Monthly Threat Pulse
November 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 November 2022 we observed a 41% increase in ransomware attacks compared to October, with the number of incidents rising from 188 to 265. For 2022, this increase represents the most reported incidents in one month since that of April, when there were 289 incidents, and is also the largest month-on-month increase since June-July's marginally larger increase of 47%. Comparatively, in 2021 the percentage increase was much smaller (4%) but the total figures of both were notably larger (314 for October and 328 for November). This is likely due to Conti and Pysa being heavy contributors to the ransomware threat landscape at this time, who are now dissolved/separated.

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

There are likely some interesting contributions to November's increase; not least of which being the insurgence of yet another new ransomware threat actor this month, operating under the alias of Royal. Furthermore, the relatively old Cuba ransomware group (first spotted in December 2019) has made an alarming and uncharacteristic contribution to the attack total in November (their largest ever in one month since at least January 2021).

These threat actors will be discussed in depth later on in the report.

Although LockBit appears to have sloped off this month in terms of total organisations compromised, it is possible that the newcomers to the top three threat actors are amassing as many victims as they can before the holidays, in preparation for 2023.

Sectors

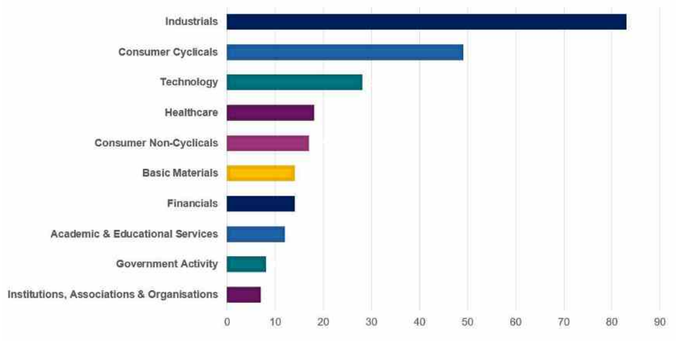

Figure 2: Top Sectors Targeted in November

In November, the top three most targeted sectors have returned to their usual ranking after a brief departure from the norm in October, where Healthcare replaced Technology for the third most targeted sector. Industrials and Consumer Cyclicals have continued to be in first and second place this month, with notable increases for both; 32% and 44% respectively.

Attacks in the Technology sector have increased by a huge 75% from October to November to solidify their place. As a side-note, Healthcare has not necessarily become less targeted, as they only have one less attack this month (from 19 - 18).

Threat actors

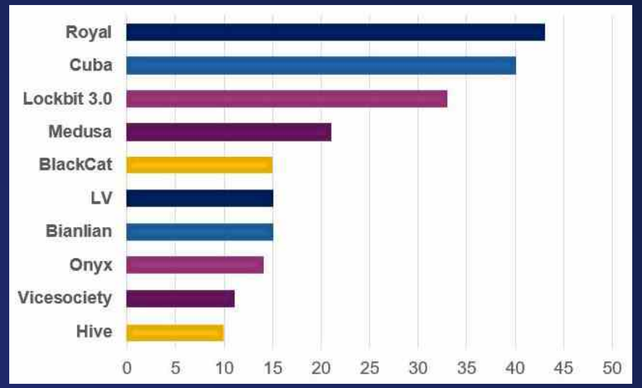

Figure 3: Top 10 Threat Actors November 2022

In addition to observing an increase in overall ransomware activity, November included several unforeseen changes to threat actor behaviour. For the first time since September 2021, LockBit was not responsible for the greatest number of ransomware attacks. Instead, the Royal ransomware strain, which appeared earlier this year, took first place accounting for 16% of attacks (43). Cuba ransomware also observed a substantial increase in attack numbers with the highest observed for the group since June 2021 (40). LockBit 3.0 remained within the top 3 ransomware actors with 33 attacks, however, this is substantially less than what we would normally expect, only accounting for 12% of total attacks, the lowest percentage observed for LockBit since January 2021.

Whilst we have observed fluctuations in ransomware activity across the year, LockBit 3.0 had remained a constant force in our database. As such, this surprising shift raises questions as to whether this is an anomaly or a reflection of wider changes across the threat landscape. We will continue to monitor and analyse ransomware trends to ascertain whether we are experiencing a more permanent shift in threat actor activity as well as the birth of new ransomware strains, for which we should be concerned.

Regions

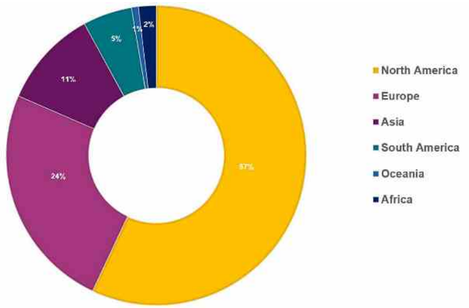

Figure 4: Regional Analysis November 2022

As observed throughout the year, the top two regions targeted globally have remained consistent; North America keeps the pole position this month with 151 (57%) total attacks, followed again by Europe with 65 incidents (25%). These two regions are likely to remain the most targeted in the near future.

In a reversal of October's dip, November has seen a 41% increase in observed ransomware attacks, from 188 up to 265. This is higher than September's count, from which October saw a reduction. This increase is not apparent globally however, but rather is localised to a select group of regions. North America observed an 80% increase in attacks from October, climbing from 84 to 151 total attacks. Attacks on Europe increased from 51 to 65, a percentage increase of 27%. Africa saw the biggest percentage increase with 400%. However, in real terms this represents 1 attack in October moving to 5 total attacks in November. Asia observed the same number of total attacks, 28, though as a proportion of total attacks it is a drop from 15% in October to 11% in November. South America and Oceania both saw a decrease in attacks in November, from 15 to 14 (7% decrease) and 9 to 2 (78% decrease) respectively.

One possible explanation for the increase in attacks against North America specifically, which represents 87% of the increase in attacks, is the occurrence of Thanksgiving. This period may have been an attractive lure to malicious actors, who counted on many companies having a reduced security team due to employees being on leave for holidays. In fact, this statement is further corroborated by November 2021's regional figures: North America accounted for an unusually high 48% of attacks, showing that Thanksgiving may very well sway threat actor attention towards North America for the month.

DDoS Analysis

In November, we observed a continued increase in DDoS numbers, from 1832 in September to 2090 in October and 3648 in November. Please note, that whilst we have observed a rise in numbers, our DDoS data collection is now much broader in scope and a by-product of this will be an increase in the overall figures. Factoring in elements such as a greater number of protocols targeted will lead to a greater number of attacks observed overall. The data collection process has however stabilised, as such, with the exception of the occasional new protocol, we can expect a more consistent dataset from November onwards.

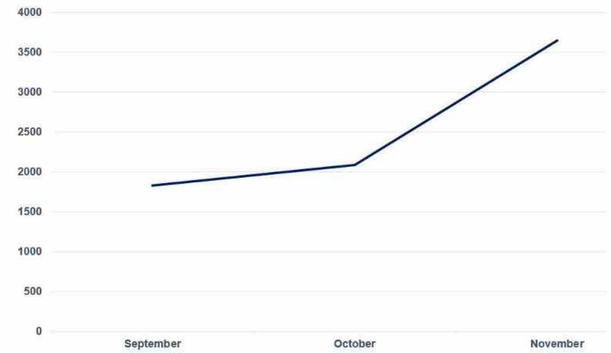

Figure 5: Month-by-Month DDoS 2022 (the following months were chosen to reflect where data collection is currently most reliable)

Threat Spotlight: Bumblebee loader

BumbleBee is a loader written in C++ first reported by Google in March, although the malware has undergone significant changes in recent months. While BumbleBee was initially associated with a single actor, it was later distributed by multiple actors such as TA578, TA579, TA580 and later on by Smokeloader used from a PPI (Pay Per Install service) actor.

The packer used in the BumbleBee campaigns right from the start were mostly unique to it, until a certain point where it was also seen with other malware such as Qbot. While the packer was fairly simple in terms of complexity, it served its purpose and remained the same for several months. By early November, another security company noticed that the heap structure used in the packer to handle the decryption process ceased to exist, along with the removal of the various anti methods in the core payload.

Research has shown that the BumbleBee packer now works in a different way – instead of directly decrypting and loading the loader, the packer decrypts a shellcode, which then loads the loader in memory. The shellcode is responsible for locating, decrypting and mapping the loader in memory, transferring the execution there.