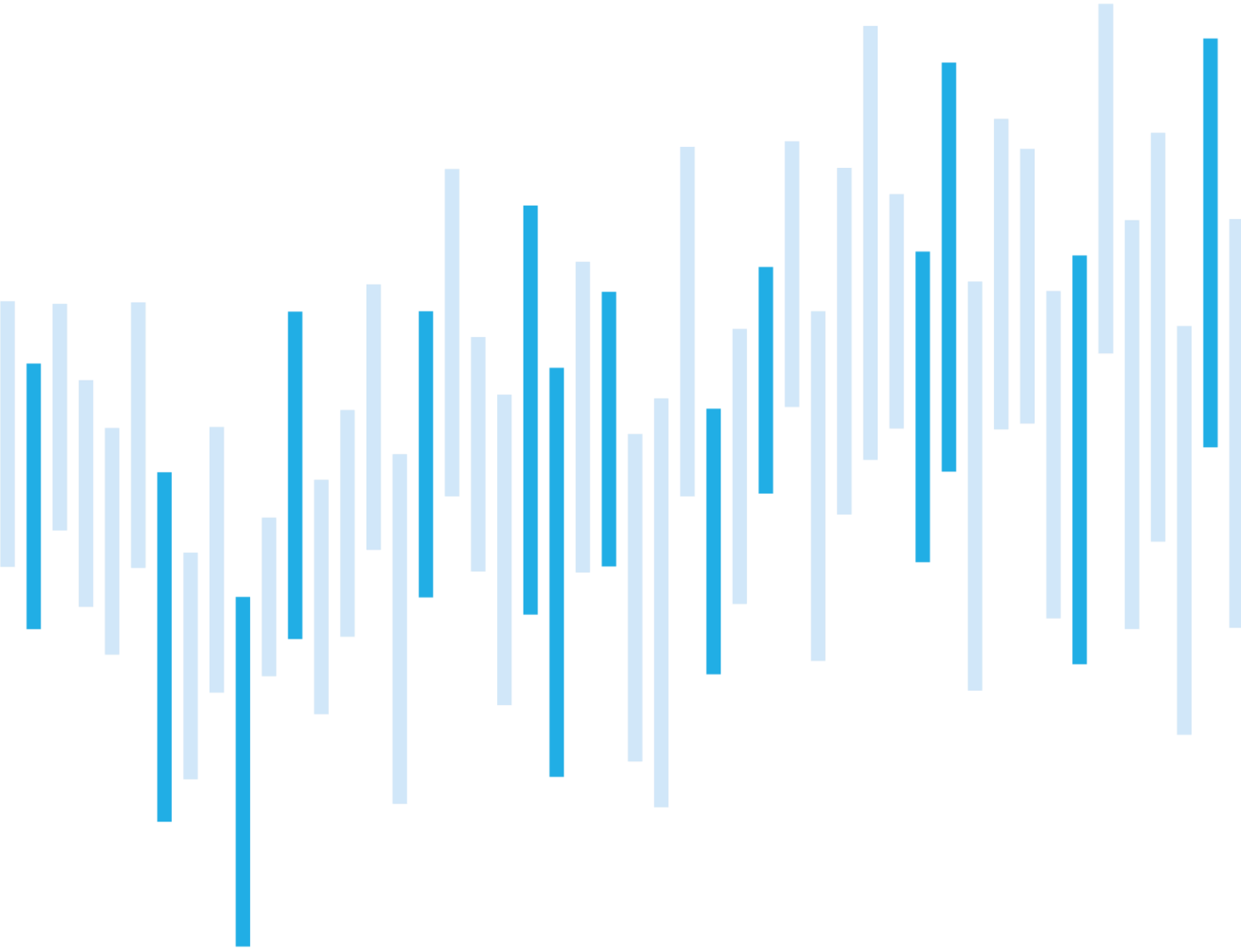
Kybernetické incidenty pohledem NÚKIB

ÚNOR 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Kyberbezpečnostní komunita v únoru upřela svou pozornost na dění na Ukrajině. Česká republika zatím nemá potvrzený žádný incident, který by byl s válkou prokazatelně spojený. Nicméně v době okolo zahájení ruské invaze probíhalo v ČR plošné skenování portů, včetně skenování vládních organizací a kritické infrastruktury. Útočníci velmi pravděpodobně hledali slabá místa v zabezpečení českých cílů, kterých by mohli později využít k návazným kybernetickým útokům. Jak argumentujeme na straně 6, nelze vyloučit, že toto skenování s válkou na Ukrajině souvisí.

Vzhledem současnému vývoji hodnotíme, že narostla hrozba kybernetické špionáže, DDoS či ransomwarových útoků. Nelze ani vyloučit, že kybernetický útok na ukrajinské cíle (např. wiperem) se neúmyslně přelije i do ČR. Vzhledem k těmto hrozbám vydal NÚKIB 25. února 2022 Varování, ve kterém dává organizacím doporučení, jak se těmto konkrétním kybernetickým hrozbám bránit. Varování také obsahuje seznam technik, které útočníci nejčastěji používají, včetně odkazů, jak tyto techniky mitigovat.

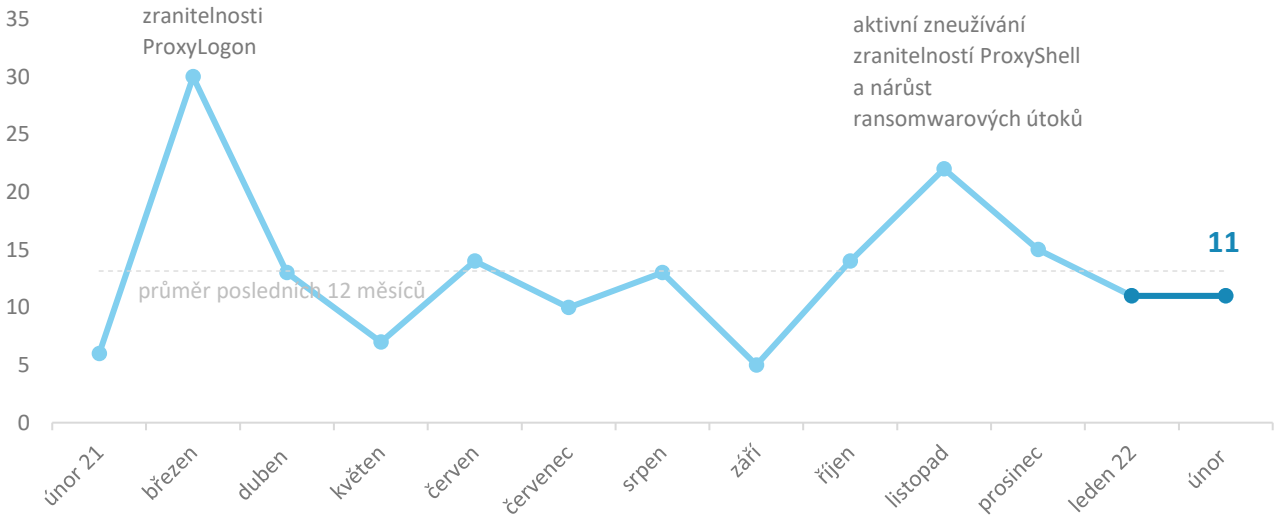
Obsah

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.

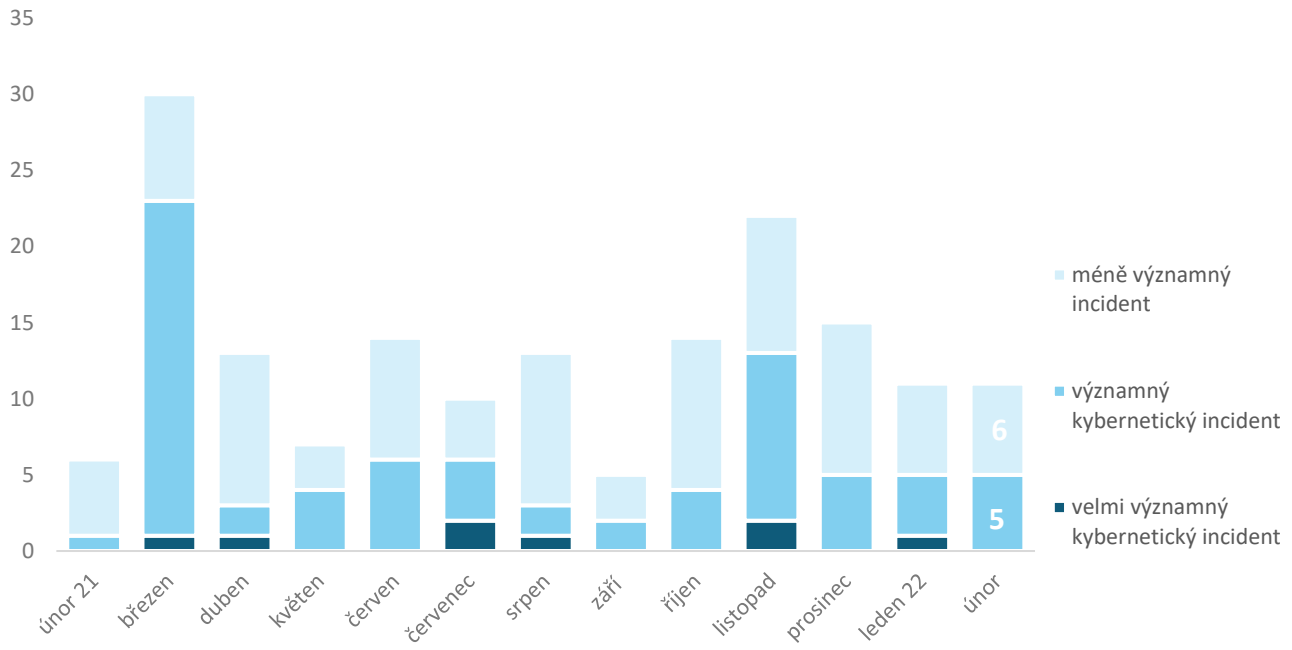
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Únor s 11 kybernetickými incidenty zůstal z hlediska počtu lehce podprůměrným měsícem.[1]



Závažnost řešených kybernetických incidentů[2]

NÚKIB neklasifikoval žádný z únorových incidentů jako velmi významný. Do incidentů s významnějšími dopady se propsaly především ransomwarové útoky, které omezily fungování napadených subjektů.

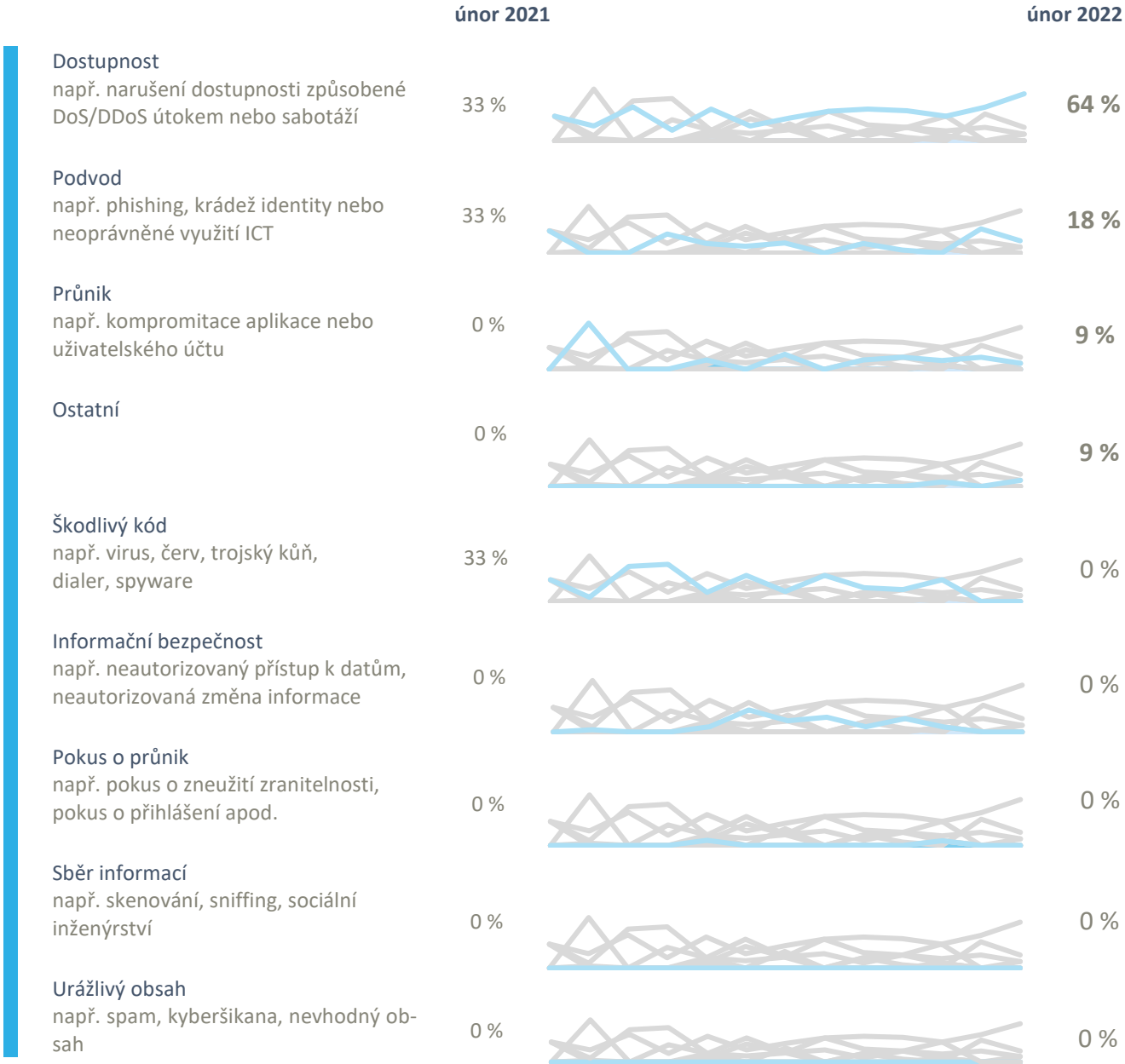


[1] Čtyři incidenty nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých sedmi incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Únorové incidenty byly rozloženy do čtyř kategorií:

- Téměř dvě třetiny incidentů skončily nedostupností služeb. Fungování napadených systémů v únoru ovlivnily ransomware, které vedle dat zašifrovaly i zálohy obětí. Dále se pak do dostupnosti propsaly DDoS útoky nebo technická chyba;
- Druhou nejčastější kategorií byly se dvěma incidenty podvody. Stály za nimi úspěšné phishingové kampaně. U dvou organizací se útočníkům podařilo získat přihlašovací údaje zaměstnanců napadených organizací a následně z kompromitovaných schránek rozesílat phishing dalším adresátům;
- Poslední dva incidenty NÚKIB klasifikoval jako průnik a „ostatní“.



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

Trendy v kybernetické bezpečnosti za únor pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Zaměstnanci české vládní instituce obdrželi na konci února phishing s ukrajinskou tématikou. Žádný z nich ale škodlivý odkaz se souborem ve formátu .zip neotevřel a ke kompromitaci nedošlo. Útočník se snažil vzbudit dojem, že e-mail přišel z Evropské rady a odkazoval na analýzu současné situace. Na základě informací od partnerů a vlastní analýzy víme, že stejný útočník rozesílá phishingové e-maily i dalším evropským vládním organizacím. Vzhledem k aktuálnosti tématu je velmi pravděpodobné, že phishigových kampaní s ukrajinskou tématikou bude dále přibývat.

Malware

ESET identifikoval dva destruktivní malwary HermeticWiper a IsaacWiper, které 23. a 24. února útočily na ukrajinské cíle. Dle vyjádření ESET „se útoky vyznačují pečlivou přípravou a dle posledních dat vše nasvědčuje tomu, že byly plánovány několik měsíců.“ V České republice nebyla v únoru aktivita těchto škodlivých kódů zjištěna, ale do budoucna takovou možnost nelze vyloučit, ať už jako neúmyslné přelití do dalších systémů nebo jako cílený útok proti zemím aktivně podporujícím Ukrajinu. HermeticWiper objevili i v lotyšských a litevských systémech.

Zranitelnosti

S tím, jak se zvyšuje hrozba kybernetických útoků, roste i pravděpodobnost zneužívání zranitelností. NÚKIB ve Varování vydaném 25. února identifikoval 14 nejčastějších zranitelností, jež často aktéři zneužívají. Ve vztahu k těmto zranitelnostem NÚKIB ve Varování českým organizacím doporučuje prověřit přítomnost vyjmenovaných potenciálně zranitelných systémů ve své infrastruktuře a zkontrolovat jejich aktuálnost.

Ransomware

NÚKIB v únoru řešil tři incidenty spojené s ransomwarem. Jeho oběťmi se staly česká soukromá společnost a zdravotnické zařízení.

I v případě ransomwaru platí zvýšené riziko související s invazí na Ukrajinu. Na ruskou stranu se přidaly některé ransomwarové skupiny a hrozí státům, které budou prostřednictvím kyberprostoru ohrožovat Rusko.

Útoky na dostupnost

NÚKIB v únoru evidoval dva DDoS útoky. První z nich, který byl typu HTTP flood, vyústil ve dvouhodinovou nedostupnost webového serveru napadené organizace. Druhý útok byl typu SYN flood a znepřístupnil webové stránky oběti na půl hodiny. Ani jeden z těchto útoků nespojujeme s děním na Ukrajině. Vzhledem k aktuálnímu rozšíření DDoS útoků proti ukrajinským cílům ale nelze do dalšího měsíce vyloučit ani jejich případné použití proti českým organizacím.

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

Technika měsíce: Phishing

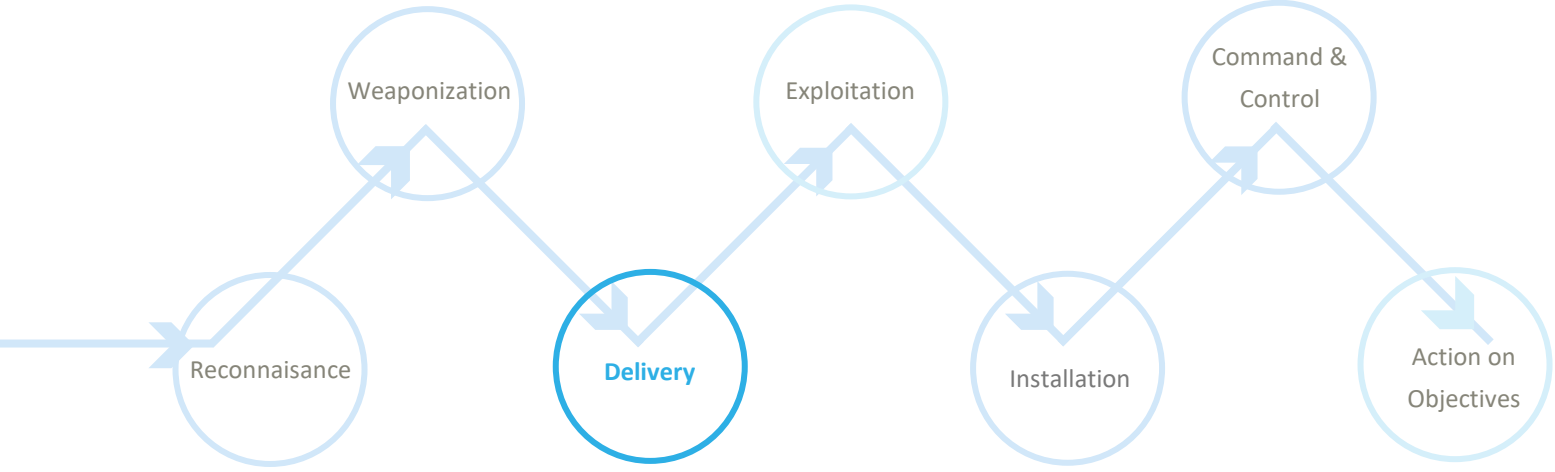
NÚKIB kybernetické incidenty vyhodnocuje také na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V únorových incidentech se nejčastěji objevil phishing. Je navíc pravděpodobné, že phishingových kampaní bude v následujících měsících přibývat. Phishing často bývá vstupní branou útočníků do systémů obětí. Proto je pravděpodobné, že s rostoucí hrozbou kyberšpionáže a destruktivních útoků vzroste i počet phishingových e-mailů.

Phishing je technika, při níž útočníci posílají svým obětem phishingové e-maily ve snaze získat přístup do systémů. Všechny formy phishingu jsou elektronickou verzí sociálního inženýrství. Phishing může být buď plošný nebo cílený (tzv. spear-phishing). Většinou obsahuje přílohy nebo odkazy, které buď po jejich otevření spustí škodlivý kód, nebo vyzvou uživatele k zadání přihlašovacích údajů.

MITRE ID: T1566

Mitigace: Mitigace této útočné taktiky běží ve dvou rovinách. Na technické úrovni lze značné množství phishingu spoléhajícího na podvrženou identitu odesílatele odfiltrovat, pokud poštovní server podporuje a provádí kontrolu příchozí pošty dle ochranného opatření NÚKIB. Vhodným protiopatřením je také sandboxing příloh, alespoň u potenciálně problematických typů souborů (zip, exe, ps1, js), a varování v případě zaheslovaných archivů. Nejčastěji zneužívanou metodou k doručení malwaru jsou stále makra v Office dokumentech. Tomuto vektoru útoku lze technickým opatřením nejsnáze zamezit zablokováním makro funkcí uživatelům, kteří je nezbytně nepotřebují ke své práci, pomocí doménových politik. Tyto technické kroky ale samy o sobě nestačí. Je potřeba neustále školit uživatele, upozorňovat je na rizika spojená se sociálním inženýrstvím a posledními trendy v oblasti phishingu, aby ho byli schopni sami odhalit.

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



Zaměřeno na hrozbu: Kybernetické útoky související s ruskou invazí na Ukrajinu

Pozornost kybernetické bezpečnostní komunity, stejně jako celého světa, se upřela na dění na Ukrajině. Jak se napětí v průběhu února stupňovalo, úměrně s tím rostly i kybernetické hrozby proti České republice. V návaznosti na současnou situaci jsou pravděpodobné cílené útoky a neúmyslné přelití útoků, např. způsobených destruktivními malwary. Pravděpodobnost narůstá i vzhledem ke kybernetickým útokům proti Litvě a Lotyšsku malwarem HermeticWiper (viz strana 4).

Jaké kybernetické události spojené s ruskou invazí na Ukrajinu jsme na území ČR zaznamenali?

NÚKIB v únoru neevidoval žádný kybernetický incident, který by byl prokazatelně spojený s ruskou invazí na Ukrajinu. Nicméně od 21. do 25. února probíhalo masivní skenování portů v celé republice. Dvě ruské IP adresy plošně mířily na české IP adresy, včetně adres české státní správy a kritické infrastruktury.

`92.63.197.97` `45.143.203.5`

Nelze vyloučit, že toto skenování portů je spojené s válkou na Ukrajině. Skenováním otevřených portů útočníci velmi pravděpodobně hledali slabá místa v zabezpečení českých organizací, kterých by mohli později využít k návazným kybernetickým útokům. Samotný fakt, že IP adresy, ze kterých probíhalo skenování, jsou registrované v Rusku, není dostačeným důkazem, že aktivita pochází právě odtamtud. Útočník si při troše snahy může zařídit hostování své infrastruktury téměř kdekoliv. Časový horizont skenování ale odpovídá narůstajícímu napětí na Ukrajině a zvýšené aktivitě ruských hackerských skupin. Navíc ty samé IP adresy vedle České republiky systematicky skenovaly také další evropské státy podporující Ukrajinu.

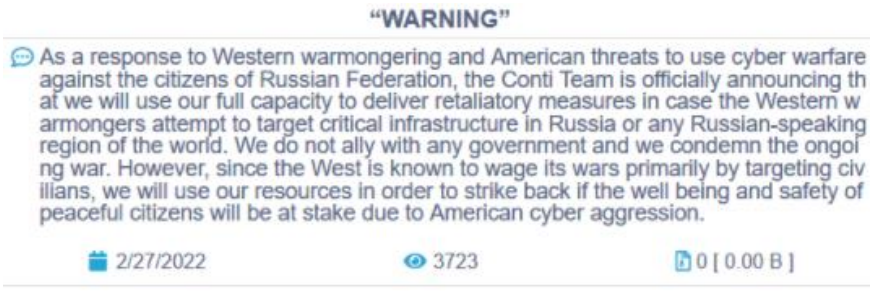
Hrozba kyberšpionáže, DDoS a ransomwarových útoků roste

Ke konci února NÚKIB nezaznamenal žádné kybernetické útoky, které by na zmíněné skeny navázaly nebo které by byly prokazatelně spojené s ruskou agresí na Ukrajině. Obezřetnost ale zůstává na místě. Vzhledem k současné situaci narostla hrozba kybernetické špionáže, DDoS či ransomwarových útoků:

- Kybernetická špionáž: S válkou na Ukrajině se na straně Ruska velmi pravděpodobně zvedla potřeba získání informací o chystaných krocích západních zemích. Nelze proto vyloučit, že státy NATO, včetně ČR, již jsou nebo se v blízké době stanou cílem intenzivnějších kyberšpionážních operací ruských APT skupin. NÚKIB podobnou špionáž v minulých měsících neodhalil, ale detekce podobných aktivit je velmi problematická. Za špionáží většinou stojí sofistikované APT skupiny, které se snaží zůstat v sítích své oběti nepozorovány, aby mohly exfiltrovat co nejvíce dat;
- DDoS: Dění na Ukrajině provází DDoS útoky. Předcházely například nasazení destruktivního malwaru HermeticWiper a vyřadily z provozu webové stránky ukrajinských vládních a finančních institucí. Cílem se staly stránky ukrajinského parlamentu nebo ministerstva zahraničí. Vzhledem k aktuálnímu rozšíření DDoS útoků proti ukrajinským institucím nelze vyloučit ani jejich případné použití proti českým organizacím;
- Ransomware: Na ruskou stranu se postupně přidávají také kyberkriminální skupiny, z nichž některé hrozí útoky vůči Ukrajině i těm, kteří budou prostřednictvím kyberprostoru útočit na Rusko. Nejvýraznější z nich je skupina Conti, která během posledního roku patří k celosvětově nejaktivnějším

ransomwarovým skupinám. Její fungování a propojení s dalšími kyberkriminálními skupinami rozkryly úniky jejích interních komunikací.

Obrázek: Prohlášení skupiny Conti vydané 27. února



zdroj: The Record

NÚKIB v souvislosti s výše zmíněnými hrozbami vydal 25. února Varování, ve kterém dává doporučení, jak se těmto konkrétním kybernetickým hrozbám bránit. Varování také obsahuje seznam technik, které útočníci ve svých útocích nejčastěji používají, včetně odkazů, jak tyto techniky mitigovat.

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.