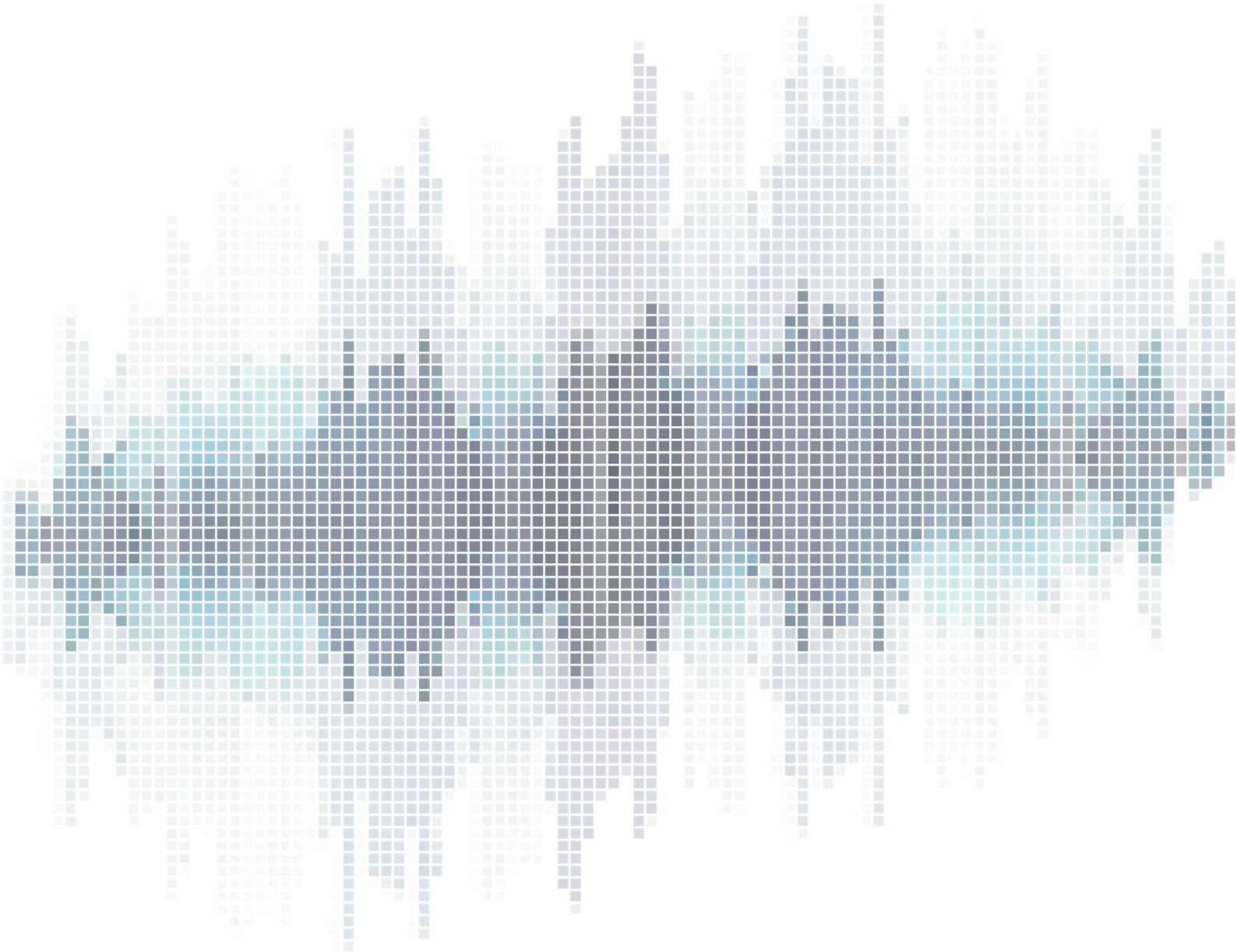
Čtvrtletní přehled hrozeb pohledem NÚKIB

Q2 2025



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí uplynulého čtvrtletí[1]

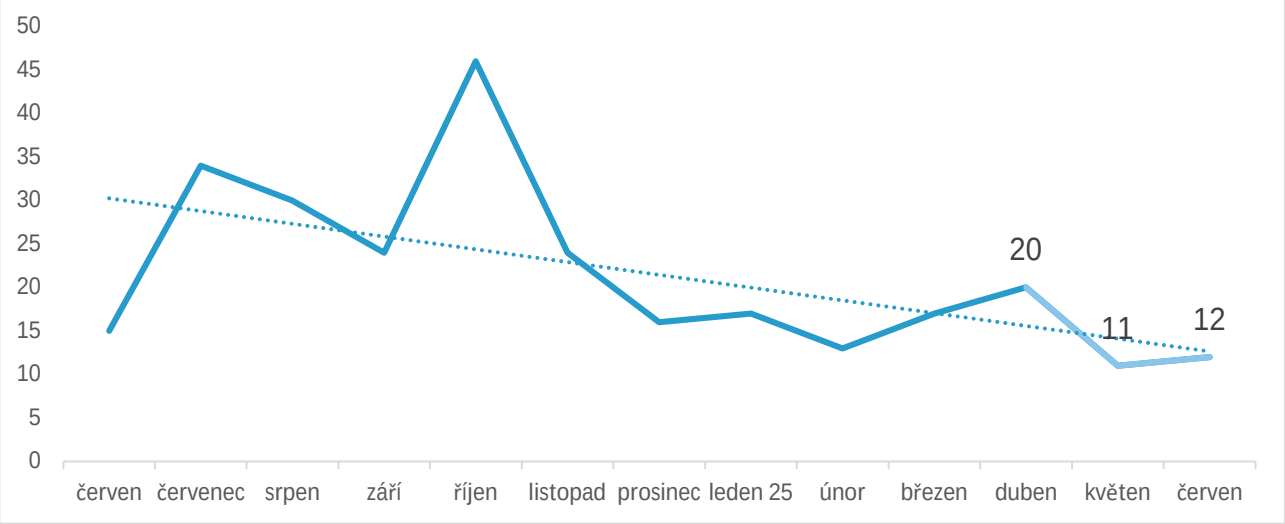
Druhé čtvrtletí roku 2025 bylo významné zejména z pohledu reakce České republiky na aktivity škodlivých kybernetických aktérů vůči tuzemským subjektům. Vláda ČR na základě analýz provedených NÚKIB, Vojenským zpravodajstvím, Bezpečnostní informační službou a Úřadem pro zahraniční styky označila Čínskou lidovou republiku (ČLR) zodpovědnou za škodlivou kybernetickou kampaň proti Ministerstvu zahraničních věcí ČR. Za útokem velmi pravděpodobně stojí skupina APT31 (známá též jako Zirconium nebo Judgment Panda), která je spojována s celou řadou útoků proti politickým a jiným cílům, mj. v EU či NATO.

Během května se pak NÚKIB také spolu s Bezpečnostní informační službou a Vojenským zpravodajstvím a řadou zahraničních partnerů připojil k upozornění na dlouhodobou kybernetickou kampaň ruského aktéra APT28.

Co se týče kybernetických incidentů, druhé čtvrtletí tohoto roku bylo obdobně jako to předchozí typické podprůměrnými hodnotami evidovaných incidentů. Data za celý uplynulý rok pak naznačují jasný klesající trend počtu zaznamenaných kybernetických incidentů (viz graf níže). V rámci tohoto trendu se promítají zejména nižší počty útoků typu Distributed Denial of Service (DDoS) oproti dřívějším obdobím. Pro srovnání – v první polovině tohoto roku NÚKIB evidoval necelé dvě desítky DDoS útoků, zatímco během druhé poloviny roku 2024 téměř čtyřnásobek. K mírnému poklesu v posledním pololetí došlo například také u ransomwarových útoků.

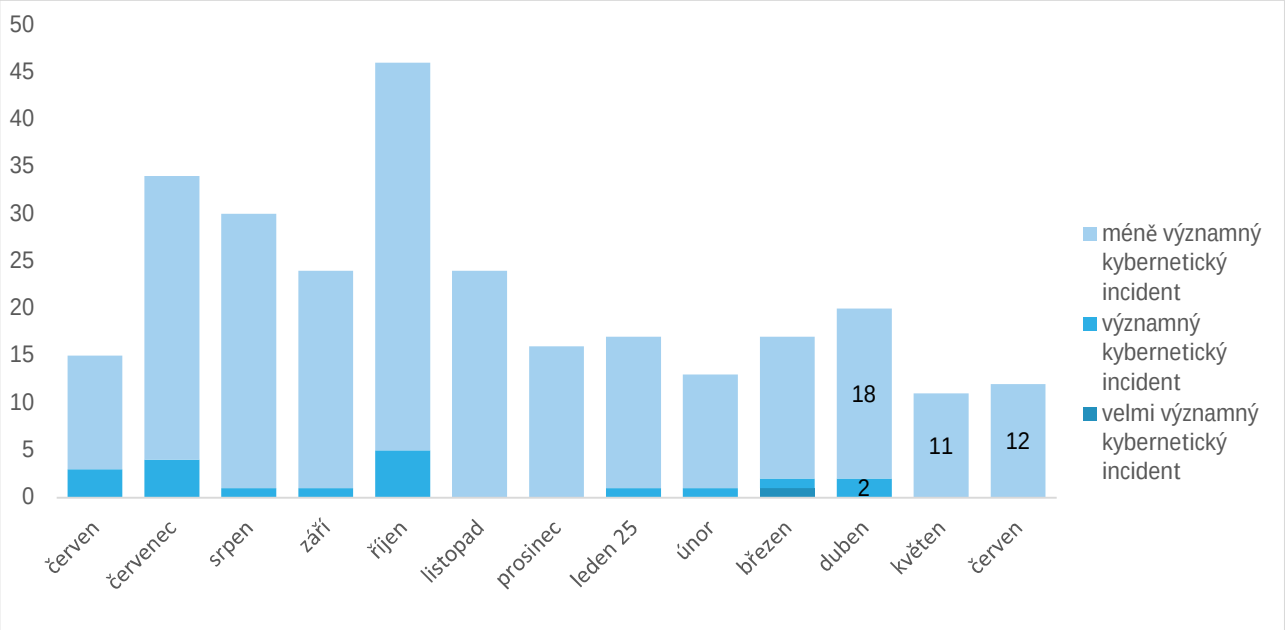
Stejně jako minulé čtvrtletí se aktuální přehled věnuje shrnutí zpráv a událostí v celosvětovém kontextu s přesahem na kybernetickou bezpečnost v tuzemsku. Zahrnují například aktivity ruských aktérů vůči evropským zemím či významný ransomwarový útok ve Spojeném království. Součástí přehledu je pak krátký výběr zpráv NÚKIB z oblasti spolupráce a sdílení informací v boji proti kybernetickým hrozbám.

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



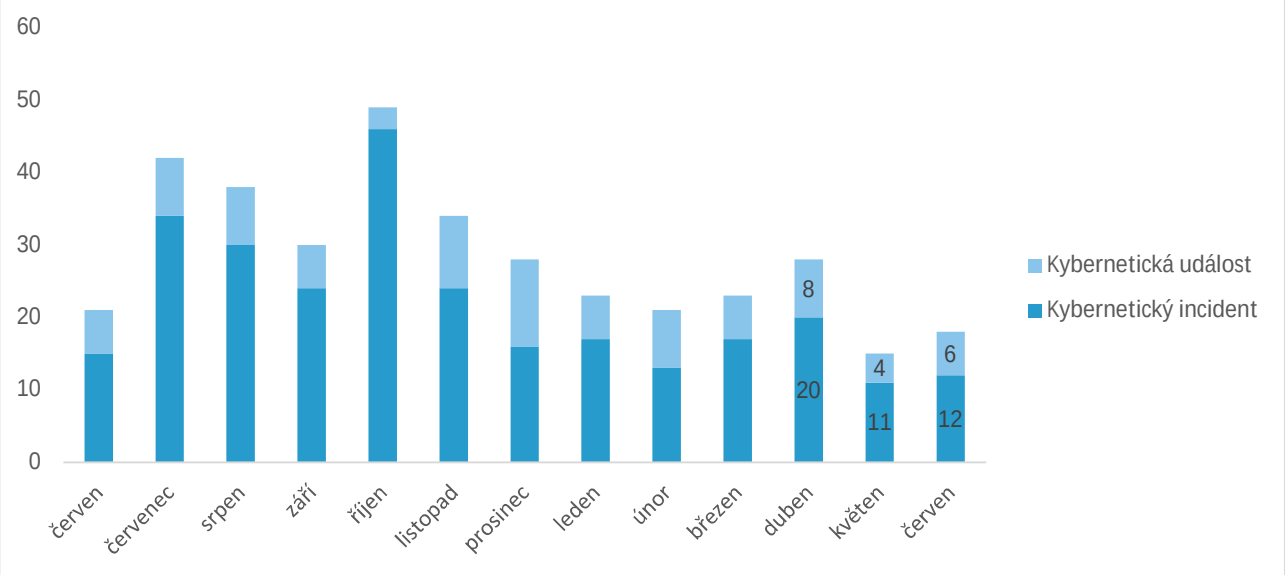
[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

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

Česká vláda atribuovala kybernetický útok na MZV ČR skupině APT31 napojené na čínskou zpravodajskou službu

Vláda České republiky 28. května 2025 na základě národního atribučního procesu označila ČLR zodpovědnou za škodlivou kybernetickou kampaň proti jedné z neutajovaných komunikačních sítí Ministerstva zahraničních věcí ČR. Závěry analýzy provedené NÚKIB, Vojenským zpravodajstvím (VZ), Bezpečnostní informační službou (BIS) a Úřadem pro zahraniční styky a informace jednoznačně ukazují, že za touto dlouhodobou škodlivou kampaní trvající od roku 2022 stojí ČLR a velmi pravděpodobně skupina APT31 (známá též jako Zirconium nebo Judgment Panda), která je spojována s celou řadou útoků proti politickým a jiným cílům, mj. v EU či NATO. Česká vláda jednoznačně odsoudila tuto škodlivou kybernetickou kampaň proti své kritické infrastruktuře a vyzvala ČLR, aby dodržovala zásady a principy odpovědného chování států v kybernetickém prostoru, které podpořily všechny státy OSN. V souvislosti s kybernetickým útokem proti ČR vyjádřila EU a její členské státy, stejně jako všichni spojenci v NATO solidaritu a podporu.

Bezpečnostní instituce zapojené do atribuce útoku APT31

Přisouzení kybernetického útoku s dostatečnou mírou jistoty za účelem provedení veřejné atribuce sofistikovanému kybernetickému aktérovi je totiž velmi náročné a vyžaduje značné schopnosti, úsilí a kapacity. Zejména díky spolupráci českých bezpečnostních institucí však bylo možné s dostatečnou mírou jistoty určit původce útoku. V současnosti je napadená síť odstavena od internetu, jelikož Ministerstvo zahraničí již v červenci 2024 nasadilo nový komunikační systém.

NÚKIB a české zpravodajské služby spolu s NSA a FBI upozorňují na ruskou kybernetickou kampaň proti subjektům podporujícím Ukrajinu

NÚKIB se připojil spolu s BIS, VZ a partnery ze Spojených států, Spojeného království, Německa, Polska, Austrálie, Kanady, Dánska, Estonska, Francie a Nizozemska k upozornění na dlouhodobou kybernetickou kampaň ruského aktéra APT28 (též Fancy Bear či Forest Blizzard) tamní vojenské rozvědky GRU. Kampaň cílila zejména na logistické a technologické firmy zapojené do zahraniční pomoci Ukrajině, ale dotkla se i státních institucí jednotlivých států či IP kamer na hraničních přechodech nebo železničních uzlech na Ukrajině a v přilehlých státech. Během kampaně APT28 využívala různé taktiky, od phishingu a slovníkových útoků po zneužívání zranitelností v softwaru, jako je Outlook či WinRAR.

Mapa zacílených států skupinou APT28, která je součástí společného upozornění

Upozornění, na kterém se spolupodílela řada západních bezpečnostních institucí, podtrhuje význam mezinárodní spolupráce při analýze kybernetických hrozeb, jelikož právě zapojení tolika aktérů umožnilo popsat aktivity APT28 v patřičné hloubce. Část zmiňovaných aktivit APT28 byla rozkryta například již v rámci české národní atribuce z června 2024. V průběhu května vydala analýzu týkající se činnosti skupiny APT28 také např. společnost ESET.

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.

APT29 pokračuje v kyberšpionážních operacích zaměřených vůči cílům v Evropě

Kyberbezpečnostní společnost CheckPoint zveřejnila analýzu nové vlny kampaně ruského státního aktéra APT29 (podléhající Službě vnější rozvědky, SVR). Kampaň je podle analýzy další iterací dlouhodobých snah APT29 kompromitovat diplomatické cíle v Evropě, zejména ministerstva zahraničních věcí a zastupitelské úřady. Prvotním vektorem zůstává spear-phishing s diplomatickou tematikou. Cílem APT29 se pravděpodobně stala i výzkumná instituce s názvem Německá společnost pro východoevropská studia (Deutsche Gesellschaft für Osteuropakunde, DGO). Ta formou veřejného prohlášení oznámila, že se stala cílem kybernetického útoku ze strany Ruské federace. Podle informací tamních médií německé zpravodajské služby vyšetřující tento případ identifikovaly jako útočníka právě APT29.

Ruský aktér COLDRIVER cílí na západní poradce, novináře a nevládní organizace skrze nový malware LOSTKEYS

Výzkumníci z Google Threat Intelligence Group (GTIG) identifikovali nový malware LOSTKEYS, který je připisován ruské státem sponzorované skupině COLDRIVER (známé též jako Star Blizzard či Callisto). GTIG, která mezi lednem a dubnem 2025 zaznamenala několikeré využití tohoto malwaru, rovněž uvedla, že skupina v nedávné době cílila primárně na současné a bývalé poradce západních vlád a armád, novináře a nevládní organizace. Nově objevený malware LOSTKEYS má být schopen sběru systémových informací, seznamu běžících procesů a odcizení souborů z přesně definovaných umístění a formátů. Distribuován je pomocí techniky sociálního inženýrství tzv. „ClickFix“, která spočívá v navedení oběti na zkopírování a spuštění útočníkova škodlivého příkazu. Útočníci pro tento účel využívají webové stránky obsahující falešnou CAPTCHA, po jejímž ověření se objeví instrukce.

Příklad instrukce navádějící oběť ke spuštění škodlivého příkazu

Nizozemské zpravodajské služby a společnost Microsoft odhalily nového ruského státního aktéra hrozeb

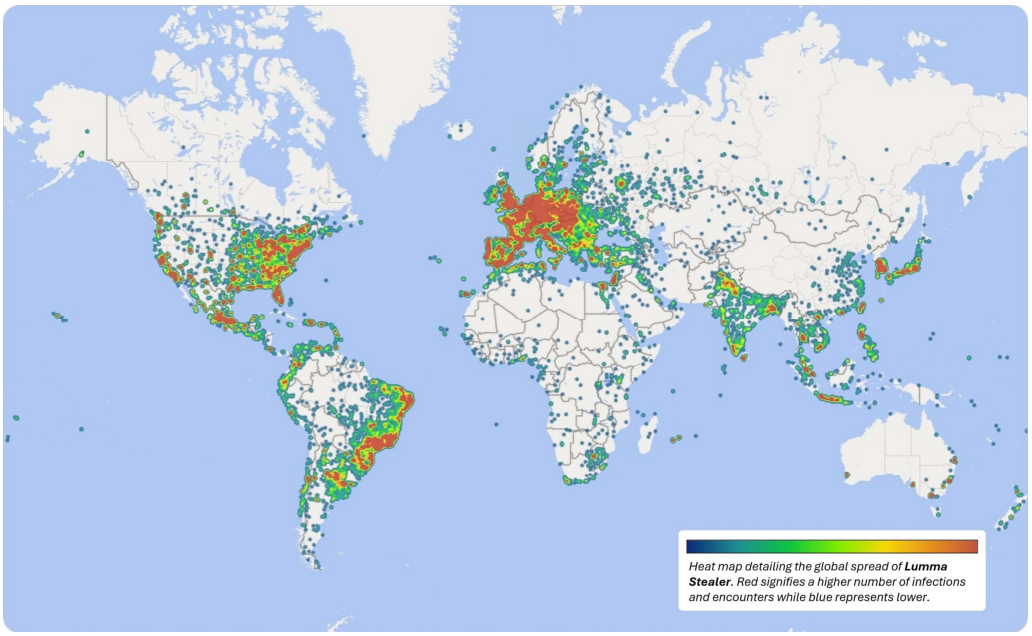
Společné vyšetřování nizozemských zpravodajských služeb AIVD, MIVD a společnosti Microsoft odhalilo nového ruského státního aktéra pojmenovaného Void Blizzard (též Laundry Bear). Ten má od dubna 2024 provádět kyberšpionážní operace s primárním zaměřením na organizace důležité pro strategické cíle Ruské federace, zejména v Evropě a Severní Americe. Mezi cíle patří subjekty

z oblasti vládních institucí, obrany, dopravy, médií, nevládních organizací a zdravotnictví. Významná část kompromitovaných subjektů se nachází v členských státech NATO a na Ukrajině. Void Blizzard získává přístup do systémů obětí a zaměřuje se ve výrazné míře na cloudová prostředí pomocí ukradených přihlašovacích údajů, které jsou pravděpodobně získány přes infostealery a online tržiště. Od dubna 2025 však skupina přešla k cílenému spear-phishingu využívajícímu techniku adversary-in-the-middle (AitM) s cílem krádeže přihlašovacích údajů.

Mezinárodní operace bezpečnostních složek a komerčních společností zasáhla proti infrastruktuře malwaru Lumma Stealer

Společnost Microsoft spolu s řadou bezpečnostních institucí a kyberbezpečnostních společností podnikla globální operaci vůči infrastruktuře malwaru Lumma Stealer. Operace zahrnující mimo jiné Europol a americké i japonské bezpečnostní služby spočívala v zablokování, zabavení či odstranění domén, které tvořily jádro jeho infrastruktury. Americký Federální úřad pro vyšetřování (FBI) od září 2023 zaznamenal zhruba 10 milionů kompromitací tímto malwarem. Dle mapy sdílené společností Microsoft se řada obětí nacházela také v České republice. Lumma Stealer je malware určený ke krádeži citlivých informací a je nabízen jako služba (Malware-as-a-Service).

Mapa znázorňující globální rozšíření malwaru Lumma Stealer



Ransomwarový útok ve Spojeném království přímo souvisel s úmrtím pacienta

Britský národní zdravotnický systém (NHS) potvrdil, že loňský ransomwarový útok skupiny Qilin měl přímý dopad na poskytování zdravotní péče a přispěl ke smrti pacienta. Útok na společnost Synnovis, která poskytuje zdravotnické služby, jako jsou krevní testy pro transfuze, měl dopad na provoz řady britských nemocnic. Podle expertů z britského zdravotnictví bylo zdržení krevních testů v důsledku kybernetického útoku jedním z faktorů vedoucích k úmrtí pacienta. Mluvčí odmítl poskytnout další informace o ostatních faktorech z důvodu ochrany osobních údajů pacientů. Kromě ztráty na životě útok způsobil také akutní nedostatek krve, kdy byly nemocnice nuceny využívat univerzální dárce a omezovat transfuze. Celkem měl útok ovlivnit více než 900 000 osob, jejichž citlivá zdravotní data byla útočníky zveřejněna.

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 uspořádal kybernetické cvičení pro spojence NATO

V průběhu dubna 2025 uspořádal NÚKIB cvičení zaměřené na schopnost podpory při kybernetických incidentech na dálku (VCISC – *Virtual Cyber Incident Support Capability*). Cílem bylo prověřit připravenost spojenců poskytovat si vzájemnou pomoc v kyberprostoru prostřednictvím mechanismu VCISC v případě vážných kybernetických incidentů. VCISC je mechanismus, jenž umožňuje spojencům v NATO čelícím rozsáhlé škodlivé kybernetické aktivitě požádat ostatní členy aliance o vzdálenou pomoc. Cvičení poskytlo příležitost ověřit národní postupy v rámci VCISC i celkovou schopnost NATO spolupracovat v případě více rozsáhlých incidentů.

Ředitel NÚKIB Lukáš Kintr jednal v USA o pokračování spolupráce v kybernetické bezpečnosti s administrativou prezidenta Trumpa

Ředitel NÚKIB Lukáš Kintr a ředitel kabinetu Roman Pačka absolvovali v květnu pracovní cestu do Spojených států amerických, kde jednali o spolupráci v kybernetické bezpečnosti. Delegace NÚKIB absolvovala sérii jednání se zástupci amerických bezpečnostních institucí, včetně Národní bezpečnostní rady Bílého domu nebo Zvláštní komise pro strategické soupeření mezi USA a Čínou při Sněmovně reprezentantů. Mezi klíčová diskutovaná témata patřily zejména hrozby proti kritické infrastruktuře ze strany státem sponzorovaných aktérů, včetně kampaní Volt Typhoon a Salt Typhoon, využívání důvěryhodných a bezpečných technologií nebo dopady rychle se vyvíjející umělé inteligence na kybernetickou bezpečnost. Dále se diskuze dotkla také témat spojených s kybernetickou ochranou energetické infrastruktury nebo kyberbezpečnosti připojených vozidel. Ve všech případech se jedná o důležitá témata, která rezonují na obou stranách Atlantiku.

NÚKIB se zahraničními partnery spolupodepsal dokumenty zaměřené na platformy SIEM a SOAR

NÚKIB se připojil k mezinárodní iniciativě vedené Australským signálním zpravodajstvím (ASD) a spolupodepsal sérii dokumentů zaměřených na bezpečnostní platformy SIEM a SOAR.

„Jsem rád, že se NÚKIB mohl podílet na druhé sérii dokumentů spolupodepsaných pod vedením ASD zaměřených na platformy SIEM a SOAR – technologie, které jsou stále častěji využívány i v České republice. Doporučené principy odrážejí dlouhodobé bezpečnostní standardy, které náš úřad systematicky prosazuje. Je nezbytné, aby se organizace zavazovaly nejen k počátečním investicím do bezpečnostních technologií, ale také k trvalé podpoře lidí a procesů, které tyto systémy provozují. Řešení typu SIEM nebo SOAR, které nezpracovává relevantní data a není aktivně sledováno a laděno, pravděpodobně nebude schopné efektivně detekovat ani reagovat na hrozby," uvedl ředitel NÚKIB Lukáš Kintr.

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.