National Cyber and Information Security Agency

NÚKIB

Annex to reference n. 26218/2026-NÚKIB-E/630 • BRNO • OCTOBER 20, 2026

[THREAT ANALYSIS]

RUSSIAN STATE-SPONSORED ACTORS EXPLOIT VULNERABILITIES AND USERS' LACK OF VIGILANCE. MANY COMPROMISES CAN BE PREVENTED BY SIMPLE COUNTERMEASURES.

SUMMARY

- **Russian state-sponsored actors have long been carrying out cyber-attacks against the Czech Republic and its NATO and EU allies. The aim is generally cyber-espionage targeting state institutions, non-governmental organisations and selected private companies or individuals. However, attempts at destructive cyber-attacks cannot be ruled out either.**
- **Russian actors combine targeted attacks with the exploitation of readily available opportunities. In addition to technically advanced methods, they also exploit known vulnerabilities, weak passwords and user inattention. Organisations cannot therefore assume that they are not a sufficiently significant target for attackers.**
- **Attackers gain initial access primarily through phishing, exploiting vulnerabilities or breaching weak security. A specific example is compromise via the supply chain.**
- **Once initial access has been gained, Russian actors often exploit legitimate tools and services, such as cloud services, remote access tools or native system processes, thereby also reducing the likelihood of detection.**
- **The risk of a successful breach is reduced by consistent updates, multi-factor authentication, secure system configurations and user training. Prevention alone, however, is not enough: the ability to detect malicious activity in a timely manner and respond to any attacks is also crucial.**

NOTICE: Information and conclusions contained in this analysis are based on publicly available information and on information obtained through National Cyber and Information Security Agency (NÚKIB) activities at the time of publication. This is an analysis of cybersecurity from NÚKIB's perspective, based on the information available to it.

RUSSIAN ACTORS IN CYBERSPACE ARE TARGETING STATE INSTITUTIONS, NON-GOVERNMENTAL ORGANISATIONS AND SELECTED PRIVATE ENTITIES AND INDIVIDUALS

Russian state-sponsored actors have long been active in the cyberspace of NATO countries, the EU and the Czech Republic. Their malicious activity most often takes the form of cyber-espionage, targeting state institutions, non-governmental organisations, as well as selected private companies and individuals. This analysis summarises findings on the main techniques observed over the past three years or so in campaigns linked to various threat actors attributed to Russia. However, the nature of the targets and the techniques used changes over time, and **the analysis therefore does not provide a list of specific indicators of compromise, but rather a basic summary of the observed tactics, techniques and procedures (TTPs), together with basic options for their mitigation (see Annex 2).**

You do not need to be the primary target of Russian actors to become a victim. Some of their activities are blanket in nature: they automatically scan the internet for unpatched or poorly secured devices, regardless of who owns them. Compromised routers or cameras can then serve as a cover for further attacks or for gathering information. Furthermore, an organisation may be of interest not in its own right, but as a supplier or partner of the target that the attackers are actually after.

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

PHISHING EMAILS AND MESSAGES ARE AMONG THE MAIN WAYS OF GAINING ACCESS TO AN ORGANISATION

Phishing is a common method used by Russian actors to gain initial access, owing to its simplicity and relative effectiveness. The form it takes depends on the objective of the operation. It varies according to the specific objective and nature of the operation. **In campaigns targeting state institutions, attackers often use government-related themes, invitations to conferences, receptions or meetings, or lures in the form of document sharing.** When targeting private companies or individuals, the lures are usually linked to their specific activities or, conversely, to routine tasks, such as administrative procedures. Phishing is often spread via email messages, but in recent years it has also spread to messaging apps (Signal, WhatsApp).

Attackers may impersonate domestic and foreign government officials and institutions in emails, including through the use of spoofed domains. [1] For example, a Russian actor impersonated the Czech Ministry of Foreign Affairs in this way: it sent emails to foreign diplomatic missions on behalf of an assistant to the Czech ambassador from a spoofed mav.cz domain (see Annex 1). Such messages may contain malicious links or attachments. Attackers may also use social engineering techniques, whereby, for example, initial messages need not contain any malicious elements in order to build trust with the victim. Malicious links may lead to spoofed login pages or to infrastructure controlled by the attackers, which offers malicious content, including malware. Attachments, typically ZIP and RAR archives, may contain LNK files disguised as PDF documents.[2] These may also be attached PDF or Word files which either contain a link to malicious infrastructure or prompt the victim to enter their login details in order to supposedly 'unlock' the content. [3] Attackers can also exploit vulnerabilities in email clients and services, such as Microsoft Outlook, Exchange or Zimbra [4] and Roundcube [5]. For more information on specific vulnerabilities in the context of email communication, see below.

A specific category of phishing involves targeting users via messaging apps, particularly Signal and WhatsApp. In these cases, the app itself and its encryption are not compromised. Instead, the attack once again relies on exploiting the user's lack of vigilance.

One of the tactics used by attackers is to pose as the app's technical support team. They contact the victim on behalf of the 'security team' and, under the pretence of protecting their account, trick them into revealing a verification code or PIN, or scanning a QR code. By doing so, the victim grants the attackers access to their account, allowing them to read their messages. [6] In other cases, they pose as a specific person. First, they gain the victim's trust and then invite them to a meeting. The link to the meeting prompts the victim to log in or enter a code, most commonly for Microsoft services. The victim thus unwittingly grants the attackers access to their work account, even if they have multi-factor authentication enabled. [7] In September 2026, NÚKIB warned of the risk of Signal account compromise and issued a set of recommendations.

So-called Adversary-in-the-Middle (AiTM) phishing platforms are also being used with increasing frequency; these act as an intermediary between the victim and the legitimate login service. They enable attackers to capture not only login credentials but also session authentication tokens, thereby bypassing multi-factor authentication. Once again, Microsoft 365 accounts and other cloud services are the primary targets.

Phishing: Detection and countermeasures

- Filter emails and block high-risk attachments (LNK, archives) and suspicious links.
- Train users to verify unexpected requests for login details, codes or meetings via another channel and to report suspicious messages.
- Detect or block suspicious processes (such as PowerShell) launched after opening an archive or LNK file.

ATTACKERS ARE EXPLOITING UNPATCHED VULNERABILITIES; TIMELY UPDATES ARE ESSENTIAL

Another common vector for gaining initial access is the exploitation of vulnerabilities. Russian threat actors have been observed exploiting various types of vulnerabilities, including zero-day vulnerabilities

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

as well as older ones. Furthermore, given the rise in the number of vulnerabilities detected using AI models, it is likely (50–75 %) that Russian threat actors will utilise this vector to an increasing extent.

Russian actors combine phishing with the exploitation of vulnerabilities in email services and clients, particularly Microsoft Outlook and Exchange, Zimbra and Roundcube. The documented campaigns involved so-called zero-click and half-click attacks, where **simply receiving or viewing a message is sufficient to trigger the malicious code, without any interaction with an attachment or link.** Both zero-day vulnerabilities and flaws for which a patch already existed were exploited. **For organisations, this means that the speed at which updates to their email infrastructure are deployed directly determines the level of risk**. [8] Attackers are also exploiting vulnerabilities in programmes such as WinRAR; a system may be compromised when a malicious archive received via email is extracted.[9]

Exploitation of vulnerabilities: Detection and countermeasures

- Keep track of your devices and services, particularly those accessible via the internet.
- Monitor vulnerabilities in your products (NÚKIB information service, CISA list of exploited vulnerabilities) and prioritise patching those that have been exploited and are accessible via the internet.
- For new vulnerabilities, check whether they have already been exploited before a patch is released.
- Decommission or isolate unsupported devices.

Another category involves vulnerabilities in devices at the network perimeter (known as 'edge devices'), such as VPN gateways, firewalls and routers. In most cases, this involves compromise through the exploitation of vulnerabilities in products from companies offering these solutions, such as Fortinet, Ivanti, Cisco or Citrix, or the compromise of smaller devices, such as routers from MikroTik, Ubiquiti or TP-Link. Compromising these devices allows attackers to intercept network traffic whilst also providing a foothold for penetrating other devices and systems within the organisation. In 2026, the APT28 group also took control of TP-Link routers in the Czech Republic. It exploited a vulnerability and unchanged default passwords, and via the compromised routers intercepted users' passwords and login tokens, for example for corporate email.[10]

WEAK PASSWORDS AND INCORRECT CONFIGURATIONS MAKE IT EASIER FOR ATTACKERS TO COMPROMISE SYSTEMS

Another point of entry is the misconfiguration or weak security of devices or services accessible via the internet. **This often involves weak or default passwords, a lack of multi-factor authentication for remote access (such as VPNs), or unnecessarily exposed ports and administrative interfaces on routers, firewalls or other devices.**

Russian actors (particularly hacktivist groups) have used this tactic primarily in campaigns targeting organisations across various industrial sectors.[11] Their main targets were control consoles and operational technology interfaces that are accessible from the internet without passwords or with only weak passwords. Once access was gained, the attackers were able to alter operational settings and sabotage systems.

In a Russian campaign against the Polish energy sector at the end of 2025, attackers penetrated the networks of more than thirty wind and solar power stations, one heating plant and one industrial enterprise via FortiGate devices accessible over the internet. They logged into VPN accounts without multi-factor authentication; in one instance, they used device configurations that had been leaked onto a criminal forum.[12]

Misconfigurations: Detection and countermeasures

- Enable multi-factor authentication for VPNs, remote management and privileged accounts, and change default passwords.
- Restrict what is accessible from the internet: administration interfaces, routers, cameras and OT systems.
- Monitor logins, particularly repeated failed attempts and logins from suspicious locations.
- Divide the network into segments and restrict permissions so that a compromise of one device does not result in the compromise of others.

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

IP cameras constitute a specific category, as they are exploited for espionage as well as to directly support military operations. [13] These devices are often protected by weak authentication mechanisms and can therefore be easily compromised if exposed to the internet. Vulnerabilities can also serve as attack vectors, particularly if the cameras do not have up-to-date firmware, are operated beyond the end of vendor support, or come from an untrusted manufacturer.

A COMPROMISED CLOUD SERVICE ACCOUNT CAN PROVIDE ACCESS TO EMAILS AND INTERNAL DOCUMENTS

In recent years, Russian actors have also been increasingly using attacks based on stolen, leaked or reused login credentials. **The most common techniques include password spraying, credential stuffing and other forms of attacks against internet-accessible services, such as VPN gateways, Outlook Web Access, Microsoft 365 and other systems enabling remote access.**[14]

The password spraying technique involves using a small number of common passwords against a large number of accounts, whereby attackers attempt to evade account lockout mechanisms and the detection of brute-force attacks. Accounts that tend to be neglected – such as service, inactive or test accounts without multi-factor authentication – are also popular targets. In 2023, the Russian APT29 group gained access to Microsoft's corporate environment via a forgotten test account.[15]

Cloud, identities and accounts: Detection and countermeasures

- Implement phishing-resistant multi-factor authentication (e.g. security keys), at least for administrators and remote access.
- Regularly review accounts and permissions: delete inactive accounts and limit service or privileged accounts to the absolute minimum.
- Restrict access to critical systems to authorized users and managed devices only (using Conditional Access).
- Monitor failed and unusual login attempts (mass attempts, unusual locations) as well as the registration of new devices or authentication methods.

COMPROMISE VIA THE SUPPLY CHAIN POSES A THREAT TO, AMONGST OTHERS, ORGANISATIONS SUPPORTING UKRAINE

Russian actors have long exploited trusted relationships between organisations, suppliers and service providers. Compromising a single entity can grant access to many others, whilst also making detection more difficult.

One example is the SolarWinds incident (2020), when APT29 spoofed a legitimate software update. [16] In 2023, the same actor exploited a large number of unpatched TeamCity servers – a development tool from JetBrains – thereby gaining access to several dozen software and IT companies, which in turn enabled attacks on JetBrains' customers. [17]

In recent years, Russian actors have also been increasingly targeting the wider ecosystem of suppliers and partners, including IT and cloud service providers, systems integrators, and logistics and technology companies. Such suppliers often have trusted access to their customers' networks, and if attackers gain control of them, they can use them to gain access to their customers. This approach was observed, for example, in a campaign that targeted organisations forming part of the defence and logistics ecosystem of Ukraine and its allies, including the Czech Republic.[18]

Supply chains: Detection and countermeasures

- Maintain an overview of your suppliers and their access to your network, and monitor this access.
- Restrict suppliers' access to only those systems they absolutely need, and require them to use multi-factor authentication.
- Monitor suppliers' activities, particularly their privileged access.
- Assess suppliers' security during the selection process and include this in contracts (in the case of public procurement, it is possible to take into account NÚKIB warnings)

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

BASIC SECURITY MEASURES WILL PREVENT MOST BREACHES; EARLY DETECTION WILL LIMIT THE DAMAGE

Russian actors employ a range of other techniques depending on the objective of the operation. Nevertheless, adherence to basic cybersecurity principles remains effective in preventing a significant proportion of their activities. However, such measures do not guarantee complete protection. If an attack is successful, it is therefore equally important to detect it in good time.

Educating users on how to identify phishing effectively complements timely updates, multi-factor authentication, privileged access management and secure system configuration. Regular identity and account management, the thorough monitoring of internet-accessible services and the restriction of default or weak login credentials are also crucial. These basic measures reduce the likelihood of a successful attack.

It is essential for an organisation to be able to detect an ongoing compromise in a timely manner. This involves the continuous monitoring of security events, detection of login anomalies, tracking of suspicious network traffic, and monitoring of privileged account activities. Attackers commonly attempt to disguise their activity amongst legitimate administrative operations; it is therefore essential to focus not only on known indicators of compromise, but also on unusual patterns of behaviour within the organisation's environment.

Attackers' techniques, tools and infrastructure are constantly evolving; many successful compromises still exploit known vulnerabilities, inadequately protected accounts, the absence of multi-factor authentication, incorrectly configured systems or human error. Vulnerability management, identity protection, network segmentation, backups, user training and the ability to detect and respond in a timely manner therefore significantly reduce both the likelihood of a breach and the impact of an incident.

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

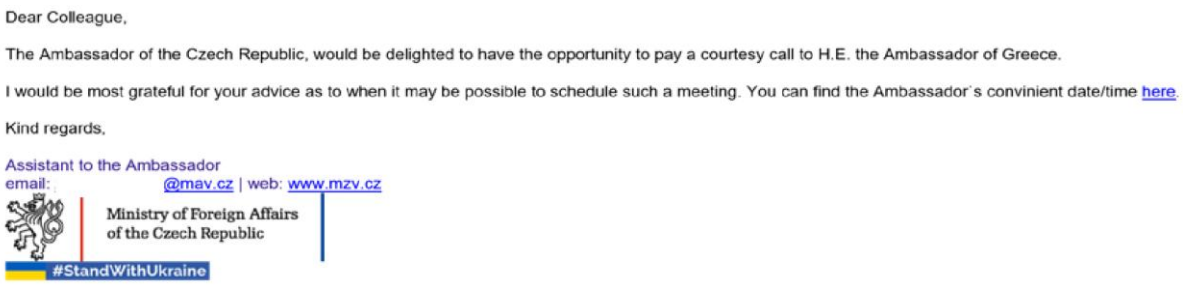
ANNEX 1: EXAMPLES OF PHISHING

Email phishing

A Russian actor spoofed the identity of the Czech Ministry of Foreign Affairs to carry out attacks against other targets (Figure 1).

As part of the campaign, the actor exploited a vulnerability in the WinRAR application to deliver cyber-espionage malware via email attachments.

Figure 1: A phishing email impersonating the Czech Ministry of Foreign Affairs



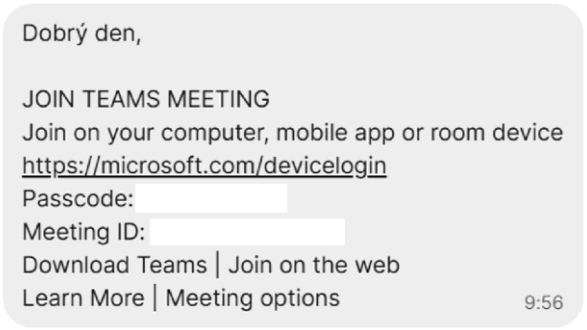
Source: NÚKIB

Phishing via the Signal messaging app

One of the techniques observed is known as 'OAuth phishing'. This involves messages in which the attacker poses as someone interested in a video call with the victim, and then asks the victim to log in to an 'authentication portal' or to send an authentication code. Microsoft applications and services are often the targets. The attacker typically begins by building trust with the victim. The victim then receives a fake meeting invitation.

'Device Code phishing', which exploits the Device Code Flow feature, operates in a similar way (Figure 2). In September 2026, NÚKIB published a warning on the NÚKIB Portal, in which it highlighted the ongoing phishing campaign and recommended how to counter the threat.

Figure 2: A message sent via the Signal app urging a user to join a fake meeting on the MS Teams platform



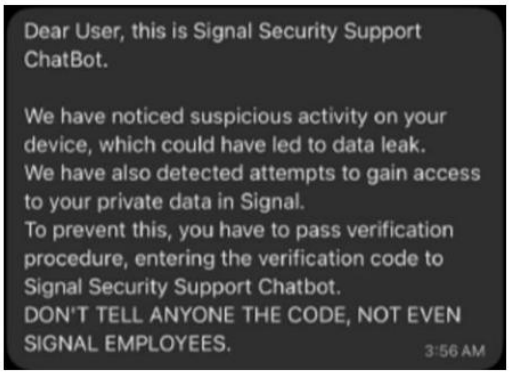
Source: NÚKIB

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

Another form of phishing involves sending out fake messages in which attackers pose as Signal's technical or security support team. In these messages, they urge users to hand over their PIN or other login details (Figure 3).

Malicious links or QR codes may also be sent to victims outside the Signal app, directing them to fake external domains. Once again, these may appear to relate to device security, invitations to various groups or requests to connect with an unknown user (Figure 4).[19]

Figure 3: A fake message urging users to disclose their security PIN



Source: Google Threat Intelligence Group

Figure 4: A fake QR code and a malicious link to join a group



Source: Google Threat Intelligence Group

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

ANNEX 2: RELATED TACTICS USED AFTER GAINING INITIAL ACCESS

THE ABUSE OF REMOTE MANAGEMENT TOOLS

Russian actors are abusing legitimate remote monitoring and management tools (RMM) as a means of gaining access to the victim's environment (see Annex 3 for a list of tools that have been abused in the past). Installation or execution may result from social engineering, whereby the attacker poses, for example, as technical support, a supplier or the internal IT department, and tricks the user to authorise remote access.

Successful exploitation of an RMM tool gives attackers a high degree of control over the compromised device and enables them to carry out further malicious activities, including data theft, the deployment of malware, lateral movement or the establishment of long-term persistence.

Remote management tools: Detection and countermeasures

- Only allow approved applications and restrict users' ability to install software. Block or detect unauthorised RMM tools (EDR).
- Monitor network traffic to known domains of remote management providers that the organisation does not use.
- Advise users never to grant remote access to unknown individuals and to verify every request via a different channel.

THE ABUSE OF LEGITIMATE CLOUD, WEB AND COMMUNICATION SERVICES FOR DATA EXFILTRATION AND C2 COMMUNICATION

Another tactic involves exploiting legitimate services for data exfiltration (see Annex 3 for a list). These services usually encrypt network traffic and, by their very nature, make it more difficult to detect malicious instances.

Misuse of services for C2: Detection and countermeasures

- Detect or block services that the organisation does not actively use.
- Monitor large volumes of outgoing data and regularly recurring connections to these services.

LIVING OFF THE LAND TECHNIQUES (LOTL)

Once they have gained access, Russian actors often exploit legitimate operating system tools rather than deploying their own malware. Typically, these include tools such as PowerShell, WMI, schtasks, rundll32, certutil or PsExec, which are standard components of system administration. This approach limits the number of detectable indicators of compromise and makes it difficult to distinguish malicious activity from legitimate administration.[20]

Living off the Land: Detection and countermeasures

- Monitor unusual use of administrative tools, such as PowerShell or PsExec, on standard users' computers or outside working hours.
- Restrict who is permitted to use these tools and from where, and enable logging for them.

ACTIVE DIRECTORY AND LATERAL MOVEMENT

Once the first account has been compromised, Russian actors typically attempt to gain higher privileges and expand their access across the network. The aim is usually to obtain domain administrator privileges, take control of the Active Directory environment and ensure long-term persistence. Techniques observed include stealing credentials from memory (the LSASS process) or from the Active Directory database (NTDS.dit), as well as Kerberoasting, Pass-the-Hash, DCSync and the exploitation of privileged and service accounts.

AD and lateral movement: Detection and countermeasures

- Monitor privileged accounts and changes in the Active Directory.
- Detect credential theft (access to LSASS, AD database export) and Kerberoasting, Pass-the-Hash and DCSync techniques, ideally using EDR.
- Restrict and regularly review service and administrator accounts. Administrators should not log in to standard workstations.

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

ANNEX 3: SELECTED VULNERABILITIES, TOOLS AND SERVICES EXPLOITED BY RUSSIAN ACTORS (2023–2026)

Category	Examples	
Remote monitoring and management (RMM)[21]	Atera, IntelliAdmin, LiteManager, RemCom, RMS, Remote Utilities, Splashtop, SuperOps, TeamViewer, UltraVNC	
Cloud, web and communication services[22]	4shared, Dropbox, Firebase, Gmail, Google Drive, Google Calendar, GMX, Notion, MEGA, OneDrive, Telegram, Trello, Koofr, VFEmail, GitHub/Gists, Pastebin, Mockbin, Mocky.io, Rclone, Webhook.site, InfinityFree, Byet, ngrok, Filen.io	
LOTL tools	PowerShell, WMI, PsExec, schtasks, certutil, rundll32, regsvr32, mshta	
Exploited vulnerabilities	**Windows**	
	CVE-2026-42897	Microsoft Exchange Server (Outlook Web Access)
	CVE-2026-21513	Windows MSHTML
	CVE-2026-21510	Windows Shell
	CVE-2026-21509	Microsoft Office
	CVE-2023-23397	Microsoft Outlook for Windows
	Apple	
	CVE-2026-20700	Apple iOS (dyld)
	CVE-2025-43520	Apple iOS kernel
	CVE-2025-43510	Apple iOS kernel
	CVE-2025-43529	Apple WebKit (iOS/Safari)
	CVE-2025-31277	Apple WebKit (iOS/Safari)
	CVE-2024-23222	Apple WebKit (iOS/Safari)
	CVE-2023-43000	Apple WebKit (iOS/Safari)
	CVE-2023-41993	Apple WebKit (iOS/Safari)
	CVE-2022-48503	Apple WebKit (iOS/Safari)
	CVE-2025-14174	ANGLE graphics library (Apple iOS/Safari, Google Chrome)
	Google	
	CVE-2024-5274	Google Chrome (V8)
	CVE-2024-4671	Google Chrome
	Zimbra	
	CVE-2025-66376	Zimbra Collaboration Suite
	CVE-2025-27915	Zimbra Collaboration Suite
	CVE-2024-27443	Zimbra Collaboration Suite
	Roundcube	
	CVE-2025-49113	Roundcube Webmail

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

	CVE-2024-42009	Roundcube Webmail
	CVE-2023-43770	Roundcube Webmail
	MDaemon	
	CVE-2025-3929	MDaemon Email Server
	CVE-2024-11182	MDaemon Email Server
	WinRAR	
	CVE-2025-8088	WinRAR
	CVE-2025-6218	WinRAR
	Ostatní	
	CVE-2026-8496	SOGo webmail (Alinto)
	CVE-2024-1709	ConnectWise ScreenConnect
	CVE-2023-48788	Fortinet FortiClient EMS
	CVE-2023-42793	JetBrains TeamCity
	CVE-2023-27532	Veeam Backup & Replication
	CVE-2023-22518	Atlassian Confluence Data Center and Server
	CVE-2023-50224	TP-Link routers (TL-WR841N)
	CVE-2018-0171	Cisco IOS and IOS XE (Smart Install)

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

SOURCES

[1] Recorded Future. 2026. BlueDelta Targets Defense and Diplomacy with HOOKEDGE. https://www.recordedfuture.com/research/bluedelta-targets-with-hookedge

[2] Mandiant. 2023. Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations. https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing

Lab52. 2026. Operation MacroMaze: new APT28 campaign using basic tooling and legit infrastructure. https://lab52.io/blog/operation-macromaze-new-apt28-campaign-using-basic-tooling-and-legit-infrastructure/

[3] DeepStrike. 2026. Star Blizzard: Credential Phishing Against Governments and Researchers. https://deepstrike.io/blog/star-blizzard

TheCitizenLab. 2024. Rivers of Phish. Sophisticated Phishing Targets Russia's Perceived Enemies Around the Globe. https://citizenlab.ca/research/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

[4] CISA. 2026. Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-204a

[5] CISA. 2025. Russian GRU Targeting Western Logistics Entities and Technology Companies. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

[6] AIVD. 2026. Cybersecurity Advisory. Phishing via messaging apps Signal and WhatsApp. https://english.aivd.nl/documents/2026/03/09/cybersecurity-advisory.-phishing-via-messaging-apps-signal-and-whatsapp

[7] Microsoft. 2025. Storm-2372 conducts device code phishing campaign. https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

Volexity. 2025. Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication. https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

[8] Proofpoint. 2026. Cleaning Out Inboxes: TA488 Comes for Outlook with Another Half-Click Exploit. https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit

[9] Trendmicro. 2026. Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open. https://www.trendmicro.com/ru_ru/research/26/f/old-winrar-flaw-fuels-attacks-on-ukraine.html

[10] NÚKIB. 2026. Routery TP-Link kompromitovány ruským státním aktérem APT28. https://nukib.gov.cz/cs/infoservis/aktuality/2394-routery-tp-link-kompromitovany-ruskym-statnim-akterem-apt28/

AWS. 2025. Amazon Threat Intelligence identifies Russian cyber threat group targeting Western critical infrastructure. https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-russian-cyber-threat-group-targeting-western-critical-infrastructure/

[11] NÚKIB. 2025. NÚKIB has joined an international warning about pro-Russian hacktivist groups attacking critical infrastructure entities. https://nukib.gov.cz/en/infoservis-en/news/2357-the-nukib-has-joined-an-international-warning-about-pro-russian-hacktivist-groups-attacking-critical-infrastructure-entities/

[12] CERT.PL. 2026. Follow-Up Analysis of the 29 December 2025 Energy Sector Incident. https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Follow_up_Report_2025.pdf

[13] AIVD. 2026. Cyberadvies Russische statelijke actoren compromitteren IP-camera's in Europa voor militaire doeleinden. https://www.aivd.nl/documenten/2026/07/10/cyberadvies-russische-statelijke-actoren-compromitteren-ip-cameras-in-europa-voor-militaire-doeleinden

[14] NCSC. 2024. SVR cyber actors adapt tactics for initial cloud access. https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access

[15]WIZ. 2024. Midnight Blizzard attack on Microsoft corporate environment: a detailed analysis, detections and recommendations. https://www.wiz.io/blog/midnight-blizzard-microsoft-breach-analysis-and-best-practices

[16] FBI. 2021. Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks. https://www.fbi.gov/news/press-releases/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabilities-to-compromise-us-and-allied-networks

[17] CISA. 2023. Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

[18] Trendmicro. 2026. Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities. https://www.trendmicro.com/en/research/26/c/pawn-storm-targets-govt-infra.html

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

[19] AIVD. 2026. Cybersecurity Advisory. Phishing via messaging apps Signal and WhatsApp. https://english.aivd.nl/documents/2026/03/09/cybersecurity-advisory.-phishing-via-messaging-apps-signal-and-whatsapp

[20] NSA. 2024. NSA Issues Updated Guidance on Russian SVR Cyber Operations. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3931959/nsa-issues-updated-guidance-on-russian-svr-cyber-operations/

Lawfare. 2023. Living Off the Land Is the New Normal + When Hacks Upset Housing Markets. https://www.lawfaremedia.org/article/living-off-the-land-is-the-new-normal-when-hacks-upset-housing-markets

[21] BushidoUK. 2026. Russian-APT-Tool-Matrix/Tools/Exfiltration. https://github.com/BushidoUK/Russian-APT-Tool-Matrix/blob/main/Tools/Exfiltration.md

[22] BushidoUK. 2026. Russian-APT-Tool-Matrix/Tools/RMM-Tools. https://github.com/BushidoUK/Russian-APT-Tool-Matrix/blob/main/Tools/RMM-Tools.md

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/

TERMS OF USE OF INFORMATION

The use of the information provided shall be in accordance with the Traffic Light Protocol methodology. The information is marked with a flag that specifies the conditions of use of the information. The following flags are set, indicating the nature of the information and the conditions of use:

Colour	Conditions of use
Red **TLP:RED**	The information may not be provided to any person other than the person to whom the information was addressed unless other persons to whom such information may be provided are specifically identified. Where the recipient considers it important to disclose the information to other bodies, this may be done only with the consent of the originator of the information.
Orange **TLP:AMBER+STRICT**	The information may only be shared within the recipient's organisation, and only to persons who meet the need-to-know and whose information is relevant to resolving the problem or threat identified in the information.
Orange **TLP:AMBER**	Information may be shared within the recipient organisation and to its partners, and only to persons who meet the need-to-know and whose information is relevant to resolving the problem or threat identified in the information.
Green **TLP:GREEN**	Information may be shared within the beneficiary's organisation and, where appropriate, with other partners of the beneficiary, but not through publicly available channels; the beneficiary must ensure the confidentiality of the communication when forwarding it.
TLP:CLEAR	The information may be further provided and disseminated without restriction. Any restrictions based on the intellectual property rights of the originator and/or recipient or third parties are not affected by this provision.

EXPRESSION OF NÚKIB PROBABILITIES

Expression	Probability
Almost certainly	*90-100 %*
Highly likely	*75-85 %*
Likely	*55-70 %*
Cannot be ruled out/Realistic possibility	*40-50 %*
Unlikely	*20-35 %*
Highly unlikely	*0-15 %*

TLP:CLEAR - Disclosure not limited. Learn more at https://www.first.org/tlp/