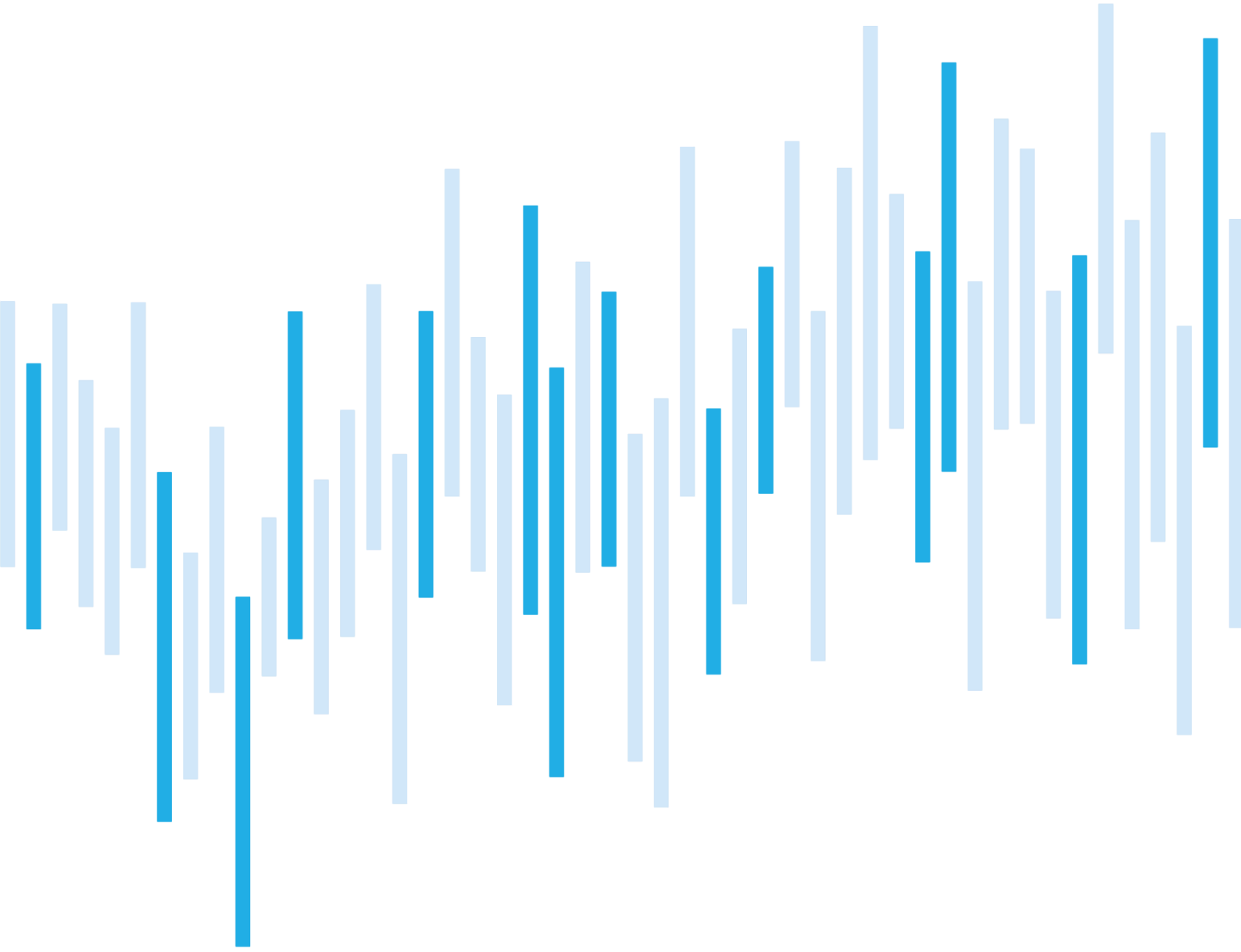
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

FEBRUARY 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

After a rise caused by last month's DDoS attacks, the number of cyber incidents has returned to the average values of the last 12 months.

In February, NÚKIB focused on a phishing campaign, which we do not register among the incidents. The campaign was aimed at Czech and European diplomatic targets and cyber espionage was its highly likely intent. We have no information at this time whether the attackers have been successful in compromising any of their targets. However, the actor´s probable origin and the choice of targets show that their activities cannot be underestimated.

Analysts of RecordedFuture connect this campaign with an actor whose operational practices, motivations, and goals overlap with previous activities of the APT29 group (also known as Nobelium or CozyBear). APT29 is a highly advanced cyber espionage actor operating under patronage of the Russian External Intelligence Service (SVR).

In this report, we analyse infection chain of the attack and take a closer look at the HTML Smuggling technique used by the attackers. It is a difficult technique to detect and therefore it is also difficult to defend against it. APT29 has been including it in their campaigns for almost two years.

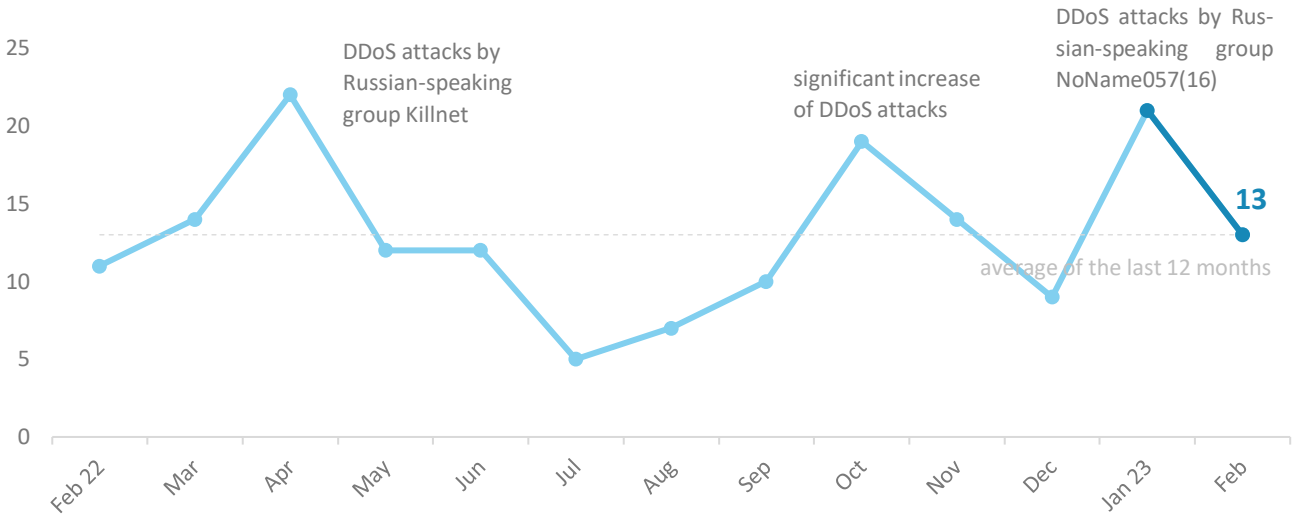
Table of contents

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.

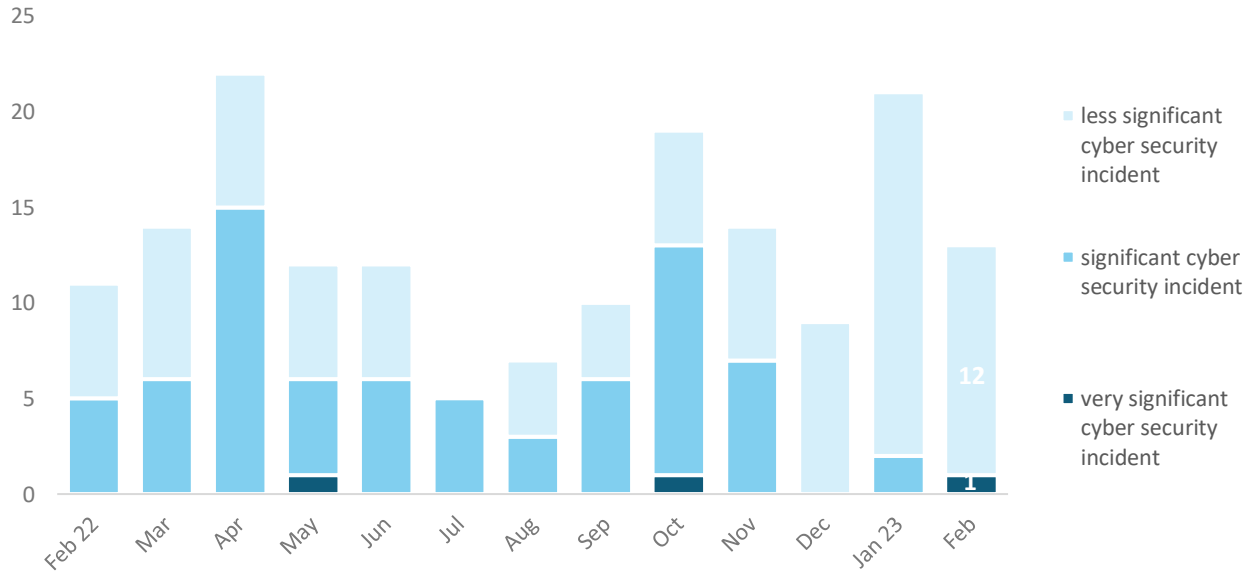
Number of cyber security incidents reported to NÚKIB

NÚKIB handled 13 cyber security incidents in February. After a sharp increase caused by January DDoS attacks, the number of incidents returned to the average of last 12 months. [1]



Severity of the handled cyber security incidents[2]

After four months, NÚKIB dealt with a very significant cyber security incident. A DDoS attack against a Czech ministry caused unavailability of its critical infrastructure systems, which significantly affected its operations. The attack occurred in a few waves, each lasting several hours and affecting more than a million users.

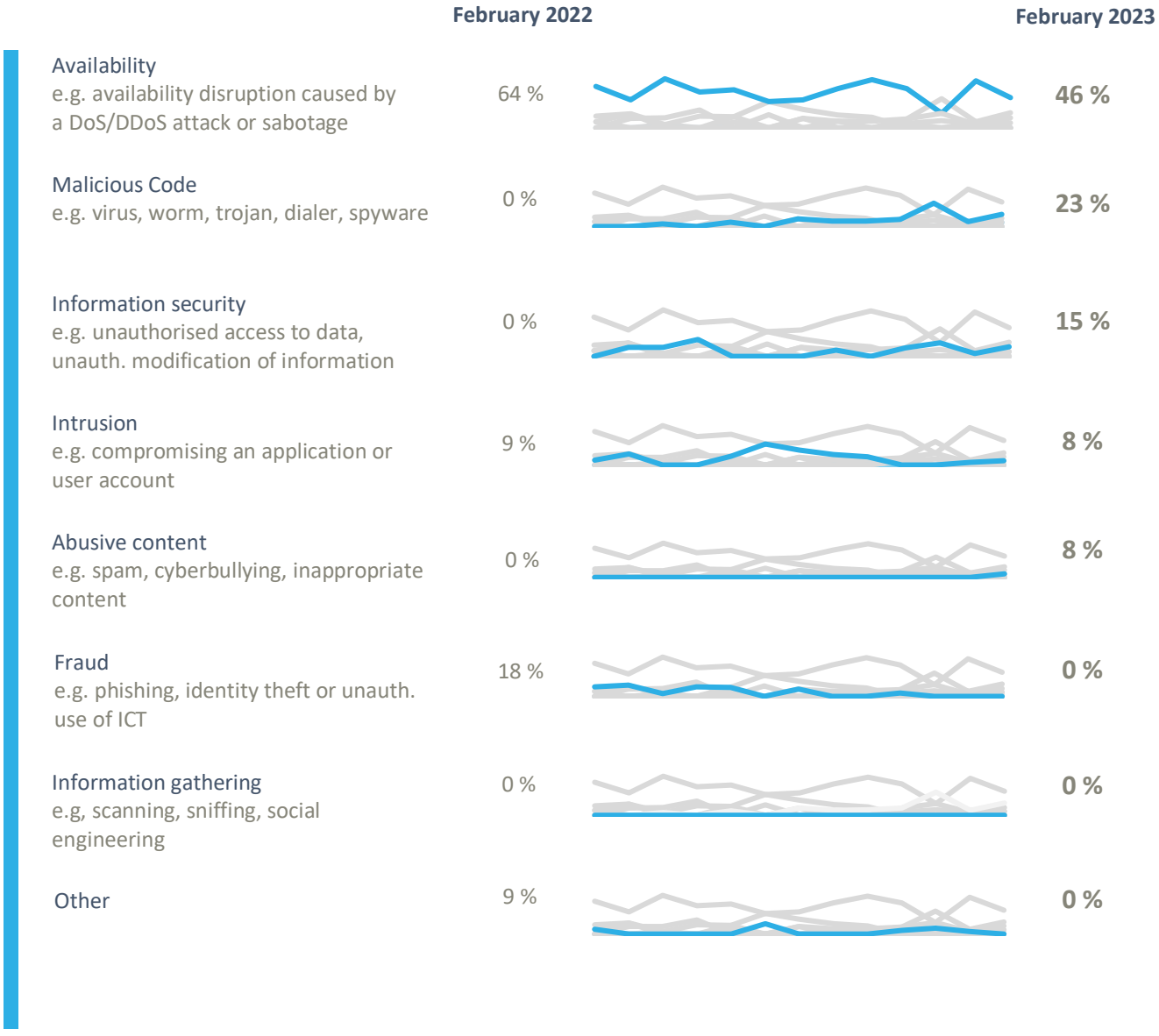


[1] NÚKIB registered seven incidents in total with liable entities according to Cyber Security Act. The remaining six incidents involved unregulated entities.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified May's incidents within the following four categories:

- The incidents resulting in unavailability of services were the most frequent ones. However, with the exception of one DDoS attack, these were incidents caused by service outages and technical errors;
- In the malicious code category, NÚKIB registered three incidents in January. All were ransomware attacks, but one of them was reported by an obligated entity more than a year late;
- In two incidents, information security was breached. The attackers accessed the victim's server, from which they subsequently downloaded data;
- NÚKIB classified the last two incidents as intrusion and abusive content. In the second case, the attackers compromised the victim's e-mail account and sent more than a thousand spam messages from it.



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

February trends in cyber seucurity from the NÚKIB's perspective [4]

Phishing, spear-phishing and social engineering

In February, NÚKIB analysed a phishing campaign aimed at Czech and European diplomatic targets. The campaign is significant mainly due to the likely origin of the attackers, their choice of targets and the high likelihood that they will continue in their activities in the forthcoming months. The campaign is detailed in the last chapter herewith.

Malware

In February, NÚKIB analysed in detail GraphicalNeutrino malware, which was used by the attackers in their phishing cyber espionage campaign described in the last chapter. Some of GraphicalNeutrino attributes coincide with EnvyScout malware that the APT29 group deployed in its phishing campaigns last year.

Vulnerabilities

VMware ESXi vulnerabilities, which are widely exploited in other European countries, appeared in two incidents. Compared to European countries, where these vulnerabilities are massively exploited, the numbers of Czech victims are relatively low.

Ransomware

The number of cyber incidents caused by ransomware handled by the NÚKIB in February was comparable to the previous ten months. ESXiArgs group hit two non-obligated entities in February. By exploiting VMware ESXi vulnerability, the group encrypted their virtual servers.

Attacks on availability

After January's wave of DDoS attacks, NÚKIB handled only one this month. However, due to its unprecedented severity, it was included among very significant incidents.

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

Technique of the month: HTML Smuggling

NÚKIB evaluates cyber incidents also on the basis of MITRE ATT&CK framework, which serves as a summary of known techniques and tactics used in cyber attacks. Within the report we focus this time on T1027.006 technique: HTML Smuggling. The attackers used it as a part of their February phishing campaign against Czech and European diplomatic targets. We cover the entire campaign in more detail in the next chapter.

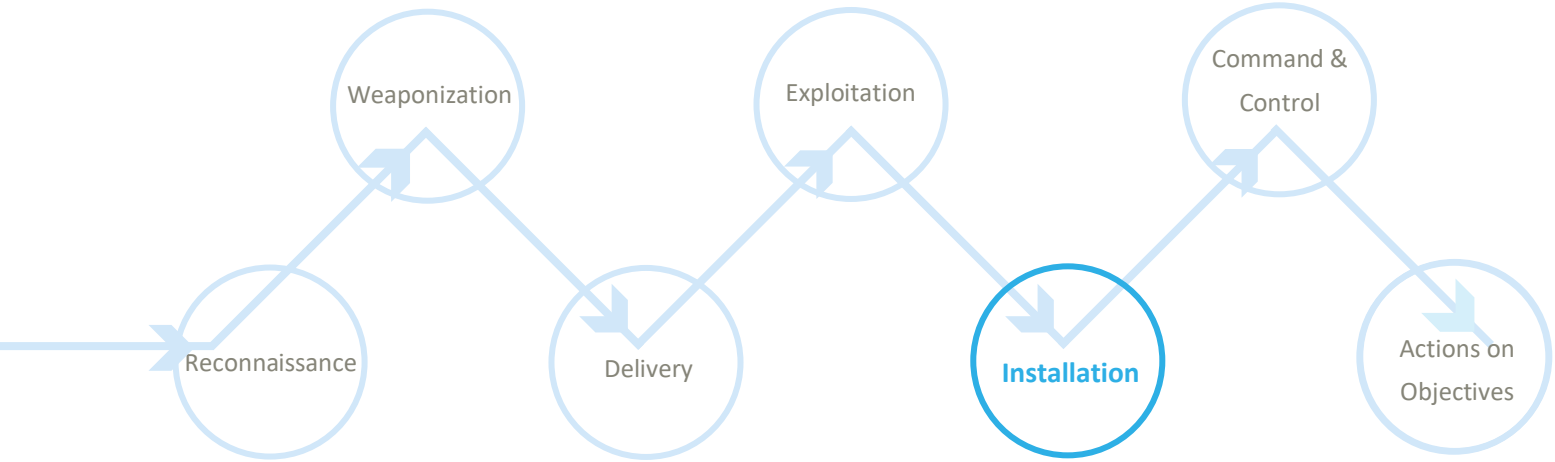
HTML Smuggling: HTML Smuggling is a technique used by attackers to avoid detection while malware is being downloaded into a computer. This is usually provides defenders with opportunity to detect and stop an attack in progress. They may identify the downloading malware in network traffic or on a web application firewall. Using HTML Smuggling, attackers try to reduce this risk of detection. The technique works as follows:

> When visiting a webpage, your browser first loads the HTML code and then displays the content of that page. Attackers “smuggle" their malicious code into HTML files that look seemingly harmless. Some security features then see it as just innocuous HTML or JavaScript traffic that can be further obfuscated to hide its true purpose. Malicious files are unpacked just only after the HTML file is uploaded to the victim's endpoint device. Because the malicious file is not downloaded over the network, but unpacked behind the firewall, it is difficult to detect it.

MITRE ID: T1027.006

Mitigation: Since the HTML Smuggling technique is difficult to detect, its mitigation is also complicated. Defending against it requires several defence in depth. The HTML Smuggling technique is often used by attackers in their phishing campaigns. From the defence point of view, it is therefore best to stop the attack at its beginning, i.e. to prevent the e-mail from reaching the user. If the e-mail gets to the user’s mailbox, the user opens it and is taken to an infected website, from which malware starts downloading via HTML Smuggling, malware execution should be prevented by security controls on endpoint devices such as antiviruses or EDR platforms.

Representation of the T1027.006 in the kill chain showing the attack phase in which the cyber actors use the technique:

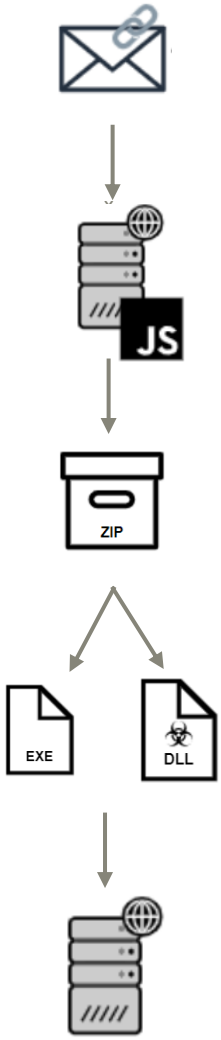


Focus on a threat: Cyber espionage campaign against diplomatic targets

In February, NÚKIB analysed a phishing campaign targeting Czech and European diplomatic targets. The attackers posed as employees of the Czech Ministry of Foreign Affairs (MFA), wrote phishing e-mails under the MFA's header, and abused the theme of ambassadors' meetings. NÚKIB has no information at this time whether the attackers have been successful in compromising any of their targets. However, the actor´s probable origin and its choice of targets show that his activities cannot be underestimated.

Analysts of RecordedFuture connect this campaign with an actor whose operational practices, motivations, and goals overlap with previous activities of the APT29 group (also known as Nobelium or CozyBear). APT29 is a highly advanced cyber espionage actor operating under the patronage of the Russian External Intelligence Service (SVR).

Based on one of the phishing e-mails, NÚKIB analysed how the attacks of the February campaign were carried out:[5]



1. The campaign started with a phishing e-mail. The attackers pretended to be employees of the Czech Foreign Ministry and claimed they wanted to schedule meetings with ambassadors. A link to the alleged schedule of the Czech ambassador was included in the e-mails.

2. The link led to a webpage with the Czech Ministry of Foreign Affairs logo and a heavily obfuscated JavaScript.

3. As soon as the victim entered the website, JavaScript immediately started downloading a ZIP archive. The attackers deployed the HTML Smuggling technique described in the previous chapter. They used this technique also during their campaigns in the previous year.

4. The ZIP archive contained two files, one with .exe and the second one with .dll extension. The DLL file was hidden, so the user could not see it in the folder after unpacking. Upon launching, the .exe file imported a hidden DLL file into itself, which was the GraphicalNeutrino malware.

5. The GraphicalNeutrino malware created persistence in the victim's device and started contacting the legitimate Notion service. Based on the previous campaigns knowledge, it is very probable that the attacker would exploit Notion service for further communication with C2 server and download additional malware. Nevertheless, at the time of writing the analysis, the authentication token for Notion was already invalid and NÚKIB was not able to analyse the attack until its very end.

[5] Infection chain includes only the information previously presented in open sources. We intentionally omit other technical findings and share them through non-public channels with our domestic and international partners.

It is highly likely that APT29 will continue its activities against Czech and European targets in the future. Very similar espionage campaigns have been conducted at least since the beginning of 2022. The time frame and the selection of targets from diplomatic circles thus indicate that APT29 seeks to obtain information related to NATO/EU, possibly the conflict in Ukraine. As long as the war lasts, the interest of Russian groups in sensitive information related to the war is expected to continue.

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/defense 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.