Monthly Threat Pulse February 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

Ransomware remains a critical threat to the security landscape with attackers all the more active and numbers at a record high for the current period. For the first time in the last three years, our ransomware database has recorded the highest number of cases for February, with 240 cases, and demonstrates a 45% increase from January 2023 (165). This not only surpasses the number of incidents for February 2022 (185) and 2021 (185), but follows a record high number of atttacks in January 2023, discussed in January's Threat Pulse, with a clear increase from 120 attacks in January 2022 and 127 in January 2021.

January and February 2023 have thus far accounted for 405 incidents, 26% more than in 2021 and 38% more than 2022, for these same time periods. Whether this is setting the tone for a growing number of ransomware attacks across the year is yet to be seen, however, it remains evident that ransomware incidents are currently on the rise. In this respect, organisations should remain alert to the threat posed, with particular consideration for those key sectors and threat actors, discussed in the subsequent sections.

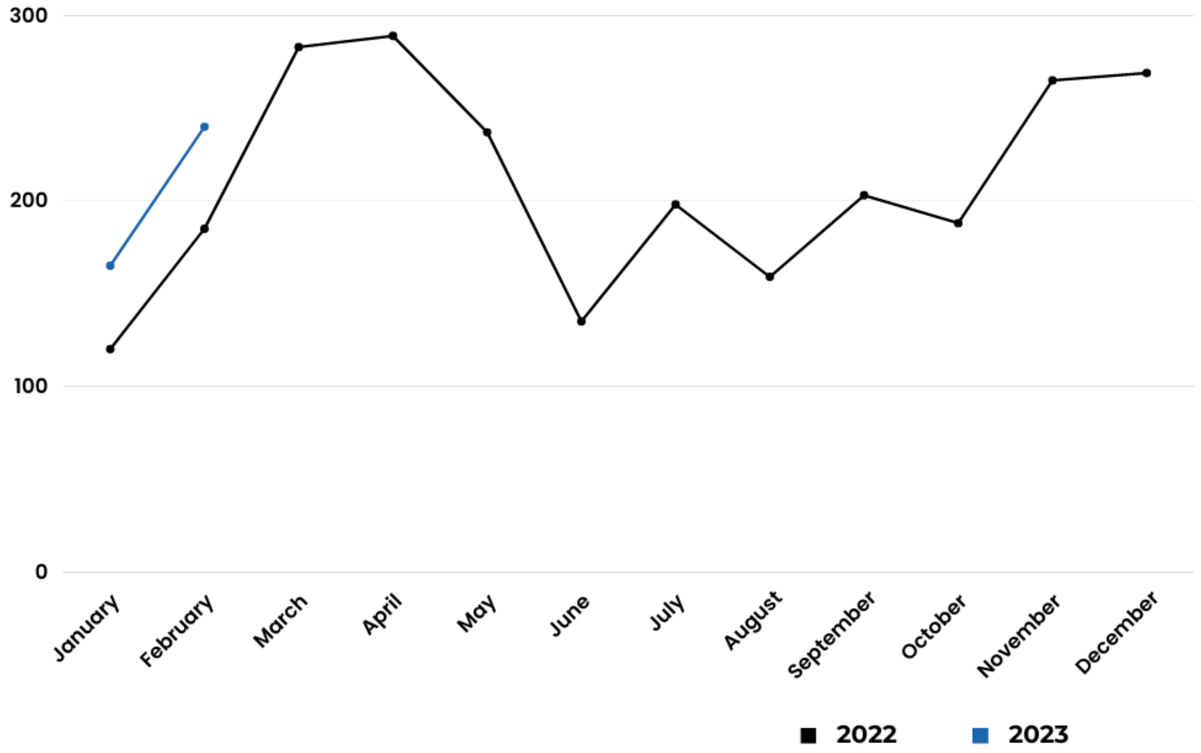


Figure 1: Global Ransomware Attacks by Month

Sectors

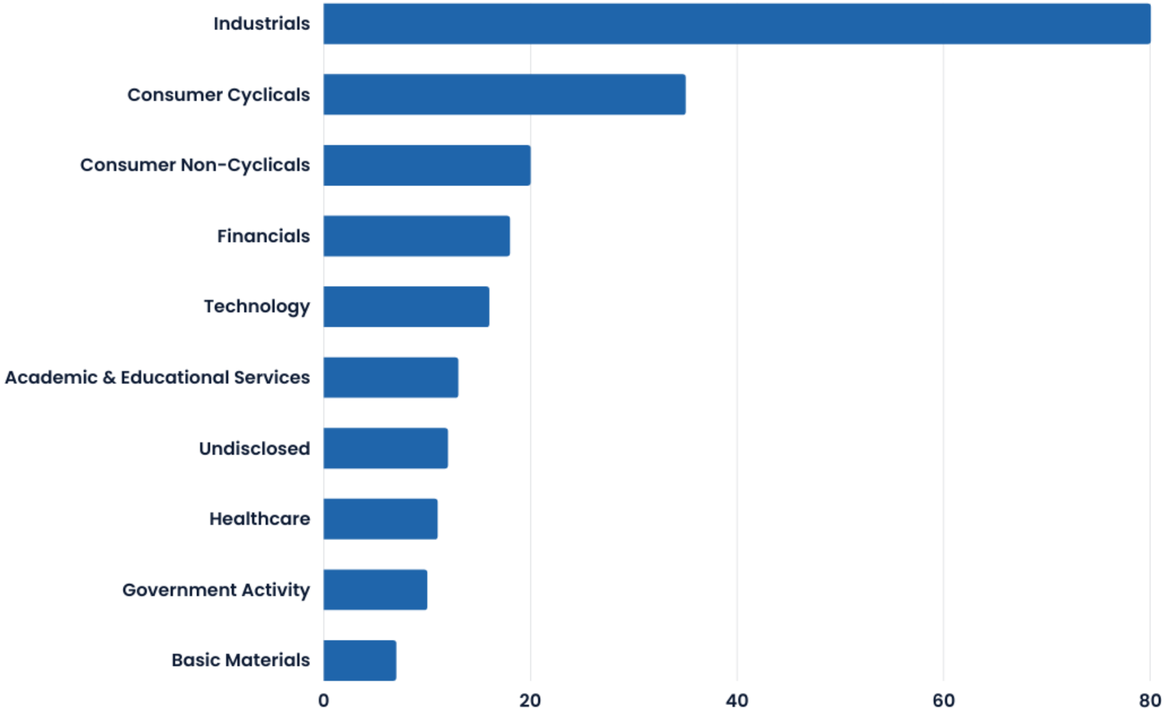


Figure 2: Top 10 Sectors Targeted February 2023

Industrials

The most targeted sector of February 2023 was Industrials with 80 of the total 240 attacks, representing 33% of the total ransomware cases this month. This is an increase of 31 attacks in total figures when compared to January, but only a proportional increase of 3%. As we have mentioned in previous reports, this sector contains a variety of industries that are of interest to OCG's for differing reasons; from the presence of an abundance of PII to be extorted (Professional and Commercial Services), to the costly ramifications of operational disruption incentivising ransom payments (Construction & Engineering).

Threat actors

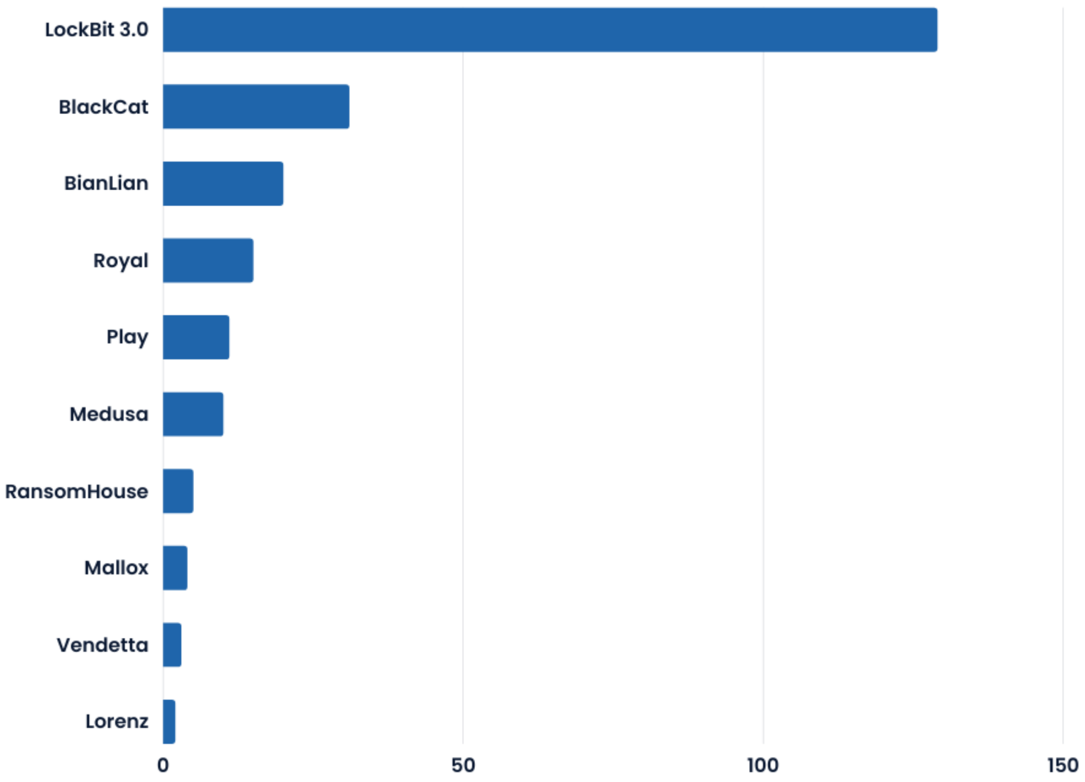


Figure 3: Top 10 Threat Actors February 2023

The three most active threat groups in February were LockBit 3.0, BlackCat, and Bianlian. This is the third month in a row in which LockBit 3.0 have been the most active group. In February they were observed to carry out 129, or 54% of, attacks, up from 50 and 30% last month respectively. BlackCat has consistently been one of the more active ransomware groups, but has over the last few months bounced up and down within the rankings. It climbs a spot this month to second most active group with 31, or 13% of, attacks.

Though this was 11 more attacks than in January, it was only a 1% increase from 12% of total monthly attacks in January. Bianlian has had an explosion of activity between January and February, increasing their output by 500% from 4 attacks, or 3% in January to 20, or 8%, in February. Despite an increase in attack output by 500%, Bianlian's share of the overall ransomware attacks merely doubled. This highlights the expected escalation in attacks after the seasonal January slump, though indicates that this increase is almost entirely accredited to LockBit 3.0's activity.

Regions

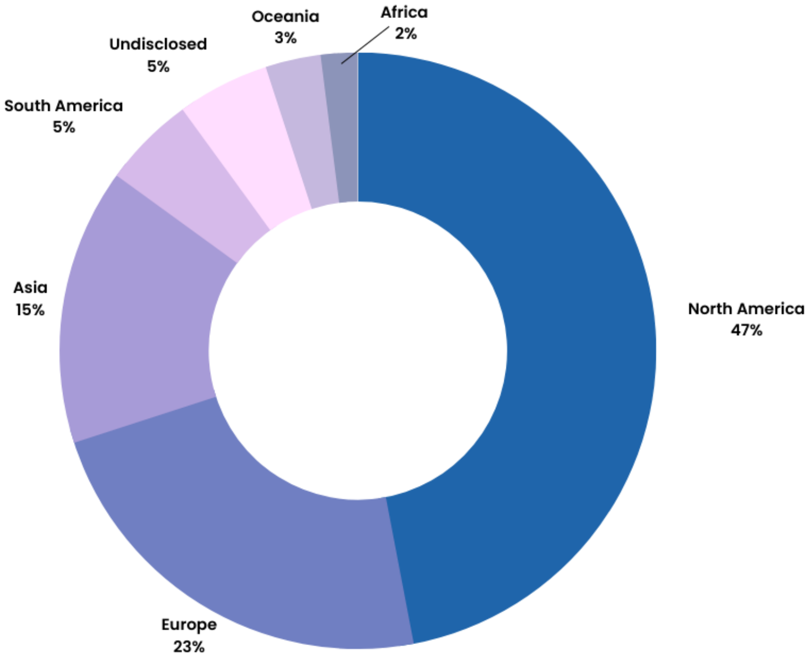


Figure 4: Regional Analysis February 2023

Whilst the number of attacks observed in February grew, similar regional targeting distribution was observed. North America continues to lead in attack prominence with 113 attacks (47%), followed by Europe with 56 (23%), Asia with 35 (15%), South America with 13 (5%), Oceania with 6 (3%) and Africa with 5 (2%). A total of 12 incidents are categorised as 'undisclosed' and shall be reviewed once ransomware actors release the names of the victims, should they fail to pay the ransom.

Although North America revealed only a 6% proportional increase in attacks, from 41% in January to 47% in February, in real terms this is a growth of 45 additional incidents. Europe observed a proportional decline of 10%, however the continent observed an equal number of attacks with 56 incidents in both January and February. As such, whilst taking up slightly less of the regional distribution, European attack numbers appeared to have stabilised in February. Overall, the increase in ransomware events is predominantly observed in North America and Asia, with 45 incidents in the former and 16 additional incidents in the latter.

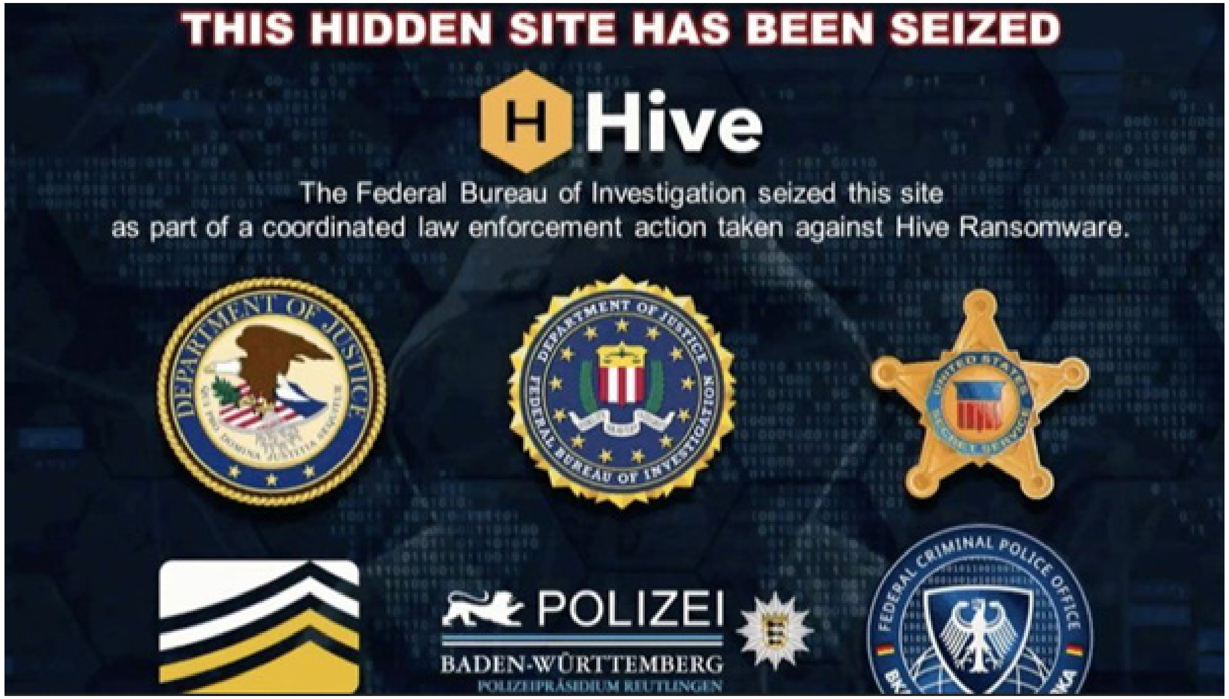
As always, we advise organisations globally to remain alert to cyber threats, however, particular emphasis may be placed on those within North America and Asia. Whilst we anticipate the greatest number of cases to be in North America each month given the sheer volume of entities there, an increase of 47% should encourage organisations to be all-the-more vigilant. Asian organisations alike should continue to arm themselves against possible ransomware attacks.

Spotlight: Move Over HIVE

Summary

The US Department of Justice reported in January 2023 that the FBI had infiltrated Hive's network and seized their infrastructure in a coordinated international effort. The infiltration began in July 2022, where they obtained Hive's decryption keys and offered them to over 300 current, and over 1,000 previous, victims of Hive ransomware, reportedly costing Hive $130 million in ransoms. Amongst the seized infrastructure was Hive's leak site and front- and back-end servers, of which two back-end servers had been located in Los Angeles.

In addition to the takedown, US and UK authorities sanctioned seven alleged members of the group, all believed to be Russian nationals. It is widely reported that Russian cybercriminal gangs are protected by the Russian state, advised by the authorities not to leave the country if targeting entities abroad. With that in mind, we can assess as likely that while Hive has lost its digital assets, its members will continue operating under a different guise.


THIS HIDDEN SITE HAS BEEN SEIZED
H Hive
The Federal Bureau of Investigation seized this site
as part of a coordinated law enforcement action taken against Hive Ransomware.
DEPARTMENT OF JUSTICE
DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE