1. Estonia was targeted by a wave of DDoS attacks

**SITUATION**

In the past quarter, distributed denial-of-service (DDoS) attacks against several state agencies and providers of vital and important services set the tone in Estonian cyberspace.

The attacks took place in waves: the first and most impactful wave took place on 21–25 April, when 13 different websites of government e-services or other vital online services were attacked. It occurred at the same time as the international cyber exercise Locked Shields was conducted in Estonia.

The second wave took place on 8–9 May, around the Victory Day celebrated in Russia, when attacks were carried out against the websites of the Ministry of Foreign Affairs, the Ministry of the Interior, and the Police and Border Guard Board among others.

The third wave began on 5 June, when government websites, as well as the websites of banks and transport companies, were attacked for nearly a week.

Most of the targeted websites had additional security measures put in place beforehand, so the impact of the attacks was very limited. However, some websites were unavailable for up to a few hours, causing inconvenience to users.

**ASSESSMENT**

The choice of targets and the timing of the attacks signal the desire of the attackers to cause reputational damage and disrupt normal services in order to create uncertainty and irritation among people.

Behind the attacks are various pro-Russian hacker groups who brag about their activities in social media groups. They do not only target Estonia, but also other countries that have condemned Russian aggression in Ukraine and supported Ukraine.

In late June, for example, similar denial-of-service attacks took place against Lithuania and Norway, both prompted by the decision of the countries to block the transport of sanctioned goods to Russia through their territory.

In the case of Estonia, the attackers used compromised websites as well as botnets to carry out the attacks. The attack waves were of different intensity – at the peak of the April wave, the number of malicious requests made to Estonian websites reached 700 million within a few hours. The impact of the attacks was relatively small, as the administrators of most of the targeted websites had prepared for it in advance, and in some cases CERT-EE also provided additional support.

This kind of hostile activity in cyberspace is currently very common and a good example of hacktivism, which we wrote about in the previous quarterly review.

Denial-of-service attacks are a fairly cost-effective way for an attacker to achieve some effect, so we expect to see more waves like this. It must also be taken into account that even if Estonian companies are not the target, attacks against other countries may bring a spillover effect, for example through shared data centres.

A general guide on how to protect yourself against denial-of-service attacks

2. Is that you in this video?

**SITUATION**

In April and May, we saw a wave of Facebook accounts takeover. This time, the attackers sent the message ‘Look what I found’ or ‘Is that you in this video?’ to the users, inviting them to click on a link. If the user opened the link, he or she was redirected to the next website where their account was taken over. Account takeovers are on the rise among incidents recorded by CERT-EE; compared to last year, the increase is almost 40%.

The statistics reflect only the incidents reported to us. In reality, the situation is certainly much worse.

After the attackers get hold of the person’s social media account, they change the password, phone number, and e-mail address, making it much more difficult to recover the account.

Getting your account back can be downright impossible, and we wrote about this in more detail on our blog (in Estonian).

**ASSESSMENT**

Accounts are typically taken over via a phishing page where the person unsuspectingly enters their username and password.

This spring, however, we saw a different approach where it only took one wrong click and the user may not have even realised that something happened.

A similar scam was also used on Instagram, where you did not even have to click on the link sent by your friend – you just had to take a screenshot of the link and send it back to your friend.

Account takeovers are an easy and cheap way for criminals to compromise your data. Therefore, keep in mind the following recommendations:

- The most important thing is to be attentive and cautious and not to open suspicious links received via message or e-mail, even if they appear to come from your friends. If you receive a suspicious message that requires urgent action, do not open the link.
- Account takeover by clicking on a single link can be done on both a smart device and a computer, and this attack method works in all social media environments. As an additional protection, CERT-EE offers the Encrypted DNS application, which blocks malware and phishing and filters malicious links from the user using DNS. The app is available for both Apple and Android devices and can be downloaded from the official app store.
- Report all suspicious e-mails and messages to our incident response department (CERT-EE) using the raport.cert.ee environment or send an e-mail to cert@cert.ee.
3. Smart home appliances are tempting for cyber attackers

SITUATION
In May, we wrote on our blog (in Estonian) about two critical security vulnerabilities affecting video surveillance cameras from one manufacturer.

With the help of the security weaknesses, an attacker can potentially take over vulnerable devices and use them to monitor video, collect sensitive information (passwords, business secrets, etc.), or connect the device to a botnet that is used to attack targets with distributed denial-of-service (DDoS) attacks.

The security weaknesses were disclosed as early as at the end of 2021, but CERT-EE still discovered several hundred potentially vulnerable devices in Estonia last quarter.

Video surveillance cameras are also not the only devices that people connect to the internet. There are more and more household appliances that have this feature and the number of companies offering various IoT solutions is increasing.

As people buy more and more such devices, they often do not have an accurate overview of all of the devices that use their home internet.

ASSSESSMENT
Internet of Things (IoT) devices such as vacuum cleaners, video surveillance cameras, light bulbs, refrigerators, or dishwashers are not generally associated with cyber threats because they perform very specific tasks and seem safe.

However, the triviality of the devices is what attracts attackers, as they are often not configured securely – they use default passwords that are often available on the internet, have outdated software that contains security vulnerabilities, or require unnecessary access rights to operate that can be potentially abused by attackers.

Here are some recommendations that should be observed when using IoT devices:
- Change all passwords of the IoT devices and update them regularly. Default passwords are often easy to find online or can be easy to guess.
- Check regularly whether your IoT devices need software updates and if so, implement them. Devices with outdated software contain security vulnerabilities that attackers can exploit.
- Make sure that the administration interfaces of the devices are not accessible to everyone from the internet. Several internet service providers have instructions for using administrative interfaces on their websites.
- If possible, separate the devices which use your home network from each other. For example, create a separate network for light bulbs, smart speakers, and sensors, while keeping devices containing important data on a separate network. Segmentation of the home network ensures that criminals cannot gain access to your personal computer if IoT devices are compromised.

4. The EU agreed on new and stricter cyber security requirements

SITUATION
In recent years, cyber threats have increased worldwide, due to the development of technology, digitalisation, and more intensive cybercrime. Thus, the need to invest more than before in the cyber security of government agencies and companies has also increased. The member states of the European Union have held in-depth negotiations over the past year and reached an agreement on the new so-called cyber security directive, i.e. the Directive on Security of Network and Information Systems (also known as NIS 2.0).

Compared to the current one (the so-called NIS 1.0), the new directive regulates more sectors that are critical for the functioning of the economy and society and should contribute to their cyber security. These include, for example, waste management, postal and courier services, space industry, chemical industry, charging points for electric cars, public sector, and many others. It is important to keep in mind that this does not automatically mean all the agencies and companies of this sector, but certain entities that, in the opinion of the state, play an important role in the functioning of social life.

In addition to the new so-called critical sectors, the NIS 2.0 directive will bring stricter cyber security requirements to its subjects, increase the levers of state supervision, enhance international cooperation, and much more.

ASSSESSMENT
The impact of the new directive on Estonia can be estimated as medium. Most importantly, the Cybersecurity Act must be changed. In addition, the number of subjects will increase, meaning that the administrative burden on both state agencies and companies will also increase. At the same time, services important to Estonian life will become more resilient to cyber attacks and therefore more reliable. Since Estonia has already been quite ambitious in its Cybersecurity Act, the new requirements will not change our course.

One of the most discussed topics during the negotiations was the scope, i.e. which sectors and organisations should comply with the cybersecurity requirements. For example, one of the hot topics was the inclusion of public sector institutions as subjects, because it was not acceptable for all countries. This was not a problem for Estonia as many of our state agencies and local governments are already subject to the Cybersecurity Act. As a compromise, it was agreed that the public sector will be within the scope of the directive (including the regional level), but each country can adapt based on the structure of its public sector.

A major topic of discussion was also the provision pursuant to which the subjects of this directive must, in addition to reporting cyber incidents, also notify the state of significant cyber threats. This was opposed by several countries, including Estonia, in order to avoid an excessive administrative burden on all parties. This requirement was finally not included in the directive.

The new cyber security directive harmonises and raises the level of cyber security in the EU. At the same time, it is important to keep in mind that the directive leaves each country free to implement stricter measures than those required by the directive.

Now that the member states have agreed on the text, the EU institutions must also give their formal approval. This will probably happen in September, after which the countries will have 21 months to introduce the necessary changes in their legislation.

GOING WELL: 🍀 🌀
In addition to the new Estonian information security standard E-ITS, an updated information portal has also been completed, from which current (state agencies, providers of vital and important services) and future (e.g. schools, family doctors, various service providers) implementers of the standard can find answers to their questions.

Upon adoption of the relevant amendments to the Cybersecurity Act currently pending in the Riigikogu, E-ITS will presumably become mandatory from 1 January 2023.

COULD BE IMPROVED: 🤔
Although it is finally summer and many people are on their holidays, criminals are not taking a break. In the last few weeks, Estonian residents have been hit with another wave of scams: criminals are massively using text message fraud with the hope of stealing money from people. Victims often react too carelessly to messages imitating, for example, SEB, DHL, and Swedbank. The web link in the message leads to a phishing page controlled by criminals, prompting victims to enter their personal and bank card data. Estonians have lost tens of thousands of euros in this way in the last few months.