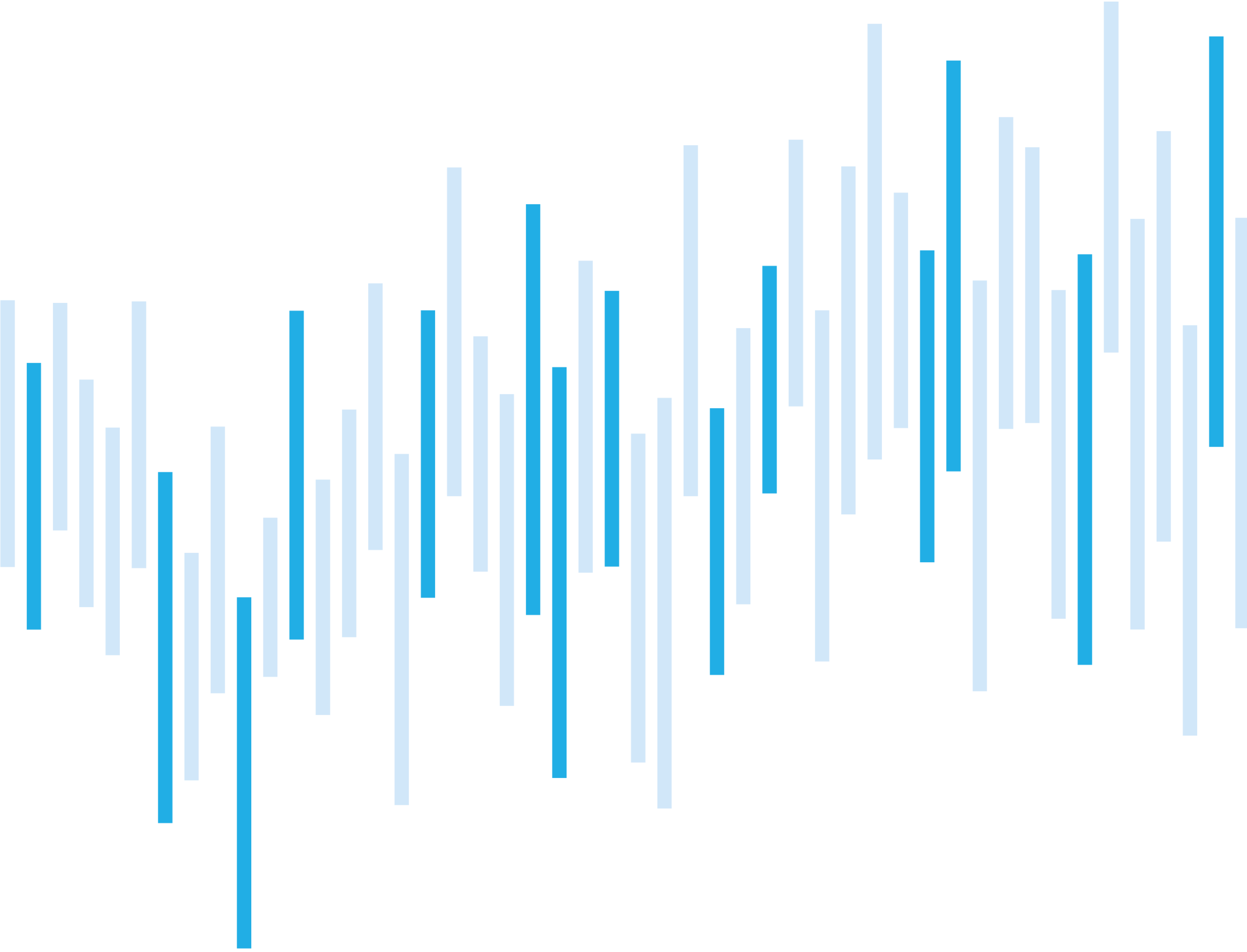
CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

OCTOBER 2023



National Cyber
and Information
Security Agency

Summary of the month

During October, there was again an increase in registered incidents, which for the third month in a row were above the average of the last twelve months. The average monthly number has therefore increased by around six incidents since last October.

As in previous months, the Availability category dominated, where DDoS attacks continued to predominate within the incident classification. However, more than a third of incidents in this category involved outages or misconfigurations. NÚKIB also registered cases of intrusion, fraud, malicious code or incidents in the Information Security category.

In the chapter Focus on a Threat we focus on a vulnerability in WinRAR with the designation CVE-2023-38831. Although this vulnerability was disclosed in August 2023, its more significant exploitation started as late as in September and October.

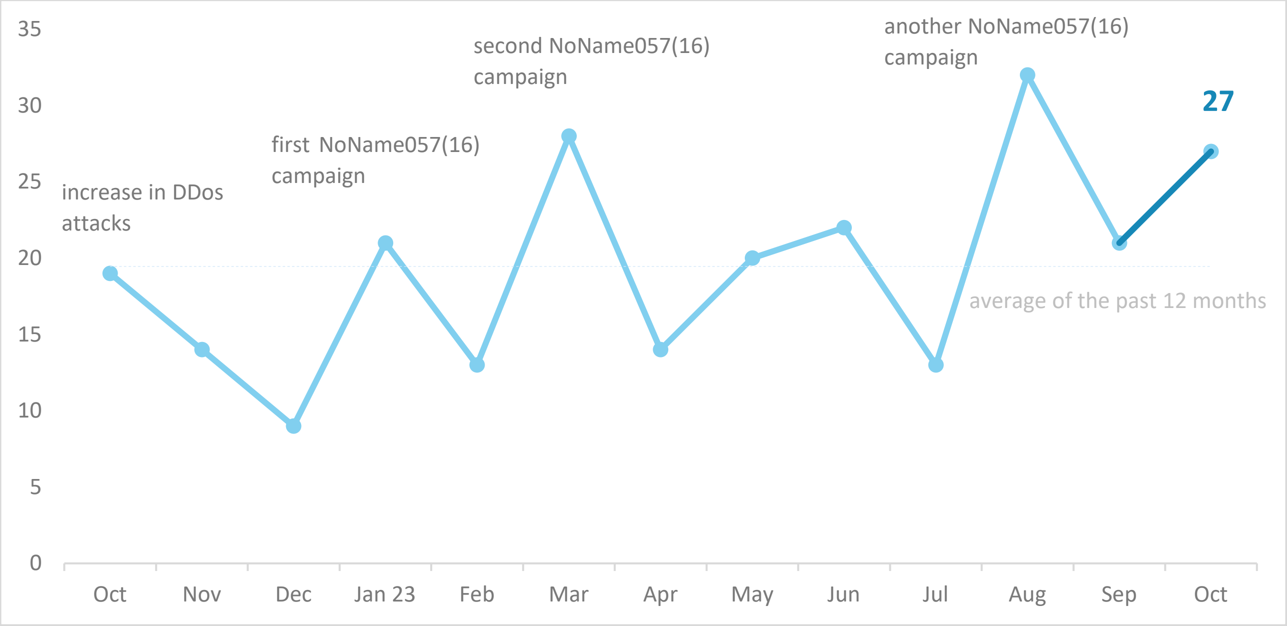
Table of content

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

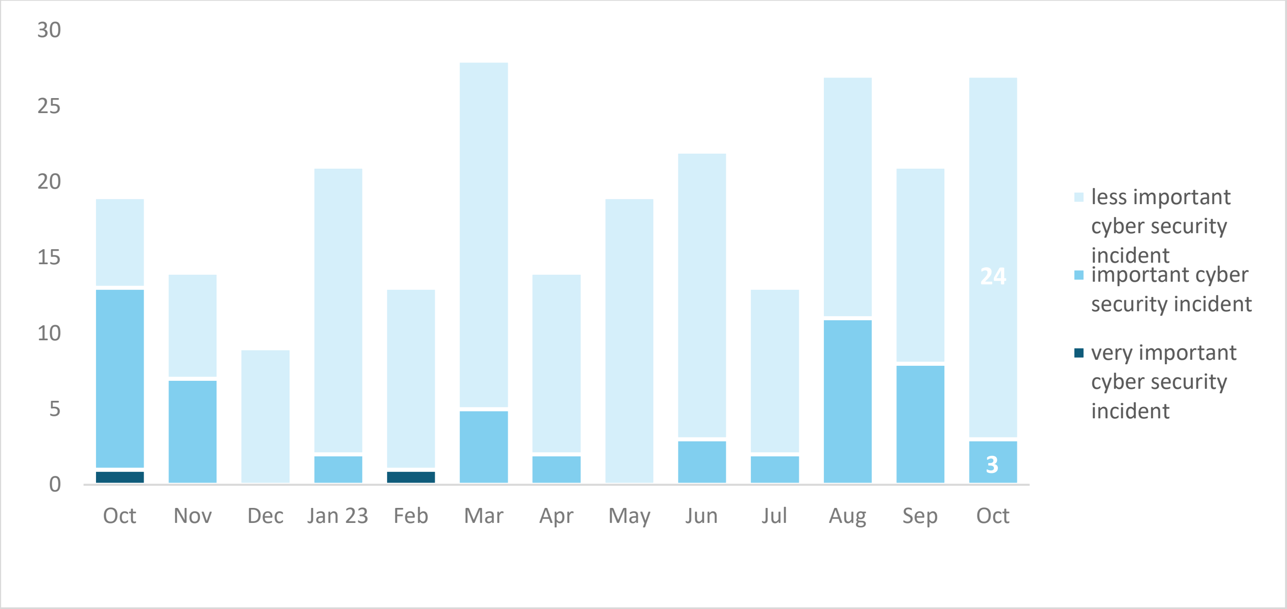
Number of cyber security incidents reported to NÚKIB[1]

During October, there was again an increase in registered incidents, which for the third month in a row were above the average of the last twelve months. The average monthly number has therefore increased roughly by six incidents since last October. Over the past year, NÚKIB records an average of 19 incidents per month.



Severity of the handled cyber security incidents[2]

The higher number of registered incidents has not been reflected in the severity statistics at all. On the contrary, during October there was a decrease in the number of registered significant incidents.



[1] NÚKIB registered 24 incidents in total with liable entities according to Cyber Security Act. The remaining 3 incidents involved unregulated entities.

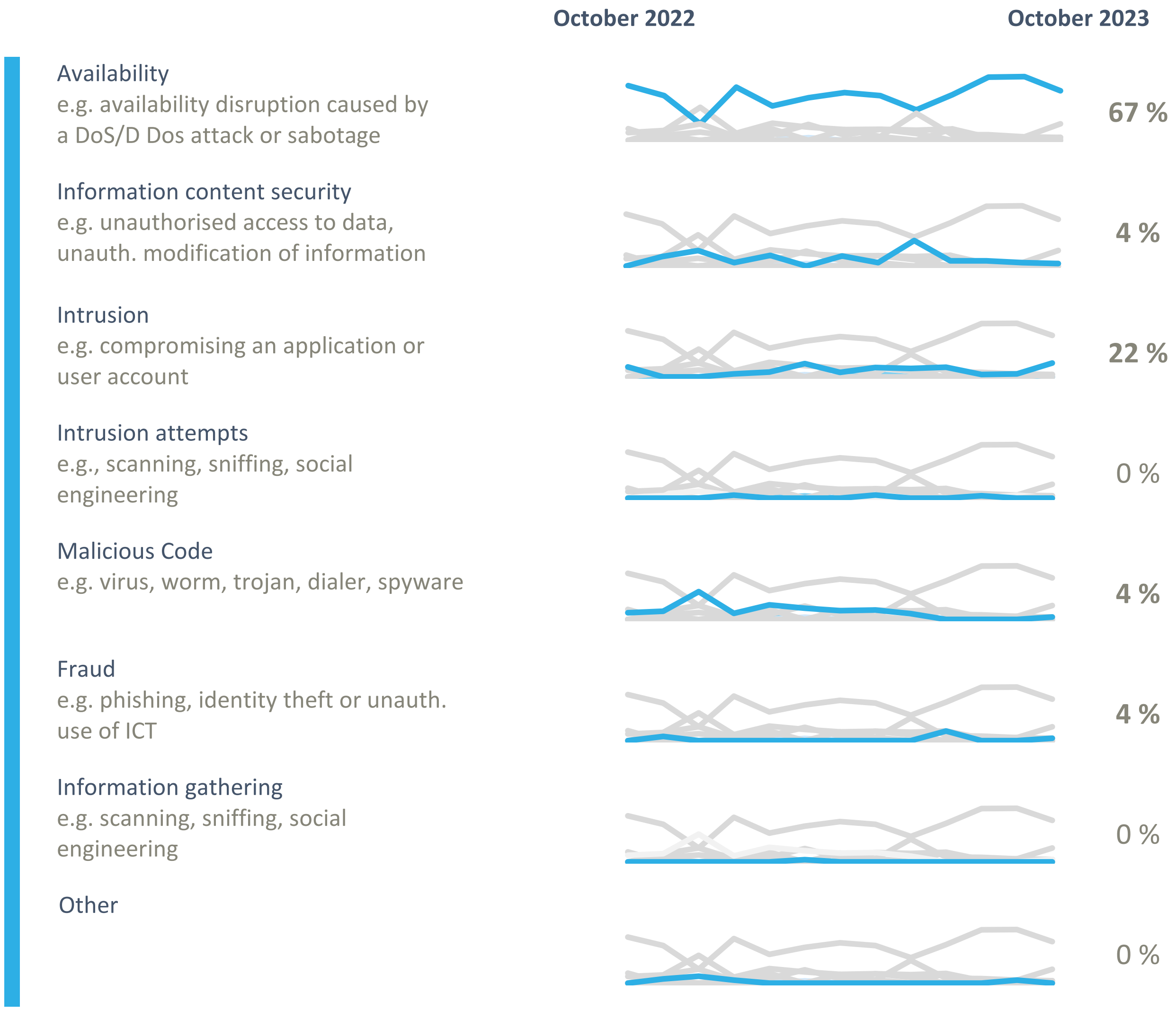
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

As in previous months, the Availability category dominated, where DDoS attacks continued to predominate within the incident classification. However, more than a third of incidents in this category involved outages and misconfigurations.

In addition to this, NÚKIB dealt with incidents in four categories in total:

- During October, NÚKIB registered several intrusions in which attackers managed to gain access not only to some user accounts, but in some cases also to internal systems and perform unauthorized actions within these systems.
- Within the Information Security category, one of the entity's mail boxes was compromised from which phishing emails were subsequently sent.
- The regulated entity intercepted malicious code in its system, which is currently being analysed by NÚKIB.
- The Fraud category includes one successful phishing which was, however, detected in time and did not lead to the compromise of the entity.



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

October trends in cyber security from the NÚKIB’s perspective [4]

Phishing, spear-phishing and social engineering

NÚKIB registered several incidents involving the use of phishing in October. Within several other incidents recorded, the use of phishing as a primary attack vector was likely but cannot be directly confirmed.

Vulnerabilities

NÚKIB issues two advisories regarding new vulnerabilities in October. Both concern the web interface of the Cisco IOS XE operating system and both are being actively exploited. NÚKIB therefore recommended updating vulnerable devices and, where appropriate, using mitigation and detection measures, which can be found in the alerts on NÚKIB website and attached links.

Attacks on availability

As in recent months, attacks by the pro-Russian hacktivist group NoName057(16) continued in October. We discussed the attacks of this group, including mitigation options against them, in Cyber security incidents from the NÚKIB´s perspective – September.

Malware

During October, NÚKIB registered several different types of malware, the analysis of which is currently ongoing.

Ransomware

For the first time in a few months, NÚKIB did not register any ransomware-related incidents.

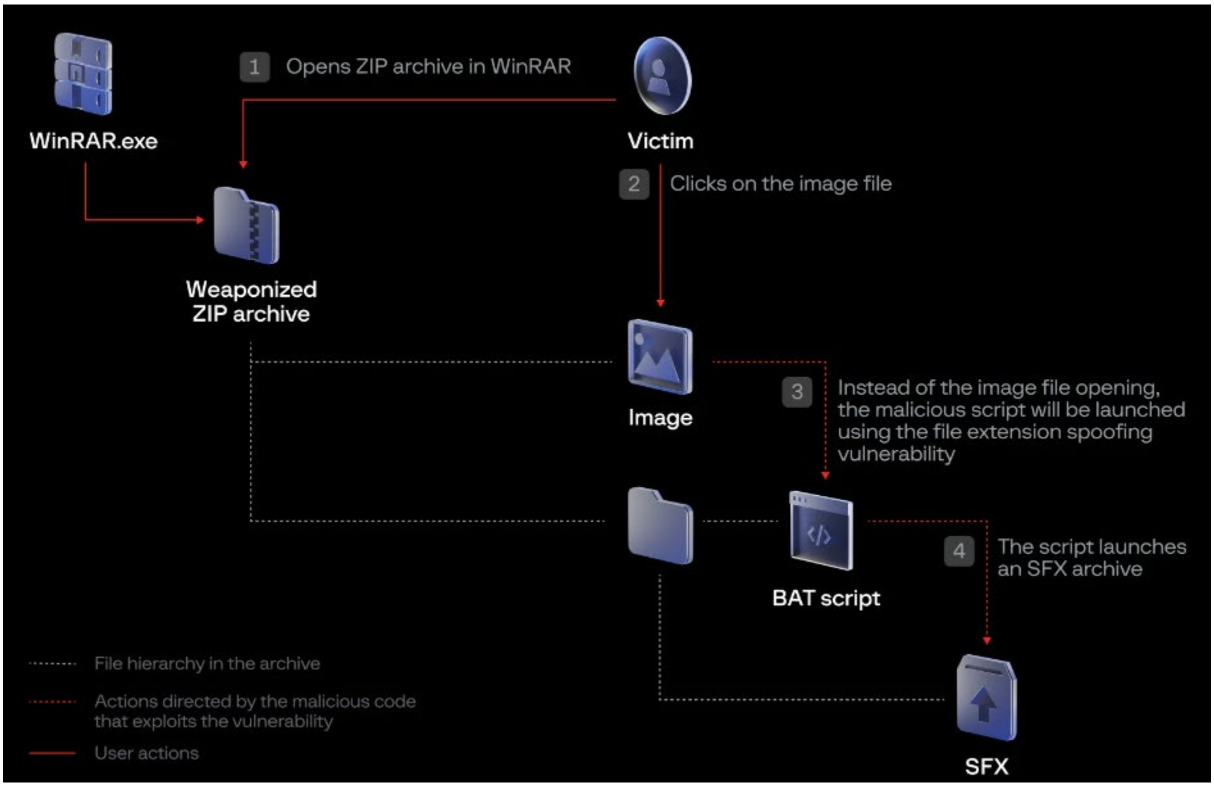
Click or tap here and enter text

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

Focus on a threat: Active exploitation of a serious vulnerability in WinRAR

Within this chapter we focus on a vulnerability in WinRAR with the designation CVE-2023-38831. Although this vulnerability was disclosed in August 2023, its active exploitation started as late as in September and October. According to Google, this vulnerability is being exploited by some state-sponsored actors in their attacks while attacks by cybercriminal groups were also reported in the past. NÚKIB also registered exploitation of this vulnerability within the Czech Republic.

Fig. 1: Graphical representation of attacker processes exploiting the disclosed vulnerability from Group-IB


WinRAR.exe
1 Opens ZIP archive in WinRAR
Victim
2 Clicks on the image file
Weaponized ZIP archive
Image
3 Instead of the image file opening, the malicious script will be launched using the file extension spoofing vulnerability
BAT script
4 The script launches an SFX archive
SFX
File hierarchy in the archive
Actions directed by the malicious code that exploits the vulnerability
User actions

Source: group-ib.com

The vulnerability affects WinRAR 6.22 and earlier versions, in which malicious code can be executed when a user attempts to view files in a ZIP archive that they have downloaded from their email inbox. Most commonly, attackers use a set of JPEG and PNG files, among which there is a file mimicking an image format containing arbitrary code, such as "poc.png .cmd" (the space is intentional here). Alternatively, a variant mimicking a PDF file may be encountered.

A security update addressing the vulnerability is already available and NÚKIB therefore recommends updating WinRAR to the latest version to all who have not already done so.

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.