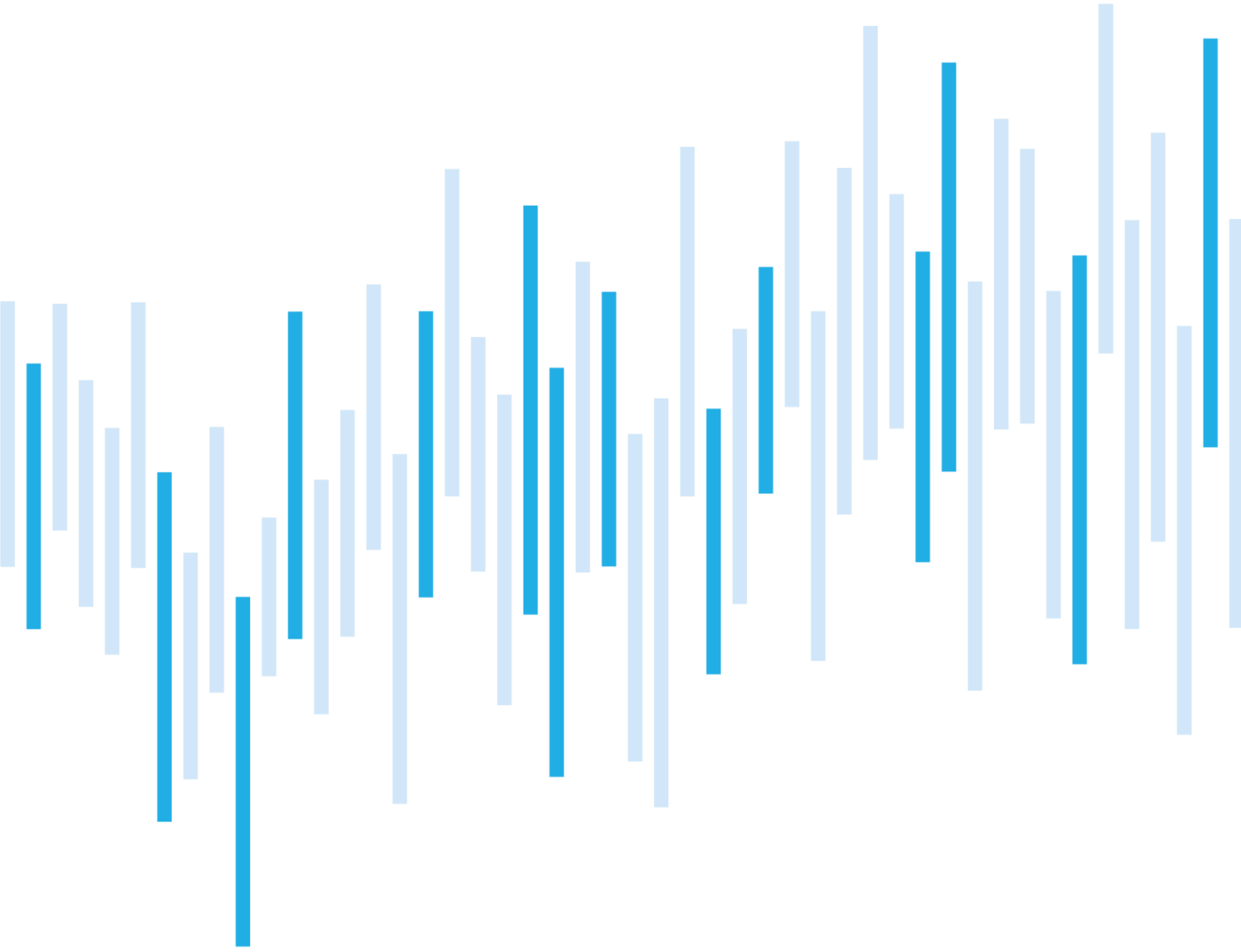
Kybernetické incidenty pohledem NÚKIB

LISTOPAD 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se během listopadu vrátil na mírně nadprůměrné hodnoty po rapidním nárůstu v měsíci říjnu. Tři pětiny incidentů byly na stupnici závažnosti klasifikovány jako významné, naopak zbytek jako méně významné. Oproti říjnu nedošlo k velmi významnému incidentu.

V listopadu převážily incidenty, které hlásily povinné osoby dle ZKB. Oběťmi byly subjekty ze sektorů veřejné správy, zdravotnictví, dopravy či bankovnictví. Velká část incidentů pak byla způsobena DDoS útoky, což ukazuje na určitou extrapolaci říjnového trendu.

Navzdory opětovné převaze útoků, které cílily na dostupnost, se tento měsíc zaměřujeme na techniku T1114: Email Collection, a to hlavně z důvodu, že útočníci mohou sbírat citlivé informace z kompromitovaných schránek.

S ohledem na trend jsme se zaměřili na ransomware jako službu (ransomware-as-a-service) navzdory tomu, že během listopadu byl evidován nižší počet vyděračského softwaru. Jde však o dlouhodobou hrozbu, která se trvale vyvíjí.

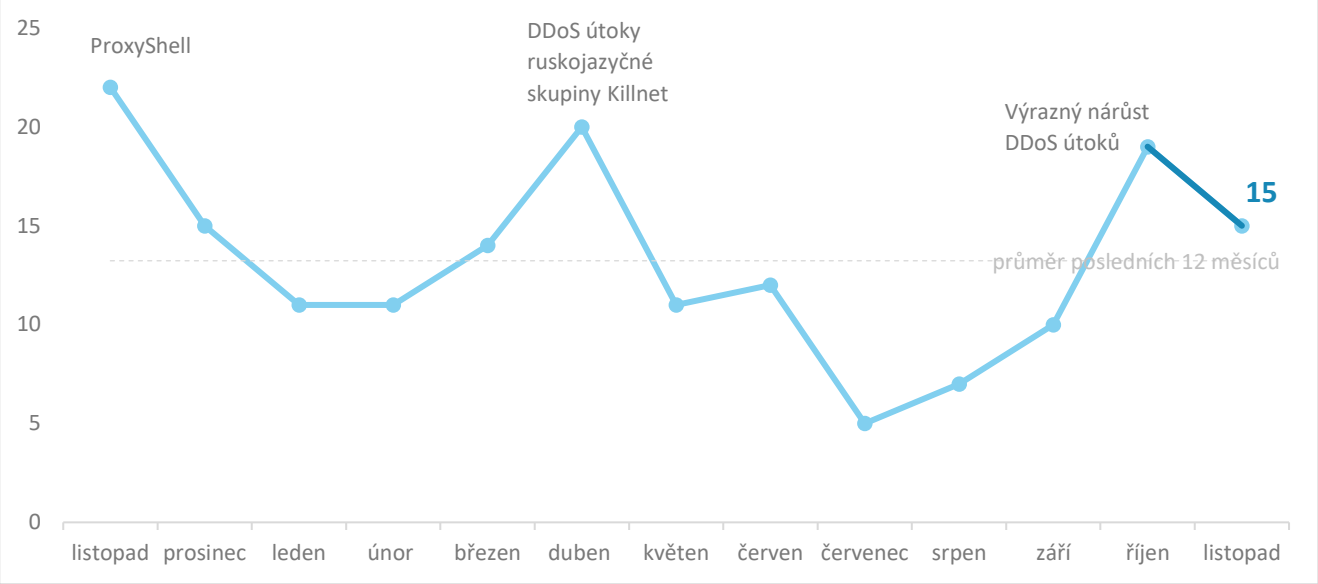
Obsah

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

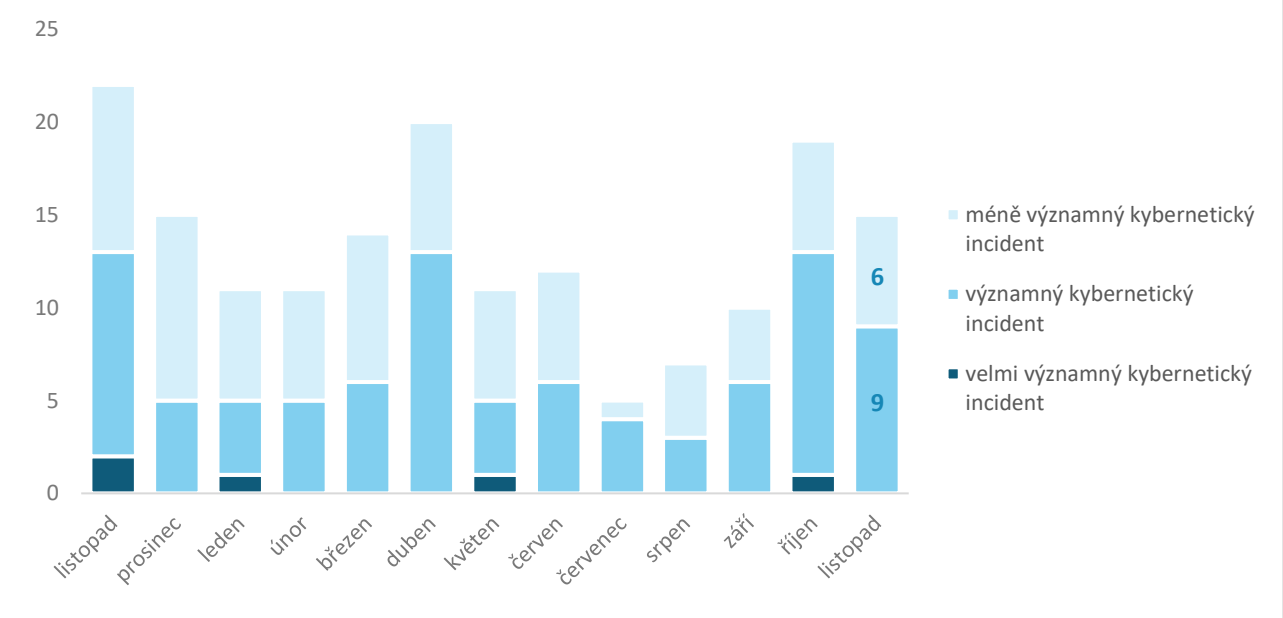
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet listopadových incidentů mírně poklesl ve srovnání s minulým měsícem, přesto se dostal na nadprůměrné hodnoty. Během podzimu a zimy GovCERT.cz běžně eviduje vyšší počet incidentů, přičemž oproti říjnu nyní neproběhl tak bezprecedentní nárůst počtu DDoS útoků, a tudíž je tedy zaznamenán pokles celkových hodnot.[1]



Závažnost řešených kybernetických incidentů[2]

Během listopadu převážily významné incidenty. Oproti říjnu však nedošlo k incidentu, jenž by byl klasifikován jako velmi významný, ke kterému letos došlo celkem třikrát.

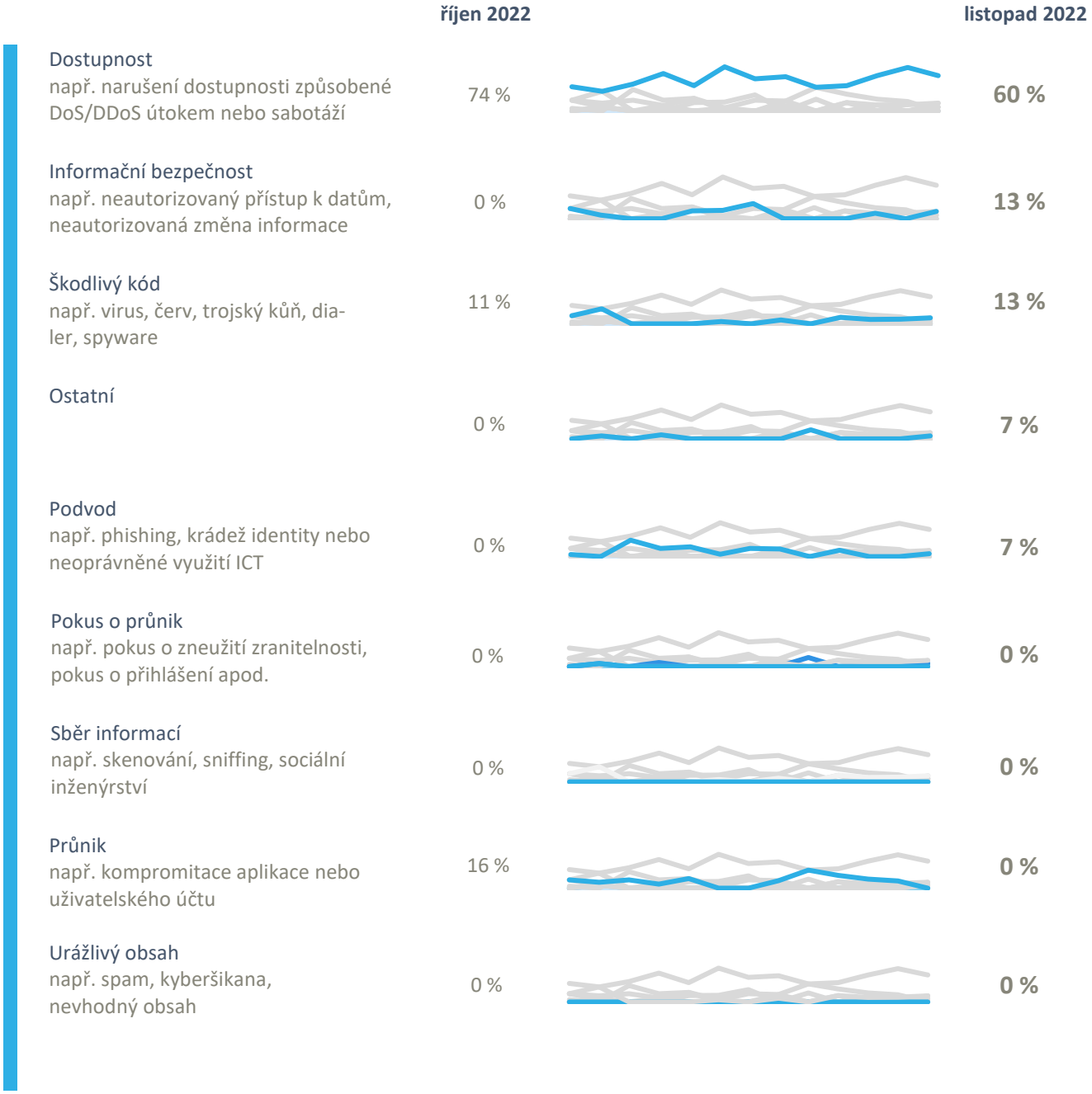


[1] Celkem 11 incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbývajících čtyřech NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Listopadové kybernetické incidenty NÚKIB zařadil do pěti kategorií:

- Z hlediska typu incidentů stále převažovaly útoky na dostupnost, kdy za drtivou většinou stály DDoS útoky, případně v minimu případů technické chyby ústící ve výpadky systému.
- Po měsíční pauze došlo opět ke dvěma incidentům týkajícím se informační bezpečnosti. Oba cíle patří mezi regulované subjekty a jsou činné ve zdravotnictví. V jednom případě byla narušena důvěrnost dat a v dalším pak bývalý zaměstnanec umožňoval přístup do systému neoprávněným osobám.
- V případě dvou incidentů typu škodlivý kód se jednalo o ransomwarové útoky.
- Jeden subjekt se stal obětí podvodu, kdy z oběti útočníci vylákali přes 900 000 Kč.
- Poprvé od července došlo k incidentu z kategorie ostatní, když byla narušena integrita aplikace.



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

Trendy v kybernetické bezpečnosti za listopad pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing nebo pokusy o něj jsou permanentní trend. Během listopadu opět některé subjekty čelily (spear)-phishingu či pokusům o něj.

Malware

NÚKIB na základě dat z listopadových incidentů žádný malware neanalyzoval. Probíhaly nicméně kontinuální aktivity v oblasti malwarové analýzy.

Zranitelnosti

Během listopadu vydal NÚKIB jedno upozornění na zranitelnost, konkrétně týkající se knihovny OpenSSL ve verzi 3. Původně vývojáři avizovali, že zranitelnosti CVE-2022-3602 a CVE-2022-3786 budou označeny za kritické. Díky moderním mitigačním technikám je nicméně obtížné až nemožné zranitelnosti zneužít ke vzdálenému spuštění kódu. Nakonec byly na stupnici závažnosti označeny stupněm vysoká.

Ransomware

Říjen byl prvním měsícem v letošním roce, kdy nebyl evidován útok pomocí ransomwaru. Naopak v listopadu se ransomware opět objevil, přičemž obětí se stala zákonem neregulovaná obecní samospráva a firma aktivní v odvětví dopravy.

Útoky na dostupnost

Oproti rekordnímu měsíci říjnu, kdy útoky na dostupnost představovaly téměř 75 % všech incidentů, přičemž dosáhly celkově vysokých hodnot, tak během listopadu došlo k určitému poklesu. Větší část incidentů byla ale opět spjata s DDoS útoky. Za částí stáli velmi pravděpodobně hacktivisté, kteří kroky napadených subjektů považovali za provokativní nebo dokonce nepřátelské, což se stalo spouštěčem útoků.

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

Technika měsíce: Email Collection

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 tomu, že útočníci často sbírají citlivé informace z kompromitovaných e-mailů, tak se nyní zaměřujeme na techniku T1114: Email Collection.

MITRE ID: T1114

Ve fázi sběru informací (v rámci MITRE ATT&CK jde o taktiku „collection“) se útočníci mohou zaměřit na jejich sběr z kompromitovaných e-mailů uživatelů. Vyjma narušení důvěrnosti může dojít i k jejich exfiltraci nebo smazání. Mnoho schránek, a to zejména výše postavených představitelů či zaměstnanců organizací s citlivou činností, obsahuje informace strategického charakteru. Daná technika má tři sub-techniky:

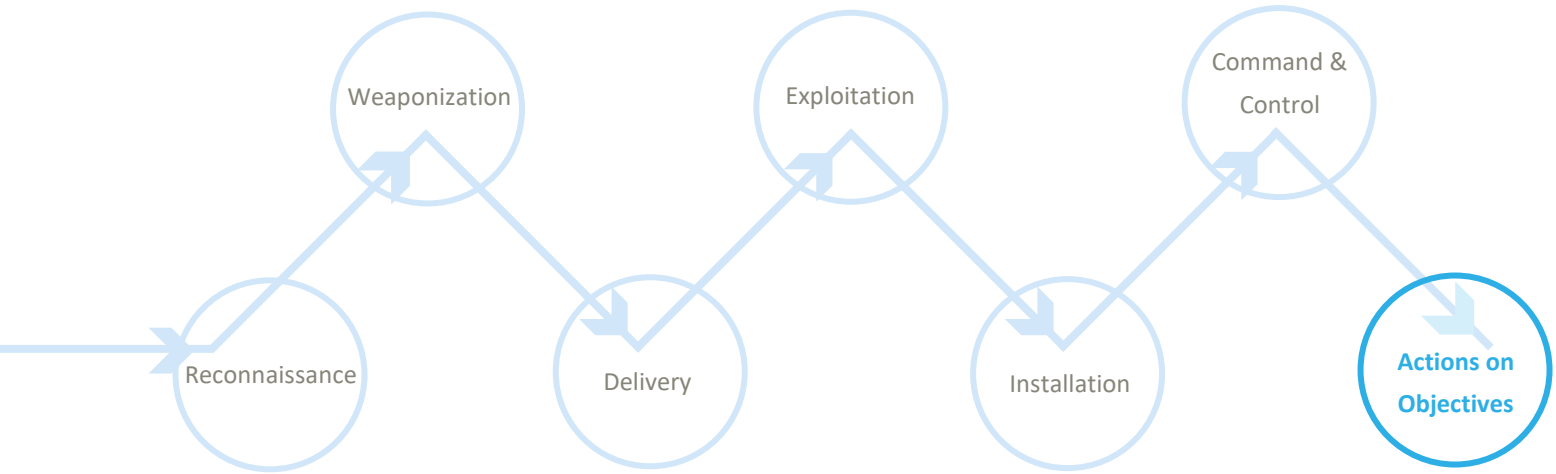
T1114.001: Local Email Collection – Útočníci cílí na e-maily na lokálních systémech. Soubory obsahující data mohou pocházet například z úložiště Outlook apod.

T1114.002: Remote Email Collection – Útočníci cílí na služby typu Exchange server nebo Office 365. Mohou být zneužívány přihlašovací údaje nebo může docházet k interakci se serverem Exchange, čímž dochází ke sběru informací zevnitř sítě.

T1114.003: Email Forwarding Rule – Útočníci mohou nastavit pravidla pro přeposílání zpráv, aby sbírali citlivé informace. Zneužitím pravidel může docházet též k monitoringu aktivit oběti a dalšímu zisku zpravodajsky cenných informací kvůli provádění navazujících škodlivých aktivit.

Mitigace: Základem pro mitigaci jsou auditování, šifrování citlivých informací nebo implementace vícefaktorového ověření.

Znázornění techniky T1114 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na trend: ransomware jako služba

NÚKIB dlouhodobě eviduje ransomwarové útoky, jejichž obětí se stává široké spektrum subjektů od veřejné správy po soukromé společnosti, které často nejsou regulovány zákonem o kybernetické bezpečnosti. **Od konce roku 2019 začal převažovat trend ransomwaru nabízeného ve formě služby (ransomware-as-a-service, RaaS).** Ten je specifický nejenom tím, že imituje legitimní software a škodlivý software mohou pořídit také jednotlivci bez nutnosti vývoje nebo dokonce technických znalostí, ale i svým důrazem na vícenásobné vydírání.

Obr 1: Znázornění vícenásobného vydírání

RaaS je fakticky obchodní model, v rámci kterého provozovatel/vývojář nabízí svůj produkt klientům, kteří jej nasazují kvůli finančnímu zisku.

Vyjma klasického zašifrování může probíhat až čtyřnásobné vydírání. Jeho součástí mohou být (nikoliv nutně v tomto pořadí) exfiltrace dat a hrozba jejich zveřejněním, DDoS útoky pro zvýšení tlaku na oběť a kontaktování zákazníků a partnerů oběti pro další navýšení tlaku z důvodu platby výkupného. **Odcizená data jsou obvykle zveřejněna na darkwebu, kde jsou eventuálně nabízena případným zájemcům, pokud by oběť nezaplatila výkupné.** Tím je tak významně narušena důvěrnost dat, což vyjma nedoporučené platby výkupného přináší obětem také možné reputační škody, včetně dopadu na jejich obchodní vztahy.

Doporučení: Uživatelům se doporučuje řídit se základními pravidly na obranu proti (spear)-phishingu, který zůstává jedním z hlavních vektorů ransomwaru, a to včetně RaaS. Stejně tak by správci sítě měli zvážit implementaci nástrojů omezujících přístup útočníků k oběti. NÚKIB vydal doporučení a metodiku, co dělat při napadení ransomwarem a také analýzu k hrozbám jež představuje. V rámci mitigace se doporučují např. pravidelné aktualizace, segmentace sítě, tvorba záloh či školení personálu. Při napadení ransomwarem se nedoporučuje platit výkupné. V případě snahy o komplexní zabezpečení mohou střední až větší organizace zvážit rozvoj Cyber Threat Intelligence, potažmo tvořit týmy specificky dedikované na tuto činnost.

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.