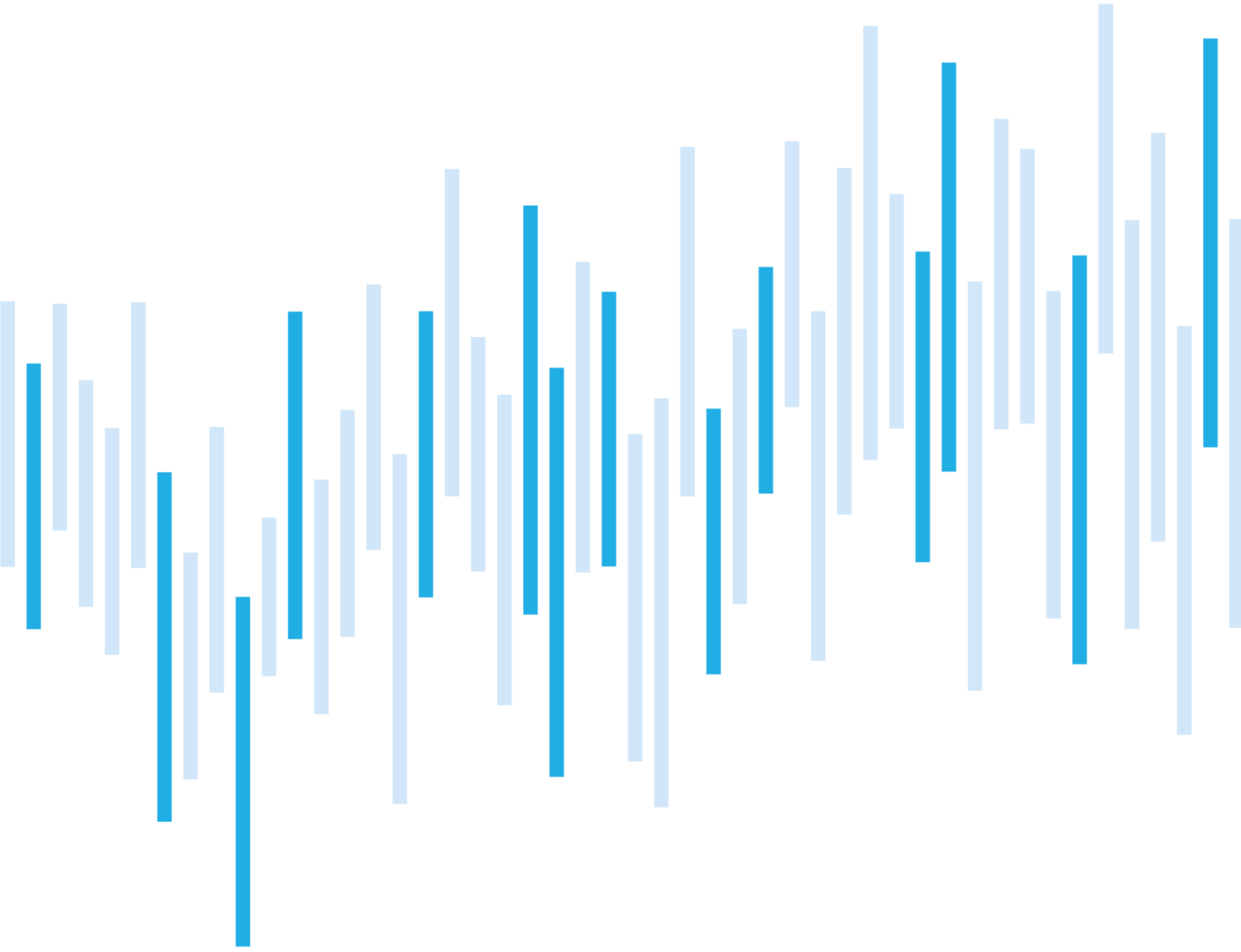
Kybernetické incidenty pohledem NÚKIB

ŘÍJEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se v říjnu dostal vysoko nad průměr a jde o dosud nejvyšší hodnoty od letošního dubna (celkem 20 incidentů). Velký podíl na nárůstu mají DDoS útoky, jejichž počet dosahuje téměř souhrnných hodnot od začátku letošního roku. Část útoků typu DDoS byla vedena ze strany hacktivistické skupiny Anonymous Russia, která své útoky deklarovala na síti Telegram.

Poprvé od května došlo k incidentu, který byl klasifikován jako velmi významný. Jednalo se o útok na dostupnost telekomunikačních služeb. V říjnu jasně převažovaly incidenty, které hlásily povinné osoby dle ZKB. Nejčastější obětí byly subjekty z veřejné správy a sektoru dopravy, které se podílí na polovině všech incidentů.

Technikou měsíce jsou tentokrát Direct Network Flood (T1498.001) a Reflection Amplification (T1498.002). Tyto techniky jsou úzce spojeny s DDoS útoky, kterým subjekty v ČR ve zvýšené míře čelí. DDoS útoky a jejich zvýšené riziko jsou pak také trendem, na nějž jsme se tento měsíc zaměřili.

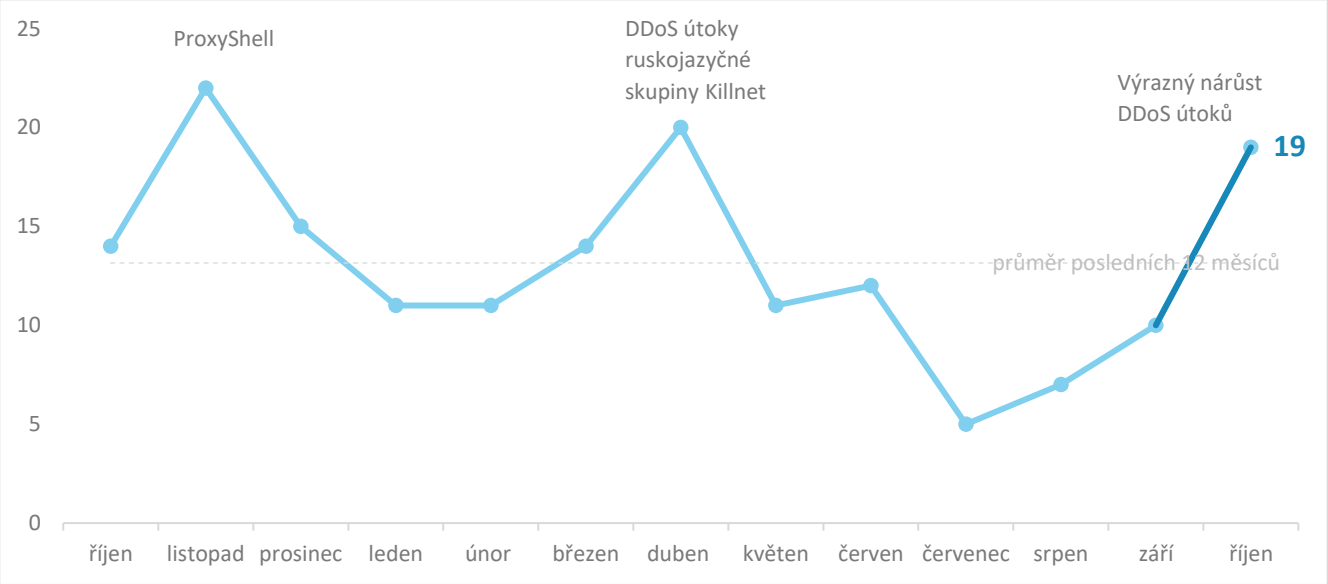
Obsah

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

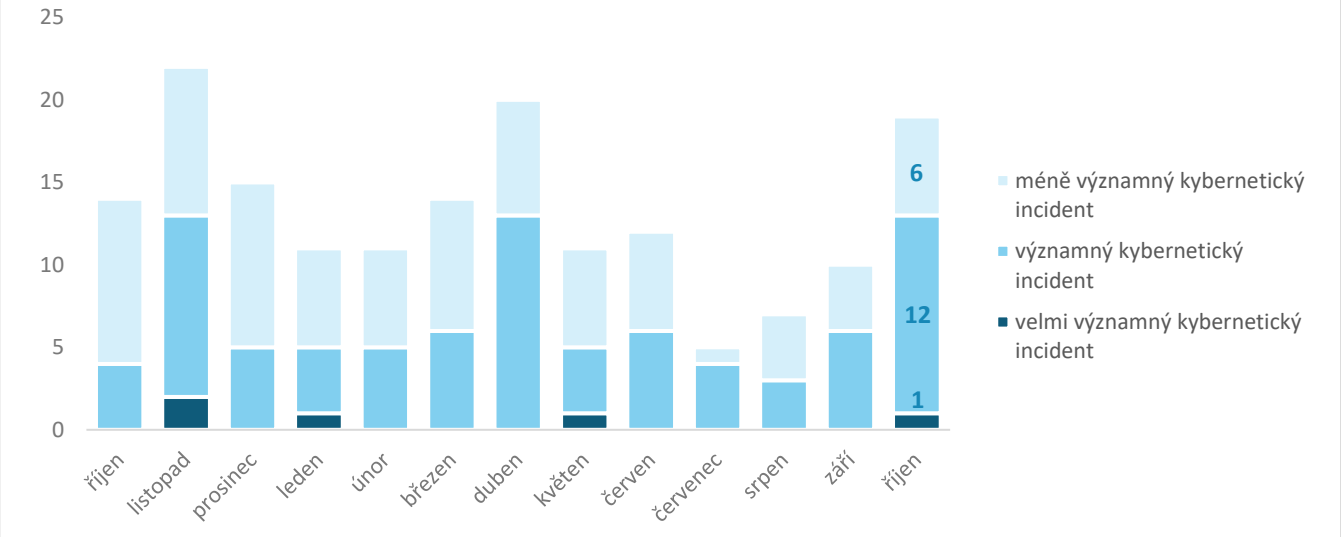
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet říjnových incidentů vysoce přesáhl průměrné hodnoty a téměř vyrovnal měsíc duben, který byl letos prozatím rekordní (celkem 20 incidentů). Podobně jako v dubnu, tak i nyní za nárůstem stojí hlavně bezprecedentní zvýšení počtu DDoS útoků. Zatímco však na jaře stály DDoS útoky za necelou třetinou incidentů, nyní jde o téměř sedmdesátiprocentní podíl.[1]



Závažnost řešených kybernetických incidentů[2]

Během měsíce října převažovaly velice mírně významné incidenty. Poprvé od května došlo k incidentu, který byl klasifikován jako velmi významný.

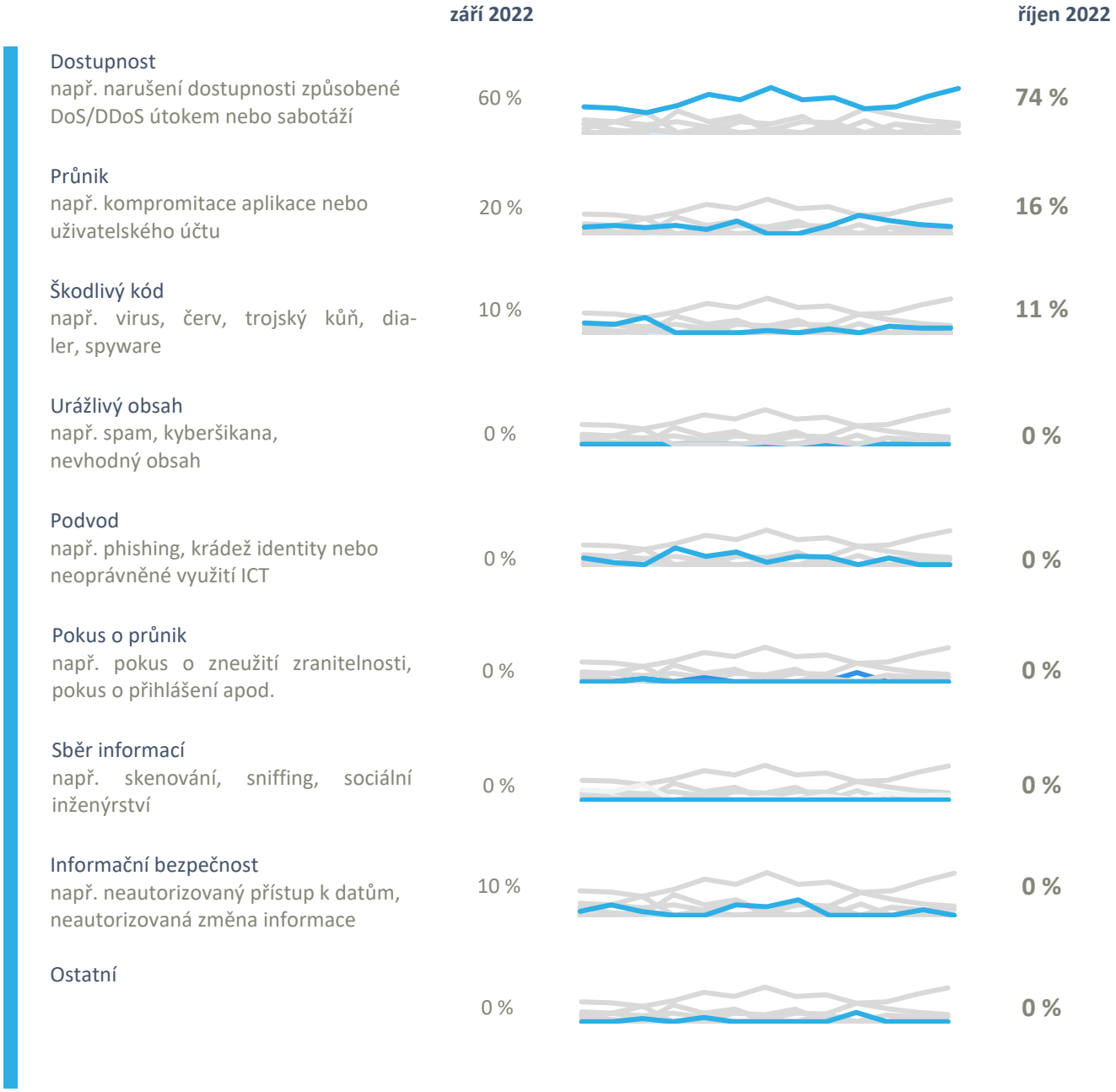


[1] Celkem 12 incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbývajících sedmi pak NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Říjnové kybernetické incidenty NÚKIB zařadil do třech kategorií:

- Přestože útoky na dostupnost jsou permanentním trendem, tak meziměsíčně jejich podíl na celkovém počtu incidentů stoupl ze 60 % na téměř tři čtvrtiny. Důvodem byl bezprecedentní nárůst počtu DDoS útoků. Jejich počet téměř vyrovnal jejich dosavadní souhrnné hodnoty za celý letošní rok, přičemž jedním z důvodů jsou útoky skupiny Anonymous Russia proti českým subjektům.
- Trvajícím trendem jsou i kompromitace sítě či uživatelských účtů. Během minulého měsíce byla zneužita infrastruktura několika subjektů k rozesílání phishingu a spamu, což zapříčinilo mj. reputační újmu domény.
- V případě škodlivého kódu vynikly dva incidenty, konkrétně zneužití zranitelnosti ProxyNotShell a posléze nasazení malwaru v organizaci ze sektoru zdravotnictví, respektive nález malwaru těžícího kryptoměny (cryptominer) v sektoru dopravy.



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

Trendy v kybernetické bezpečnosti za říjen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing nebo pokusy o něj jsou permanentní trend. Během října byla infrastruktura několika subjektů zneužita k masovému rozesílání phishingu. Dopadem byla mj. reputační újma domén kompromitovaných subjektů.

Malware

NÚKIB na základě dat z říjnových incidentů žádný malware neanalyzoval. Probíhaly kontinuální aktivity, během kterých se analytici zaměřili na malware RedLine Steler či botnet Mirai.

Zranitelnosti

Během října vydal NÚKIB dvě upozornění na zranitelnosti. První se týkalo CVE-2022-26113 (CVSS 7.5) ve FortiClient. Tato zranitelnost umožňuje získat vzdálený přístup do administrátorského rozhraní ve FortiOS (firewall) a FortiProxy (webové proxy). Druhé upozornění se věnovalo závažné zranitelnosti Wi-Fi v linuxovém jádru.

Ransomware

Poprvé v letošním roce nebyl hlášen ransomware. Ten přitom dlouhodobě zůstával permanentním trendem, především pak ty druhy vyděračského softwaru, které jsou nabízeny ve formě služby (ransomware-as-a-service).

Útoky na dostupnost

Přestože útoky na dostupnost jsou víceméně trvalým trendem, tak v měsíci říjnu došlo k mimořádnému nárůstu. Vyjma jediného případu šlo o DDoS útoky, kdy jejich počet takřka vyrovnal souhrnný počet všech útoků daného typu za celý rok 2022. Jednou z příčin byly útoky skupiny Anonymous Russia, která útoky proti českým subjektům deklarovala na svém účtu na síti Telegram. Primárně byla útočníky použita metoda HTTP flooding, která patří mezi méně sofistikované.

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

Technika měsíce: Direct Network Flood a Reflection Amplification

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. Vzhledem k masivnímu nárůstu počtu DDoS útoků se tentokrát zaměřujeme na podtechniky T1498.001 (Direct Network Flood) a T1498.002 (Reflection Amplification).

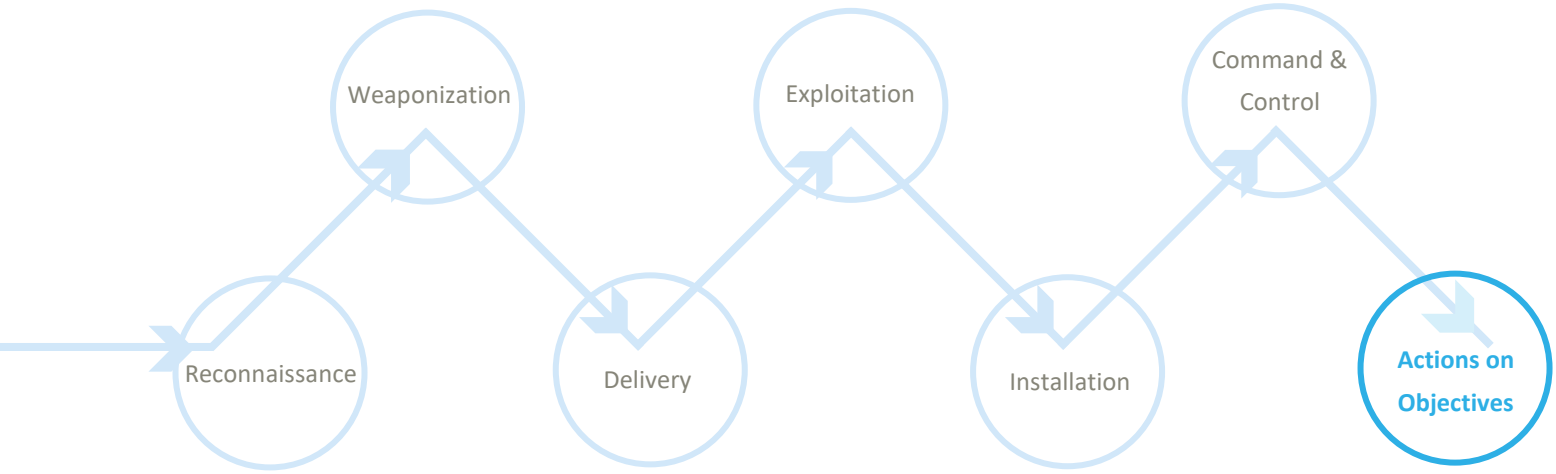
MITRE ID: T1498.001 + T1498.002

Direct Network Flood: Útočníci se mohou pokusit odepřít službu tím, že napřímo „zahltí“ cílový systém značným provozem. Takový útok může mít dopad na dostupnost. V případě tohoto útoku je použit jeden či více systémů k zasílání síťových paketů, kdy k „zahlcení“ může být využit téměř jakýkoli síťový protokol. Obvykle se jedná o protokoly UDP a ICMP, ale může být využit i protokol TCP atd.

Reflection Amplification: Útočníci mohou také využít zprostředkovatele serveru třetí strany, který je hostitelem a bude odpovídat na podvrženou zdrojovou IP adresu. Server daného typu je označován jako reflektor. Útok pak probíhá posíláním paketů na reflektor s podvrženými adresami oběti. Během útoku je odeslána mnohonásobně větší odpověď na server oběti, a to vzhledem k velikosti dotazu zadaného útočníkem.

Mitigace: Klíčovou mitigační technikou je filtrování síťového provozu. Je třeba odfiltrovat škodlivý provoz od legitimního, což poskytují poskytovatelé internetových služeb (ISP) či třetí strany. V závislosti na objemu může být on-premises filtrování možné blokováním IP adres, jež jsou zdrojem útoku, zacílených portů či protokolů používaných pro přenos.

Znázornění technik T1498.001 a T1498.002 v kill chainu ukazujícím, kdy útočníci techniku používají:

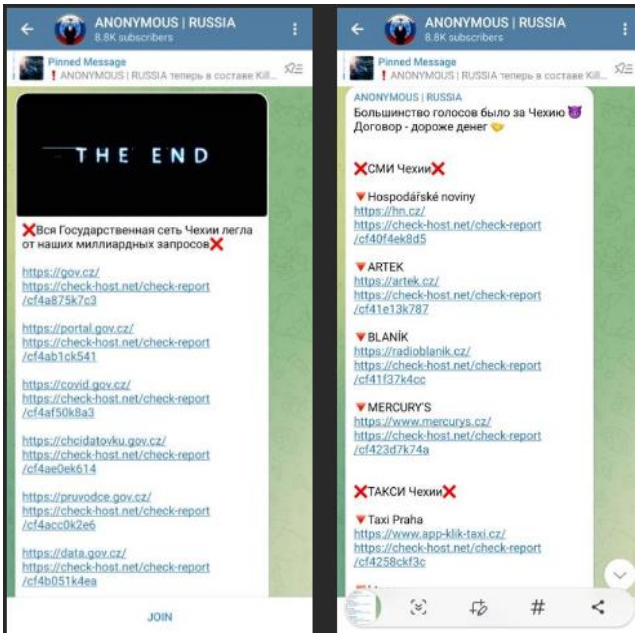


Zaměřeno na trend: zvýšené riziko DDoS útoků

Trendem posledního měsíce byl významný nárůst počtu DDoS útoků. **Jejich počet, jak bylo zmíněno výše, dosáhl skoro stejných hodnot jako za prvních devět měsíců roku 2022 dohromady.** K části říjnových útoků se přihlásila ruskojazyčná skupina Anonymous Russia. Podobná vlna DDoS útoků proběhla také v dubnu, kdy se některé české subjekty staly obětí skupiny Killnet.

Dne 2. října 2022 oznámila na sociální síti Telegram skupina Anonymous Russia útoky proti českým organizacím. Mezi nimi byly vládní instituce, média, banky nebo letiště, ale také cíle jako jsou restaurace. **Reálný dopad byl přesto nízký a byl zasažen pouze zlomek původně deklarovaných cílů.**

Obr 1: Cíle deklarované skupinou Anonymous Russia



Podobné skupiny jsou označovány za hacktivistické a mohou mít široké spektrum motivací. Separátně vydané upozornění ze dne 1. listopadu 2022 pak zmiňuje, že hacktivisté nebo tzv. vlastenečtí hackeři mohou útočit v návaznosti na politická rozhodnutí či prohlášení, jež jsou jimi vnímána jako nepřátelská. Podobným útokům během letošního roku čelily také Polsko, Litva, Lotyšsko, Estonsko, Rumunsko, Itálie či Německo. **Navzdory kontextu zacílení však nelze vyhodnotit, zda a případně nakolik jsou tito aktéři spjatí s konkrétními státy a jejich silovými složkami.**

Doporučení: Přestože útoky typu DDoS nemají dlouhodobý dopad a v jejich důsledku dochází primárně k nedostupnosti webů či na ně navazujících služeb, tak je žádoucí implementovat vybraná opatření. Varování ze dne 25. února 2022 obsahuje doporučení, jež se týkají přímo DDoS útoků. Opatření v bodech 3.1 a 3.2 může využít jakákoli organizace, naopak body 3.3 a 3.4 jsou určena specificky poskytovatelům internetového připojení.

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.