Cyberwatch Finland

# WEEKLY REVIEW

# WEEK 12/2024

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

Cyberwatch Finland

# KEY TAKEAWAYS

1. In the Gaza conflict, Hamas' role in the cyberspace has diminished. Instead, Iran has taken on the role of main adversary in the cyberwar against Israel.

2. Cyber resilience is a significant part of an organisation's overall resilience. It includes, in particular, the ability to anticipate, tolerate and recover from disruptions.

3. Gift card scams are a common form of cybercrime. Platform giants have been urged to take tougher measures to combat the phenomenon.

Cyberwatch Finland

# 1. GAZA'S CYBER CONFLICT CONTINUES

Last week, Google's security company Mandiant reported on the recent activity of a hacker group called UNC1549, which it had surveilled for some time. According to the company, it is almost certainly Iran's state threat actor, or APT group. The group has recently carried out extensive intelligence gathering and espionage campaigns targeting countries in the Middle East, in particular Israel. Some of the activities have directly exploited the ongoing Israeli-Hamas conflict, and efforts have been made to gather information especially on actors in the defence and aviation sectors. In many ways, the operation is a good description of what is currently happening on the cyber front of the conflict. The front has been very active throughout the war, and cyber influencing towards Israel in particular has grown steadily in recent months.

However, most cyberattacks have not been carried out by Hamas or actors directly linked to it (who were, however, remarkably active before the start of the war itself), but specifically by Iranian hacker groups. It appears that Hamas' "role" in the cyberspace of the conflict has been taken by Israel's old adversary Iran. Although cyber struggles and mutual attacks between the two countries have been commonplace for years, the conflict in Gaza has clearly accelerated this activity. As soon as the war began, Iranian hackers rushed to support Hamas. Interestingly, these initial Iranian operations appeared to be of rather poor quality and ill-prepared. It is possible that this was due, for example, to the fact that the groups would not have been informed in advance of the impending attack and therefore had to carry out attacks in a hurry without proper preparation. Another reason may be that the prepared attacks could have specifically revealed close cooperation between Iranian state hacker groups and Hamas. Since the beginning, the level of attacks has increased, but no significant impact has been achieved in influencing Israel.

Israel has not been merely a victim of attack, but has actively invested in and improved its own defense capabilities and, at the same time, has carried out attacks on both Hamas and Iran. However, attacks on Hamas are less noteworthy, as the organization does not have many targets to hit in the cyber world. For this reason, too, most of the influence has been directed specifically at Iran. The most significant group to strike Iran is Gonjeshke Darande (also known as Predatory Sparrow) – an actor widely identified as one of the cyber strike groups linked to the State of Israel. The same group has previously exerted influence on Iran. Targets have included, for example, the country's public transport and state-owned steel mills. In December, the group managed to cripple most of Iran's fuel stations, 70% according to its own statement, causing considerable fuel distribution difficulties. In addition to direct attacks, Israel is likely to support reconnaissance operations and other projects related to physical war using the cyber environment, even if there is little publicity about these.

In the cyber environment, there is a constant and mutual struggle. In recent weeks, it has begun to appear that Iran's attention, in particular, has shifted from Israel itself to the states or actors that support it. This is also well illustrated by the campaign identified by Mandiant, mentioned earlier, in which the focus was no longer only on Israel, but on the search for targets more extensively in nearby areas. A similar conclusion has been reached by Microsoft, which has analysed the cyber conflict in February. In its analysis in Microsoft has concluded that the cyber conflict between Israel and Hamas has been divided into three clear phases. The first of these included initial reactive and ill-prepared attacks against Israel, and the second phase involved escalating mutual cyberattacks between Israel and Iran. The third phase, which is now underway, is the escalation of the war, and especially Iran's influence on the allies and supporters of the opposing side.

It is difficult to assess why Iran has chosen to shift its attention away from Israel. One possible reason is that, so far, the operation against Israel has not had any significant impact. Israel's cyber defense can be considered one of the best in the world. It also has years of experience in being the target of Iranian influence, and its investment in cyber defence has certainly increased during the conflict. For these reasons, attacks on allies perhaps have the potential for greater success.

Another interesting point to assess is how the cyber conflict from here will continue. It is highly likely that operations in support of Israel's broad strategic objectives will continue behind closed doors. What is more uncertain is how far Iran seeks to spread its influence and how successful its operations will be. It is good to remember that Iran itself has some kind of ally in the cyber world. The country's hacker groups have long been collaborating with Russian threat actors. At the moment, Russia's cyber resources may be fairly tied up in its own operations, but the possible sharing of information or the development of cooperation may still be worrying, even if no clear signs of this have been detected.

# 2. RESILENCE AS A PART OF CYBER SECURITY

Resilience has become a modern buzzword and it is used in many different contexts. Political speeches can refer to societal resilience, and in the business world, organisational resilience can be discussed. In addition, concepts such as economic or ecological resilience occasionally appear in public debate. Today, the resilience-prefix can be added to almost all possible areas of life where undesirable events can occur due to external factors. The term is also used in cybersecurity: we talk about the cyber resilience of an organisation or society. In the end, what is actually hidden behind the word?

Resilience as a concept is slippery and there is no single accepted definition or frame of reference. It also makes the discussion of the concept difficult. However, there have been attempts to define resilience. In Finland, attempts have been made to define the concept, for example, by the Security Committee, a co-operation and expert body focusing on preparedness, operating in connection with the Ministry of Defence. According to the Cyber Security Glossary published by the Committee, resilience refers to "the ability of individuals and communities to maintain their ability to function in changing circumstances and the readiness to face and recover from disruptions and crises". However, it is also much more than that, for example flexibility and adaptability.

Cyber resilience, on the other hand, can refer to, among other things, to the ability to anticipate, tolerate and recover from cyberattacks. Resilience can be reflected in both proactive and reactive measures that are taken when cyberattacks occur, or even before. When a cyber threat materialises, it is not just a question of restoring data and systems to their pre-event or better state. It is also about adapting to the new threat landscape, which can be seen, for example, in identifying new cyberattack methods and threat actors. Maintaining an up-to-date situational picture cannot be overemphasized and is an important pillar in building organisation's cyber resilience.

**Areas of cyber resilience**

**Anticipation:** Up-to-date situational awareness, personnel training and instructions, risk assessments and audits, testing activities

**Tolerance:** Firewalls and other technical information security measures, backups and backup systems, training in case of disturbances and implementation of measures in a crisis, crisis management and communication

**Recovery:** Damage limitation and repair, incident investigation, learning from mistakes and development of cyber security

There are no unambiguous ways to measure cyber resilience or any other kind of resilience. However, for example, the World Economic Forum (WEF) has published its own proposal for measuring cyber resilience. It has developed the so-called Cyber Resilience Index, which is freely available to organisations on its website. The index result is affected by, among other things, the training provided by the organisation to its personnel, the implementation of risk assessments, and the identification and reduction of vulnerability surface area.

Outside the cyber sector, more applications have been made to measure resilience. In Norway, for example, the resilience of municipalities has been studied using a number of factors, such as social, economic, environmental and infrastructural factors. In addition, there is the so-called Critical Infrastructure Resilience Index (CIRI), which measures resilience through seven stages, such as risk assessment, prevention, response and recovery. In the model, general and operator-specific indicators are set for each stage on a maturity scale of 0–5, which is later added together as the operator's overall resilience. Although there is no single correct way to measure or calculate an organisation's resilience or cyber resilience, quantifying it could provide a basis for identifying weaknesses and raising the level of resilience.

Cyberwatch Finland

For an organisation, the importance of cyber resilience is emphasised as part of the organisation's overall resilience and is partly linked to traditional risk management, although resilience is a broader concept than standardized risk management. The concept also includes the possibility of surprise – not everything can be predicted or identified even in the finest risk management scenarios. However, instead of conceptual gimmicks and semantic debates, it would be appropriate to recognise the significance of cyber security in an organisation's day-to-day operations, as well as its broader strategic significance for the organisation's operations as a whole. An important part of an organisation's overall resilience is also the personal resilience of its employees, which is the individual ability to cope and recover from challenging situations.

# 3. GIFT CARD SCAMS ARE A SIGNIFICANT PHENOMENON

One tool widely used in low-level cybercrime is various gift cards. Cyber scammers use social engineering to trick victims into buying a gift card and handing over its details to the scammer. Although it may sound strange to someone familiar with cyber threats that someone would go and buy a gift card at the advice of a foreign scammer and end up handing over the card details to them, it is still a common and effective way to transfer money from victims to scammers. In practice, there are almost unlimited reasons on how a fraudster justifies the need for a gift card.

One popular way to carry out a scam is to impersonate Google's support service and make the victim believe that they have unpaid invoices that are in the process of collection and should be dealt with as soon as possible. A quick alternative can be a payment "directly to Google", i.e. buying a Google Store gift card. The situation often emphasizes - typical for social engineering - haste. The victim may think they are in trouble, and a scammer pretending to be trustworthy can help them out. Gift card information can also be hijacked through various phishing sites. These mimic real e-commerce platforms, but the information entered into them ends up in the hands of a scammer. These types of scams are becoming more common, especially around Christmas and other holidays, and their credibility continues to evolve as criminal techniques improve.

The scam can target both physical and digital gift cards, as both have number sequences and PIN codes that allow the amount loaded onto the gift card to be used to pay for purchases. In practice, gift cards serve as a means of currency transfer. For scammers, they are a good tool for a variety of reasons. Firstly, since no actual "currency" is transferred, for example, from one bank account to another, it is very difficult to trace the money and return it to the victims, even if the scam is later revealed. Secondly, since there are no official banks involved with which the victim deals, the risk of someone warning them about a possible scam is lower. Thirdly, not only is it difficult to trace the money, but it is also difficult to catch the fraudster who has seized it. Even if the victim realises that they have been scammed and reports the gift card numbers obtained by the scammers to the issuer of the gift card, they alone make it very difficult to reach the scammers themselves. Gift cards from major platforms such as the Google Store, Amazon or Apple work all over the world. They can either be used by yourself or sold quickly, making tracing even more difficult.

According to the FTC, in the United States alone, amounts scammed through gift cards run into hundreds of millions of dollars annually. For example, in 2021, $17 million worth of Google gift cards alone were used in scams. Apple's figure was 16 million, but the clear top spot was held by retail chain Target, whose gift cards were used in scams to the tune of $35 million. The number of scams is also growing. However, this does not necessarily indicate the growing popularity of gift card scams, but rather the general growth of cyber scams.

In gift card scams, the responsibility of retail chains and different platforms in combating the phenomenon should also be considered. According to estimates, the margins of gift cards are good and, in the case of Google and Apple, for example, the platform holder receives up to 15–30% of all purchases made with gift cards. Thus, platform giants, at least indirectly, benefit from this criminal phenomenon. Lawsuits have also been filed against them. At the beginning of March, a lawsuit was filed against Google in California, alleging that its efforts to combat the phenomenon were minor. For example, Google doesn't refund payments made using gift cards or lost gift cards. It has also been criticised for inadequate warnings and mention of risks. A similar lawsuit had already been filed against Apple in January, but it was eventually settled outside the courtroom.

On the other hand, the question arises as to what measures would ultimately be sufficient to prevent this phenomenon. For example, Google warns about gift card scams both on its website and in its support service. Apple Support also has its own section for the scam phenomenon. Both operators also have a warning about possible scams in connection with physical gift cards. So, measures have been taken, but for one reason or another, the number of gift card scams is still high. One reason for this may be that blocking measures are often known to scammers. When the victim is manipulated into buying cards, they are often informed of these warnings beforehand, which can reduce their effectiveness. Moreover, when you contrast a scammer posing as a Google support person, who has already gained the victim's trust, and a short piece of text on a shop wall, it should come as no surprise that the impact of warnings is small.

A better solution would therefore be to raise awareness in advance and to provide clearer and more visible instructions indicating that no official entity uses gift cards as a means of payment. A practical benefit would be, for example, that with each gift card purchase, the buyer would have to answer the question of whether a previously unknown party had advised the buyer to buy the card. However, not all responsibility can be shifted solely to the companies; the responsibility also lies with the buyer himself. Therefore, the development of citizens' digital skills and continuous information on various cyber scams and fraud could serve as a tool to limit the phenomenon. The cost of cybercrime to individuals and society is high on an annual level, and the problem will certainly not diminish in the future.

# REFERENCES


## 1. Gaza's cyber conflict continues

https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east
https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/
https://www.darkreading.com/threat-intelligence/hamas-cyberattacks-ceased-after-october-7-attack-but-why
https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/
https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/
https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/

## 2. Resilience as a part of cyber security

https://csrc.nist.gov/glossary/term/cyber_resiliency
https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf
https://www.sciencedirect.com/science/article/pii/S2212420918312032
https://www.weforum.org/publications/the-cyber-resilience-index-advancing-organizational-cyber-resilience/
Pursiainen, Christer (2023): "Resilienssin ulottuvuudet". Kosmopolis, 4/2023, 30–54

## 3. Gift card scams are a significant phenomenon

https://play.google/giftcards/
https://support.apple.com/fi-fi/gift-card-scams
https://support.google.com/googleplay/answer/9057338?hl=en
https://www.theregister.com/2024/03/07/google_sued_for_profiting_gift_card_fraud/
https://www.ftc.gov/business-guidance/blog/2021/12/gift-card-scams-out-shadows-ftc-data-spotlight
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do


Pictures: Pixabay

Cyberwatch Finland