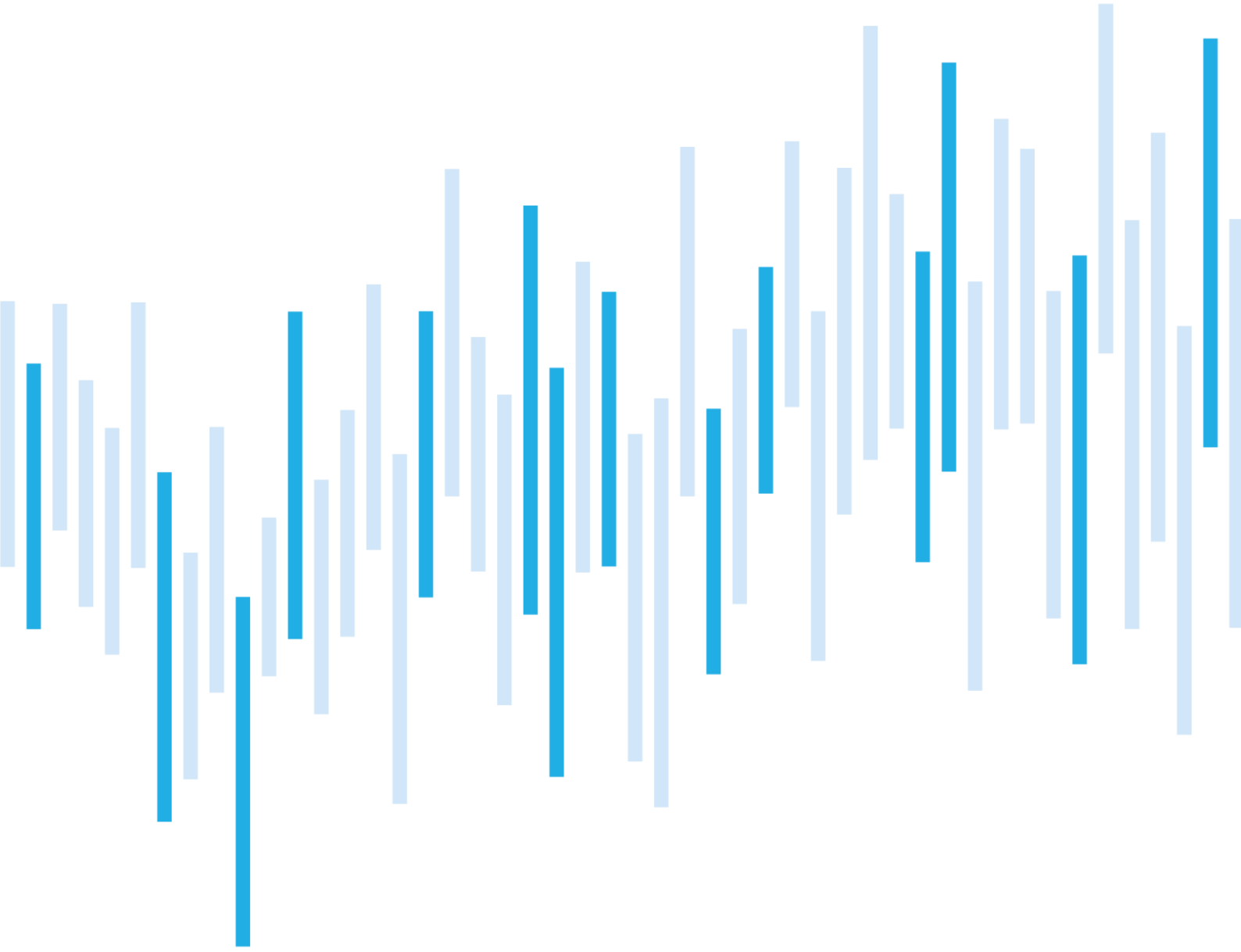
Kybernetické incidenty pohledem NÚKIB

BŘEZEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Březen 2023 se co do počtu kybernetických incidentů evidovaných NÚKIB stal rekordním měsícem. Překonal ho jen březen roku 2021, kdy útočníci ve velkém zneužívali tehdy novou zranitelnost MS Exchange Server. Drtivá většina nynějších incidentů však z pohledu závažnosti spadala mezi méně významné. Je to dáno především vysokým počtem zaznamenaných DDoS útoků, které neměly vážné dopady a jen krátkodobě narušily dostupnost webových stránek obětí.

V březnovém reportu dále přibližujeme probíhající smishingovou kampaň, která se zaměřuje na širokou veřejnost a jejímž primárním cílem je získat údaje občanů k jejich bankovní identitě. Útočníci v rámci kampaně napodobují domény a webové stránky Ministerstva práce a sociálních věcí ČR, České správy sociálního zabezpečení, Portálu občana nebo České pošty. Kampaň je problematická zejména kvůli své vytrvalosti a poměrně vysoké aktivitě útočníků. Útoky začaly už v srpnu 2022 a pokračují dodnes. Útočníci měsíčně vytvářejí desítky nových domén, které používají ke svým škodlivým aktivitám. Vzhledem k obtížné mitigaci probíhajících útoků doporučujeme zejména obezřetnost na straně uživatele a důsledné prověřování domén. Jakékoliv nové podvodné domény můžete nahlásit na webu StopOnline.cz, provozovaném sdružením CZ.NIC, a případně také Policii ČR.

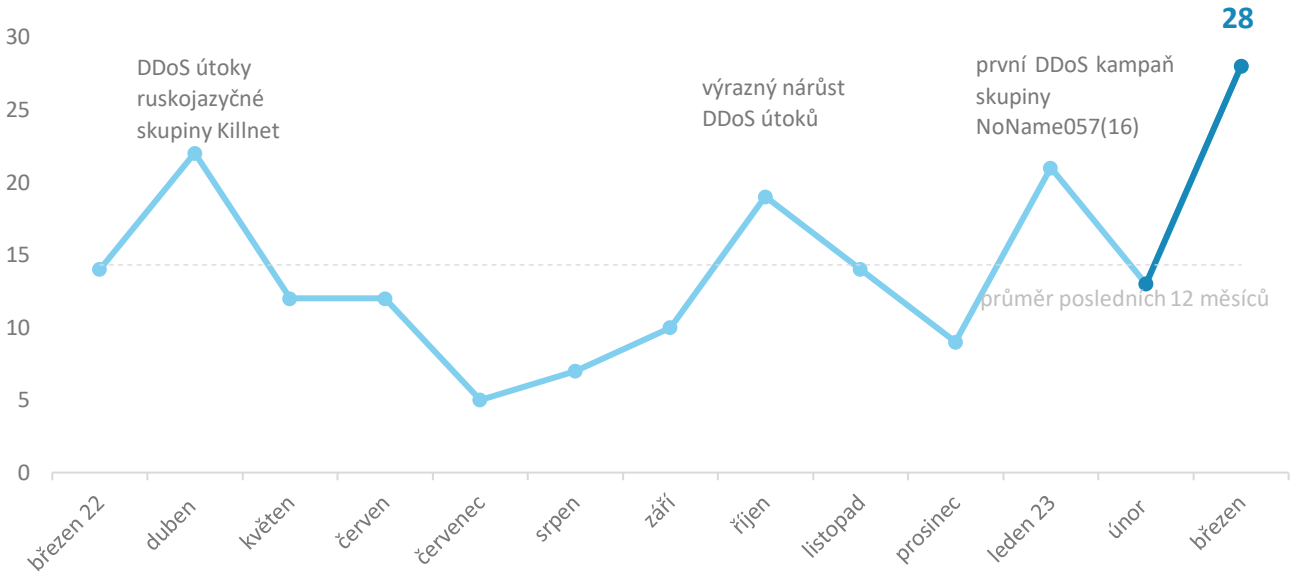
Obsah

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

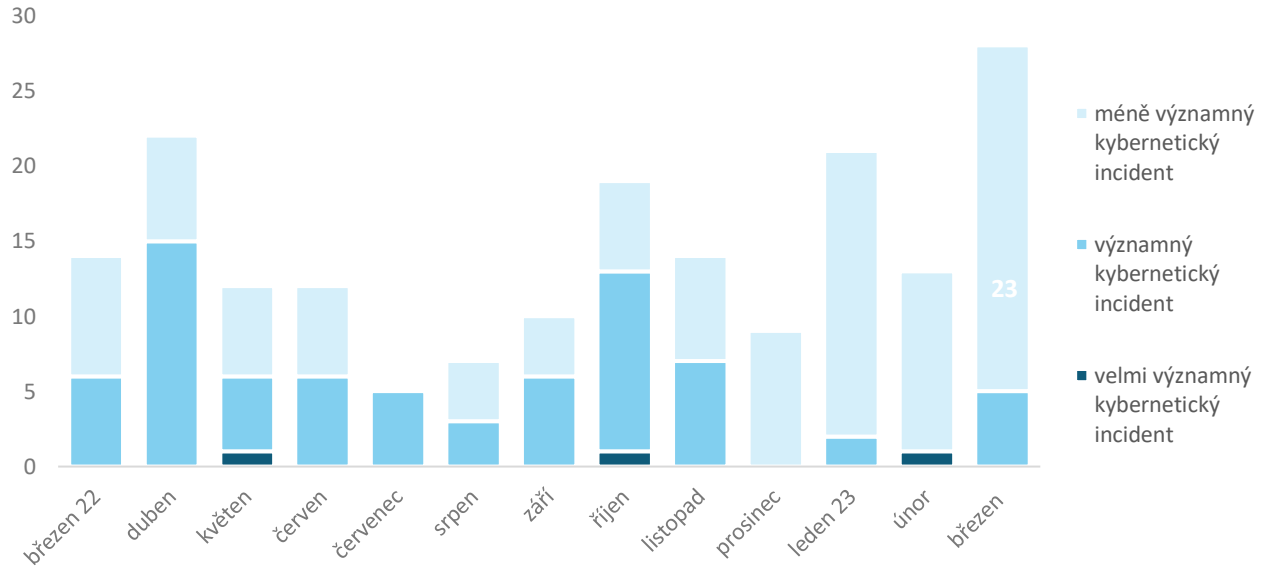
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Březen 2023 byl z hlediska počtu kybernetických incidentů rekordním měsícem. Překonal ho jen březen 2021, kdy útočníci ve velkém zneužívali tehdy novou zranitelnost MS Exchange Server.[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 většinou nemají vážnější dopady a vedou k dočasné nedostupnosti webových stránek napadených organizací.



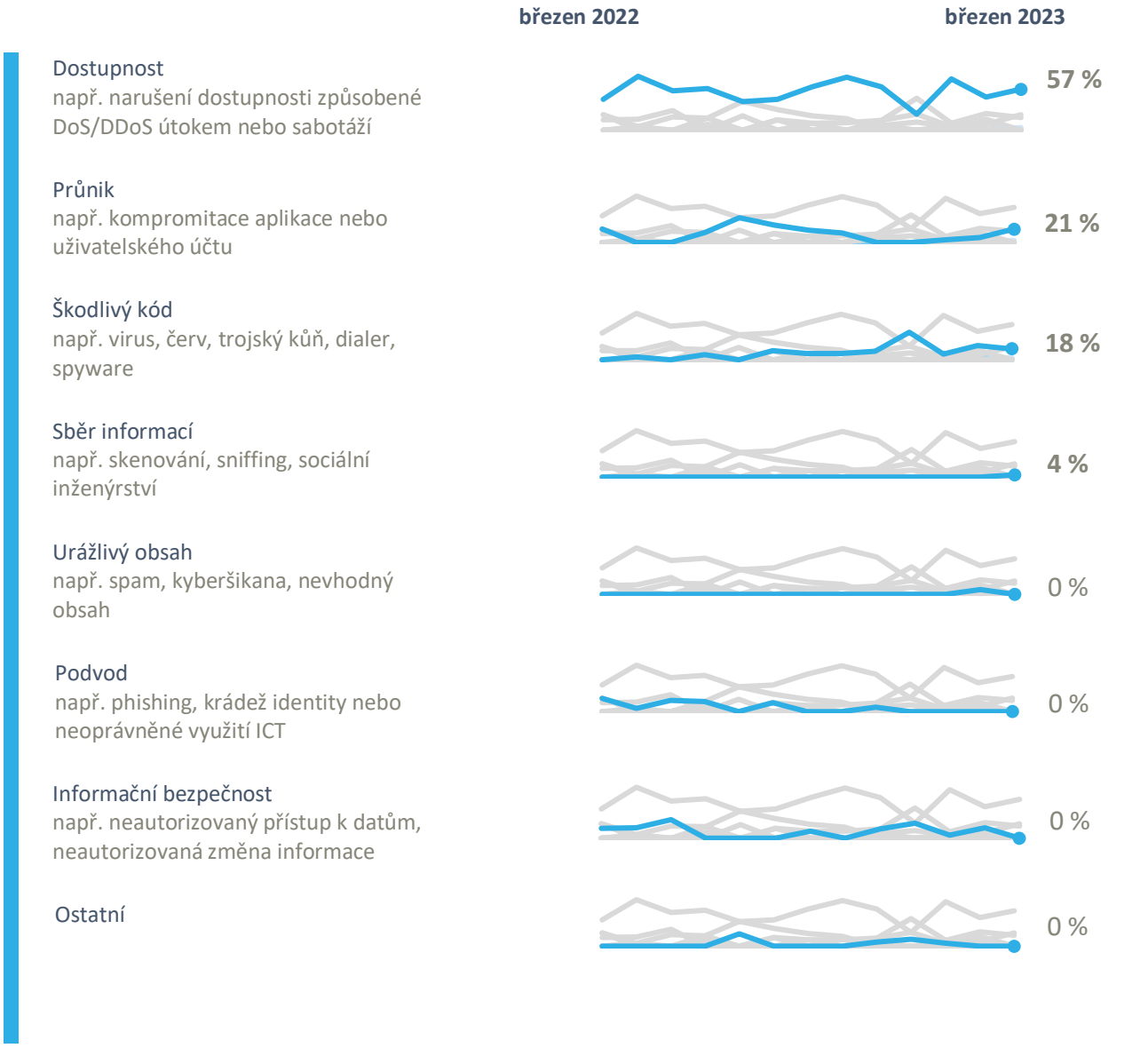
[1] 12 incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývajících 16 incidentů nahlásily NÚKIB neregulované subjekty.

[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]

NÚKIB březnové incidenty zařadil do čtyř kategorií:

- Více než polovinu všech březnových incidentů zapříčinily DDoS útoky, které negativně ovlivnily dostupnost služeb na straně oběti. Jak ukazuje graf níže, narušení dostupnosti se dlouhodobě drží na čele kybernetických incidentů evidovaných NÚKIB;
- Šest organizací v březnu nahlásilo kompromitaci uživatelských účtů. V několika případech kompromitaci předcházel brute-force útok na hesla, kdy útočník zkoušel všechny možné kombinace hesel, dokud se netrefil. Slabá hesla je tímto způsobem možná prolomit během několika sekund;
- Třetí nejčastější kategorií se stal škodlivý kód. Všechny s ním spojené incidenty způsobil ransomware;
- Poslední incident NÚKIB klasifikoval jako sběr informací. Útočník se v tomto případě snažil získat informace o duševním vlastnictví soukromé společnosti tím, že vytvořil bota, který na službu společnosti posílá stovky dotazů denně, a snaží se tak prolomit její algoritmus.



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

Trendy v kybernetické bezpečnosti za březen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

V březnu pokračovala smishingová kampaň, která napodobuje stránky českých státních institucí. První útoky začaly v srpnu 2022 a NÚKIB je kontinuálně eviduje dodnes. Převládajícím vektorem útoku je smishing, tedy forma sociálního inženýrství, kdy uživatel obdrží sms zprávu s odkazem na podvržené webové stránky. Útočníci zprávy posílají široké veřejnosti za účelem finančního zisku. Více informací k celé kampani naleznete v poslední kapitole tohoto reportu.

Malware

Několik organizací ze zdravotnického sektoru v březnu zachytilo phishingové zprávy s přílohou obsahující malware Agent Tesla. Podle textu phishingového e-mailu se ale pravděpodobně jednalo o generickou kampaň, která namísto přesně zamířeného phishingu na zdravotnická zařízení cílila spíše plošně. Agent Tesla je Malware-as-a-Service, který používá celá řada aktérů a v České republice se dlouhodobě řadí k nejčastěji detekovaným škodlivým kódům.

Zranitelnosti

NÚKIB upozornil na novou zranitelnost týkající se aplikace Microsoft Outlook. Zranitelnost CVE-2023-23397 umožňuje útočníkům poslat svým obětem speciálně upravenou e-mailovou zprávu, která nevyžaduje žádnou interakci ze strany oběti, a přitom útočníkovi umožní pohyb v síti napadené organizace. NÚKIB sice zatím neeviduje žádný incident způsobený zneužitím této zranitelnosti, ale pokusy o něj zaznamenal. Více informací ke zranitelnosti samotné i její mitigaci je k dispozici na webových stránkách NÚKIB.

Ransomware

V březnu se zvýšil počet ransomwarových útoků nahlášených NÚKIB. Zatímco v průběhu posledního roku NÚKIB v průměru řešil dva případy ransomwaru měsíčně, tento měsíc došlo k celkem pěti incidentům. Mezi zaznamenanými ransomwary byly mj. LockBit 3.0, LokiLocker a MedusaLocker. LockBit NÚKIB ve svých incidentech řeší nejčastěji.

Útoky na dostupnost

Ruskojazyčná hacktivistická skupina NoName057(16) spustila další vlnu DDoS útoků proti českým cílům. Její útoky se podepsaly na více jak třetině všech incidentů, které NÚKIB v březnu evidoval. Podle vyjádření skupiny na telegramovém účtu jsou její akce odvetou za české kroky podporující Ukrajinu, jako například dodávky zbraní. Zaznamenané DDoS útoky neměly závažnější dopady a vedly pouze k dočasné nedostupnosti webových stránek napadených subjektů.

OT – operační technologie

Agentura pro kybernetickou bezpečnost Evropské unie (ENISA) vydala 21.3. zprávu mapující kyberbezpečnostní hrozby v sektoru dopravy, ve kterém jsou OT komponenty často nasazeny. Ve zprávě jsou zmapovány a analyzovány incidenty v letecké, námořní, železniční a silniční dopravě za období od ledna 2021 do října 2022. Zpráva také přináší hodnocení aktérů hrozeb, motivací útočníků a hlavní trendy pro jednotlivé subsektory. Zprávu je možné stáhnout na odkazu ENISA Transport Threat Landscape.

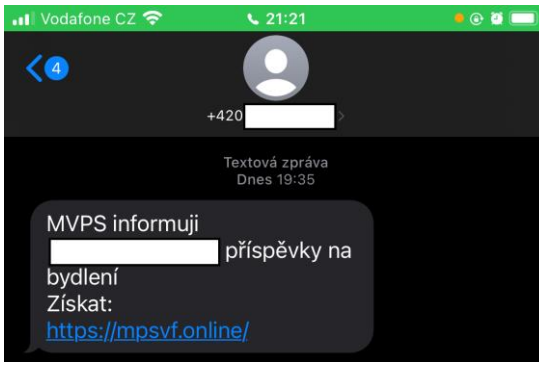
[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Technika měsíce: Smishing

Smishing je převládající vektor útoku u aktuálně probíhající kampaně v ČR, která napodobuje stránky českých státních institucí a snaží se tak z široké veřejnosti získat přihlašovací údaje do jejich bankovnictví. Samotná kampaň je podrobněji popsána v následující kapitole.

Smishing: Název této techniky vznikl spojením slov „phishing“ a „sms“ a napovídá o jejím charakteru. Jedná se o formu sociálního inženýrství, kdy útočníci svým obětem pošlou textovou zprávu, často s odkazem na webovou stránku zdánlivě důvěryhodného zdroje jako například banka nebo pošta. Po otevření odkazu už útok pokračuje jako běžný phishing. Oběť je přesměrována na podvrženou stránku, do které má buď zadat své přihlašovací údaje, nebo se z ní do jejího mobilu stáhne škodlivý kód.

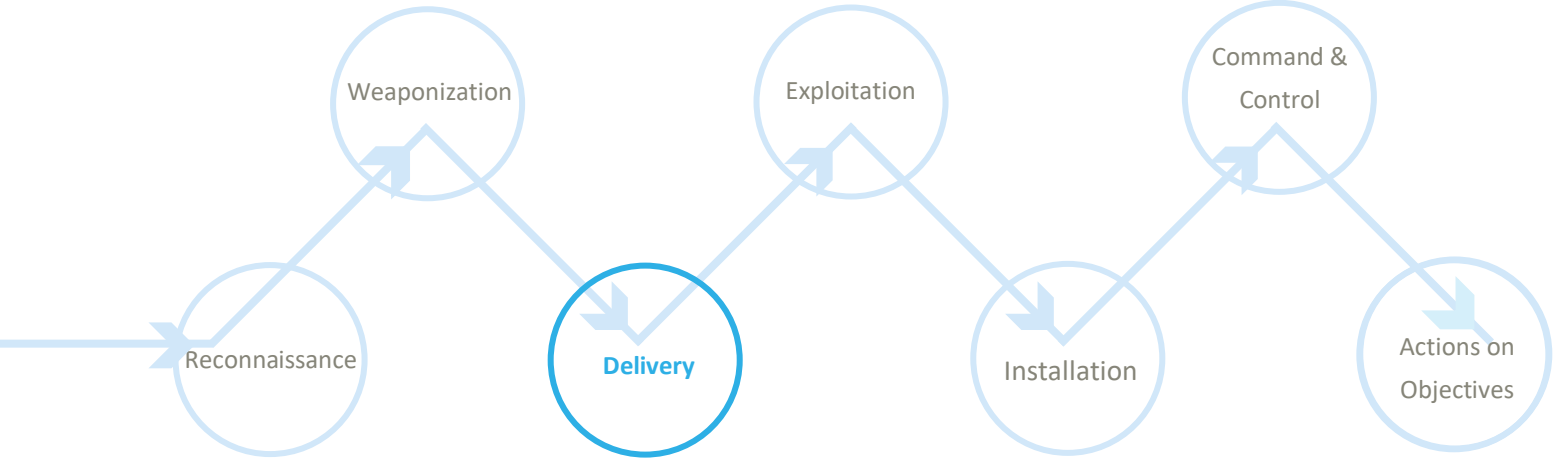
Obr. 1: Redigovaná phishingová SMS zpráva rozesílaná v rámci kampaně popisované v následující kapitole. Útočníci se v tomto případě snažili zvýšit důvěryhodnost textové zprávy tím, že v ní oslovili uživatele jeho jménem.



MITRE ID: T1566

Mitigace: U smishingu doporučujeme zejména obezřetnost na straně uživatele. Doporučujeme věnovat zvýšenou pozornost příchozím zprávám a upozornit na riziko i rodinu a blízké. V případě přihlašování (zejména k bankovnictví) vždy prosím důsledně prověřujte, zda jde skutečně o legitimní adresu. Pokud ne, nahlašte ji prosím sdružení CZ.NIC, které škodlivé domény blokuje.

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



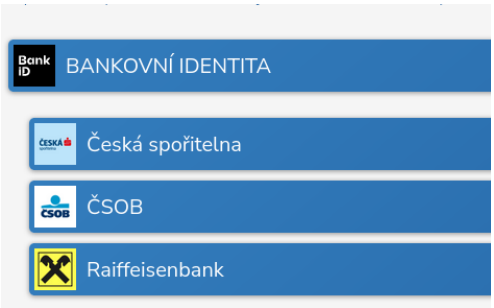
Zaměřeno na hrozbu: Smishingová kampaň napodobující stránky českých státních institucí

NÚKIB dlouhodobě zaznamenává finančně motivovanou smishingovou kampaň, která se zaměřuje na širokou veřejnost a jejímž primárním cílem je získat údaje občanů k jejich bankovní identitě. Útočníci v rámci kampaně napodobují domény i webové stránky Ministerstva práce a sociálních věcí ČR, České správy sociálního zabezpečení, Portálu občana nebo České pošty. Zneužívají přitom například motivy nabídky příspěvků na bydlení, vyplácení sociálních dávek či výzvy k založení datové schránky.

Útočníci většinou postupují následovně:

1. V prvním kroku kampaně rozesílají phishingové SMS zprávy s různými motivy, které obsahují hypertextové odkazy (viz Obr. 1 na předchozí straně). Tyto odkazy typicky imitují domény českých státních institucí. Například v případě MPSV dochází k vytváření domén s různými obměnami typu ceska-mpsv[.]cz, mpsv-egov[.]online, mpsv[.]info apod.
2. Po kliknutí na přiložený odkaz je oběť přesměrována na podvržené stránky imitující web příslušné instituce s možností přihlášení přes bankovní identitu (viz Obr. 2). Falešné webové stránky jsou vizuálně velmi dobře připravené. Obsahují nejen oficiální loga institucí, ale i téměř identickou grafickou podobu.

Obr 2: Screenshot z podvržených webových stránek



3. V případě přihlášení oběti do podvržené bankovní identity útočníci využijí její údaje k přihlášení do legitimního bankovnictví, čímž dojde k zaslání výzvy pro dvoufázové ověření. Možnost úspěšného zneužití údajů pro přihlášení do internetového bankovnictví není příliš pravděpodobná (15–20 %) díky dvoufaktorovému ověření při přihlašování. Existuje však reálná možnost (25–50 %), že útočníci tyto údaje mohou dále přeprodávat. V některých případech docházelo také k přesměrování oběti na další stránku s výzvou k zadání údajů k platební kartě. Po zadání těchto údajů pak útočníci odváděli finanční prostředky prostřednictvím vybrané platební brány.

Kampaň je problematická zejména kvůli své vytrvalosti a poměrně vysoké aktivitě útočníků. NÚKIB na kampaň upozorňoval v srpnu 2022, kdy útočníci začali mířit na české cíle. Kampaň od té doby ale stále pokračuje. Útočníci průběžně vytvářejí nové domény pro podvržené stránky, jen nyní v březnu takových domén vytvořili více než sedm desítek. Ačkoli sdružení CZ.NIC nově vytvářené domény postupně blokuje, útočníci stále tvoří nové. Velká část nových stránek navíc vzniká mimo českou národní (.cz) doménu, kde CZ.NIC k blokaci nemá kompetence.

Vzhledem k obtížné mitigaci doporučujeme zejména obezřetnost na straně uživatele. Oficiální web pro podání žádosti na příspěvek na bydlení se nachází pouze na adrese https://www.mpsv.cz/web/cz/-/prispevek-na-bydleni. Jakékoliv nové podvodné domény můžete nahlásit na webu StopOnline.cz, provozovaném sdružením CZ.NIC, a případně také Policii ČR.

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.