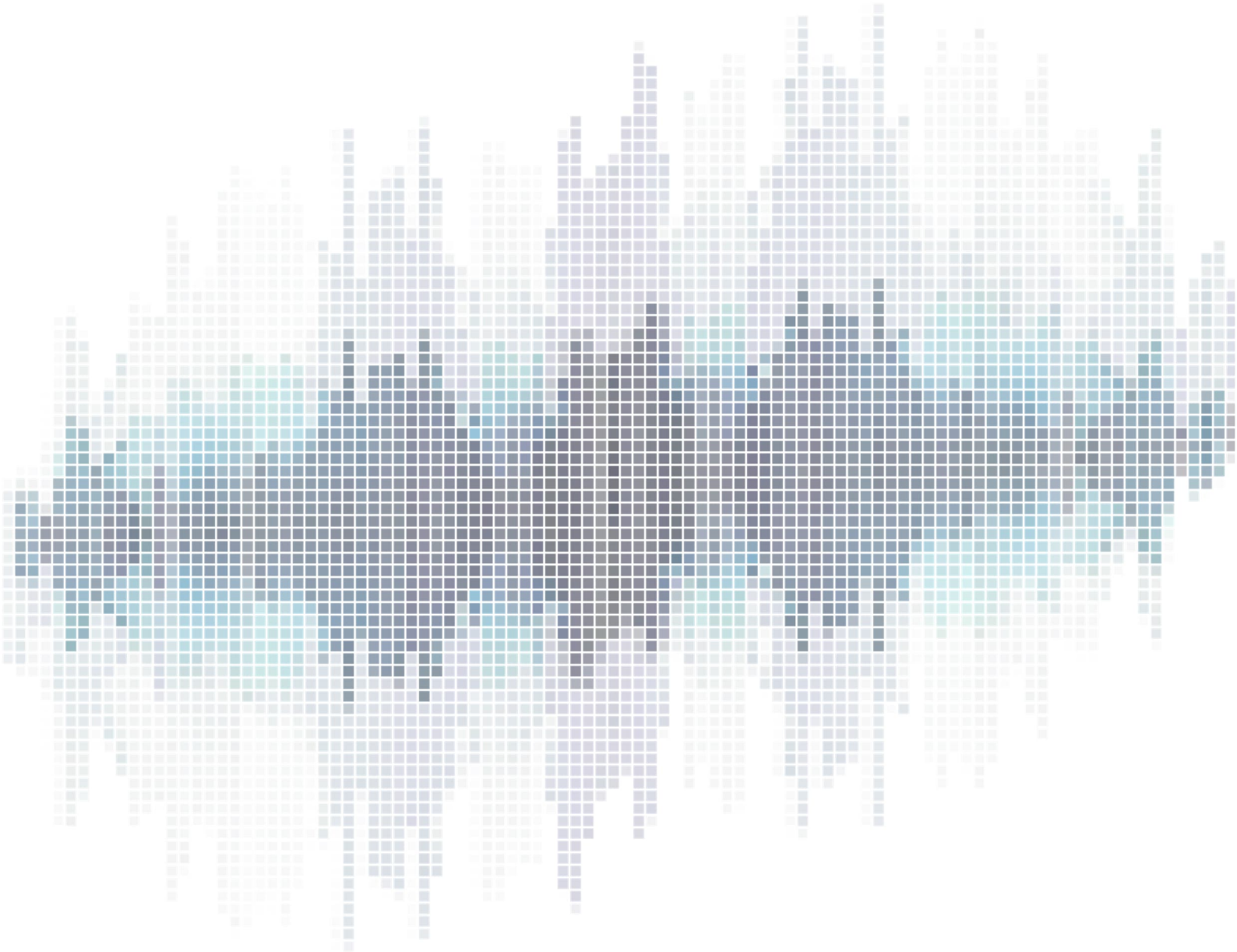
Čtvrtletní přehled hrozeb pohledem NÚKIB

Q4 2025



Národní úřad
pro kybernetickou
a informační bezpečnost

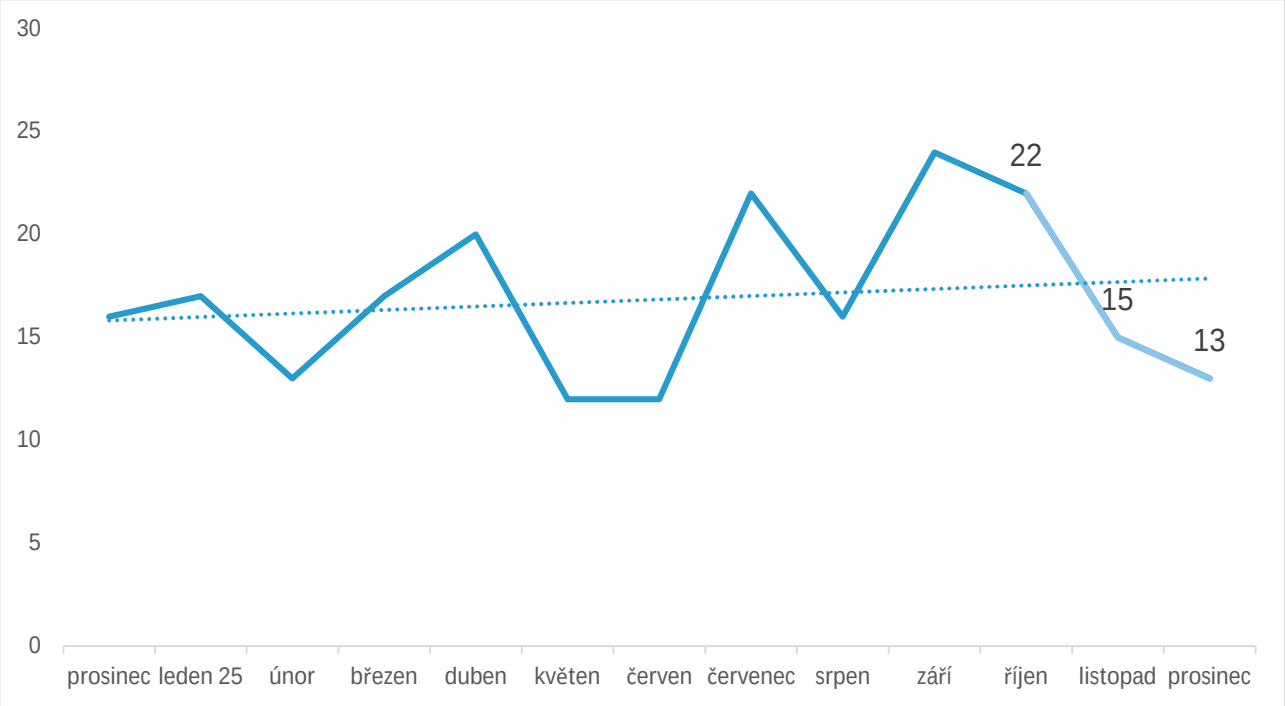
Shrnutí uplynulého čtvrtletí[1]

V posledním čtvrtletí roku 2025 NÚKIB zaznamenal mírný pokles evidovaných incidentů. Ten byl dán mimo jiné nižším počtem zaznamenaných DDoS útoků, kterých oproti předešlému čtvrtletí ubylo na čtvrtinu. Nejpočetnějšími typy incidentů v daném období tak byly provozní výpadky a ransomwarové útoky. Navzdory četnosti žádný z ransomwarových útoků nespadal mezi významné či velmi významné incidenty. Stála za nimi řada různých skupin, včetně gangů Qilin, Inc. Ransom, Warlock, J Group či Obscura. Dále NÚKIB evidoval také několik phishingových útoků, kompromitací účtů a systémů či škodlivých kódů. Incidentů spojených s DDoS útoky za celé čtvrtletí NÚKIB evidoval pouze pět.

NÚKIB posledním čtvrtletí reagoval na řadu hrozeb. Jako příklad lze uvést společné upozornění na aktivity proruských hacktivistů, ke kterému se úřad spolu s dalšími českými i mezinárodními partnery připojil. V prosinci pak podpořil upozornění Spojeného království na škodlivé kybernetické aktivity čínských společností I-S00N a Integrity Tech, které podporovaly ofenzivní kybernetické operace Čínské lidové republiky. Ekosystém soukromých subjektů v Čínské lidové republice, které pro tamní zpravodajské a bezpečnostní složky mimo jiné vyvíjejí ofenzivní nástroje a samy provádějí kybernetické operace proti ostatním zemím, představuje významnou hrozbu i pro české subjekty.

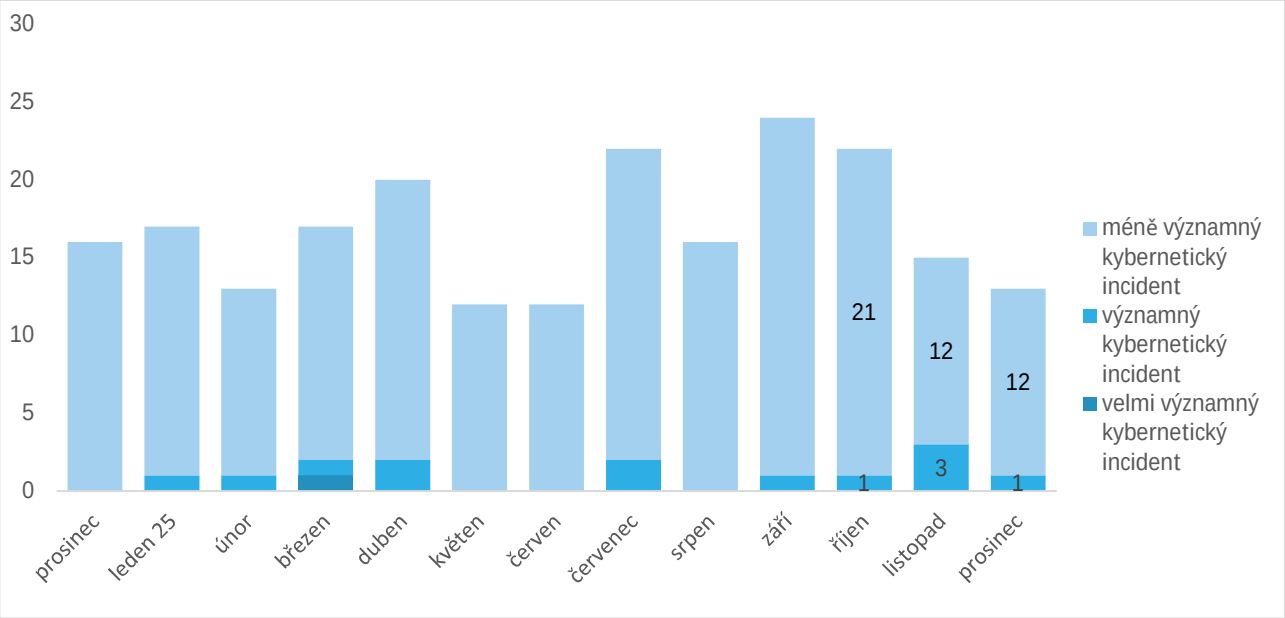
Součástí publikace je opět také širší přehled kybernetických hrozeb relevantních pro Českou republiku a aktivity NÚKIB v oblasti mezinárodní spolupráce.

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



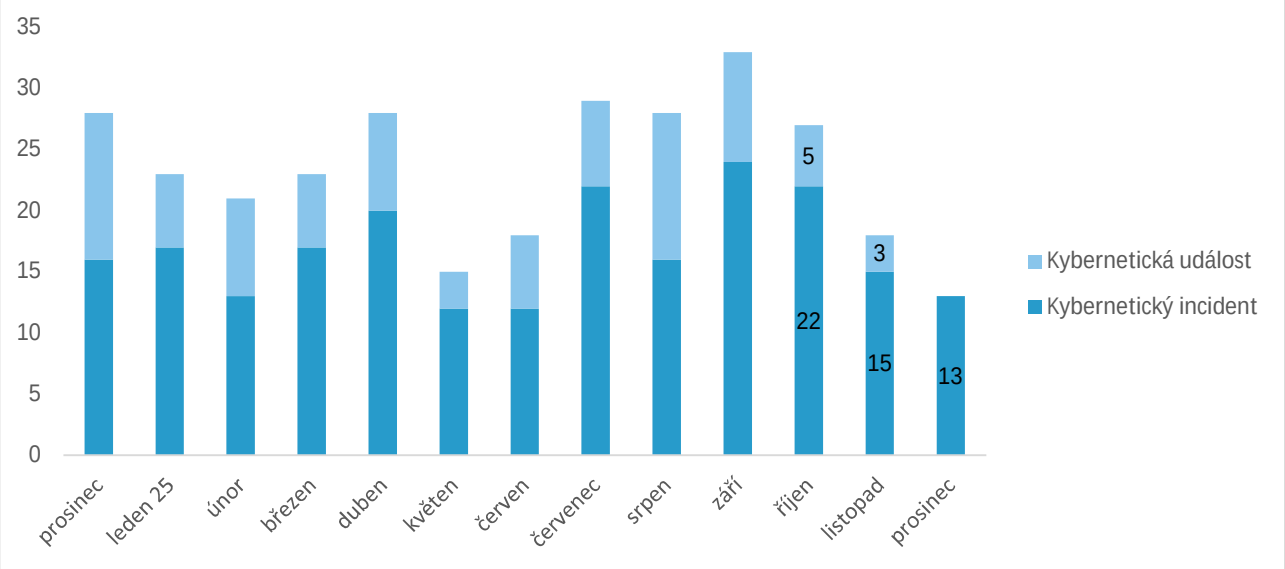
[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

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

NÚKIB se připojil ke společnému mezinárodnímu upozornění na proruské hacktivistické skupiny útočící na subjekty kritické infrastruktury

NÚKIB se spolu s dalšími českými i mezinárodními partnery připojil ke společnému upozornění na proruské hacktivisty, které vydaly americký Federální úřad pro vyšetřování (FBI) a Agentura pro kybernetickou a infrastrukturní bezpečnost (CISA). Upozornění se týká skupin Cyber Army of Russia Reborn (CARR), Z-Pentest, NoName057(16), Sector16 a dalších s nimi spojených aktérů.

Tyto entity jsou pravděpodobně finančně podporovány ruským státem a jednají v jeho zájmu, nejedná se však o pokročilé státní aktéry (APT), čemuž odpovídají i méně sofistikované metody s menším dopadem. Skupiny jsou známy kupříkladu svými DDoS útoky, jež byly v minulosti zaměřeny i proti českým institucím.

Tato uskupení jsou velmi aktivní od začátku ruské invaze na Ukrajinu v roce 2022, přičemž vedou útoky zejména proti Ukrajině a členským státům NATO. V tomto kontextu je možno zmínit, že ve Spojených státech byla rovněž obviněna Ukrajinka Victoria Dubranova z podpory výše zmíněných skupin CARR a NoName057(16) a hrozí jí až 27 let vězení.

Bezpečnostní instituce zapojené do upozornění

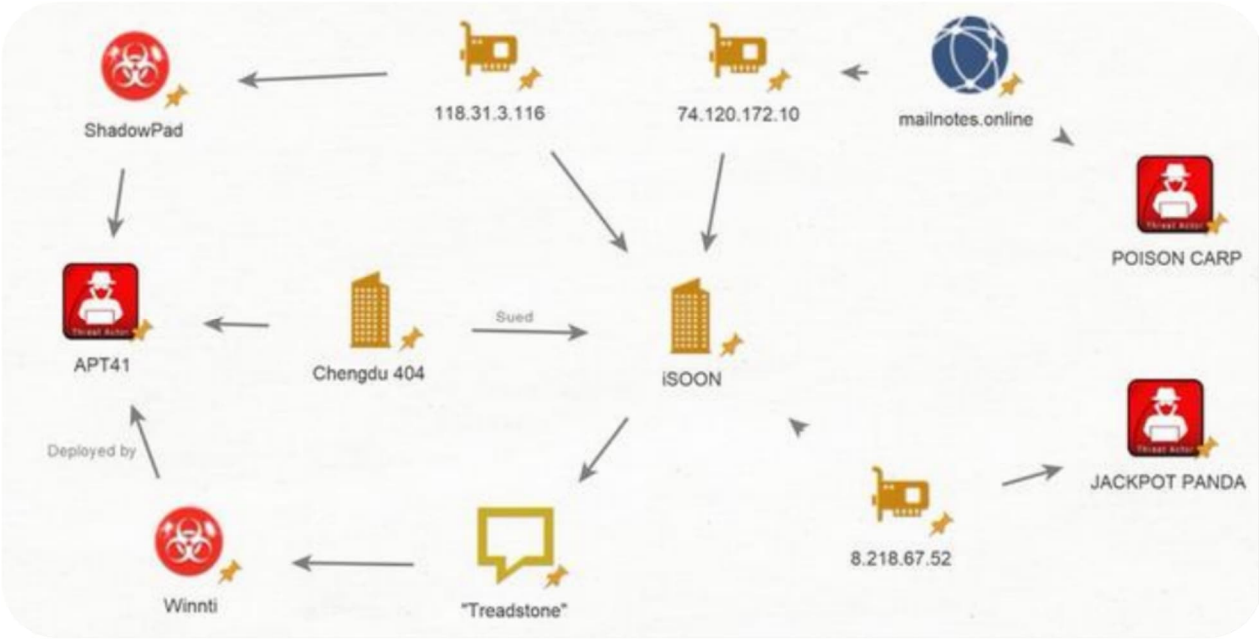
NÚKIB podpořil upozornění Spojeného království na škodlivé kybernetické aktivity čínských společností I-S00N a Integrity Tech

NÚKIB vydal 10. prosince prohlášení, ve kterém podpořil vyjádření partnerů ze Spojeného království, kteří upozornili na škodlivé aktivity čínských společností Anxun Information Technology (též „I-S00N“) a Beijing Integrity Technology (též „Integrity Tech“). Tyto společnosti jsou součástí komplexního ekosystému soukromých subjektů v Čínské lidové republice (ČLR), které pro tamní zpravodajské a bezpečnostní složky mimo jiné vyvíjejí ofenzivní nástroje a samy – s vědomím čínské vlády – provádějí kybernetické operace proti ostatním zemím včetně ČR. Spojené království uvalilo na obě společnosti sankce.

NÚKIB na základě vlastních zjištění i informací od domácích a zahraničních partnerů opakovaně varuje před aktivitami vycházejícími z tohoto ekosystému i ze strany státních aktérů. Tyto činnosti představují pro ČR rostoucí hrozbu, což dokládá kybernetická kampaň APT31, kterou Vláda České republiky v roce 2025 veřejně přisoudila ČLR, stejně jako společné analýzy vypracované se zahraničními partnery, zejména ze září 2025 zaměřující se na aktéra Salt Typhoon.

Souběžně s vyjádřením podpory NÚKIB zveřejnil vlastní analýzu ke společnosti I-S00N, která přináší detailní pohled na její fungování v rámci ekosystému soukromých společností, jejichž škodlivé aktivity ČLR umožňuje, podporuje a využívá.

Napojení I-S00N na další čínské aktéry hrozeb



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.

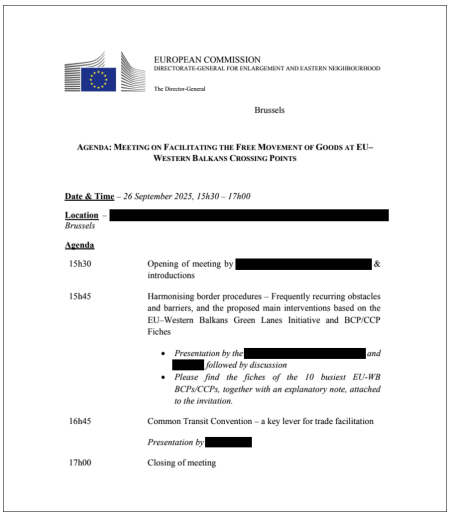
Severokorejský aktér Lazarus podniká kyberšpionáž zaměřenou na společnosti zabývající se bezpilotními letouny

Společnost ESET zaznamenala nové útoky v rámci dlouhotrvající kampaně severokorejského státního aktéra Lazarus. Skupina cílila na několik evropských společností působících v obranném průmyslu, z nichž některé se zabývají vývojem a výrobou bezpilotních leteckých systémů (UAV). Útoky spadají do dlouhotrvající kampaně s názvem Operation DreamJob, která spoléhá na techniky sociálního inženýrství, konkrétně na falešné nabídky prestižních nebo významných pracovních pozic. Ve výše zmíněných případech bylo zaznamenáno využití malwaru ScoringMathTea, který byl použit již v řadě dřívějších útoků. S ohledem na napadené subjekty ESET odhaduje, že operace může souviset s aktuálními snahami Severní Koreje o rozvoj svého UAV programu. Dodává také, že i dosavadní vývoj do značné míry spoléhal na krádeže duševního vlastnictví.

Čínský aktér prováděl špionáž proti diplomatickým misím v Maďarsku, Belgii a dalších evropských zemích

Společnost Arctic Wolf Labs odhalila novou špionážní kampaň čínského aktéra UNC6384 zaměřenou na diplomatické subjekty v Maďarsku, Belgii, Srbsku, Itálii a Nizozemsku. Spear-phishingové e-maily s tematikou setkání Evropské komise a NATO naváděly oběti ke stažení škodlivých souborů obsahujících kompromitovaný legitimní nástroj Canon Printer Assistant, který spouštěl malware PlugX. Útočníci využili zranitelnost ZDI-CAN-25373 v zástupci souboru Windows (LNK), která umožňuje spustit skrytý kód. Dále projevili detailní znalost diplomatického prostředí a v reálném čase využívali kalendáře evropských jednání. Zároveň tak prokázali vysokou úroveň schopností v sociálním inženýrství, která kampani dodala dojem důvěryhodnosti.

Ukázka spear-phishingové návnady (větší rozlišení)



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENLARGEMENT AND EASTERN NEIGHBOURHOOD
The Director-General

Brussels

AGENDA: MEETING ON FACILITATING THE FREE MOVEMENT OF GOODS AT EU–WESTERN BALKANS CROSSING POINTS

Date & Time – *26 September 2025, 15h30 – 17h00*

Location – [redacted]
Brussels

Agenda

15h30	Opening of meeting by [redacted] & introductions
15h45	Harmonising border procedures – Frequently recurring obstacles and barriers, and the proposed main interventions based on the EU–Western Balkans Green Lanes Initiative and BCP/CCP Fiches • *Presentation by the* [redacted] *and* [redacted] *followed by discussion* • *Please find the fiches of the 10 busiest EU-WB BCPs/CCPs, together with an explanatory note, attached to the invitation.*
16h45	Common Transit Convention – a key lever for trade facilitation *Presentation by* [redacted]
17h00	Closing of meeting

Skupina UNC6384 se dlouhodobě zaměřuje na diplomatické subjekty, přičemž dříve cílila na diplomaty v jihovýchodní Asii a nově rozšířila své aktivity i na evropské diplomatické cíle. Specializuje se na nasazování variant malwaru PlugX, který se aktivně používá nejméně od roku 2008 a zůstává oblíbeným nástrojem čínských aktérů. Podle analytiků společnosti Google existuje překryv mezi tímto aktérem a skupinou Mustang Panda, a to v rámci infrastruktury, cílení i TTPs.

Nová fáze Operace Endgame úspěšně narušila další část kyberkriminální infrastruktury

V polovině listopadu 2025 proběhla zatím poslední fáze Operace Endgame, která vedla k neutralizaci více než tisíce serverů a dvaceti domén. Při této realizaci byl narušen botnet Elysium a také bylo narušeno šíření rodin malwarů Rhadamanthys Stealer a Venom RAT. V případě Venom RAT pak došlo i k zatčení hlavního podezřelého, který se v té době nacházel v Řecku. Zasažená infrastruktura byla využita k infikování stovek tisíc zařízení po celém světě.

Operace Endgame 3.0, které se účastnily policejní orgány z devíti států napříč kontinenty, je pokračováním mezinárodní spolupráce v boji s kyberzločinem, jež je koordinována evropskými institucemi Europol a Eurojust a která začala v roce 2022. Významného úspěchu tato mezinárodní operace dosáhla v květnu 2024, kdy byly zatčeny čtyři osoby a bylo neutralizováno přes sto serverů a dva tisíce domén.

Logo operace Endgame

Německo obvinilo Rusko z kyberútoku na řízení letového provozu a pokusu o ovlivnění voleb

Německá vláda obvinila Ruskou federaci z kybernetického útoku na řízení letového provozu v roce 2024 a z pokusu o ovlivnění posledních federálních voleb prostřednictvím dezinformační kampaně. V návaznosti na tento krok si také předvolala ruského velvyslance.

Za kyberútokem na německou společnost Deutsche Flugsicherung (DFS), pověřenou řízením letového provozu nad Německem, dle tamní vlády stála ruská státem sponzorovaná skupina APT28 (též Forest Blizzard či Fancy Bear). DFS kompromitaci potvrdila, uvedla nicméně, že lety nebyly útokem nijak ovlivněny.

Mluvčí německého ministerstva zahraničí rovněž uvedl, že Rusko se pokusilo ovlivnit a destabilizovat poslední federální volby a vnitřní záležitosti státu prostřednictvím dezinformační kampaně nazvané Storm-1516. Jako příklad těchto aktivit uvedla německá vláda falešná videa, která jen několik dní před volbami tvrdila, že došlo k manipulaci s hlasy.

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.

NÚKIB úspěšně absolvoval 17. ročník největšího aliančního kyberbezpečnostního cvičení Cyber Coalition 2025

NÚKIB se zúčastnil Cyber Coalition 2025, jednoho z nejvýznamnějších mezinárodních cvičení kybernetické bezpečnosti pořádaného NATO ve spolupráci s NATO CCD COE. Hlavním cílem bylo procvičit spolupráci, koordinaci a sdílení informací při řešení kybernetických incidentů, které mohou ohrozit kritickou infrastrukturu, spojenecké operace i mezinárodní organizace.

Účastníci reagovali na realistické scénáře podle principu „train as you fight“, zahrnující technické útoky, procesní postupy i právní aspekty řešení krizových situací. Do cvičení se kromě členských států NATO zapojily také Rakousko, Austrálie, Japonsko, Korejská republika Švýcarsko, Ukrajina, zástupci Evropské unie, akademické sféry a soukromého sektoru. Českou republiku tradičně reprezentoval tým odborníků z NÚKIB doplněný kolegy z Velitelství informačních a kybernetických sil Armády ČR.

Ředitel NÚKIB Lukáš Kintr navštívil Austrálii a jednal o posílení spolupráce v oblasti kybernetické bezpečnosti

Ředitel NÚKIB Lukáš Kintr a ředitel kabinetu Roman Pačka absolvovali během října cestu do Austrálie zaměřenou na rozvoj bilaterální spolupráce v oblasti kybernetické bezpečnosti. Tato první oficiální návštěva vedení NÚKIB v Austrálii potvrdila rostoucí význam česko-australského partnerství v kybernetické bezpečnosti.

Mezi hlavní témata jednání patřily hrozby vůči kritické infrastruktuře ze strany státem sponzorovaných aktérů, otázky důvěryhodných a bezpečných technologií či dopady rychlého rozvoje umělé inteligence na kybernetickou bezpečnost. Diskuze se dotkly také ochrany energetické infrastruktury a bezpečnosti připojených vozidel, tedy oblastí, které mají rostoucí význam jak v Evropě, tak v indo-pacifickém regionu.

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.