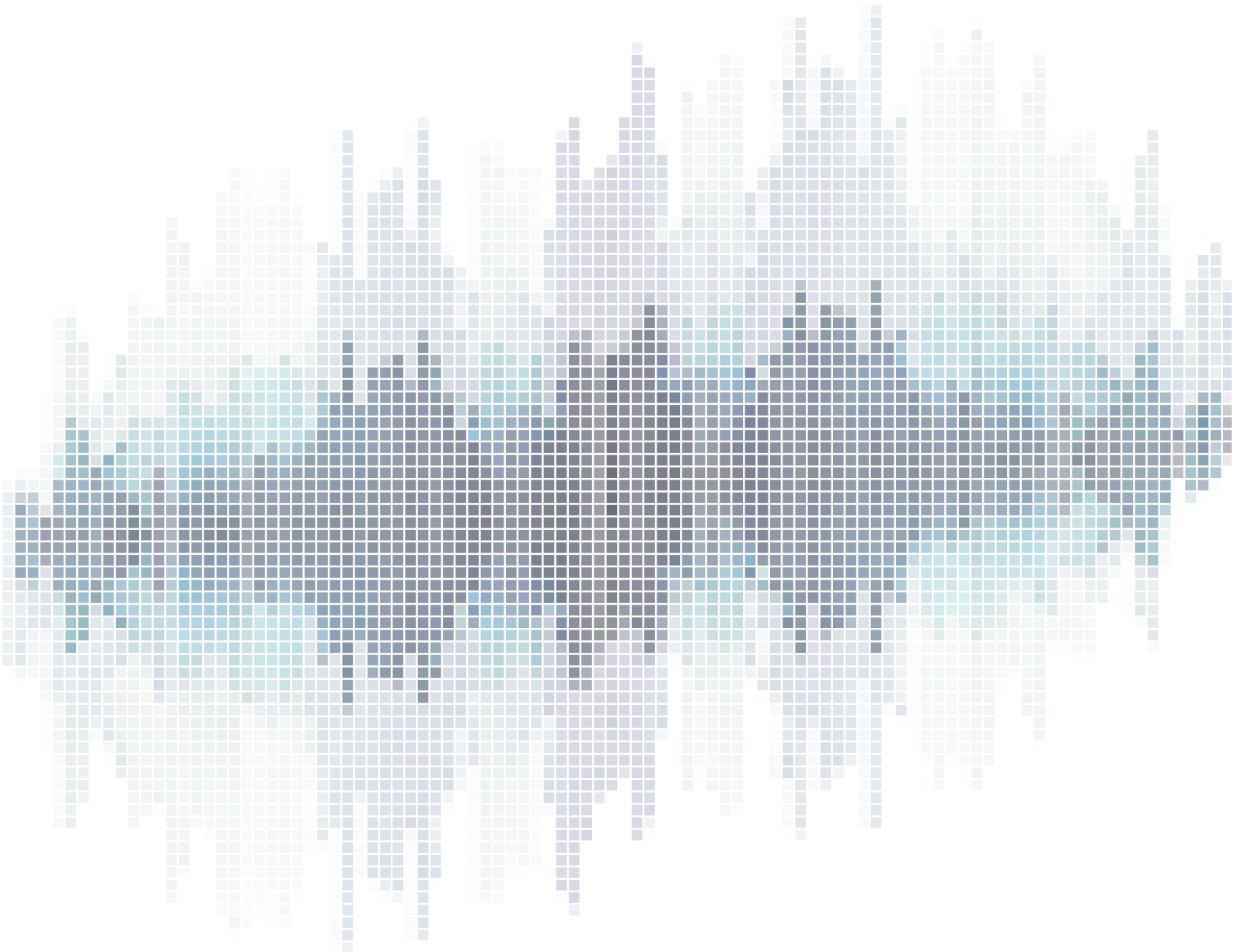
Čtvrtletní přehled hrozeb pohledem NÚKIB

Q1 2026



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí uplynulého čtvrtletí[1]

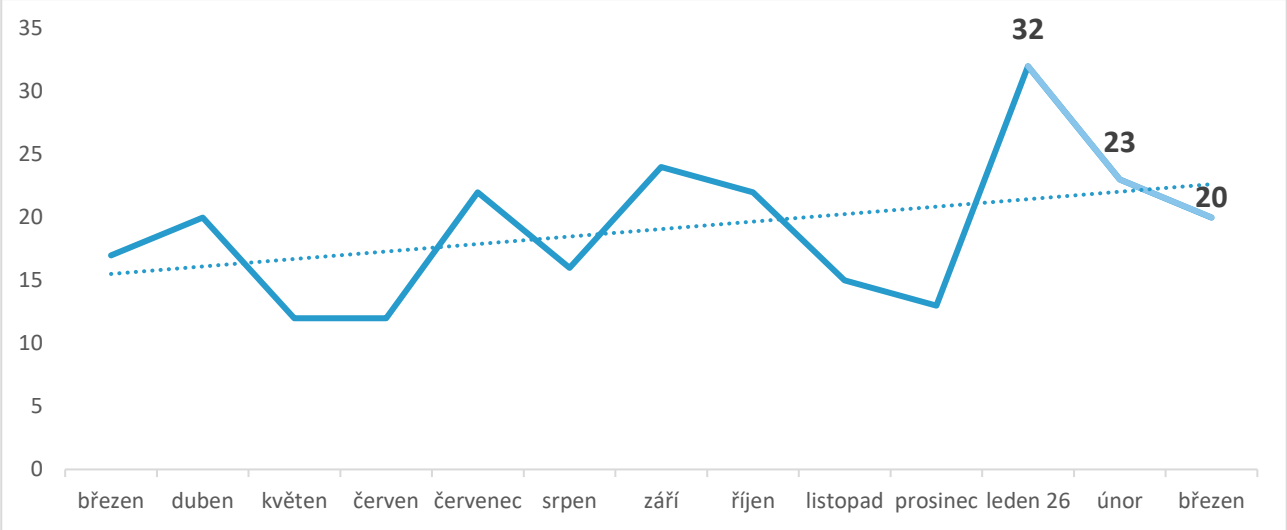
Za první čtvrtletí roku 2026 NÚKIB evidoval přes 70 kybernetických incidentů, což je nejvyšší hodnota za poslední rok. Za tímto nárůstem stála primárně lednová vlna DDoS útoků proruských hacktivistů, ale také relativně vysoký počet incidentů v rámci kategorie Průnik. Zvýšená aktivita hacktivistů vedla NÚKIB k vydání upozornění spolu s doporučením pro mitigaci útoků. Spolu s tím NÚKIB řešil také problematiku nedostatečně zabezpečených VNC služeb vystavených do internetu, které byly zneužívány nejen hacktivistickými aktéry. Ačkoliv se tento problém výrazněji neprojevil ve statistikách incidentů, NÚKIB důrazně doporučuje zajistit odpovídající zabezpečení VNC služeb, zejména v případech, kdy jsou dostupné z internetu a chráněné slabým autentizačním mechanismem nebo vůbec žádným.

Zatímco počet DDoS útoků od ledna postupně klesl, úspěšné průniky se v průběhu čtvrtletí držely na stejných hodnotách. Do této kategorie spadaly incidenty různé závažnosti, přičemž se jednalo o kompromitace systémů, okrajových zařízení, databází, e-mailových schránek či jednotlivých uživatelských účtů.

NÚKIB za celé první čtvrtletí neevidoval žádný ransomwarový útok proti subjektu v režimu vyšších povinností dle nového zákona o kybernetické bezpečnosti. Ransomwarové útoky však postihly poskytovatele regulovaných služeb v režimu nižších povinností, u nichž je řešení kybernetických bezpečnostních incidentů koordinováno prostřednictvím Národního CERT (CSIRT.CZ). Kategorie Informační bezpečnost, kam ransomware běžně spadá, byla zastoupena primárně úniky informací a dat.

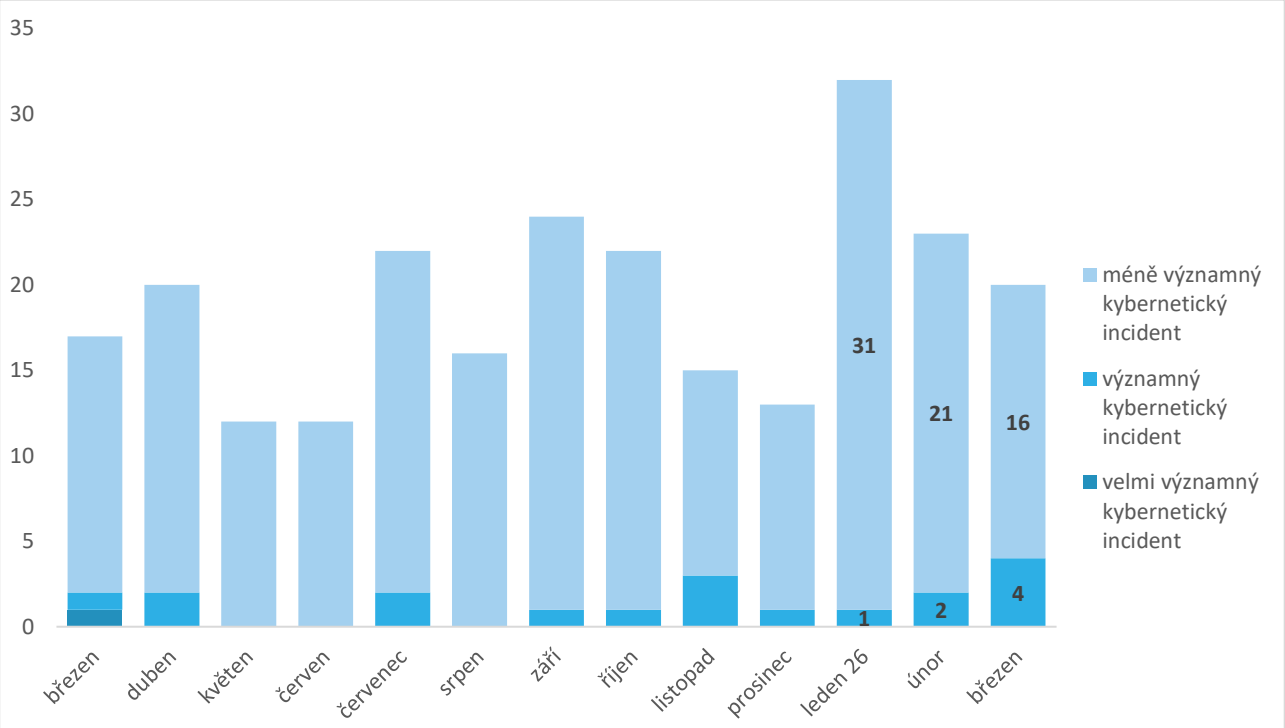
Spolu s celkovým počtem incidentů mírně narostla také závažnost řešených incidentů. NÚKIB za uplynulé čtvrtletí evidoval celkem 7 významných incidentů, přičemž většina z nich se týkala státních institucí. Všechny ostatní incidenty spadaly mezi méně významné.

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



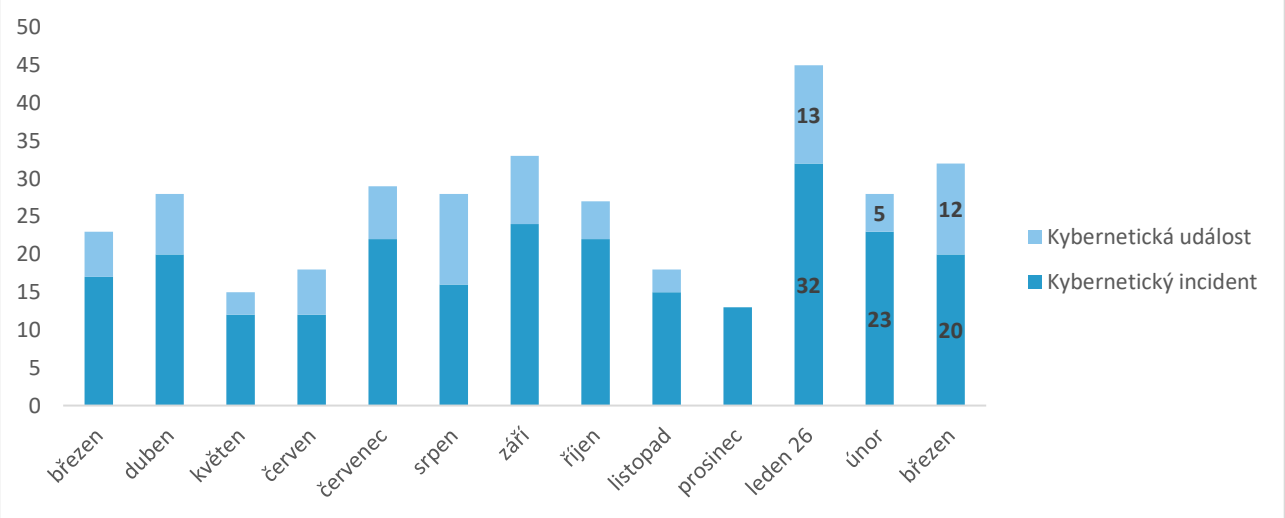
[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

Závažnost řešených kybernetických incidentů[2]



Podíl kybernetických incidentů a událostí zaznamenaných NÚKIB[3]

NÚKIB v rámci své činnosti přijímá, zpracovává a vyhodnocuje hlášení kybernetických incidentů. Na základě provedené analýzy může být hlášení klasifikováno buď jako kybernetický incident, kybernetická událost, nebo jako nerelevantní podnět. Graf níže ukazuje podíl kybernetických incidentů a kybernetických událostí.



[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

[3] Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Oba pojmy definuje zákon o kybernetické bezpečnosti.

Kybernetické hrozby s bezprostředním dopadem na Českou republiku

V lednu došlo ke zvýšené aktivitě ze strany hacktivistických aktérů

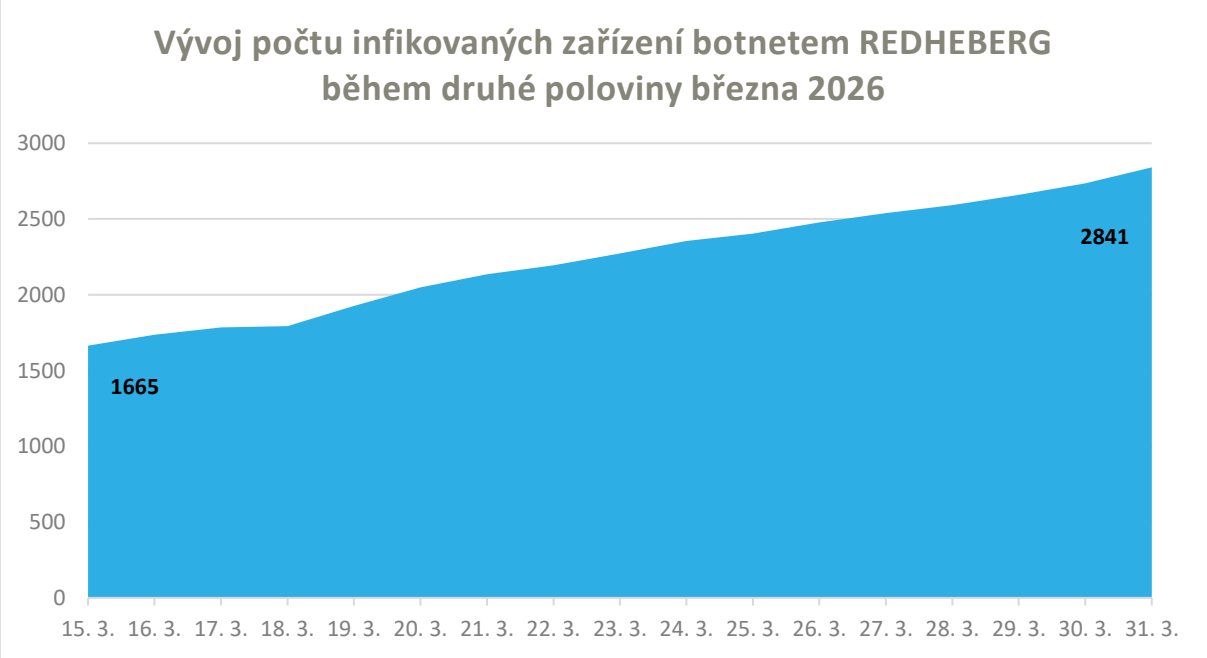
Již na začátku ledna došlo ke zvýšené aktivitě proruských hacktivistů v České republice, která se projevila vlnou DDoS útoků na české subjekty. Ta se poměrně významně propsala do počtu incidentů evidovaných NÚKIB, kdy DDoS útoky tvořily jednoznačně nejpočetnější podkategorii všech incidentů. NÚKIB v návaznosti na tyto útoky vydal upozornění pro regulované subjekty prostřednictvím Portálu NÚKIB včetně doporučení pro prevenci a mitigaci těchto útoků.

Souběžně NÚKIB v lednu upozornil na zvýšený zájem proruských hacktivistů o útoky na VNC rozhraní PLC zařízení se slabými nebo žádnými hesly a zneužívání dalších provozovaných služeb otevřených do internetu. Veškeré dosavadní zaznamenané útoky měly minimální dopady a týkaly se primárně neregulovaných subjektů. NÚKIB nicméně v této souvislosti doporučuje nepoužívat VNC rozhraní exponovaná do internetu nebo alespoň používat dostatečně silná hesla. Nedostatečná ochrana těchto zařízení zvyšuje riziko neautorizovaného přístupu k provozním technologiím (OT) a umožňuje snadnou manipulaci s nimi.

V obou případech se jednalo o aktivity, které neměly výraznější dopady na české subjekty. Činnost těchto aktérů navíc s koncem ledna postupně ustala a v rámci incidentů se projevovala minimálně.

Upozornění na aktivní šíření botnetu REDHEBERG v České republice

S nedostatečně zabezpečenými VNC službami vystavenými do internetu souviselo také další upozornění, které NÚKIB vydal prostřednictvím Portálu během března. V daném období totiž došlo k výraznému nárůstu počtu zařízení kompromitovaných botnetem REDHEBERG na území České republiky. V době psaní tohoto přehledu je v České republice stále evidováno přes 3200 kompromitovaných zařízení. Podle dostupných informací dochází ke kompromitaci zařízení prostřednictvím vzdáleného neautentizovaného přístupu k VNC službám vystaveným přímo do internetu. Kompromitace zařízení a jeho začlenění do botnetu je relativně snadno detekovatelná, mimo jiné na základě specifických zpráv a bannerů s extremistickou tematikou.



Botnet je zpravidla označován jako síť infikovaných zařízení, která jsou bez vědomí svých uživatelů na dálku ovládána útočníkem. Takto kompromitovaná zařízení mohou být zneužívána k dalším kybernetickým útokům, například k šíření škodlivého obsahu, zahlcování internetových služeb nebo k dalšímu šíření nákazy. Přestože samotné zařízení může na první pohled fungovat zcela běžně, jeho zapojení do botnetu představuje riziko nejen pro jeho provozovatele, ale i pro ostatní uživatele internetu.

NÚKIB v kontextu tohoto typu hrozeb důrazně doporučuje:

- Nevystavovat VNC ani jiné vzdálené přístupové služby přímo do internetu.
- Omezit dostupnost vzdálených přístupových služeb výhradně na interní sítě nebo zajistit jejich přístup prostřednictvím VPN.
- Zajistit, aby vzdálený přístup nebyl možný bez autentizace, a používat silné autentizační mechanismy.
- V případě podezření na kompromitaci zařízení neprodleně přijmout nápravná opatření a postupovat dle standardních postupů řešení kybernetických bezpečnostních incidentů.

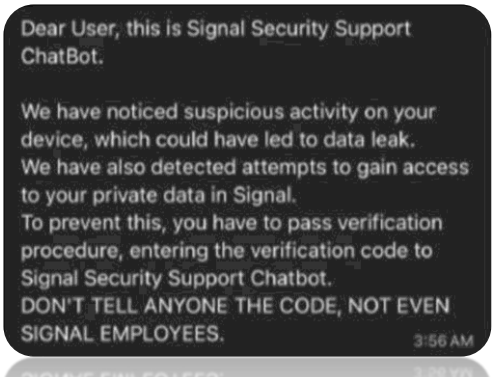
Situační přehled kybernetických hrozeb relevantních pro Českou republiku

NÚKIB dlouhodobě monitoruje relevantní hrozby, které nemají bezprostřední dopad na bezpečnost České republiky. I tyto hrozby však mohou mít přímý či nepřímý vliv na kybernetickou bezpečnost českých subjektů, ať již v současnosti, či budoucnu. Udržování situačního povědomí o aktuálních hrozbách je tak klíčovou součástí aktivit NÚKIB.

Rusko realizuje globální kyberšpionážní kampaň přes komunikační aplikaci Signal

Nizozemské zpravodajské služby upozornily na globální kyberšpionážní kampaň vedenou přes komunikační platformu Signal. Ta je mířena primárně na politické představitele, úředníky a příslušníky ozbrojených složek, přičemž ale nebyl blíže specifikován konkrétní státem sponzorovaný aktér. Ke kompromitaci mělo dojít i v samotném Nizozemsku, a to na úrovni individuálních účtů. Platforma samotná kompromitována nebyla. Vektorem útoku je dle zprávy phishing, kdy se útočník vydává za technickou podporu Signalu, aby od cíle vylákal ověřovací kód nutný k získání přístupu k účtu. Objevily se rovněž případy podvodného zneužití QR kódu, který skrze legitimní funkci aplikace dovolil propojit účty útočníka a oběti. Nejnověji byla kampaň ze strany amerických úřadů atribuována aktérům napojeným na ruské zpravodajské služby.

Phishingová zpráva na platformě Signal



Ruští státní a čínští kyberkriminální aktéři využili nástroj k prolomení zařízení iPhone, původně vyvinutý pro západní zpravodajské služby

Výzkumníci společnosti Google v roce 2025 monitorovali rozsáhlé využívání pokročilého nástroje pro kompromitaci zařízení iPhone označovaného jako Coruna, který byl použit v několika kampaních po celém světě. Analýza společnosti iVerify a výpovědi bývalých zaměstnanců naznačují, že část nástroje mohla vzniknout v divizi Trenchant amerického obranného kontraktora L3Harris. Ten své ofenzivní kybernetické technologie dodává vládě USA a jejím zpravodajským partnerům v alianci Five Eyes. Nástroje se však následně zřejmě dostaly mimo původně zamýšlený okruh uživatelů. Coruna byla později použita ruskou kyberšpionážní skupinou UNC6353 proti vybraným cílům na Ukrajině prostřednictvím kompromitovaných webových stránek. Následně se podobné nástroje objevily i v kampaních čínských kyberkriminálních skupin zaměřených na finanční podvody a krádeže kryptoměn.

Kyberkriminální aktér odcizil data Evropské komise při kompromitaci cloudových služeb Amazonu

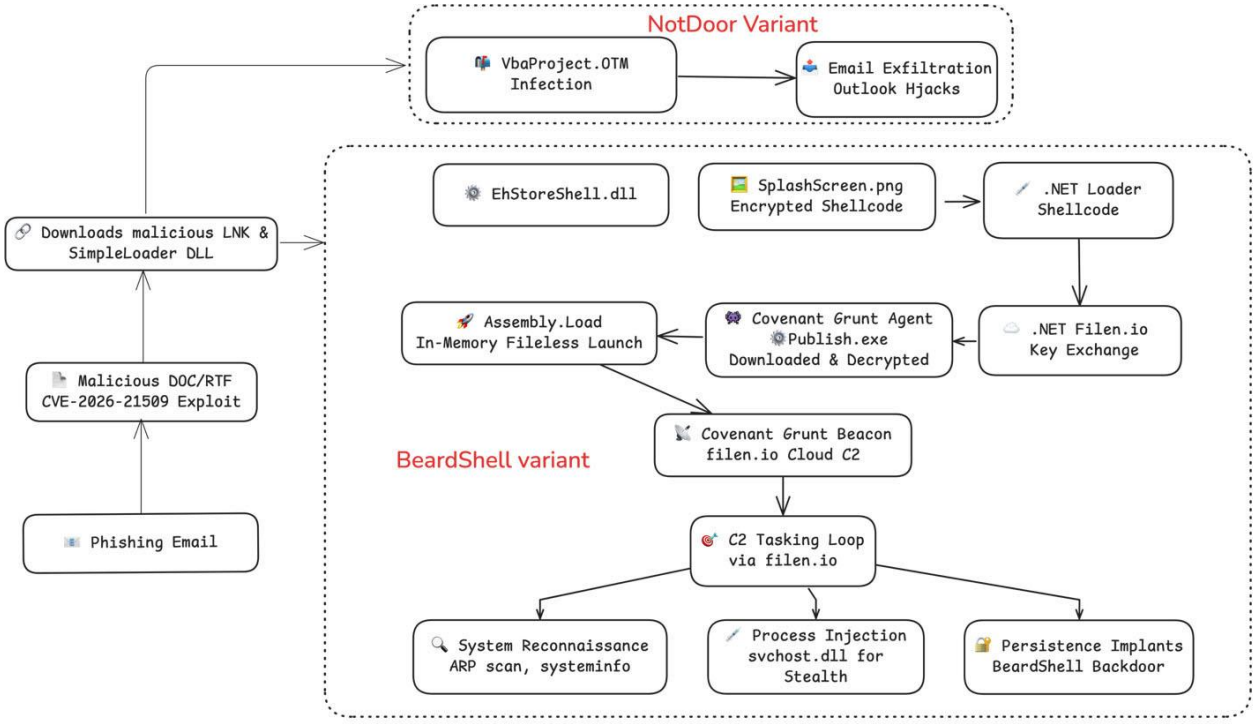
Evropská komise vyšetřuje bezpečnostní incident spojený s kompromitací cloudových služeb Amazonu (Amazon Web Services, AWS), jež hostí některé její účty. K incidentu, který byl odhalen

24. března, se přihlásila kyberkriminální skupina ShinyHunters. Evropská komise přiznala odcizení svých dat, zároveň informovala, že její vnitřní systémy nebyly útokem dotčeny. Dle dalších informací mělo být odcizeno více než 350 GB dat, včetně několika databází, přičemž útočník ShinyHunters již část dat zveřejnil na své stránce na dark webu. Dle zprávy vydané CERT-EU byl počáteční přístup zajištěn v důsledku narušení dodavatelského řetězce společnosti Trivy, kdy byl získán přístupový klíč ke cloudové službě Amazonu. Tento klíč následně umožnil získat kontrolu nad dalšími účty AWS spojenými s Evropskou komisí.

Ruský aktér APT28 realizoval kyberšpionážní spear-phishingovou kampaň proti evropským státům

Ukrajinský CERT a kyberbezpečnostní společnosti Zscaler a Trellix odhalily kyberšpionážní kampaň v Evropě. Za tzv. operací Neusploit má být ruský státem sponzorovaný aktér APT28, jenž spadá pod ruskou vojenskou zpravodajskou službu GRU. Kampaň stála na zneužití zranitelnosti CVE-2026-21509 v softwaru Microsoft Office, která útočníkovi umožnila obejít ochranné mechanismy, odeslat upravené dokumenty a spustit škodlivé příkazy. Konkrétně se mělo jednat o malwary Covenant a MiniDoor, jež umožňovaly exfiltrovat data, zejména e-mailovou komunikaci. Součástí útoku bylo i sociální inženýrství, kdy zprávy byly psány jak v angličtině, tak v národních jazycích cílových subjektů. Nejprve byly odhaleny útoky mířící na státní instituce na Ukrajině, v Rumunsku a na Slovensku, později byly popsány útoky na námořní dopravu a diplomatické subjekty v Polsku, Slovinsku, Turecku a Řecku.

Schéma útoku kampaně Neusploit



Spolupráce a sdílení informací v boji proti kybernetickým hrozbám

Zajišťování kybernetické bezpečnosti nezahrnuje pouze monitorování hrozeb a řešení kybernetických incidentů. Nezanedbatelnou součástí této činnosti je také vzájemná spolupráce, její rozvoj, sdílení zkušeností a informací o aktuálních hrozbách a způsobech, jak jim efektivně čelit.

V Praze proběhl sedmý ročník mezinárodní Prague Cyber Security Conference 2026

V březnu se v Praze uskutečnil sedmý ročník mezinárodní Prague Cyber Security Conference (PCSC), pořádaný NÚKIB ve spolupráci s Ministerstvem zahraničních věcí ČR. Konference přivítala přibližně čtyři sta odborníků z řad státní správy, akademické sféry a technologických firem z desítek zemí světa a potvrdila svou roli významné evropské platformy pro strategickou debatu o kybernetické bezpečnosti.

Diskuse se zaměřily na regulatorní přístupy k digitálním produktům napříč regiony, financování kybernetické bezpečnosti, důvěru v dodavatelské řetězce a dopady nových technologií včetně umělé inteligence a kvantových technologií. Pozornost byla věnována i zkušenostem z války na Ukrajině a rostoucím státem podporovaným kybernetickým operacím. Konference zdůraznila význam mezinárodní spolupráce jako klíčového prvku odolnosti v kyberprostoru.

NÚKIB hostil Cyber Champions Summit se zástupci NATO a indo-pacifických partnerů

NÚKIB ve spolupráci s Ministerstvem zahraničních věcí ČR a NATO uspořádal mezinárodní Cyber Champions Summit 2026, kterého se zúčastnili seniorní představitelé spojeneckých zemí NATO a klíčových partnerů z indo-pacifického regionu (Austrálie, Japonsko, Jižní Korea a Nový Zéland). Akci zahájil prezident České republiky Petr Pavel, jenž ve svém vystoupení zdůraznil rostoucí bezpečnostní provázanost euroatlantického a indo-pacifického prostoru a význam pevných spojenectví v době zhoršujícího se globálního bezpečnostního prostředí.

Cílem summitu bylo posílení mezinárodní spolupráce v oblasti kybernetické bezpečnosti a obrany, zejména prostřednictvím sdílení informací, zkušeností a koordinace postupů při prevenci a řešení kybernetických incidentů. Diskuse se soustředily na aktuální hrozby v kyberprostoru i další rozvoj společných aktivit na politické, vojenské a technické úrovni. Setkání zároveň potvrdilo aktivní roli NÚKIB v indo-pacifickém regionu a dlouhodobé zapojení České republiky do posilování mezinárodní kybernetické spolupráce.

Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

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 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách NÚKIB). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
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.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know.
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.
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.