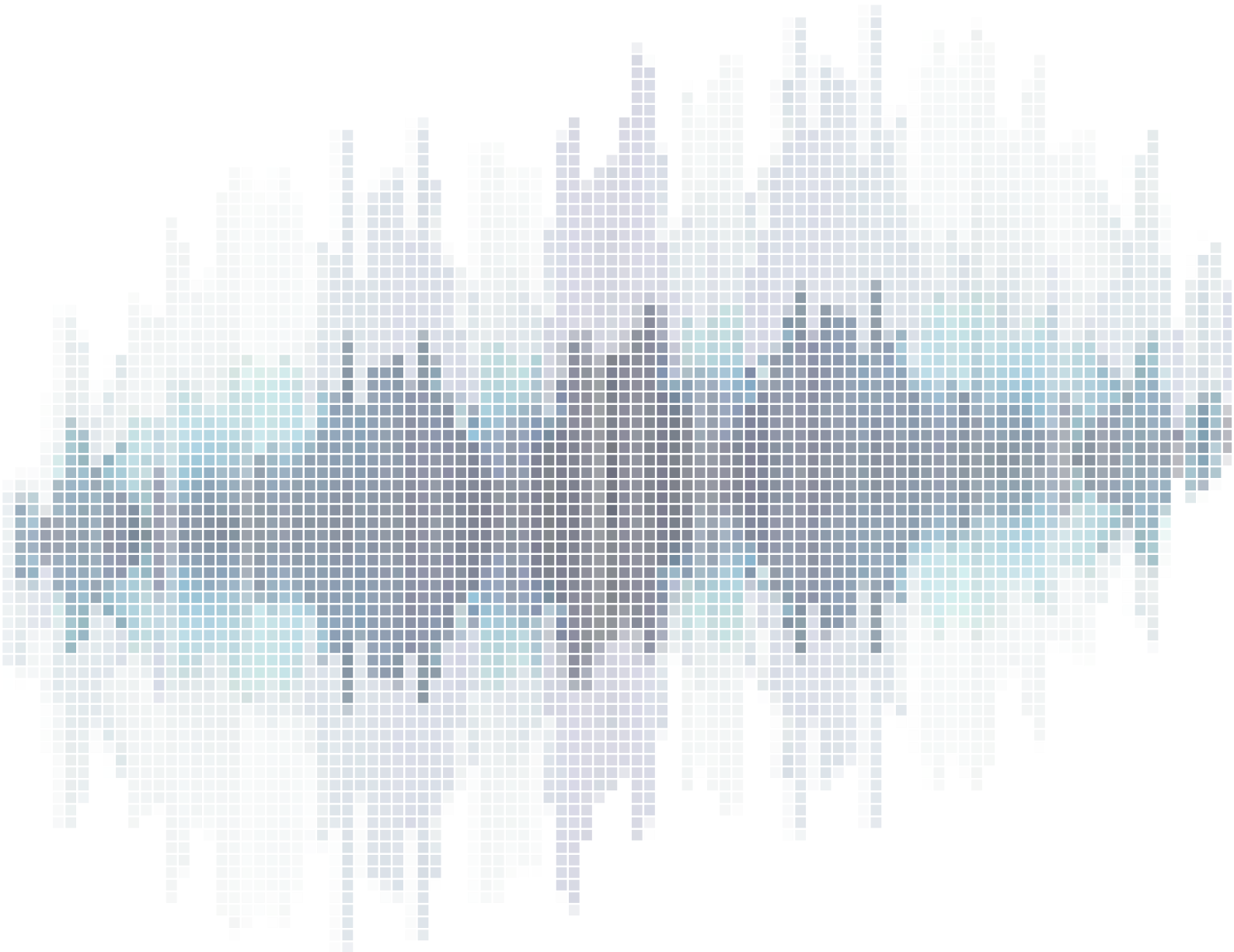
Čtvrtletní přehled hrozeb pohledem NÚKIB

Q1 2025



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí uplynulého čtvrtletí[1]

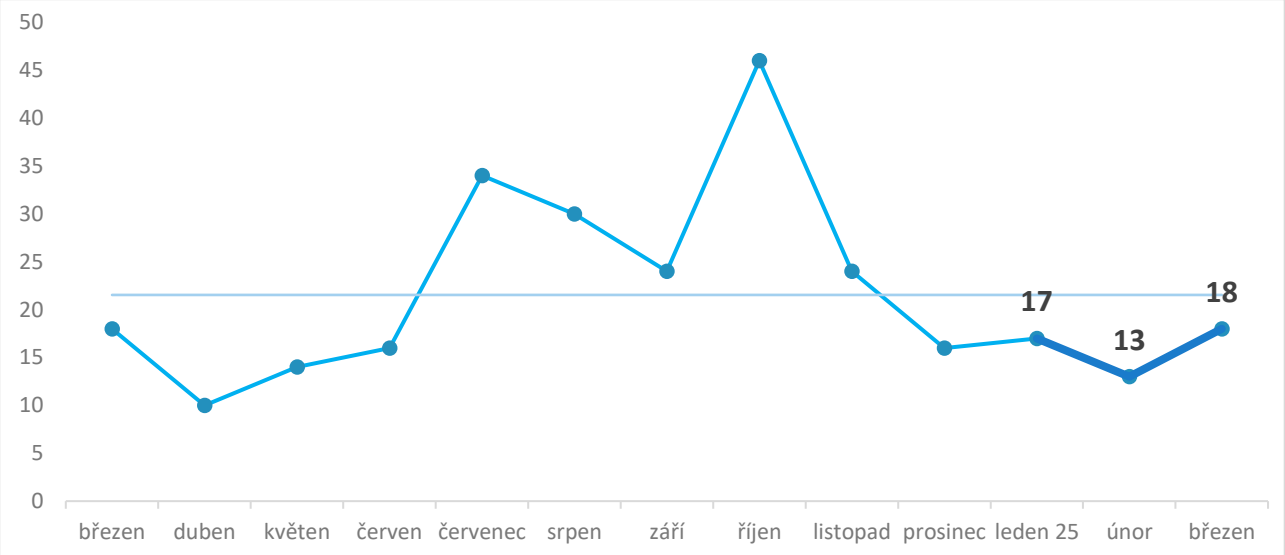
První čtvrtletí roku 2025 provázel podprůměrný počet kybernetických incidentů. Celkem jich Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) evidoval 48. Většina z nich představovala zejména útoky na dostupnost, tudíž se vesměs jednalo o méně významné kybernetické incidenty. V každém měsíci prvního čtvrtletí však NÚKIB evidoval i jeden významný incident, přičemž během března byl jako velmi významný incident klasifikován ransomwarový útok na systémy Hasičského záchranného sboru ČR (HZS), konkrétně v Královéhradeckém a Zlínském kraji.

Hlavním trendem prvního čtvrtletí byl opětovný nárůst ransomwarových útoků, kterých NÚKIB evidoval deset, přičemž šest z nich proběhlo během března. Opakuje se tak situace z posledního čtvrtletí roku 2024, kdy taktéž došlo k nárůstu evidovaných ransomwarových útoků. Ani v tomto případě se však nejedná o koordinovanou kampaň, ale o vyšší aktivitu různých útočníků.

Dále se tento dokument zaměřuje na shrnutí zpráv a událostí v celosvětovém kontextu, nicméně s přesahem na kybernetickou bezpečnost v tuzemsku. Jedná se například o pozitivní globální trend snižujícího se objemu financí vyplacených v rámci ransomwarových útoků za rok 2024 nebo situaci v kontextu údajného úniku dat společnosti Oracle. Z událostí relevantních pro ČR uvádíme například kampaň ruského aktéra Seashell Blizzard, čínskou kyberšpionážní kampaň vůči evropskému zdravotnickému sektoru či aktuální kybernetické hrozby spojené s událostí Expo 2025 právě probíhající v Japonsku.

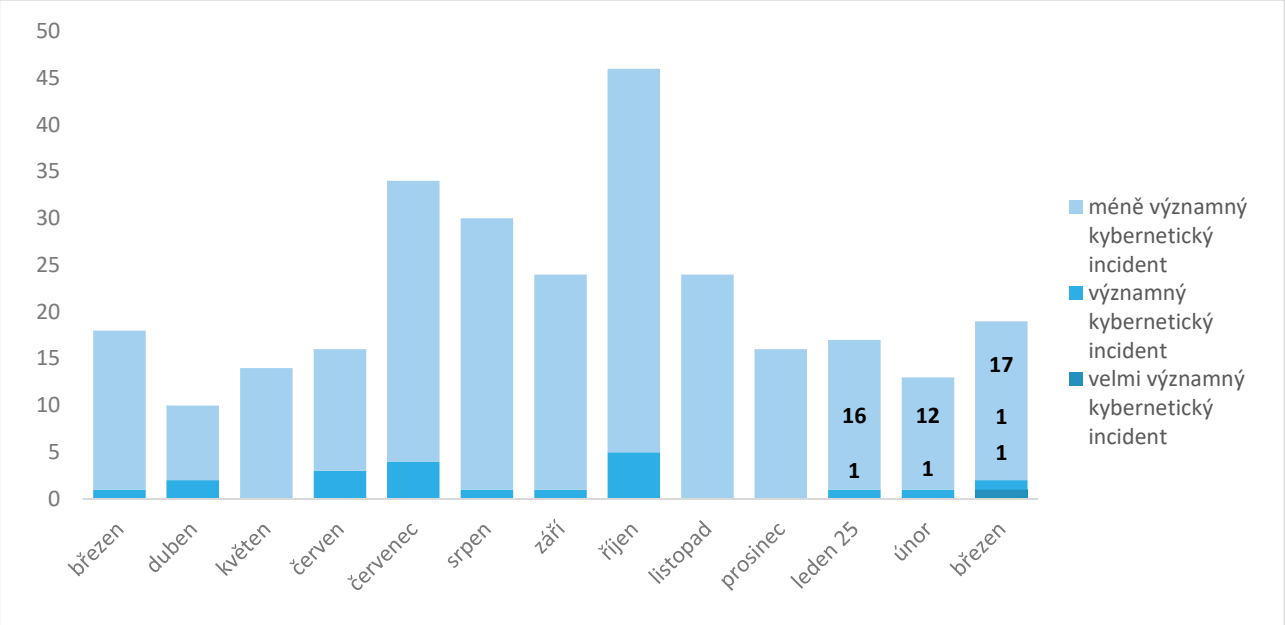
Závěrem sdílíme přehled hlavních aktivit NÚKIB v kontextu mezinárodní spolupráce. Kromě shrnutí průběhu události Prague Cyber Security Conference 2025 zmiňujeme aktivitu NÚKIB v otázce bezpečnosti hraničních síťových prvků.

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



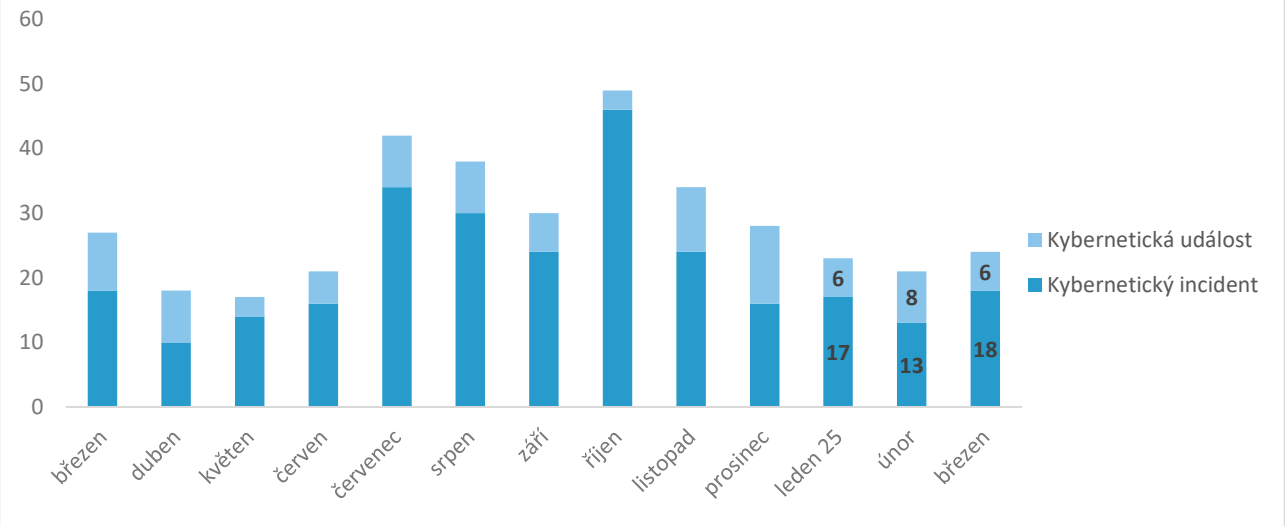
[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

Závažnost řešených kybernetických incidentů[2]



Poměr 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 jako kybernetický incident, kybernetická událost nebo jako nerelevantní podnět. Graf níže ukazuje poměr 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

Objem zaplaceného výkupného v souvislosti s ransomwarem se meziročně snížil

Podle v únoru zveřejněné analýzy společnosti Chainalysis došlo v roce 2024 ke snížení celkového objemu výkupného zaplaceného v souvislosti s ransomwarovými útoky. Meziročně tak došlo k 35% propadu z 1,25 miliardy USD na 812 milionů USD (z cca 30 mld. Kč na cca 19,8 mld. Kč). Zároveň se snížil také celkový počet plateb výkupného. Data z poloviny roku 2024 přitom původně naznačovala, že by mělo jít o dosud rekordní rok. Mezi jedny z klíčových faktorů ovlivňující tento vývoj patřila mezinárodní policejní Operace Cronos, která zneškodnila do té doby nejaktivnější ransomwarový gang LockBit. Dalším zásadním faktorem pak měl být odchod ze scény dalšího z významných ransomwarových aktérů, Black Cat/AlphV.

V kontextu incidentů evidovaných NÚKIB však stále platí, že ransomwarové útoky patří k nejzávažnějším hrozbám pro tuzemské subjekty. Přestože jejich počty se stále pohybují spíše v jednotkách měsíčně, řadě subjektů mnohdy působí výrazné finanční škody, omezení provozu či poskytování služeb, ale i reputační riziko, pakliže dojde ke zveřejnění zcizených dat jejich klientů. Závažnost a aktuálnost hrozby ukazuje i současný incident vůči HZS. Ten byl svou závažností vyhodnocen jako velmi významný.

Únik dat společnosti Oracle se může týkat i jejích českých klientů, přesná povaha uniklých dat je však stále diskutována

V pátek 21. března 2025 zveřejnil uživatel rose87168 na platformě BreachForums příspěvek, ve kterém tvrdil, že má přístup k přihlašovacím serverům společnosti Oracle Cloud a nabízí k prodeji citlivé údaje, včetně přihlašovacích údajů a autorizačních klíčů. Únik dat se měl týkat více než 6 milionů uživatelů v rámci více než 140 tisíc společností. Své tvrzení se autor snažil dokázat zveřejněním seznamu domén, jimiž měl disponovat, i zbytkem výše zmíněných dat. Samotná společnost Oracle únik informací ze svého cloudového prostředí nejprve popírala, následně však přiznala možný únik části dat ze zastaralých serverů, které však nemají pro útočníky žádnou hodnotu.

Navzdory stále aktivní debatě o povaze incidentu došlo k vydání preventivního varování na Portálu NÚKIB. NÚKIB však dosud neeviduje žádný incident spojený s tímto údajným únikem dat. Existuje tudíž reálná šance (40–50 %), že tvrzení společnosti Oracle je pravdivé a k úniku sice došlo, nicméně daná data neumožňovala provádět útočníkům další škodlivé aktivity.

Upozornění na další vlnu podvodných telefonátů zneužívající identitu NÚKIB

V únoru NÚKIB zveřejnil upozornění na další vlnu podvodných telefonátů zneužívajících identitu NÚKIB s cílem finančního zisku. Útočníci při nich využívají techniku tzv. spoofingu, kdy se oběti zobrazí telefonní číslo dle útočníkovi volby. Útočníci se tak snaží docílit důvěry obětí a přesvědčit je o nutnosti ochránit jejich finance skrze převedení na jejich „rezervní“ účet. Nedávno však došlo k integraci antispoofingové ochrany mezi sítěmi všech tří hlavních českých operátorů, což by mělo podobné útoky s využitím spoofingu v budoucnu omezit.

Detailnější popis kampaně lze nalézt na našem webu.

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.

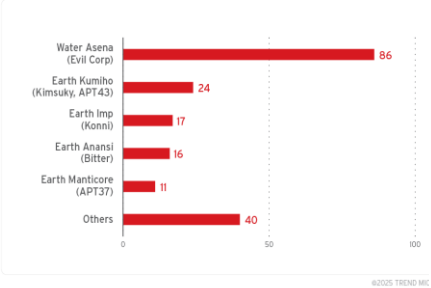
Ruský aktér Seashell Blizzard útočil v dlouhodobé globální kampani na dodavatelské společnosti, mezi cíli je i ČR

(23.02.2025, cert.gov.ua) Ukrajinský CERT-UA odhalil na začátku roku 2024 škodlivou aktivitu podskupiny ruského aktéra Seashell Blizzard (taktéž známého jako Sandworm či APT44, podléhající vojenské rozvědce, GRU) s cílem provést destruktivní kyberútoky na informační a komunikační systémy přibližně dvaceti společností zabývajících se dodávkami energie, vody a tepla v deseti oblastech Ukrajiny. Zároveň uvádí, že v řadě souvisejících kampaní, které proběhly mezi červencem 2024 a únorem 2025, byly zacíleny dodavatelské společnosti mj. i v České republice. V počáteční fázi kompromitace se útočníci vydávají za potenciálního zákazníka, přičemž oběť navádějí ke stažení technické dokumentace v podobě dokumentu PDF se zkresleným obsahem. Použitý malware zahrnuje SECONDBEST, EMPIREPAST, SPARK a CROOKBAG.

Státem sponzorovaní aktéři ve svých útocích zneužívají LNK soubory

(18.03.2025, therecord.media) Výzkumníci společnosti Trend Micro identifikovali rostoucí trend v používání zástupců Windows (LNK souborů) v rámci kampaní státem sponzorovaných skupin. Podle Trend Micro útočníci zneužívají zranitelnost, kterou společnost označila jako ZDI-CAN-25373. Ta spočívá ve způsobu, jakým Windows zobrazuje obsah LNK souborů. Při kontrole vlastností souboru skrze běžné uživatelské rozhraní totiž uživatel nepozná, zda soubor obsahuje škodlivý obsah či nikoliv. Trend Micro ve své zprávě dokumentuje příklady zneužití LNK souborů více než 10 APT skupinami napojenými na Írán, Severní Koreu a Čínskou lidovou republiku, přičemž každá z nich implementuje techniku odlišně.

Počet vzorků LNK souborů spojených s vybranými APT skupinami (větší rozlišení)



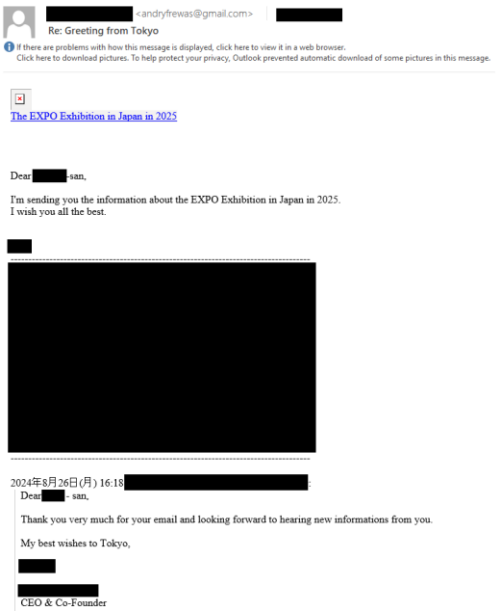
Čínská skupina cílila na evropské zdravotnické instituce

(21.02.2025, therecord.media) Podle zprávy společnosti Orange Cyberdefense podnikala dosud neznámá skupina spojovaná s Čínskou lidovou republikou v druhé polovině roku 2024 kyberútoky vůči evropským zdravotnickým institucím. Skupina, která byla pojmenována Green Nailao, zřejmě zneužila zranitelnost nultého dne v produktech izraelské kyberbezpečnostní společnosti Check Point. Zranitelnost pak umožnila útočníkům ukrást přihlašovací údaje uživatelů a získat přístup k virtuálním privátním sítím (VPN) pomocí legitimních účtů. K útokům využila nástroje, které jsou obvykle spojovány s čínskými APT skupinami (zejména malwary ShadowPad a PlugX), ale i zcela nové a méně tradiční nástroje včetně nového typu ransomwaru, který analytici pojmenovali NailaoLocker.

Kyberšpionážní kampaň čínského aktéra MirrorFace zneužívající téma Expo 2025 cílila na středoevropský subjekt

(18.03.2025, thehackernews.com) Společnost ESET informovala o kyberšpionážní kampani aktéra MirrorFace (taktéž známého jako Earth Kasha), který je spojován s Čínskou lidovou republikou. V rámci této kampaně nazvané Operation AkaiRyū (Rudý drak) byly zacíleny diplomatický institut ve střední Evropě a japonská výzkumná instituce. Útok na evropský subjekt představuje novinku v rámci viktimologie aktéra, který se dosud orientoval primárně na japonské cíle. Spear-phishing byl zaznamenán již v roce 2024, přičemž zneužíval téma světové výstavy Expo 2025 v japonské Ósace, která začala letos v dubnu. ESET považuje MirrorFace za podskupinu APT10, aktéra spadajícího pod čínské Ministerstvo státní bezpečnosti. Jedním z hlavních důvodů je využívání backdooru ANEL, který byl dosud používán exkluzivně skupinou APT10.

Příklad phishingového e-mailu z kampaně Operation AkaiRyū (větší rozlišení)



Skupina Salt Typhoon napadla další telekomunikační společnosti, tentokrát pomocí zranitelností v Cisco routerech

(13.02.2025, cyberscoop.com) Společnost Recorded Future vydala zprávu, ve které popisuje další sérii kompromitací telekomunikačních společností čínskou APT skupinou Salt Typhoon. Skupina se v tomto případě zaměřila na zranitelnosti nacházející se v routerech značky Cisco a pronikla tak mezi prosincem 2024 a lednem 2025 do sítí pěti dalších společností v USA, Thajsku, Itálii a Jihoafrické republice. Salt Typhoon se od začátku prosince 2024 pokusila zneužít více než 1 000 routerů této značky po celém světě, přičemž se zaměřila především na ty, které běží v telekomunikačních sítích. Skupina využívala sérii dvou známých zranitelností (CVE-2023-20198 a CVE-2023-20273), která jí umožnovala dosáhnout eskalace přístupových oprávnění v Cisco IOS XE, operačním systému výrobce pro síťová zařízení.

Ruský státem sponzorovaný aktér Star Blizzard nově cílí na WhatsApp účty svých obětí

(16.01.2025, microsoft.com) Podle analýzy společnosti Microsoft došlo u ruského aktéra Star Blizzard (též Callisto či COLDRIVER), podléhajícího Federální službě bezpečnosti (FSB), ke změně taktik, což dokazují odhalením jeho kampaně z října minulého roku. Během ní měl aktér cílit na kompromitaci účtů na messengerové aplikaci WhatsApp skrze škodlivý QR kód a odkaz. QR kód byl vydáván za pozvánku do skupiny, která má údajně sdružovat nevládní organizace a další osoby aktivní v podpoře a rekonstrukci Ukrajiny. QR kód byl však záměrně nefunkční a po vzoru předchozích kampaní aktéra vyzýval oběť k interakci s útočníky. Ti na případnou zprávu o nefunkčnosti kódu reagovali zasláním škodlivého odkazu, který po rozkliknutí a splnění úkonů k autentizaci v reálu zpřístupnil účet oběti útočníkům.

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.

Šestý ročník mezinárodní Prague Cyber Security Conference 2025

Ve dnech 18.–19. března 2025 se v Praze odehrál již šestý ročník mezinárodní Prague Cyber Security Conference, uspořádaný NÚKIB ve spolupráci s Ministerstvem zahraničních věcí České republiky.

Akce nesla podtitul „Invisible frontlines“. Odborníci diskutovali o vyvíjejících se strategiích na neviditelných frontách boje za kybernetickou bezpečnost – prostřednictvím spolupráce mezi vládami, orgány činnými v trestním řízení a soukromými subjekty. Diskuse se týkaly také postupů proti kyberútokům ze strany Čínské lidové republiky, Ruska a Íránu, hovořilo se o skrytých kybernetických taktikách nebo tzv. stínových operacích, které Čínská lidová republika uskutečňuje v západních zemích.

Paralelně s hlavním programem konference probíhala bilaterální jednání zástupců NÚKIB a mezinárodních partnerů. Právě posilování mezinárodní spolupráce bylo jedním z hlavních cílů akce. Více informací o konferenci naleznete zde.

NÚKIB se zahraničními partnery spolupodepsal dokumenty o bezpečnosti hraničních síťových prvků

Národní úřad pro kybernetickou a informační bezpečnost se připojil k mezinárodní iniciativě vedené Australským signálním zpravodajstvím a spolupodepsal dva dokumenty zaměřené na zvýšení bezpečnosti hraničních síťových prvků. K podpisu se připojili i další mezinárodní partneři, jako např. americké instituce CISA a NSA či Kanadské centrum kybernetické bezpečnosti.

Dokumenty shrnují aktuální poznatky o zneužívaných hraničních síťových prvcích, jako jsou podnikové routery, firewally a VPN koncentrátory, a poskytují doporučení pro zmírnění těchto hrozeb. Cílem obou dokumentů je tak přispět k navýšení odolnosti organizací prostřednictvím kombinace robustních bezpečnostních opatření a mezinárodní spolupráce. Dokumenty zaměřené na zvýšení bezpečnosti hraničních síťových prvků naleznete zde.

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	15–35 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách nukib.gov.cz). 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 a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
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.
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.