Monthly Review

Cybersecurity news from around the world

ARTICLE

Nordea Bank faces cyberattacks and IT disruptions

Read article →

SECTRA

General cybersecurity news

1 Telephone-assisted cyberattacks are evolving

Telephone-based cybercrime has seen an increase in recent years, with over 10 million cyberattack-related calls occurring worldwide each month. While many of these calls are easily recognizable scams, there are also more sophisticated attacks targeting specific organizations. Known as TOAD (telephone-operated attack delivery), these attacks involve using the phone to manipulate or trick victims into carrying out harmful actions. This can include opening malware-infected files, accepting fraudulent authentication requests, clicking on links, or sharing sensitive information. These attacks rely on social engineering techniques, often starting with an email or message asking the victim to contact a provided phone number. By avoiding direct calls, scammers can bypass spam filters and exploit victims' trust. Perpetrators use information about the target to appear trustworthy, such as stolen invoice numbers or knowledge of ongoing projects. Technological advancements, like audio converters and AI translation, have made these attacks more sophisticated. Deepfake voice messages are also used to deceive victims, making it appear as though a familiar person is requesting a call.

This type of cyberattack is becoming increasingly prevalent, with services offered on dark web forums in multiple languages. Despite efforts to combat these attacks, it is crucial to remain vigilant as phone scams can be professional and difficult to identify.

2 Cyber war between Iran and Israel escalates

The recent conflict between Israel and Iran, as well as their respective proxy groups, has spilled over into the cyber realm. Both sides have been engaged in a long-standing cyber war, with a focus on hack-and-leak attacks aimed at causing psychological impact. The Handala Hack Team, believed to be under the control of the Iranian state, has targeted Israel, while Predatory Sparrow, a group separate from the Israeli state but likely affiliated, has attacked Iran. Physical damage from cyberattacks is rare but has been seen in instances like the Predatory Sparrow's attack on the Iranian steel industry. It is widely believed that both Iran and Israel receive external support for their cyber activities, with Iran having signed a cyber cooperation agreement with Russia, and Israel with the United States.

3 Genetic data at risk

Concerns have arisen about the fate of sensitive personal data after DNA testing company 23andMe faced difficulties in 2024. The company allows users to learn about their ancestry and health information by submitting their DNA. With 15 million users, 23andMe is a medium-sized player in the industry. The company has recently experienced share price drops, board member resignations, and rumors of bankruptcy. This has raised questions about the use and future of user-provided genetic data. The company's privacy notice states that personal data may be transferred to a new operator in the event of bankruptcy or acquisition. Many users were surprised by this revelation, as they often do not read privacy policies. The company's privacy policy allows for flexibility in processing personal data, with separate consent currently required for research or targeted advertising. The case of 23andMe underscores trust issues with personal data and highlights the challenges of navigating changing privacy policies and practices. It serves as a reminder for individuals to be cautious about how their sensitive information is used and what rights they grant companies when disclosing such data.

ARTICLE

Caution while granting access rights to applications

Cyber security company Kaspersky recently exited the U.S. market after authorities banned the sale and distribution of its antivirus software to consumers.

The use of the company's products in U.S. government organizations was already banned, with the first restrictions coming into effect already in 2017, eventually leading to a total ban. This relates to the background of the Russian company, which officials say could pose a risk to U.S. national security. In practice, Kaspersky is suspected of having links to Russian authorities and security services. Kaspersky itself has assured itself to be a reliable security partner and an independent operator. No smoking gun has been found for the company, but the company's founder is known to have a background in Russian intelligence. Kaspersky's exit from the US market has been known since July, but events received an update at the end of September as Kaspersky apps left consumers' hardware. The app was automatically replaced by the antivirus app UltraAV. The new application came to many users unexpectedly and unsolicited, thus causing great confusion and outright outrage among users. Kaspersky had the installation of a replacement application, but many users had missed the news. The incident highlights at least two security phenomena. →

The first of these concerns the permissions given to security and antivirus applications, which need quite extensive access rights and the ability to monitor the system and its network traffic in order to function effectively. The operation of a security application is often the most important piece in the information security puzzle. An example of this is the IT problem that spread in July with a faulty update from the security company CrowdStrike, which led to global disruptions in air traffic, as well as numerous other services.

"If an application refuses to work without seemingly unjustified permissions, alarm bells should start ringing."

Secondly, attention should be paid to rights beyond those granted to antivirus software. On mobile devices, it is common for apps to be downloaded on demand, and often they request or require significantly more permissions than are needed. Although many applications ask for it, few actually need access to, for example, a calendar, contacts or photos. Every time downloading a new application, it is good to consider with common sense whether it actually needs to have asked rights for its operation. If an application refuses to work without seemingly unjustified permissions, alarm bells should start ringing. For example, it is legitimate for a navigation app to request access to your device's location data, but there is no natural need to do so for a calendar or photos. Allowing extra permissions can expose personal data to application providers or, at worst, cybercriminals. On mobile devices, as well as computers, it is often easy to check through the settings what permissions each application has, and which of these it necessarily needs to work. →

As in many other areas of cyber security, individual responsibility becomes critical here. It is possible for an organization to limit the number of applications that can be installed on work devices and, through them, what permissions are required from users. If personal devices are used for work, this important aspect of cyber security is the sole responsibility of users. Guidelines alone are often not enough, and it would be important to make employees understand what kind of threat each guideline has been drawn up for. Gaps in application security can not only expose the employer's data but also compromise the individual's own security, so there should be a great interest in maintaining it. ■

ARTICLE

Nordea Bank faces cyberattacks and IT disruptions

Nordea, the largest bank in the Nordics, has been in the middle of a storm after falling victim to cyberattacks and large-scale IT disruptions. The problems have been going on for a month and have been visible to customers, for example, as customer accounts disappearing from services and login difficulties.

The case has garnered a lot of publicity. In Finland, Nordea has even been invited to appear before the Parliamentary Finance Committee. Strong and long-lasting denial-of-service attacks on the organization and failed updates aimed at responding to the threat have been cited as the cause of the problems to the public. Nordea's events are a prime example of Russian-sourced cyber and hybrid influencing.

There has been only a little public speculation about the perpetrator of the DDoS attack, although cautious comments have been made about possible Russian interference. In practice, however, it seems clear that the attacks come from Russia. Russia has both the ability and motivation to carry out attacks. Also, the modus operandi refers to Russian activities. The recent problems began when Sweden approved a new aid package for Ukraine. Thus, the timing of the attacks would argue in favor of Russian complicity. At the same time as Nordea, several other banks operating in Sweden have been targeted. →

Another factor pointing to Russia is the RootDoS group, which claimed responsibility for at least part of the attacks. The group states that its motive is the burning of Korans in Sweden and that the group itself comes from Arab countries. However, it is not unusual for groups linked to Russia to state false origins and false motives. The deniability of the activities is one of the cornerstones of Russian hybrid influencing.

"This is exactly the kind of multifaceted impact Russia is aiming for with its cyber and hybrid influencing."

Thirdly, the manner in which the attack is carried out, publicly mentioned denial-of-service attacks are a well-known low-level cyberattack method used by Russia. Of course, denial-of-service attacks are carried out by other threat actors in the cyber world, but lately they have been part of Russia's toolbox in particular. The implementation of DDoS attacks has already been estimated to have cost millions of euros. This also refers to a well-resourced state cyber actor. Hijacked smart devices, such as IoT household items, have been used in carrying out the attacks. This underscores the risks associated with the Internet of Things and the need to take care of the cybersecurity and updates of one's own personal devices.

Fourthly, hitting the financial sector with cyberattacks is straight out of Russia's playbook. The target is a critical sector of society, the inaction of which causes uncertainty and a sense of insecurity for ordinary citizens. At the same time, it affects the day-to-day functioning of society and undermines citizens' trust in it. The mere fact that the banking system can be disrupted fulfils one of the objectives of the operation, but the reactions of society and the media will certainly produce valuable information on the behavior and operating methods of Nordic residents and also serve the objective of information influencing of the operation. This is exactly the kind of multifaceted impact Russia is aiming for with its cyber and hybrid influencing. →

For Nordea and Western societies, the ongoing cyberattack offers several lessons. The case highlights the possible wide-ranging and long-lasting effects of cyberattacks and underscores the role of the financial sector as part of critical infrastructure and its core. The financial sector complies with the EU's DORA regulation, which aims to manage and minimize the digital risks faced by the sector. It includes, among other things, obligations related to risk management, incidents and their reporting. Nordea's case shows that even the best regulation may not always help if cyberattacks succeed in hitting a weak spot in the system. In addition to technical failures, the failure of services has led to a loss of confidence in the eyes of customers, and the bank has already lost hundreds of customers.

This is a reminder of the reputational damage and financial losses associated with cyberattacks. The incident also highlights the importance of preparedness. The ability to conduct threat intelligence and detection must be maintained in every situation. Once the problems have been solved, the lessons learned from the attack should be shared in society with other actors in the critical sector. This would increase society's overall resilience and prevent future threats. ■

Key takeaways

1. Telephone-assisted cyberattacks are on the rise and are used as part of professional and serious cybercrime.

2. Proxy cyber war escalates between Israel and Iran, with hack-and-leak attacks and external support playing a role.

3. 23andme's difficulties have raised questions about the fate of the DNA data it holds.

4. Unnecessary permissions for applications can compromise cyber security.

5. The cyberattacks on Nordea Bank are a prime example of Russian cyber and hybrid influencing.

communications.sectra.com
communications@sectra.com

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

SECTRA