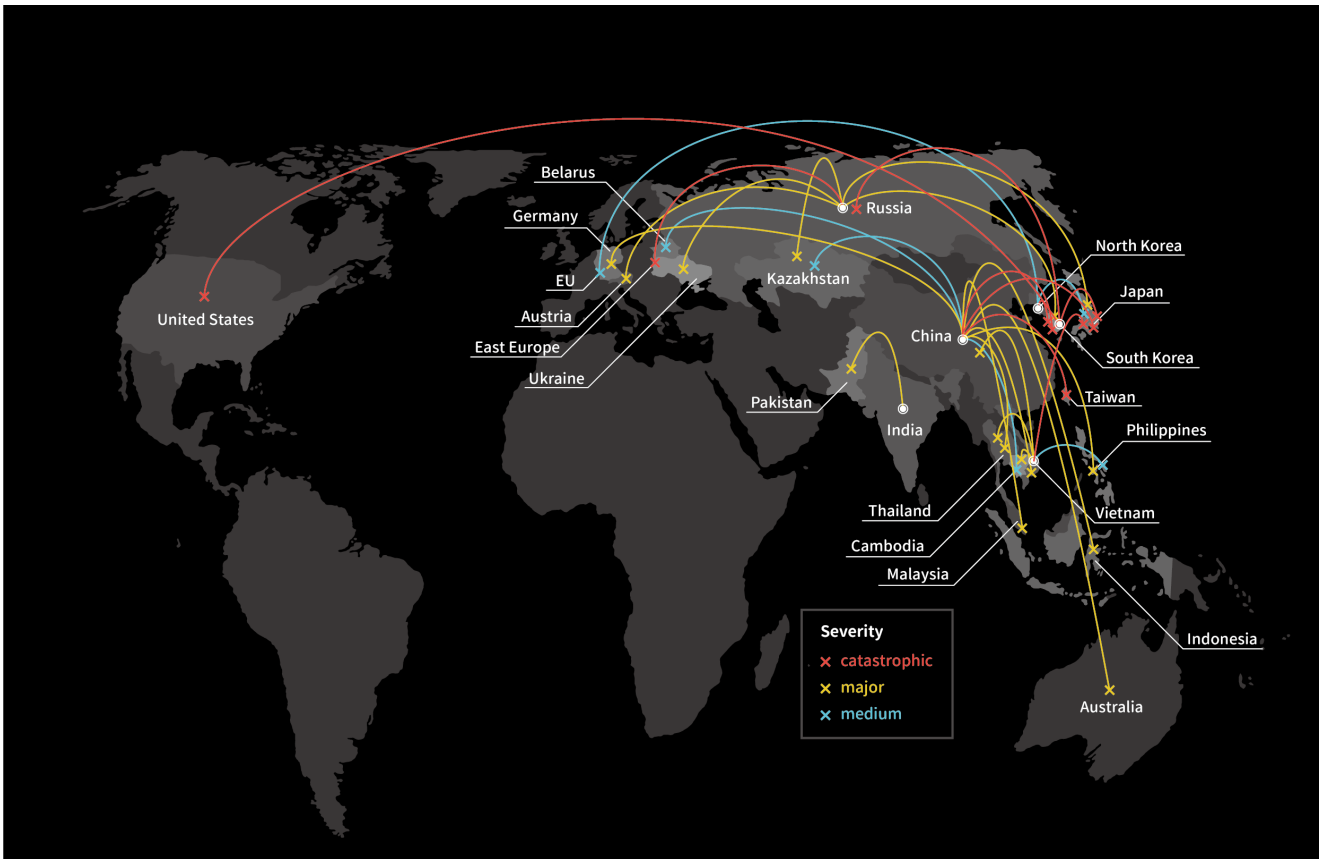
APT Threat Landscape of Taiwan in 2020

teamt5.org/en/posts/apt-threat-landscape-of-taiwan-in-2020/

Charles Li



5.10.2021Charles Li

Share:

By TeamT5 CTO Charles Li

2020 was considered to be a year of chaos and disaster. Big events such as the outbreak of COVID-19, geopolitical conflicts escalations in several areas, Brexit, and the U.S. president election, all influenced people around the world. In 2020, TeamT5 continued helping numerous security breaches caused by state sponsored targeted instruction attacks (APT) . In the meantime, TeamT5 intelligence Team proactively tracked APT actors' new activities. Compared with real world, the cyber world was also full of turmoil in 2020 and many of them are reflections or extensions to events in real world. In this article, we will discuss our observation of APT trends in Taiwan in 2020.

In this article, we will first walk you through some remarkable trends, including:

- Evolution of APT tactic

- Supply Chain attack became a primary method in APT attacks
- COVID-19 driven cyber attacks

We will try to dissect the attacks happened in Taiwan in industrial view and adversarial view, which is a common method in threat intelligence analysis. Last part will be our conclusion and suggestions to respond with APT attacks.

Evolution of APT tactic

In 2020, the most notable APT event in public would be the ransom-attack that strike several energy related companies in May [1]. TeamT5 research shows it to be a well-organized campaign from a notorious Chinese adversary group. Whether financial gain or political deterrence is the real motivation behind the ransom-attack remains a mystery. However, it has marked a milestone of China's cyber-attacks against Taiwan: Chinese APT have aimed Taiwan for more than 20 years but only limited in cyber espionage operations in the past but the threat actors are now exercising new tactics to evade us.

Another cyber-attack supporting our hypothesis occurred on PTT, the most popular BBS platform in Taiwan. TeamT5 tracked a series of posts related to some scandals, with attempts to uglify Taiwanese governments or military, on PTT in July 2020. The actors abused hopping servers from various countries to hide their footprints. However, TeamT5 intelligence database shows that one of the source IP address was also used by a Chinese APT that has targeted Taiwan for more than ten years. Besides, another private source also verified the same APT group to be the culprit behind the attack. We consider both events to be indicators of China's expansion on offensive cyber operations, which we have not observed in the past.

Supply Chain attack becoming a primary method in APT attacks

Supply chain attack has become a major intrusion method for threat actors in 2020 and TeamT5 had warned such tactic in advance [2]. SolarWinds breach was undoubtedly the most successful story among them. Many high-profile US government agencies, Fortune 500 companies and even cybersecurity vendors were affected. It is so sophisticated that the scope is still uncertain yet. In Taiwan, we also observed at least three waves of similar attacks that infiltrated service providers and further leveraged their products or services to infect more victims. The first two had been published by the Ministry of Justice Bureau (MJIB) of Taiwan in August [3]. The third was still under investigation and the impact could be

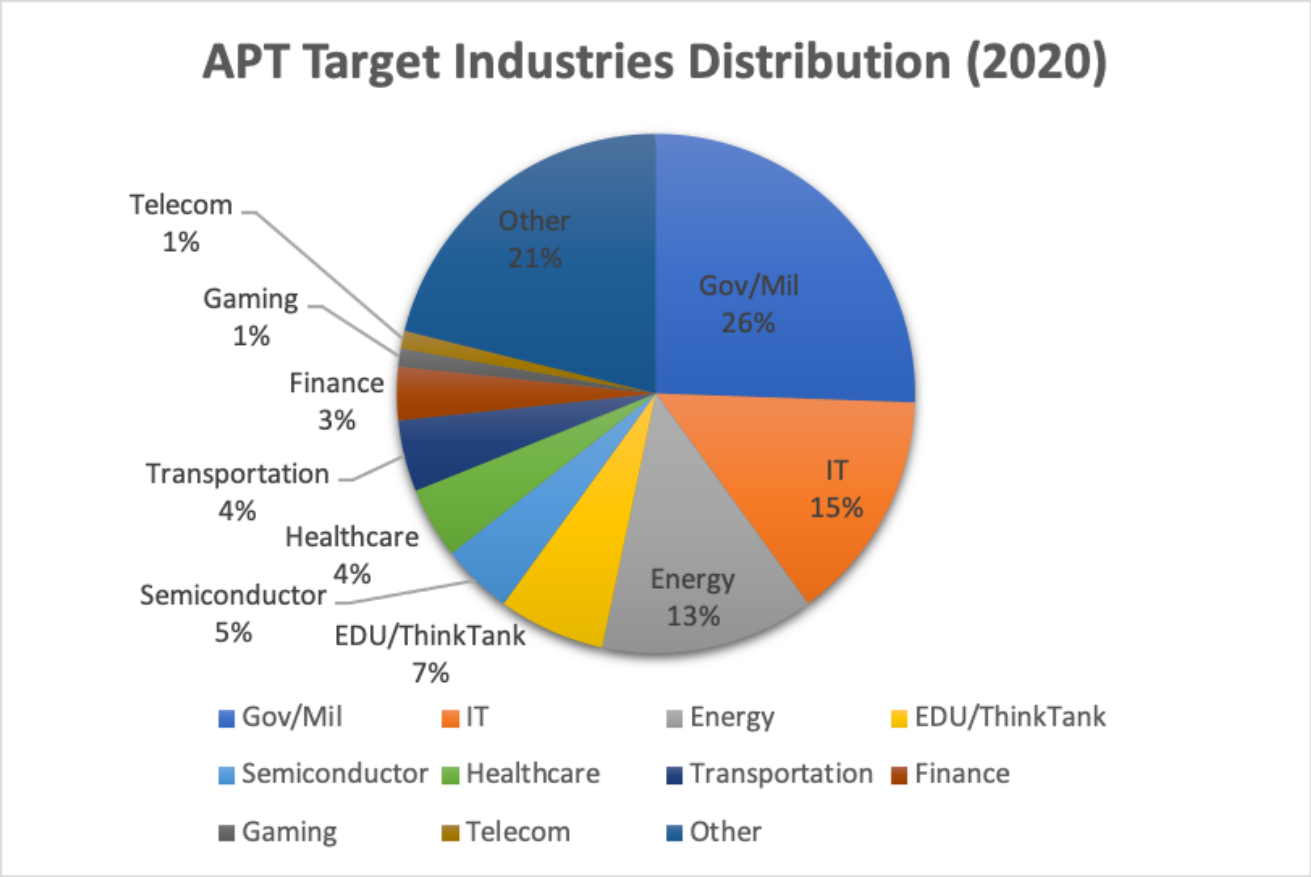
even bigger. We have seen a significant numbers of government agencies or private corporates in Taiwan being compromised. TeamT5 research shows that at least 3 distinct China nexus group were involved in these operations.

COVID-19 driven cyber attacks

Another interesting phenomenon would be COVID-19 related cyber-attacks. Soon after the outbreak of COVID-19 pandemic, we observed state sponsored actors collecting intelligence for the pandemic. In the second half of 2020, threat actors shifted their focus to chasing COVID-19 vaccine information with the advance of COVID-19 vaccine development. In Taiwan, TeamT5 also intercepted several spear phishing emails using COVID-19 as lure theme or even more campaigns related to healthcare related entities. We believe the trend will continue as long as the COVID-19 pandemic still exists.

TeamT5 Intelligence Team had analyzed around one hundred APT attacks from China in 2020. Our statistic shows government and military agencies are still the biggest target and attacks against them counts for more than 1/4 in total and almost every APT groups that are active in Taiwan are coveting them. This trend has lasted for long since the ultimate goal of Chinese espionage operation is to obtain confidential national information. Information Technology (IT) industry also got attention a lot by APT actors and TeamT5 has observed a dramatical increase of attacks against IT industry. We believe this phenomenon is a result of threat actors' attempts to abuse supply chain attacks and IT companies are considered to be good hopping points by actors to access various industries.

The third industry being targeted in 2020 is Energy industry and TeamT5 had observed at least attacks from 5 adversary groups. It could be a sign of our adversaries' ambitions to control our critical industries because they will be top priorities of sabotages in wartime. Education or think tanks have been long ranked as the most attacked victims because they tend to involve in classified research projects hosted by governments or political decision makings. There were several targeted attacks against companies in semiconductor industries. It makes sense since Semiconductor industry is listed as a priority to be fostered by Chinese authority in their thirteen and fourteen Five-Year projects. Cyber espionage was also adopted as a mean to improve their techniques. Healthcare and transportation are also two industries that got coveted by APT actors. As we mentioned in the previous paragraph, COVID-19 could be an incentive for APT actors to attack Healthcare industries. Lastly, we would like to raise a phenomenon TeamT5 observed: There was an adversary group which we called GouShe (a.k.a TroppicTropper, Keyboy) focus on infiltrating Transportation related entities in Taiwan. More than 70% of transportation related cases we observed were from this specific group.

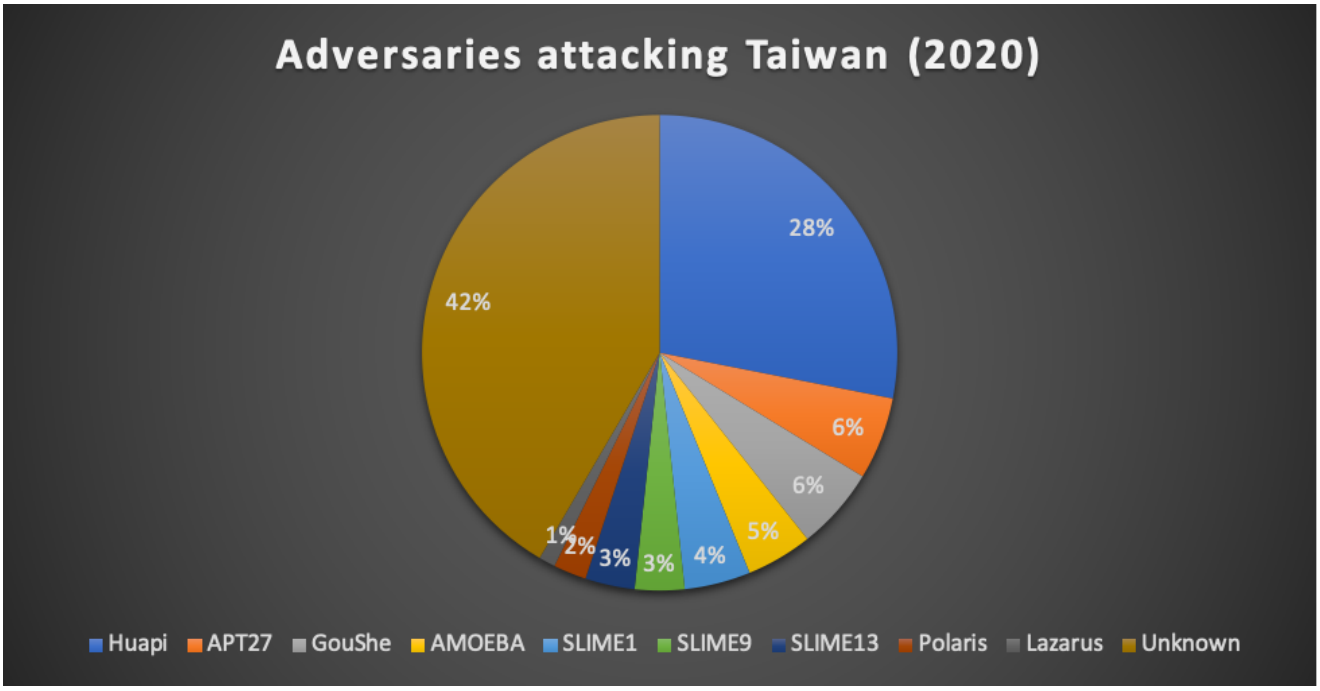


2020 APT target industries distribution

TeamT5 has tracked activities from at least 9 APT groups and 8 of them are from China. HUAPI (a.k.a BlackTech/PLEAD) was definitely the most ambitious group in Taiwan. Their attacks counts around 30% of incidents we analyzed and the targeting scope includes almost all the industries we listed. The supply chain attacks we mentioned in previous paragraphs were also conducted by them. APT27 (a.k.a EmissaryPanda, IronTiger, LuckyMouse, BronzeUnion), GouShe and AMOEBA (a.k.a APT41, Barium, Winnti) are groups that are quite active in 2020. APT27 was mostly attacking government, healthcare, and financial entities. GouShe showed a peculiar interest in transportation related entities while their footprints are also observed in energy and government entities. TeamT5 has tracked this group for many years. Our research shows that the actors might bear some responsibility from their higher commands to monitor some critical infrastructure facilities in Taiwan and take control of them in case of emergency status.

AMOEBA attacked energy companies, semiconductor companies, educational institutes, and IT companies. Their primary goal appears to be more for intellectual property or secret theft. But the possibilities exist that the actor might further leverage their achievement, like what they did in the ransom-attack in May. SLIME1, SLIME9 and SLIME13 are temporary code names for three Chinese APT campaigns against Taiwan that have lasted for a few years. Their activities still continued in 2020. Polaris (a.k.a MustangPanda) is another Chinese APT group that attacked almost all neighboring countries of China. We intercepted several of their spear phishing emails against government and research institutes in early stage of COVID-

19 and we surmise they were gathering for information related to pandemic. One last interesting discovery: we discovered some Linux based malware used by Lazarus, a notorious North Korean APT group, circulated in Taiwan but we are unable to obtain the victim identity information. Although Taiwan is not a primary target of North Korean APT. But the Lazarus actors are believed to bear financial supporting responsibilities for their government agencies. For example, Lazarus is believed to be the culprit behind a Taiwanese bank SWIFT heist in 2017 [4]. The sample we uncovered might suggest their activities still exist in Taiwan.



Adversaries attacking Taiwan in 2020

Conclusion

The purpose of this article is to provide a high-level overview of APT threat landscape of Taiwan in 2020, since TeamT5 believes knowing your enemy is the first step of effective defense. TeamT5 research shows that APT attacks keep evolving to become very complex and impossible for a security product to defend. TeamT5 has a cyber threat intelligence (CTI) centered solution, ThreatVision, and we rely on a dedicated team of security experts to keep us steps ahead of threat actors. Feel free to contact TeamT5 in case you want to know more about our products, solutions or discuss about threats you are facing.

> Contact us:

Reference

[1] https://www.ithome.com.tw/news/139331
[2] https://www.slideshare.net/codeblue_jp/cb19-resistance-is-futilethe-undefendable-supplychain-attack-by-sungting-tsai-linda-kuo
[3] https://www.youtube.com/watch?v=1KXb-sf_wos
[4] https://www.reuters.com/article/us-cyber-heist-north-korea-taiwan-idUSKBN1CL2VO
Share: