Monthly Review

Cybersecurity news from around the world

GENERAL CYBERSECURITY NEWS 2

ARTICLES

Commercial spyware threatens privacy 4

Young Western cybercriminals playing into Russia's hands ... 7

KEY TAKEAWAYS 10

ARTICLE

Young Western cyber-criminals playing into Russia's hands

Read article →

SECTRA

General cybersecurity news

1 What lessons can be learned from the explosions in Lebanon

In September, several pagers and walkie-talkies belonging to Hezbollah exploded in Lebanon, killing dozens of people and injuring thousands. Hezbollah is a party and paramilitary organization considered a terrorist organization by many actors globally. Hezbollah had switched to older technology for communication due to security concerns. They had ordered the exploded equipment from a Hungarian front company, but little information is available about the company. It is unclear who manufactured the explosive devices.

The explosions in Lebanon serve as a reminder of the importance of supply chain security in today's world. One major concern is the presence of malware or backdoors in Chinese-made hardware or software, which can provide threat actors with unauthorized access to devices and the data processed on them. Organizations that prioritize safety must be thorough in investigating the origins of the technical solutions they use, ensuring they come from reputable sources. With the increasing complexity of supply chains, it is crucial to mitigate potential risks and protect against cyber threats. By taking proactive measures to ensure the safety and integrity of their supply chains, organizations can minimize the likelihood of incidents like the explosions in Lebanon and strengthen their overall cybersecurity posture.

2 The food industry is facing a growing cyber threat

Cyber threats in the food industry are increasing, with 167 attacks reported in the U.S. in 2023. The sector's critical role in ensuring a reliable food supply, makes it an attractive target for financially motivated criminals and malicious actors. Vulnerabilities include outdated systems, long supply chains, and lack of cybersecurity awareness, especially among small producers. Last year's most significant attack was probably the ransomware attack on Dole, the world's largest fruit and vegetable producer, at a total cost of more than ten million dollars. As cyberattacks grow, the industry is working to improve its cybersecurity, but gaps remain, particularly in securing operational technology (OT) systems.

3 The gap between ideological and economic cybercrime is narrowing

The landscape of hacktivism is changing, with a shift towards more traditional cybercrime. Russian hacktivist groups have expanded into financially motivated cybercrime, such as ransomware. This evolution has led to a more organized and professional approach. Some individuals involved in hacktivism have been drawn into cybercrime activities. Additionally, financially motivated cybercriminals, including Russian ransomware actors, have started to act with political motives, particularly against Western countries. This convergence between hacktivism and financially motivated cybercrime poses challenges for victims and makes it difficult to differentiate between different types of threat actors.

ARTICLE

Commercial spyware threatens privacy

Commercial surveillance vendors (CSVs) pose a significant threat to people's privacy and cybersecurity. These are private companies that develop and offer products that enable spying on devices operating in the online environment.

In recent years, commercial surveillance vendors have been under scrutiny especially with the development of software suitable for eavesdropping on mobile devices, such as the Pegasus and Predator spyware software developed by the Israeli origin NSO Group and Intellexa. These have been used to spy on journalists, business leaders and opposition activists around the world. Often, they can be delivered to the victim's device unnoticed without an error from the victim's side. After delivery, spying can be targeted, for example, at the microphone, camera and other data contained in the phone of the victim.

The general attitude towards commercial surveillance vendors is highly critical, and United States, for example, has placed both NSO Group and Intellexa on its sanctions list. Not only is there a lack of transparency in the way the companies operate, but there is also a fear that the technologies they use will spread and end up in harmful hands, as has already happened. Intellexa, for example, has delivered its products to various authoritarian states, with NSO Group claims to only provides services to members of the US-Israeli coalition and their security authorities. The power to spy on almost anyone gives these companies considerable power and capabilities, even beyond what some governments possess. →

The latest example of CSVs and their impact came at the end of August, when Google's Threat Analysis Group (TAG) monitored an operation by the Russian group APT29 targeting the Mongolian government between 2023 and 2024. APT29 is a Russian state cyber threat actor operating under the authority of the country's foreign intelligence agency SVR. The attack targeted Mongolian government websites and manipulated them by downloading malware to the device of a user visiting the website using a so-called watering hole attack method. The goal was to steal cookies on victims' devices, including login cookies, by exploiting vulnerabilities in Apple's iOS operating system and Google's Chrome web browser.

"What makes the case remarkable is that the techniques used in the attack showed extreme similarities to commercial espionage tools developed by NSO and Intellexa."

What makes the case remarkable is that the techniques used in the attack showed extreme similarities to commercial espionage tools developed by NSO and Intellexa. It appears that APT29 gained access to this attack method only months after it appeared in the repertoire of commercial surveillance vendors. There is no direct evidence that the tools are from commercial operators, but the timing and technology used in practice suggest so. This speaks about the effectiveness of private companies' products, as even Russia, known as an advanced cyber state, is apparently forced to buy these cyberweapons. Of course, it cannot be completely ruled out that the Russians themselves have succeeded in developing a similar method of attack or have managed to spy on information about a working method of attack from private companies. Attention should therefore be paid also to the level of Russian cyber intelligence and cyber expertise, as well as to the development of attack methods. →

It was already known that private companies had offered their services to dictatorships such as Azerbaijan and Saudi Arabia, so providing services to Russia is a logical continuation of this cooperation. The case underscores that morality should not be expected from commercial surveillance vendors, and in principle, services can be assumed to be available to any solvent customer. In the big picture, this erodes trust in, for example, the privacy and protection of mobile phones and other online activities.

Efforts are underway to prevent the spread and misuse of commercial cyber intrusion tools. The Pall Mall Process, launched by the UK and France in February 2024, aims to address this issue. This process got an update in August, when the countries opened a consultation round on the topic aimed at governments, industry, and civil society. The statements must be submitted by October 14, and its goal is to spark discussion and gather information. However, there are concerns that cooperation and restrictions may be too limited and arrive too late, as cases like APT29 show that dangerous tools have already fallen into the wrong hands. ■

ARTICLE

Young Western cybercriminals playing into Russia's hands

In early September, London's public transport system was hit by a cyberattack. Although there was no actual impact on the flow of traffic, disturbances in payment transmission and a significant slowdown in the organization’s internal operations were observed.

It was later revealed that the attackers likely obtained personal data of registered users of public transport and, in some cases, payment information. The suspect in the case is only a 17-year-old British citizen. This isn't the only serious cyberattack carried out by a teenager in the UK over the summer. Most recently, in July, another 17-year-old was arrested after being linked to a 2023 attack on the MGM hotel chain that led to several days of inoperability of the hotel chain's slot machines, ATMs and online bookings, among other functions.

Of course, cybercrime among young people has been talked about before, but cyberattacks of this magnitude are rare. Typically, youth cybercrime has focused on low-level cyberattacks, such as denial-of-service attacks on school systems. What makes the recent cases remarkable is that there has been talk of links to the Scattered Spider cybercrime group, especially in the case of the MGM hotel attacks. Its members are thought to be mainly US and British citizens between the ages of 16 and 22. →

This is a rather exceptional cybercrime group due to the age and nationality of the perpetrators. The group is believed to have links to the Russian ransomware operator BlackCat. In addition to ransomware, Scattered Spider has used phishing and impersonating as IT support as its techniques.

"The group was born on dark web forums, where there is often competition to see who dares and knows how to do the most damage with cyber attacks."

The Scattered Spider can be thought of as a symptom or manifestation of a long-known problem. Young people are skilled at operating in the cyber world, and unfortunately often their skills are directed to the wrong side of the law. There are many reasons for this. Independently acquired skills are not recognized, regular jobs do not seem interesting but the need to prove one's abilities is high, the risk of being caught is perceived as low, and there is plenty of encouragement to commit crimes on the dark side of the web. In the case of the Scattered Spider, probably the latter reason plays a significant role. The group was born on dark web forums, where there is often competition to see who dares and knows how to do the most damage with cyber attacks. The like-minded youngsters found each other and in 2022 began carrying out larger operations together, forming the group now known as the Scattered Spider. After the first few successful attacks, the group's activities continued to accelerate as they attracted the attention of Russian ransomware groups. Well-known extortionists, such as BlackCat and Lockbit, became interested in a group of young Westerners, whose targets were mainly found in the United States, and began to support and guide them in more serious attacks. →

The aim of these groups is all forms of harassment in Western countries, and recruiting their own citizens is effective in many ways. It obscures Russia's involvement in crimes and, at the same time, serves as an excellent tool for information influencing, highlighting how Westerners themselves oppose the actions of their home countries. Attractive factors for young people include money, influence and the fact that their skills are recognized and valued. Scattered Spider's operations are both ruthless and effective. The group focuses especially in social engineering, which is often used to gain first access to the target organization's systems. Manipulation is effective because, unlike hackers from abroad, there is no language barrier with English, and young people understand Western culture and practices better than Russian hackers.

The Scattered Spider has gained attention for its serious and successful attacks. Some group members have been arrested, but their operations remain unaffected. It is concerning that young people are drawn to cybercrime, especially when influenced by foreign criminal groups. These criminals encourage more serious crimes, which may result in a "turning" against the West if the trend continues. Cybercrime is one of Russia's hybrid influencing methods, and if it also acts as a lure to turn young people towards their own societies, it works as a very effective and beneficial tool for the country's goals. ■

Key takeaways

1. The explosions in Lebanon highlight the significance of supply chain security, as pagers and walkie-talkies belonging to Hezbollah exploded.

2. Cyber threats in the food industry are on the rise. At worst, cyberattacks can have catastrophic consequences.

3. The gap between ideological hacktivism and financially motivated cybercrime has narrowed. Especially in the case of Russian actors, motives are increasingly overlapping and differentiation between groups is difficult.

4. Commercial surveillance vendors pose a significant threat to privacy and cybersecurity. These are private companies that develop products that enable spying on devices operating in the online environment.

5. Serious cyber attacks carried out by Western teenagers have made headlines. In the background, the encouragement and motives of Russian cybercriminal groups can be seen.

communications.sectra.com
communications@sectra.com

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

SECTRA