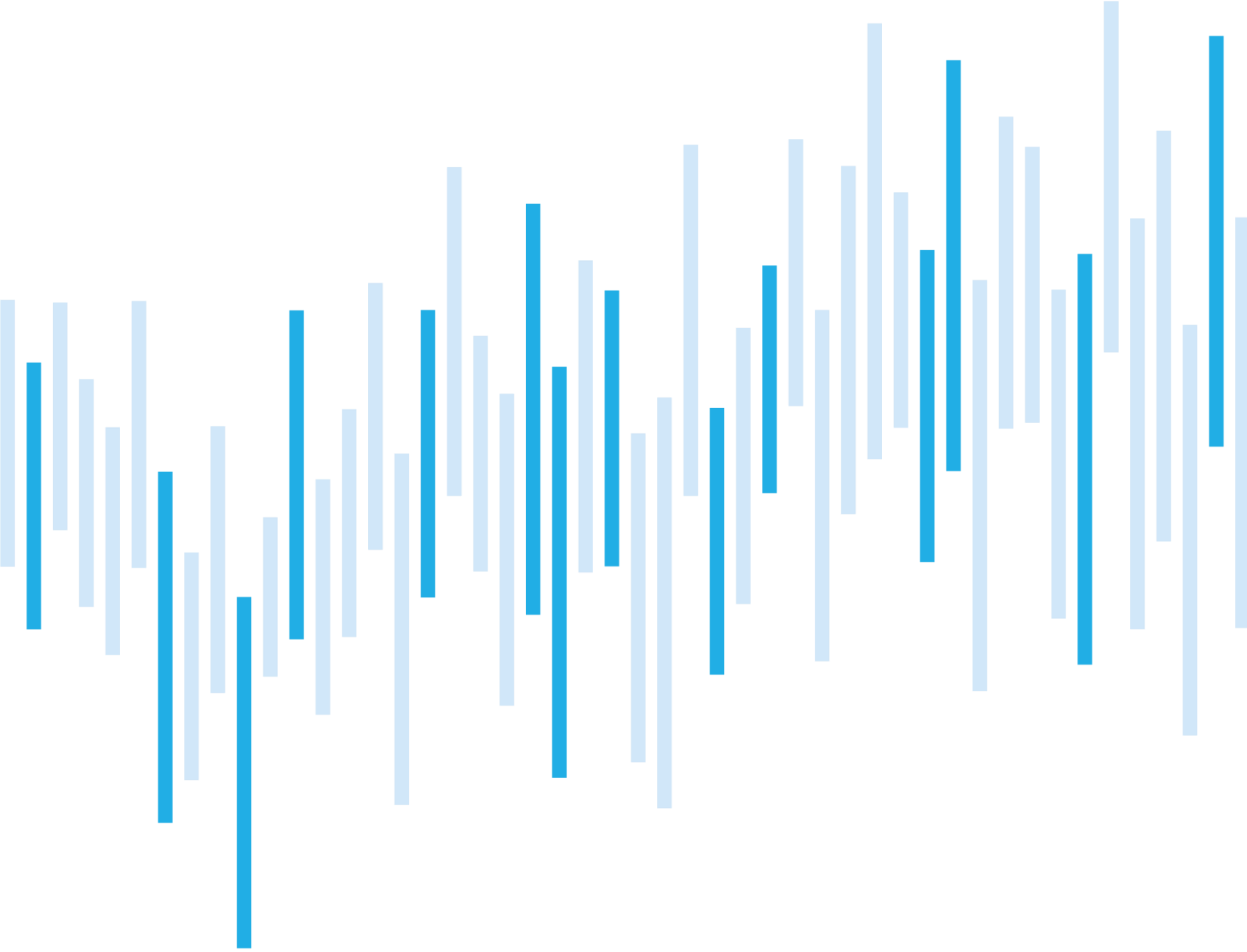
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

# JULY 2023



National Cyber
and Information
Security Agency

## Summary of the month

After a two-month period of above-average incident rates, there was a significant drop in July, which was mainly due to a reduction in the number of registered DDoS attacks. Despite this, incidents falling into the category of availability continued to predominate. However, the majority of incidents of this type were caused by system failures or misconfiguration.

In the chapter *Focus on a Threat* we discuss the topic of phishing campaigns in the Czech Republic. Phishing has long been one of the most frequently used cyber-attack vectors, which is also reflected in its regular occurrence in NÚKIB's recorded incidents. This vector can be deployed either for individual attacks or in phishing campaigns as well.

In July, NÚKIB recorded another phishing campaign against Czech targets using the publicly available Vjw0rm malware. NÚKIB does not currently have information on the actor behind the campaign.

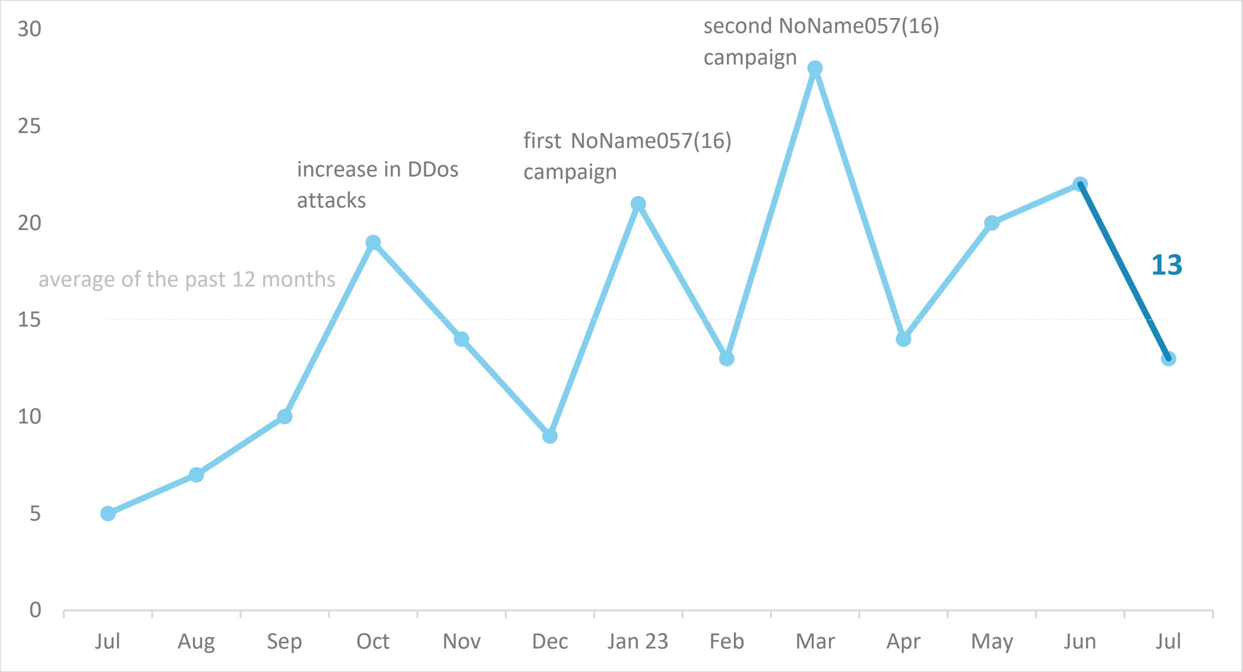
## Table of content

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.

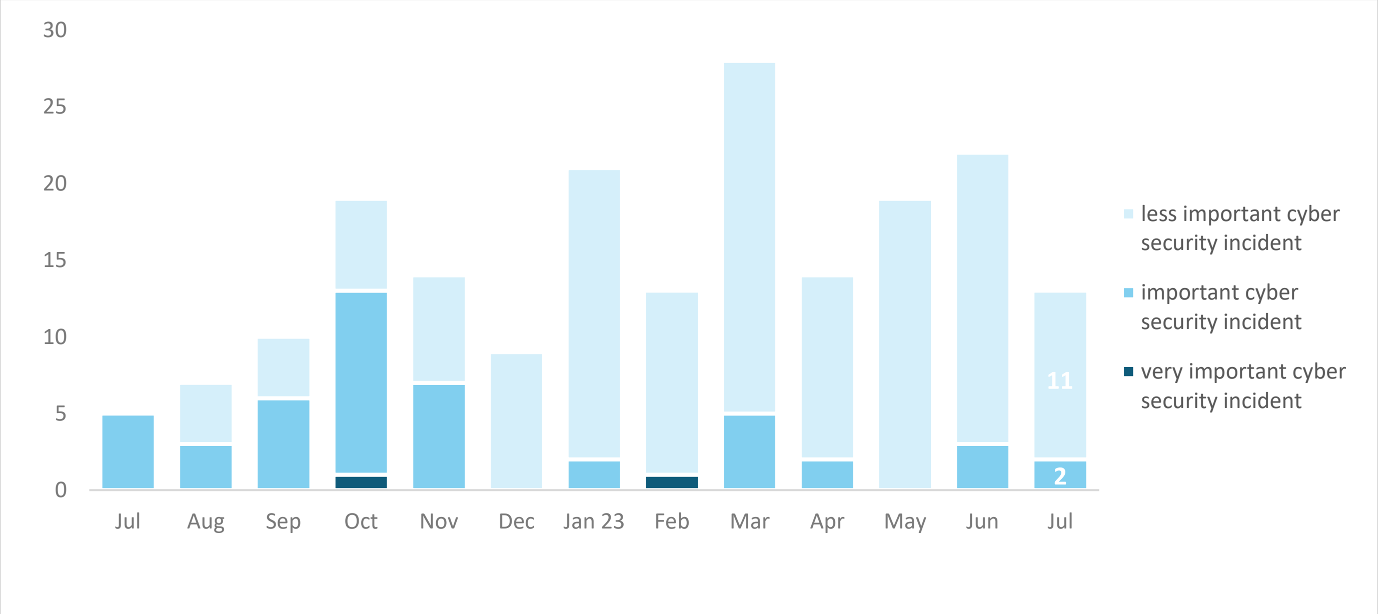
## Number of cyber security incidents reported to NÚKIB

After a two-month period of above-average incident rates, there was a significant drop in July, which was mainly due to a lower number of registered DDoS attacks.[1]



## Severity of the handled cyber security incidents[2]

July became the fifth month in a row when no severe cyber incident was recorded. Only important and less important cyber incidents were recorded, which have long been the predominant cyber incidents on record.



[1] NÚKIB registered 10 incidents in total with liable entities according to Cyber Security Act. The remaining 3 incidents were reported to the NÚKIB by unregulated entities.

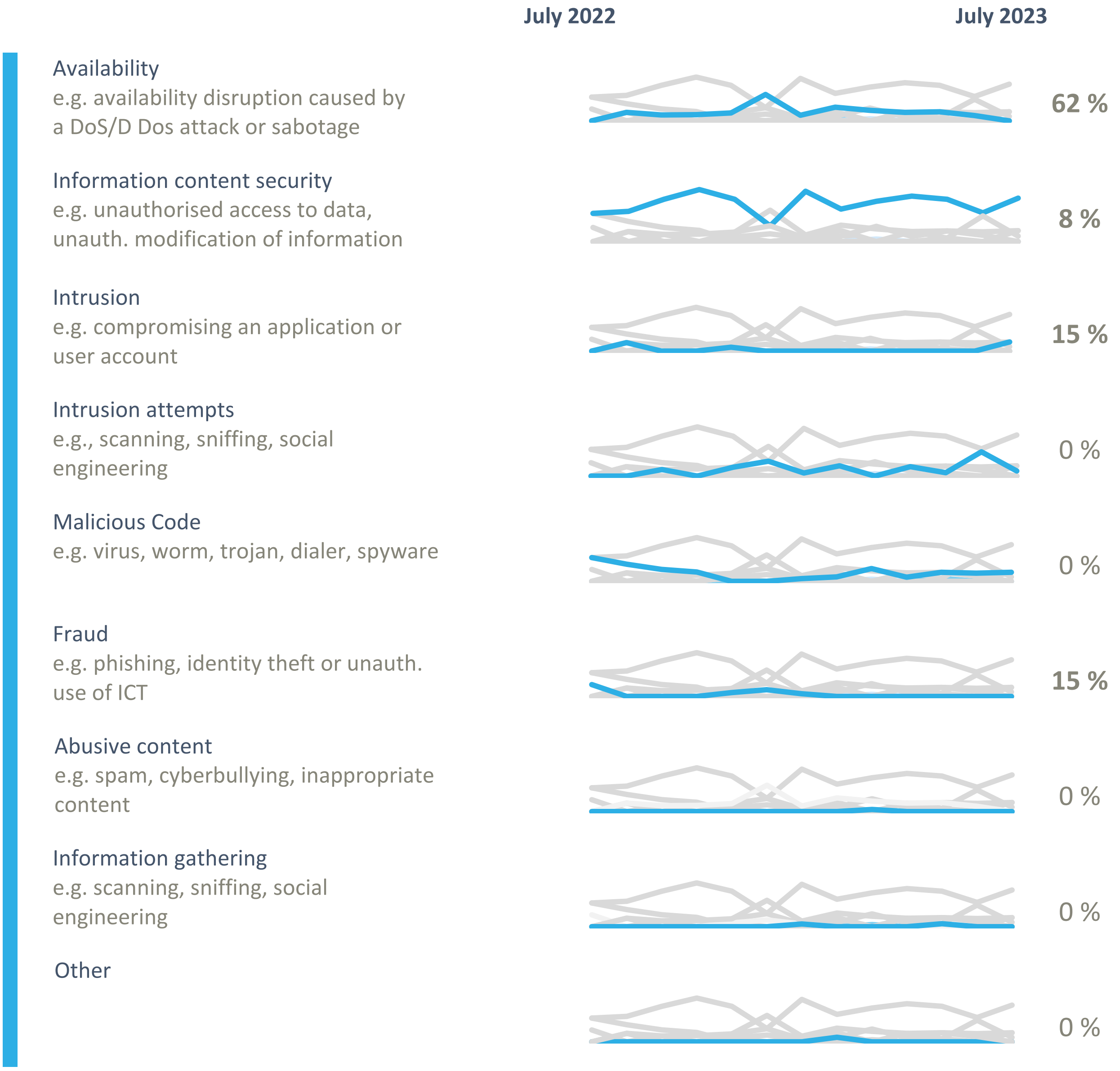
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

## Classification of the incidents reported to NÚKIB[3]

The trend of incidents falling under the category of availability also continued in July. This time, however, the majority of availability-related incidents were caused by system failures or misconfiguration, not DDoS attacks.

In addition to this, NÚKIB dealt with incidents in the following three categories:

- In July, two intrusions were recorded but without significant impacts.
- Two incidents were recorded in the fraud category. During these incidents, the attackers compromised the victims' mailboxes, from which they sent spam or phishing e-mails.
- One Information Security incident was associated with the MedusaLocker ransomware, which led to the encryption of data of an unregulated entity.



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

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

### Phishing, spear-phishing and social engineering ↗

This month, NÚKIB registered two cases of phishing at regulated entities, in which attackers compromised the mailboxes of victims, from which they sent spam or phishing e-mails. In both cases, NÚKIB received information about incidents from the recipients of the phishing, not from the compromised entities.

In addition, NÚKIB registered a phishing campaign, which is detailed in the chapter *Focused on a Threat.*

### Malware →

In July, NÚKIB detected the Vjw0rm malware used in the phishing campaign against, among others, Czech targets. More information about this malware and the phishing campaign itself is provided in the chapter below.

### Vulnerabilities →

NÚKIB issued a warning on a new vulnerability CVE-2023-30799, which affects the MikroTik RouterOS operating system. According to Shodan, up to 24,000 devices from this manufacturer were vulnerable in the Czech Republic at the time of the alert.

### Ransomware ↘

After a growth in ransomware attacks in June, there was a significant drop in July. NÚKIB recorded only one successful ransomware attack. An unregulated entity was hit by MedusaLocker ransomware, which caused a significant amount of internal data to be encrypted.

### Attacks on availability ↘

There was a decrease in recorded DDoS attacks in July. The pro-Russian hacktivist group NoName057(16), which has been regularly targeting Czech targets since January this year, was the originator of all registered DDoS attacks.

Click or tap here to enter text.

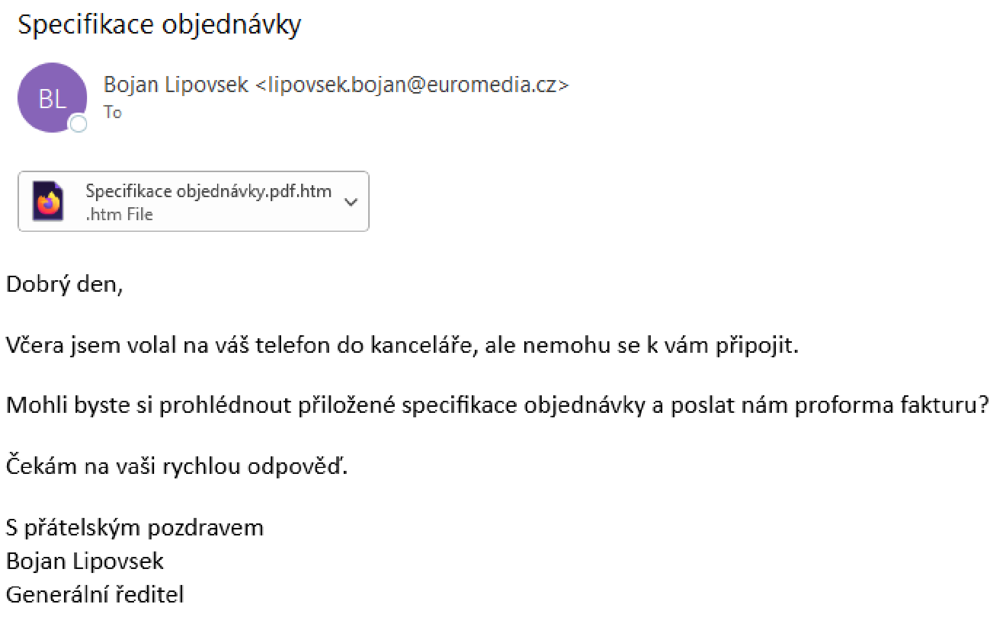
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

## Focus on a threat: Phishing campaigns in the Czech Republic

Phishing has long been one of the most frequently used cyber-attack vectors, which is also reflected in its regular occurrence in the NÚKIB's recorded incidents. This vector can be deployed either for individual attacks or in phishing campaigns focused on higher numbers of targets as well. This year, the NÚKIB has recorded several such widespread phishing campaigns. We can mention, for example, cyber espionage campaigns conducted against Czech and European diplomatic targets, behind which, according to available information, were state-sponsored actors (more see Cyber security incidents from the NÚKIB´s perspective - February 2023 and Cyber security incidents from the NÚKIB´s perspective - April 2023).

In July, NÚKIB registered another phishing campaign targeting Czech entities, which has already been warned about by Aricoma (formerly AEC). According to Aricoma, the campaign is targeting a number of entities not only in the Czech Republic, but also in France, Spain and Russia. As part of this campaign, a fraudulent e-mail with a malicious attachment is sent. This attachment contains a link that downloads a ZIP file containing the Vjw0rm malware.

Figure 1: Example of the campaign's phishing e-mail



Specifikace objednávky

BL Bojan Lipovsek <lipovsek.bojan@euromedia.cz>
To

Specifikace objednávky.pdf.htm
.htm File

Dobrý den,

Včera jsem volal na váš telefon do kanceláře, ale nemohu se k vám připojit.

Mohli byste si prohlédnout přiložené specifikace objednávky a poslat nám proforma fakturu?

Čekám na vaši rychlou odpověď.

S přátelským pozdravem
Bojan Lipovsek
Generální ředitel

Source: aec.cz

Vjw0rm is a publicly available malware that first appeared as early as in November 2016. It is a so-called Remote Access Trojan written in JavaScript that allows an attacker to gain remote access to a victim's device. In the past, Vjw0rm has been exploited by cybercriminal groups such as TA558 or TA2541. At present NÚKIB does not have information about the actor behind the campaign, which is due, among other things, to the public availability of the malware, which makes subsequent attribution difficult.

## 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 % |

## Traffic Light Protocol

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 of use |
|---|---|
| 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+STRICT | Restricts sharing to the organization only. |
| 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: 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/defence 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. |