Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j. 26218/2026-NÚKIB-E/630 • BRNO • 20. ŘÍJNA 2026

[ANALÝZA HROZBY]

RUŠTÍ STÁTEM SPONZOROVANÍ AKTÉŘI ZNEUŽÍVAJÍ ZRANITELNOSTI I NEPOZORNOST UŽIVATELŮ. ŘADĚ KOMPROMITACÍ PŘEDEJDOU JEDNODUCHÁ PROTIOPATŘENÍ.

SHRNUTÍ

- **Ruští státem sponzorovaní aktéři dlouhodobě podnikají kybernetické útoky proti ČR a spojencům v NATO a EU. Cílem je zpravidla kyberšpionáž zaměřená na státní instituce, nevládní organizace i vybrané soukromé společnosti či jednotlivce. Nelze však vyloučit ani pokusy o destruktivní kybernetické útoky.**
- **Ruští aktéři kombinují cílené útoky s vyhledáváním snadno dostupných příležitostí. Vedle technicky pokročilých metod využívají také známé zranitelnosti, slabá hesla a nepozornost uživatelů. Organizace proto nemohou spoléhat na to, že pro útočníky nejsou dostatečně významným cílem.**
- **Počáteční přístup útočníci získávají primárně prostřednictvím phishingu, zneužitím zranitelností či prolomením slabého zabezpečení. Specifickým případem jsou kompromitace skrze dodavatelský řetězec.**
- **Po získání počátečního přístupu ruští aktéři často zneužívají legitimní nástroje a služby, jako jsou cloudové služby, nástroje vzdáleného přístupu či nativní systémové procesy, čímž zároveň snižují pravděpodobnost odhalení.**
- **Riziko úspěšného průniku snižují důsledné aktualizace, vícefaktorové ověřování, bezpečné nastavení systémů a školení uživatelů. Samotná prevence však nestačí: klíčová je rovněž schopnost včasné detekce škodlivé aktivity a reakce na případné napadení.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

RUŠTÍ AKTÉŘI V KYBERPROSTORU CÍLÍ NA STÁTNÍ INSTITUCE, NEVLÁDNÍ ORGANIZACE I VYBRANÉ SOUKROMÉ SUBJEKTY A OSOBY

Ruští státem sponzorovaní aktéři jsou v kyberprostoru zemí NATO, EU i ČR dlouhodobě aktivní. Jejich škodlivá aktivita má nejčastěji podobu kyberšpionáže, jejímž cílem se stávají státní instituce, nevládní organizace i vybrané soukromé společnosti a jednotlivci. Tato analýza shrnuje poznatky o hlavních technikách, které byly v posledních přibližně třech letech pozorovány v kampaních spojovaných s různými aktéry hrozeb připisovaných Rusku. Povaha cílů i použité techniky se však v čase mění a **analýza tudíž nenabízí výčet konkrétních indikátorů kompromitace, ale základní shrnutí pozorovaných taktik, technik a procedur (TTPs) spolu se základními možnostmi jejich mitigace (viz Příloha 2)**.

Pro ruské aktéry nemusíte být hlavním cílem, abyste se stali obětí. Část jejich aktivit je plošná: na internetu automatizovaně vyhledávají neopravená či slabě zabezpečená zařízení bez ohledu na to, komu patří. Ovládnuté routery či kamery pak mohou sloužit jako zástěrka pro další útoky nebo ke sběru informací. Organizace navíc může být zajímavá nikoli sama o sobě, ale jako dodavatel či partner cíle, o který útočníci skutečně usilují.

PODVODNÉ E-MAILY A ZPRÁVY PATŘÍ MEZI HLAVNÍ CESTY DO ORGANIZACE

Phishing je pro ruské aktéry běžnou cestou k prvotnímu přístupu díky jednoduchosti a relativní účinnosti. Podoba závisí na cíli operace. Jeho podoba se liší podle konkrétního cíle a charakteru operace. **Při kampaních zaměřených na státní instituce útočníci často využívají vládní tematiky, pozvánky na konference, recepce, jednání či návnady v podobě sdílení dokumentů.** Při cílení na soukromé společnosti či jednotlivce bývají návnady spojené s jejich konkrétní činností, nebo naopak běžnou agendou, například administrativními

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

úkony. Phishing je často šířen prostřednictvím e-mailových zpráv, ale v posledních letech se rozšířil i na komunikační aplikace (Signal, WhatsApp).

Útočníci mohou v e-mailech zneužívat identitu tuzemských i zahraničních vládních představitelů a institucí, včetně podvržených domén.[1] Takto ruský aktér zneužil například identitu českého Ministerstva zahraničních věcí: zahraničním diplomatickým misím rozesílal e-maily jménem asistenta českého velvyslance z podvržené domény mav.cz (viz Příloha 1). Takové zprávy mohou obsahovat škodlivé odkazy nebo přílohy. Útočníci taktéž mohou využít prvky sociálního inženýrství, kdy například počáteční zprávy nemusejí obsahovat škodlivý prvek, aby došlo k vybudování důvěry s obětí. Škodlivé odkazy mohou vést na podvržené přihlašovací stránky nebo na infrastrukturu ovládanou útočníky, která nabízí škodlivý obsah včetně malwaru. Přílohy, typicky archivy ZIP a RAR, mohou obsahovat LNK soubory maskované jako PDF dokumenty.[2] Může jít také o přiložené PDF či Word soubory, které buď obsahují odkaz na škodlivou infrastrukturu či vyzývají oběť k zadání přihlašovacích údajů za účelem údajného ‚odemčení' obsahu.[3] Útočníci mohou zneužívat také zranitelnosti e-mailových klientů a služeb, například Microsoft Outlook, Exchange či Zimbra[4] a Roundcube[5]. Více informací ke konkrétním zranitelnostem v kontextu e-mailové komunikace viz níže.

Specifickou kategorii phishingu představuje cílení skrze komunikační aplikace, zejména Signal či WhatsApp. Zde nedochází k prolomení samotné aplikace a jejího šifrování, ale opět ke zneužití nepozornosti uživatele.

Jedním z postupů útočníků je vydávání se za technickou podporu aplikace. Oběť osloví jménem „bezpečnostního týmu" a pod záminkou ochrany účtu ji přimějí sdělit ověřovací kód či PIN nebo naskenovat QR kód. Tím útočníkům předá přístup ke svému účtu a ti pak mohou číst její zprávy.[6] V jiných případech se vydávají za konkrétního člověka. Nejprve si získají důvěru oběti a poté ji pozvou na schůzku. Odkaz na schůzku ji vyzve k přihlášení nebo k zadání kódu, nejčastěji ke službám Microsoft. Oběť tak útočníkům nevědomky otevře přístup ke svému pracovnímu účtu, a to i v případě, že má zapnuté vícefaktorové ověřování.[7] Na hrozbu kompromitace aplikace Signal v září 2026 upozornil i NÚKIB a vydal sadu doporučení.

Stále častěji jsou využívány také tzv. Adversary-in-the-Middle (AiTM) phishingové platformy, které fungují jako prostředník mezi obětí a legitimní přihlašovací službou. Umožňují zachytit nejen přihlašovací údaje, ale i autentizační tokeny relace, a obejít tak vícefaktorové ověřování. Cílem bývají opět zejména účty Microsoft 365 a další cloudové služby.

Phishing: detekce a protiopatření

- Filtrujte e-maily a blokujte rizikové přílohy (LNK, archivy) i podezřelé odkazy.
- Školte uživatele, aby neočekávané žádosti o přihlášení, kód nebo schůzku ověřovali jiným kanálem a podezřelé zprávy hlásili.
- Detekujte či blokujte podezřelé procesy (například PowerShell) spuštěné po otevření archivu nebo LNK souboru.

ÚTOČNÍCI ZNEUŽÍVAJÍ NEOPRAVENÉ ZRANITELNOSTI, VČASNÉ AKTUALIZACE JSOU ZÁSADNÍ

Dalším častým vektorem pro získání prvotního přístupu je zneužívání zranitelností. Ruští aktéři hrozeb byli odhaleni při zneužívání různých druhů zranitelností, včetně zranitelností nultého dne, ale i starších. V kontextu nárůstu počtu odhalovaných zranitelností odhalovaných pomocí AI modelů bude navíc pravděpodobně (50–75 %) tento vektor ruskými aktéry využíván v rostoucí míře.

Ruští aktéři phishing kombinují se zneužitím zranitelností v e-mailových službách a klientech, zejména Microsoft Outlook a Exchange, Zimbra a Roundcube. V dokumentovaných kampaních šlo o tzv. zero-click a half-click útoky, kdy **ke spuštění škodlivého kódu stačí zprávu přijmout nebo zobrazit bez interakce s přílohou či odkazem**. Zneužity byly zranitelnosti nultého dne i chyby, pro které již existovala oprava. **Pro organizace to znamená, že rychlost nasazení aktualizací e-mailové infrastruktury přímo určuje míru rizika**.[8] Útočníci zneužívají také zranitelnosti programů, například WinRAR; ke kompromitaci může dojít při rozbalení škodlivého archivu doručeného e-mailem.[9]

Další kategorií jsou zranitelnosti zařízení na perimetru sítě (tzv. edge devices), například VPN bran, firewallů a routerů. Většinou se jedná o kompromitaci prostřednictvím zneužití zranitelností v produktech

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

společností nabízejících tato řešení, například Fortinet, Ivanti, Cisco či Citrix, případně o kompromitaci menších zařízení, jako jsou routery značek MikroTik, Ubiquiti či TP-Link. Jejich kompromitace útočníkům umožňuje zachytávat síťový provoz a zároveň poskytuje výchozí bod pro průnik k dalším zařízením a systémům organizace. V roce 2026 skupina APT28 ovládla i routery TP-Link v ČR. Zneužila zranitelnost a neměněná výchozí hesla a přes napadené routery zachytávala hesla a přihlašovací tokeny uživatelů, například k firemní poště.[10]

Zneužívání zranitelností: detekce a protiopatření

- Mějte přehled o svých zařízeních a službách, zejména o těch dostupných z internetu.
- Sledujte zranitelnosti ve svých produktech (infoservis NÚKIB, seznam zneužívaných zranitelností CISA) a nejdřív opravujte ty zneužívané a dostupné z internetu.
- U nových zranitelností ověřte, zda nebyly zneužity už před opravou.
- Nepodporovaná zařízení vyřaďte nebo izolujte.

SLABÁ HESLA A CHYBNÉ NASTAVENÍ USNADŇUJÍ ÚTOČNÍKŮM PRŮNIK DO SYSTÉMU

Další vstupní bránou je miskonfigurace či slabé zabezpečení zařízení či služeb dostupných z internetu. **Jde často o slabá či výchozí hesla, chybějící vícefaktorové ověření u vzdáleného přístupu (například VPN) nebo zbytečně otevřené porty a administrační rozhraní routerů, firewallů či jiných zařízení.**

Ruští aktéři (zejména hacktivistické skupiny) tuto taktiku používali zejména v kampaních vůči cílům v různých průmyslových odvětvích.[11] Jejich cílem byly zejména ovládací konzole a rozhraní operačních technologií, která jsou přístupná z internetu bez hesel či jen se slabými hesly. Po získání přístupu tak mohli útočníci měnit provozní nastavení a provádět sabotáž systémů.

V ruské kampani proti polské energetice na konci roku 2025 útočníci pronikli do sítí více než třiceti větrných a solárních elektráren, jedné teplárny a jednoho průmyslového podniku, a to přes internetově dostupná zařízení FortiGate. Do VPN se přihlašovali k účtům bez vícefaktorového ověření, v jednom případě pomocí konfigurace zařízení, která unikla na kriminální fórum.[12]

Specifickou kategorií jsou IP kamery, které jsou zneužívány pro špionáž i přímou podporu vojenských operací.[13] Tato zařízení jsou často chráněna slabým autentizačním mechanismem a mohou tak být snadno ovládnuta, jsou-li vystavena do internetu. Vektorem mohou být také zranitelnosti, a to zejména pokud kamery neobsahují aktualizovaný firmware, jsou provozovány po skončení servisní podpory či pocházejí od nedůvěryhodného výrobce.

Miskonfigurace: detekce a protiopatření

- Zapněte vícefaktorové ověření pro VPN, vzdálenou správu a privilegované účty a změňte výchozí hesla.
- Omezte, co je dostupné z internetu: administrační rozhraní, routery, kamery a OT systémy.
- Sledujte přihlašování, zejména opakované neúspěšné pokusy a přihlášení z podezřelých míst.
- Rozdělte síť na části a omezte oprávnění, aby napadení jednoho zařízení neznamenalo ovládnutí dalších.

ODCIZENÝ ÚČET CLOUDOVÉ SLUŽBY MŮŽE OTEVŘÍT CESTU K E-MAILŮM I INTERNÍM DOKUMENTŮM

Ruští aktéři v posledních letech v rostoucí míře využívají i útoky založené na odcizených, uniklých nebo znovu použitých přihlašovacích údajích. **Mezi nejčastější techniky patří password spraying, credential stuffing a další formy útoků proti internetově dostupným službám, jako jsou VPN brány, Outlook Web Access, Microsoft 365 a další systémy umožňující vzdálený přístup.[14]**

Technika password spraying spočívá v použití malého počtu běžných hesel proti velkému množství účtů, čímž se útočníci snaží obejít mechanismy blokace účtů a detekci bruteforce útoků. Oblíbeným cílem jsou také účty, které bývají zanedbané: servisní, neaktivní či testovací účty bez vícefaktorového ověření. Ruská skupina APT29 tak v roce 2023 pronikla do firemního prostředí společnosti Microsoft přes zapomenutý testovací účet.[15]

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

Cloud, identity a účty: detekce a protiopatření

- Nasaďte vícefaktorové ověření odolné vůči phishingu (např. bezpečnostní klíče), alespoň pro administrátory a vzdálený přístup.
- Pravidelně kontrolujte účty a oprávnění: rušte neaktivní účty a servisní či privilegované účty omezte na nezbytné minimum.
- Omezte přístup ke kritickým systémům jen na potřebné uživatele a spravovaná zařízení (podmíněný přístup, tzv. Conditional Access).
- Sledujte neúspěšná a neobvyklá přihlášení (hromadné pokusy, nezvyklá místa) i registraci nových zařízení či ověřovacích metod.

KOMPROMITACE PROSTŘEDNICTVÍM DODAVATELSKÉHO ŘETĚZCE HROZÍ MIMO JINÉ SUBJEKTŮM PODPORUJÍCÍM UKRAJINU

Ruští aktéři dlouhodobě zneužívají důvěryhodné vztahy mezi organizacemi, dodavateli a poskytovateli služeb. Kompromitace jednoho subjektu může otevřít přístup k mnoha dalším a zároveň ztěžuje detekci.

Příkladem je SolarWinds (2020), kdy APT29 podvrhla legitimní aktualizaci softwaru.[16] V roce 2023 zase stejný aktér hromadně zneužíval neopravené servery TeamCity, vývojářský nástroj společnosti JetBrains, čímž získal přístup k několika desítkám softwarových a IT firem, což dále umožnilo útoky na zákazníky JetBrains.[17]

Dodavatelské řetězce: detekce a protiopatření

- Mějte přehled o dodavatelích a jejich přístupu do vaší sítě a tyto přístupy kontrolujte.
- Omezte dodavatelům přístup jen na systémy, které nezbytně potřebují, a vyžadujte u nich vícefaktorové ověření.
- Sledujte činnost dodavatelů, zejména privilegované přístupy.
- Posuzujte bezpečnost dodavatelů při výběru a požadujte ji ve smlouvách (při veřejných zakázkách je možné zohledňovat varování NÚKIB).

V posledních letech ruští aktéři stále častěji cílí také na širší ekosystém dodavatelů a partnerů, včetně poskytovatelů IT či cloudových služeb, systémových integrátorů či logistických a technologických společností. Takový dodavatel má často důvěryhodný přístup do sítí svých zákazníků, a pokud ho útočníci ovládnou, mohou ho využít k průniku k nim. Tento přístup byl pozorován například u kampaně, která cílila na organizace tvořící součást obranného a logistického ekosystému Ukrajiny a jejích spojenců, včetně ČR.[18]

ZÁKLADNÍ OPATŘENÍ ZABRÁNÍ VĚTŠINĚ PRŮNIKŮ, VČASNÁ DETEKCE OMEZÍ ŠKODY

Ruští aktéři používají řadu dalších technik v závislosti na cíli operace. Před značnou částí jejich aktivit stále chrání důsledné dodržování základních principů kybernetické bezpečnosti. Taková opatření však nezaručují úplnou ochranu. Pokud je útok úspěšný, je proto stejně důležité ho včas odhalit.

Vzdělávání uživatelů v rozpoznávání phishingu vhodně doplňuje včasné aktualizace, vícefaktorové ověřování, správu privilegovaných přístupů a bezpečnou konfiguraci systémů. Stěžejní je i pravidelná správa identit a účtů, důsledná kontrola internetově dostupných služeb a omezení výchozích či slabých přihlašovacích údajů. Tato základní opatření snižují pravděpodobnost úspěšného útoku.

Zásadní je schopnost organizace včas odhalit probíhající kompromitaci. To zahrnuje průběžný monitoring bezpečnostních událostí, detekci anomálií v přihlašování, sledování podezřelého síťového provozu a monitorování činností privilegovaných účtů. Útočníci se běžně snaží skrývat svoji aktivitu mezi legitimní administrátorské operace a je proto nezbytné zaměřit se nejen na známé indikátory kompromitace, ale i na neobvyklé vzorce chování v prostředí organizace.

Techniky, nástroje i infrastruktura útočníků se průběžně mění, mnoho úspěšných kompromitací stále využívá známé zranitelnosti, nedostatečně chráněné účty, chybějící vícefaktorové ověřování, nesprávně nakonfigurované systémy nebo lidskou chybu. Pravděpodobnost průniku i dopady incidentu proto významně snižuje řízení zranitelností, ochrana identit, segmentace sítí, zálohování, vzdělávání uživatelů a schopnost včasné detekce a reakce.

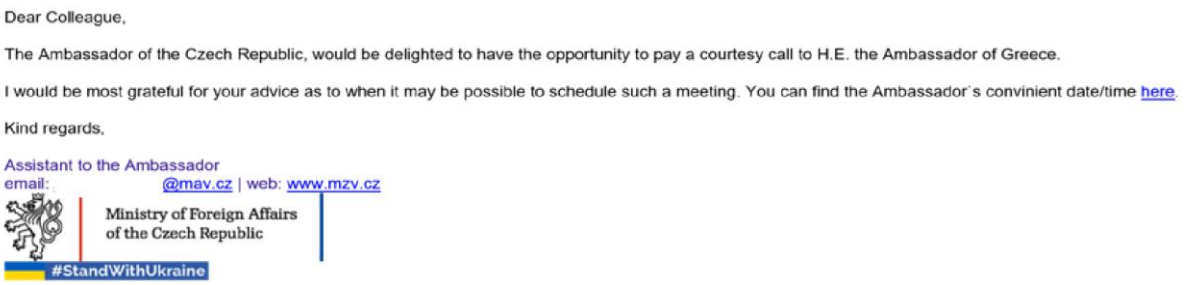
TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

PŘÍLOHA 1: PŘÍKLADY PHISHINGU

E-mailový phishing

Ruský aktér podvrhl identitu českého Ministerstva zahraničních věcí pro útoky proti dalším cílům (Obrázek 1). V rámci kampaně aktér zneužíval zranitelnost v aplikaci WinRAR k doručení kyberšpionážního škodlivého kódu prostřednictvím příloh.

Obr. 1: Phishingový e-mail zneužívající identitu českého MZV


Dear Colleague,

The Ambassador of the Czech Republic, would be delighted to have the opportunity to pay a courtesy call to H.E. the Ambassador of Greece.

I would be most grateful for your advice as to when it may be possible to schedule such a meeting. You can find the Ambassador´s convinient date/time here.

Kind regards,

Assistant to the Ambassador
email: @mav.cz | web: www.mzv.cz
Ministry of Foreign Affairs
of the Czech Republic
#StandWithUkraine

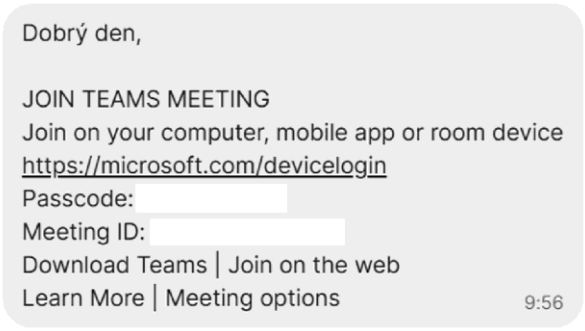
Zdroj: NÚKIB

Phishing přes komunikační aplikaci Signal

Jednou z pozorovaných technik je tzv. „OAuth phishing“. Jde o zprávy, v nichž se útočník vydává za někoho, kdo má zájem o videokonferenční hovor s obětí, po níž požaduje přihlášení do „ověřovacího portálu“ nebo zaslání autentizačního kódu. Terčem jsou často aplikace a služby Microsoft. Nejprve zpravidla dochází k budování důvěry mezi útočníkem a obětí. Následně oběť obdrží falešnou pozvánku ke schůzce.

Obdobným způsobem funguje tzv. Device Code phishing zneužívající funkci Device Code Flow (Obrázek 2). NÚKIB v září 2026 vydal na Portálu NÚKIB upozornění, ve kterém na probíhající phishingovou kampaň poukázal a doporučil, jak hrozbě čelit.

Obrázek 2: Falešná zpráva zaslaná přes aplikaci Signal vyzývající uživatele k připojení ke schůzce na platformě MS Teams


Dobrý den,

JOIN TEAMS MEETING
Join on your computer, mobile app or room device
https://microsoft.com/devicelogin
Passcode:
Meeting ID:
Download Teams | Join on the web
Learn More | Meeting options
9:56

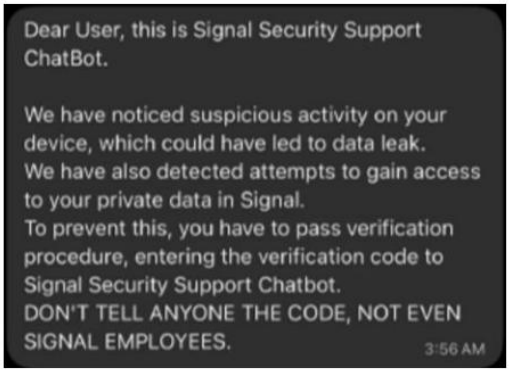
Zdroj: NÚKIB

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

Další formu phishingu představuje rozesílání falešných zpráv, ve kterých se útočníci vydávají za technickou či bezpečnostní podporu společnosti Signal. Ve zprávách vyzývají uživatele k předání PIN kódu či jiných přístupových údajů (Obrázek 3).

Škodlivé odkazy či QR kódy mohou být oběti doručeny i mimo aplikaci Signal a navádět ji na podvržené externí domény. Zdánlivě se mohou opět tematicky týkat bezpečnosti zařízení, pozvánek do různých skupin nebo výzev k propojení cizího uživatele (Obrázek 4).[19]

Obrázek 3: Falešná zpráva vyzývající uživatele k předání bezpečnostního PIN kódu



Zdroj: Google Threat Intelligence Group

Obrázek 4: Falešný QR kód a škodlivý odkaz na připojení ke skupině



Zdroj: Google Threat Intelligence Group

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

PŘÍLOHA 2: SOUVISEJÍCÍ TAKTIKY VYUŽÍVANÉ PO ZÍSKÁNÍ PRVOTNÍHO PŘÍSTUPU

ZNEUŽITÍ NÁSTROJŮ VZDÁLENÉ SPRÁVY

Ruští aktéři zneužívají legitimní nástroje vzdálené správy (RMM) jako prostředek pro získání přístupu do prostředí oběti (seznam historicky zneužitých nástrojů viz Příloha 3). Instalace nebo spuštění může být výsledkem sociálního inženýrství, kdy útočník vystupuje například jako technická podpora, dodavatel nebo interní IT oddělení a přiměje uživatele vzdálený přístup povolit.

Úspěšné zneužití RMM nástroje dává útočníkům vysokou míru kontroly nad kompromitovaným zařízením a umožňuje provádět další škodlivé aktivity, včetně krádeže dat, nasazení malwaru, laterálního pohybu nebo vytvoření dlouhodobé perzistence.

Nástroje vzdálené správy: Detekce a protiopatření

- Povolte jen schválené aplikace a omezte uživatelům právo instalovat software. Neschválené RMM nástroje blokujte nebo detekujte (EDR).
- Sledujte síťovou komunikaci na známé domény poskytovatelů vzdálené správy, které organizace nepoužívá.
- Poučte uživatele, aby neznámým osobám nikdy nepovolovali vzdálený přístup a ověřovali každou žádost jiným kanálem.

ZNEUŽITÍ LEGITIMNÍCH CLOUDOVÝCH, WEBOVÝCH A KOMUNIKAČNÍCH SLUŽEB PRO EXFILTRACI DAT A C2 KOMUNIKACI

Další taktikou je zneužití legitimních služeb pro exfiltraci dat (seznam viz Příloha 3). Tyto služby obvykle šifrují síťový provoz a ze své podstaty komplikují detekci škodlivých instancí.

Zneužití služeb pro C2: Detekce a protiopatření

- Detekujte či blokujte služby, které organizace aktivně nepoužívá.
- Sledujte velké objemy odesílaných dat a pravidelně se opakující spojení na tyto služby.

LIVING OFF THE LAND TECHNIKY (LOTL)

Po získání přístupu ruští aktéři často zneužívají legitimní nástroje operačního systému namísto nasazení vlastního malwaru. Typicky se jedná o nástroje jako PowerShell, WMI, schtasks, rundll32, certutil nebo PsExec, které jsou běžnou součástí administrace systému. Tento přístup omezuje množství detekovatelných indikátorů kompromitace a ztěžuje odlišení škodlivé aktivity od legitimní správy.[20]

Living off the Land: Detekce a protiopatření

- Sledujte neobvyklé použití administrátorských nástrojů, například PowerShell či PsExec na počítačích běžných uživatelů nebo mimo pracovní dobu.
- Omezte, kdo a odkud smí tyto nástroje používat a zapněte jejich zaznamenávání.

ACTIVE DIRECTORY A LATERÁLNÍ POHYB

Po kompromitaci prvního účtu se ruští aktéři běžně snaží získat vyšší oprávnění a rozšířit svůj přístup napříč sítí. Cílem bývá dosažení doménových administrátorských oprávnění, převzetí kontroly nad prostředím Active Directory a zajištění dlouhodobé perzistence. Pozorovány jsou techniky jako krádež přihlašovacích údajů z paměti (proces LSASS) či z databáze Active Directory (NTDS.dit), techniky Kerberoasting, Pass-the-Hash, DCSync nebo zneužití privilegovaných a servisních účtů.

AD a laterální pohyb: Detekce a protiopatření

- Sledujte privilegované účty a změny v Active Directory.
- Detekujte krádež přihlašovacích údajů (přístup k LSASS, export databáze AD) a techniky Kerberoasting, Pass-the-Hash a DCSync, nejlépe pomocí EDR.
- Omezte a pravidelně kontrolujte servisní a administrátorské účty. Administrátoři se nemají přihlašovat na běžné pracovní stanice.

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

PŘÍLOHA 3: VYBRANÉ ZRANITELNOSTI, NÁSTROJE A SLUŽBY ZNEUŽÍVANÉ RUSKÝMI AKTÉRY (2023-2026)

Kategorie	Příklady	
Nástroje vzdálené správy (RMM)[21]	Atera, IntelliAdmin, LiteManager, RemCom, RMS, Remote Utilities, Splashtop, SuperOps, TeamViewer, UltraVNC	
Cloudové, webové a komunikační služby[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 nástroje	PowerShell, WMI, PsExec, schtasks, certutil, rundll32, regsvr32, mshta	
Zneužívané zranitelnosti	**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 informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/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 informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

ZDROJE

[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 informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/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 informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*

TLP:CLEAR informace jsou určeny pro volnou distribuci. Více informací o TLP označení: https://nukib.gov.cz/cs/TLP