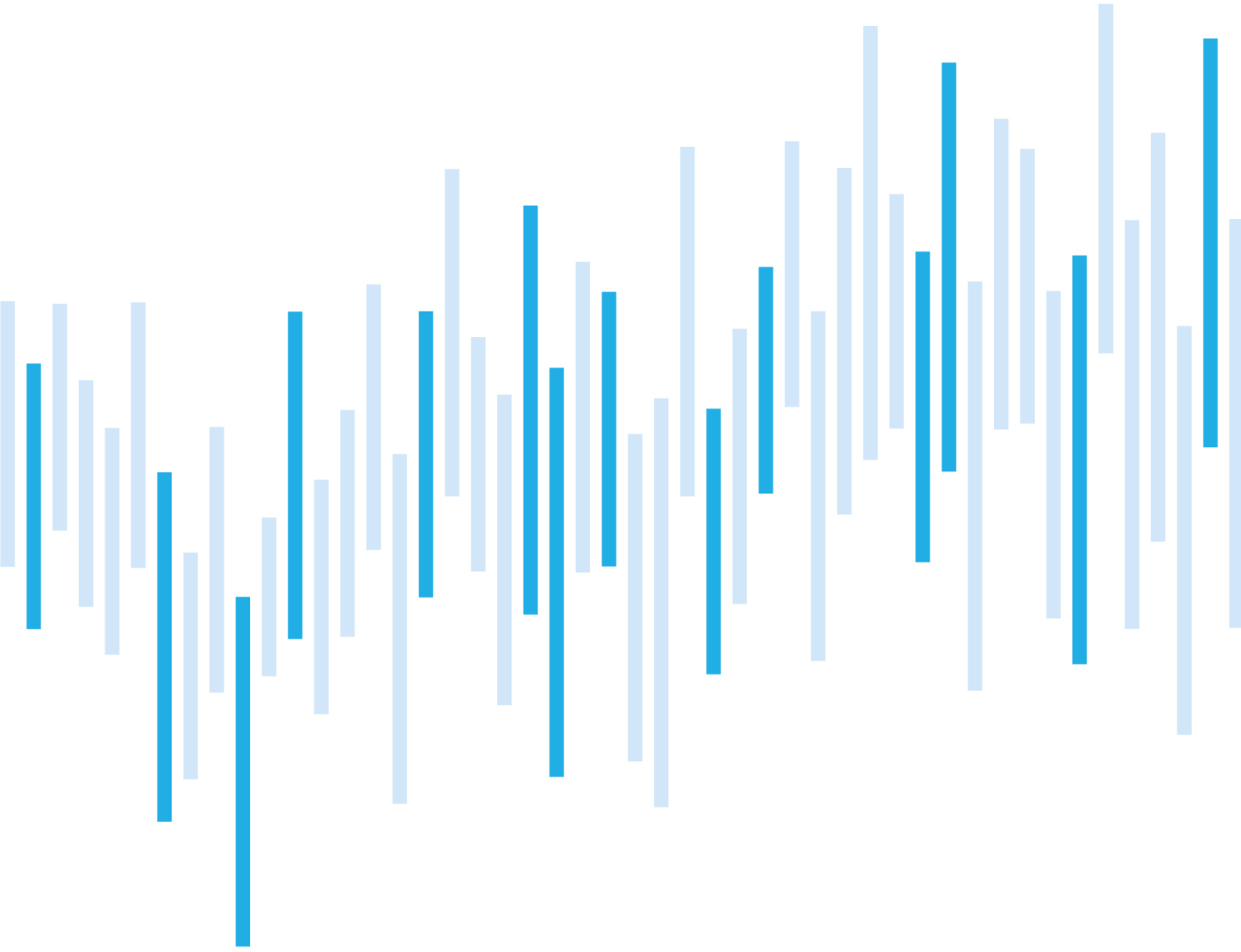
Kybernetické incidenty pohledem NÚKIB

BŘEZEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

NÚKIB stále v České republice neeviduje žádný incident, který by byl prokazatelně spojený s válkou na Ukrajině. Situaci ale stále monitorujeme a vyhodnocujeme případné kybernetické hrozby pro ČR. I proto NÚKIB v březnu vydal Varování související s ekonomickými sankcemi proti Ruské federaci.

Do březnových incidentů se opět promítly phishingové kampaně a ransomware. Každá z těchto kategorií tvořila pětinu incidentů.

Případy phishingu, které NÚKIB evidoval, nebyly nijak výjimečné. Nicméně na kybernetické scéně se objevila nová technika Browser-in-the-Broswer, která dělá phishing obtížně rozeznatelným. Popisujeme ji v kapitole „Technika měsíce“.

Jeden z březnových ransomwarových útoků se odlišoval od ostatních. Útočník tentokrát nezašifroval stanice a servery pomocí škodlivého kódu, ale legitimním nástrojem Bitlocker. V poslední kapitole podrobně rozebíráme chování útočníka.

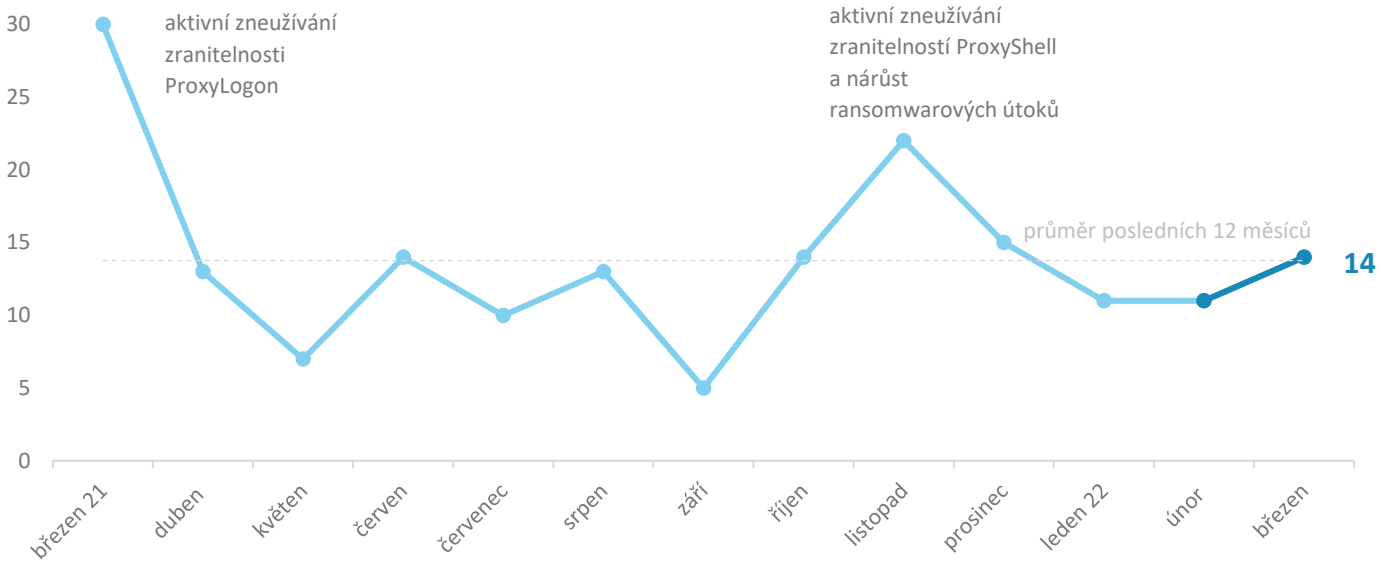
Obsah

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.

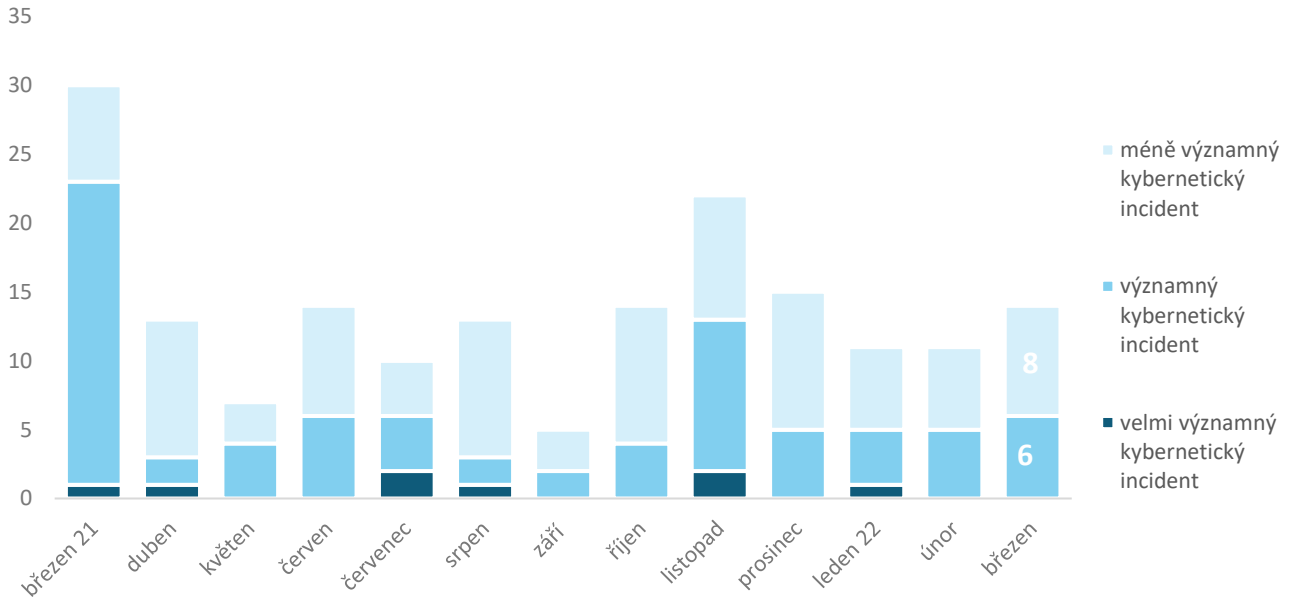
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Z hlediska počtu byl březen se 14 incidenty průměrným měsícem posledního roku.[1]



Závažnost řešených kybernetických incidentů[2]

Březen se z hlediska závažnosti incidentů podobal většině měsíců posledního roku. Žádný incident neměl natolik závažné důsledky, aby mu NÚKIB přiřadil nejvyšší možnou závažnost, většina incidentů byla méně závažného charakteru. Do těch s významnějšími dopady se propsaly především ransomwarové útoky, které omezily fungování napadených subjektů.

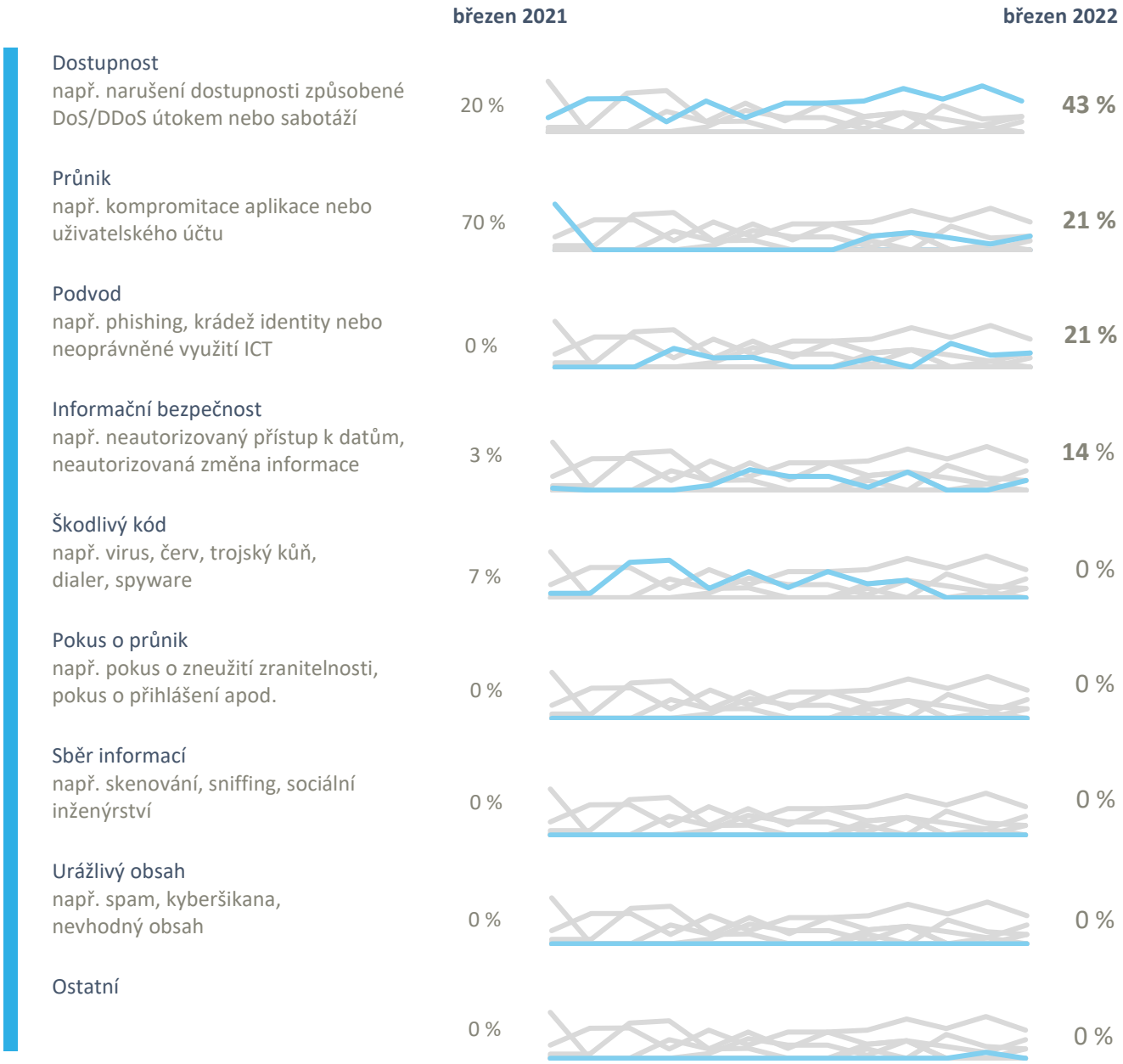


[1] Polovinu incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých sedmi incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Březnové incidenty byly rozloženy do tří kategorií:

- Šest incidentů vyústilo v nedostupnost služeb. Za polovinou z nich stála technická chyba, ne cílený útok. Ve dvou případech pak ovlivnil fungování organizací ransomware, který na čas vyřadil napadené systémy z provozu. Za poslední nedostupností systémů napadené organizace stojí DDoS útok;
- Druhou a třetí nejčastější kategorií byly průniky a podvody. Do podvodů se promítly incidenty, ve kterých neznámí útočníci kompromitovali e-mailové schránky a z nich dál rozesílali phishing a spam dalším institucím;
- Poslední březnovou kategorií se stala informační bezpečnost. Spadl do ní i poslední ze tří březnových ransomwarových útoků, při kterém se útočníkům podařilo exfiltrovat data oběti. Útočník použil tzv. double-extortion, kdy oběti vyhrožoval nejen ztrátou dat, ale také jejich zveřejněním.



[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

NÚKIB v březnu řešil tři případy, během nichž útočníci zneužili přihlašovacích údajů k e-mailovým schránkám a z nich následně rozesílali další spam a phishing. Ve srovnání s předchozími třemi měsíci se jedná o setrvalý trend, kdy phishing tvoří zhruba pětinu incidentů NÚKIB (viz graf „Podvod“ na str. 3).

V jedné z napadených společností útočník navázal na historickou konverzaci mezi jejím zaměstnancem a klientem. Klienta následně kontaktoval z podvržené e-mailové adresy, která se legitimní adrese zaměstnance podobala, a pokusil se s klientem domluvit změnu bankovního účtu, na který klient vyplácí faktury.

Malware

Kromě níže zmíněných ransomwarů se v březnových incidentech neobjevil žádný jiný škodlivý kód.

Zranitelnosti

NÚKIB začal v březnu monitorovat nově zveřejněné zranitelnosti v průmyslových automatizačních systémech. Prozkoumal více než 500 upozornění, které byly vydané v roce 2021, a objevil 111 zařízení, která jsou umístěna v ČR, dostupná z internetu a pravděpodobně zranitelná. Žádné z těchto zařízení se nenacházelo v regulovaném systému dle ZKB. NÚKIB přesto kontaktoval providery, kteří mají tato zařízení ve své síti, a na výskyt možné zranitelnosti je upozornil.

Ransomware

Podobně jako minulý měsíc stojí za pětinou březnových incidentů ransomware. Stojí za nimi jak velké organizované kriminální skupiny (LockBit), tak menší aktéři cílící na malé a střední podniky.

V jednom z březnových případů útočník nepoužil k šifrování dat žádný škodlivý kód, ale legitimní nástroj Bitlocker. Více informací k tomuto útoku je k dispozici na straně 7.

Útoky na dostupnost

Mezi březnovými incidenty byl jeden úspěšný DDoS útok, který se napadenému subjektu podařilo zvládnout vlastními prostředky. Na útoku bylo zajímavé, že ho doprovázel vyděračský e-mail, ve kterém útočníci za zastavení útoku požadovali 4000 USD. Vyhrožovali také, že pokud oběť nezaplatí, zveřejní její data. K žádné exfiltraci dat ze sítě oběti ale nedošlo, útočníci se do sítě oběti vůbec nedostali. Na konci e-mailu se útočníci podepsali jako DarkSide. Vzhledem k tomu, že ale skupina DarkSide už zanikla, nelze vyloučit, že se někdo na jejím jméně přiživuje.

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

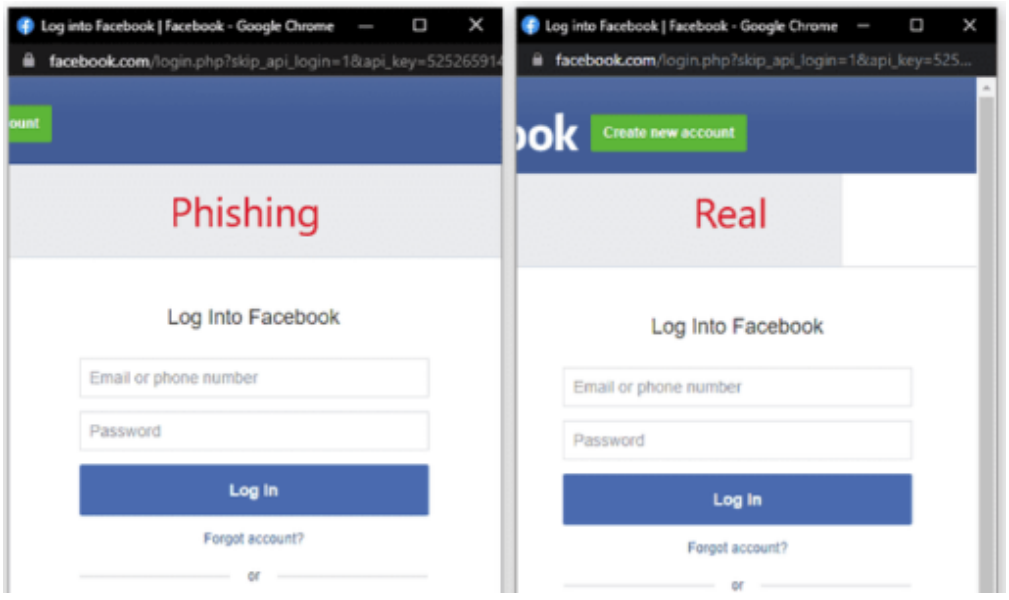
Technika měsíce: Browser-in-the-Browser

Podobně jako v předchozích měsících převažovaly v březnových incidentech techniky spojené s phishingem. V souvislosti s phishingem se v březnu na kybernetické scéně objevila nová technika Browser-in-the-Browser, která je pro běžného uživatele těžko rozpoznatelná. V rámci MITRE ATT&CK spadá pod T1204.001: User Execution: Malicious Link. NÚKIB se s ní zatím ve svých incidentech nesetkal, ale jelikož ji útočníci v posledním měsíci používali při útocích na ukrajinské cíle, nelze vyloučit, že se vzhledem k české aktivní podpoře časem objeví i v námi zaznamenaných incidentech.

Technika **Browser-in-the-Browser (BITB)** je metoda phishingu, kterou se útočníci snaží odcizit přihlašovací údaje obětí. Mnoho online služeb využívá k přihlášení Single Sign-on třetí strany, nejčastěji Google, Apple, Microsoft nebo Facebook, tedy ty účty, ke kterým se útočník snaží získat přístup. V běžném případě se uživateli po kliknutí na přihlášení otevře nové okno prohlížeče s polem pro přihlašovací údaje k jeho účtu. V případě Browser-in-the-Browser ale po kliknutí dojde k otevření falešného přihlašovacího okna, které imituje podobu a chování prohlížeče. Jde pouze o interaktivní objekt vytvořený pomocí HTML, CSS a Javascriptu. Tímto způsobem útočník může zneužít i kód z dvoufaktorového ověření, pokud ho má uživatel zapnuté.

Pečlivě připravený phishing vytvořený pomocí této techniky může být vizuálně zcela nerozpoznatelný od skutečného přihlašovacího boxu, a to včetně URL v adresním řádku "okna" a indikace HTTPS spojení, což ještě více přidává na věrohodnosti (obr. 1). Nelze spoléhat ani na zobrazení cílové URL po najetí kurzorem na tlačítko s odkazem, tuto informaci lze taktéž pomocí Javascriptu podvrhnout.

Obrázek 1

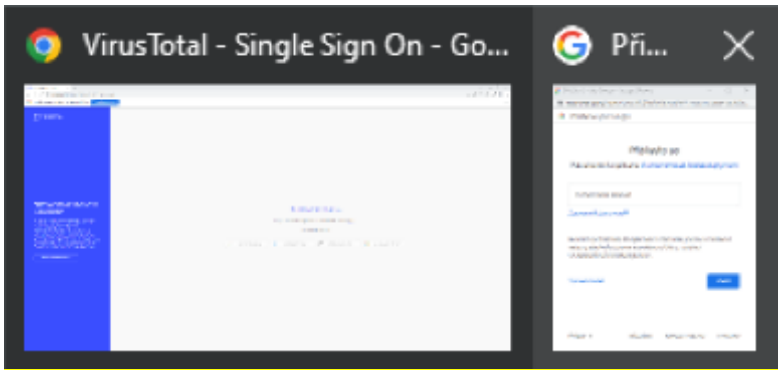


Zdroj: Browser In The Browser (BITB) Attack | mr.d0x (mrd0x.com)

Mitigace: BITB je možné rozpoznat následujícím způsobem:

- V případě, že přihlašovací box vytáhnete mimo aktuální otevřený prohlížeč, otevře se nové okno (obr. 2). Falešné okno ale nelze narozdíl od skutečného přemístit nebo zvětšit mimo plochu aktuální stránky (obr. 3);

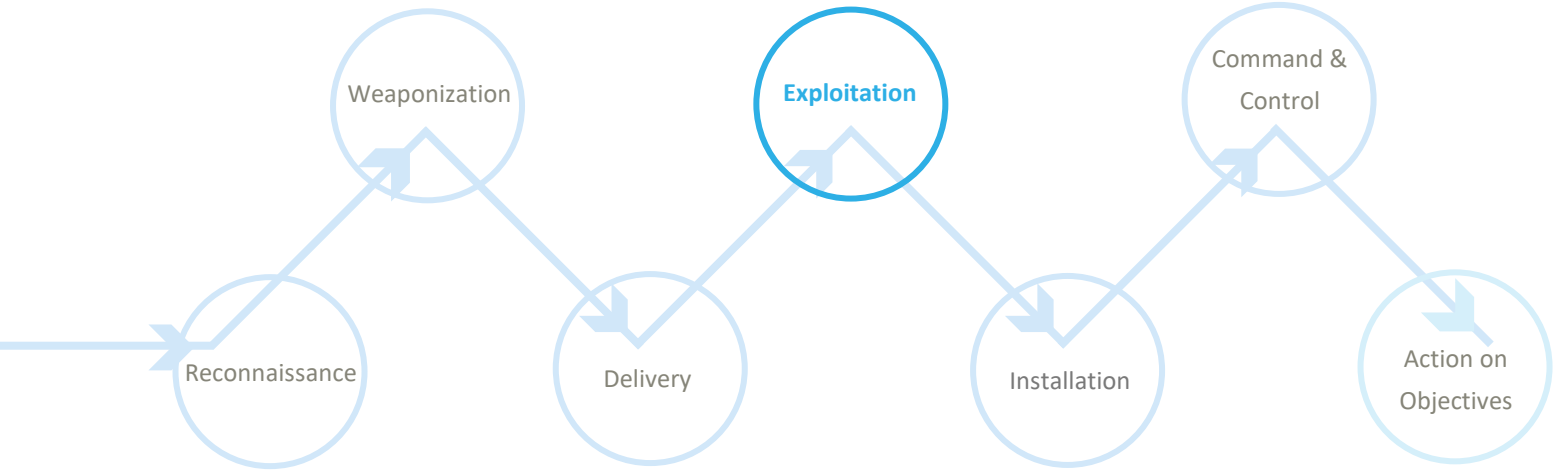
Obrázek 2



Obrázek 3

- Skutečný přihlašovací dialog otevře nové okno prohlížeče, což lze ověřit v panelu spuštěných aplikací. Pokud běží pouze jedna instance prohlížeče, může jít o podvod;
- Ověřte, jestli podoba přihlašovacího okna odpovídá vašemu operačnímu systému a vizuálnímu schématu prohlížeče a zda je dialog ve vašem jazyce;
- Ikona indikující HTTPS je v podvrženém okně pouze vizuální prvek, ve skutečném lze po kliknutí na ni zobrazit certifikát stránky.

Znázornění BITB kill chainu, který ukazuje, ve které fázi útočníci techniku používají:



Zaměřeno na incident: Ransomware ve veřejné správě

Jeden z březnových ransomwarových útoků se odlišoval od většiny případů, které NÚKIB řeší. Na rozdíl od ostatních incidentů útočník tentokrát nezašifroval stanice a servery pomocí škodlivého kódu, ale legitimním nástrojem Bitlocker, který chrání data uložená na discích uživatelů před neoprávněným zneužitím.

Obětí tohoto útoku se stala organizace veřejné správy. Útočníku se podařilo zašifrovat přibližně 10 % jejích uživatelských stanic a několik serverů. Ve vzkazu, který oběti zanechal vytisknutý v tiskárně, vyhrožoval, že pokud nedostane zaplaceno, její data také zveřejní. NÚKIB zatím nestanovil, jestli k exfiltraci dat skutečně došlo, jelikož analýza dat z postupně obnovovaných logů ze starších záloh stále probíhá. Napadená organizace se o útočníku dozvěděla ve chvíli, kdy začal šifrovat disky a servery.

Jelikož analýza incidentu stále probíhá, NÚKIB ještě nemá k dispozici veškeré potřebné informace, na jejichž základě by mohl učinit přesné závěry o cíli a motivaci útočníka. I z toho důvodu nemůžeme v současné chvíli incident připsat konkrétnímu aktéru.[5]

Pro větší představu o chování útočníka jsme dosavadní poznatky z incidentu zasadili do cyber kill chainu:

Recoinnassance

Vzhledem k nedostatku dat nemůže NÚKIB určit, zda útočník před napadením organizace aktivně skenoval její vnější prostředí. Nelze ani vyloučit, že útočník v prvotní fázi hledal informace o oběti v otevřených zdrojích a následně je použil k phishingové kampani. Napadenou organizací je veřejná instituce, která má ze své podstaty řadu potenciálně využitelných informací jako jména a kontakty na klíčové zaměstnance veřejně dostupné.

Weaponization

Jelikož není znám prvotní vektor útoku, nemá NÚKIB k této fázi kill chainu potřebné informace.

Delivery

Z aktuálně dostupných dat nelze s jistotou potvrdit, jak útočník získal prvotní přístup do sítě organizace. Zatím nejpravděpodobnější možností je zneužití zranitelnosti ProxyShell na Microsoft Exchange serveru. Server byl touto zranitelností prokazatelně kompromitován už v srpnu minulého roku, což potvrdily nálezy webshellů. Nemůžeme ale vyloučit, že se jedná o separátní útoky a útočník se do sítě oběti dostal jiným způsobem.

[5] Některá data z incidentu se překrývají s touto analýzou: Exchange Exploit Leads to Domain Wide Ransomware (thedfirreport.com)

Exploitation

Pokud by se útočník dostal do sítě oběti zneužitím zranitelnosti ProxyShell, pak by mu to umožnilo spustit na serveru kód s oprávněním administrátora a v dalším kroku si založit účet pro persistenci. NÚKIB v současnosti analyzuje, zda je tato hypotéza pravdivá.

Installation

Útočník si v systému založil účet *DefaultAccount*, který je v nových verzích Windows nativně přítomný. Ve starší verzi Serveru, kterou používala oběť, legitimně neexistoval a útočník ho pravděpodobně takto pojmenoval, aby při běžném pohledu jeho přítomnost nebudila podezření. Následně do systému přenesl a spustil soubor *dllhost.exe*, který v sobě obsahoval funkcionalitu běžně dostupného nástroje *Fast Reverse Proxy* pro zahájení spojení s řídícími servery a pohyb v síti.

Dvě hodiny po založení účtu útočník přenesl nástroj na doménový řadič a získal oprávnění doménového administrátora. Je pravděpodobné, že se k přihlašovacím údajům doménového administrátora dostal dumpem z LSASS procesu poté, co se na řadič přihlásil servisní technik.

Pomocí Plánovače úloh a skriptu CacheTask.bat si útočník vytvořil persistenci k automatické instalaci a spouštění nástroje *Fast Reverse Proxy* pro komunikaci s řídícím serverem.

Command and Control

Kvůli nainstalovanému nástroji *Fast Reverse Proxy* se útočník mohl opakovaně vracet do napadené sítě a podnikat v ní další kroky. S řídícím serverem komunikoval skrze RDP spojení tunelovaným přes port 443 z adres *148.251.71[.]182* a *107.173.231[.]114*.

Actions on Objectives

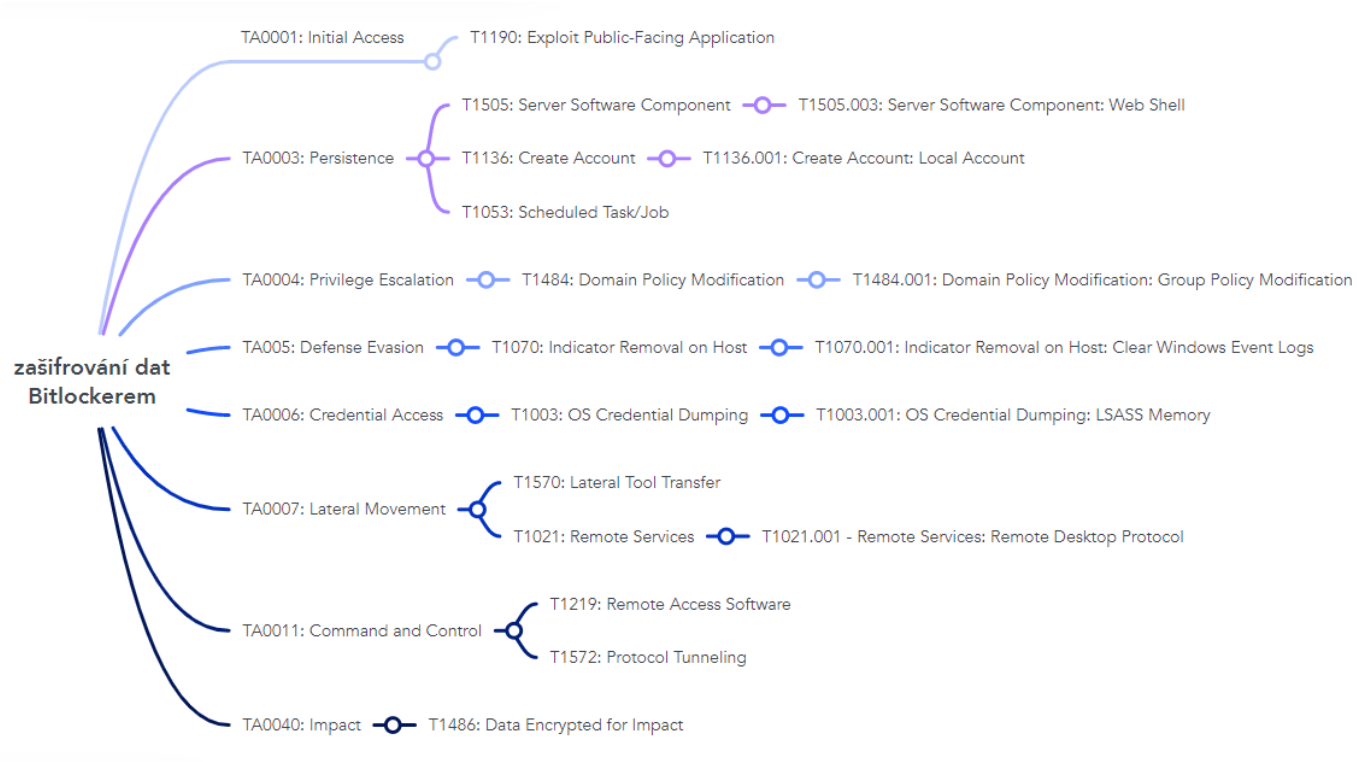
Útočník pod účtem doménového administrátora vymazal z doménového řadiče event logy.

V průběhu března spustil šifrování doménových strojů pomocí legitimního nástroje Bitlockeru. Administrátoři šifrování rychle zaznamenali kvůli velkému zatížení sítě a na většině strojů ho úspěšně zastavili. Útočník mezitím stihl vyřadit z provozu přibližně 10 % uživatelských stanic a několik serverů.

Během šifrování zanechal útočník vyděračskou zprávu s kontaktním e-mailem *jolyoga@yandex.com*. Její podoba ale nepůsobí přesvědčivě a nelze vyloučit, že cílem bylo pouze způsobení škody a zničení stop, nikoliv vymáhání platby.

Z dosud dostupných dat není zřejmé, zda docházelo k exfiltraci dat. Analýza aktivit v mezičase probíhá z postupně obnovovaných logů ze starších záloh.

Zde je seznam MITRE ATT&CK technik, které útočník ve svých aktivitách proti české instituci veřejné správy použil:



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. Původce informace může rozsah sdílení dále omezit.
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:WHITE	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.