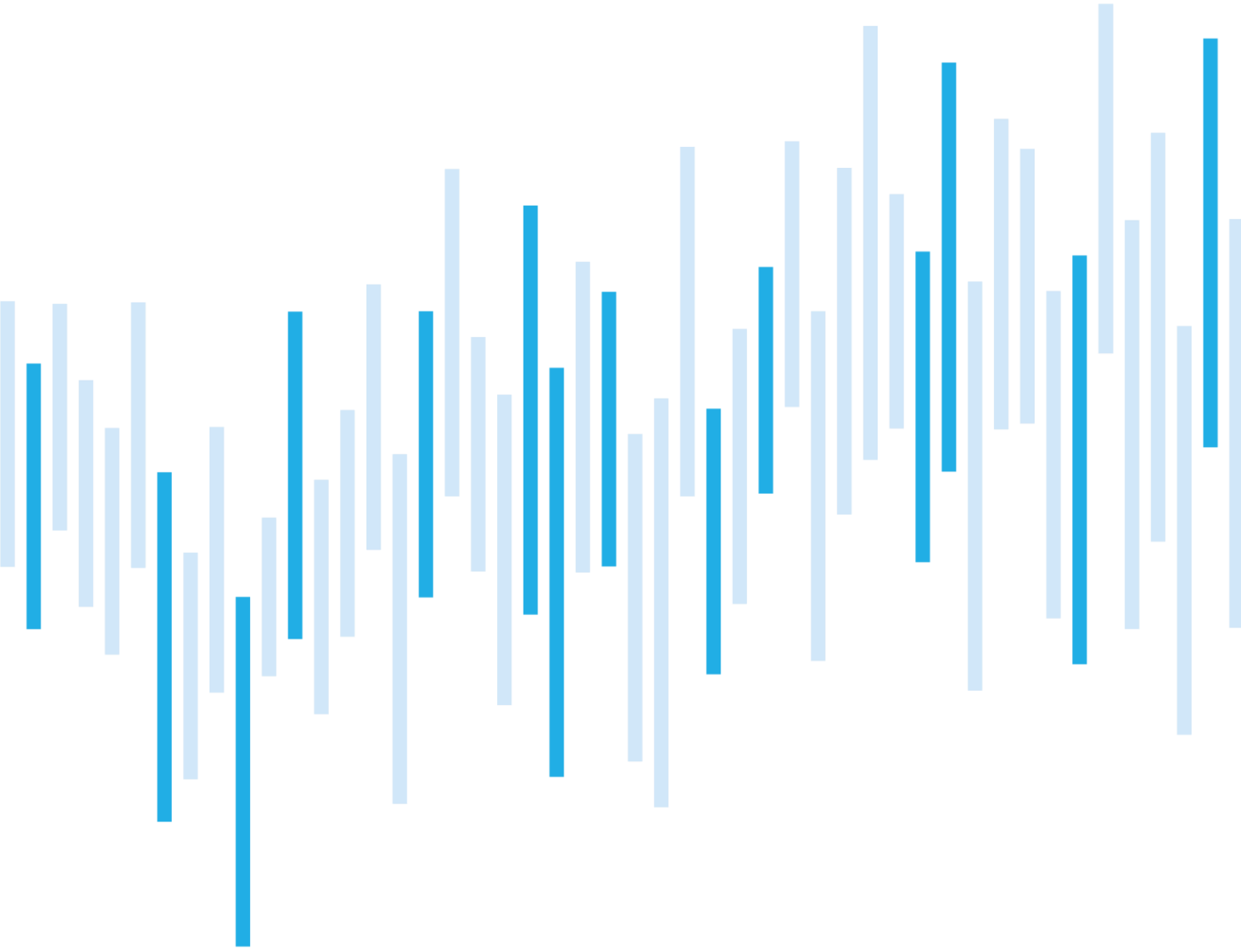
Kybernetické incidenty pohledem NÚKIB

KVĚTEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V květnu došlo k opětovnému růstu počtu evidovaných kybernetických incidentů na celkový počet 14. Stále je však výsledná hodnota pod dlouhodobým průměrem.

Evidované incidenty byly během května poměrně rozmanité a zaznamenány tak byly téměř všechny jejich kategorie. Z pohledu dopadů byly nicméně všechny zařazeny do kategorie méně významných.

V kapitole Zaměřeno na událost se věnujeme politické atribuci kyberšpionážních operací ruské státem sponzorované skupiny APT28 (též Fancy Bear či Forest Blizzard). Přisouzení provedla Česká republika a Německo počátkem května, spolu s podporou EU, NATO a Spojených států, Spojeného království a Francie. Prohlášení se týkalo dlouhodobých škodlivých aktivit skupiny vůči strategickým institucím vládního sektoru, ale i konkrétně její poslední kampaně zneužívající zranitelnost ve službě Microsoft Outlook pro získávání citlivých informací.

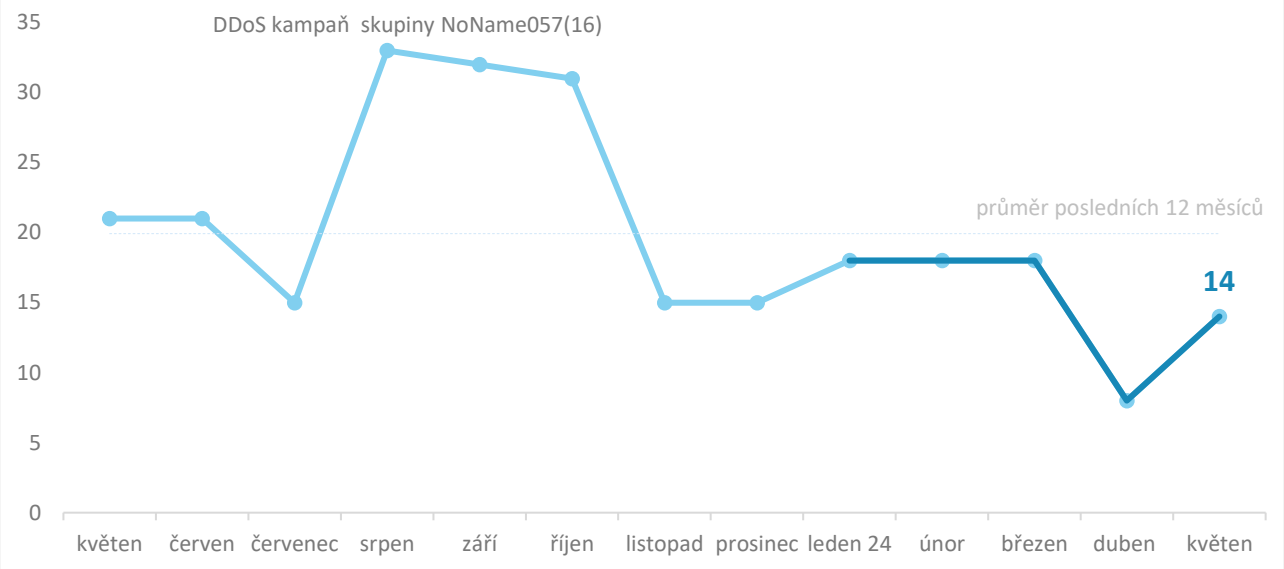
Obsah

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

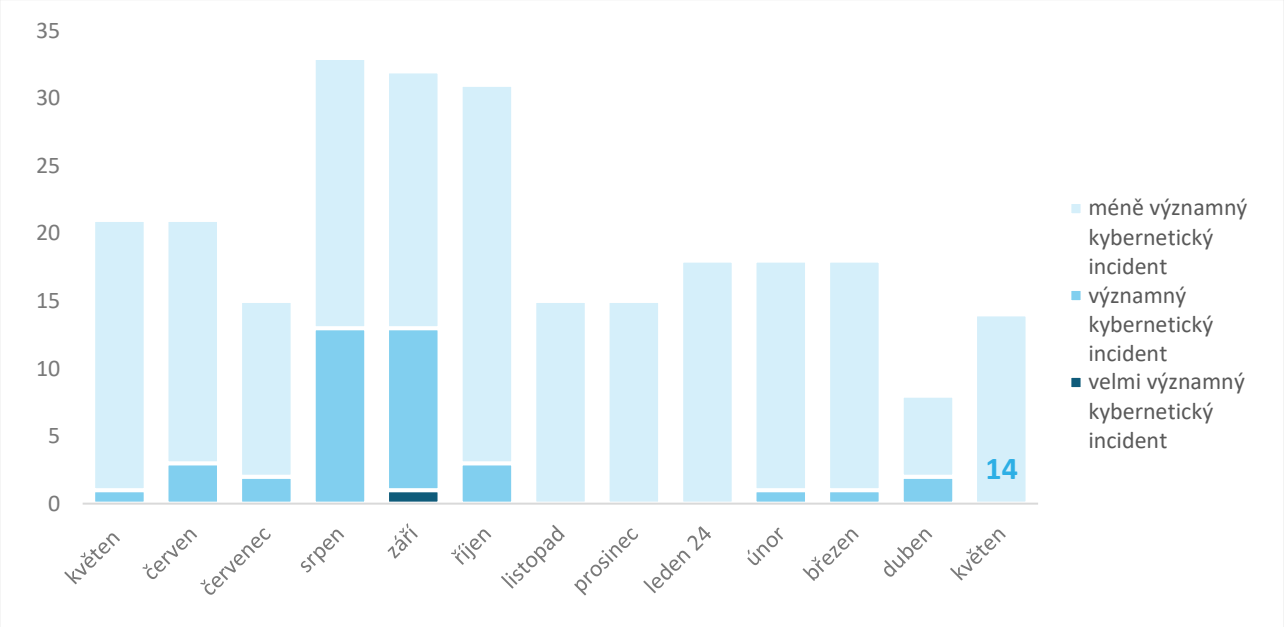
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Během května bylo evidováno celkem 14 incidentů, což představuje postupný návrat k průměrným hodnotám z uplynulého roku. Stejně jako v dubnu NÚKIB neregistroval DDoS útoky, které historicky průměrný počet incidentů významně zvyšovaly.



Závažnost řešených kybernetických incidentů[1]

Všech 14 květnových kybernetických incidentů spadá do kategorie méně významných.



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

Klasifikace incidentů nahlášených NÚKIB[2]

V květnu byla evidována celá řada různých druhů incidentů. Od škodlivého kódu a výpadků dostupnosti služeb přes průniky a různé druhy podvodného jednání, včetně podvodných CEO e-mailů s cílem zisku finančních prostředků.

Specificky NÚKIB řešil incidenty v kategoriích Podvod, Informační bezpečnost, Dostupnost, Škodlivý kód a Průnik.

- Objevily se mj. dva ransomwarové útoky. Jeden z nich má na svědomí skupina RansomHub operující v režimu RaaS (Ransomware jako služba), druhý pak skupina Akira Ransomware.
- Dva incidenty v kategorii Dostupnost byly způsobeny technickou závadou na infrastruktuře.
- V kategorii Průnik a Podvod se vyskytly zejména úspěšné phishingové kampaně, které vedly buď k úniku přihlašovacích údajů či dalšímu rozesílání škodlivých zpráv. V jednom případě však došlo k úspěšnému přesměrování plateb klientů kompromitované společnosti na finanční konto útočníka, a tudíž i k finanční škodě.

[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Trendy v kybernetické bezpečnosti za květen pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v květnu evidoval čtyři případy incidentů, při kterých došlo k využití techniky phishingu. Ve všech případech však byly dopady incidentů nízké. Nicméně v jednom případě došlo v důsledku falešného CEO e-mailu k odeslání platby na účet útočníka. Podvod byl však obratem odhalen a platba stornována.

Malware

V květnu podobně jako v uplynulých měsících probíhaly kontinuální aktivity v oblasti malwarové analýzy v souvislosti s některými dříve evidovanými incidenty.

Zranitelnosti

Během května NÚKIB nevydal žádné upozornění týkající se zranitelností.

Ransomware

V květnu byly evidovány dva případy incidentů spojených s ransomwarem. Jeden z nich má na svědomí skupina RansomHub operující v režimu RaaS (Ransomware jako služba), za druhý incident je pak zodpovědná skupina Akira Ransomware.

Útoky na dostupnost

V průběhu května NÚKIB evidoval dva incidenty v kategorii Dostupnost, které však byly způsobeny technickou závadou. V jednom případě se výpadek služeb týkal dvou systémů kritické informační infrastruktury.

[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

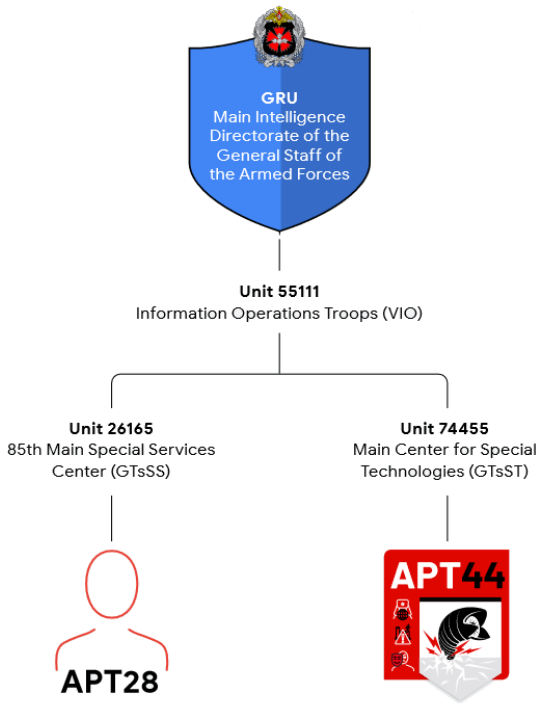
Zaměřeno na událost: Atribuce škodlivých aktivit v kyberprostoru Ruské federaci

V pátek 3. května 2024 došlo k přisouzení škodlivých aktivit v kyberprostoru (tzv. atribuci) Ruské federaci. Konkrétně se jednalo o atribuci kyberšpionážních útoků ruské státem sponzorované skupině APT28 (též známé jako Fancy Bear či Forest Blizzard), která podléhá ruské vojenské rozvědce GRU. **APT28 se dlouhodobě zaměřuje na vládní sektor západních zemí, včetně České republiky.** I díky tomu podobnou atribuci provedlo souběžně s Českem i Německo, přičemž obě veřejná prohlášení byla doprovázena vyjádřením podpory Evropskou unií, Severoatlantickou aliancí, ale i na národní úrovni Spojenými státy, Spojeným královstvím a Francií.

Mezi hlavní atribuované útoky patří zneužívání zranitelnosti CVE-2023-23397 v e-mailové aplikaci Outlook či provádění útoků skrze síť kompromitovaných routerů Ubiquity. Vůči této síti byl v únoru proveden zásah s názvem operace Dying Ember, na němž se podílelo i české Vojenské zpravodajství.

APT28 je jednou ze dvou známých jednotek podléhajících GRU, přičemž tou druhou je APT44 (též známá jako Sandworm). APT28 se zaměřuje primárně na dlouhodobé kyberšpionážní operace, přičemž mezi ty významnější se řadí například vměšování do amerických prezidentských voleb v roce 2016 či francouzských prezidentských voleb v roce 2017. **Vysoké procento současné aktivity skupiny se potom v posledních dvou letech soustřeďuje zejména vůči Ukrajině v kontextu tamního konfliktu.**

Obr. 1: Diagram předpokládané struktury kybernetických jednotek GRU dle společnosti Mandiant



Zdroj: services.google.com

Politická atribuce kybernetických útoků je významným nástrojem států, jak odradit útočníky od dalších škodlivých aktivit, ale i poukázat na svoji schopnost detekce a vůli přisoudit takové aktivity konkrétním útočníkům. Může také sloužit jako základ případným odvetným krokům či demonstrace jednoty.

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 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.