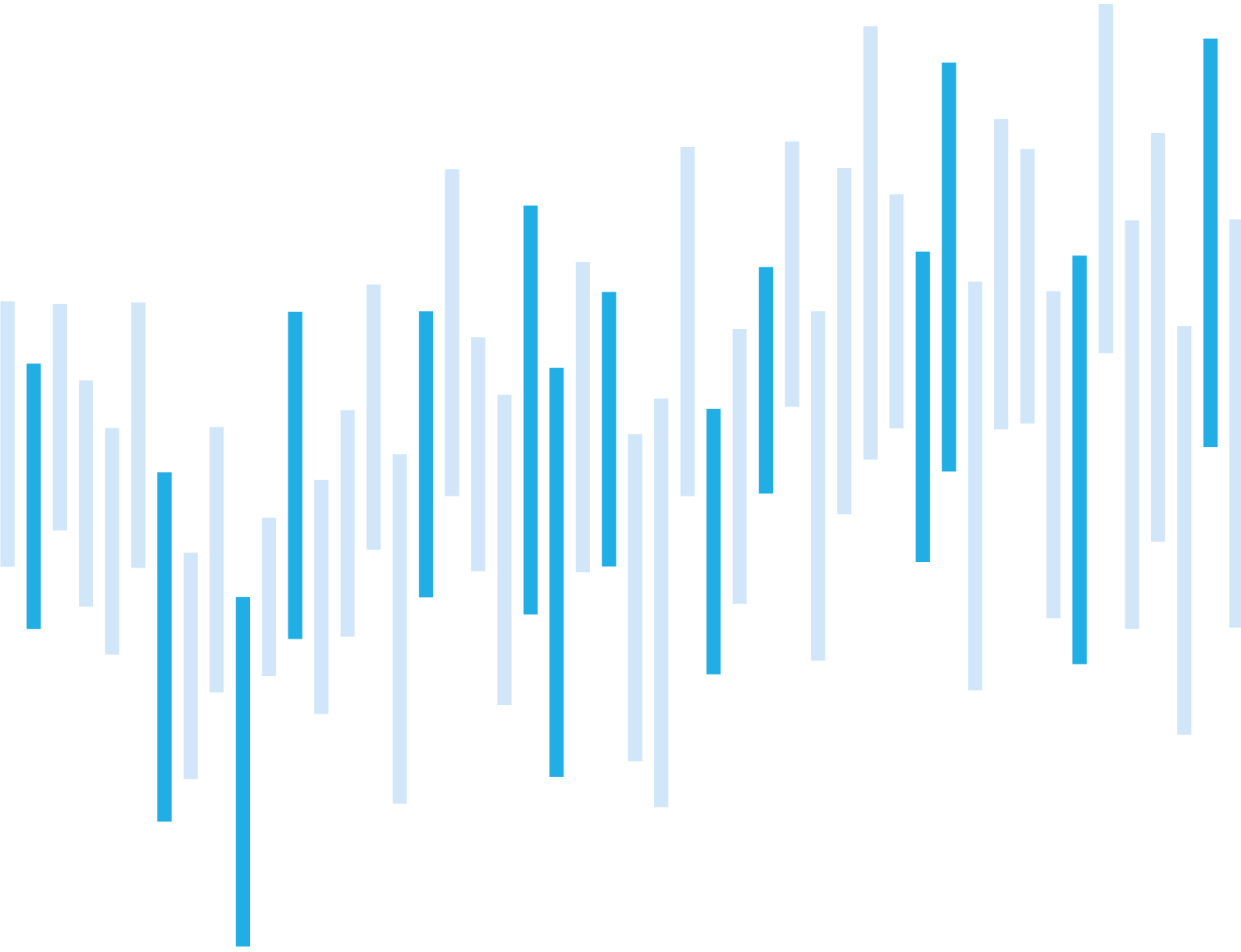
Kybernetické incidenty pohledem NÚKIB

KVĚTEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet květnových incidentů se pohyboval vysoko nad průměrem posledních 12 měsíců. Opět dominovaly případy, ve kterých došlo k narušení dostupnosti služeb, včetně DDoS útoků. NÚKIB také monitoruje další phishingové kampaně proti českým strategickým cílům.

Při jednom z květnových incidentů NÚKIB zaznamenal relativně nový trend v chování ransomwarových útočníků. Útočníci data své oběti nezašifrovali, pouze je exfiltrovali a vyhrožovali jejich zveřejněním. Jedná se o tzv. „extortion-only" přístup. Tyto nové trendy v chování ransomwarových operátorů mění i způsob, jakým by se organizace na ransomware měly připravit.

Vzhledem k dynamičnosti ransomwarového prostředí se NÚKIB rozhodl aktualizovat veřejný dokument Ransomware: Doporučení pro mitigaci, prevenci a reakci. Chování ransomwarových operátorů se mění a posouvá se i přístup obránců. Nová verze dokumentu proto bude brát v potaz nově používané techniky útočníků, nejnovější doporučení našich partnerů nebo nejčastější otázky, které organizace ve vztahu k ransomwaru řeší.

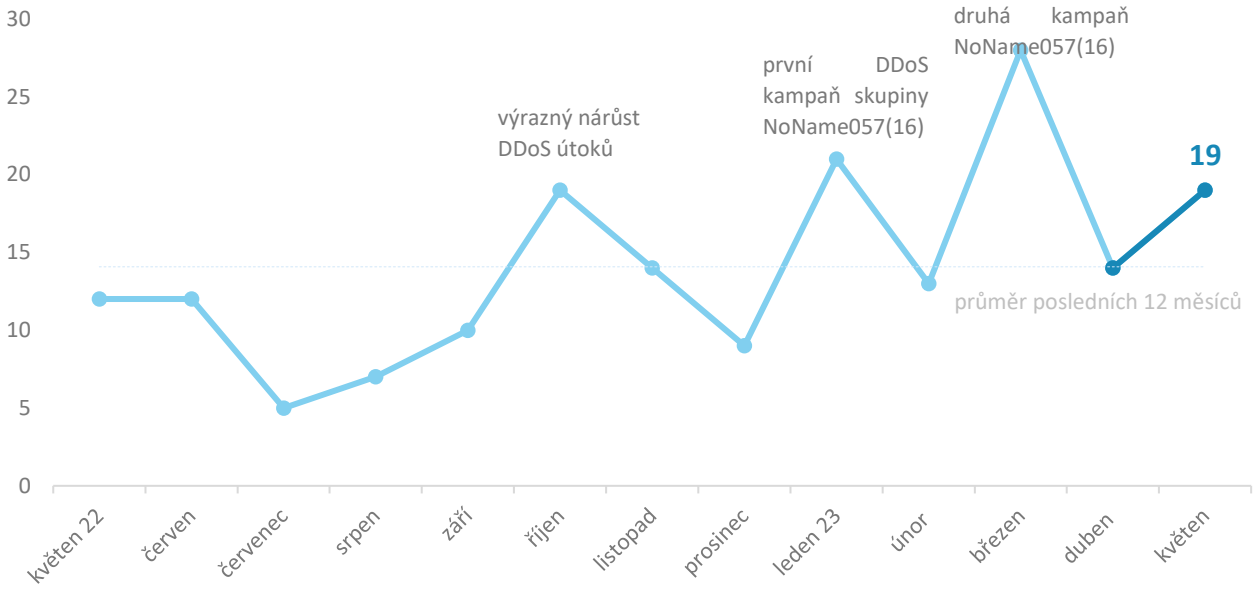
Obsah

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

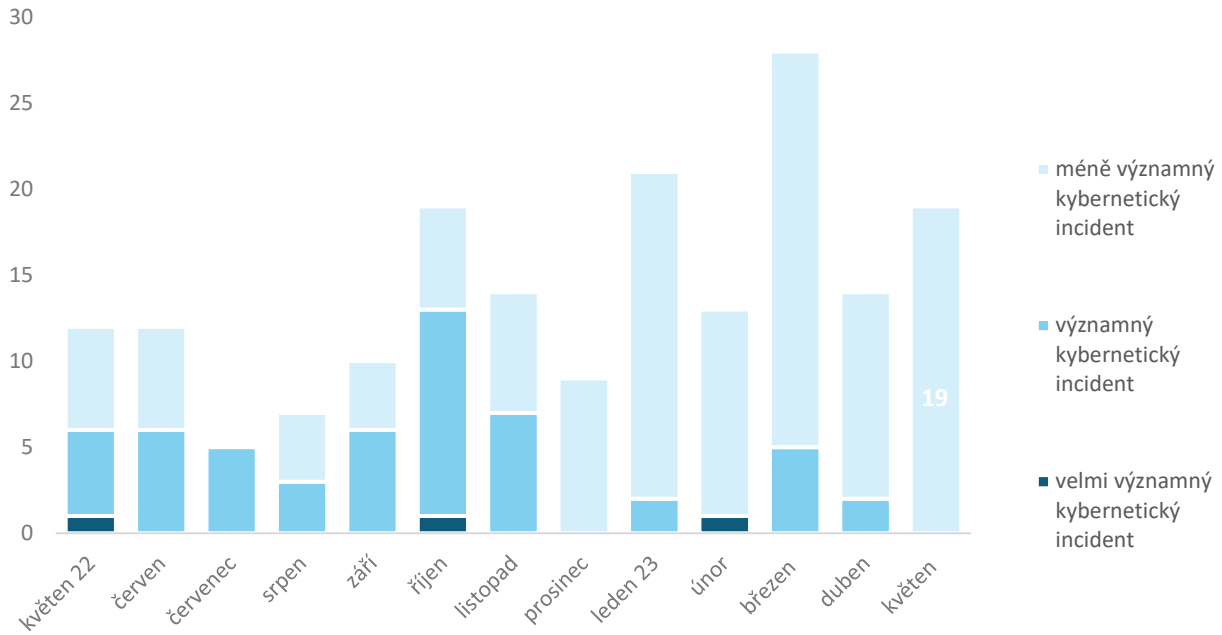
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

NÚKIB v květnu evidoval 19 kybernetických incidentů. Jak ukazuje graf, počet incidentů v posledním půl roce osciluje mezi průměrnými a výrazně nadprůměrnými hodnotami. Do těch se i tentokrát promítly DDoS útoky proti státním institucím.[1]



Závažnost řešených kybernetických incidentů[2]

Všechny květnové kybernetické incidenty se obešly bez závažných důsledků, které by výrazně ovlivnily chod napadených organizací, a NÚKIB je proto eviduje jako méně významné.



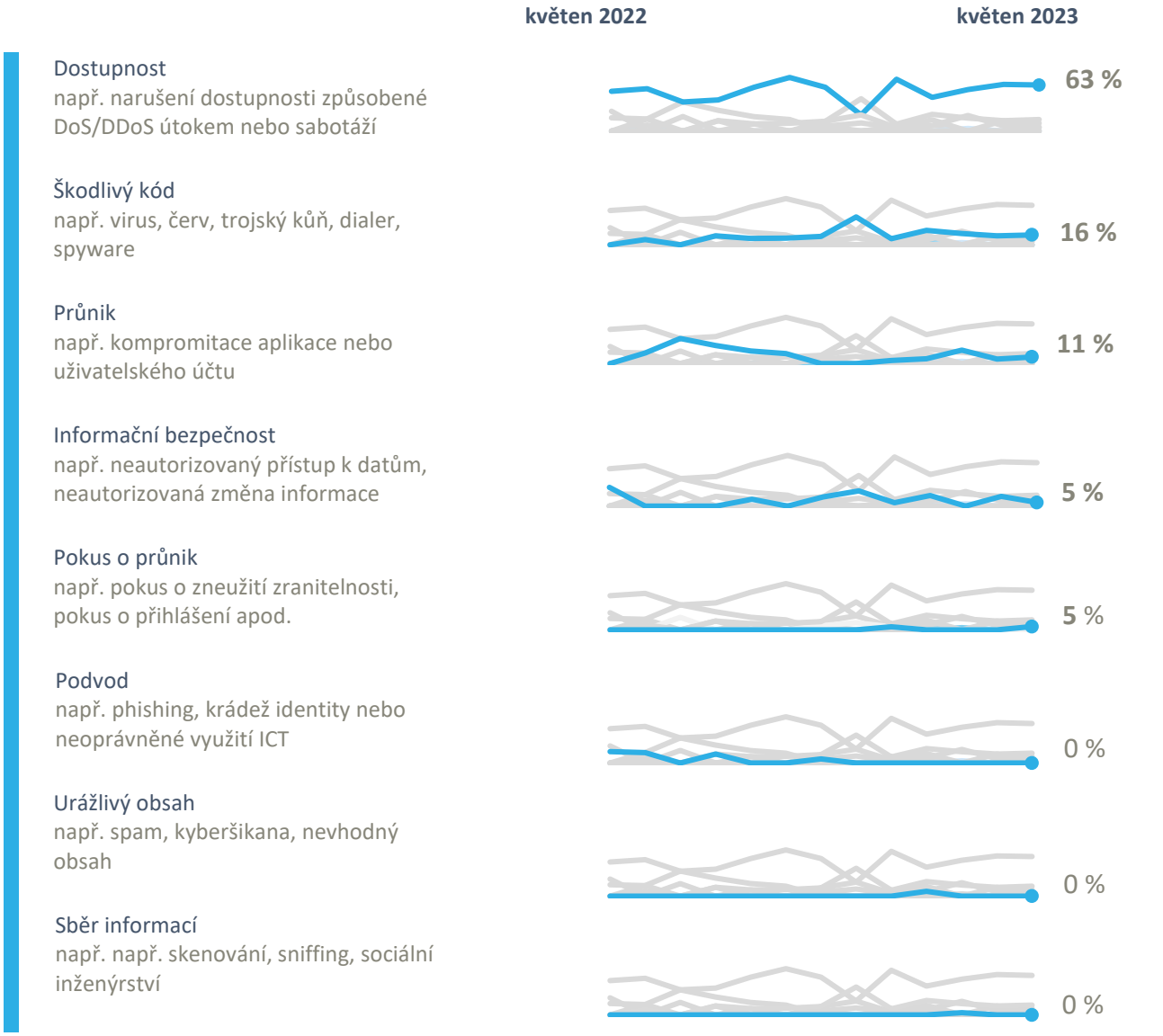
[1] 15 incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající čtyři incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

V květnu pokračoval trend posledních 12 měsíců, kdy incidentům dominovalo narušení dostupnosti služeb. NÚKIB takto klasifikoval 11 incidentů, tedy téměř dvě třetiny všech květnových incidentů. Vyjma dvou případů narušily dostupnost služeb DDoS útoky, které cílily zejména na instituce státní správy.

Vedle dostupnosti NÚKIB řešil incidenty mimo jiné i v těchto kategoriích:

- Dva incidenty, při nichž došlo k zašifrování dat ransomwarem, NÚKIB evidoval jako škodlivý kód. U třetího incidentu v této kategorii došlo ke kompromitaci e-mailové schránky uživatele;
- Další z ransomwarů je v kategorii informační bezpečnost. Při tomto incidentu útočníci data nezašifrovali, ale pouze exfiltrovali a oběti hrozili jejich zveřejněním;
- Jeden z řešených incidentů NÚKIB klasifikoval jako pokus o průnik. Téměř tři desítky zaměstnanců státní instituce otevřeli škodlivou přílohu phishingového e-mailu, ale škodlivý kód už byl nefunkční a k žádné kompromitaci tak nakonec nedošlo.



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

Trendy v kybernetické bezpečnosti za květen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Stále evidujeme probíhající phishingové kampaně proti českým strategickým vladním cílům. V námi zachycených květnových kampaních útočníci zneužívali evropské tématiky a rozesílali phishingové e-maily pod zdánlivou hlavičkou Evropské služby pro vnější činnost (EEAS). Kompromitaci dotčené organizace nezaznamenaly, ale vzhledem k dlouhotrvající a vysoké intenzitě podobných kampaní je pravděpodobné, že útočníci v krátkodobém horizontu uspějí, uživatele obelstí a některý ze svých cílů kompromitují. Úspěšnost jejich aktivit pak bude záviset na rychlosti odhalení ze strany napadených organizací.

Malware

Při analýze jedné z květnových phishingových kampaní NÚKIB narazil na malware PlugX, který je známý už od roku 2008 a bývá součástí phishingových kampaní. PlugX je modulární malware s různými funkcionalitami. Může zajišťovat spojení s řídicím serverem, zjišťovat informace o systému oběti, pořizovat screenshoty obrazovky nebo stahovat dodatečné soubory.

PlugX ve svých kampaních jako backdoor používají především čínští špionážní aktéři. Podle spekulací ale zdrojový kód PlugX unikl a je nyní k dispozici širšímu spektru aktérů. Před pár měsíci ho například začala používat ransomwarová skupina BlackBasta.

Zranitelnosti

V květnu se neobjevila nová závažná zranitelnost, u které bychom předpovídali plošné zneužívaní a která by mohla být zneužívána napříč povinnými osobami dle ZKB.

Ransomware

NÚKIB v květnu řešil čtyři případy ransomwarových útoků, o dva více něž v předešlém měsíci. Za útoky stály ransomware skupiny Monster, Snatch, DarkTrace a Trigona.

V incidentu spojeném s ransomwarovou rodinou Snatch využili útočníci tzv. „extortion-only“ přístupu, kdy data oběti nezašifrovali, ale pouze exfiltrovali a pak ji vydírali jejich zveřejněním. Snatch je ransomwarová skupina aktivní od roku 2018. Běžně ve svých útocích využívá tzv. „double-extortion“, kdy data zašifruje a poté i zveřejní. Zveřejnění dat bez jejich zašifrování jsme zaznamenali poprvé. Více informací naleznete v poslední kapitole tohoto reportu.

Útoky na dostupnost

V květnu se opět zvýšil počet hacktivistických DDoS útoků proti českým cílům. DDoS útoky tvořily téměř polovinu všech květnových incidentů a útočníci mířili především na instituce státní správy. Vedle skupiny NoName057(16), která na české cíle útočí už čtyři měsíce v kuse, se v incidentech objevila také skupina Anonymous Russia DDoS Attacks, jejíž aktivitu jsme naposledy řešili v říjnu loňského roku.

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

Technika měsíce: Exfiltration over C2 Channel

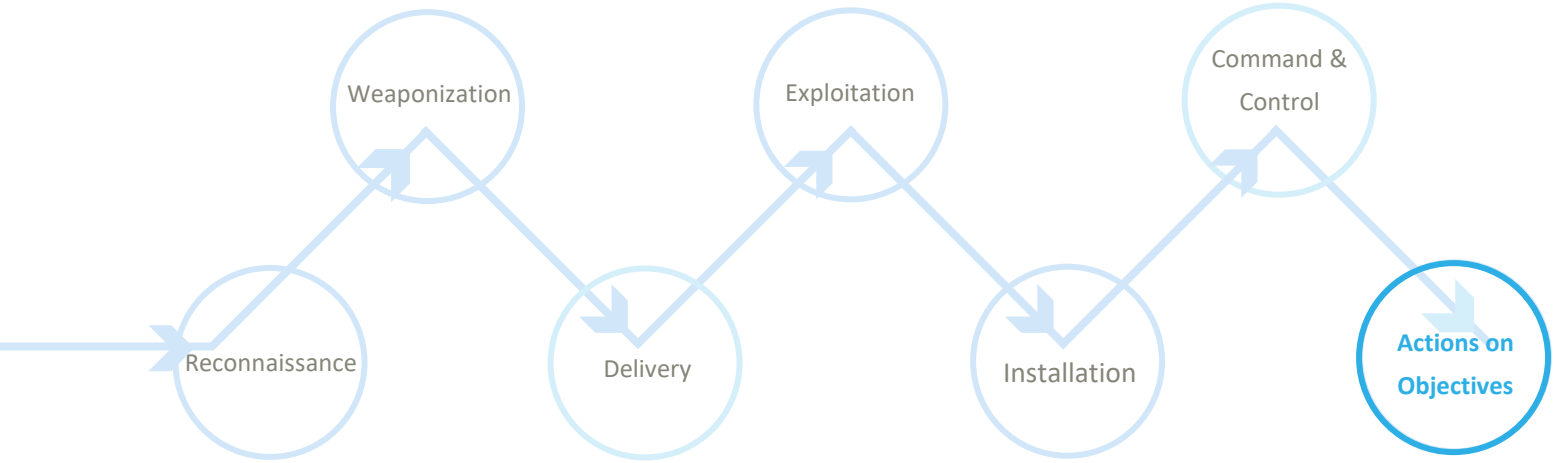
V jednom z květnových incidentů operátoři ransomwaru Snatch exfiltrovali data z české společnosti bez toho, aniž by je následně zašifrovali. NÚKIB dosud nemá dostatek informací potřebných k přesnému určení, jakým způsobem k exfiltraci dat došlo. Jelikož ale k tomu ransomwarové skupiny nejčastěji používají techniku Exfiltration over C2 Channel, zaměřujeme se v této kapitole právě na ni.

Exfiltration over C2 Channel: Tato technika popisuje postup, při kterém útočníci k exfiltraci dat využívají existující kanál pro řízení a kontrolu (C2). Využívají tak komunikačních kanálů nebo protokolů, které jsou již povoleny v síti oběti. Ukradená data jsou zakódována do běžného komunikačního kanálu pomocí stejného protokolu jako pro C2 komunikaci. Příkladem může být HTTP, ale i celá řada méně obvyklých protokolů. Tímto způsobem mohou útočníci přenést ukradená data bez nutnosti vytvářet nový kanál, což snižuje pravděpodobnost odhalení jejich činnosti.

MITRE ID: T1041

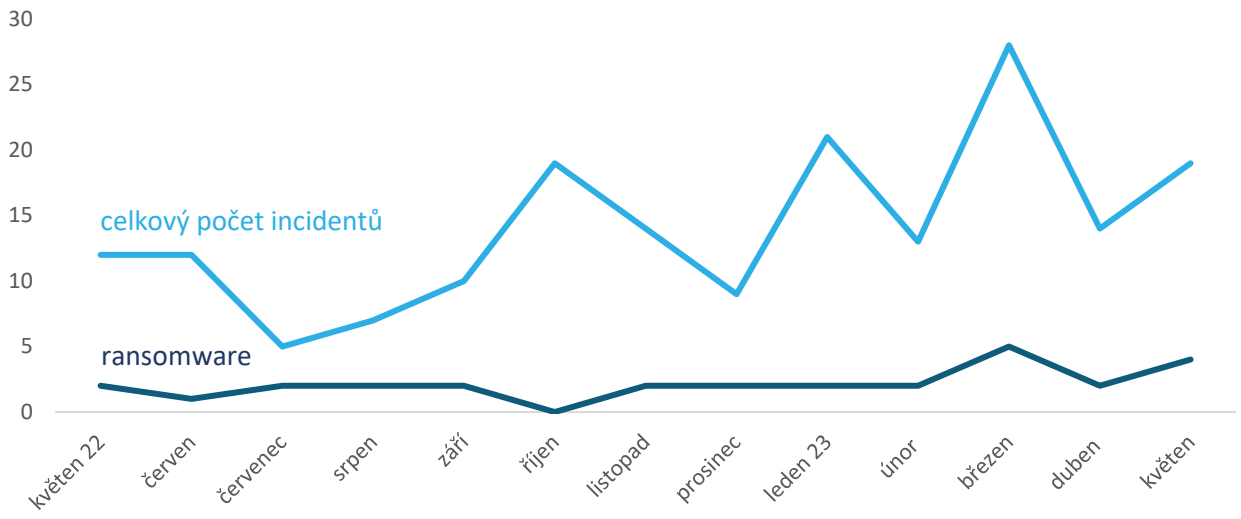
Mitigace: Mitigace vyžaduje kombinaci preventivních opatření a monitorování síťového provozu. Monitoring provozu a analýza logů mohou odhalit neobvyklé vzorce chování, velký objem datového přenosu nebo podezřelé komunikační protokoly. Implementace systémů IDS/IPS, které jsou schopny detekovat anomálie v síťovém provozu, a nástrojů pro odhalování hrozeb, které pracují s heuristikami a strojovým učením, mohou také pomoci identifikovat neobvyklou komunikaci spojenou s exfiltrací dat. Je proto nutné sledovat exekuci příkazů a argumentů vedoucích k exfiltraci, izolované podezřelé soubory (např. .pdf, .docx, .jpg atd.) nebo nově vytvořená síťová spojení, která jsou odesílána nebo přijímána nedůvěryhodnými hosty.

Znázornění T1041 v kill chainu ukazujícím, v jaké fázi útoku kybernetičtí aktéři techniku používají:



Zaměřeno na hrozbu: Ransomware a vyhrožování bez zašifrování dat

Ransomwarové útoky se mezi incidenty NÚKIB objevují pravidelně od roku 2018. Jak je vidět na grafu dole, NÚKIB téměř každý měsíc řeší minimálně dva útoky způsobené ransomwarem. Jeho oběťmi jsou v posledním roce především malé a střední podniky a vzdělávací instituce.



Ransomwarové prostředí je dynamické, proměňují se ransomwarové skupiny i jejich chování. Jak jsme popsali ve Zprávě o kybernetické bezpečnosti za rok 2021, útočníci už nezůstávají pouze u šifrování dat. Během útoků je i exfiltrují a po oběti vyžadují výkupné za to, že ukradená data nezveřejní. Chtějí tím na organizace vyvinout větší tlak a zvýšit tak pravděpodobnost, že jim zaplatí.

Při jednom z květnových incidentů NÚKIB zaznamenal další novinku. Česká IT společnost se stala obětí ransomwaru Snatch. Na rozdíl od běžných ransomwarových útoků jí ale útočníci data nezašifrovali. Pouze je exfiltrovali a české společnosti pak vyhrožovali, že pokud nezaplatí, její data začnou zveřejňovat. Bezpečnostní společnost RedCanary to popsala jako „extortion-only“ přístup.

Tyto nové trendy v chování ransomwarových útočníků mění i způsob, jakým by se organizace na ransomware měly připravovat. V ochraně před ransomwarem by měly pamatovat také na ochranu před technikami, kterými ransomwarový útočníci exfiltrují data ze sítí obětí. Nejčastěji se mezi takovými technikami objevují Exfiltration over C2 Channel (T1041), kterou popisujeme v předešlé kapitole, a Exfiltration to Cloud Storage (T1567.002). Jsou to dvě nejčastější techniky, kterými velké ransomwarové skupiny jako Lockbit, Hive nebo Conti, které často míří i na české cíle, data exfiltrují.

V roce 2020 NÚKIB ve spolupráci s AFCEA připravil dokument Ransomware: Doporučení pro mitigaci, prevenci a reakci. Od té doby se však ransomwarové prostředí proměnilo a posunul se i přístup obránců. Proto se NÚKIB rozhodl toto reflektovat a dokument spolu s partnery aktualizovat. Nová verze bude k dispozici během pár týdnů. Bude mimo jiné brát v potaz změnu chování útočníků, nejnovější doporučení našich partnerů nebo nejčastější otázky, které organizace ve vztahu k ransomwaru řeší.

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+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
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: 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.