Monthly Threat Pulse
August 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?

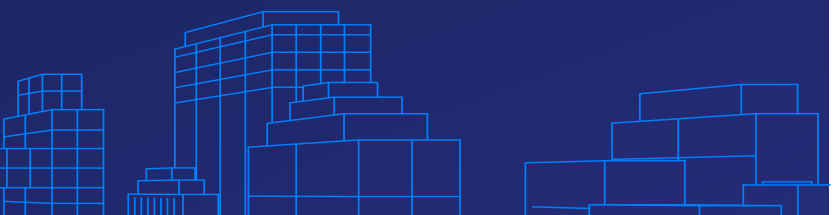
Ransomware Tracking

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?

Analyst Comments

From July to August we observed a 19% decrease in ransomware attacks, with the amount of incidents falling from 198 to 160. This moderate drop comes after a 47% rise from June to July, and LockBit appear to be the only consistent presence in the threat landscape in August (from 62 attacks in July to 64 in August). Other groups such as ALPHV and Hiveleak have exhibited significant drops in their activity in August, contributing to this dip in the volume of attacks.



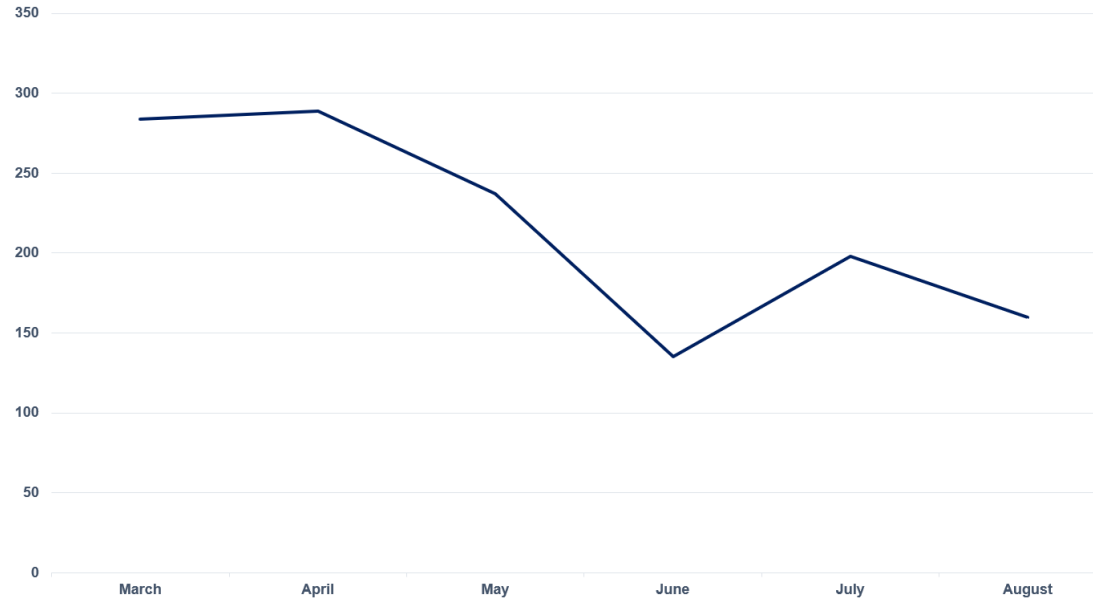


Figure 1: Total Hack & Leak Cases Month-by-Month

Contrarily, from July to August 2021, there was a significant increase in the number of ransomware cases: from 159 to 309 total attacks (a 94% increase). In July 2021, Conti were largely inactive (they only performed 7 hack & leak attacks) but, by the end of August 2021 they had accumulated a total of 146 victims, thereby contributing to the enormous increase in this time period.

Given that Conti are no longer operational as a ransomware gang but have instead diffused into other smaller groups, they are likely no longer contributing to the threat landscape in such a concentrated fashion, thus resulting in the year-on-year disparity from 2021 and 2022.

Sectors

Running consistently with previous months, the most targeted sectors in August were Industrials with 55 incidents (34%), Consumer Cyclicals with 28 (18%), and Technology with 22 (14%). Given the minor decrease in total cases in August, the individual figures for each of these sectors have decreased proportionately alongside, by no more than 8 less victims (as is the case with the industrials sector).

Irrespective of the fluctuations in attack frequency for each sector, we can expect these sectors to remain the most targeted by ransomware groups for the rest of 2022. Given the vastness of the industries and activities within, these organisations remain an attractive opportunity for extortive threat actors due to the costliness of operational disruption and the varying types of sensitive data that they often store.

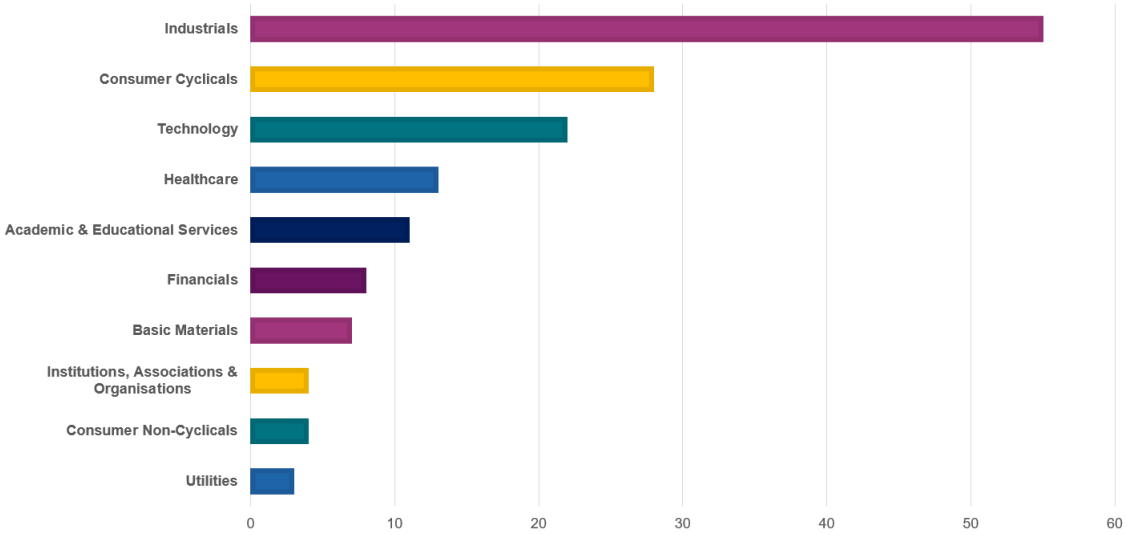


Figure 2: No. of Hack & Leak Cases by Sector in August 2022

Threat actors

The top three threat actors observed in August are Lockbit 3.0, Blackbasta, and IceFire, with Lockbit 3.0 maintaining its position at the top of the list of threat actors and BlackBasta moving up a level to the second place compared to last month's analysis.

In August, we observe a change in activity as a new ransomware threat actor called IceFire joined the top three list of threat actors. This is a big change as this threat group has not yet been observed within the top 10 reported lists of threat actors.

This new ransomware threat actor was first observed in March 2022 and has been reported to deploy ransomware attacks against English speaking victims.

Research of IceFire shows that this ransomware group implements common TTPs used by most threat groups, such as compromised email or websites for initial payload delivery, with the subsequent deployment of ransomware onto target systems.

As a new ransomware group in the threat landscape this month with a significant victim count already, we will continue to observe this group in the coming weeks.

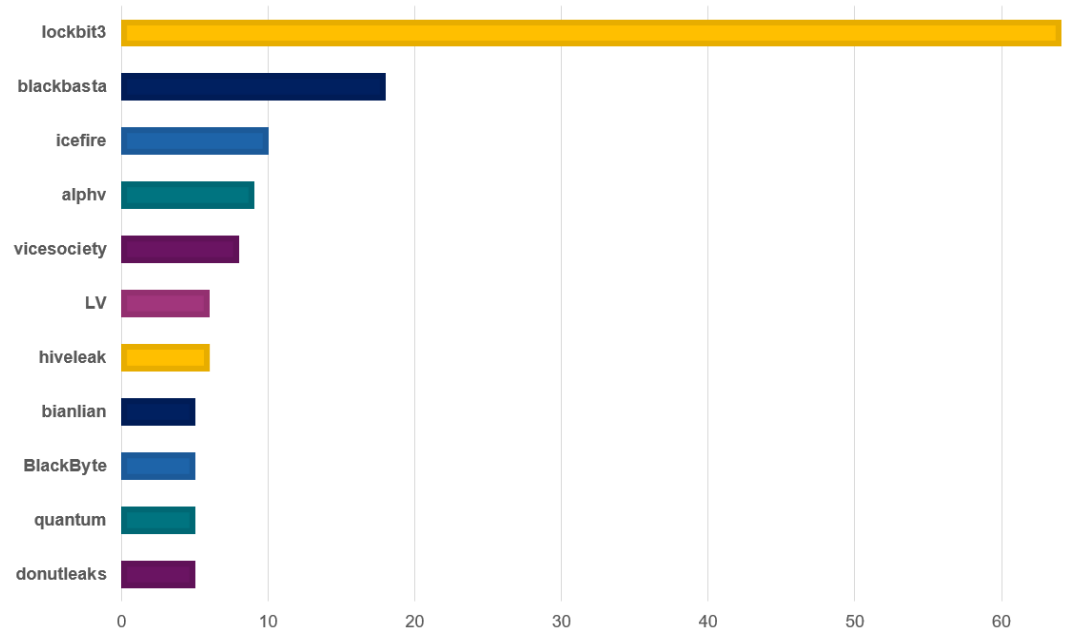


Figure 3: Top 10 Threat Actors August

Regions

In the month of August, North America had 71 incidents (45%) and Europe had 63 incidents (40%) reported. These regions have maintained their positions at the top of the list as the most targeted regions. However, a slight decrease in attacks was identified following the July report, with North America reflecting a 14% decrease and Europe having a 20% decrease. This decrease in attacks is reflected across all regions, with Asia reporting 15 incidents at a 29% decrease, South America with 4 incidents at a 20% decrease, Africa with 3 incidents with no decrease in attacks, and Oceania with 2 incidents and reports a 71% decrease.

For the month of August, we reported a total 160 incidents, which is a 38 point (19%) decrease in incidents deployed against organisations. Analysis of the sectors within these regions reveals that, Industrials with 55 incidents, Consumer Cyclicals with 28 incidents and Technology with 22 incidents, all remain as top sectors under continued attack. This shows that irrespective of a decreased number of attacks generally reported across regions, these top three sectors remain of interest to malicious actors and require continuous implementation of preventive security controls by organisations' within these regions to protect against threat actors.

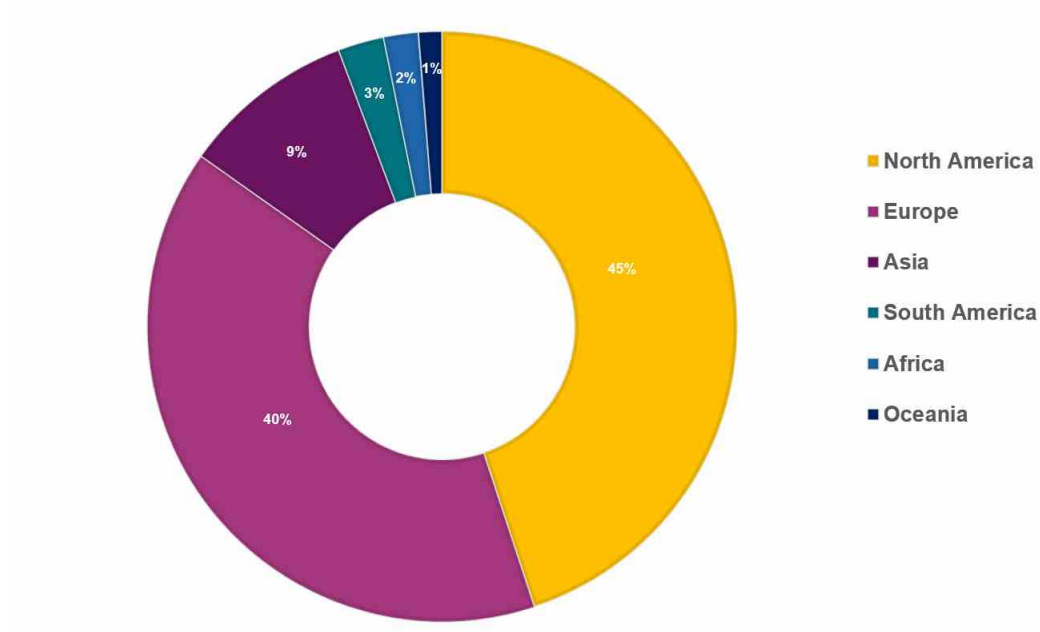


Figure 4: Percentage of Hack & Leak Victims by Region

Threat actor spotlight:

Sandworm

The Sandworm Team is a state-sponsored Advanced Persistent Threat (APT) group attributed to the cyber-military Unit 74455, within Russia's General Staff Main Intelligence Directorate (GRU).

This highly capable threat group have operated out of the Russian state since at least 2009, conducting global espionage and destruction campaigns that seek to advance Russian foreign policy.

Interestingly, attribution was not achieved until 2020, when the United States Department of Justice (DoJ) identified Sandworm as pertaining to the GRU.

Sandworm's victims span different sectors; however, their most notable and widely destructive attacks have sought to cripple the industrial control systems that power the energy and electrical sectors of their adversaries, i.e. Ukrainian 2015/2016 power outages.

Destructive events have mainly targeted Ukraine, as Russia undergoes territorial wars, seeks to prevent democratic encirclement in its surrounding territories and deter perceived threats to Putin's re-establishing of a Russian empire.

Sandworm's targets do however remain global, and historic events include the targeting of the 2017 French Presidential Campaign, 2018 Winter Olympics in South Korea, and the large-scale attack on cross-sector Georgian websites and servers in 2019.

Attacks across the varying geographies represent attempts to advance Russian interests but have also encompassed specific retaliatory behaviours, such as those of the 2018 Winter Olympics for Russian doping offences. To an extent, this allows us to better predict Sandworm's activities, as we can theorise to which global events Russia may seek to react.

Additional motivations behind Sandworm's attacks may include fierce rivalry between the Russian security agencies that increases the risk-seeking attitude of the GRU overall.

Russian agencies such as The Foreign Intelligence Service (SRV) and The Federal Security Service (FSB) compete for resources, personnel and influence, a secondary objective of the Sandworm Team could therefore be advancing its relative position to the other Russian intelligence agencies by undertaking high-risk/high-reward operations.

Earlier operations carried out by Sandworm Team have illustrated that the threat actor has an unusual low risk sensitivity, especially for an actor involved in state-sponsored operations.

The deployment of the NotPetya ransomware is a prime example of this; without any consideration for collateral damage, the group let loose a malware worm that wiped more than 49,000 computers and caused havoc worldwide.

Figure 5: Indicted Russian Nationals believed to be Members of Sandworm Group

The above operators were indicted on the 19th of October 2020, following the FBI's two year pursuit of the GRU operatives responsible for "conducting the most disruptive and destructive series of computer attacks ever attributed to a single group, including by unleashing the NotPetya malware." This series of attacks also included the usage of the Olympic Destroyer malware and KillDisk, as well as their involvement in targeted spearphishing campaigns.