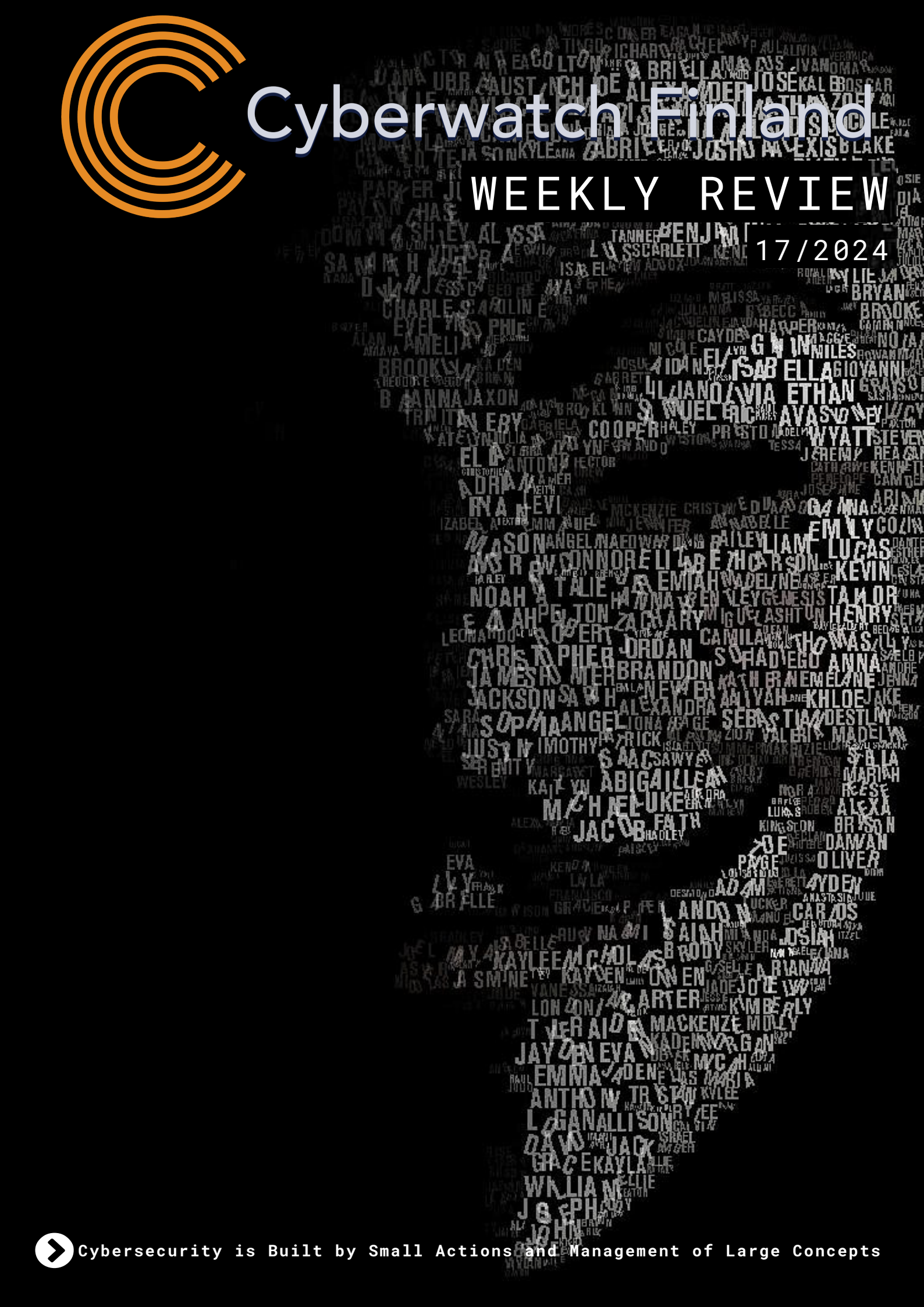
Cyberwatch Finland

WEEKLY REVIEW

17/2024



Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

17/2024

MYSTERIOUS DARK WEB

The dark web often appears as an evil and mysterious platform where cybercriminals roam. The general public is familiar with, for example, news about illegal arms and drug trafficking and other forms of crime taking place there. What is the current situational picture of the dark web?

In practice, the dark web refers to those parts of the internet that cannot be reached using ordinary web browser tools. Practical examples include Tor and I2P networks, both of which require their own browser. The dark web should be distinguished from the deep web, which means all web content that cannot be directly found by search engines, but is nevertheless accessible with a surface web browser. For example, newspapers behind a paywall, secure databases, intranets of organizations and the content of closed social media profiles belong to the deep web. A caricaturing but functional iceberg analogy is often used for different parts of the internet, where the part visible on the surface depicts the surface net and the parts below the water surface represent the deep and dark web. The proportion of surface web is small both in the picture and in reality. By far the largest is the deep web, which is estimated to cover about 80-90% of all internet content, with the surface and dark web sharing the rest.

The dark web is not a single entity either, but there are several networks, each behind its own browser tool. By far the most popular is the Tor network, which takes its name from the encryption technology it uses. Tor stands for The Onion Router. This is intended to describe how the network is constructed from separate layers like an onion. In practice, it is a complex process in which user traffic is directed through several intermediate points to the desired pages. This connection is almost impossible to trace. The Tor network offers a high level of anonymity and is therefore popular with those who, for one reason or another, need to remain anonymous. In addition to criminals, it also enables anonymous use of the Internet for persecuted political opposition and dissidents, for example.

However, simply opening Tor Browser won't take you to the dark web. With the help of the browser, it is also possible to browse only surface network platforms and take advantage of the high level of encryption brought about by the technology. This is a very popular way to use Tor Browser. While there are no exact statistics on the subject, it's estimated that the majority of Tor Browser users never end up or seek to access the dark side of the web, i.e. sites that can be accessed with Tor Browser alone. On the Tor network, dark web sites can be identified by the extension .onion. One is very likely to come across illegal content on these sites.

The most popular services on both the Tor network and other dark networks are forums related to drug trafficking. However, there are also other types of platforms on the web, such as a dread for general discussion, similar to the Reddit service on the surface web. Unlike its more innocent cousin, it contains mostly criminal or criminal content. Various hacker forums are also popular, where information captured in data breaches is shared, hackers are recruited into groups or information about potential targets is shared.

It is critical for an organization to understand what kind of information about it can be on the dark web. Typically, the issue may be data lost in a data breach, such as usernames and passwords, which may end up being sold on black marketplaces or freely distributed to various aggregate lists. The target of the data breach may have been the organisation itself or its user ID data may have been lost in a data breach targeting another platform to which they have logged in. Discussions about organization or its activities on dark web forums and forums can also be valuable information when mapping one's target profile.

A recent trend has been observed for criminals to move from the dark web to commonly used instant messaging apps such as WhatsApp, Telegram and Signal. This is partly true, but the dark web has stayed alongside, at least for the time being. For example, the Finnish dark web drug marketplace Sipulitie is alive and active. Information shared by instant messengers is also often different for criminal groups than for dark web channels. Hacker groups may report and share information about their operations via instant messengers, not only to make them more accessible, but also to increase their reputation and appear more threatening. The hacker group's scary reputation can increase the likelihood that the victim will be frightened and pay the ransom if they are attacked. Lately activity in instant messengers have also started to include selling criminal services or trading hijacked data, but in quantitative terms this is still low compared to dark web platforms, where internal communication and operational planning are usually done.

As a whole, one should at least be aware of the threat posed by the dark web, as it can pose threats to an organization regardless of its size and industry. However, diving into the dark web on your own should be carefully considered. While downloading and using Tor browser, for example, does not pose a risk per se, an inexperienced dark web user is at great risk of accidentally coming across illegal content and of being the victim of a scam, data breach or crime themselves.

THE DARK SIDE OF YOUNG PEOPLE'S ONLINE BEHAVIOUR

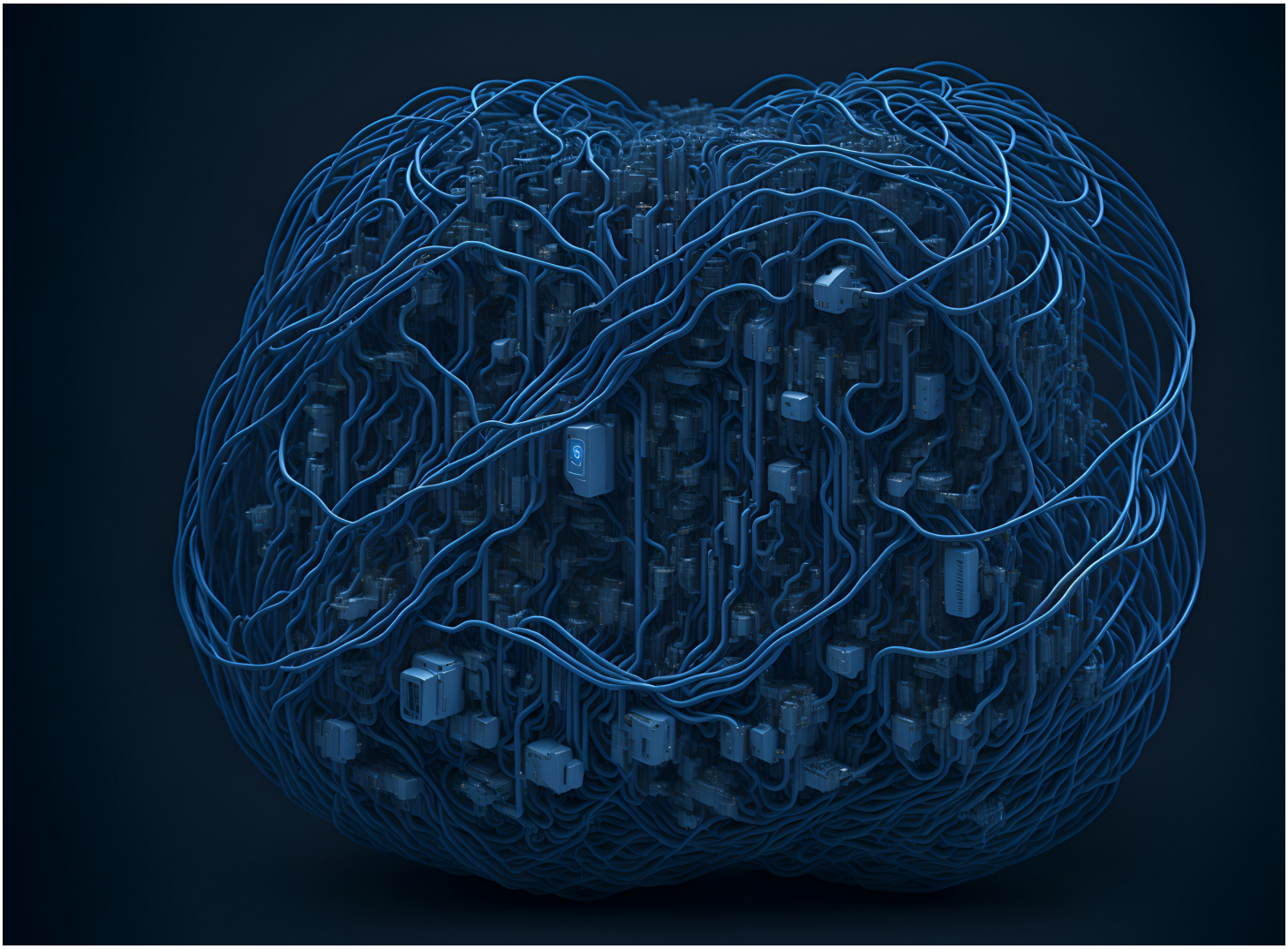
When talking about cybercrime, the personal profiles of the perpetrators are often forgotten in the discussion. Instead, the focus is on how the attacks are carried out, and the attacks themselves are primarily attributed to, for example, state APT actors or pseudonymous hacker gangs. However, cybercrime is not always faceless, and often faces are also amazingly young. There have been several examples in recent years where minors or young perpetrators have committed cybercrimes. Other disruptive online behaviour is also common among young people.

There are many statistics and assessments on young people's online behaviour and cybercrime. For example, according to a 2022 study published by the University of East London, up to two-thirds of Europeans aged 16-19 have been involved in malicious online behaviour or cybercrime. Of course, the study was limited, as it did not distinguish between actual crimes and malicious online behaviour, which included sending so-called "spam messages", cyberbullying, identity theft and cyberfraud. According to another estimate, the UK's National Crime Agency, as many as one in five children between the ages of 10 and 16 are involved in some form of illegal online activity. The amounts are significant in both cases, but it is necessary to distinguish between unequivocally illegal and purely 'harmful' acts. Also significant is the division into cyber-assisted and cyber-related crimes, both of which young people can commit. Cyber-assisted crimes mean traditional crimes committed using the network. These include, for example, various frauds, identity theft and defamation, which account for the majority of cybercrimes. Cyber-related crimes, on the other hand, can only be committed using computers and information networks, and they also target information networks and information systems. Typical examples are data breaches and traffic jamming, the most common form of the latter being a denial-of-service attack. According to the Finnish National Bureau of Investigation, it is one of the most common cybercrimes committed by young people.

The usual path to cyber-related crimes is through the child's or young person's interest in information technology, which may later turn into illegal online activities. According to Europol's research, important background factors are the various groups to which people belong online. Peer pressure, community encouragement or want of fame can motivate criminal acts. The web can also be understood as a place where surveillance and law do not extend to, and where parents have neither sight nor power. In addition, it is typical that the consequences of actions are not fully understood or attacks are perceived as funny tricks or, for example, "trolling". The consequences of attacks and possible financial consequences may come as a surprise to the young person as well as to the parents. Often there is no other criminal activity linked to cybercrime.

There are many examples of serious cybercrimes committed by young people around the world. In recent years, the most significant has been the activities of the Lapsus$ hacker group. In the case of Lapsus, the group managed to hack the website of the Brazilian Ministry of Health and steal up to 50 terabits worth of data from the ministry's servers. Other notable attacks by the group included attacks on tech giants Nvidia and Samsung, both of which ended up in the group's hands with valuable data from the companies. Eventually, a successful international operation by the authorities brought the operation to an end and led to the arrest of seven young people between the ages of 16 and 21. The main perpetrators of the group were considered to be a 16-year-old British teenager and a Brazilian teenager, whose exact age has not been disclosed. As a whole, the group's activities caused millions in damages to the companies affected, but the exact amount of ransom money seized by the group has not been made public. In addition to financial motives, the activities also seemed to be driven by the hacking and fame pursuit of the highest possible profile.

In Finland, the problem has been tackled, for example, through the Cybercrime Exit project organised by the Finnish National Bureau of Investigation (Keskusrikospoliisi, KRP), which aims to prevent serious cybercrime among young people. Young people can apply for exit activities themselves or be guided to them by a professional, for example. Key means of preventing cybercrime can be identifying young people at risk and, in general, raising young people's awareness of the damage caused by cybercrime and the consequences of its actions. At the same time, young people should be supported, encouraged and guided to use their interest in technology and skills correctly and for acceptable purposes.



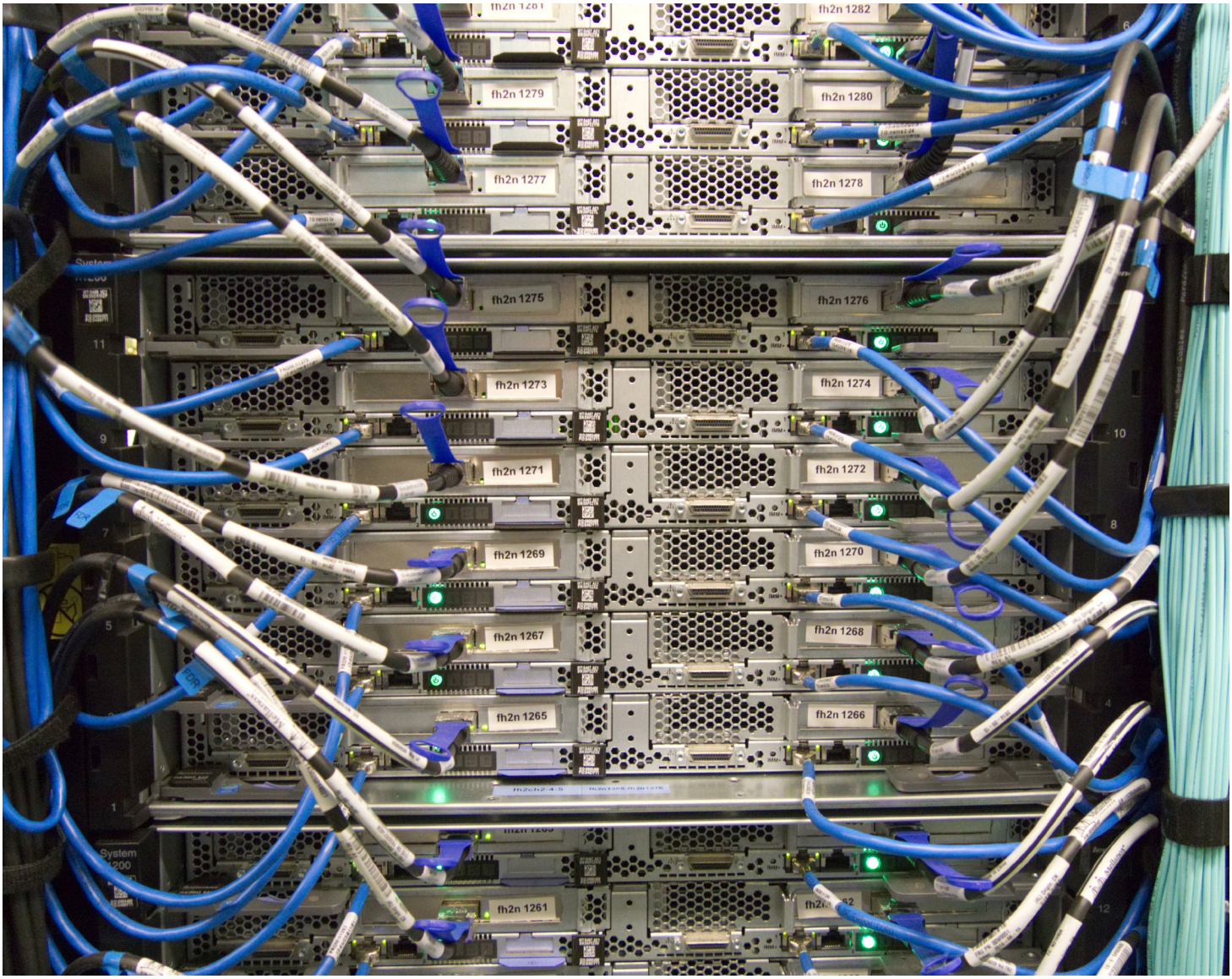
ROUTERS AND NETWORK EDGE DEVICES AS THREATS

In simplified terms, a network device vulnerability refers to a security vulnerability found in the device or the system it uses. These gaps are constantly being discovered and are being filled by equipment manufacturers as observations come in. However, pending a corrective update, the vulnerability is open to an attacker. It can take time for an update to be prepared and, in particular, for it to reach end users' devices. The most critical environments and the network devices connected to them are often updated quickly, but the delay may be longer for devices operating at the edges of the network infrastructure and in less important locations.

Modems or other network devices are very often the first target of a cyberattacker. Poorly secured or unupdated devices are attractive targets and can be found in both homes and organizational premises. For example, poor protection can be caused by a device being forgotten, that is, it has been removed from active use but still remains operational and connected to the internet. It is also common that a modem in active use simply has not been remembered to update. Very often it is both of these. Vulnerable network devices are rarely at the heart of an organization's network infrastructure, but open devices lurking on its edges are also a good first target for an attacker. By breaking into these, it is often possible to continue the attack further deeper into the network. A forgotten device can also contain valuable data in itself, such as decomissioned databases or backups.

Vulnerable network edge devices are used in attacks by state-motivated APT actors, aiming at cyber espionage or cyber sabotage, as well as purely financially motivated hackers in an attempt to find a way to infect the ransomware target. Threat actors have been found to actively monitor manufacturers' update logs because a quick attack can often strike before everyone can install the update. Another reason to monitor logs is that criminals may then become aware that a vulnerability that was already known to them has now been discovered, and as a result, previously undetected operations will soon be detected or stopped when the gap is filled. This, too, could accelerate action when hiding in target networks would soon come to an end anyway.

Last week, the topic made headlines both in Finland and internationally when news broke about a vulnerability found in the firewall of Palo Alto Networks' network devices. This was classified as a highly critical vulnerability, and shortly after the manufacturer's announcement, reports began to emerge around the world of ongoing



exploits of the vulnerability. Palo Alto's devices are also widely used in Finland, and the National Cyber Security Centre issued an official warning on the matter. The severity of the threat is probably indicated by the fact that the last such warning was issued about two years ago, even though vulnerabilities in network equipment are detected almost weekly. The National Cyber Security Centre (NCC) has previously warned of vulnerable network edge devices, although not in connection with a concrete threat. Last autumn, Finnish Intelligence Service Suojelupoliisi (Supo) also warned about vulnerable modems and routers and this received a lot of media attention at the time. In Supo's publication vulnerable devices were even identified as a threat to national security, and their owners, both citizens and organisations, must ensure that they are protected.

In network devices, the most concrete threats concern forgotten and old devices for which security updates may no longer be available. So one needs to make sure that the devices are new enough to receive updates and that they are installed quickly. For individual users, one only needs to worry about this if the device has been purchased directly from a store and not provided by an internet service provider. In Finland, network operators usually take care of updating the equipment they supply, but if the router or modem was purchased by a customer themselves, no one is likely to take care of its up-to-dateness. For organizations, it is also critical to know their own network infrastructure and what devices are used in which configurations. The NCC may also contact organizations that it knows or detects are using vulnerable devices. According to the center, it's not uncommon for the first reaction on the other end of the phone to be amazement that such would be in use. Organizations responsible for their infrastructure must maintain an active situational awareness of what devices are in use and what kind of updates are available for them. Device manufacturers' websites usually provide the latest updates, and vulnerabilities are reported by many authorities based on information provided by CISA, the U.S. cybersecurity agency. Since criminals also monitor published vulnerabilities, there is less time for their own actions. Being active in monitoring information and prompt updates reduce the vulnerability area and thus the risk of being attacked.

REFERENCES:

MYSTERIOUS DARK WEB

https://www.kaspersky.com/resource-center/threats/deep-web

https://www.stealthmole.com/blog/telegram-channel-for-fraud-and-cybercrime#why-do-cybercriminals-use-telegram

https://flare.io/learn/resources/blog/dark-web-forums/

THE DARK SIDE OF YOUNG PEOPLE'S ONLINE BEHAVIOUR

Nuoret ja kyberrikollisuus: KRP:n CyberCrime Exit-hanke - Miten Keskusrikospoliisi ehkäisee nuorten vakavaa tietoverkkorikollisuutta. Viivi Lehtinen, Keskusrikospoliisi. Presentation at Digiturvamessut-convention in Jyväskylä 18.4.2024.

https://cybernews.com/editorial/teen-cyber-cartels/

https://poliisi.fi/cybercrime-exit

https://uel.ac.uk/about-uel/news/2022/december/two-thirds-european-youth-involved-some-form-cybercrime-online-risk-taking

https://www.bbc.com/news/technology-60864283

https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

https://www.cybereason.com/blog/lapsus-activity-betrays-nation-state-motivation

https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf

https://www.nationalcrimeagency.gov.uk/news/one-in-five-children-found-to-engage-in-illegal-activity-online

https://www.reuters.com/technology/cybersecurity/lapsus-hacker-who-targeted-uber-grand-theft-auto-maker-indefinitely-detained-2023-12-21/

ROUTERS AND NETWORK EDGE DEVICES AS THREATS

https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter

https://www.securityweek.com/thousands-of-palo-alto-firewalls-potentially-impacted-by-exploited-vulnerability/

https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoja-palo-alto-globalprotect-tuotteisiin-vaatii-valittomia-toimia

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena

https://yle.fi/a/74-20054897

Kiristyshaittaohjelmat, palvelunestohyökkäykset. Missä mennään tällä hetkellä? Matias Mesiä, tietoturva-asiantuntija & Helinä Turunen, erityisasiantuntija, Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Presentation at Digiturvamessut-convention in Jyväskylä 18.4.2024.

Cyberwatch Weekly

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Pixabay
Unsplash

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi