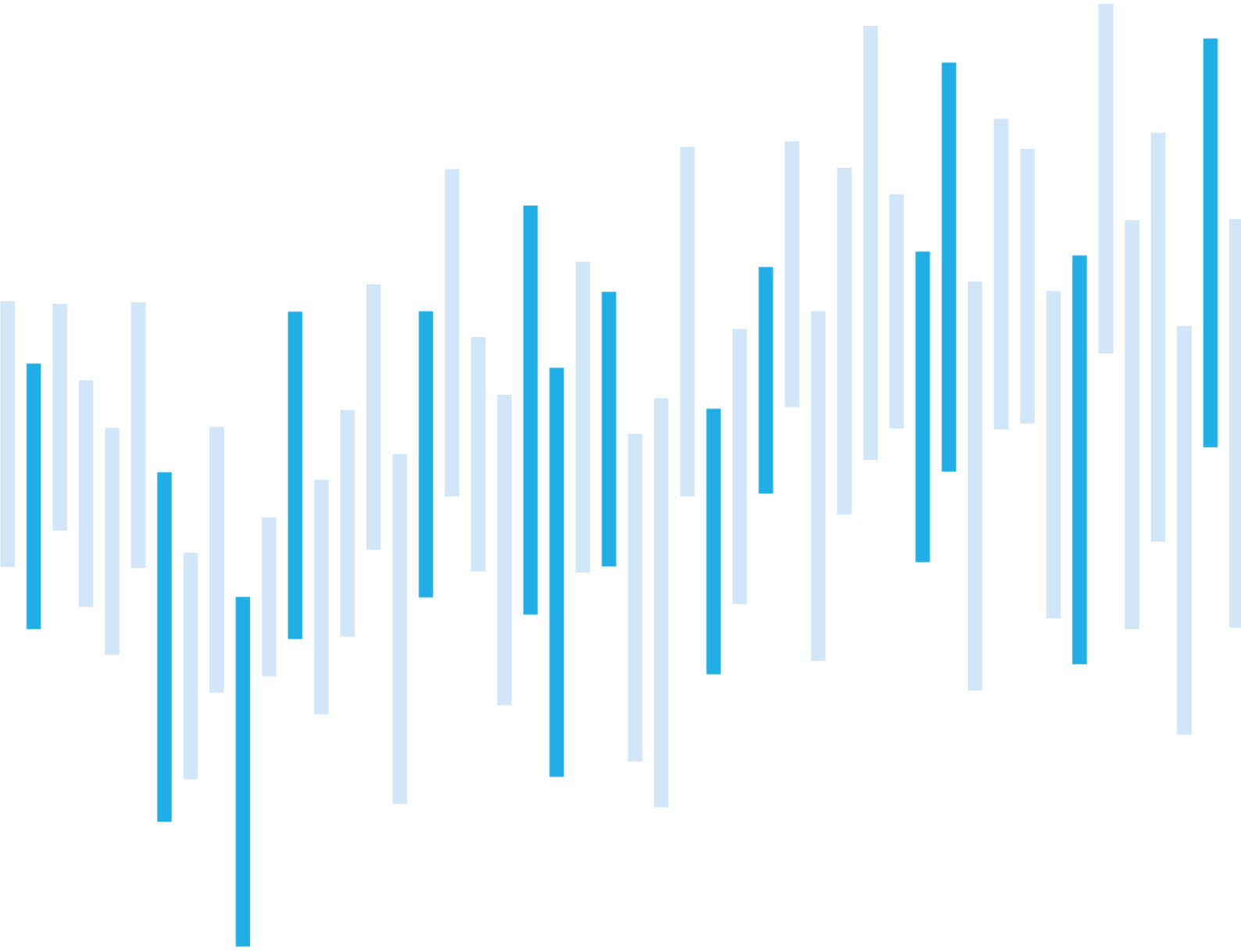
Kybernetické incidenty pohledem NÚKIB

DUBEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Duben se stal měsícem s druhým nejvyšším počtem incidentů za posledních dvanáct měsíců. Oproti předchozím měsícům NÚKIB nahlásilo incident o pětinu více organizací.

Do nárůstu incidentů se promítla především kampaň ruskojazyčné hacktivistické skupiny Killnet. Související kybernetické incidenty NÚKIB nahlásilo sedm organizací. Celkově se jednalo o méně sofistikované útoky, které způsobily nedostupnost webových stránek. Skupina informační systémy svých cílů nekompromitovala, a tudíž se ani nedostala k datům v nich uložených. Motivací Killnetu bylo pravděpodobně způsobit reputační škody.

Útoky pravděpodobně souvisí s českou podporou Ukrajiny. Killnet je ruskojazyčná skupina, která podle svých vyjádření podporuje Ruskou federaci. S tím souvisí i její výběr cílů. Vedle České republiky skupina od začátku invaze zaútočila na organizace a vládní instituce dalších států NATO a Ukrajiny. DDoS útoky v partnerských státech se překrývaly s významnými událostmi, přičemž se typicky jednalo o vojenskou či humanitární podporu Ukrajiny. Stejně tomu bylo i v případě ČR. První vlna, která proběhla od 19. do 21. dubna, se kryla s oznámením oprav ukrajinské těžké vojenské techniky v ČR.

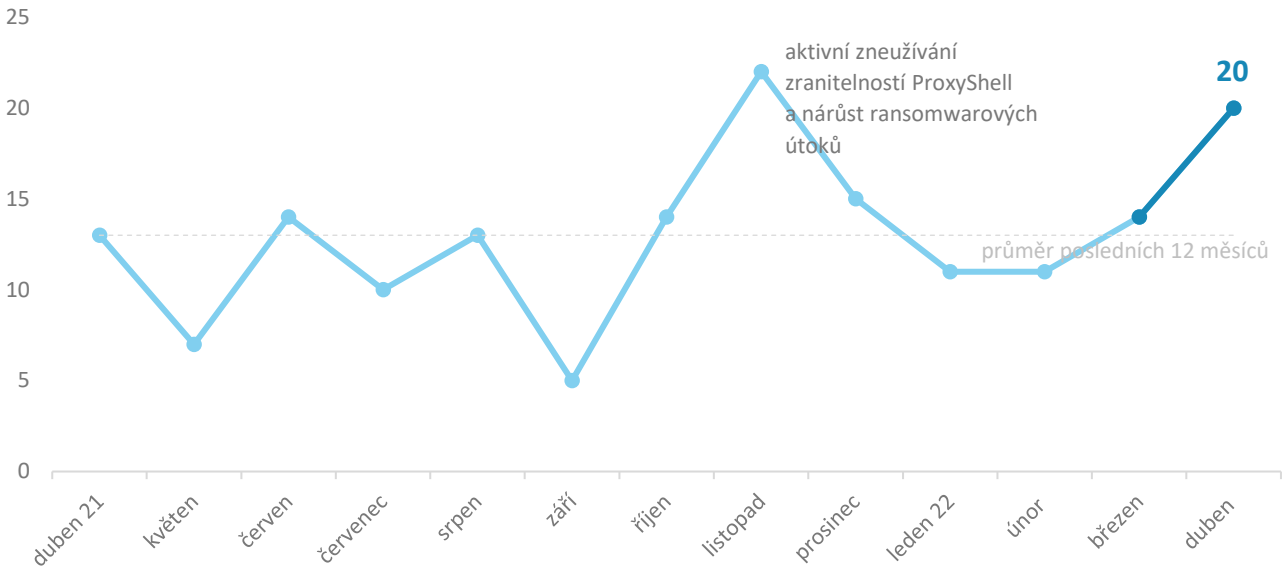
Obsah

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.

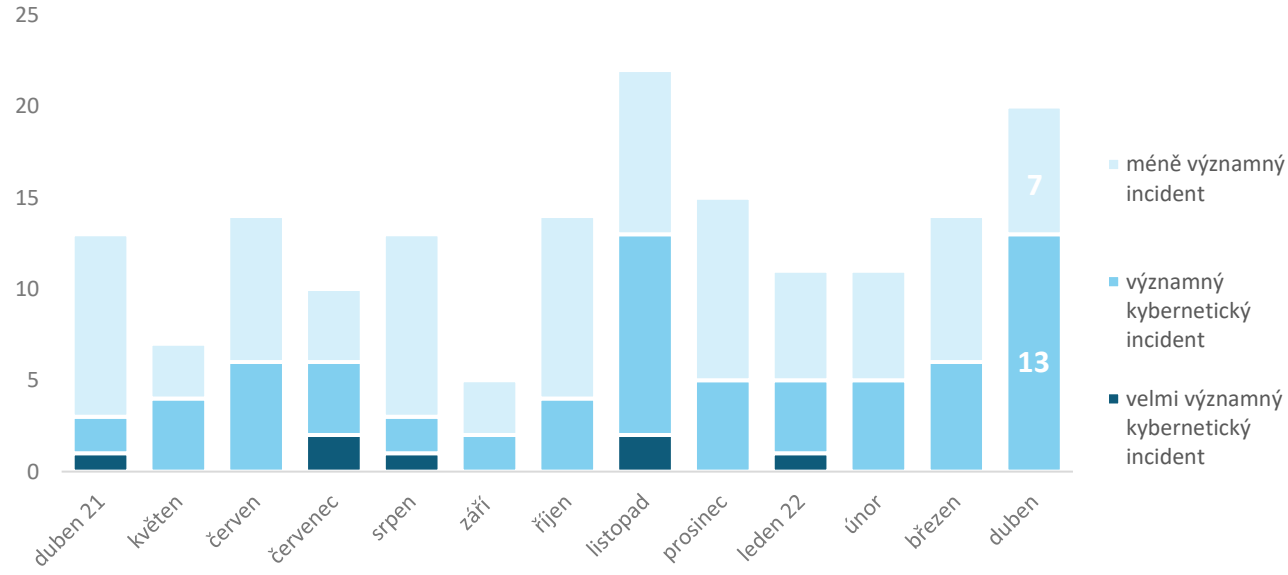
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Duben se stal měsícem s druhým nejvyšším počtem incidentů za posledních dvanáct měsíců. Předčil jej pouze listopad, kdy docházelo k aktivnímu zneužívání zranitelností ProxyShell.[1]



Závažnost řešených kybernetických incidentů[2]

Dvě třetiny dubnových incidentů měly významné dopady. Promítly se do nich především DDoS útoky, které mířily i na důležité státní instituce, a ransomware, který napadl menší neregulované subjekty.

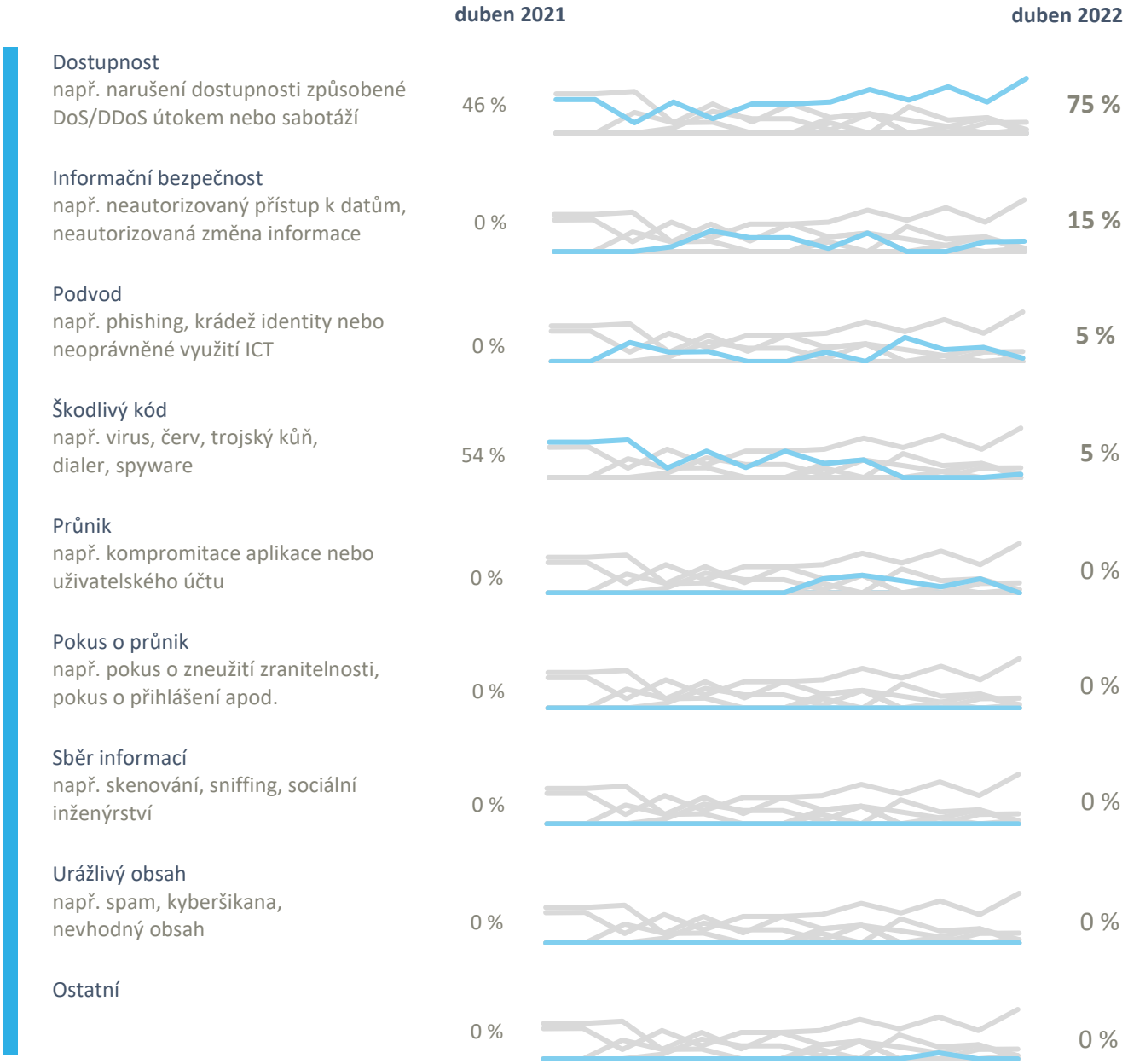


[1] 13 incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých sedmi incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Dubnové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Tři čtvrtiny incidentů vyústily v nedostupnost služeb. Za sedmi z nich stály DDoS útoky, které v minulých měsících tvořily spíše minoritní složku incidentů hlášených NÚKIB. V pěti případech dostupnost negativně ovlivnily případy ransomwaru a cryptomineru a u tří incidentů došlo k výpadku služeb následkem technické chyby;
- Druhou nejčastější kategorií byly incidenty, při nichž došlo k neoprávněnému přístupu k informacím. Jeden z nich byl následkem cíleného útoku na databáze městské samosprávy a útočníci při něm ukradli jejich obsah. Data zatím podle dostupných informací nezveřejnili, ale nelze vyloučit, že se tomu tak v blízké době stane;
- Jeden incident NÚKIB zařadil do kategorie podvodů. Útočníci pravděpodobně kompromitovali e-mailový účet zaměstnance významné státní instituce a rozesílali z něj phishingové e-maily s diplomatickou tématikou dalším vládním organizacím evropských zemí (viz strana 4);
- Poslední z dubnových incidentů NÚKIB klasifikoval jako škodlivý kód poté, co zjistil, že prvky infrastruktury české společnosti komunikují s řídícími servery malwaru Emotet.



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

Trendy v kybernetické bezpečnosti za duben pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Jeden z dubnových incidentů se týkal zachyceného phishingového e-mailu, který útočníci rozesílali z nakaženého účtu zaměstnance státní organizace. Phishing měl diplomatickou tématiku a z české e- mailové adresy dorazil na téměř 200 dalších adres vládních organizací evropských zemí.

NÚKIB neustále eviduje pokračující vlnu podvodných vishingových telefonátů, a proto na tuto kampaň opět upozornil. V upozornění jsou uvedené body, které jsou pro tuto vlnu charakteristické.

Malware

NÚKIB v rámci proaktivních aktivit (tzv. threat hunting) objevil prvky infrastruktury české společnosti, které komunikovaly s řídicím serverem malwaru Emotet. Emotet útočníci používají jako vstupní malware (payload), který se často šíří phishingem a který po kompromitaci stáhne do systému oběti další malwary. Emotet je v ČR aktivní. NÚKIB od podzimu, kdy se Emotet znovu objevil na kybernetické scéně, téměř každý měsíc nachází české společnosti, které tento malware nakazil a jejichž infrastruktura komunikuje nebo hostuje jeho řídicí servery.

Zranitelnosti

V dubnu se objevila nová kritická zranitelnost produktů VMware Workspace ONE Access a Identity Manager (CVE-2022-22954). Zranitelnost umožní útočníku obejít autentizační mechanismy a vzdáleně nahrát na server škodlivý kód. Jelikož zranitelnost začali hned zneužívat útočníci, NÚKIB regulované subjekty, které měly zranitelné systémy, na problém upozornil a poslal jim doporučení pro řešení problému (mitigace).

Ransomware

Ransomwarové útoky od začátku roku stabilně tvoří přibližně pětinu incidentů, které NÚKIB eviduje. I v dubnu tento trend přetrval. Za útoky stál ransomware Phobos, který cílí především na menší a zranitelné cíle, a NÚKIB ho v hlášených incidentech zaznamenává pravidelně. V jednom z dubnových případů se pak objevil LokiLocker, což je relativně nový ransomware nabízený jako služba, který se začal šířit v létě 2021 a NÚKIB ho v hlášeních incidentů zaznamenal podruhé.

Útoky na dostupnost

DDoS útoky v posledním roce tvořily spíše minoritní část incidentů, které NÚKIB eviduje. V dubnu se ale situace změnila. Více než třetinu incidentů způsobily DDoS útoky, které proti českým cílům podnikla skupina rusko-jazyčná hackerská Killnet (více informací ke kampani na straně 6). DDoS útoky v některých případech vyřadily z provozu webové stránky na několik hodin. NÚKIB takový incident nahlásilo sedm organizací regulovaných dle ZKB, ale českých obětí Killnetu bylo přibližně třikrát víc.

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

Technika měsíce: Malicious File

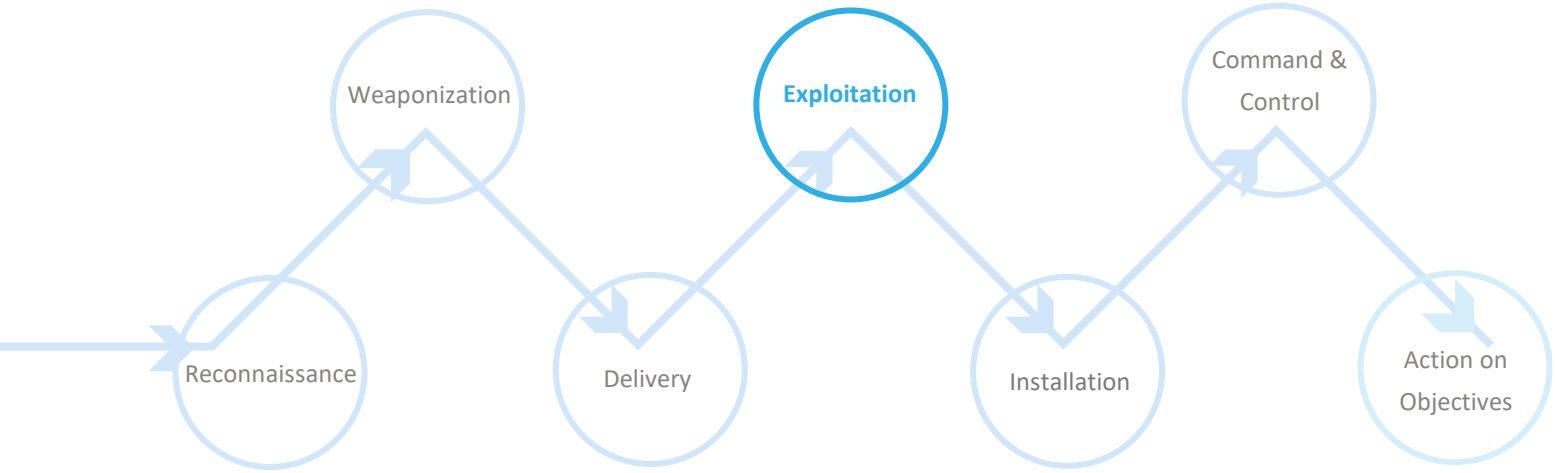
NÚKIB kybernetické incidenty vyhodnocuje mimo jiné na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V dubnových incidentech výrazně převažovala technika „Malicous File“, kterou ve svých kampaních využívá velká většina APT a kyberkriminálních skupin a která je běžnou součástí phishingových útoků.

Malicious File je technika, při níž se útočníci spoléhají na to, že uživatel otevře soubor a sám spustí škodlivý kód. Toto je typické například pro spear-phishingové e-maily, které se snaží uživatele přesvědčit, aby otevřeli nakaženou přílohu a tím na pozadí spustili škodlivý kód, který je do přílohy zakomponovaný. Techniku Malicious File jsme v dubnových incidentech nejčastěji evidovali ve spojitosti s phishingem, kdy ji útočníci používali především v počátečních fázích kybernetických útoků. Tuto techniku ale můžou použít i později, když už se v sítích oběti nacházejí. Mohou si například vytvořit soubor, který po kompromitaci uloží na sdílený disk a čekají, až ho otevřou další uživatelé a tím jim umožní se dál rozšířit po síti.

MITRE ID: T1204.002

Mitigace: Mitigace techniky T1204.002 je možná ve dvou rovinách. Na technické úrovni je vhodným řešením sandboxing příloh, alespoň u potenciálně problematických typů souborů (zip, exe, ps1, js), a varování uživatele v případě zaheslovaných archivů. Nejčastěji zneužívanou metodou v souvislosti se škodlivými přílohami 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. 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.

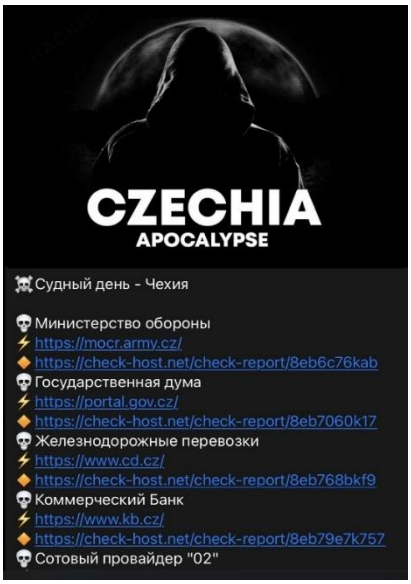
Znázornění techniky Malicious File v kill chainu, který ukazuje, ve které fázi útočníci techniku používají:



Zaměřeno na hrozbu: DDoS kampaň skupiny Killnet

Ve druhé polovině dubna provedla ruskojazyčná hackerská skupina Killnet dvě série DDoS útoků proti webovým stránkám českých subjektů. Útoky pravděpodobně souvisí s českou podporou Ukrajiny.

Obr 1: telegramový účet Killnetu



První vlna proběhla od 19. do 21. dubna a zasáhla třináct subjektů, včetně NÚKIB a českých ministerstev. Zahájení útoků se překrývalo s oznámením oprav ukrajinské těžké vojenské techniky v ČR. Během noci na 27. dubna pak proběhla druhá vlna, kdy útočníci napadli dalších devět subjektů. Skupina Killnet zahájení útoků proti českým organizacím oznámila na svém telegramovém účtu (viz obrázek 1).

Celkově šlo o méně sofistikované útoky, které v důsledku způsobily nedostupnost webových stránek. DDoS útoky obecně zahltí provoz na službách přístupných z internetu, informační systémy organizací ale nekompromitují. Skupina Killnet se proto ani nedostala k datům uložených v napadených organizacích. Jejím cílem bylo pravděpodobně způsobit napadeným organizacím reputační škody.

> Technická stránka útoků skupiny Killnet
>
> Na základě dat z jednoho z incidentů NÚKIB identifikoval L4 TCP ACK DDoS. Jde o útok na transportní vrstvě za použití TCP ACK či TCP ACK-PUSH segmentů, které se v legitimní komunikaci používají k potvrzení přijatých dat. Tento druh útoku je složitější mitigovat, jelikož je poměrně obtížné odlišit legitimní ACK pakety od škodlivých. Dopadem na infrastrukturu je vyčerpání výpočetního výkonu serveru či firewallu, jež musí podvrhnuté komunikaci dedikovat svůj výkon.

Killnet je rusko-jazyčná skupina, která podle svých vyjádření podporuje Ruskou federaci. S tím souvisí i její výběr cílů. Vedle České republiky skupina zaútočila na organizace a vládní instituce dalších států NATO nebo Ukrajiny. Kromě jednoho případu se vždy jednalo o DDoS útoky. Výjimkou byla údajná krádež dat kyjevského prokurátora, která se časově překrývala s odhalením masakru v Buče.[5] Ta spadá právě pod jurisdikci prokuratury ukrajinského hlavního města. DDoS útoky v dalších státech se také překrývaly s významnými událostmi, přičemž typicky se jednalo o vojenskou či humanitární podporu Ukrajiny.

NÚKIB na zvýšené riziko kyberútoků upozorňuje od začátku ruské agrese. 25. února vydal Varování, které mimo jiné obsahuje i celou řadu preventivních i reaktivních opatření proti DDoS útokům. Vzhledem k tomu, že je velmi pravděpodobné, že se válka na Ukrajině bude v kybernetickém světě dotýkat ČR i nadále, na Varování znovu upozorňujeme a doporučujeme všem organizacím, aby zmíněná doporučení včas implementovaly. Dokument poskytuje návod nejen na to, jak se na případný DDoS útok připravit, ale i na to, jak DDoS útok mitigovat ve chvíli, kdy už probíhá.

[5] Killnet o útoku informoval na svém telegramovém účtu

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.