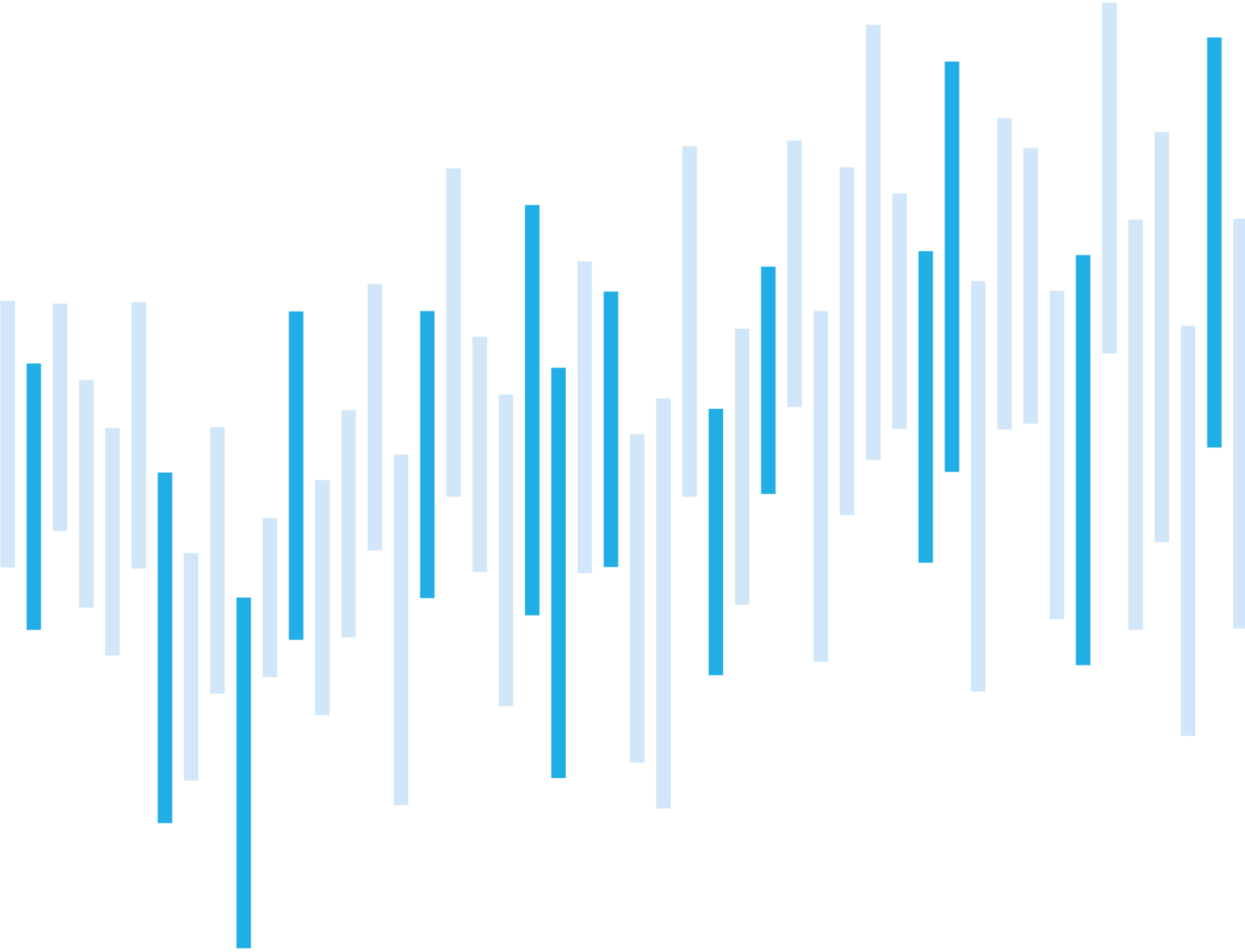
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JUNE 2024



National Cyber
and Information
Security Agency

Summary of the month

In June, NÚKIB recorded 16 incidents, two more than in May. The gradual increase in incidents is therefore continuing, although the overall figure is still below the average for the past year. Two incidents were classified as important, while the remaining 14 incidents fell into the less important category.

After two months, DDoS attacks have also reappeared, of which NÚKIB recorded five in June, all targeting the banking sector. In addition, NÚKIB recorded two ransomware attacks, a spear-phishing campaign and an internal data leak.

In the chapter Focusing on a threat, this time we deal with the topic of education in the context of the youngest users and general cybersecurity tips for the summer period. The number of attacks against this target group usually increases during the summer holidays. This is mainly due to the increased activity of children in cyberspace during summer, with one of the main vectors being, for example, fake applications that may contain various types of malware. The chapter therefore contains a set of general tips on how to avoid these threats, together with links to NÚKIB's educational materials also for the youngest users.

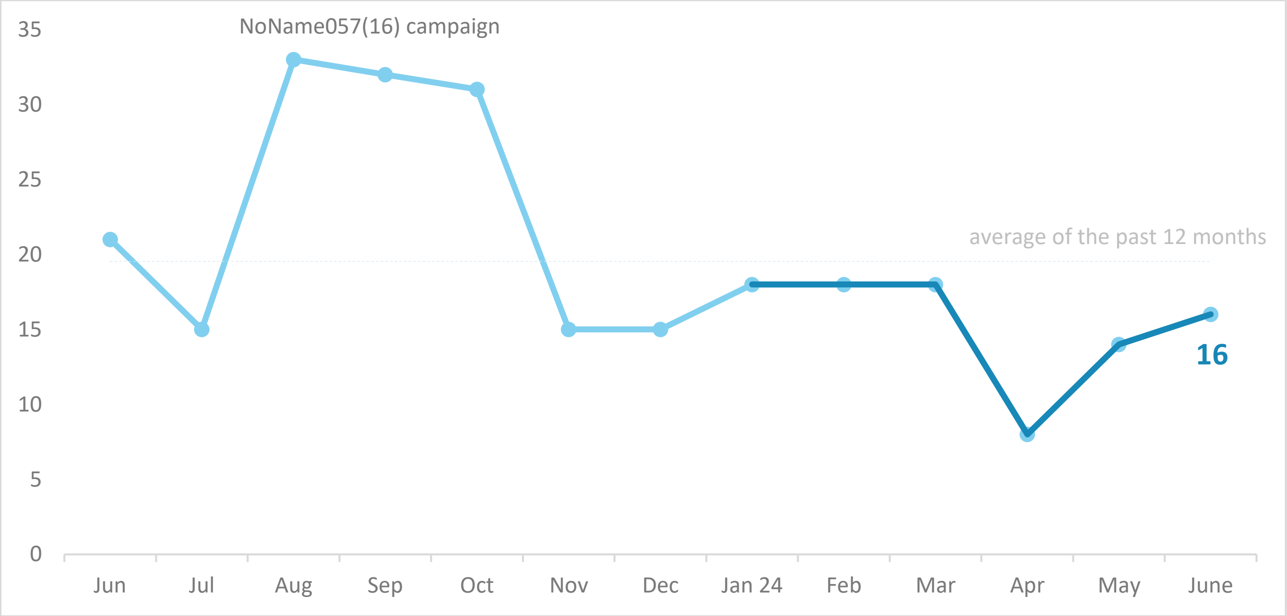
Table of content

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.gov.cz

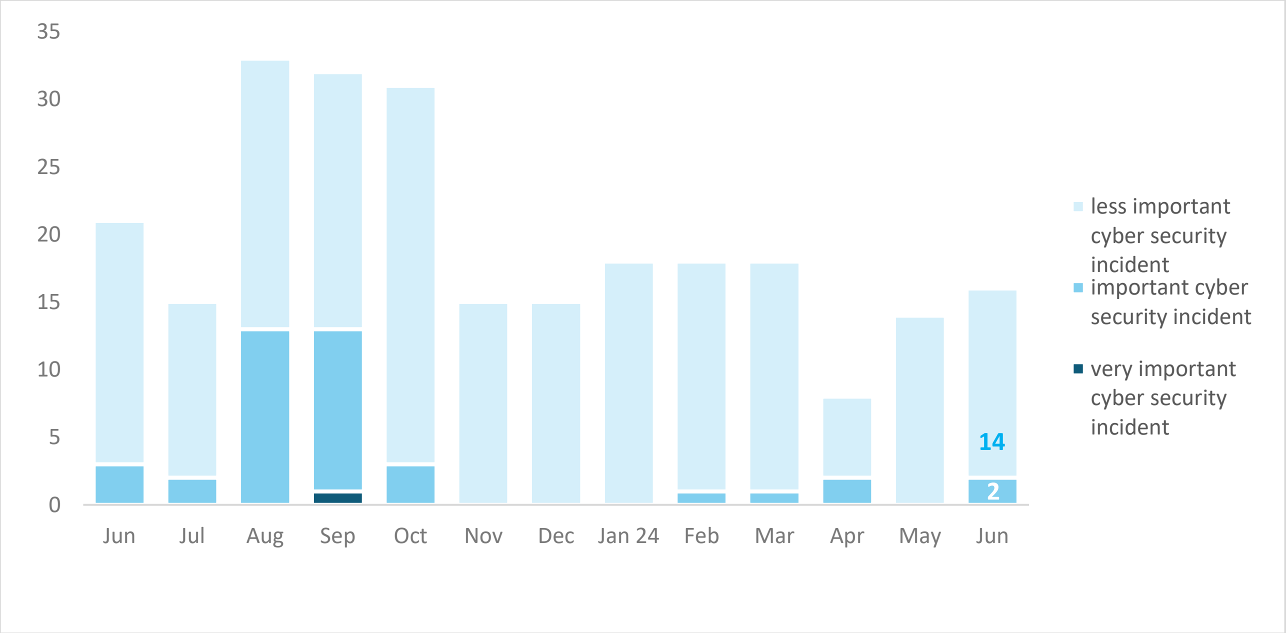
Number of cyber security incidents reported to NÚKIB

In June, 16 incidents were recorded, indicating a continuation of the gradual increase in the number of incidents to the annual average. After a short pause, five incidents related to DDoS attacks targeting banking sector entities also reappeared during June.



Severity of the handled cyber security incidents[1]

In terms of the severity of recorded cyber incidents, most of them fell into the category of less important incidents, but NÚKIB also recorded two important ones in June.

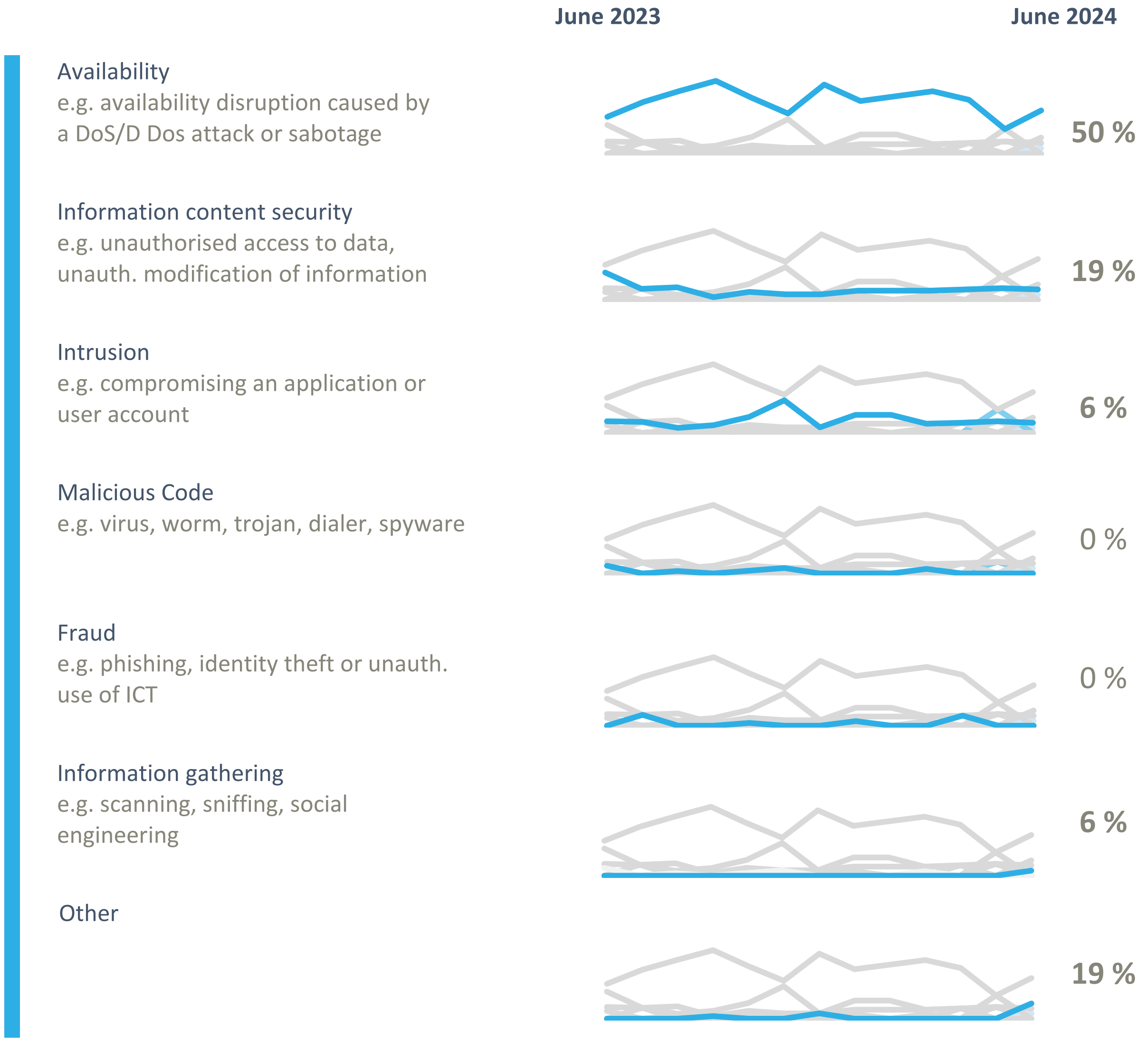


[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

During June, NÚKIB recorded incidents in three categories. The most numerous category was Availability, where, in addition to five DDoS attacks, there were also three outages due to technical malfunctions.

- In the Availability category, after a few months, a higher number of DDoS attacks have appeared again. NÚKIB does not have information on the attackers in these incidents, but all attacks were directed against organisations in the banking sector.
- Within the Information Security category, NÚKIB recorded two ransomware attacks during June. In both cases, part of the internal systems of the attacked entities were encrypted, but in neither case do we have information on the attackers.
- In addition, NÚKIB recorded, for example, a spear-phishing campaign, intrusion of a user's account and subsequent spamming, and leak of user data from an unregulated system.



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

June trends in cyber security from the NÚKIB's perspective [3]

Phishing, spear-phishing and social engineering

In June, NÚKIB registered one incident involving the use of spear-phishing. The attackers used the identity of a high-ranking official of the organisation to send fake emails about a pay rise. The email also contained a malicious link leading to a site designed to steal login credentials.

Vulnerabilities

During June, there was a resumption of government CERT vulnerability reporting activity on social network X. During that month, a number of posts appeared there, both in the context of vulnerabilities and current threats. Vulnerabilities of note include CVE-2024-37882 in Nextcloud or CVE-2024-23110 in Fortigate OS, which was assessed as severe.

Attacks on availability

During the month of June, NÚKIB registered five DDoS attacks. All of them were aimed exclusively at entities in the banking sector, but their perpetrators could not be identified.

Malware

In June, as in the previous months, there were continuous activities in the area of malware analysis in connection to some previously recorded incidents.

Ransomware

In June, two ransomware-related incidents were recorded. However, in neither case does NÚKIB have information about the attackers.

Click or tap here and enter text.

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

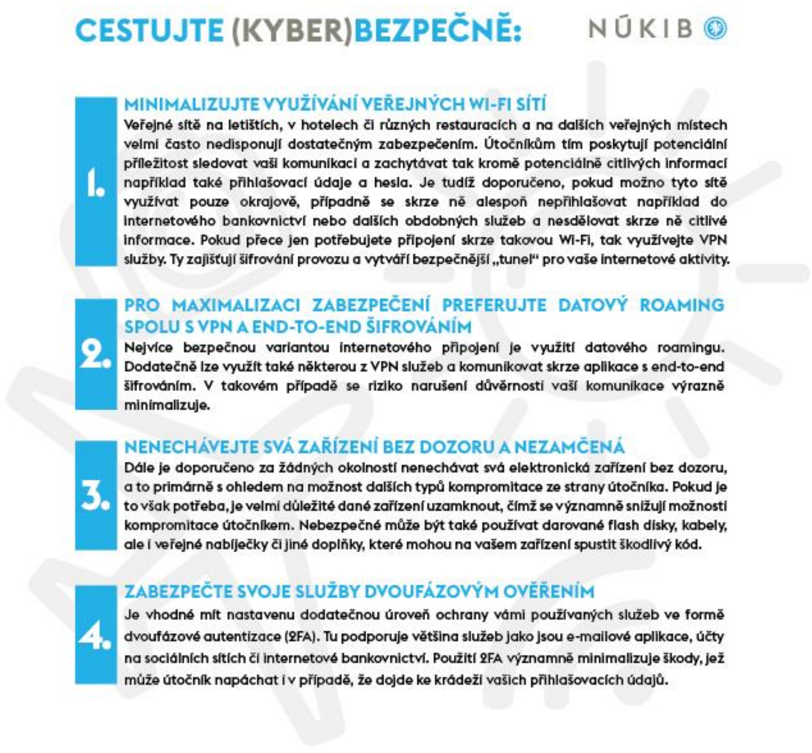
Focus on a threat: attackers are taking advantage of the summer season, targeting younger users, among others

Especially during summer season, specific cyber threats are coming to the fore. Their perpetrators can exploit, for example, users' reduced attention or, conversely, their increased online activity. While this may apply to all users, the above may be more relevant to younger users in particular. Warning in this regard has been published by the Slovak cybersecurity company ESET, which is currently registering an increase in threats primarily targeting this vulnerable group. In their press release, they identified three main types of malware that can pose a threat to child users. These are different types of adware, spyware and different variants of Trojans. Fake apps, including mobile games, remain a common vector and can affect younger users at an increased rate.

Public networks, for another example, can also be a risk. These tend to be poorly secured and can be exploited by attackers in man-in-the-middle attacks, where they try to intercept network traffic between the victim's device and the rest of the internet. In this way, login credentials or passwords can be intercepted, potentially leading again to financial loss. In the summer months, especially in the context of travel, this risk is elevated. For cases where the use of public networks is necessary, the use of a VPN that encrypts user activity on the Internet is highly recommended.

The image below can be used as a list of basic simple tips for all users. Educational materials freely available on the NÚKIB's educational portal can then be used to raise awareness of the threats and principles of safe online behaviour, not only for the youngest users.

Figure 1: For similar tips in English visit cisa.gov



CESTUJTE (KYBER)BEZPEČNĚ: NÚKIB

1. MINIMALIZUJTE VYUŽÍVÁNÍ VEŘEJNÝCH WI-FI SÍTÍ

Veřejné sítě na letištích, v hotelech či různých restauracích a na dalších veřejných místech velmi často nedisponují dostatečným zabezpečením. Útočníkům tím poskytují potenciální příležitost sledovat vaši komunikaci a zachytávat tak kromě potenciálně citlivých informací například také přihlašovací údaje a hesla. Je tudíž doporučeno, pokud možno tyto sítě využívat pouze okrajově, případně se skrze ně alespoň nepřihlašovat například do internetového bankovnictví nebo dalších obdobných služeb a nesdělovat skrze ně citlivé informace. Pokud přece jen potřebujete připojení skrze takovou Wi-Fi, tak využívejte VPN služby. Ty zajišťují šifrování provozu a vytváří bezpečnější „tunel" pro vaše internetové aktivity.

2. PRO MAXIMALIZACI ZABEZPEČENÍ PREFERUJTE DATOVÝ ROAMING SPOLU S VPN A END-TO-END ŠIFROVÁNÍM

Nejvíce bezpečnou variantou internetového připojení je využití datového roamingu. Dodatečně lze využít také některou z VPN služeb a komunikovat skrze aplikace s end-to-end šifrováním. V takovém případě se riziko narušení důvěrnosti vaší komunikace výrazně minimalizuje.

3. NENECHÁVEJTE SVÁ ZAŘÍZENÍ BEZ DOZORU A NEZAMČENÁ

Dále je doporučeno za žádných okolností nenechávat svá elektronická zařízení bez dozoru, a to primárně s ohledem na možnost dalších typů kompromitace ze strany útočníka. Pokud je to však potřeba, je velmi důležité dané zařízení uzamknout, čímž se významně snižují možnosti kompromitace útočníkem. Nebezpečné může být také používat darované flash disky, kabely, ale i veřejné nabíječky či jiné doplňky, které mohou na vašem zařízení spustit škodlivý kód.

4. ZABEZPEČTE SVOJE SLUŽBY DVOUFÁZOVÝM OVĚŘENÍM

Je vhodné mít nastavenu dodatečnou úroveň ochrany vámi používaných služeb ve formě dvoufázové autentizace (2FA). Tu podporuje většina služeb jako jsou e-mailové aplikace, účty na sociálních sítích či internetové bankovnictví. Použití 2FA významně minimalizuje škody, jež může útočník napáchat i v případě, že dojde ke krádeži vašich přihlašovacích údajů.

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	*40–50 %*
Unlikely	*20–35 %*
Highly unlikely	*0–15 %*

Traffic Light Protocol

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://ww.first.org/tlp/). 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.