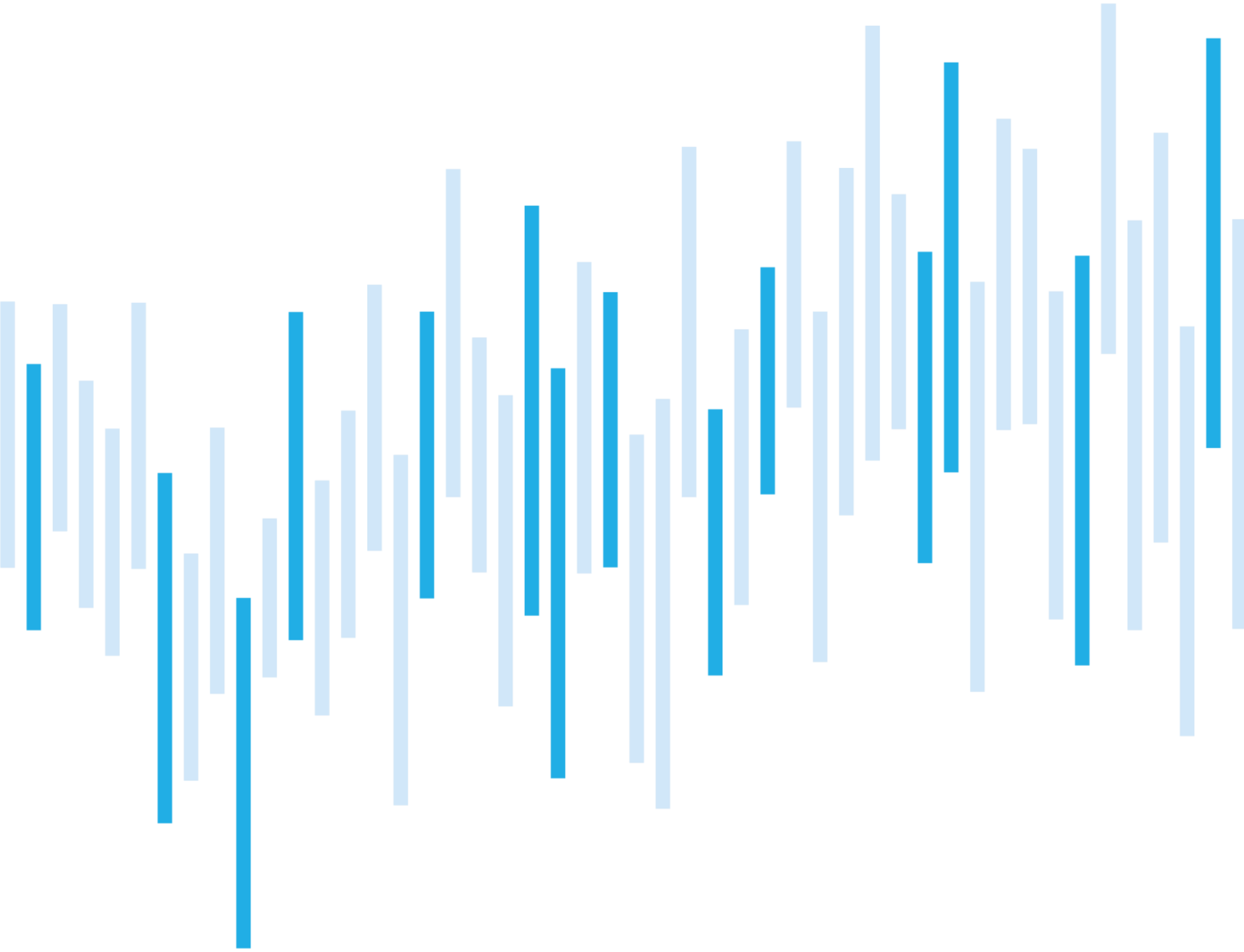
CYBER SECURITY INCIDENTS FROM THE NÚKIB’S PERSPECTIVE

APRIL 2022



National
Cyber and Information
Security Agency

Summary of the month

April was a month with the second highest number of incidents in the last twelve months. Compared to the previous months, the number of organisations that notified NÚKIB about an incident has grown by one-fifth.

The growth in the number of incidents was mainly caused by a campaign led by a pro-Russian hacktivist group known as Killnet. NÚKIB was notified about associated cyber incidents by seven organisations. The attacks were generally less sophisticated, causing the unavailability of web pages. The group did not compromise the information systems of their targets and hence did not access the data stored in them. It is likely that Killnet's motivation was to harm the reputation of its targets.

The attacks are likely to be associated with the Czech Republic's support to Ukraine. Killnet is a Russian-speaking group and based on its statements, supports the Russian Federation. Since the beginning of the invasion, the group has attacked not only organisations and governmental institutions in the Czech Republic but also other NATO states and Ukraine. The DDoS attacks in partner states coincided with important events, typically military or humanitarian support to Ukraine. The attacks in the Czech Republic were no exception in this regard.

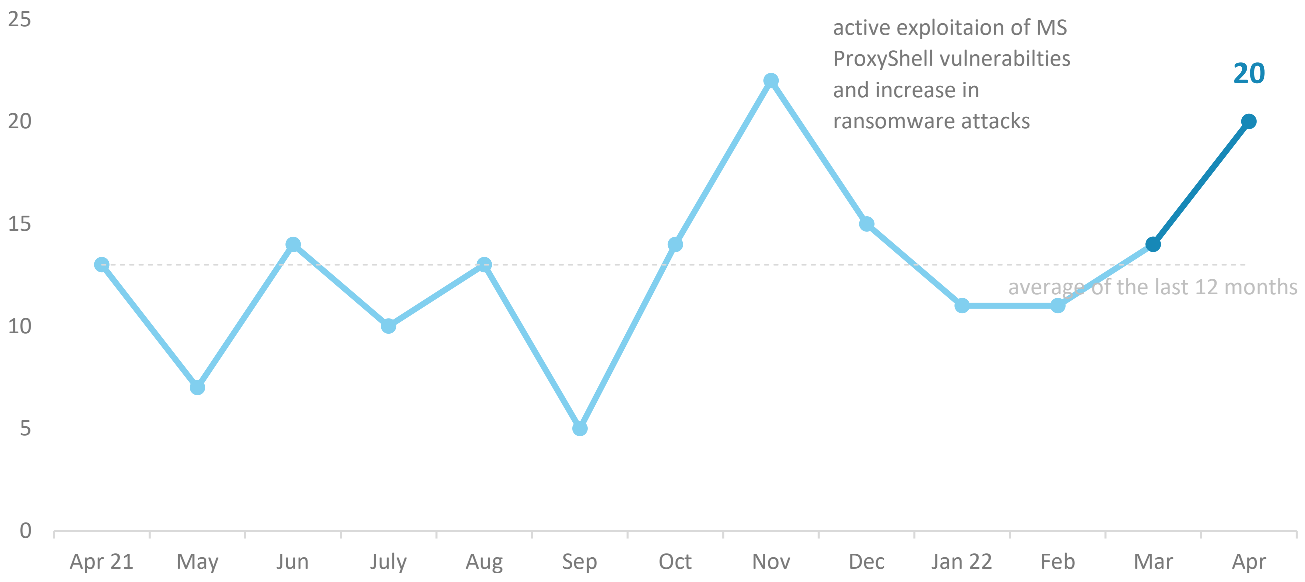
Table of contents

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. Where the report contains information from open sources in some sections, the source of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.cz.

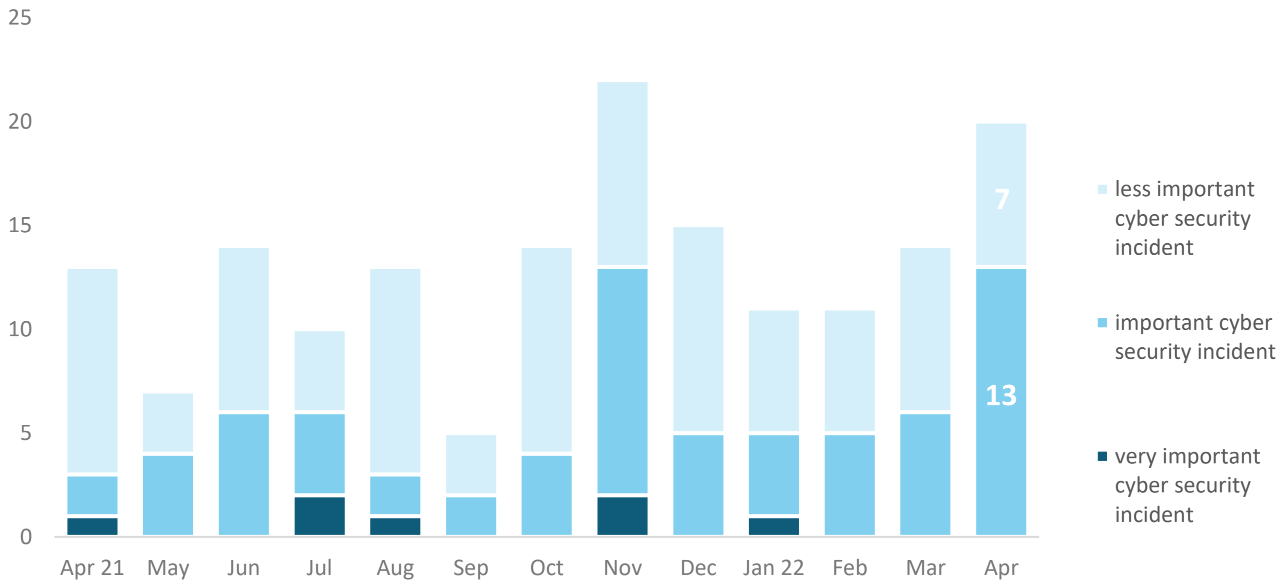
Number of cyber security incidents reported to NÚKIB

April was a month with the second highest number of incidents in the last twelve months. It was only surpassed by November when the ProxyShell vulnerability was actively abused.[1]



Severity of the handled cyber incidents[2]

Two-thirds of April's incidents had significant impacts. They were mainly caused by DDoS attacks, which, among others, targeted important state institutions, and ransomware, which attacked smaller non-regulated entities.



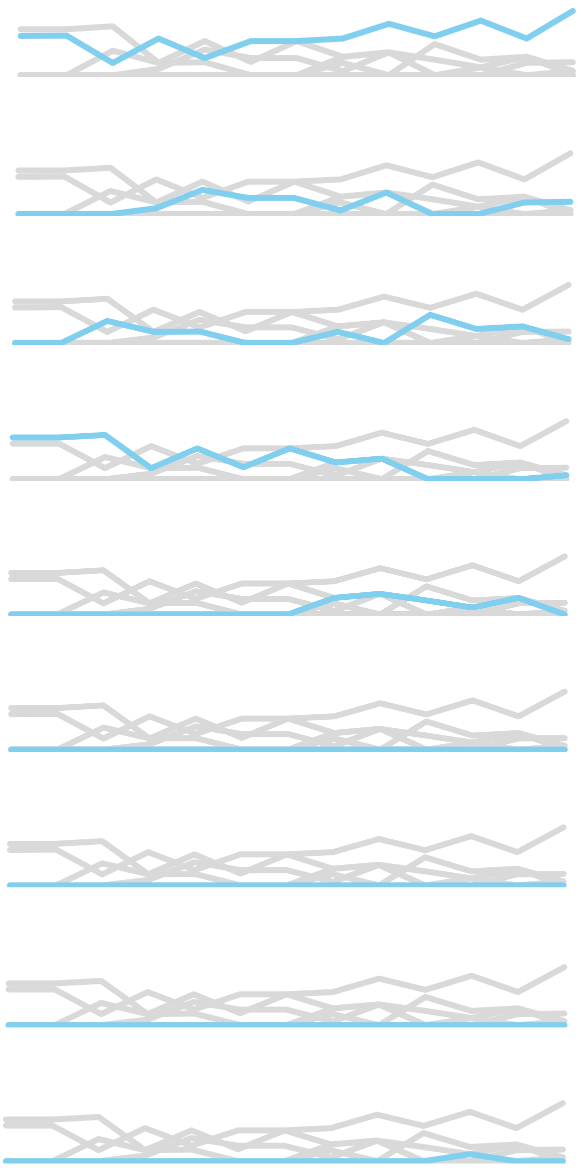
[1] Thirteen incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining seven incidents were reported by entities that do not fall under this law.

[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified April’s incidents within the following four categories:

- Three-quarters of all the incidents resulted in the unavailability of services. Seven of these incidents were caused by DDoS attacks, which had only represented a minor part of the incidents reported to NÚKIB in the preceding months. Ransomware and cryptomining malware had adverse effects on availability in five cases; in three incidents, the service unavailability was caused by a technical failure;
- The second most frequent category included incidents with unauthorised access to information. One of them was an attack against a local authority’s database, whose content the attackers stole. The attackers have not published the data so far; nevertheless, its publishing cannot be ruled out in the near future;
- NÚKIB classified one attack as fraud. The attackers probably compromised an e-mail account of an important state institution’s employee. subsequently, they sent phishing e-mails with diplomatic theme from the e-mail account to governmental organisations in other European countries (see page 4);
- The last remaining April’s incident was classified by NÚKIB within the malicious code category after NÚKIB had found elements of a Czech company’s infrastructure communicating with Emotet malware control servers.



	April 2021	April 2022
Availability e.g. availability disruption caused by a DoS/DDoS attack or sabotage	46 %	**75 %**
Information security e.g. unauthorised access to data, unauth. modification of information	0 %	**15 %**
Fraud e.g. phishing, identity theft or unauthorised use of ICT	0 %	**5 %**
Malicious code e.g. virus, worm, Trojan, dialer, spyware	54 %	**5 %**
Intrusion e.g. compromising an application or user account	0 %	0 %
Intrusion attempts e.g. attempt to exploit a vulnerability, attempt to log in, etc	0 %	0 %
Information gathering e.g. scanning, sniffing, social engineering	0 %	0 %
Abusive content e.g. spam, cyberbullying, inappropriate content	0 %	0 %
Other	0 %	0 %

[3] The cyber incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu)

April trends in cyber security from the NÚKIB's perspective[4]

Phishing, spear-phishing, and social engineering

One of April's incidents involved an intercepted phishing e-mail that the attackers were sending from an infected e-mail of a state organisation's employee. The phishing had diplomatic theme and was sent from the Czech e-mail address to another nearly 200 addresses of governmental organisations in European countries.

As fraudulent vishing phone calls continue, NÚKIB drew attention to this campaign again. The alert on our website lists features typical for this wave.

Vulnerabilities

In April, a new critical vulnerability of VMware Workspace ONE Access and Identity Manager (CVE-2022-22954) products appeared. This vulnerability enables an attacker to bypass authentication mechanisms and remotely upload a malicious code onto a server. Since attackers instantly started to exploit the vulnerability, NÚKIB warned the regulated subjects with vulnerable systems about the problem and sent them recommendations regarding its mitigation.

Attacks on availability

In the last twelve months, DDoS attacks had only represented a minor part of the incidents registered by NÚKIB. The situation changed in April, though. More than one-third of the incidents were caused by DDoS attacks launched against Czech targets by Killnet, a pro-Russian hacker group (for more information, see page 6). In some cases, DDoS attacks took down web pages for several hours. NÚKIB was notified about such incidents by seven organisations regulated under the Cyber Security Act; however, the actual number of Killnet's Czech victims was approximately three times higher.

Malware

Within the scope of its pro-active activities (known as threat hunting), NÚKIB uncovered an infrastructure of a Czech company hat communicated with Emotet C2 server. Attackers deploy Emotet as a first stage payload, which is often spread by phishing. Upon compromising the victim's network, Emotet downloads other malware. Emotet is currently active in the Czech Republic. Since last autumn, when Emotet re-appeared on the cybersecurity scene, NÚKIB has been finding Czech companies infected with this malware.

Ransomware

Since the beginning of the year, ransomware attacks have constantly amounted to approximately one-fifth of the incidents registered by NÚKIB. This trend continued in April. The Phobos ransomware was behind the majority of attacks. Phobos primarily aims at smaller and more vulnerable targets. It regularly appears among the incidents reported to NÚKIB. One of April's incidents also involved LokiLocker, which is quite a new ransomware offered as a service; it started to spread in the summer of 2021, and this was its second occurrence reported to NÚKIB so far.

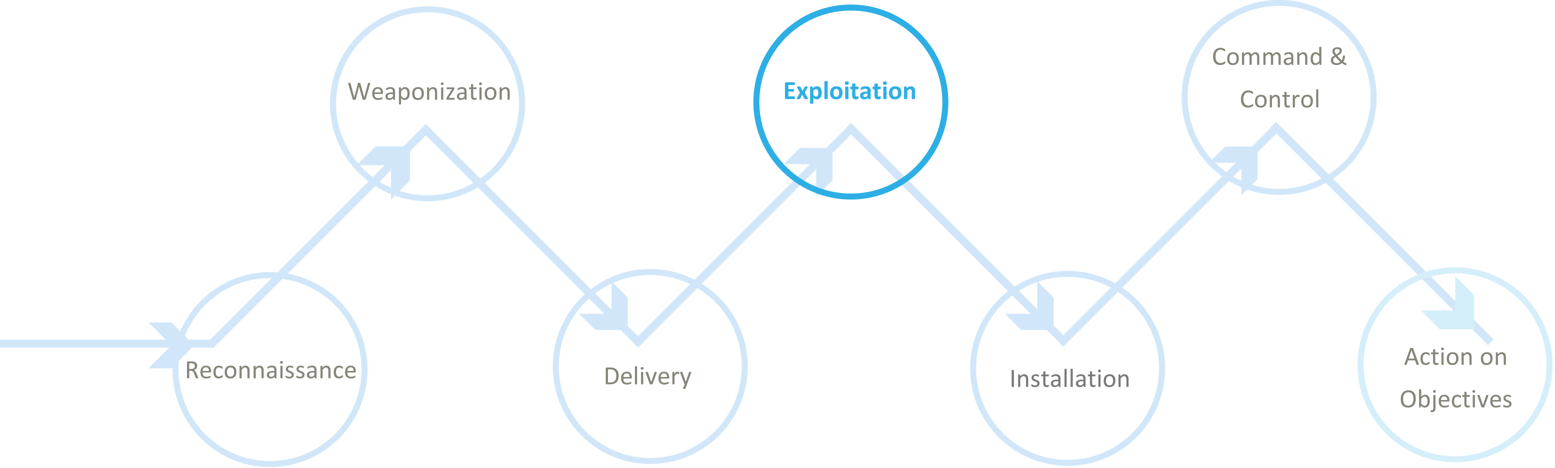
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Technique of the month: Malicious File

NÚKIB also evaluates cyber incidents on the basis of the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in cyber attacks. The prevailing method among April's incidents was Malicious File, which is a method employed by most APT and cybercriminal groups in their campaigns and which is a common part of phishing attacks.

> With **Malicious File**, attackers rely on a user to open a file and run the malicious code. This method is typical for spear-phishing e-mails, for example, which try to persuade the user to open an infected attachment and thereby launch the malicious code hidden in it. Among April's incidents, the Malicious File method was most often reported in connection with phishing. The attackers used the method in the initial stages of cyberattacks; however, it can also be used later when the attackers are already present in the victim's network. After compromising the network, they can create a file, save it on a shared disc and wait until other users open it and enable them lateral movement.
>
> **MITRE ID:** T1204.002
>
> **Mitigation:** The T1204.002 technique can be mitigated at two levels. At the technical level, sandboxing of attachments, at least in the case of potentially problematic file types (zip, exe, ps1, and js) and warning users about password-protected archives are suitable measures. The most frequently abused method in connection with malicious attachments is still macros in Office documents. At the level of technical measures, this attack vector can be most easily prevented via domain policies by blocking macro functions for users that do not need them for their work. Yet technical measures alone are not enough. It is essential to train users continuously and draw their attention to the risks associated with social engineering and the latest trends in phishing so that they are able to detect them themselves.

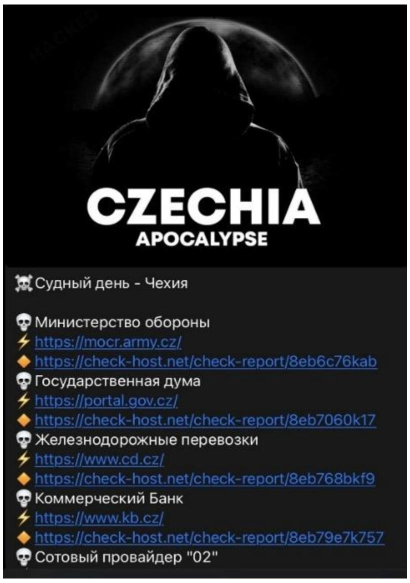
A representation of the Malicious File in the Kill Chain showing at which point attackers use the technique:



Focus on a threat: DDoS campaign launched by Killnet

In the second half of April, a pro-Russian hacker group known as Killnet launched two series of DDoS attacks against webpages of Czech subjects. The attacks are likely connected to the Czech Republic's support to Ukraine.

Fig. 1: Killnet's telegram account



☠ Судный день - Чехия

💀 Министерство обороны
⚡ https://mocr.army.cz/
🔶 https://check-host.net/check-report/8eb6c76kab
💀 Государственная дума
⚡ https://portal.gov.cz/
🔶 https://check-host.net/check-report/8eb7060k17
💀 Железнодорожные перевозки
⚡ https://www.cd.cz/
🔶 https://check-host.net/check-report/8eb768bkf9
💀 Коммерческий Банк
⚡ https://www.kb.cz/
🔶 https://check-host.net/check-report/8eb79e7k757
💀 Сотовый провайдер "02"

The first wave occurred between 19 and 21 April and affected thirteen subjects, including NÚKIB and Czech Ministries. The beginning of the attacks coincided with the announcement of Ukrainian heavy weaponry being repaired in the Czech Republic. The second wave took place in the night of 27 April, when the attackers launched attacks against another nine subjects. Killnet announced the initiation of the attacks against Czech organisations on its Telegram account (see Figure 1).

The attacks were generally less sophisticated, causing the unavailability of web pages. In principle, DDoS attacks overwhelm a service accessible via the Internet with a flood of traffic but do not compromise the organisation's information systems. Consequently, Killnet did not get to the data stored in the attacked organisations. Its goal probably was to harm the reputation of the attacked organisations.

Technical aspects of the attacks by Killnet

Based on data from one of the incidents, NÚKIB identified the attacks as L4 TCP ACK DDoS. It is an attack on the transport layer that employs TCP ACK or TCP ACK-PUSH segments, which are used to confirm received data in legitimate communication. This sort of attack is more difficult to mitigate since it is not easy to distinguish legitimate ACK packets from the malicious ones. As a result, the computational power of the infrastructure's server or firewall is exhausted due to the heavy traffic of forged communication.

Killnet is a Russian-speaking group that, based on its statements, supports the Russian Federation. This affects its choice of targets. Besides those in the Czech Republic, the group has also attacked organisations and governmental institutions in other NATO states and Ukraine. But for one case, all the attacks were of the DDoS type. An exception was an alleged theft of the Kyiv prosecutor's data, which coincided with the discovery of the Bucha massacre.[5] Bucha falls under the jurisdiction of the prosecution office in the capital of Ukraine. Like in the Czech Republic, the DDoS attacks in other states also coincided with important events, typically military or humanitarian support to Ukraine.

NÚKIB has been pointing out the increased risk of cyberattacks since the beginning of the Russian aggression. On 25 February, NÚKIB issued a Warning, which, among others, contains a whole range of preventive and reactive measures against DDoS attacks. Since the Ukrainian war is very likely to continue affecting the Czech Republic in cyberspace, we draw attention to the Warning again and recommend all organisations to implement the mentioned measures. The document provides a guide on how to prepare for a potential DDoS attack and mitigate one that has already occurred.

[5] Killnet informed about the attack on its Telegram account

Probability terms used

Probability terms and expression of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	25–50 %
Unlikely	15–20 %
Highly unlikely	0–10 %

Conditions for the information use

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website www.nukib.cz). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions
TLP:RED	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.