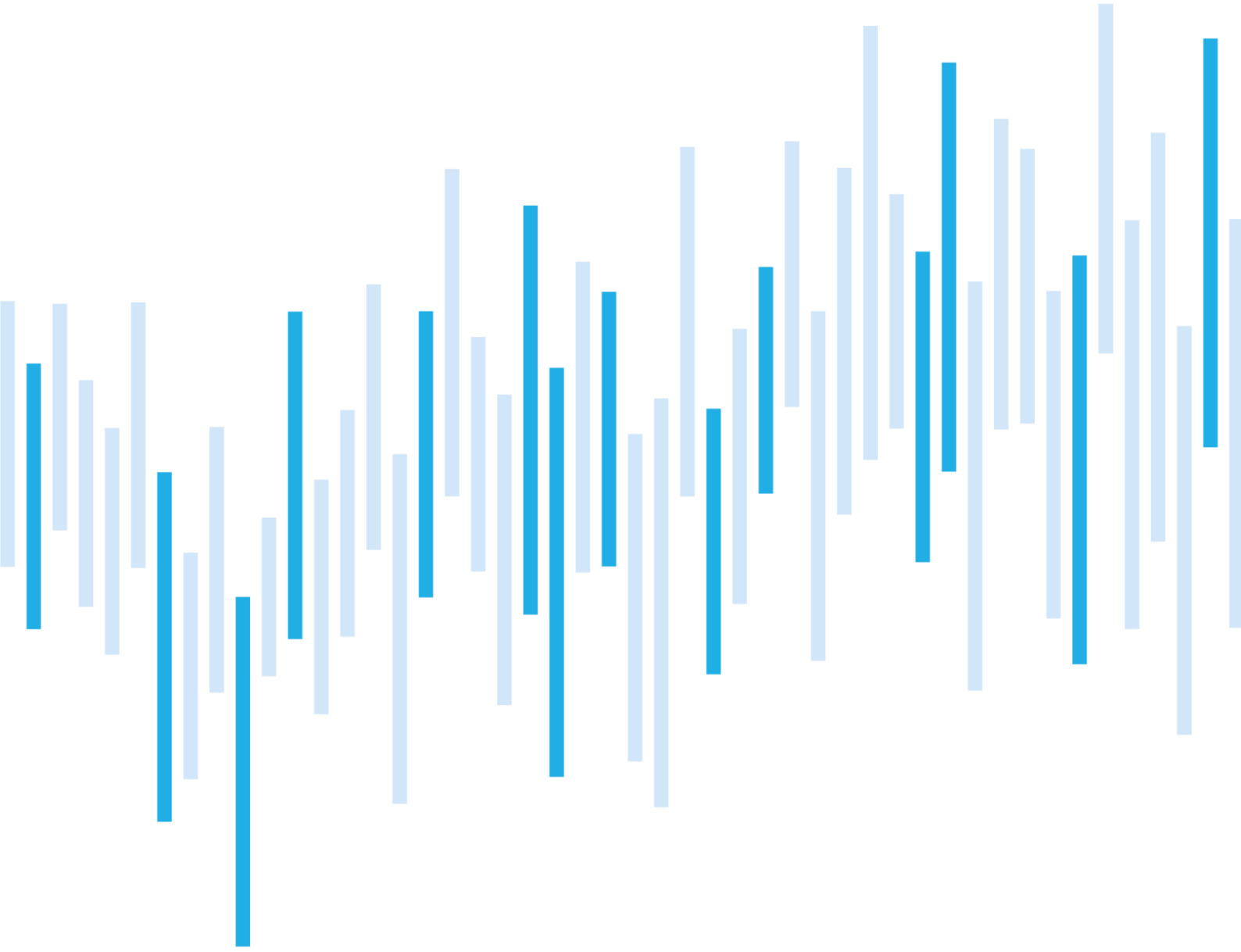
Kybernetické incidenty pohledem NÚKIB

LEDEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

NÚKIB v lednu 2023 evidoval více než dvojnásobný nárůst kybernetických incidentů oproti předchozímu měsíci. Drtivá většina z nich však z pohledu závažnosti spadala mezi méně významné, což je dáno především vysokým počtem zaznamenaných DDoS útoků, které zpravidla nemají významnější dopady. Významné incidenty byly registrovány pouze dva, zatímco velmi významné incidenty absentovaly.

V lednu výrazně převažovaly incidenty u povinných osob dle ZKB, přičemž převážná většina zasažených subjektů spadá do sektoru veřejné správy. Nejpočetnějším typem incidentu se staly útoky na dostupnost, v rámci kterých převažovaly DDoS útoky na webové stránky obětí.

V návaznosti na nárůst zaznamenaných DDoS útoků se věnujeme technice T1498: Network Denial of Service s důrazem na možnosti mitigace. Za zvýšeným počtem DDoS útoků stála ruskojazyčná skupina NoName057(16), která v průběhu ledna zasáhla webové stránky více než desítky státních i soukromých subjektů. V závěrečné kapitole se proto zaměřujeme na tuto skupinu a její lednovou kampaň.

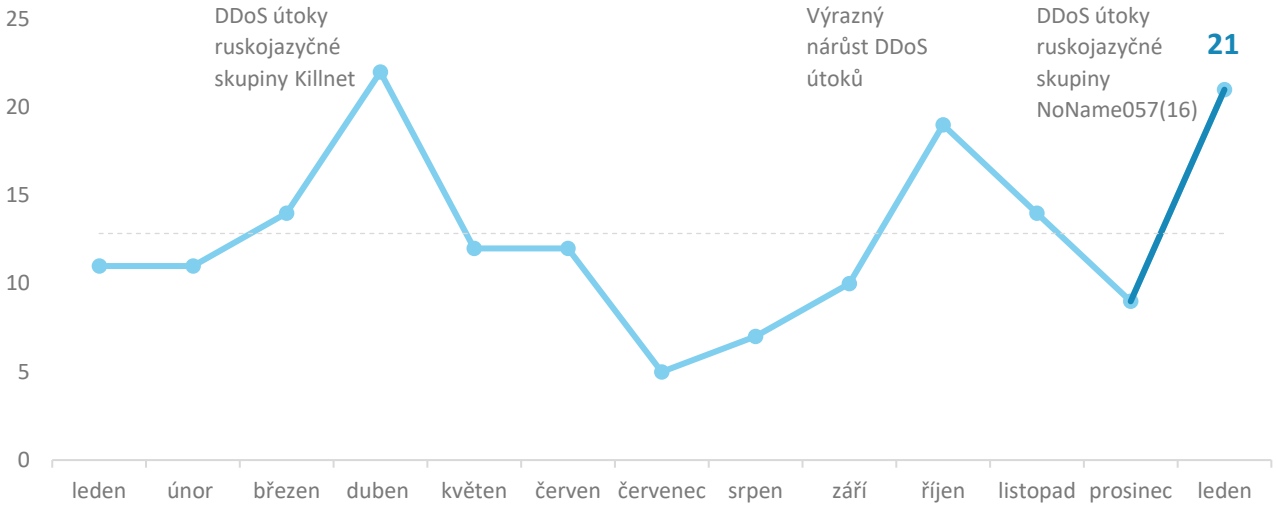
Obsah

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.cz

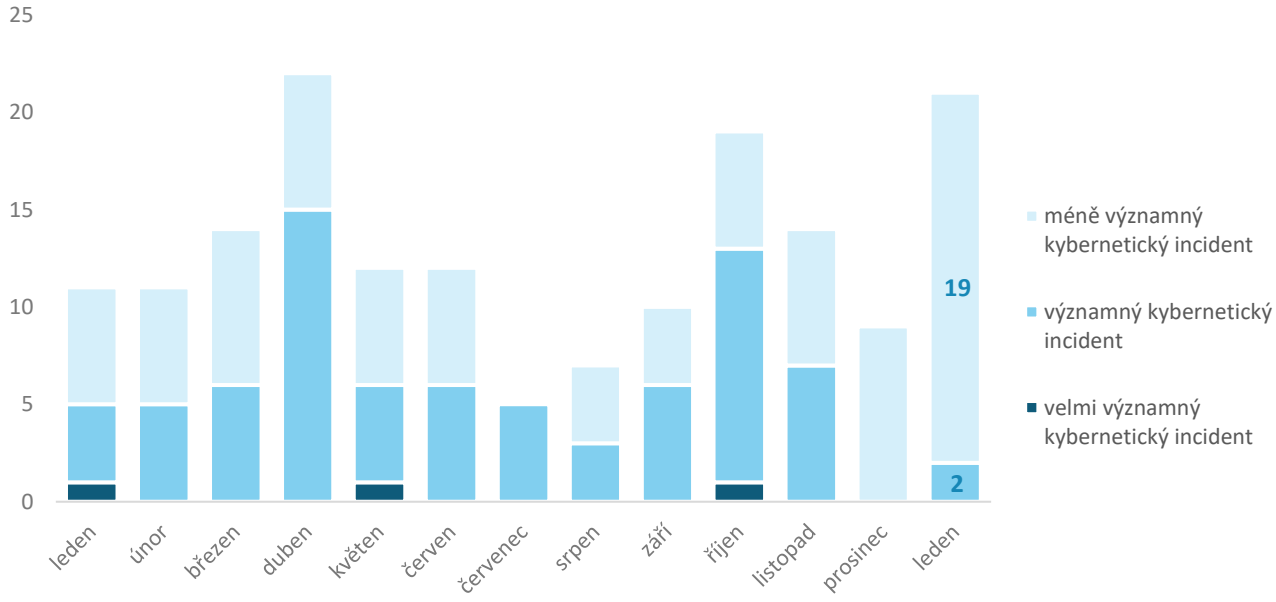
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V lednu NÚKIB zaznamenal více jak dvojnásobný nárůst počtu kybernetických bezpečnostních incidentů oproti předchozímu měsíci. Již první měsíc roku 2023 tak téměř dosáhl loňského maxima, jež činilo 22 incidentů za měsíc. [1]



Závažnost řešených kybernetických incidentů[2]

Navzdory vysokému počtu evidovaných kybernetických incidentů spadala drtivá většina z nich do kategorie méně významných incidentů, což je dáno především vysokým počtem DDoS útoků, které zpravidla nemají významnější dopady. Významné incidenty byly registrovány pouze dva. Podobně jako v předchozích dvou měsících, i v lednu pokračovala absence zaznamenaných velmi významných incidentů.

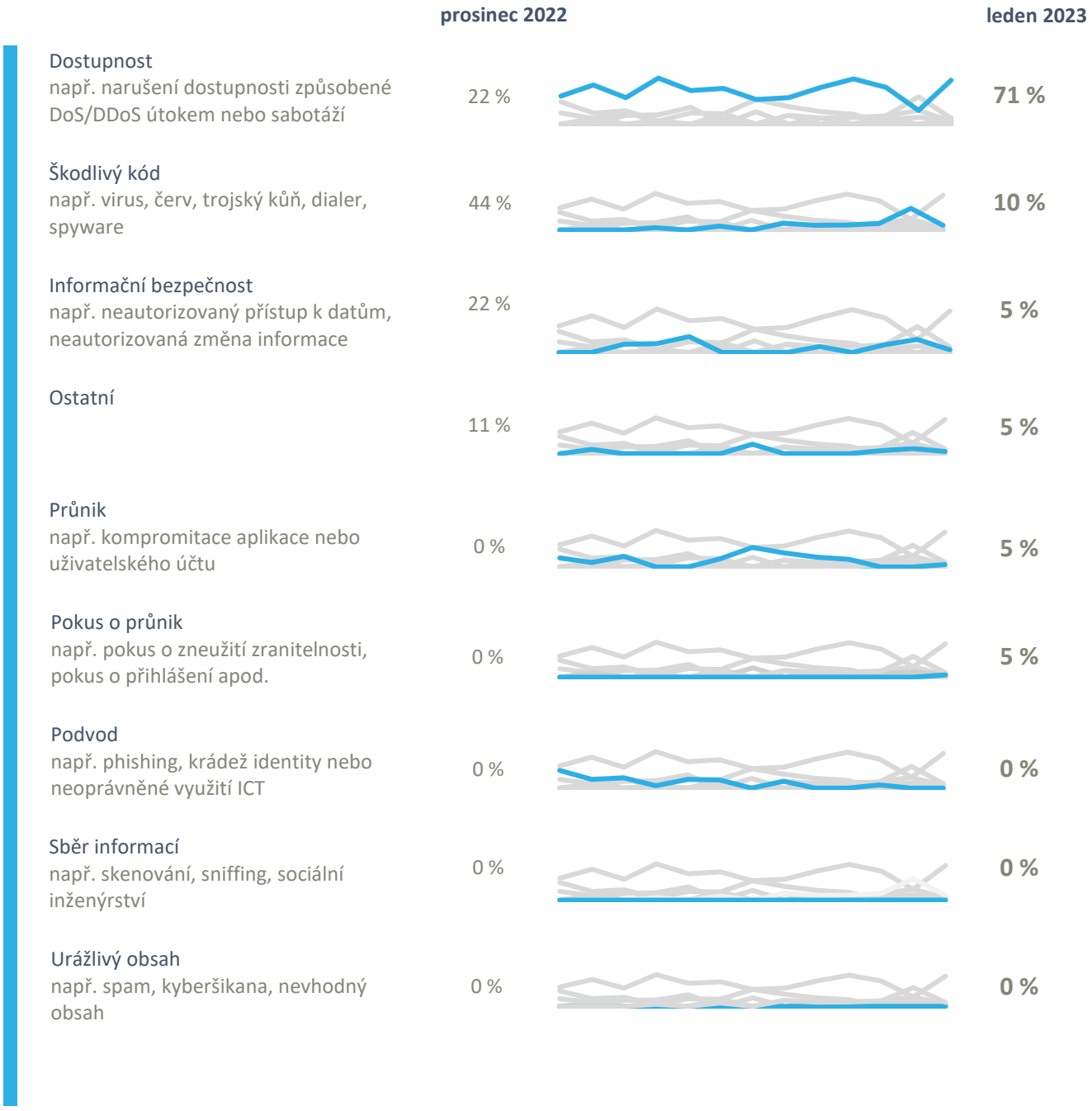


[1] Celkem 17 incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 4 incidenty se týkaly neregulovaných subjektů.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Lednové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Nejčastěji evidovaným typem incidentu byly útoky na dostupnost, kde drtivou většinu tvořily DDoS útoky na webové stránky obětí. Zbylé incidenty byly způsobeny výpadky služeb.
- V kategorii škodlivý kód NÚKIB v lednu zaregistroval dva incidenty. V obou případech se jednalo o ransomwarové útoky.
- Lednové incidenty zahrnovaly také jeden průnik a jeden neúspěšný pokus o něj. Oba útoky přitom cílily na regulované subjekty.
- NÚKIB v lednu evidoval také po jednom incidentu v kategoriích informační bezpečnost a ostatní.



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

Trendy v kybernetické bezpečnosti za leden pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing a další techniky sociálního inženýrství jsou stálým trendem. V lednu byl zaregistrován úspěšný phishingový útok na státní instituci, v rámci kterého útočníci využili kompromitovaného účtu k rozeslání dalších phishingových e-mailů.

Malware

Mimo níže zmíněné případy ransomwaru NÚKIB v lednu neevidoval incidenty zahrnující využití malwaru. Probíhaly nicméně kontinuální aktivity v oblasti malwarové analýzy v návaznosti na prosincové incidenty.

Zranitelnosti

NÚKIB během ledna nevydal upozornění na nové zranitelnosti, ani nedetekoval výraznější zneužívaní konkrétních dosud známých zranitelností.

Ransomware

NÚKIB v lednu evidoval dva ransomwarové útoky. Opět byl zaznamenán výskyt ransomwaru PLAY a nově pak ransomwaru Dark Power. Oba útoky mířily na neregulované subjekty.

Ačkoli je PLAY poměrně novým ransomwarem, od začátku června 2022 úspěšně napadl řadu významných obětí po celém světě. Podle některých výzkumníků za touto operací stojí stejní aktéři jako za ransomware Hive a Nokoyama. Ransomware Dark Power je rovněž velmi nový, nicméně dosud není příliš rozšířený.

Útoky na dostupnost

Po měsíční odmlce došlo opět k významnému nárůstu DDoS útoků. Za tímto nárůstem stála kampaň ruskojazyčné skupiny NoName057(16). Podobně jako v případě jiných zaznamenaných DDoS kampaní byly následky útoků pouze dočasné a neměly závažnější dopady.

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

Technika měsíce: Network Denial of Service

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V rámci reportu se zaměřujeme na techniku T1498: Network Denial of Service. Ačkoli jsme se v našich veřejných reportech této technice v minulosti věnovali, v návaznosti na nárůst zaznamenaných DDoS útoků ji zařazujeme znovu s důrazem na možnosti mitigace.

MITRE ID: T1498

Útočníci mohou provádět útoky Network Denial of Service (DoS) za účelem snížení nebo zablokování dostupnosti. Daný typ útoků pak lze provést vyčerpáním šířky pásma sítě, na něž se služby spoléhají. Může se jednat o webové stránky, e-mailové služby, DNS či tzv. web-based aplikace. K tomuto typu útoku dochází, když útočníci „zahltí“ šířku pásma síťového připojení svým škodlivým provozem. Ten může generovat jeden systém (Denial of Service, DoS) nebo mnoho systémů (Distributed Denial Service, DDoS). Tento typ úroku vede k omezení dostupnosti dat a obvykle nemá dlouhodobější dopady.

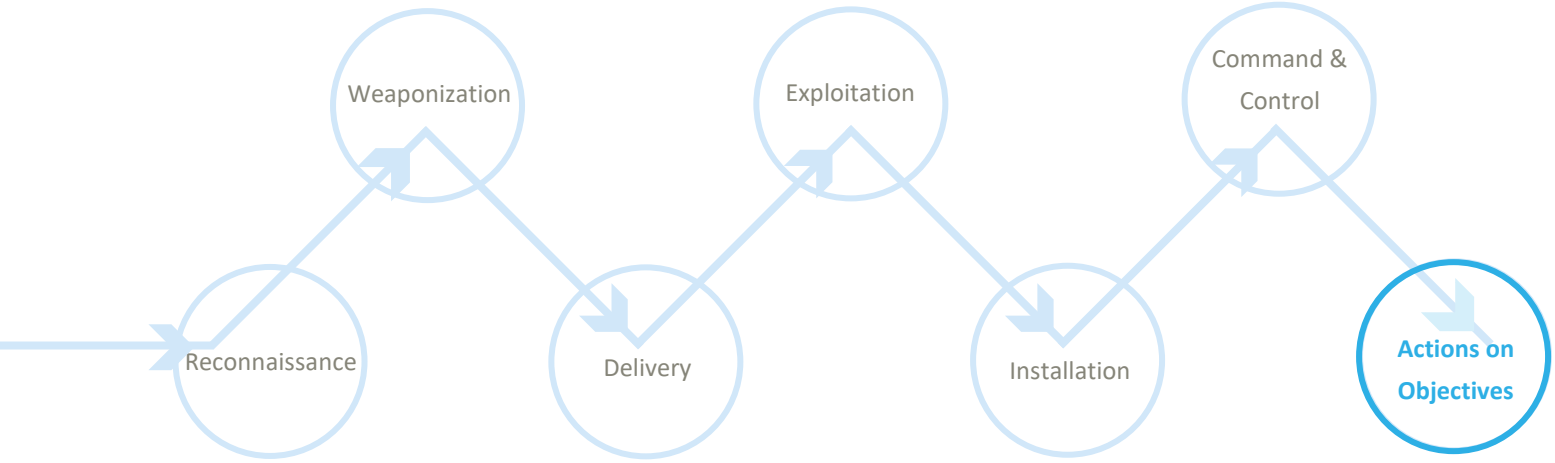
Mitigace: Klíčovou mitigační technikou je filtrování síťového provozu. Obrana proti DDoS útokům je nicméně do jisté míry závislá na tom, o jaký typ útoku se jedná. Níže uvádíme některé příklady typů útoků a potenciálních mitigačních opatření:

Například vůči útoku typu HTTP flood vedenému ze zahraniční je možné využít tzv. geoblocking neboli omezení přístupu na základě geografické lokace. Dalším operativním řešením může být zablokování vybraného ASN, tzn. celé skupiny IP rozsahů. Pokročilejší možnosti mitigace zahrnují monitoring provozu v reálném čase a dynamické upravování pravidel.

Pří útocích typu TCP flood je možné dočasně navýšit kapacity skrze navýšení tzv. backlog queue či „recyklace“ starších polootevřených spojení.

Obrana vůči tzv. DNS amplification zahrnuje především ověřování a filtrování zdrojových adres a omezování doby odezvy či počtu dotazů. Tato odpovědnost však leží na samotných provozovatelích DNS serverů a samotná oběť tak má pouze omezené možnosti mitigace.

Znázornění techniky T1498 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na hrozbu: DDoS kampaň skupiny NoName057(16)

Ruskojazyčná hackerská skupina NoName057(16) provedla v průběhu ledna sérii DDoS útoků, které mířily na webové stránky více než desítky státních i soukromých subjektů.

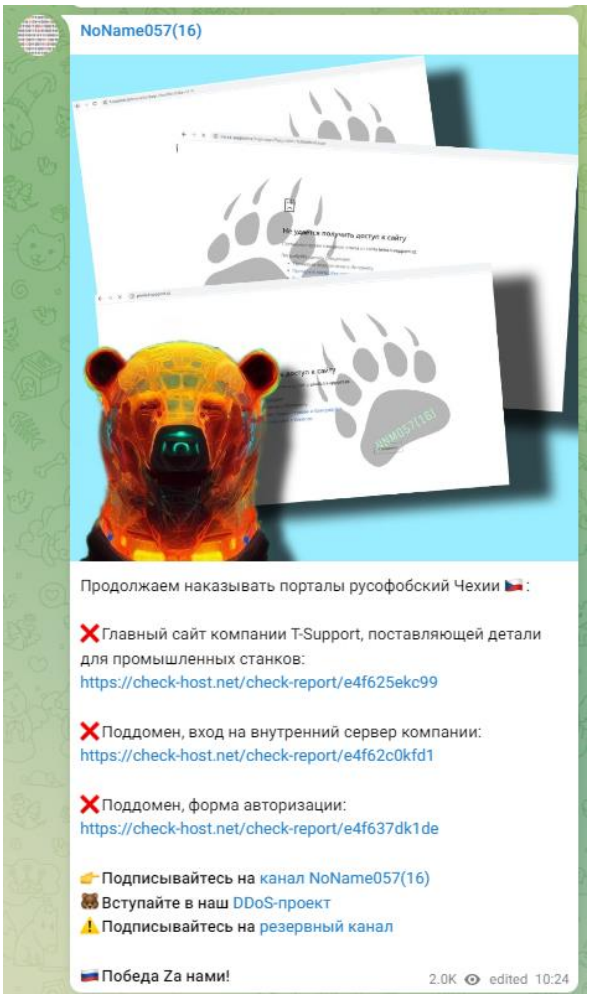
Poprvé byla tato skupina zaznamenána v březnu 2022, tedy krátce po začátku války na Ukrajině. Zpočátku se NoName057(16) zaměřovala na ukrajinské cíle, nicméně později začala cílit na subjekty napříč sektory v zemích NATO. V nedávné době se skupina zaměřila například na cíle v Rakousku, Itálii, Velké Británii, Litvě, Polsku či Dánsku. Od 11. ledna byly zaznamenány útoky skupiny na cíle v ČR.

NoName057(16) na svém telegramovém účtu zveřejňuje příspěvky podporující Rusko a odsuzuje rusofobní nepřátele, jak označuje i některé své cíle. Této orientaci odpovídá také výběr cílů, který má v řadě případů zřetelnou politickou motivaci. Skupina provádí primárně DDoS útoky na vybrané webové stránky, zejména na cíle v zemích NATO.

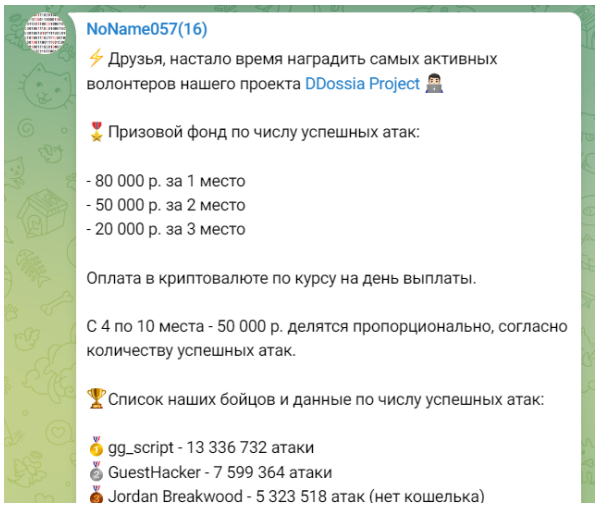
Zaznamenané útoky neměly závažnější dopady a vedly pouze k dočasné nedostupnosti webových stránek napadených subjektů. DDoS útoky obecně zahlcují provoz na službách přístupných z internetu, informační systémy organizací ale nekompromitsují.

NoName057(16) se v určitém ohledu liší od ruskojazyčných skupin jako Killnet či Anonymous Russia. Specifická je zejména svým projektem DDosia, skrze který nabízí zájemcům peněžní odměny za provedení co nejvíce úspěšných útoků DDoS. Projekt DDosia tvoří komunita dobrovolníků, kterým NoName057(16) nabízí nástroj DDosia, skrze nějž poté provádí DDoS útoky. Nejproduktivnější členové pak získávají finanční odměny v kryptoměnách (viz Obr. 2).

Obr 1: Telegramový příspěvek skupiny NoName057(16)



Obr 2: Telegramový příspěvek skupiny NoName057(16) oznamující pořadí nejproduktivnějších útočníků



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	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.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	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
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.