Cyberwatch Finland

WEEKLY REVIEW

WEEK 10/2024

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

Cyberwatch Finland

KEY TAKEAWAYS

1. Russia's anti-war opposition operates online. So far, the activities have focused mostly on information influencing, although there could be also other options.

2. New information has emerged on China's cyber activities. The country is making greater use of outsourcing cyber espionage to private actors than expected.

3. There are plenty of statistics available on cybersecurity-related phenomena. However, their reliability is undermined by questions of interpretation and divergent aggregation methods.

1. ONLINE ENVIRONMENT AS A BACKBONE FOR RUSSIAN ANTI-WAR OPPOSITION?

March is politically interesting in Russia. The funerals of Aleksey Navalny, the most prominent opposition politician, took place on the first day of the month, and presidential elections are just around the corner from 15th to 17th of March. The outcome of the “elections” is already clear in advance, with opposition actors being either in prison or in exile. At the same time, legislation has sought to curb the information space. An example of this is the vague laws on the so-called "fakes" that extend to social media and can result in prison sentences of up to years. Despite this, social media and the online environment are already important channels for the anti-war opposition to exert influence and oppose the regime when other means are scarce. Could the online dimension or cyber activity become even more important for its activities?

Russian opposition activities online can be roughly divided into two categories: information influencing and cyber sabotage and related cyber intelligence. The former is considerably more common than the latter. The most well-known Russian opposition politicians, including Maria Pevchikh, Kira Yarmysh and Leonid Volkov from the younger generation, skillfully use social media to produce and share content. The most significant platform is YouTube, which has not yet been banned in Russia. YouTube also served as a platform for the late Alexei Navalny, who became known especially for his videos exposing the corruption of those in power. Russian opposition media and newspapers also live mainly online. These include online magazines Meduza and Novaya Gazeta Europa, access to both of which require a VPN connection in Russia as they are blocked in the country.

The Free Russian Foundation (FRF), based in the United States, is also active in the field of information influencing, as it has coordinated efforts to respond to Russian propaganda and social media trolls with the help of the so-called Elf Legion. This kind of work is carried out by 100 activists. They are active on more than 900 pro-Russian social media pages and leave up to 160,000 comments criticizing the government monthly.

The second category, cyber sabotage, meaning actual cyberattacks or data leaks, is much less common and does not appear to be coordinated. However, individual examples can be found. This was seen, for example, in the "Vulkan files" leak in the first weeks of the war in Ukraine, where a single NTC Vulkan employee leaked the organization's data, thus revealing the company's connection to Russian security services as well as information about Russian cyber operations. We have also seen cyber resistance. For example, a Russian who carried out DDoS attacks on behalf of Ukraine was sentenced to three years in prison in Russia in May 2023.

In the light of the examples described above, it is easy to judge the importance of the online environment for the opposition as small and the opposition's influence as non-existent. The Russian opposition has indeed received criticism, for example, for focusing on making YouTube videos and vlogging from abroad instead of concrete action. Although the online dimension and its various platforms offer the opposition a way to keep in touch, unite and coordinate their activities, information influence alone is unlikely to achieve the outcome desired by many, i.e. an end to the war in Ukraine and a change of power in Russia. However, there is potential for better. In Russia, some critical functions of society are also connected online, as in the west. This would open up the possibility, for example, for insiders opposed to war to cause harm or leak vulnerabilities to the party carrying out the attack later. Other Russia-specific expertise that Russians opposing the war possess could also help in opposition activities. On the other hand, the current location of opposition actors in Western countries could allow the support of Western advisers in both planning and conducting cyber operations opposing the current regime. As physical resistance in Russia is practically impossible, the cyber dimension could become a means for the opposition to implement more active resistance.

2. DATA LEAK THAT GAVE A NEW PERSPECTIVE ON CHINESE CYBER INFLUENCING

A massive data leak suffered by Chinese cybersecurity company I-Soon in February offers a rare glimpse into the Chinese cyber influencing field. Although neither the leaker nor the authenticity of the leaked information has yet been verified, the content of the exposed material is generally considered to be authentic. The material shows that the Chinese government is calling for bids in cyber espionage and hacker assignments with private service providers. The leaked information had been published on the GitHub online software repository, where one can, among other things, share files without cost for access by anyone and everyone. According to the leak, I-Soon operates as a private cyber espionage contractor for Chinese security authorities. The leak reveals that I-Soon has developed its own malware and participated in competitive bidding for state-sponsored cyber espionage operations. The company's victims are a diverse group of organisations, including foreign governments, academia, telecommunications, healthcare and air transport operators in different countries.

The current leak changes the perception of Chinese cyber espionage activities. In the past, China has been thought to carry out mainly state-led cyber espionage using APT groups. However, competitive bidding of cyber operations with private service providers shows that China's cyber espionage machinery has been decentralised. It is not only high-level APT actors from China that strike abroad, but private cyber companies can also be behind the attacks. In this way, the Chinese security authorities are able to tailor operations in terms of cost, quality and quantity. In practice, competitive tendering works in such a way that a state security authority submits an invitation to tender, in which private service providers can submit their own tender for the execution of the assignment.

There is also competition between service providers and even disputes that go to court. For example, a company called Chengdu 404 sued the aforementioned I-Soon in a contract dispute related to software development. Chengdu 404 has previously been linked to the APT41 threat actor, which in turn is linked to many malicious activities on foreign targets. It should be considered whether these private companies participating in competitive tendering, including I-Soon, are just front companies for various APT operators.

In the future, China's cyber environment can be examined from a new perspective, as we know that some of the Chinese threat actors are private companies thanks to the current data leak. This may also have an impact on the outcome of cyber operations. Future operations may be even more efficient and destructive as operators compete "in the market" with each other. It is also possible that if the selection criteria of the client of the assignments, i.e. the Chinese state security authorities, change, the selection criteria for cyber operations may also focus on price instead of quality. This, in turn, would potentially have the opposite effect on effectiveness. In this sense, when looking at your organization's ties to China, it is worth taking this change into account.

3. CHALLENGES OF CYBERSECURITY STATISTICS

When reading cyber security publications, one often comes across statistics. They can indicate an increase in a particular type of threat, trends in crime or other measurable things. Statistics are useful because they help one to quickly understand how a phenomenon has developed or how significant it is. However, there are always significant challenges associated with the use of statistics – as well as in cybersecurity. Statistics describing the same phenomena, collected from different sources and compiled by different actors may differ significantly from each other or, at worst, contradict each other. For example, if you look at the statistics compiled for the second half of 2023 on the prevalence of ransomware, depending on the source, the situation may look very different. Comparing the publications of information security actors paints a contradictory picture. For example, according to cloud and cybersecurity company Sangor, the number of ransomware attacks increased by 95% in 2023 compared to the previous year. According to cybersecurity solutions provider CheckPoint, the figure would be closer to 33%, according to threat intelligence firm CyberInt 56%, and security software and hardware company Sophos said the frequency of attacks was the same as the previous year. Meanwhile, online magazine BleepingComputer writes that in 2023, earnings from ransomware attacks decreased as victims increasingly refused to pay. Rival Wired, however, says 2023 was the best year in extortionists' history, with ransoms paid surpassing the billion-dollar mark. What, then, should be understood from this mess, and why are the statistics so contradictory?

The simplest reason for the discrepancy in the statistics of different information security actors, in particular, is the different sources used in them and different ways of measuring the phenomenon. Sangor bases its estimates on the figures of insurance company Corvus, CheckPoint has produced the data with its own artificial intelligence application, Cyberint does not specify its sources, and Sophos says the figure is based on the responses to its customer survey. Similarly, online journals have used publications by various actors as sources. BleepingComputer's figure is based on statistics compiled by IT company Coveware's Incident Response team, while Wired's figure comes from data from cryptocurrency analyst Chainalysis on how much cryptocurrency traffic can be linked to ransomware activity. Statistics are therefore collected and compiled in significantly different ways. Naturally, these pieces of data are therefore not comparable with each other. It should also be noted that for almost all of the actors mentioned, the company who provides the statistics is a company selling cyber security services, whose interest may be to present the situation as threatening and at the same time attach a short description of its own services to mitigate the threat at the end of the report. Of course, reliable statistics compiled without marketing purposes are available. For example, many authorities produce comprehensive descriptions of a specific threat field. On the other hand, their use is often challenged by either industry or country specificity, and they are not intended to describe the entire threat field. In addition to all this, statistics related to cyber security are still challenged by the number of related hidden crimes or unreported cases. A significant proportion of cyber events are always left in the dark. For one reason or another, the party that has experienced an attack does not always want to publicly announce the event.

Therefore, when reading cyber security statistics, one should be careful about by whom and how the data has been compiled and published, and how relevant the results are to your own organisation. Objectively compiled and honestly presented statistics can be useful in mapping one's own threat picture, and by comparing statistics made by different actors on the same issue, one can get a picture of a broader trend, even if the results themselves are not comparable. Therefore, when examining statistics, it is necessary to be able to look beyond individual figures. It should also be borne in mind that statistics supporting one's own claim are almost always available. As for the ransomware used as an example, it should be clear that all actors believe that the threat is indeed increasing, although the rate of growth varies depending on the region or industry. There may be many opinions about the profitability of ransomware, but perhaps more indicative of the economic benefit than statistics is the fact that new actors with dreams of fast profits are constantly emerging on the "market", while hacker groups that have been engaged in extortion for a long time are constantly developing their own operations.

REFERENCES

1. Online environment as a backbone for Russian anti-war opposition?

https://aif.ru/society/rostovskogo_it-specialista_osudili_na_tri_goda_za_ukrainskuyu_ddos-ataku
https://meduza.io/feature/2022/03/04/meduza-zablokirovana-v-rossii-my-byli-k-etomu-gotovy-i-prodolzhaem-rabotat
https://novayagazeta.eu/articles/2022/04/29/budem-govorit-kak-est
https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics
https://meduza.io/en/feature/2023/11/18/elves-vs-trolls

2. Data leak that gave a new perspective on chinese cyber influencing

https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/
https://hongkongfp.com/2024/02/24/hackers-for-sale-what-we-know-about-chinas-massive-i-soon-cyber-leak/
https://thereadable.co/the-i-soon-data-leak-chinese-apts-and-implications-for-southeast-asia/
https://www.crunchbase.com/organization/i-soon
https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/
https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/
https://readwrite.com/chinas-hired-hackers-a-massive-cybersecurity-breach-exposing-chinas-operations/
https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41
https://www.infosecurity-magazine.com/news-features/isoon-github-leak-chinese-cyber/

3. Challenges of cyber security statistics

https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023
https://www.corvusinsurance.com/blog/q3-ransomware-report?utm_campaign=FY23-Q4-Quarterly%20Ransomware%20Report&utm_source=ransomware%20blog&utm_medium=press
https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/
https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/
https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-as-victims-refuse-to-pay/
https://www.wired.com/story/ransomware-payments-2023-breaks-record/

Pictures: Pixabay