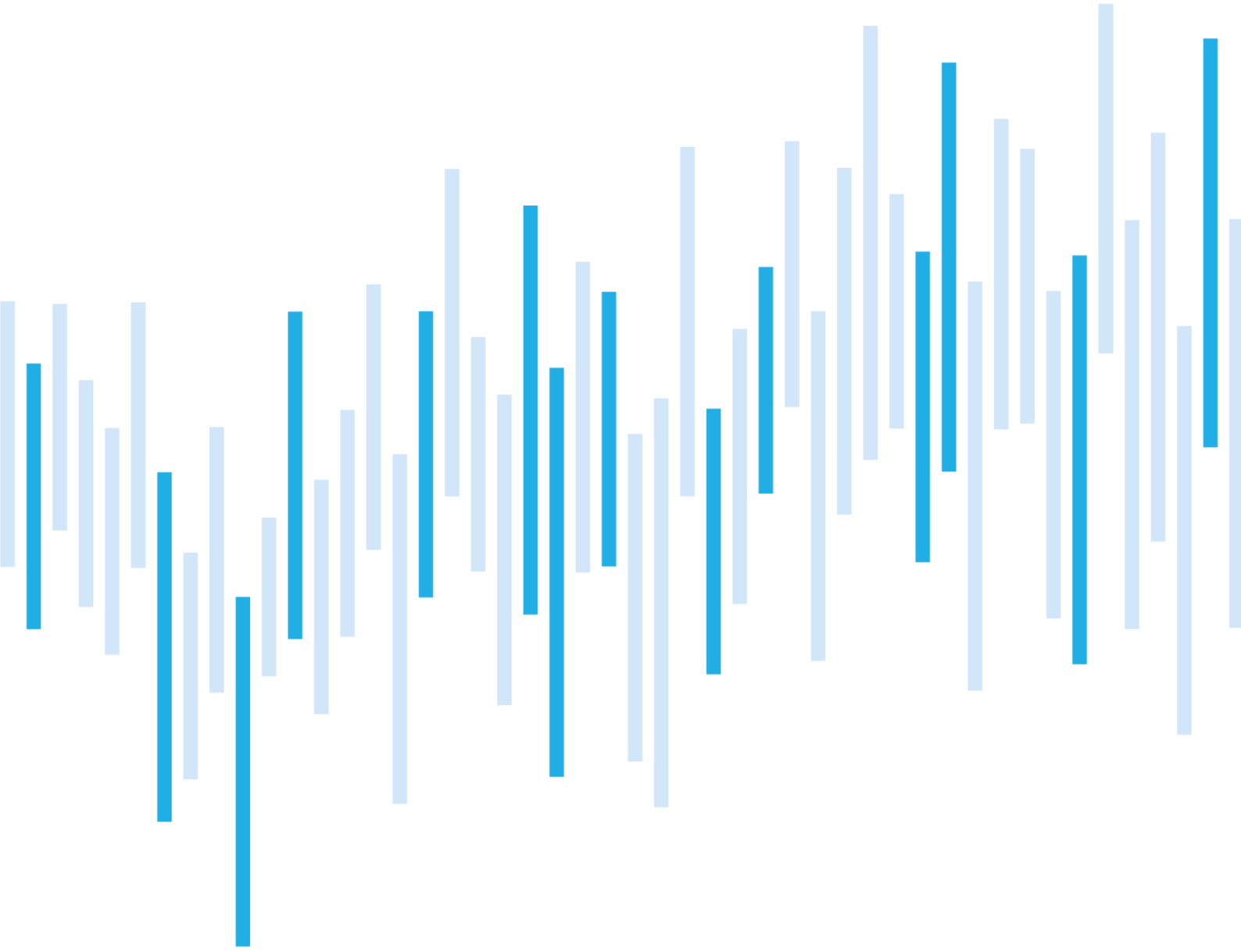
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

AUGUST 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In August, the number of cyber incidents remained well below the average, though it has slightly increased compared to July. NÚKIB typically records fewer incidents during the summer months. Nearly half of the incidents were categorised as significant.

Incidents reported by non-regulated entities significantly prevailed during August. Like in the preceding month, which sector was the most affected cannot be said.

Since a new academic year starts in September, this report focuses on attacks against universities. These are attractive targets for cyber espionage both because they often carry out advanced research of non-public nature as well as for the financial gain opportunities.

Table of contents

Number of cyber incidents reported to NÚKIB

Severity of the handled cyber incidents

Classification of the incidents reported to NÚKIB

August trends in cyber security from the NÚKIB's perspective

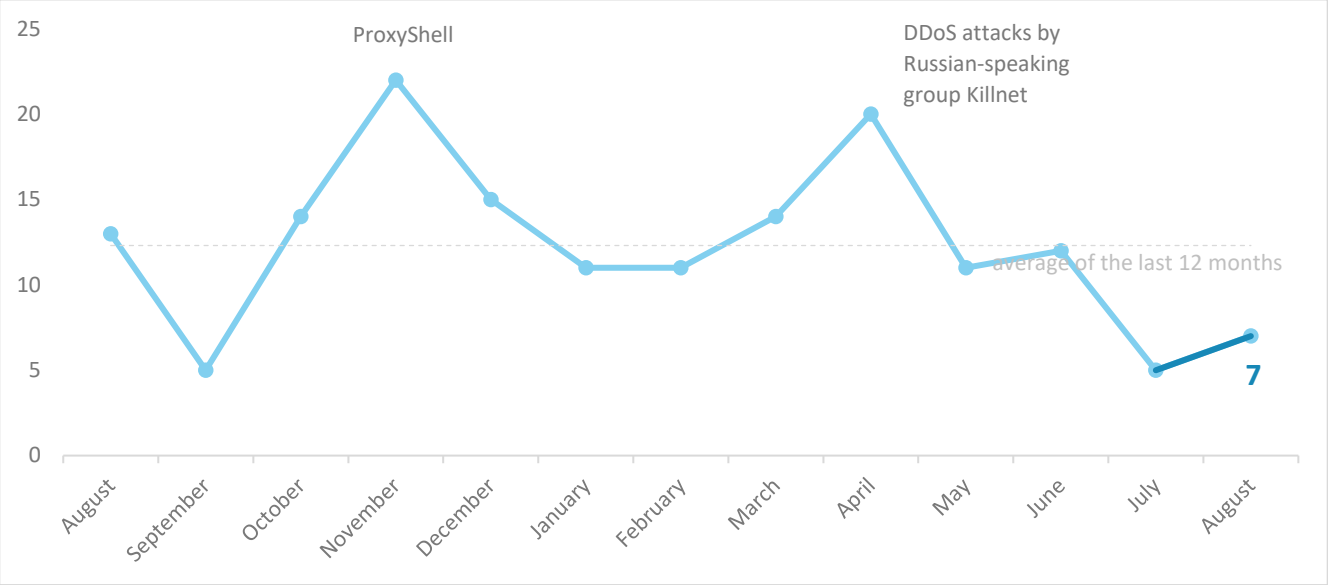
Focused on a trend: Attacks on universities and advanced research

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. If the report contains information from open sources in some sections, the origin of this information is always stated.

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

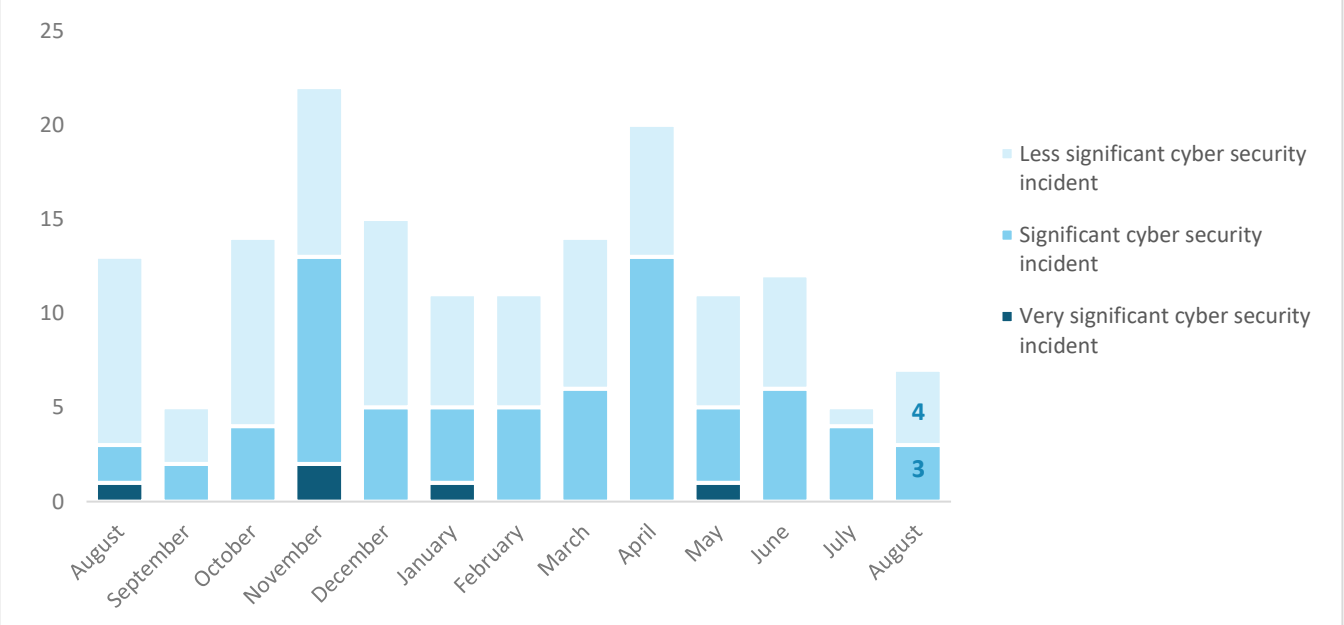
Number of cyber incidents reported to NÚKIB

The number of incidents remained well below the average value during last month. Still, there has been a slight increase compared with July.[1]



Severity of the handled cyber incidents[2]

In August, less significant incidents very slightly outweighed significant incidents. Once again, no very significant incident was registered; the last incident of this classification occurred in May.



[1] Two incidents were reported to NÚKIB by regulated entities according to the Cyber Security Act. The remaining five incidents were reported by entities that do not fall under this law.
[2] NÚKIB determines the severity of cyber incidents based on Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified August's incidents within the following four categories:

- There were attacks on availability again, which is a lasting trend. Two cases of unavailability that occurred in August involved DDoS attacks, and one case was caused by ransomware.
- Penetrations, whose numbers have remained constant since June, also show a steady trend.
- After a month's break, an incident involving malicious code was registered again, specifically ransomware known as Loki Locker.
- Likewise, a fraud-type incident was registered again after a month's break. The incident involved phishing in the Dutch language, which was almost certainly used to harvest credentials.

	August 2021		August 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	31 %		**43 %**
Intrusion e.g., compromising an application or user account	23 %		**29 %**
Fraud e.g., phishing, identity theft or unauth. use of ICT	15 %		**14 %**
Malicious code e.g., virus, worm, trojan, dialer, spyware	15 %		**14 %**
Information Security e.g., unauthorised access to data, unauth. modification of information	15 %		**0 %**
Intrusion attempts e.g., scanning, sniffing, social engineering	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)

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

Phishing, spear-phishing, and social engineering

Phishing and phishing attempts constitute a lasting trend. The most interesting case that occurred in August was phishing written in the Dutch language. It was almost certainly used as a credential harverster.

Malware

NÚKIB did not analyse any malware based on the data from August's incidents.

Vulnerabilities

NÚKIB issued two alerts in August. The first warned about a set of vulnerabilities related to the VMware software and the VMware vRealize Operations platform. There were ten vulnerabilities in total, receiving scores ranging from 4.7 to 9.8 according to the CVSSv3 standard (9-10 is a critical vulnerability). The second alert was issued at the end of the last month and warned about a phishing campaign that attempted to abuse bank identities. It had a theme of alleged financial donation by the Ministry of Labour and Social Affairs.

Ransomware

The trend of ransomware continued in August. The number of registered attacks remained the same, with Hive and Loki Locker ransomware used for the attacks.

Attacks on availability

DDoS attacks were registered for the first time since April. SYN Flood was used in the first case, affecting about 10 thousands users. In the second case, the attack combined TCP SYN Flood, DNS Flood, and ICMP Flood.

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

Technique of the month: Network Denial of Service

Among others, NÚKIB evaluates cyber incidents based on the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in attacks. Considering the re-emergence of DDoS attacks, this month's report focuses on Network Denial Service.

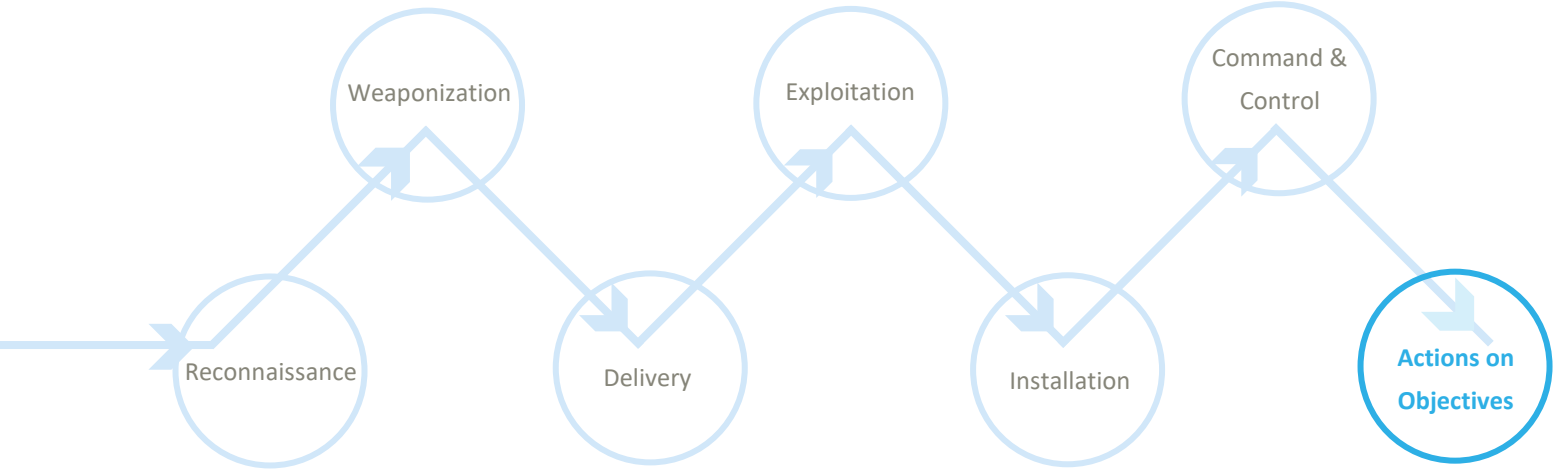
MITRE ID: T1498

Attackers perform Network Denial of Service (DoS) attacks in order to degrade or block availability. This type of attack can be carried out by exhausting the network bandwidth that services rely on. It can affect websites, e-mail services, DNS, or web-based applications. Attackers' motivations vary from political reasons through hacktivism to efforts to divert attention from other attacks.

This attack occurs when attackers exhaust the bandwidth capacity of network with malicious traffic. It can be generated either by a single system (Denial of Service, DoS) or by multiple systems (Distributed Denial Service, DDoS). This type of attack results in limited data availability, but usually does not have longer-term impacts.

Mitigation: Filtering network traffic is a crucial mitigation technique. Malicious traffic should be filtered out from legitimate traffic; it can be performed by internet service providers (ISP) or third parties. Depending on the volume, on-premises filtering can be done by blocking the source addresses that are sources of the attack, targeted ports, and the transfer protocols used.

A representation of the T1498 using a kill chain showing at which point attackers use the technique



Focused on a trend: Attacks on universities and advanced research

As a new academic year is just about to begin, we have decided to focus on a trend of cyber threats targeted at higher education and research carried out in the academic setting.

Fig. 1: Illustrative image of a university

Universities constitute a tempting target due to the range of information they work with. Moreover, a significant part of these information is linked to so far unpublished research. There are often considerable resources in higher education, which make it attractive for attackers motivated by financial gain. Usually, such attackers employ ransomware in their attacks. With thousands and even tens of thousands of users (students), universities are extremely dependent on information systems, which can often suffer ordinary problems (such as obsolete software/hardware versions). Furthermore, users might not have sufficient training.

With the high number of users, it is most efficient for attackers to use (spear)phishing to ensure initial access. Once persistence in the target system is established, the attacker concentrate either on cyber espionage primarily in the area of advanced or so far unpublished research or on encrypting systems with the opportunity of financial gains.

A very specific and still underestimated threat is an attack from inside, i.e. caused by an insider. Likewise, the entities do not realise the risks associated with suppliers.

Recommendation: It is imperative that basic safety standards are observed; some materials prepared by NÚKIB can be used for this purpose (e.g., the Minimum safety standard). Besides, NÚKIB also issued recommendations related to specific threats (e.g., spear-phishing).

Academic institutions should seek to have sufficient human, technical as well as financial resources to be able to create an efficient defence against a wide range of attackers. Considering the extensiveness of systems and the number of users, it is vital to train users regularly. Particular emphasis should be put on protection against insider attacks or compromising through risk suppliers.

Probability terms used

Probability terms and expressions 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	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:AMBER+STRICT	Restricts sharing to the organization only.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.