SECTRA NEWSLETTER – MAY 2024

Monthly Review

Cybersecurity news from around the world

ARTICLE

Concerns on the cybersecurity of power grids

Read article →

SECTRA

General cybersecurity news

1 The rise of biometric identification and the emerging risks

Biometric identification, the use of physical characteristics for identification, is slowly spreading to different sectors of society, much like artificial intelligence. The most common use of biometrics is logging in to mobile devices, which is more convenient than passwords. However, as the technology becomes more common, new risks arise. There is debate around the use of biometrics for mass surveillance, especially when combined with artificial intelligence. France has been developing a system that combines AI and camera surveillance for the 2024 Summer Olympics, which has raised concerns about privacy and data security. While the technology will not be used for biometric identification, critics argue that it could easily be modified for such purposes. The EU has laws in place to restrict facial recognition, but there are fewer controls outside the EU. China and Russia, for example, use biometric surveillance extensively. A recent data breach at an Australian company that produces facial recognition systems highlighted the risks associated with the widespread collection of biometric data.

2 Intensified measures against commercial spyware continues

The United States has imposed visa bans on individuals involved in cyber spyware development, reinforcing the message that these activities are unacceptable. The use of commercial spyware remains widespread outside the EU and the US. There is a debate about the boundaries between legal business and crime in this industry. While efforts are being made to restrict commercial spyware, many countries are also developing and using similar applications. The outcome of this competition is uncertain, but stricter measures against commercial operators are expected.

3 Traces of Russian hacktivism lead to the Kremlin

Hacktivist groups have been active in the cyber operations during the war in Ukraine, particularly Russian hacktivism targeting the West. These attacks are low-level cyber operations often exaggerated by hacktivist groups. While hacktivism may not have lasting effects such as state cyber activities, it can benefit the state by showing public support and diverting resources from the target. There are speculations of collaborations between Russian hacktivist groups and intelligence services, with evidence suggesting some groups are associated with the Russian military intelligence GRU. During the spring, Google's security company Mandiant linked the hacktivist group CyberArmyofRussia_Reborn to GRU and its subordinate Sandworm (APT 44) threat actor. Supporting hacktivist groups helps intelligence services avoid responsibility and outsourcing activities. This focus on low-level hacktivism can also aid state-sponsored advanced persistent threat (APT) operations.

ARTICLE

The acceleration of cyber espionage

In recent weeks, several cases of cyber espionage and intelligence involving Germany have come to day light. In early May, Germany publicly accused Russia of its years-long cyber operations against German targets.

The operator has been the military intelligence service GRU and its subordinate APT28 group. This group, also known as Fancy Bear and Strontium, is one of the most active high-threat actors identified for Russia, but by no means the only one. Nor is it the only Russian group to have exerted influence on Germany.

At the end of April, Google's security company Mandiant reported on a large-scale campaign it had identified, in which APT29, under Russia's foreign intelligence agency SVR, had targeted German politicians and parties for its espionage and influence operations. In addition, earlier in April, Germany announced that it had detained two dual citizenship individuals with serious suspicions of plotting sabotage attacks on German soil with the aim of undermining support for Ukraine. The common denominator seems to be Russia. In connection with almost all the news, there has been talk about how the increased threat of cyber influencing and espionage does not only concern Germany, but the same activities are certainly taking place all over Europe. Germany is, of course, in a unique position as one of the EU's powerhouses and an industrially significant player, but it would be naive to think that similar action would not also be targeted at smaller countries. →

Russia is also not the only one engaged in cyber espionage. There have been reports across Europe of increased activity attributed to Chinese state threat actors.

Several reasons for increased activity

Why, then, does cyber influencing and espionage seem to have increased in Europe? There can be many reasons for this, and in reality, the cases that end up in the public domain are only the tip of the iceberg of all state action. The most natural reason for the increased activity is that the parties carrying it out have increased the resources allocated to the activities and the intelligence objectives have been expanded. This was brought up, for example, in the Mandiant's analysis of the APT29 campaign, based on its exceptional selection of targets. The increased need for information or influencing may be related to, for example, the European elections waiting around the corner. Another reason why the amount of cyber intelligence has increased may be that the effectiveness of both China's and Russia's other intelligence tools in Europe has declined. The heightened state of preparedness due to the recent unrest has certainly affected the implementation of human intelligence gathering of the countries, for example. In addition, when diplomatic relations, especially with Russia, are poor, there may be interruptions in the flow of espionage information, which cyber espionage aims to remedy.

> *“Russia is also not the only one engaged in cyber espionage.”*

Cyber influencing should not be seen as a separate entity in state influencing, but as one part of it among others. Cyber intelligence is used around the world to both support and, if necessary, replace the activities of other intelligence branches. →

The third reason why more cases are making headlines is simply that more and more of these operations are now being revealed, even if the number itself has not increased. This is likely due to the increased level of preparedness related to cyber influencing, but also to the fact that, as a result of the change in the political climate, states now have the courage to more directly accuse states they consider hostile of influencing themselves.

Cyber espionage may evolve to sabotoge

It is likely that all three of these reasons together will contribute to why cyber espionage cases are now becoming increasingly public, both across Europe and in Germany. There are certainly other factors behind this. In the cyber world, intelligence and espionage can serve as early warning signs or initial steps that often pave the way for various sabotage attacks. →

In the cyber environment, a reconnaissance operation can be modified into a destructive attack, as intelligence has often been based on a successful and undetected break-in into the target's information systems. Once enough information has been obtained, detection seems likely, or the time otherwise becomes appropriate, the hiding can be stopped and operations aimed at paralyzing or disrupting be carried out. Russia's toolkit includes, for example, data destruction wiper attacks, which were widely used in the early stages of the war in Ukraine, where potentially irreversible data is destroyed from target systems to prevent them from functioning.

The increased level of cyber threats must be considered throughout EU countries, both in public administration and in the business world. Although the focus areas of influencing are political decision-making actors and critical infrastructure providers, it should be borne in mind that due to the complexity of impact chains and the length of subcontracting chains, virtually any actor can act either as a means of influencing these targets or suffer indirectly from operations targeting them. ■

ARTICLE

Concerns on the cybersecurity of power grids

Cyber risks to the electricity grid and other critical infrastructure are constantly being discussed. According to information security experts and international authorities, the threat level is rising significantly, but on the other hand, the preparedness and protection of organizations is still too weak in many respects.

In the United States, for example, concerns have been raised about the cyber security of the country's expanding power grid. According to the North American Electric Reliability Corporation (NERC), which is responsible for the reliability of the country's power grid, geopolitical risks in particular, such as the wars in Ukraine and, for example, Gaza, have increased the cyber threat to the country's power grids.

A successful cyberattack on power grids could have immediate effects on critical functions in society. Although hospitals, for example, often have backup systems in place, it goes without saying that prolonged power outages have serious effects. Thus, the electricity grid is an attractive target especially for state-sponsored cyber sabotage, which can be used as one of the means of hybrid influencing. →

This has also been reflected in the war in Ukraine, where the electricity grid has been one of Russia's main targets since the beginning of the conflict in 2014. The 2015 cyberattack succeeded in crippling the electricity supply of hundreds of thousands of consumers. In addition to concrete physical effects, attacks on the power grid and critical infrastructure always have an information-psychological effect. Attacks on key functions of society have a fundamental impact on the sense of security of the inhabitants of the target society.

> *"Attacks on key functions of society have a fundamental impact on the sense of security of the inhabitants of the target society."*

Other actors, such as financially motivated cybercriminals, have also recently targeted critical infrastructure actors, such as hospitals. The aim of this is to maximize financial gain, as criminals hope that crippling critical functions will lead higher probability of ransom payments. When the threat comes from both state actors and financially motivated cybercriminals, it is probably only a matter of time before the wider problem of the power grid caused by a cyberattack arises in Western countries.

Around the world, attacks on critical infrastructure in general and the power grid in particular are common. So far, however, protection against them has been commendably good. In Finland, at best, dozens of cyberattacks have been reported to target electricity networks every day. Statistically, however, it is the United States that takes the most hits. A significant part of the attacks is carried out by Russia, which continues to exert continuous physical and cyber influence on Ukraine's power grids. →

More attention has been paid to cyber risks to electricity suppliers. In addition to warnings from authorities around the world about the threat, the EU, for example, is stepping up controls on electricity suppliers. In March, the European Commission adopted a law that both increases the level at which electricity grids must be protected and increases obligations to carry out an assessment of the level of cyber security. Suppliers are required to implement and report on the state of their own cyber security every three years, and it is hoped that repeated reviews will force them to maintain active and evolving protection instead of meeting the minimum requirements only once. The act is coming in addition to the NIS2 directive, which will make cyber security more binding, so at least in the EU, a lot of effort is being put into combating this threat.

However, the best way to implement protection would always be to build it into the systems already at the development stage. Security by design thinking should be remembered both when expanding networks and, for example, in increasing the role of new forms of energy. ■

Key takeaways

1. Biometric identification is expanding, but it raises surveillance and data breach concerns, as seen in France and Australia.

2. US visa bans on spyware developers have sparked debate and stricter measures due to widespread use of commercial spyware.

3. Hacktivist groups support states through cyber operations and collaborations with intelligence services, aiding APT operations.

4. Germany and Europe face increasing cyber espionage and influencing activities, primarily by Russia and China, targeting political decision-making actors and critical infrastructure providers.

5. Power grid cybersecurity concerns are rising due to weak protection and potential attacks by state-sponsored actors and cybercriminals.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

SECTRA