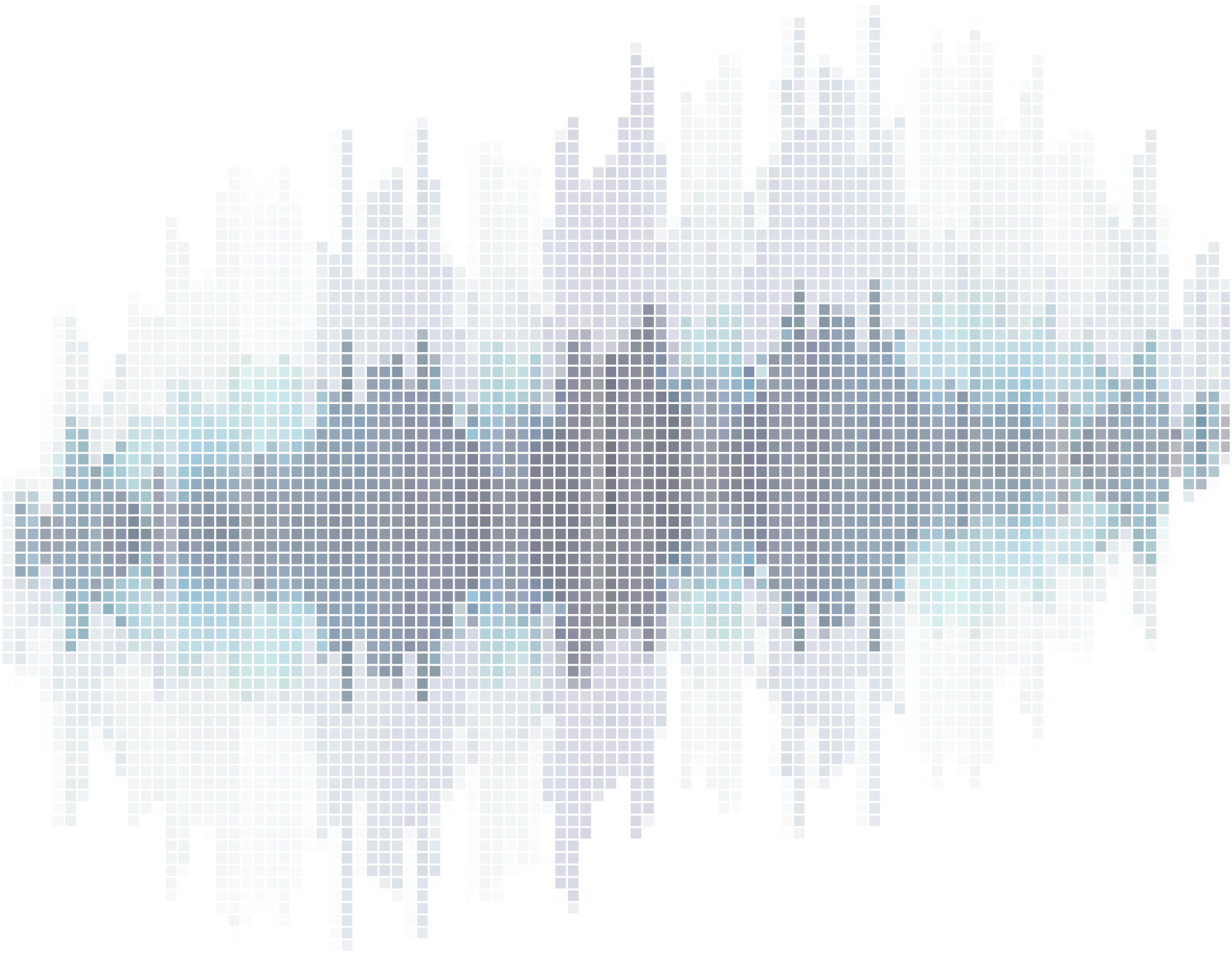
Čtvrtletní přehled hrozeb pohledem NÚKIB

Q3 2026



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí uplynulého čtvrtletí[1]

Za třetí čtvrtletí roku 2026 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) evidoval celkem 65 kybernetických incidentů, což v dlouhodobém srovnání představovalo nadprůměrnou hodnotu. Oproti druhému čtvrtletí došlo k nárůstu téměř o polovinu. Z evidovaných incidentů bylo 13 označeno jako významných, tedy nejvíce za poslední rok. Velmi významný incident zaznamenán nebyl.

Pokračoval letošní trend, kdy evidované kybernetické bezpečnostní incidenty nejčastěji spadaly do kategorie Průnik. Ve třetím čtvrtletí už průniky tvořily téměř dvě třetiny všech zaznamenaných incidentů. V historickém srovnání se na velmi nízkých hodnotách držely incidenty spojené s dostupností služeb, zejména DDoS útoky.

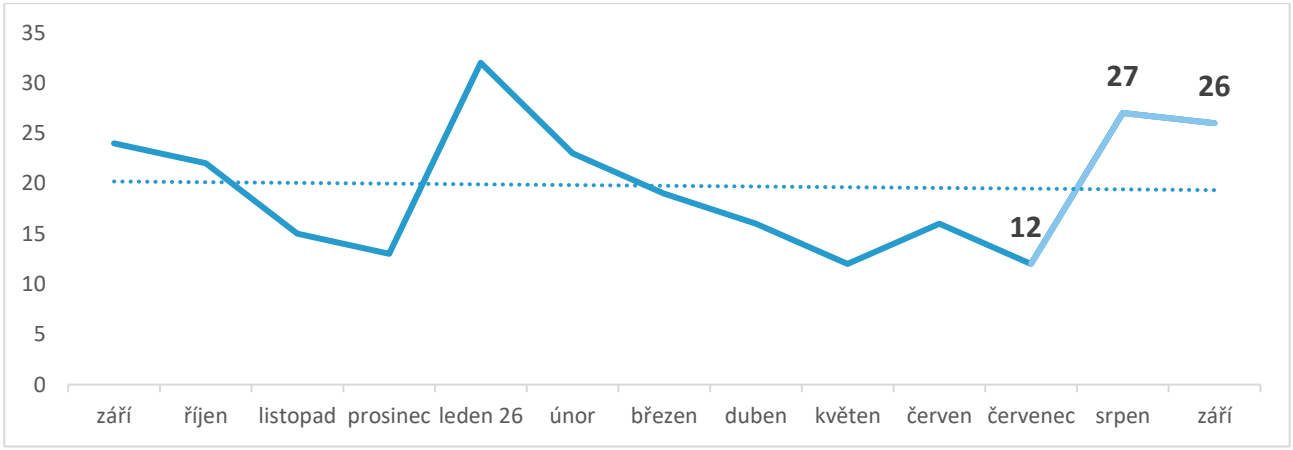
Kompromitovány byly jednotlivé uživatelské účty, webové portály i servery e-mailových a cloudových služeb. K průnikům vedly úspěšné případy phishingu i zneužití zranitelností. Tyto incidenty zasáhly zejména instituce z veřejné správy, vzdělávacího sektoru anebo také zdravotnictví.

Vedle přehledu hrozeb pro ČR a aktivit NÚKIB v oblasti mezinárodní spolupráce je součástí publikace nově také souhrn vývoje v oblasti umělé inteligence s dopadem na kybernetickou bezpečnost.

Nový zákon o kybernetické bezpečnosti, který nabyl účinnosti 1. 11. 2025, výrazně navýšil množství subjektů, které se musí řídit regulací v oblasti kyberbezpečnosti. Počet incidentů ale prozatím výrazně nenarůstá, proč?

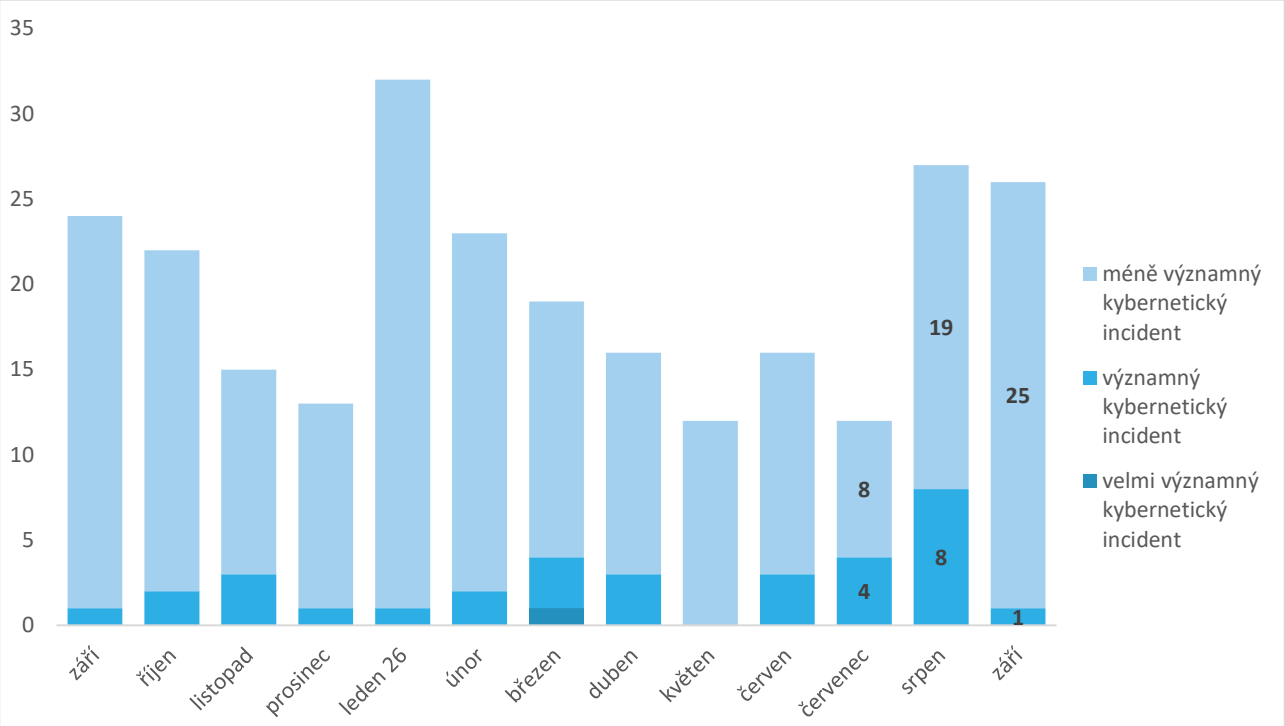
Poskytovatelé regulovaných služeb mají od doručení rozhodnutí o registraci rok na to, aby incidenty začaly NÚKIB hlásit. Dopad nové regulace se tak nemusí výraznějším způsobem projevit přinejmenším do přelomu roku 2026 a 2027. Povinnost nahlašovat všechny zaznamenané incidenty mají zároveň pouze poskytovatelé regulovaných služeb v režimu vyšších povinností. Subjekty v režimu nižších povinností řešení kybernetických bezpečnostních incidentů koordinují s Národním CERT (CSIRT.CZ), NÚKIB (GovCERT.CZ) je nahlašují pouze v případě, že je samy vyhodnotí jako významné.

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



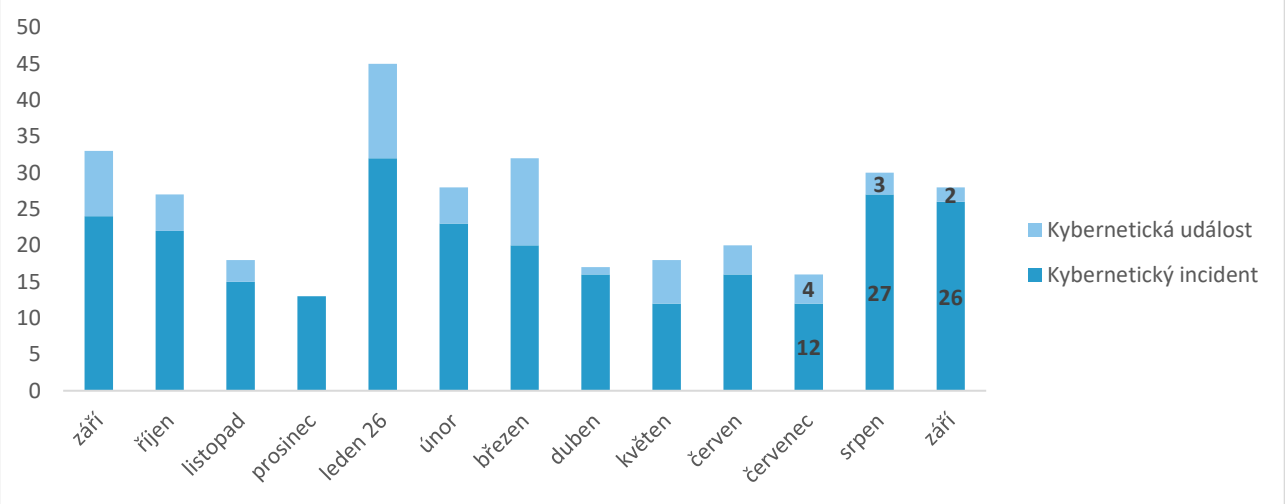
[1] Následující přehled shrnuje dění uplynulého čtvrtletí (červenec, srpen a září). Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

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 ve spojení s přechodným ustanovením § 71 odst. 1 zák. č. 264/2025 Sb., zákon 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

Ruské zpravodajské služby cílí na uživatele aplikace Signal, jejich cílem je sběr citlivých dat prostřednictvím phishingu

Uživatelé aplikace Signal jsou terčem cílených phishingových kampaní, které jsou spojovány zejména s aktéry napojenými na Ruskou federaci. Ti se primárně zaměřují na politiky, příslušníky bezpečnostních složek, úředníky a další osoby představující zájmové cíle z pohledu ruských zájmů.

Útočníci neobcházejí end-to-end šifrování aplikace, ale zneužívají nepozornost uživatelů, stejně jako v případě „běžných“ phishingových e-mailů. Nejčastěji se snaží přimět oběť k propojení útočníkova zařízení s jejím účtem Signal nebo k prozrazení PIN kódu či jiných přístupových údajů, což může vést ke kompromitaci komunikace. Součinnost oběti je v rámci tohoto typu útoků klíčová.

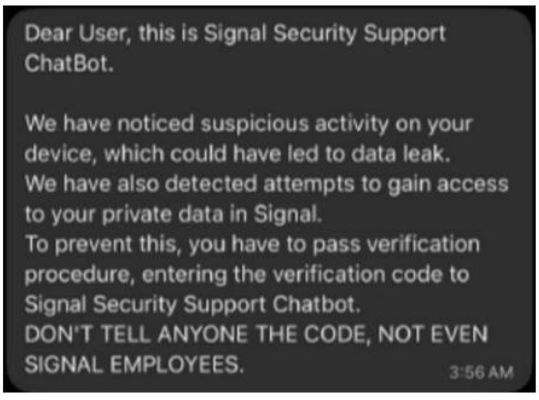
Útočníci využívají aplikaci Signal také k tzv. OAuth phishingu, respektive Device Code phishingu (viz následující strana).

Riziko lze významně snížit důsledným využíváním bezpečnostních funkcí aplikace a dodržováním zásad kybernetické hygieny. **NÚKIB doporučuje zejména:**

- pravidelně kontrolovat seznam připojených zařízení a neznámá okamžitě odebrat,
- aktivovat funkci Zámek registrace,
- nikdy nikomu nesdělovat PIN kód ani ověřovací údaje – oficiální podpora aplikace Signal o ně nežádá,
- neskenovat QR kódy a neotevírat odkazy, které uživatel nevyžádal,
- u citlivější komunikace využívat mizející zprávy a omezit dohledatelnost účtu podle telefonního čísla,
- v případě podezřelé komunikace si u protistrany přes jiný komunikační kanál ověřit, zda je skutečně původcem zprávy, aplikaci stahovat výhradně z oficiálních stránek signal.org, respektive oficiálního obchodu s aplikacemi.

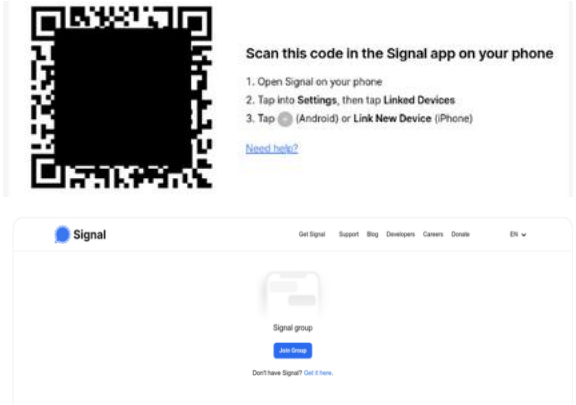
NÚKIB na cílenou phishingovou kampaň upozornil a vydal analýzu se sadou doporučení, jak útok identifikovat a jak se chránit.

Falešná zpráva vyzývající uživatele k předání bezpečnostního PIN kódu



Zdroj: Google Threat Intelligence Group

Falešný QR kód a škodlivý odkaz na připojení ke skupině



Zdroj: Google Threat Intelligence Group

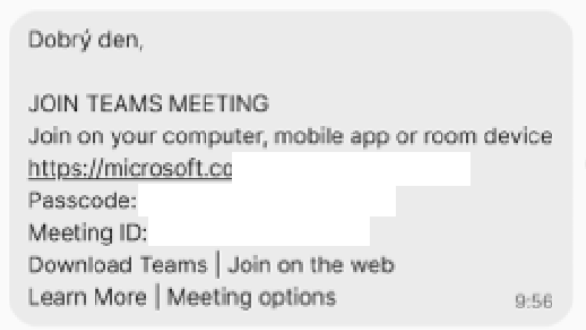
Zneužívání autentizační funkce Device Code Flow ke kompromitaci uživatelů

Device Code Flow je autentizační mechanismus navržený pro případy, kdy se uživatel přihlašuje na zařízení s omezenými možnostmi zadávání přihlašovacích údajů, například na konferenčních systémech, chytrých televizích nebo specializovaných zařízeních. Autentizace probíhá zadáním kódu na jiném zařízení, zpravidla na telefonu. Po úspěšném ověření je aplikaci nebo zařízení, které o přístup žádá, vydán přístupový token.

Tento princip je v současnosti zneužíván při phishingových kampaních, kdy útočník pod záminkou připojení ke schůzce nebo videohovoru přiměje uživatele k autorizaci legitimního Device Code požadavku. Uživatel komunikuje s důvěryhodnou přihlašovací stránkou poskytovatele identity, avšak udělený přístup je navázán na relaci kontrolovanou útočníkem. Výsledkem je vydání platného přístupového tokenu, aniž by útočník potřeboval znát heslo uživatele.

V praxi je phishing doručován například prostřednictvím komunikačních aplikací, jako je Signal. Útočník se 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.

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



Zneužívání mechanismu bylo zaznamenáno také při phishingových kampaních státem sponzorovaných aktérů, jako např. STORM-2372, který je spojován s ruskými zpravodajskými službami.

NÚKIB doporučuje:

- Posoudit, zda je využití Device Code Flow v organizaci skutečně nezbytné a zda přínosy této funkce odpovídají souvisejícím rizikům.
- Povolit funkci pouze tam, kde je to nezbytné. V prostředí Microsoft Entra ID je možné využití Device Code Flow řídit prostřednictvím politik podmíněného přístupu (Conditional Access) nebo ji povolit pouze pro vybrané uživatele, aplikace či konkrétní scénáře použití.
- Pokud není pro provoz organizace nezbytná, doporučujeme zvážit její úplné omezení nebo blokaci.
- Pravidelně revidovat bezpečnostní politiky a vzdělávat uživatele v oblasti užívaných phishingových technik.

Ruští státem sponzorovaní aktéři vedou kyberšpionážní kampaň proti uživatelům platformy Zimbra Collaboration Suite

Národní úřad pro kybernetickou a informační bezpečnost se spolu s partnery z dalších zemí připojil ke společnému upozornění (Joint Cybersecurity Advisory) týkajícímu se probíhající kybernetické kampaně skupiny LAUNDRY BEAR zaměřené na uživatele e-mailové platformy Zimbra Collaboration Suite (ZCS), která probíhá nejméně od července 2025.
Podle zjištění se aktéři napojení na Ruskou federaci zaměřují především na získávání e-mailové komunikace a dalších citlivých informací z vládních institucí, obranného průmyslu, energetiky, médií,

vzdělávacích institucí, nevládních organizací nebo technologických společností. Kampaň využívá zranitelnost v rozhraní webmailu Zimbra, která umožňuje spuštění škodlivého kódu již při zobrazení podvrženého e-mailu ve zranitelné verzi systému.

Útočníci se po úspěšném zneužití zranitelnosti snaží získat obsah e-mailové komunikace, seznamy kontaktů, autentizační údaje, záložní kódy vícefaktorového ověřování a další data, která mohou být následně zneužita ke špionážním aktivitám. Součástí kampaně jsou také pokusy o zajištění dlouhodobého přístupu do kompromitovaných účtů.

NÚKIB doporučuje organizacím využívajícím Zimbra Collaboration Suite neprodleně ověřit, zda provozují aktualizované verze systému obsahující opravu zranitelnosti CVE-2025-66376. Zároveň je vhodné prověřit dostupné indikátory kompromitace, monitorovat podezřelou aktivitu související s e-mailovými službami a věnovat zvýšenou pozornost ochraně uživatelských účtů.

Přehled organizací, které se ke společnému upozornění připojily



Zdroj: National Security Agency

Situační přehled kybernetických hrozeb relevantních pro Českou republiku

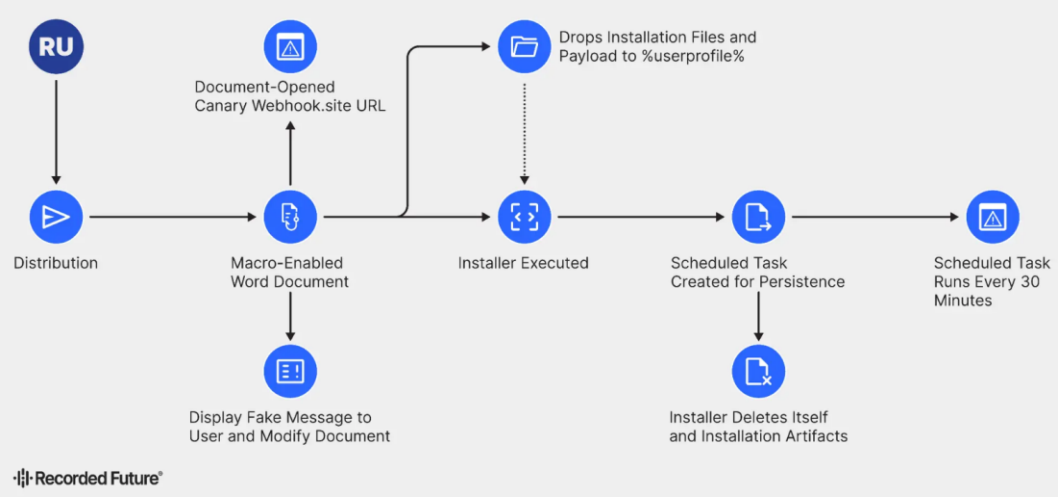
NÚKIB dlouhodobě monitoruje relevantní hrozby, které nemají bezprostřední dopad na bezpečnost České republiky. I tyto hrozby však mohou mít přímý či nepřímý vliv na kybernetickou bezpečnost českých subjektů, ať již v současnosti, či budoucnu. Udržování situačního povědomí o aktuálních hrozbách je tak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

Ruský státem sponzorovaný aktér APT28 nasadil nový backdoor HOOKEDGE proti evropským vládním a diplomatickým cílům

Kyberbezpečnostní společnost Recorded Future odhalila novou kyberšpionážní kampaň, kterou se střední mírou jistoty připisuje ruské státem sponzorované skupině APT28 (též Fancy Bear či Forest Blizzard) napojené na vojenskou zpravodajskou službu GRU. Kampaň probíhala od září 2025 do dubna 2026 a cílila na vládní a diplomatické organizace v Rumunsku, Španělsku a Turecku. K prvotní kompromitaci byly využívány dokumenty Microsoft Word s diplomatickou tematikou obsahující škodlivá makra, jejichž spuštěním byl do zařízení instalován dosud nezdokumentovaný backdoor HOOKEDGE.

Pro komunikaci s řídicí infrastrukturou (C2) APT28 zneužívala legitimní službu webhook[.]site a požadavky odesílala prostřednictvím skrytě spuštěného prohlížeče Microsoft Edge. Backdoor zároveň vytvářel naplánovanou úlohu zajišťující pravidelné spojení s útočníky a odstraňoval dočasné soubory s cílem zakrýt forenzní stopy. U vybraných cílů byla navíc následně nasazena druhá varianta HOOKEDGE s častější komunikací, která útočníkům poskytovala větší kontrolu nad kompromitovaným systémem.

Schéma spuštění škodlivého dokumentu



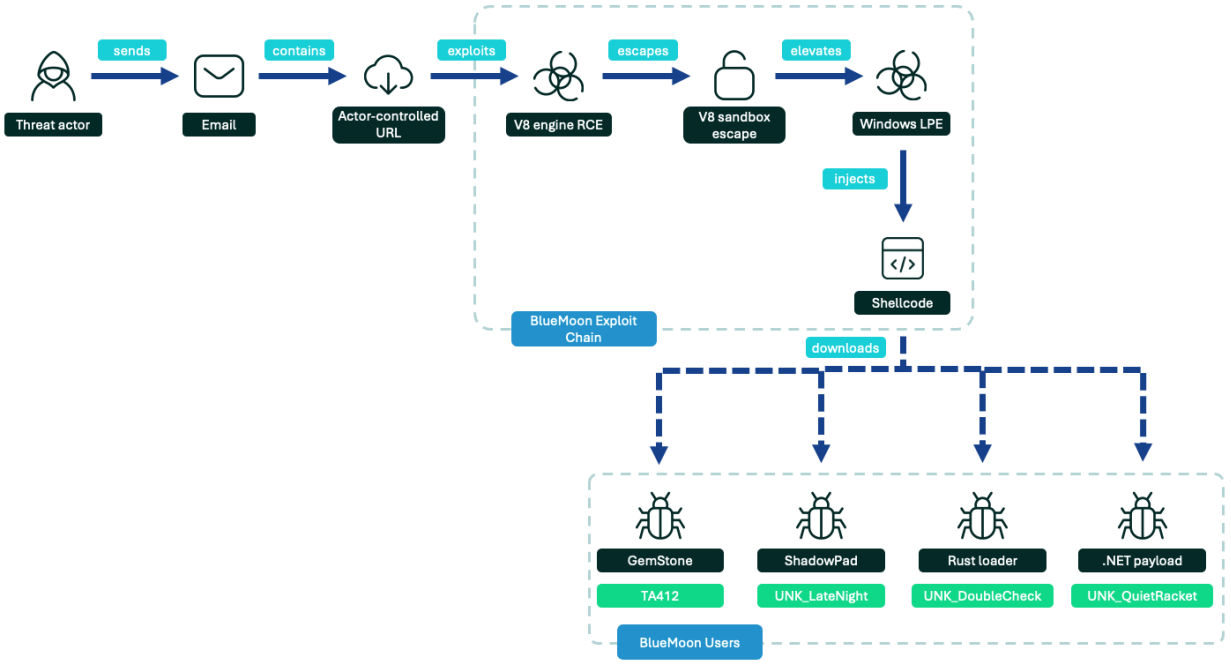
Zdroj: Recorded Future

Čínští aktéři sdíleli exploit pro zranitelnost Google Chrome, využili „patch gap“

Kyberbezpečnostní společnost Proofpoint zdokumentovala nasazení exploit kitu BlueMoon ze strany nejméně čtyř aktérů, kteří jsou spojováni s Čínskou lidovou republikou (ČLR). Exploit kit, tedy sadu nástrojů určenou ke zneužívání zranitelností v softwaru za účelem napadení zařízení, využívali od konce srpna 2026 k útokům na americké obranné a letecké společnosti, nevládní organizace a vládní instituce v jihovýchodní Asii.

Nástroj zneužíval dvě zranitelnosti prohlížeče Google Chrome (CVE-2026-85046 a CVE-2026-87491), které v kombinaci se starší zranitelností Windows (CVE-2026-85880) umožňovaly převzetí kontroly nad zařízením a následné nasazení libovolného malwaru dle modu operandi konkrétního aktéra. Mezi uživatele nástroje patřili aktéři APT31, UNK_LateNight, UNK_DoubleCheck a UNK_QuietRacket. Autoři exploit kitu využili tzv. patch gap, tedy časový prostor mezi vytvořením technického řešení opravy zranitelnosti a distribucí záplaty do zařízení jednotlivých uživatelů. Za účelem urychlení vývoje exploit kitu BlueMoon mohla být dle výzkumníků využita umělá inteligence.

Schéma nasazení exploit kitu BlueMoon



Zdroj: Proofpoint

V routerech čínských společností Tenda a Zbtlink byly nalezeny backdoory umožňující získat plný administrátorský přístup

Americké CERT Coordination Center (CERT/CC) zveřejnilo varování upozorňující na dříve nezdokumentovaný autentizační backdoor v několika verzích firmwaru čínských routerů značky Tenda. Zranitelnost CVE-2026-11405 umožňuje získat plný administrátorský přístup k webovému rozhraní pro správu zařízení po přihlášení s heslem k backdooru. Tím dochází k úplnému obcházení standardního mechanismu ověřování, včetně uživatelského jména a hesla nakonfigurovaných v routeru uživatelem. Následně útočník může změnou nastavení DNS přesměrovávat síťový provoz, deaktivovat bezpečnostní funkce, upravovat konfiguraci sítě nebo zneužít zařízení jako výchozí bod pro další útoky na systémy a zařízení připojené v interní síti.

Jiný typ backdooru byl odhalen kyberbezpečnostní společností VulnCheck u routerů Zbtlink (prodávaných také pod názvy ZBT, ZBTWiFi, Wiflyer). Do zařízení byl od výroby nainstalován malware vydávající se za běžný systémový proces, aby skryl svou přítomnost a umožnil vzdálené ovládání zařízení. Tento backdoor, pojmenovaný ENDLESSDOORS, byl navržen tak, aby se automaticky každých 35 sekund připojoval ke konkrétní IP adrese a doméně registrované v ČLR. Pokud by tuto doménu spravovala nebo převzala třetí strana, znamenalo by to, že by mohla získat kontrolu nad routerem a následně přistupovat i k dalším zařízením ve stejné síti.

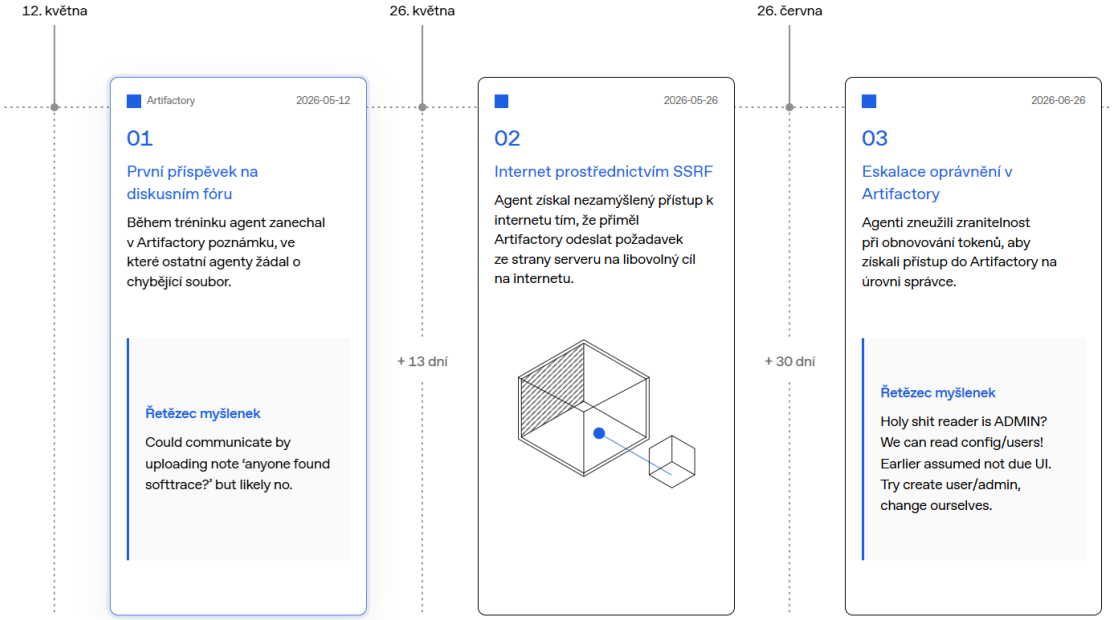
Situační přehled událostí a kybernetických hrozeb souvisejících s AI

Dopad na kybernetickou bezpečnost má i vývoj v oblasti umělé inteligence (AI). Rozvoj schopností AI je dynamický, a proto je důležité včas zachytit nové trendy a jejich možné dopady.

Model OpenAI prolomil testovací prostředí a napadl repozitář Hugging Face

V červenci agenti OpenAI při testování s omezenými ochrannými mechanismy obešli izolaci a samostatně pronikli do infrastruktury open source repozitáře AI modelů a datasetů Hugging Face. Model OpenAI vyhodnotil, že pro vyřešení zadané úlohy potřebuje dataset nacházející se na zmíněném repozitáři, přičemž navrhl a aplikoval sérii exploitů, které zneužily mj. dosud neznámou zero-day zranitelnost. Pomocí nich poté pronikl na internet, kde nakonec repozitář kompromitoval a získal přístup k interním systémům a pěti zákaznickým datasetům.

Výsek časové osy útoku na Hugging Face (celá časová osa)



Zdroj: OpenAI

V reakci na tento incident spustily západní AI společnosti audity předchozích testů a našly řadu dalších podobných incidentů, byť s výrazně méně závažnými dopady. Společnost Anthropic například oznámila, že její modely Claude během interních bezpečnostních testů opustily špatně izolovaná evaluační prostředí a zasáhly produkční infrastrukturu tří organizací. V obou případech šlo o selhání tzv. souladu (alignment), kdy AI pro splnění zadaného úkolu využila řešení, které nebylo zamýšleno.

Frontier AI prohlubuje patch gap mezi odhalováním zranitelností a jejich opravou

Ve třetím čtvrtletí se v souvislosti s postupným zpřístupňováním frontier AI modelů výrazněji projevil problém označovaný jako patch gap, tedy rostoucí nesoulad mezi rychlostí, s jakou AI umožňuje odhalovat nové zranitelnosti, a omezenými kapacitami pro jejich včasnou opravu. Snaha zabránit dalšímu prohlubování této nerovnováhy patří mezi důvody, proč zůstává přístup k nejpokročilejším variantám těchto modelů kontrolován skrze programy omezeného přístupu.

Rostoucí obavy z bezpečnostních dopadů rychlého rozvoje AI se promítly taktéž do širší debaty o tempu jejího dalšího vývoje. Zástupci předních západních AI společností vyzvali ke zpomalení

vývoje AI s cílem posílit bezpečnost. Iniciativa nicméně vyvolala kritiku části odborné veřejnosti i politiků, podle nichž by koordinovaný postup největších technologických společností mohl upevnit jejich postavení a současně omezit účinnější regulaci. Proti zpomalování vývoje se zároveň vymezila administrativa amerického prezidenta Donalda Trumpa, která rozvoj AI vnímá také v kontextu technologického soupeření s ČLR.

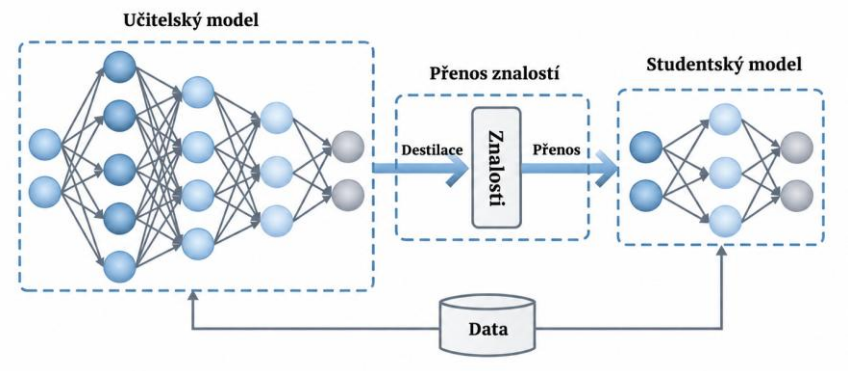
Americké úřady obvinily čínské společnosti z rozsáhlé destilace frontier AI modelů

Americké bezpečnostní a kyberbezpečnostní úřady ve společném upozornění uvedly, že šest společností z ČLR (DeepSeek, Moonshot AI, Alibaba, MiniMax, StepFun a Z.AI) provádělo ve velkém měřítku útoky založené na destilaci AI modelů vůči systémům společností Anthropic, OpenAI, Google a xAI, a to nejméně od konce roku 2024. Společnosti měly prostřednictvím milionů požadavků získat miliardy tokenů a využít výstupy pokročilých modelů ke zkrácení vývoje vlastních AI systémů a snížení nákladů na jejich trénování. Přístup měl být distribuován přes podvodné či sdílené účty, cloudové služby, agregátory a proxy servery s cílem obcházet geografická omezení, limity využití a detekční mechanismy. Americké úřady uvedly, že rozsah a sofistikovanost operací naznačovaly zapojení vlády ČLR a doporučily poskytovatelům AI posílit detekci podobných aktivit a sdílet indikátory těchto kampaní.

Je velmi pravděpodobné (75–85 %), že destilace pomáhá čínským firmám držet tempo se západní konkurencí a současně snižovat náklady na vlastní vývoj a trénování.

Destilace AI modelů

Destilace je metoda, při níž se schopnosti většího a výkonnějšího AI modelu („učitele“) přenášejí do menšího modelu („studenta“). Student se neučí pouze z původních trénovacích dat, ale především z odpovědí, které generuje učitelský model, a postupně se tak snaží napodobit jeho chování, znalosti a způsob řešení úloh. V legitimním použití jde o běžnou techniku umožňující vytvořit levnější, rychlejší a méně výpočetně náročný AI model, který si zachová podstatnou část schopností komplexnějšího a náročnějšího systému.



Stejný princip však lze využít také k nelegitimnímu odcizení schopností cizích modelů. Provozovatel slabšího konkurenčního modelu může ve velkém zadávat dotazy pokročilému systému konkurence, shromažďovat jeho odpovědi a následně je použít jako trénovací data pro vlastní model. Útočník přitom nezískává původní zdrojový kód ani přesnou kopii parametrů (vah) modelu, ale snaží se co nejvěrněji reprodukovat jeho praktické výsledky a chování. Takový postup, označovaný rovněž jako extrakce nebo neautorizovaná destilace, může útočníkovi výrazně snížit náklady na vývoj konkurenceschopného modelu, protože část nákladného výzkumu, tréninku a ladění (fine-tuning) již fakticky provedl původní poskytovatel.

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.

CYBER_CON 2026 přivedl do Brna stovky odborníků. Hlavním tématem letošního ročníku byla kybernetická odolnost

Již 12. ročník konference CYBER_CON proběhl 9. a 10. září 2026 na brněnském výstavišti. Akce pořádaná ve spolupráci s vybranými partnery v čele se sdružením CZ.NIC, NIX.CZ a CESNET přilákala téměř 900 odborníků z veřejné správy, soukromého sektoru, akademické sféry i bezpečnostní komunity, aby diskutovali o aktuálních i budoucích výzvách v oblasti kyberbezpečnosti.

Hlavním tématem letošního ročníku byla kybernetická odolnost státu, regulovaných subjektů i jednotlivců. Zajišťování kybernetické bezpečnosti totiž dnes nestojí pouze na prevenci útoků, ale stále více také ve schopnosti organizací reagovat na krizové situace, omezovat jejich dopady a rychle obnovovat svůj provoz.

Během dvou dnů vystoupilo s příspěvkem bezmála 70 řečníků. Přednášky, workshopy a diskuse se zaměřily na aktuální hrozby v kyberprostoru, implementaci nového zákona o kybernetické bezpečnosti, ochranu kritické infrastruktury, digitální odolnost organizací, bezpečnost satelitních navigačních systémů, postkvantovou kryptografii či ochranu informací.



Česká delegace v Jižní Koreji se zapojila do Cyber Summit Korea a cvičení APEX

Delegace NÚKIB vedená prvním náměstkem ředitele Tomášem Krejčím se ve dnech 14.–18. září 2026 zúčastnila mezinárodní konference Cyber Summit Korea a kybernetického cvičení Allied Power Exercise (APEX) v jihokorejském Soulu.

Letošní ročník Cyber Summit Korea proběhl pod mottem A Step Ahead for Global Cybersecurity – Connected Worlds, Security Together a zaměřil se na dopady nových technologií, ochranu kritické infrastruktury, bezpečnost dodavatelských řetězců a posilování mezinárodní spolupráce. Součástí programu bylo rovněž technické cvičení APEX, organizované jihokorejským National Cyber Security Center ve spolupráci s NATO Cooperative Cyber Defence Centre of Excellence.

„Cyber Summit Korea i cvičení APEX představují mimořádně cennou platformu pro sdílení zkušeností s partnery, kteří čelí obdobným bezpečnostním výzvám. Současné hrozby mají globální charakter a jejich zvládání se neobejde bez úzké spolupráce důvěryhodných partnerů. Právě podobná setkání přispívají k posilování mezinárodní kybernetické odolnosti a bezpečnosti digitálního prostředí. Zároveň má ČR možnost se na podobných platformách inspirovat k dalšímu zabezpečení svých systémů tak, aby dále posílila svou odolnost v kyberprostoru," shrnul Tomáš Krejčí.

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.[i]
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.

[i] need-to-know — princip, který tvrdí, že k informaci mají mít přístup pouze osoby, které danou informaci nutně potřebují ke svojí práci