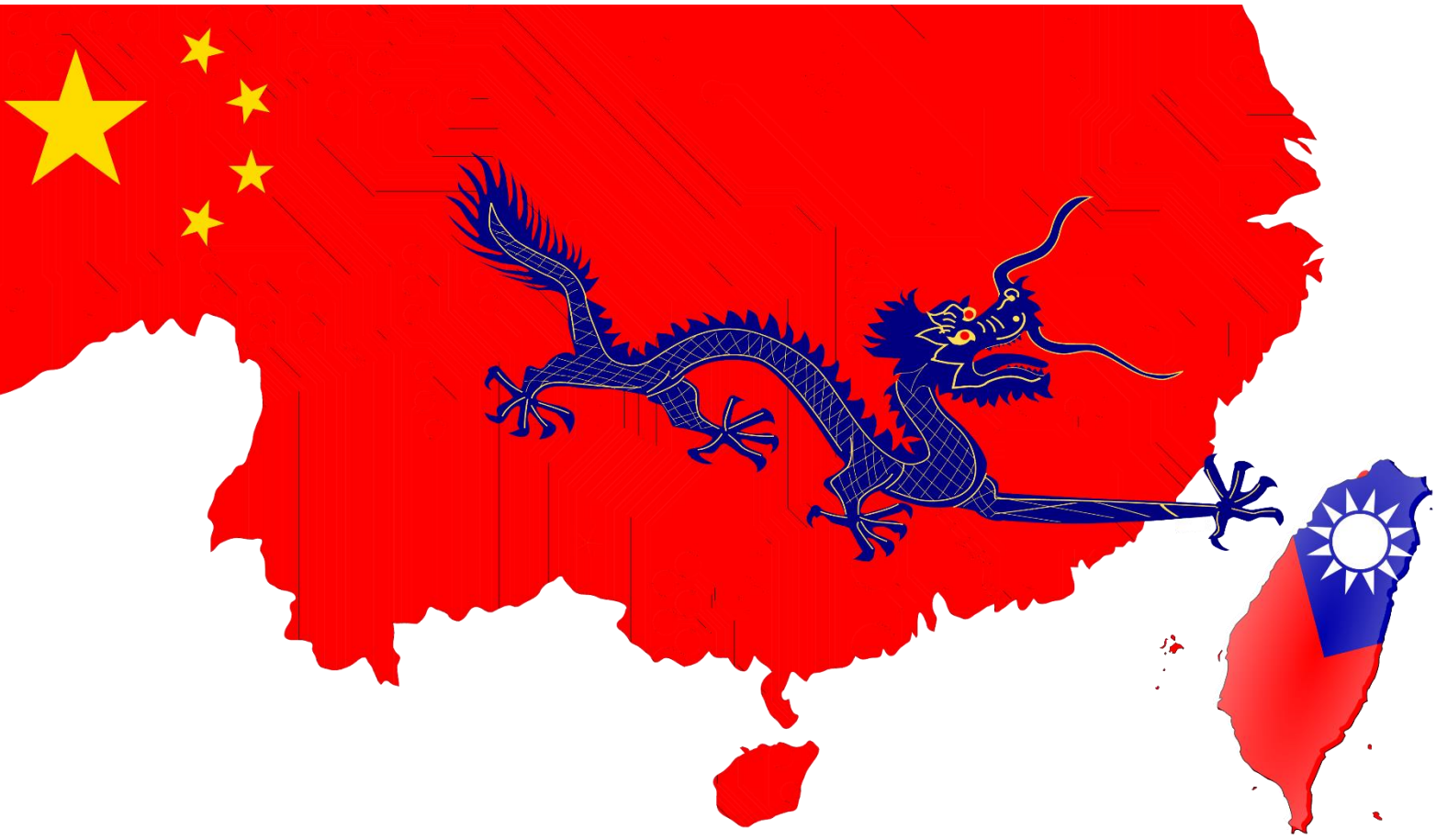
Cyberwatch Finland



WEEKLY REVIEW

WEEK 3/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. China's influence on Taiwan's presidential elections demonstrates China's ability and interest in influencing abroad. Relations between China and Taiwan are also important from the point of view of global chip production.

2. Successful law enforcement operations have prompted two major ransomware groups to signal unprecedented cooperation intentions on the dark web.

3. Organizations should be aware of the value and effectiveness of their own social media accounts. They can be an attractive target for cybercriminals.

1. GLOBAL SIGNIFICANCE OF THE TAIWANESE PRESIDENTIAL ELECTIONS

The presidential elections in Taiwan last weekend received a great deal of attention in the international media. In the end, the winner was Lai Ching-te, candidate of the Democratic Progressive Party (DPP). As expected, the victory came with more than 40% of the vote and the DPP retained its position as the country's leading party. The main theme of the presidential election was Taiwan's relationship with China, and its definition also served as a key dividing line between the candidates. In certain circles, Lai's victory was even celebrated as a victory for Taiwan´s sovereignty and democracy, as the DPP actively promotes Taiwan´s independence. For historical reasons, Taiwan's international status is unclear and controversial. The election result was not to China's liking, as the country regards Taiwan as its rebellious province and plans to reunite it to mainland China. The victory of one candidate who breaks away from the so called "one-China" -model may be reflected in heightened tensions and further escalations in the future.

Taiwan's presidential election is also significant from the perspective of cyber security and cyber influencing. Before the election, cybersecurity firm Mandiant warned of cyberattacks and cyber espionage against Taiwan's government and critical infrastructure. Another cybersecurity firm, Cloudflare, reported a 3370% increase in cyberattacks in the pre-election period, in the fourth quarter of 2023, compared to the same period last year. In addition to cyberattacks, China used a wide range of other hybrid means during the elections. For example, disinformation was widely disseminated on social media, in addition to which there were reports of spy balloons sailing over Taiwan. While Taiwan occupies a special place in the policies and priorities of the Chinese state, in a broader context it is not just about China's cyber threat to Taiwan. China's actions imply more broadly the toolbox and ability of both China and other authoritarian states to interfere in the internal affairs of other states. In addition to Taiwan, China's cyber influence for political reasons has targeted Australia, with which the country has been in a trade war in recent years. The most significant political event in 2024 will be the US presidential election, and it is not excluded that China – along with Russia – will also seek to influence them. This can be seen, for example, in information influencing directed at a significant Chinese minority in the United States or in an increase in the number of cyberattacks, similar to the elections in Taiwan. China has both the motive and the means to exert hostile influence on a global scale.

More important than election interference, however, is probably the future development of relations between China and Taiwan and their possible straining as a result of the elections. From time to time, China's stated goal of uniting Taiwan as part of the country by the centenary of the Communist Party's rule by 2049 comes up in the media. According to China, reunification could take place by peaceful means, but military means have not been ruled out. Any military intervention and escalation would be of great global significance for microchip production, as according to The Economist, more than 60% of microchips and 90% of all advanced microchips are produced in Taiwan. Microchips are used in all modern technologies, from household appliances to mobile networks and cars. If there were supply problems due to the threat to Taiwan, global production chains would be paralysed in the worst case. In addition, if all chip production were to end up in China's hands, this would have a significant impact on the reliability of components. China has long been suspected of using the technology and applications it manufactures for espionage purposes. If the majority of the world's microchip production would end up in the hands of China, it would provide the country not only with significant economic benefits but also with new means of obtaining information. Western countries have become aware of the situation and have tried to start their own chip production. For its part, the United States has sought to block chip technology supplies to China. This is one of the key elements in the great power struggle between the two countries.

Although the elections are unlikely to immediately escalate the situation in one direction or another, they are an important pointer in the direction in which Taiwan's path will lead in the near future. The choice of DPP candidate is a step in an unpredictable direction. The representative of Taiwan's other major party, the Kuomintang (KMT), was clearly more conciliatory and cooperative towards China. The events in Taiwan prove China's ability and willingness to influence other societies through various cyber and hybrid means, but the situation must be monitored globally, especially because of the threats related to microchip production.

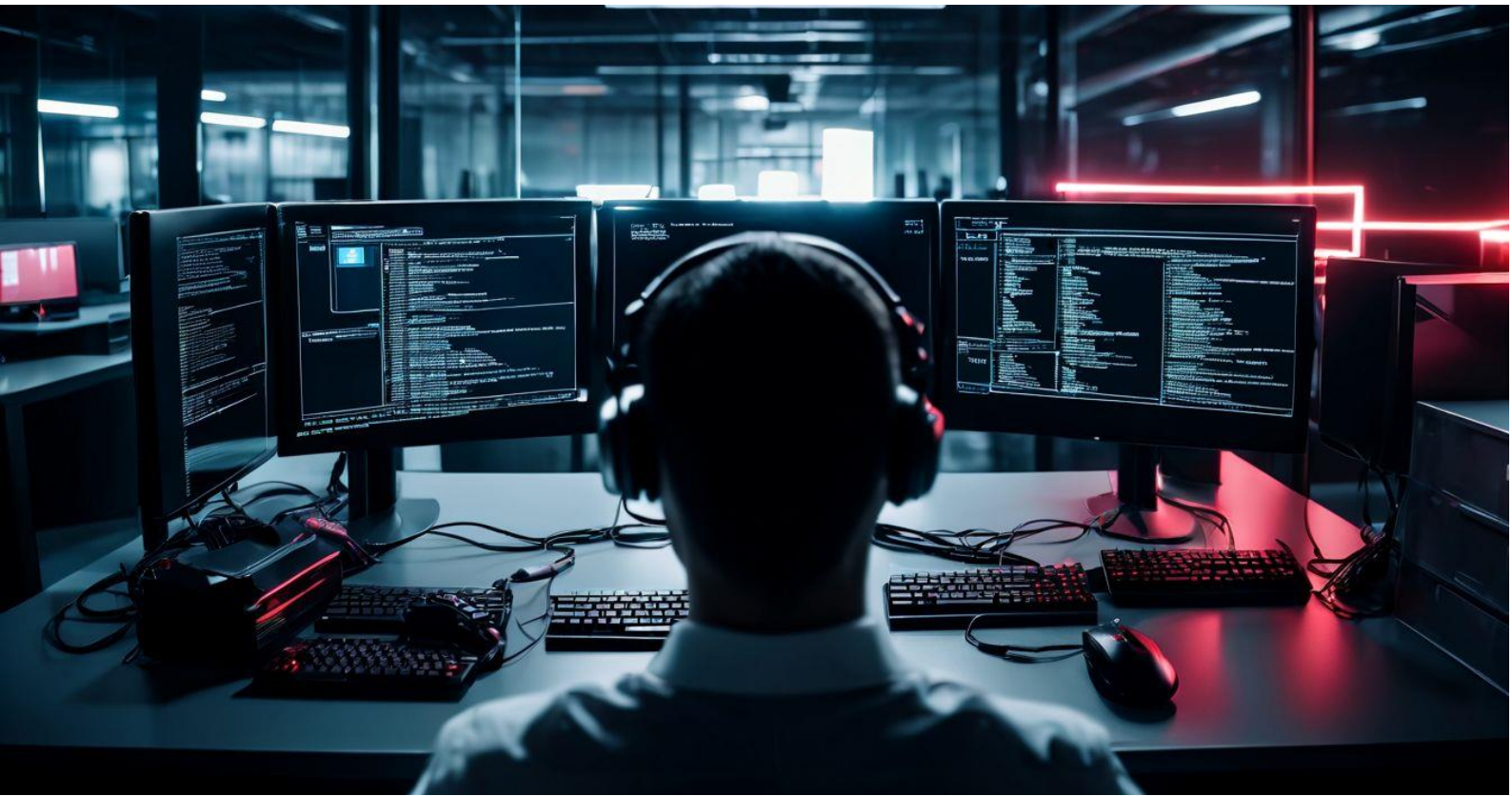
2. RANSOMWARE ACTORS SEEK COOPERATION

The basic assumption is that criminals are always one step ahead of law enforcement. This also applies to cybercrime. The activities of the authorities have often been limited to investigating crimes that have already occurred and preparing for future attacks. However, the authorities have tried to take a more active approach and have also stepped-up operations that have a direct impact on the activities or cybercriminals. The United States, in particular, has developed proactive influencing towards threat actors. This is a broad change in the strategic concept, which aims to respond to cyber threats with active and aggressive operations instead of passive defence and investigation of crimes that have occurred. This targets both state adversaries and identified cybercriminal groups. A good example of an operation that had a significant impact on criminals' activities is the attack by US authorities in December against the Russian cybercrime group BlackCat (also known as ALPHV and Noberus).

BlackCat is a major and well-known group of hackers whose BlackCat ransomware has for years been one of the most widely used ransomware in the world. The group rarely carries out attacks by themselves, but rather acts as a kind of service provider, producing the tool (i.e. malware) and offering it to other threat actors in exchange for commissions. The attack on its servers provided the FBI with information about the groups exploiting the malware and their ongoing operations. Of particular significance was the fact that the authorities also obtained decryption keys, which enabled hundreds of organisations that had already fallen victim to the group to recover their encrypted files. In addition, some of the dark web sites maintained by BlackCat were down for several days, and anyone trying to access them was greeted by a message from the FBI announcing the successful operation. This, too, had a clear effect, because although a few days later the group regained control of the site and published a message downplaying the seriousness of the attack, the damage had already been done and the group's credibility had been damaged. Since BlackCat operates specifically as a service provider, credibility is an important part of operations. In addition, knowing that authorities are in possession of decryption keys will certainly influence the decision of many criminal groups to use competing ransomware instead of BlackCat. However, getting hold of the keys does not mean that the malware in question is unusable. Same decryption keys do not work on all cases, as they are specific to both version of the malware and the way its implemented. Therefor a key usually only works for a single victim.

The FBI operation had clear and immediate effects on the group's activities, but a few weeks after the attack took place, more surprising consequences emerged. During discussions about the attack on various dark web forums, BlackCat gained sympathy from other criminals. Particularly surprising were the messages from a representative of the LockBit group, which is considered as its worst competitor. The damage suffered by a competitor is usually in beneficial to others operating on the same field, but the account linked to LockBit expressed sympathy for BlackCat and clear concern about the development of government operations. The exchange of messages between the groups expressed the need to develop cooperation between criminal gangs. They even talked about forming a 'cyber cartel' in order to be stronger together, especially against operations carried out by the US authorities. Calling for this kind of cooperation between two groups competing for the same customers is unheard of. Although the mere exchange of messages on the forum does not necessarily indicate real intentions to cooperate, it is still a clear consequence of the development of law enforcement operations. However, if the groups actually decide to join forces, this could have a significant impact on the threat posed by criminal groups. For example, if groups develop mutual information sharing, it increases the likelihood that a victim of one group will also experience another attack, as information about protection and response flows from one hacker group to another. Of course, this is already happening today, and in particular information about which organizations are willing to pay the ransom is shared a lot in dark web conversations. In the past, however, groups have been reluctant to share information on, for example, how they have penetrated the victim's networks or avoided retaliation, as this is exactly where the aim has been to be better than the competition.

The real aim of the exchange of messages is perhaps to send some kind of message rather than to initiate actual cooperation. If cooperation was actually prepared, the agreement would certainly take place through encrypted bilateral communication and not in an open forum that any user of the platform can read. The purpose of open communication is likely to attract attention and highlight the perception of authorities as a threat to operations, regardless of the group targeted by their operations. Even if no concrete cooperation is emerging, it is important to express a public common line. It is good to keep in mind that both of these groups are known to be Russian. Although both are thought to be driven almost exclusively by economic motivation, geopolitics still plays a clear role in the operation of these groups as well. Most of the attacks are directed at Western countries, especially the United States, so it is only natural that the authorities in this particular country should be seen as a common evil against which rivalries can be forgotten. In any case, it is clear that more active and aggressive cyber defense works and can influence not only state adversaries, but also cybercriminals. Although there are challenges and only a few authorities have the capacity for large-scale operations, the development of these operations may change the situation between cybercriminals and law enforcement in the future.



3.ORGANIZATIONS' SOCIAL MEDIA ACCOUNTS ARE VALUABLE

The value of social media accounts can rise to unpredictable values. In the first week of January, Google's security company Mandiant's X account was hacked and used to spread a cryptocurrency scam. Likewise last week, the United States Securities and Exchange Commission SEC's account was briefly hijacked, and misinformation was published. This affected, among other things, the current bitcoin exchange rate. Cyber scams and other cyber operations carried out through social media accounts can be highly effective. Other one of the recent victims, Mandiant, is a credible and trusted security actor, while the SEC is one of the most important institutions in the financial world.

The value of social media accounts consists of, for example, the information value achieved through them and the possibility to disseminate the desired information. The social media accounts of reliable and significant organisations serve as primary news sources for organisations and individual citizens, and the information they convey may not be questioned. Misinformation published in hijacked accounts can be used for financial gain, as was likely the case with both the SEC and Mandiant. Attacks can be profitable. For example, according to Mandiant, the attack campaign has generated at least $900,000 in total for the scammers. In addition to financial gain, threat actors can also seek other effects. State threat actors may be interested in spreading disinformation or sabotage. If, for example, in the face of a national crisis, the social media accounts of the country's most popular news channel were to fall into the wrong hands, it could have significant consequences for society as a whole. In the case of individual companies, if social media accounts end up in the wrong hands, depending on the level of information security of the organization and the content of the message, it could cause many kinds of reputational damage as well as emergence and spread of false rumours and perceptions.

An organization's social media credentials can end up in the wrong hands in many different ways. Account credentials often end up with hackers, for example through phishing or social engineering. Various dictionary attacks or password reuse can also expose you to account hijacking. The email address and password used in connection with an account may be leaked, for example, as a result of a data breach affecting another service, if the same email address and password are used in several different places. The security of log-in details is further weakened if they are accessed by several employees of the organization. It would also be important to take advantage of the login options recommended by experts. In Mandiant's case, the reason for the successful hack appears to be that Mandiant's X account was had not implemented two-factor authentication (2FA). This allowed the attacker to launch a brute force attack that allowed the password to be cracked. Mandiant itself claims that 2FA was not in use "due to personnel changes and X's changed 2FA policies". In reality, it is probably due to laziness or carelessness.

Attention should be paid to the security of social media accounts. Although for example hacking an X account does not in itself expose the organization's systems to attack, the value of this asset should also be recognized. Social media accounts are a visible part of an organization, and it is a clear reputational damage if they are successfully hijacked and thereby used to spread false or harmful information. The security of social media accounts is not the target that is most invested in protective means, but it is still attractive from the point of view of attackers. Mandiant's operations are based specifically on information security, so the incident obviously caused it serious reputational damage. At the same time, the incident reminds us how important good information security practices are also in services whose breach would not directly harm one's own operations. Social media accounts make up a significant part of an organization's outwardly visible brand and reputation, so protecting it is also a top priority.

REFERENCES

1. Global Significance of the Taiwanese Presidential Elections

Computer and information security at nuclear facilities | IAEA
Sellafield nuclear site hacked by groups linked to Russia and China | Energy industry | The Guardian
UK nuclear waste firm thwarts cyberattack | SC Media (scmagazine.com)
Sellafield's longest serving director to step down - GOV.UK (www.gov.uk)
Stuxnet explained: The first known cyberweapon | CSO Online
What to do about the Zaporizhzhia nuclear power plant | Brookings

2. Ransomware Actors Seeking Cooperation

https://thecyberexpress.com/lockbit-and-blackcat-join-to-form-cyber-cartel/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-22nd-2023-blackcat-hacked/
https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
https://www.bleepingcomputer.com/news/security/fbi-disrupts-blackcat-ransomware-operation-creates-decryption-tool/
https://www.itworldcanada.com/article/alphv-blackcat-allegedly-calls-for-ransomware-gang-cartel-to-stand-up-to-police/555578
https://twitter.com/vxunderground/status/1737871230772945321?t=2QsgjQa3h64VHBlTf4rbNQ&s=09

3. Organizations' Social Media Accounts are Valuable

https://thehackernews.com/2024/01/mandiants-x-account-was-hacked-using.html
https://www.securityweek.com/mandiant-details-crypto-theft-campaign-that-hacked-its-x-account-via-brute-force-attack/
https://www.theguardian.com/technology/2024/jan/09/sec-twitter-account-hacked-bitcoin-etf-not-approved

Pictures: Pixabay, im2go