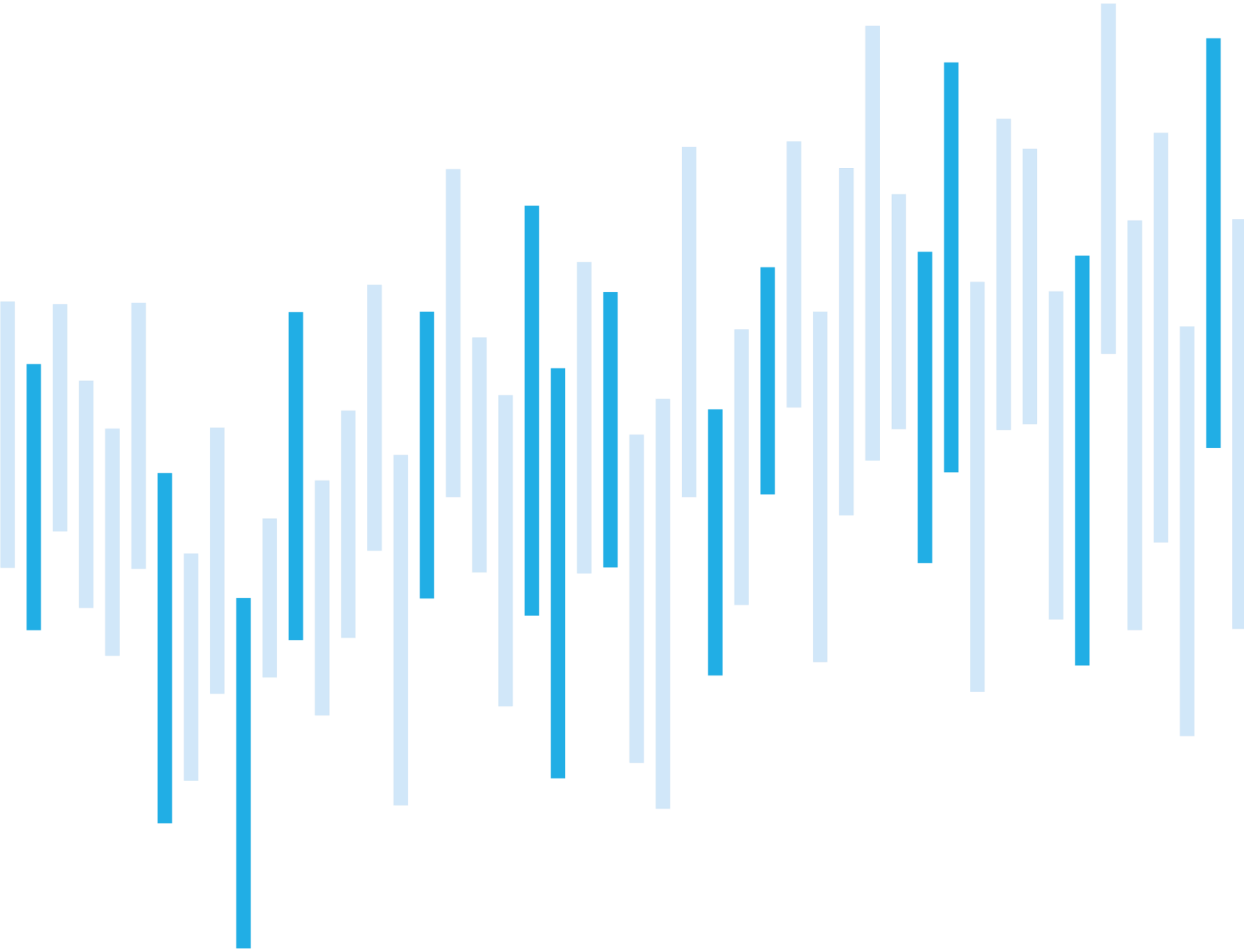
CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

APRIL 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

After the previous record month, the number of cyber security incidents handled by NÚKIB returned to average levels. Incidents were again dominated by loss of availability. This time, however, the unavailability was not only caused by DDoS attacks, but in many cases also by a technical error.

In April continued the trend of intensive phishing campaigns against strategic government targets in NATO countries, including the Czech Republic. The Russian aggression in Ukraine accelerated the rate of espionage attacks. According to publicly available information, not only Russian actors, but also the Chinese ones intensified their cyber espionage efforts.

Czech diplomatic organisations were targeted by another cyber espionage actor in last couple of months. ESET associates this campaign with Chinese group Mustang Panda. The group used the new MQsTTang malware which is unusual for its communication with C2 server, as it communicates via the MQTT protocol used for Internet of Things (IoT) devices. No publicly known malware has used the MQTT protocol so far. We describe the campaign and the new technique used in it in more detail in the last two chapters.

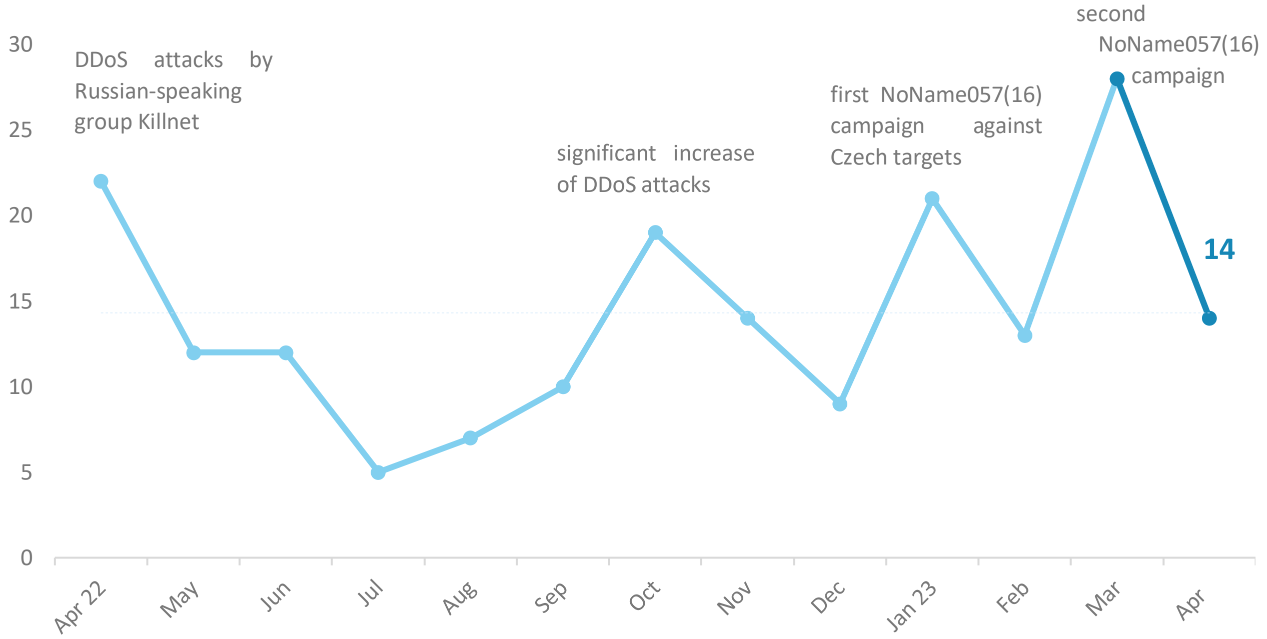
Table of contents

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

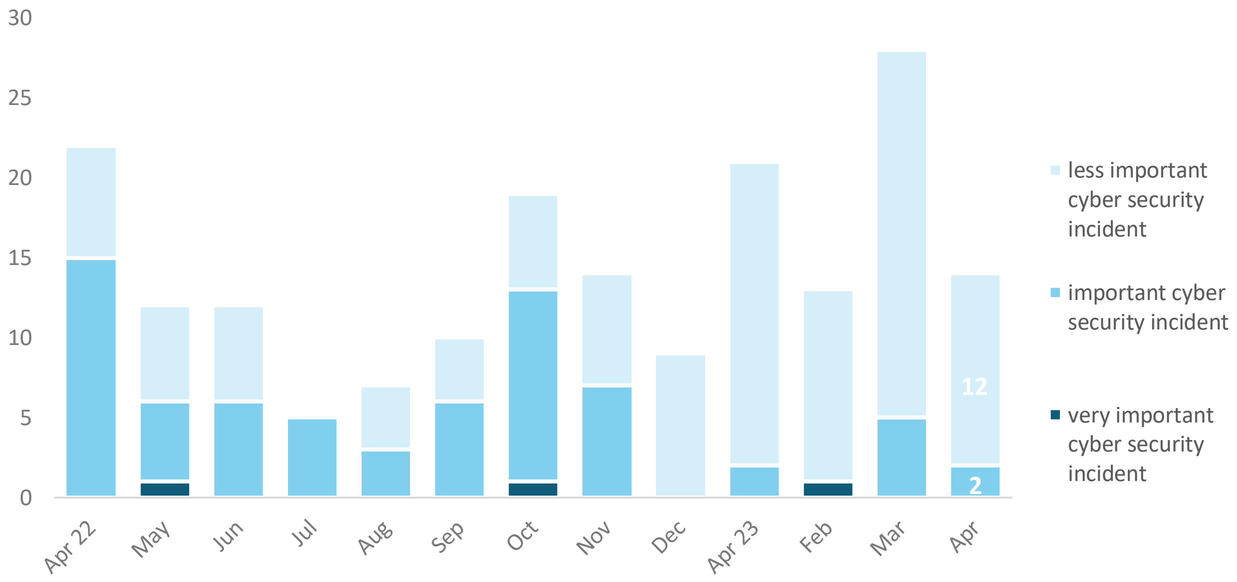
Number of cyber security incidents reported to NÚKIB

In April, NÚKIB registered 14 cyber security incidents. After the previous record month, the number of incidents returned to the average levels of the last year.[1]



Severity of the handled cyber security incidents[2]

As in the last few months, most cyber incidents did not have serious consequences that would significantly affect the functioning of the attacked organizations, and NÚKIB therefore registers them as less significant.



[1] NÚKIB registered five incidents in total with liable entities according to Cyber Security Act. The remaining nine incidents reported not regulated subjects to NÚKIB.

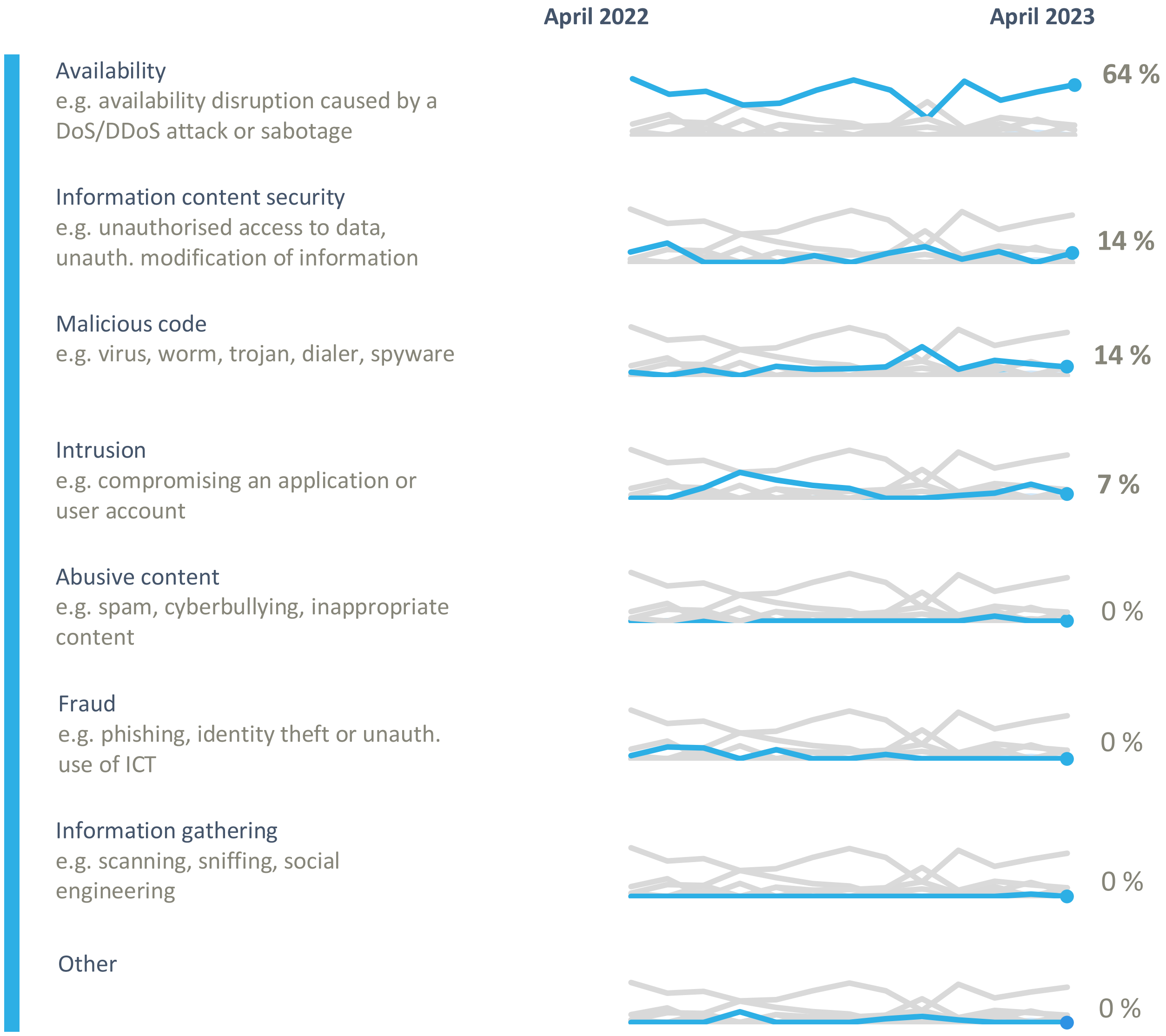
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

The trend of the past year where incidents were dominated by disruptions to availability continued in April. NÚKIB classified almost two-thirds of incidents this way. Unlike the last month, however, not only DDoS attacks, but largely technical errors were the causes. Five organizations reported NÚKIB the service outage caused by the error.

In addition to availability, NÚKIB also dealt with incidents in the following categories:

- Two incidents in which the attacker changed data on the victim's website after a compromise were classified by NÚKIB as information security;
- Two incidents caused by ransomware were registered as malicious code by NÚKIB;
- And in the last case, unknown attackers compromised the e-mail box of a private organization employee and then sent spam from it to other addresses.



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

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

Phishing, spear-phishing and social engineering

The trend of intensive phishing campaigns against strategic government targets in NATO countries, including the Czech Republic, continued in April. The Russian aggression in Ukraine, which increased the interest of state actors in the opponents' strategic information, accelerated the rate of espionage attacks. According to publicly available information, not only Russian actors intensified their espionages attacks against NATO countries but also the Chinese ones.

Malware

In one of the recent phishing campaigns analysed by NÚKIBB and described in the last chapter, the new MQsTTang malware appeared. Attackers used it as a backdoor, and the most interesting thing about it is the way it communicates with its control server. The communication goes via the MQTT protocol, which is used for Internet of Things (IoT). No publicly known malware has used the MQTT protocol so far. More information to this technique you can find in the following chapter.

Vulnerabilities

In April, no new critical vulnerabilities emerged that we would expect to be exploited in the wild and have effect across NÚKIB liable entities.

Ransomware

NUKIB recorded two cases of ransomware attacks, both against small and medium-sized enterprises. One of the incidents was caused by LockBit 2.0, ransomware from one of the most active "ransomware families" in ČR.

April's ransomware attacks were similar to the previous 12 months in number and nature of victims. Attacks recorded by NÚKIB in the last year most often affect smaller businesses or primary and secondary schools.

Attacks on availability

March wave reverberations of hacktivist DDoS attacks against Czech targets continued also in April. However, their intensity was lower than in the previous month and the number of DDoS attacks dealt by NÚKIB in this context dropped to a third. The attackers focussed mainly on transport sector organizations.

OT – operational technologies

In April, the Ukrainian CERT (CERT-UA) reported an incident where an energy company employee downloaded piracy Microsoft Office 2019 from a torrent network. As a result, the computer was compromised by the DarkCrystal and DWAgent malware. The two applications provided unauthorized access to the company's network for two months. More details at CERT-UA.

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

Technique of the month: Application Layer Protocol

In the phishing campaign we describe in the following section, the attackers used an unusual method of communication between their control server (C2 server) and the compromised victim station. They sent the communication through the MQTT protocol, which is used to manage IoT devices. This distinguishes them from other actors. In the MITRE matrix this technique generally falls under Application Layer Protocol.

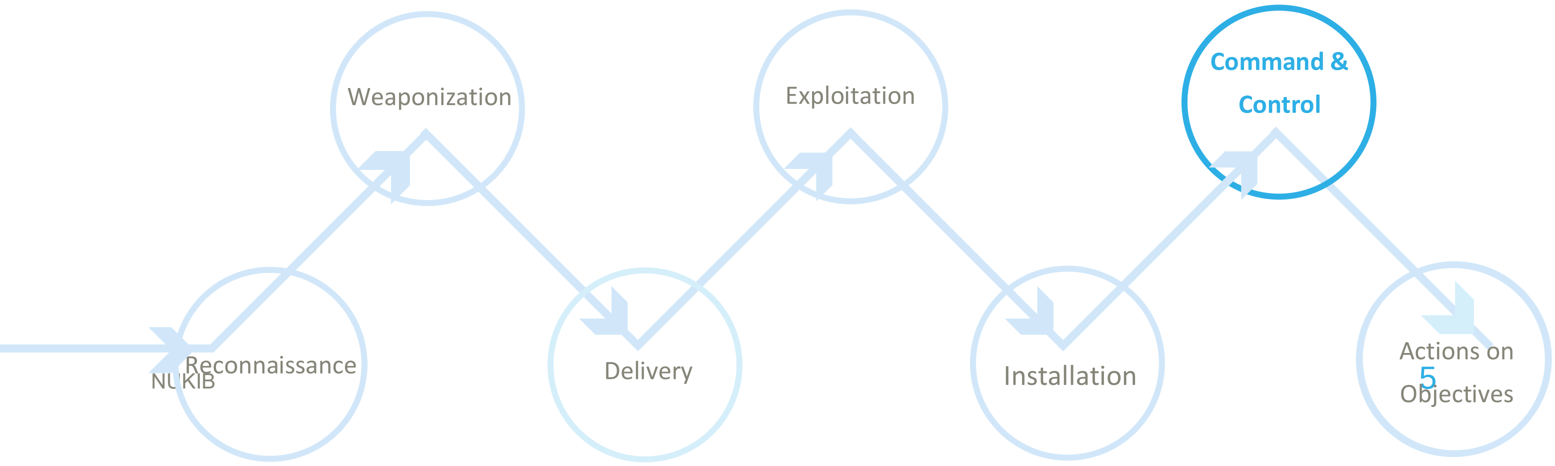
Application Layer Protocol: When the attackers penetrate their victim's network and install a backdoor, they need it to start communicating with their infrastructure so that they can use it to access and take further action on the victim's network. To avoid detection, attackers often try to hide malicious communication with the C2 server among commonly used protocols such as HTTP/HTTPS, DNS or email protocols (SMTP, POP3). They hope to blend in with the large volume of legitimate traffic and thus increase the probability of being overlooked by defenders.

However, in the campaign we describe, the attackers did not communicate with their infrastructure via commonly known protocols, but through the MQTT protocol (port 1883). MQTT is used for communication among IoT devices. From an attacker's perspective, it has the advantage of having its infrastructure hidden behind a public broker (the central element managing communication between IoT devices). Thus, the victim never communicates directly with the attacker's control server, but with the broker's server. This makes the attacker's infrastructure less visible. ESET analysts also assess that since the broker used by the attackers is a public service that has many legitimate users, it is unlikely to be removed.

MITRE ID: **T1071**

Mitigation: The difficulty of mitigating this technique depends on the frequency of the MQTT protocol in the organizations network traffic. Some organizations using IoT devices actively, such as industry, energy or healthcare, may have the MQTT protocol in their network traffic very often. However, in other organizations that do not have extensive IoT device deployments, the MQTT protocol may not appear frequently or at all in network traffic. Network defenders can then more easily monitor and filter MQTT protocol traffic or disable it completely. Segmenting the network and placing any IoT devices, such as printers, on a separate VLAN is also recommended.

Representation of Application Layer Protocol in the Cyber Kill Chain showing the attack phase in which the cyber actors use the technique:



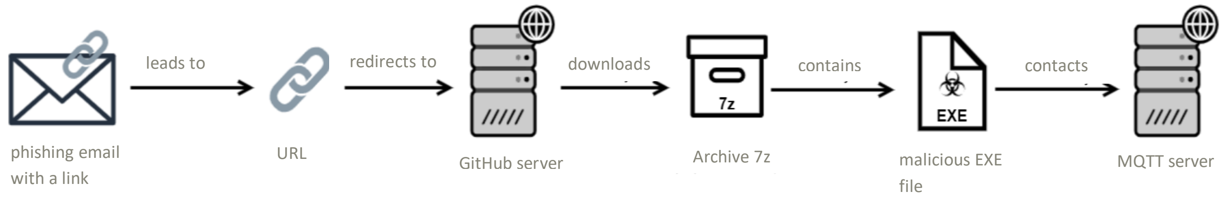
Focus on a threat: Another phishing campaign against Czech diplomatic targets

Czech diplomatic targets were targeted by another cyber espionage actor in last months. ESET associates this campaign to the Chinese group Mustang Panda. The group is typical mainly for its focus on diplomatic organizations. Since the start of Russia's aggression in Ukraine, it has accelerated the pace of its attacks and shifted most of its attention to European entities. The campaign described herein was not focussed on the Czech Republic only, but also on more NATO and EU countries.

What is interesting about this campaign is the new MQsTTang malware that the group used in their attacks. Attackers use it as a backdoor and what is unusual about it is the way it communicates with its control server. The communication goes via the MQTT protocol, which is used for Internet of Things (IoT). No publicly known malware has used the MQTT protocol so far.

Based on one of the phishing e-mails obtained by NÚKIB, the attacks of the recent campaign were carried out in the following way:

The attack began with a phishing email with diplomatic themes and a malicious link. After clicking on the link, the victim was taken to a URL from where they were redirected to the attacker's page on the GitHub platform. The attackers placed an archive there, which the victim downloaded to its computer. The archive, when unzipped, contained an EXE file, which is the MQsTTang malware. If the victim ran the file, the malware started communicating with its control server using the MQTT protocol (see the previous section). In the next steps, the attackers then created persistence in the victim's network and started downloading additional tools for cyberespionage purposes.



Although Chinese APT groups have been targeting European organisations for a long time, the invasion to Ukraine has given them a new impetus to their attacks. Considering the increased activity of Chinese groups described by security companies, it is almost certain (90-100%) that for the duration of the war Mustang Panda will continue to target European organizations from which it will seek to obtain strategic information. And as its latest campaign shows, it is also likely (55-70%) that the group will continue to refine its attacks and deploy new techniques and tools.

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	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/defence community.
TLP: CLEAF	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.