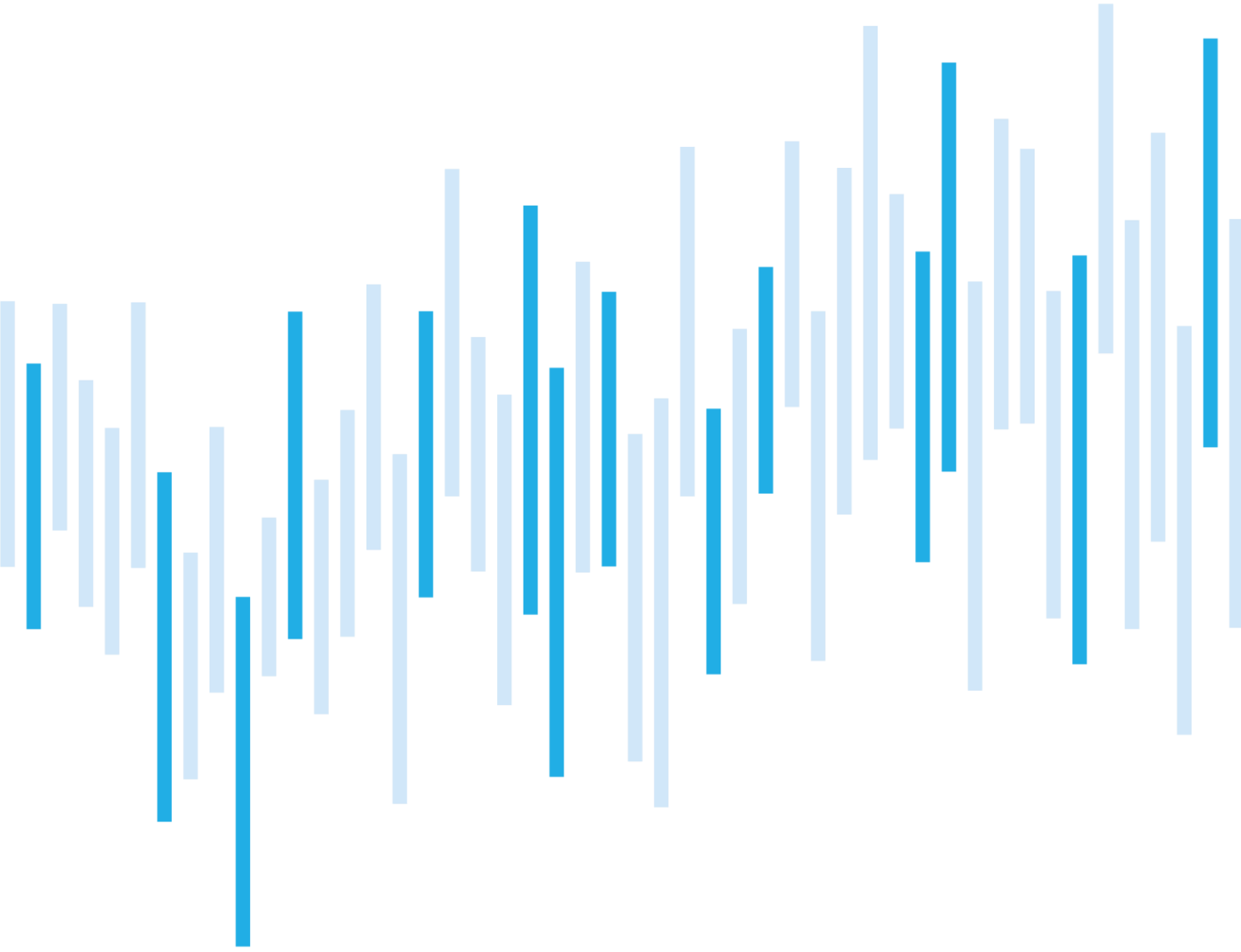
Kybernetické incidenty pohledem NÚKIB

ZÁŘÍ 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se v září dostal na téměř průměrnou hodnotu po období relativního a tradičního klidu během léta. Letos začal nárůst počtu incidentů již v září, naopak loni šlo sledovat vzestupnou tendenci až od října. Značný podíl na zářijových incidentech mají incidenty klasifikované jako významné.

V září převažovaly incidenty, které hlásily regulované subjekty. Opět nepřevažovaly konkrétní sektory. Zasaženy byly organizace v oblastech státní správy, dopravy, zdravotnictví či bankovnictví.

Tento měsíc jsme se zaměřili na techniku Gather Victim Identity Information, u níž útočníci musí před započetím samotného útoku nejprve získat informace o potenciální oběti,

Vzhledem ke stále se vyvíjejícím útokům proti vícefaktorovému ověřování (MFA) pak věnujeme kapitolu „Zaměřeno na trend“ právě jim.

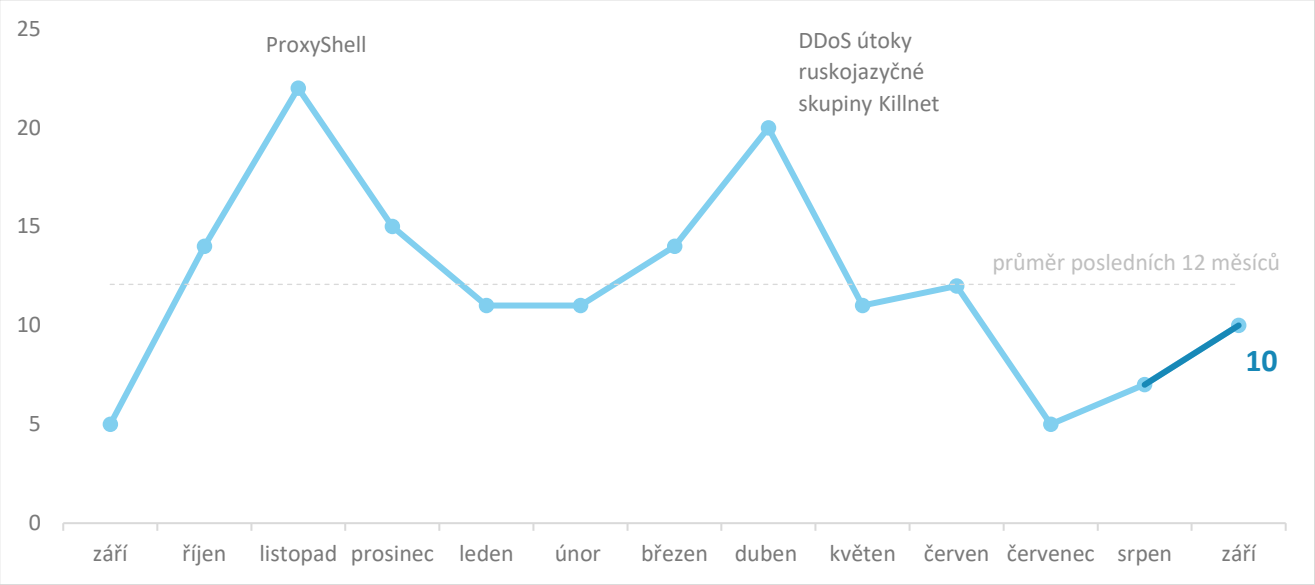
Obsah

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

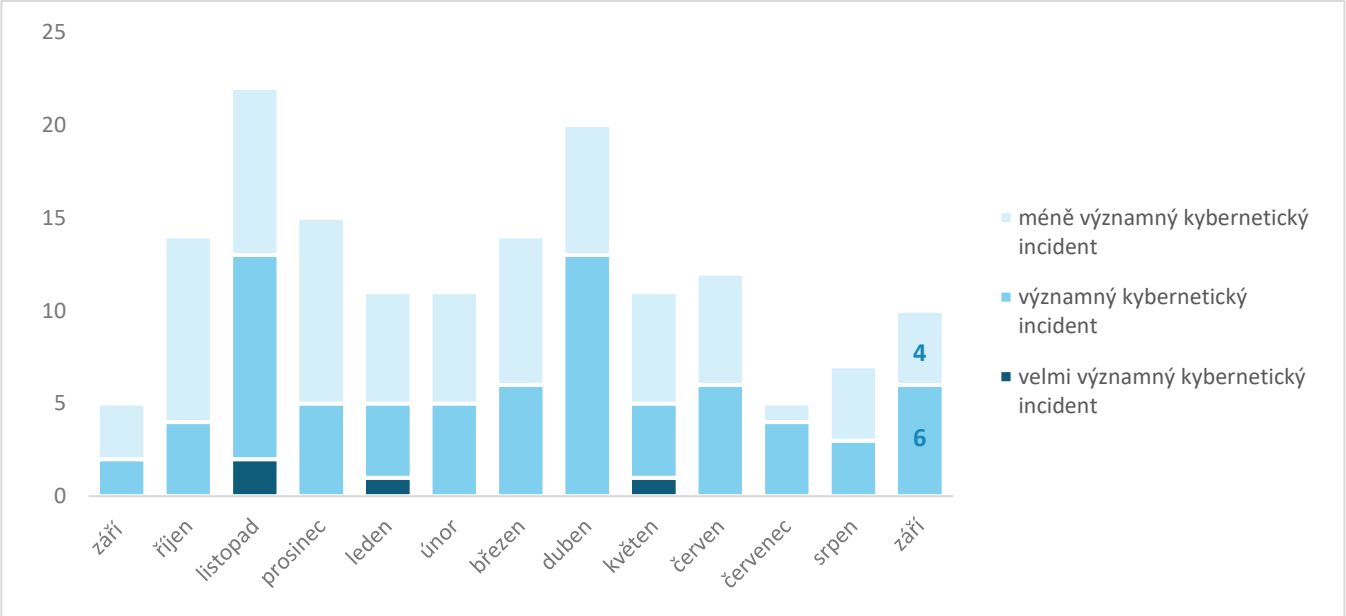
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet incidentů dosáhl v září téměř průměrných hodnot. Jde o každoroční trend, kdy po obvykle klidnějším létě dochází ke vzestupné tendenci.[1]



Závažnost řešených kybernetických incidentů[2]

Během měsíce září převažovaly velice mírně významné incidenty. Stejně jako v předchozích třech měsících nedošlo k velmi významnému incidentu.

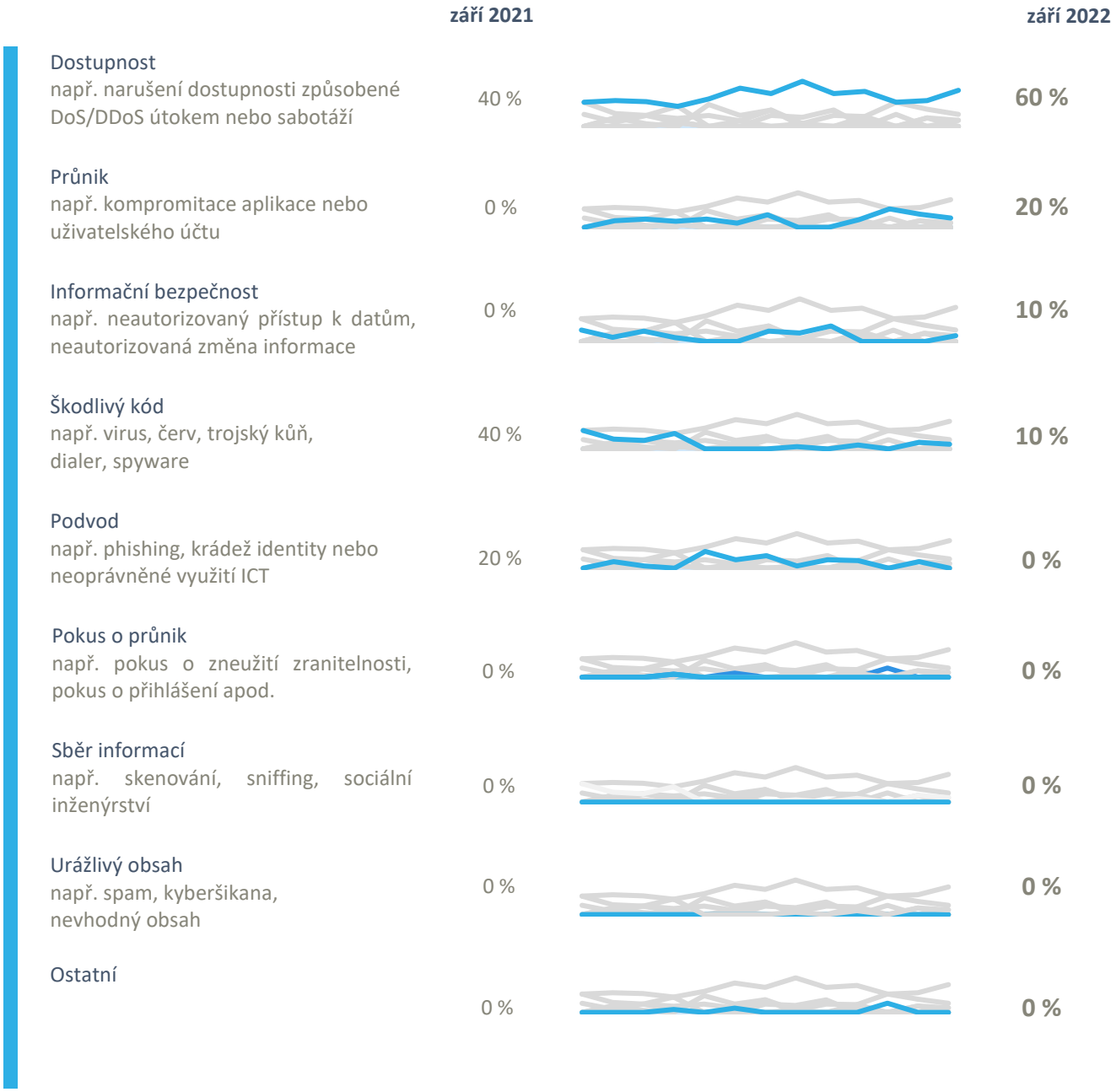


[1] Sedm incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O třech incidentech NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Zářijové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Nadále docházelo k útokům na dostupnost, které jsou trvalým trendem. Ve dvou případech šlo o DDoS útok a v dalších dvou pak o ransomware.
- Trvajícím trendem jsou i kompromitace sítě či uživatelských účtů.
- U jednoho z hlášených incidentů došlo ke spuštění škodlivého kódu na počítači oběti a následnému pokusu o komunikaci se serverem pod kontrolou útočníka.
- Poprvé od května došlo k incidentu z kategorie informační bezpečnosti. Konkrétně šlo o únik dat. Oběť však incident aktivně řešila a neoprávněnému přístupu zamezila.



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

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing nebo pokusy o něj jsou permanentní trend, přičemž v posledním měsíci jsme nezaznamenali výrazně zajímavý případ.

Malware

NÚKIB na základě dat ze zářijových incidentů žádný malware neanalyzoval.

Zranitelnosti

Během září vydal NÚKIB dvě upozornění na zranitelnosti. První se týkalo CVE-2022-26113 (CVSS 7.5) ve FortiClient. Tato zranitelnost pak umožňuje neprivilegovanému uživateli s přístupem ke koncové stanici s nainstalovaným VPN klientem FortiClient získat na této stanici práva uživatele SYSTEM. Druhé upozornění se týkalo dvou zranitelností MS Exchange Server, jmenovitě CVE-2022-41040 (CVSS 6.3) a CVE-2022-41082 (CVSS 8.8).

Ransomware

Trend vyděračských útoků pokračoval i v září. Počet evidovaných útoků pak zůstal na stejných hodnotách, přičemž tentokrát se jednalo o Phobos a DeadBolt.

Útoky na dostupnost

Stejně jako v srpnu, i v září došlo k DDoS útokům. Během jednoho z incidentů došlo ke kombinaci UDP Flood, IP Fragmentation a DNS Amplification.

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

Technika měsíce: Gather Victim Identity Information

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V první fázi závažného kybernetického útoku musí útočníci nejprve získat informace o identitě svých obětí. V rámci MITRE ATT&CK je tento postup znám jako T1589: Gather Victim Identity Information.

MITRE ID: T1589

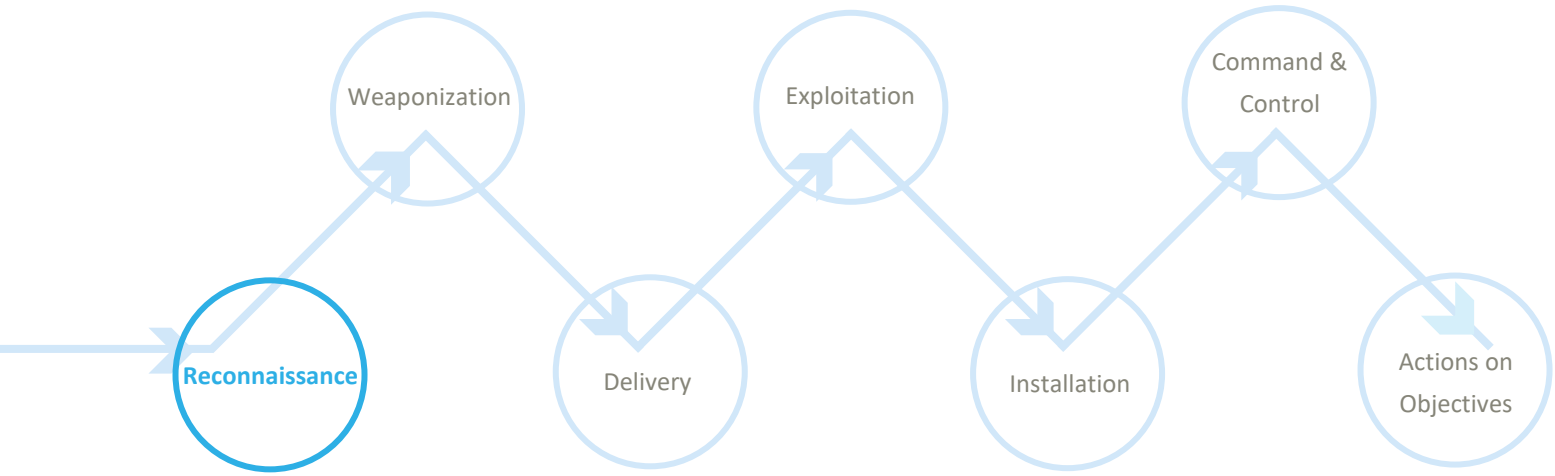
Útočníci se v první fázi průzkumu zaměřují na sběr informací o identitě svých případných obětí. Informace mohou zahrnovat jak osobní data (např. jména zaměstnanců) i citlivé údaje (např. přihlašovací údaje). Informace mohou být získávány „aktivněji“, tedy formou phishingu nebo aktivního skenování, ale i neinvazivně tím, že útočníci je získají z veřejně dostupných zdrojů (např. sociální sítě). Ve druhém případě se hovoří o tzv. OSINT, tedy získávání znalostí z otevřených zdrojů (Open-Source Intelligence).

Zisk těchto informací slouží jako ideální stavební kámen pro další fáze průzkumu (tzv. re-connaissance), vytvoření operačních zdrojů nebo prvotní přístup do sítě oběti. Samotná technika se dále rozpadá do trojice sub-technik, jmenovitě T1589.001: Credentials, T1589.002: Email Addresses a T1589.003: Employee Names.

Velice podobnou technikou je T1589: Gather Victim Org Information. V té se útočníci za-měřují na zjištění fyzických lokací (např. infrastruktura), byznysové vztahy, zjištění tempa byznysu a identifikaci rolí.

Mitigace: Danou techniku nelze snadno mitigovat. Subjekty by se měly primárně zaměřit, aby minimalizovaly množství dat (primárně citlivých), která jsou externě dostupná, a tedy zneužitelná v rámci OSINT.

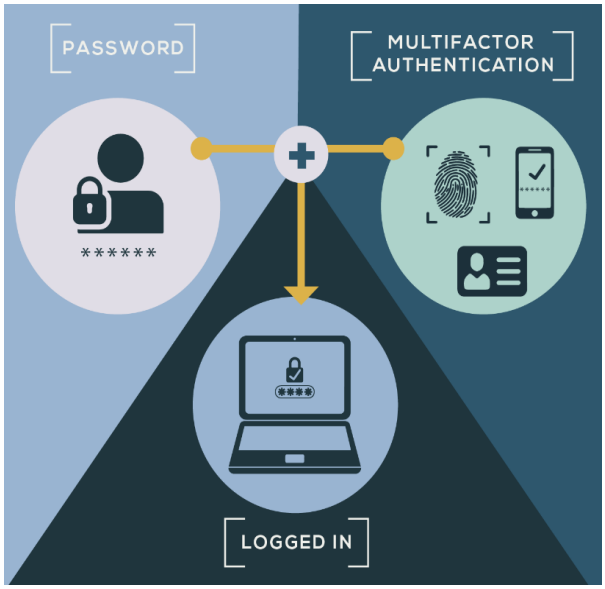
Znázornění techniky T1589 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na trend: útoky proti MFA (vícefaktorové ověřování)

Vícefaktorové ověřování (Multi-Factor Authentication, dále MFA) je doporučovanou praxí, jak zabezpečit účty a vzdálený přístup. Ověřování jen heslem je z bezpečnostního hlediska považováno za překonané a neodolné vůči běžným útokům jako phishing či hádání hesla hrubou silou. I přes důslednou ochranu též nejsou ojedinělé úniky databází hesel, čímž dochází ke kompromitaci hesla zcela bez zavinění uživatele. Vyžadováním druhého faktoru je případnému útočníkovi znemožněn přístup i v případě získání hesla. Nicméně se jedná pouze o zvýšení ochrany vůči útokům na heslo, nikoliv o neprolomitelné zabezpečení.

Obr 1: Ilustrativní obrázek vícefaktorového ověřování



Počet útoků na MFA v posledních měsících výrazně roste. Útočníci se na rozšířené zavádění MFA rychle adaptují a vzniká navíc řada volně dostupných nástrojů, které dále usnadňují obcházení či krádeže ověřovacích tokenů. Nejrozšířenějšími typy útoku jsou zejména:

1) Odposlech ověřovacího kódu

Stejně jako lze pomocí keyloggeru nebo při komunikaci nezabezpečeným kanálem odposlechnout heslo, lze stejným způsobem získat i zadaný ověřovací kód. Ověřovací kód chrání proti prolomení hesla zvenčí, ale v případě kompromitace uživatelského zařízení odcizení účtu nezabrání.

2) MFA fatigue

Jednou z metod MFA je potvrzování přístupu pomocí aplikace, v níž uživatel obdrží notifikaci pro schválení nebo zamítnutí přístupu. Vzhledem k tomu, že nedochází k opisování žádného kódu, je tento typ odolný vůči odposlechům, ale je zranitelnější skrze lidský faktor. Stále více používaným útokem je tzv. MFA fatigue neboli únava z množství obdržených notifikací, kdy uživatel v důsledku nevěnuje upozorněním dostatečnou pozornost a omylem či nevědomky povolí přístup.

3) Adversary-in-the-middle

Uživatel v tomto útoku obdrží odkaz na vizuálně podobnou doménu vlastněnou útočníkem (např. g00gle.com), jež slouží jako prostředník mezi zařízením uživatele a reálnou službou (google.com). Vyjma pečlivé kontroly domény a jejího certifikátu nelze podvod odhalit, neboť se na stránce skrze přesměrování nachází skutečný obsah požadované služby. Metoda vyžaduje ze strany útočníka pouze registraci domény sloužící jako proxy, která přeposílá přihlašovací údaje na danou službu. Stránka zprostředkovaně komunikuje se skutečným serverem cílové služby, kdy uživateli po zadání hesla přijde legitimní výzva k MFA ověření. Zadaný kód nicméně útočník obratem zachytí a získá přístup.

Dané útoky lze mitigovat kupříkladu ověřením pomocí fyzického tokenu, např. s využitím standardu FIDO.

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.