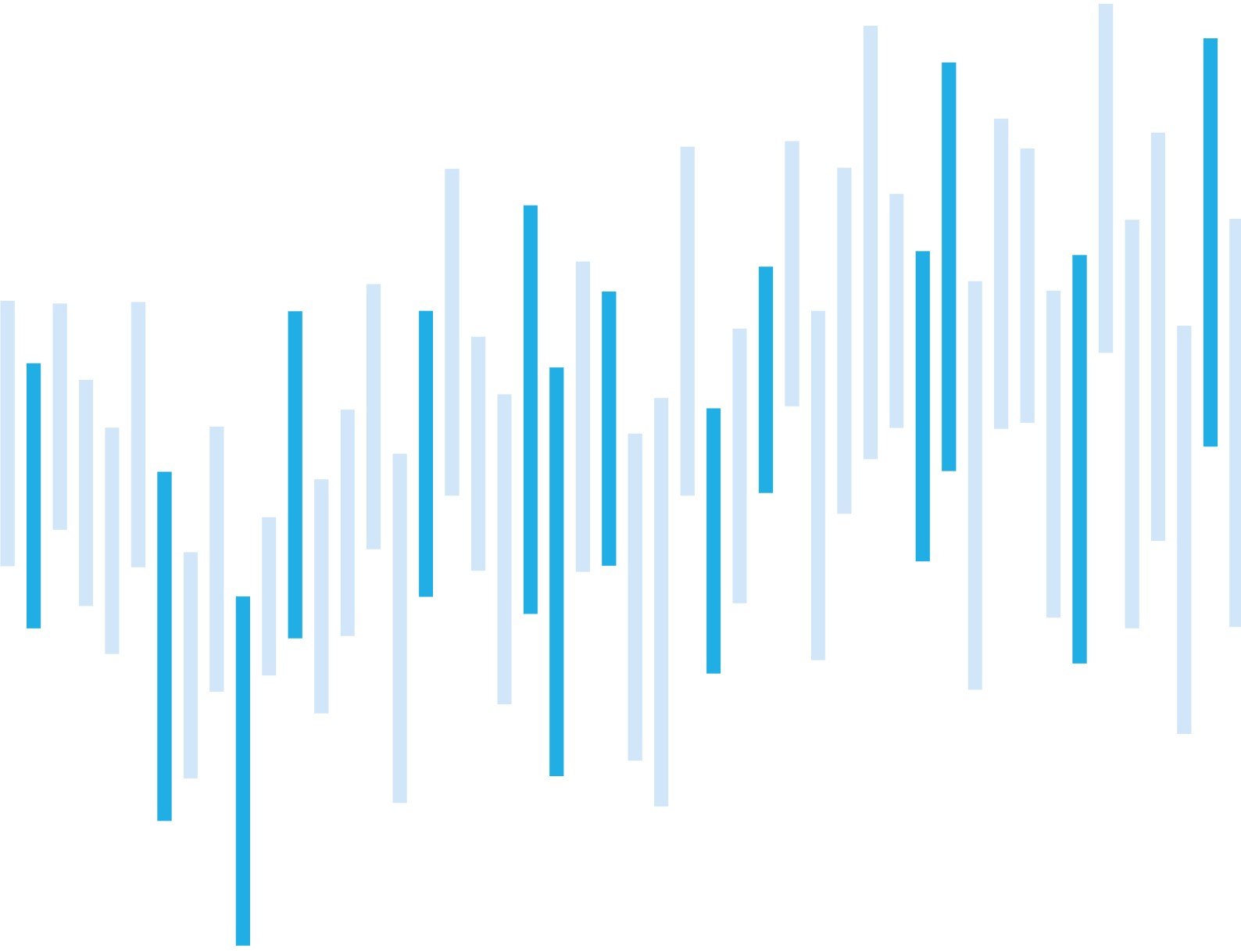
CYBER SECURITY INCIDENTS FROM THE NÚKIB' S PERSPECTIVE

AUGUST 2023



National Cyber and Information Security Agency

Summary of the month

In August, the number of registered cyber incidents more than doubled compared to July. Another new wave of DDoS attacks led by the NoName057(16) group had big impact on this increase. Majority of these attacks were directed at Czech bank websites, the unavailability of which may have affected a large part of the general public.

In the chapter *Focus on the Threat*, we focus on LockBit, one of the most active ransomware gangs at present. According to the findings of expert Joe DiMaggio, the gang's operations have been significantly affected by a number of internal problems in recent months.

The struggle with the disclosure of stolen data due to insufficient infrastructure is one of them. These findings suggest, among other things, that paying the LockBit gang's ransom may not be very worthwhile. NÚKIB generally does not recommend paying ransoms for several reasons.

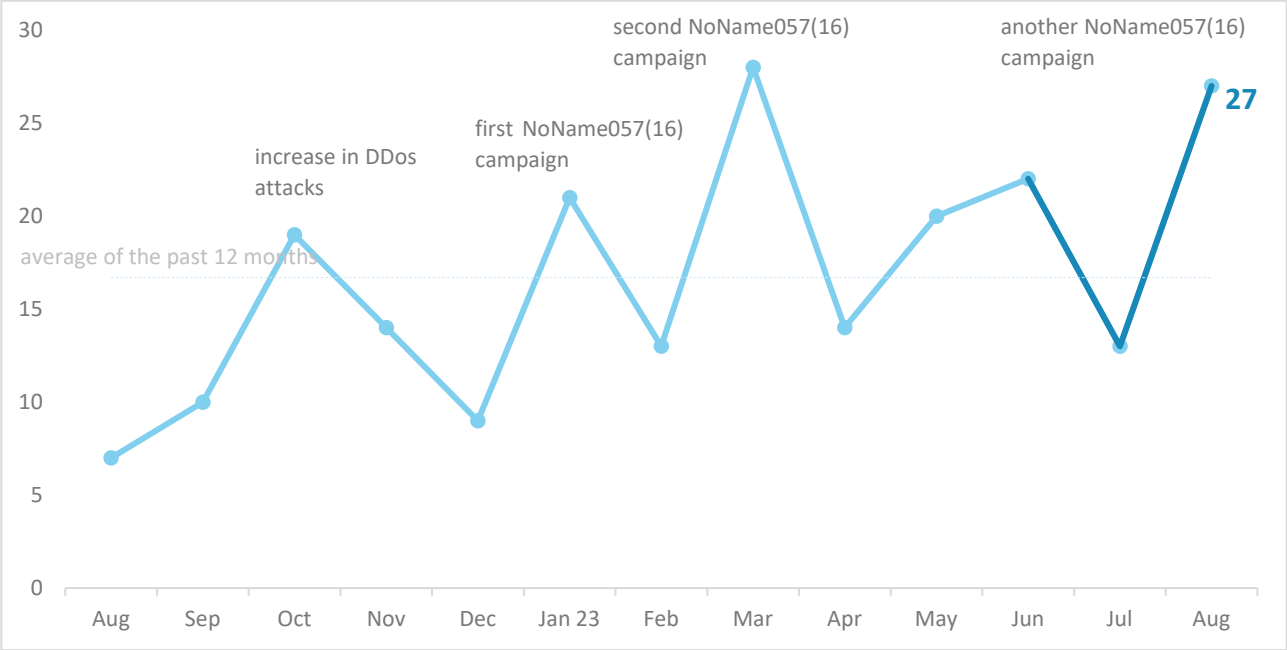
Table of content

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

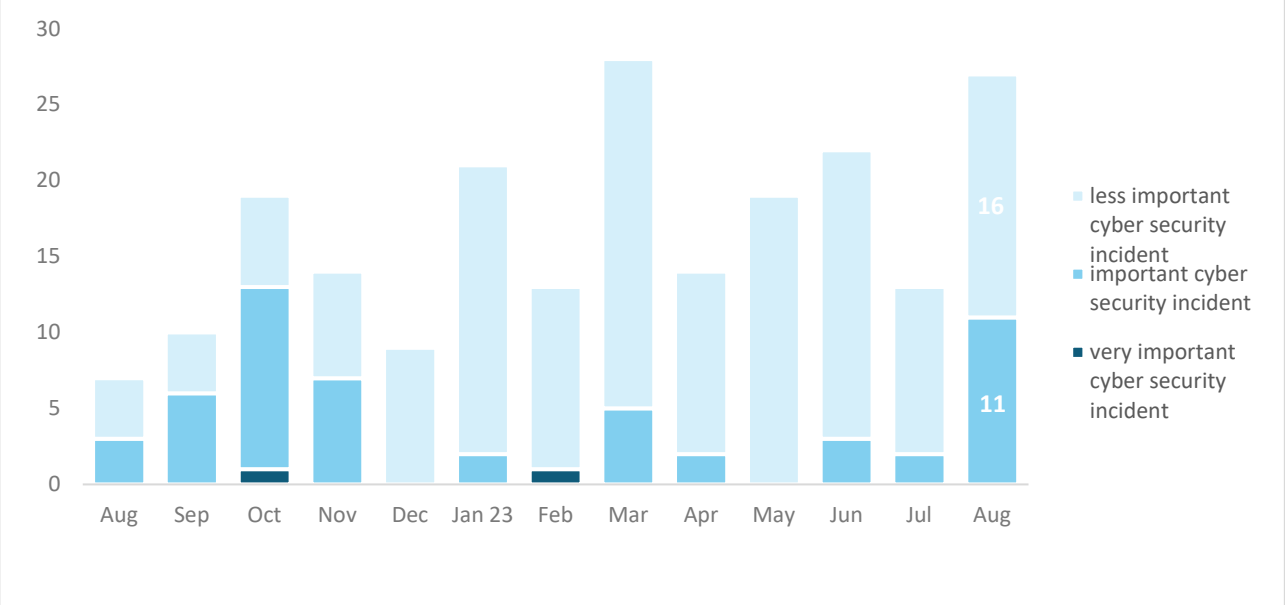
Number of cyber security incidents reported to NÚKIB

In August, the number of registered cyber incidents more than doubled compared to July. Another new wave of DDoS attacks led by the NoName057(16) group had big impact on this increase. [1]



Severity of the handled cyber security incidents[2]

Although minor cyber incidents continued to predominate in August, there was a significant increase in major incidents. This particularly included DDoS attacks on Czech banks websites, the unavailability of which could affect a large part of the public.



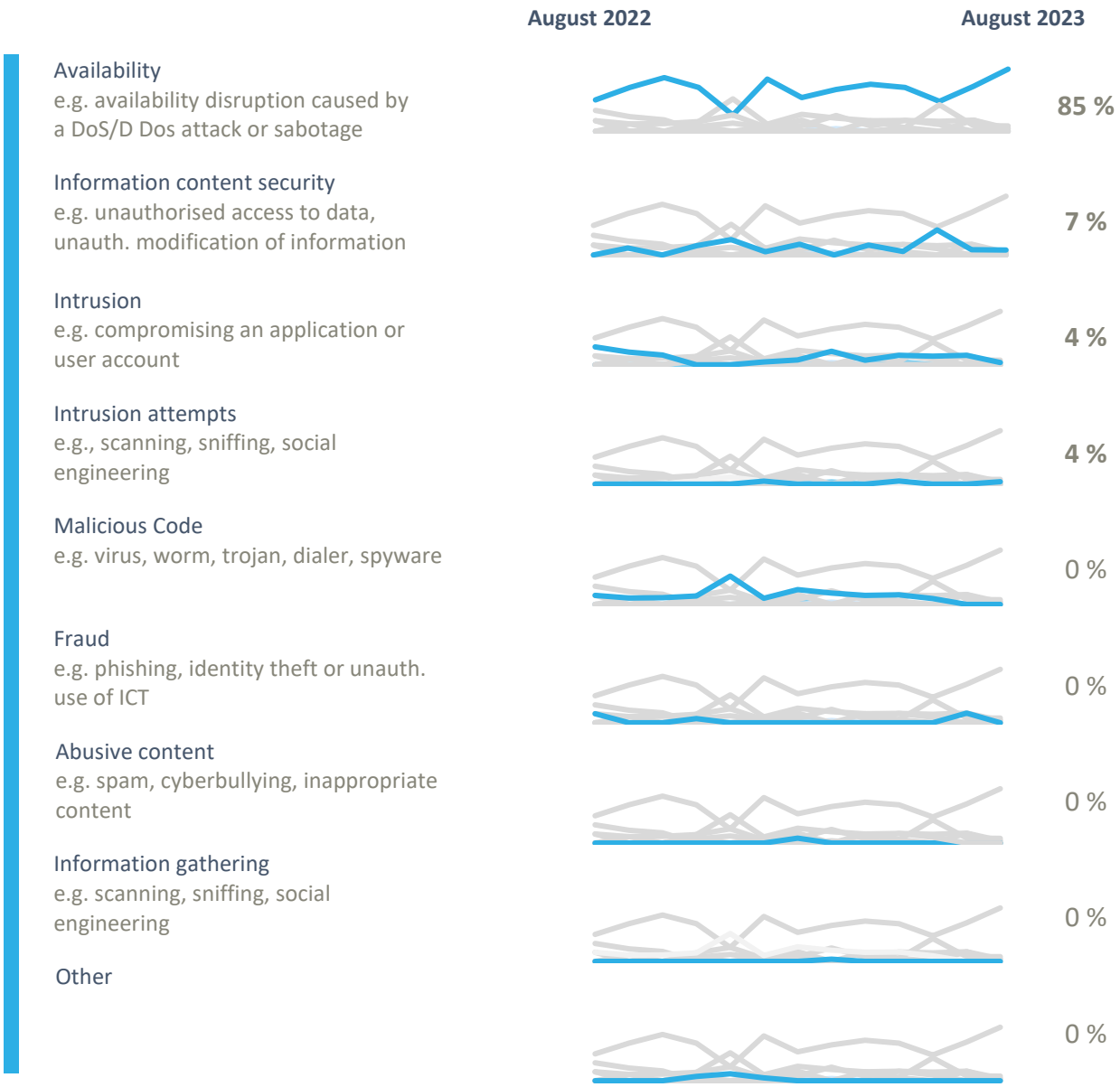
[1] NÚKIB registered 18 incidents in total with liable entities according to Cyber Security Act. Remaining 9 incidents reported not regulated subjects to NÚKIB.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

In August, similarly to previous months, incidents falling into the availability category predominated, accounting for more than four-fifths of all incidents this time. These were predominantly caused by DDoS attacks.

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

- Within the Information Security category, two ransomware attacks against unregulated entities were registered.
- In August, there was one case of intrusion, where an unknown attacker compromised a user's account on a portal and subsequently carried out further malicious activity based on the access gained.
- NÚKIB also registered one incident in the intrusion attempts category, the only confirmed impact of which was temporary unavailability of services.



[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

In August, NÚKIB alerted to a vishing campaign targeting the general public. As part of this campaign, unknown attackers pretending to be bank employees try to force the victim to transfer funds to a "reserve account" with reference to NÚKIB or its employees, in order to avoid a fictitious threat of these funds being stolen by the attacker.

NÚKIB calls for maximum caution and has published recommendations on its website to prevent fraudulent phone calls.

Malware

After a longer period, NÚKIB has not registered any malware within incident records, except for the two ransomware ones mentioned below.

Vulnerabilities

In August, NÚKIB did not issue any warnings about newly discovered vulnerabilities.

Ransom ware

NÚKIB recorded a total of 2 ransomware attacks during August. In the first case, an unregulated entity was attacked by Cryptolocker ransomware, in the second case the ransomware used has not yet been identified.

Attacks on availability

The pro-Russian hacktivist group NoName057(16) has carried out a series of DDoS attacks on Czech entities several times this year. Banking institutions were the main target of the next wave of attacks, which took place at the end of August. More information about NoName057(16) group can be found in the January cyber incidents overview.

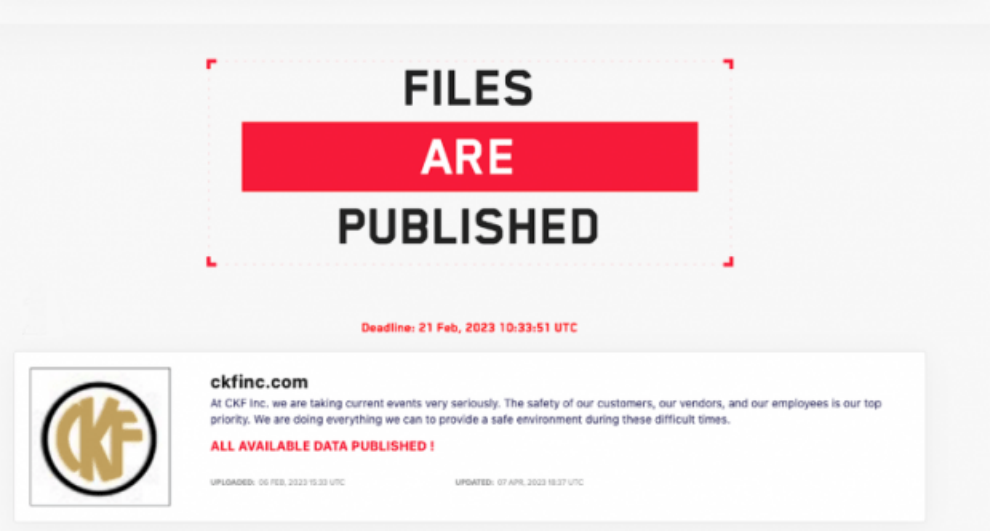
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Focus on a threat: Problems of ransomware gang LockBit

The LockBit ransomware gang is currently one of the most active cybercriminal actors in the world. The gang functions on the basis of the Ransomware-as-a-service (Raas) model, in which they offer ransomware to its affiliates for a share of the profit from the ransom. Ransomware LockBit has already appeared several times in various variants in incidents recorded by NÚKIB, and due to the success rate so far, it is likely (55–70%) that some Czech entities will become the target of this gang in the future as well.

Although LockBit is often considered a very effective and relatively sophisticated actor, cybersecurity expert Jon DiMaggio has come up with some surprising findings revealing serious internal problems for the gang. One of the most significant and relevant findings for victims is the fact that LockBit has been having trouble disclosing stolen data since early 2023. According to DiMaggio, the gang's inadequate infrastructure leads to LockBit often merely announcing the release of data on its website without actually releasing it. This situation, together with some other internal problems, leads to the fact that many gang members prefer to switch to the competitors. Full version of the article with all the findings on the LockBit gang can be found on Analyst1 website.

Fig. 1: Example of a victim posted on the LockBit site whose data was not published.



The above findings suggest that paying the LockBit ransom gang may not be very profitable, as the gang has trouble delivering on its threats. NÚKIB generally does not recommend paying ransoms for a number of reasons. In terms of cybersecurity in general, paying ransoms helps to empower attackers, both financially and in terms of the confidence associated with the success of an attack. Successful attacks can increase the number and intensity of further attacks by the same and other attackers, and the risk of a repeated attack on a victim who has already paid the ransom cannot be ruled out. Another reason for not paying the ransom is the absence of a factual guarantee that the data will be decrypted after payment or that the attackers will not resell or disclose the data.

In June 2023, NÚKIB issued an updated version of the document, which not only provides recommendations regarding ransom payment, but in particular recommendations including preventive and mitigation measures against ransomware.

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.