nccgroup

Monthly Threat Pulse September 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

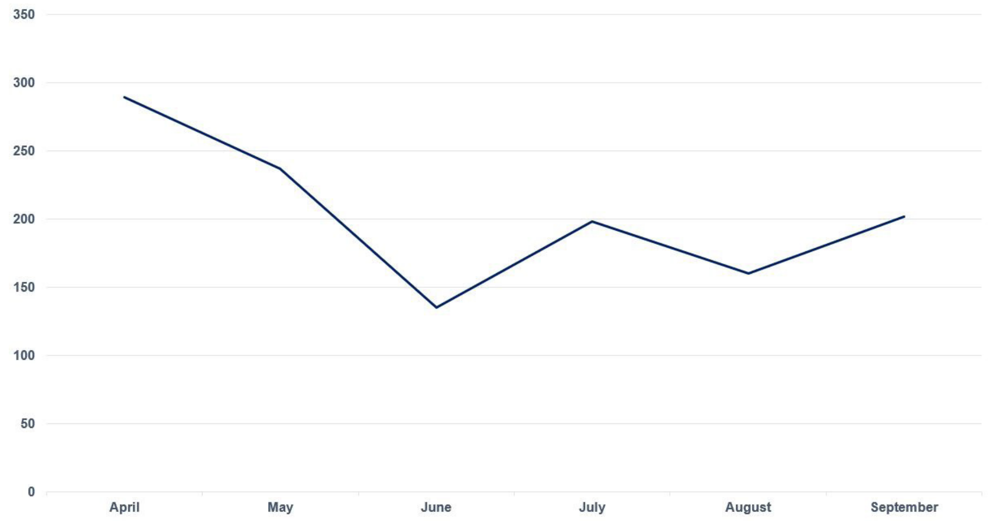


Figure 1: Total Hack & Leak Cases Month-by-Month

Following the July-August decline in which we reported a 19% decrease in ransomware incidents, the number of ransomware attacks are once again on the rise. In September, we observed 202 ransomware attacks, a 26% increase from the 160 reported in August. Since the figures began to decline in April, the data suggests a rather turbulent spring and summer period for ransomware this year, with the most pronounced drop in May-June. As discussed in our recent reports, a combination of seasonal fluctuations and changes to threat actor groups including Conti's disbanding, Lockbit's rebrand, and new threats actors on the scene, has resulted in a rather unstable trend at present.

In 2021, whilst the numbers peaked at greater heights, a similarly volatile pattern was observed with fluctuations between July (148), August (306), and September (182). Numbers increased but stabilised over the October and November periods (313 and 328 respectively). As we move into the autumn and winter months of 2022, we may therefore expect to see some stability in both, with respect to threat actors, and in line with previous trends.

Sectors

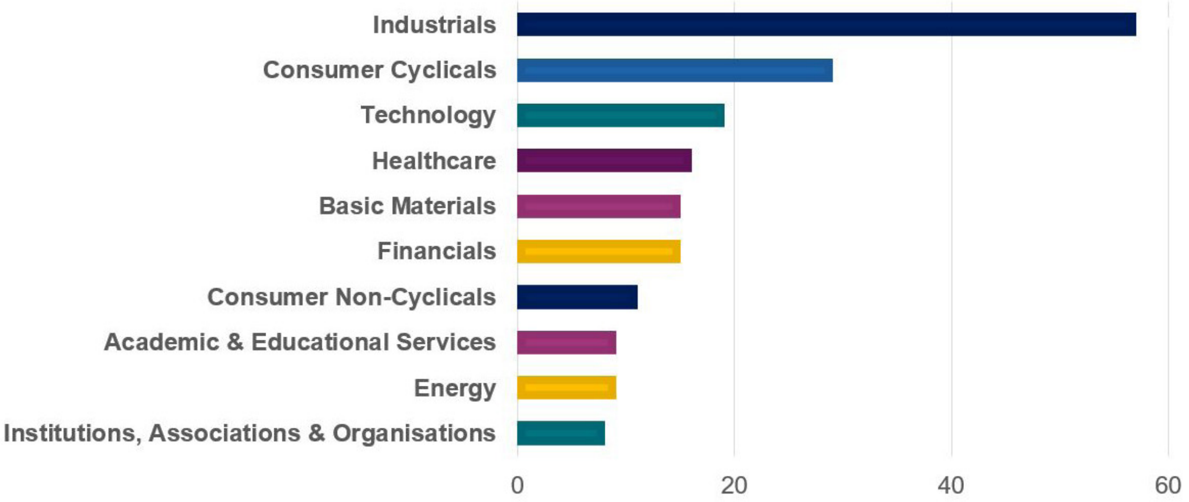


Figure 2: No. of Hack & Leak Cases by Sector in September 2022

In line with previous months, our top three sectors remain the Industrials with 57 incidents (28%), Consumer Cyclicals with 29 incidents (14%), and Technology with 19 (9%). Although we have observed an increase in the overall statistics this month, in each of these three categories the number of attacks remains similar to those of August. The Industrials sector increased by 3 incidents (55-58), Consumer Cyclicals by 1 (28-29) and Technology decreased by 3 (22-19). Minimal fluctuations in attack numbers suggests continued interest by threat actors in these sectors as ransomware targets.

Throughout the year, this pattern has persisted and we have come to expect the targeting of these three sectors as the months unfold. As discussed in previous reports, these sectors provide critical services to which disruption would prove extremely costly, hence forming strong targets. Whilst these sectors remain important and we continue to monitor their respective trends, a number of additional sectors demonstrate a growth in attack numbers and warrant analysis.

Threat actors

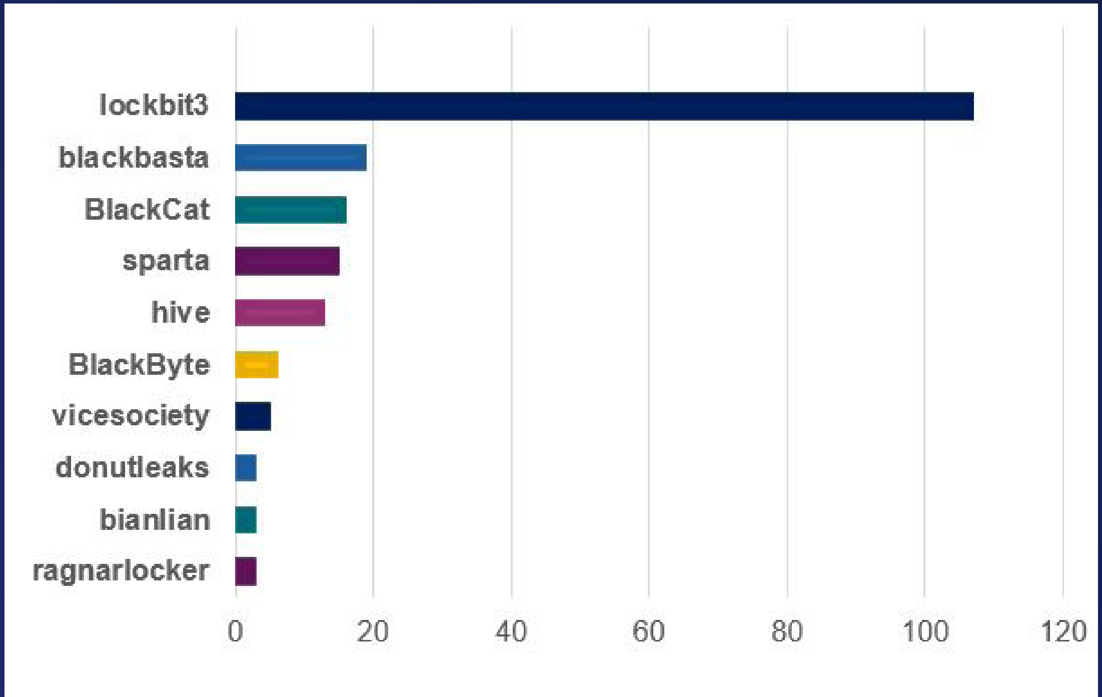


Figure 3: Top 10 Threat Actors in September 2022

The top three threat actors observed in September were Lockbit 3.0, BlackBasta and BlackCat, with Lockbit 3.0 and BlackBasta maintaining their positions in first and second place, like in August 2022. Interestingly, in August we observed a new hack & leak threat actor on the scene, IceFire. However, they are not present in September's ransomware leak data and their leak site is currently inaccessible. This implies that they have either wilfully discontinued their operations or have been forced to go offline by law enforcement. NCC Group will monitor for any further information regarding the absence of the group.

What makes this more significant is the fact that yet another new ransomware hack & leak group has joined the scene, Sparta. First spotted by NCC Group on the 13th of September, where it appears that they successfully compromised 12 victims in one day, showing that they are also off to an explosive start.

Regions

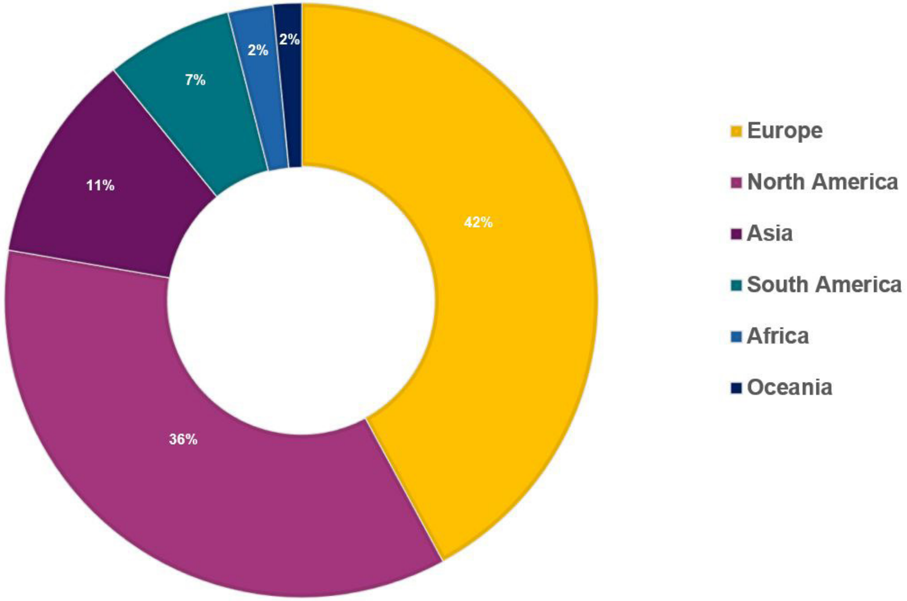


Figure 4: Percentage of Hack & Leak Victims by Region September 2022

In the month of September, Europe suffered 85 attacks (42%) whilst North America suffered 72 (35%). These regions have swapped position since last month, though they remain the top two targeted regions globally. Overall attack numbers are up in September, as well as for each region individually: Europe reported a total increase of 21 attacks (33%), North America had 1 more total attack over August (1.4%), Asia had 8 more total attacks (53%), South America reported 11 more (275%), Africa witnessed 2 more attacks (67%), and Oceania saw 1 more (50%).

We reported a total of 205 ransomware attacks, up from 160 in August, representing an increase of 28.75%. This increase in attacks was not the result of one specific region becoming of higher interest to malicious actors but was felt globally. This highlights the importance, regardless of which region an organisation is situated in, of maintaining strict security controls and keeping up to date with emerging vulnerabilities and patches; the rewards of taking the basic steps consistently and in a timely manner often outweigh the effort of taking them.

Spotlight:

China and APT 41

Chinese Espionage Overview

These last months have revealed numerous efforts by China to conduct widespread cyberespionage campaigns to advance their nationalistic objectives. Security research reports, news headlines and strategic decisions by Governments suggest that the threat posed by Chinese APTs is present, perhaps even heightened. Since early 2021, highly sophisticated cyber capabilities, lengthy campaigns and new malicious tools have targeted, and continue to target, organisations worldwide.

NCC Group's CIRT team also published new research analysing a recent incident response engagement exploiting ShadowPad malware. Notably, the malware is closely associated with Chinese threat actors leading researchers to assess with high confidence that the case involved Chinese APT actors. The blog explores key TTPs employed including a previously undocumented backdoor, providing key technical insight into ongoing campaigns by Chinese threat groups.

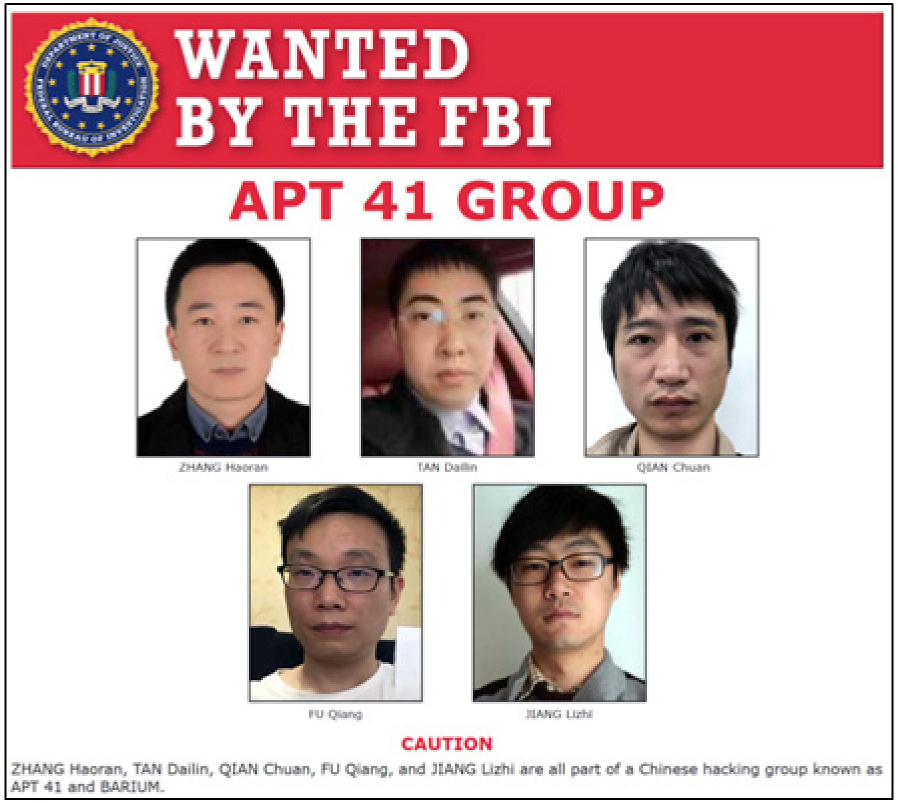
Much of the activity reported by researchers and news headlines alike has been attributed to the Chinese nation state actors, APT40 and APT41. Between the two groups, China's victimology is diverse, reflecting the highly expansive reach of their espionage capabilities and objectives alike. Whilst the focus of their intelligence efforts is manifold, certain campaigns demonstrate how China are quick to respond to geopolitical events, seeking to identify information that furthers their position on the world's stage. This is not only indicative of Chinese APTs but threat actors more generally who, like any business, define their strategy in the context of global events.

Who are APT41?

Overview

APT41 (AKA BARIUM, Wicked Panda or Double Dragon), is a prolific advanced persistent threat group believed to be working under the instruction of the Chinese Ministry of State Security (MSS). This highly sophisticated and innovative adversary has leveraged supply chain compromises against its targets, compromised digital certificates and developed a wide selection of custom malware such as bootkits for their operations. The group is unique among tracked China-based actors in that it also leverages custom malware typically reserved for espionage operations in what appears to be activity that falls outside the scope of normal state sponsored missions. Based on earlier activity, this includes cybercrime activities for personal financial gain or showcasing their hacking skillset. This contrasts the state-sponsored goals that likely drive the group's targeting of organisations in sectors like finance, government, healthcare, higher education, and industrials.

In September 2020, the US Justice Department unsealed charges against five Chinese nationals believed to be members of the group. According to the indictment, the operators have been responsible for more than 100 breaches of organisations globally; the document also mentions that the group is suspected of financially motivated and state directed operations. The charges accuse the group of coordinating its operations out of Chengdu 404 Network Technology Company, a security company operating out of mainland China. The operators are therefore not believed to be intelligence officers directly employed by the Chinese government, but contractors hired for specific operations or tasking.



ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

Figure 5: APT41 Chinese Nationals Charged

Motivation

China's offensive cyber operations support the country to gather intelligence without resorting to conventional military recourse. As such, APT41s role helps avoid traditional military conflict when supporting China's economic development plans; this has included gathering intelligence ahead of critical procedures like mergers and acquisitions (M&A) and political events. Finally, the group's dual motivations are reflected in one of their naming conventions, the 'Double Dragon'. With one side representing espionage and the other finance, this embodies the groups' national policy priorities by day, and targeting of gaming and software industries for profit by night.

Intended Effect

The potential spectrum of intended effects is broad and diverse, and includes:

- Strategic national advantage through information superiority.
- Defensive security through demonstration of potential for offensive capabilities (establishing and maintaining a cyber 'balance-of-power').
- Commercial / Economic benefit through the theft of Intellectual Property.
- Maintenance of internal stability (i.e., prevention of dissent, strikes, riots etc.).