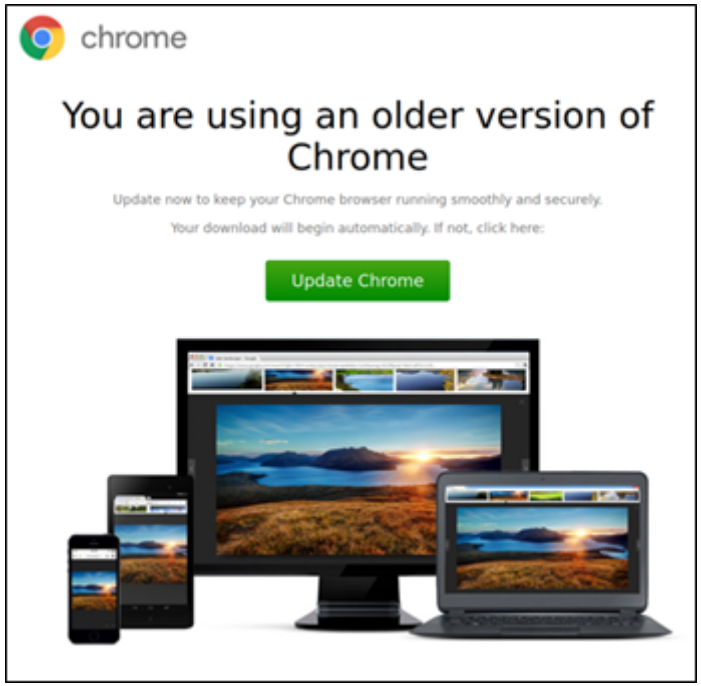

Figure 6 Fake Browser Update Page