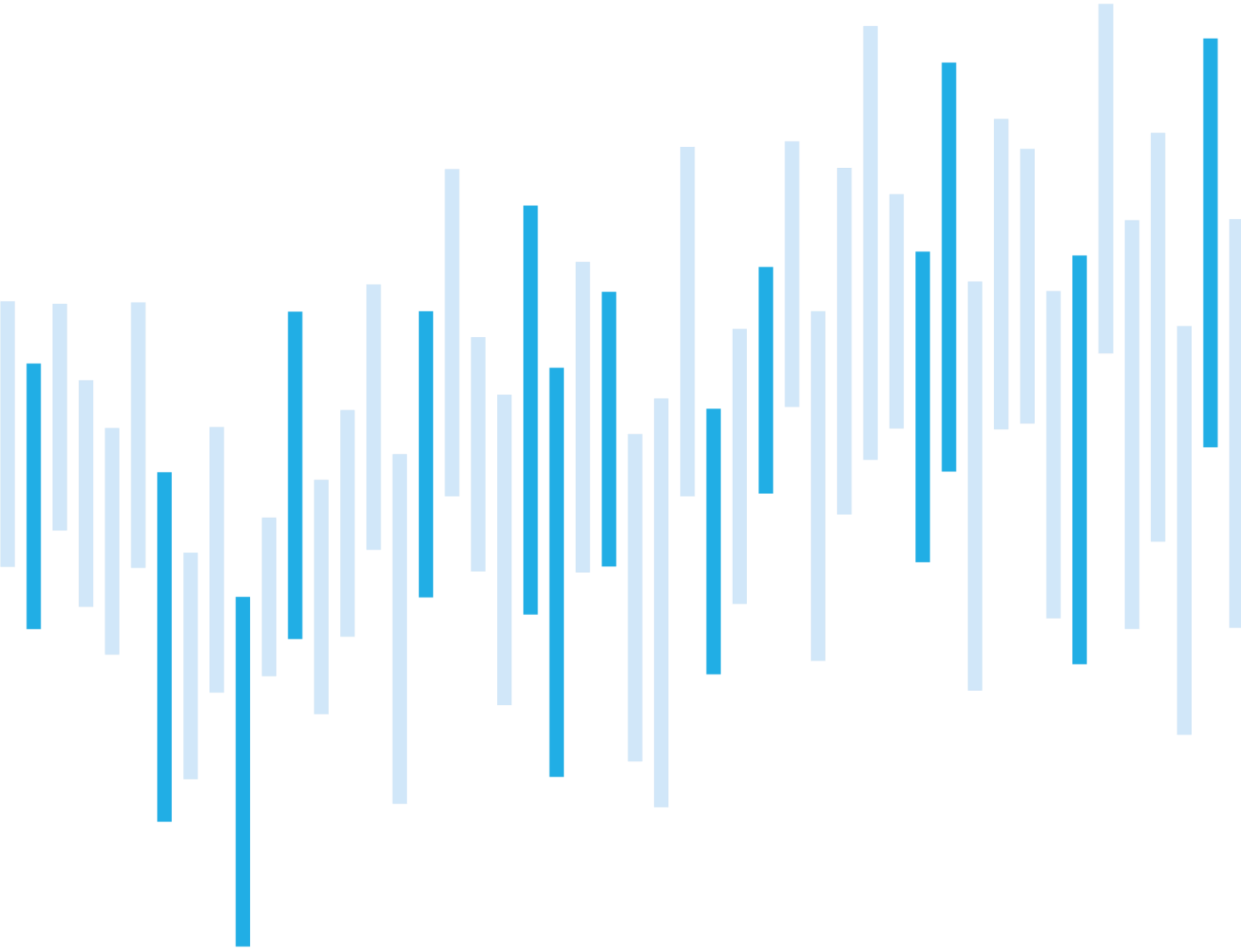
Kybernetické incidenty pohledem NÚKIB

# ČERVEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

## Shrnutí měsíce

Počet červnových incidentů se pohyboval nad průměrem posledních 12 měsíců. Vedle DDoS útoků, které posledního půl roku pravidelně zvyšují počty incidentů, se tentokrát do čísel promítl i nárůst útoků ransomwaru.

Nejčastěji byl v rámci incidentů využíván ransomware PLAY. Z šesti červnových případů, kterými se NÚKIB zabýval, měl PLAY na svědomí tři. Pro PLAY je charakteristické jeho vysoké operační tempo. Jen za rok své existence má minimálně sto obětí a jejich počty dál rostou. Geografické rozložení napadených organizací navíc jasně ukazuje, že Česká republika je vysoko v hledáčku jeho operátorů.

Jelikož je pravděpodobné (55–70 %), že útočníci budou ve svých aktivitách proti českým cílům v krátkodobém horizontu pokračovat, upozornění na zvýšené riziko ransomwarových útoků, které NÚKIB publikoval na svých webových stránkách v průběhu června, zůstává aktuální. Toto upozornění obsahuje mj. výčet kritických zranitelností, které jsou aktuálně zneužívány ransomwarovými aktéry v ČR i ve světě a které doporučujeme prověřit.

## Obsah

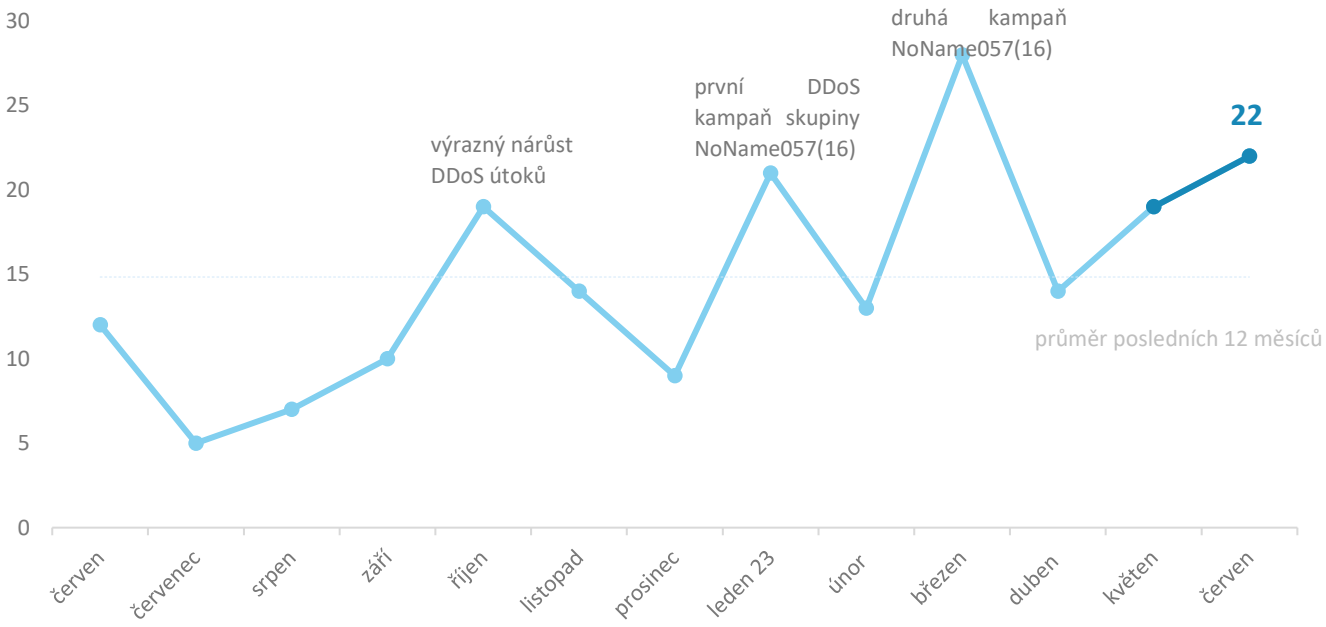


Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz

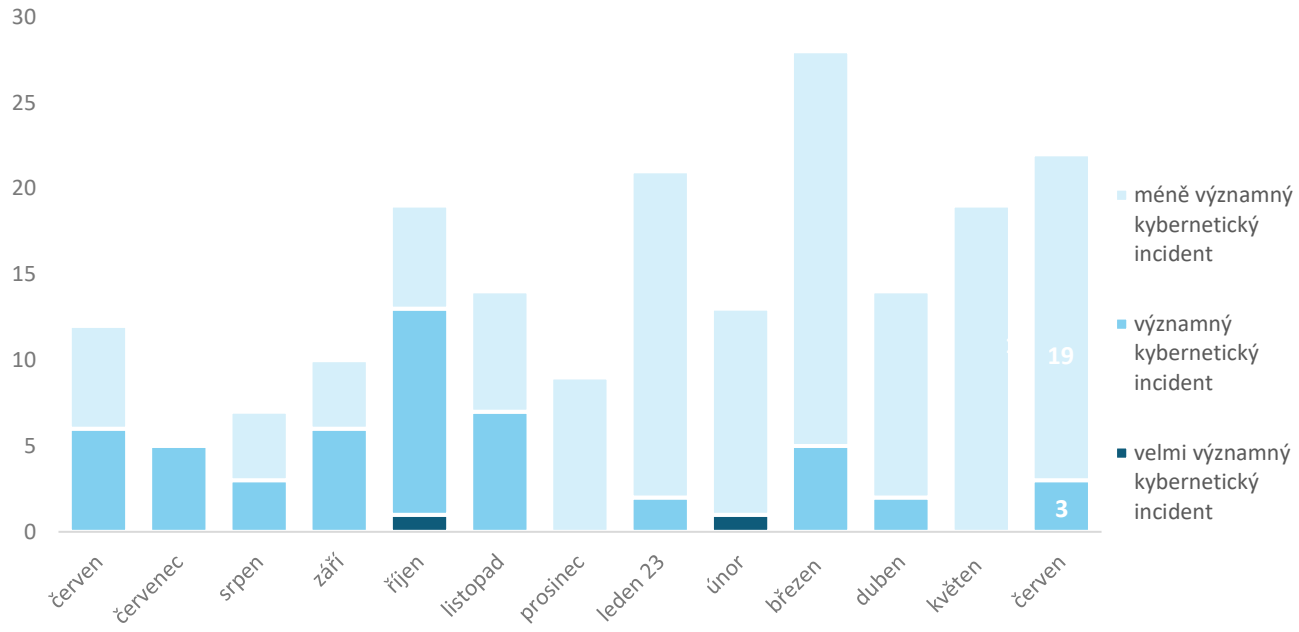
## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet incidentů se podobně jako minulý měsíc držel vysoko nad průměrem. [1]




## Závažnost řešených kybernetických incidentů[2]

Ransomwarové útoky se propsaly také do závažnosti kybernetických incidentů. Jelikož dva z nich smazaly napadeným organizacím zálohy a znemožnily jim rychlou nápravu situace, klasifikoval je NÚKIB jako významné incidenty.



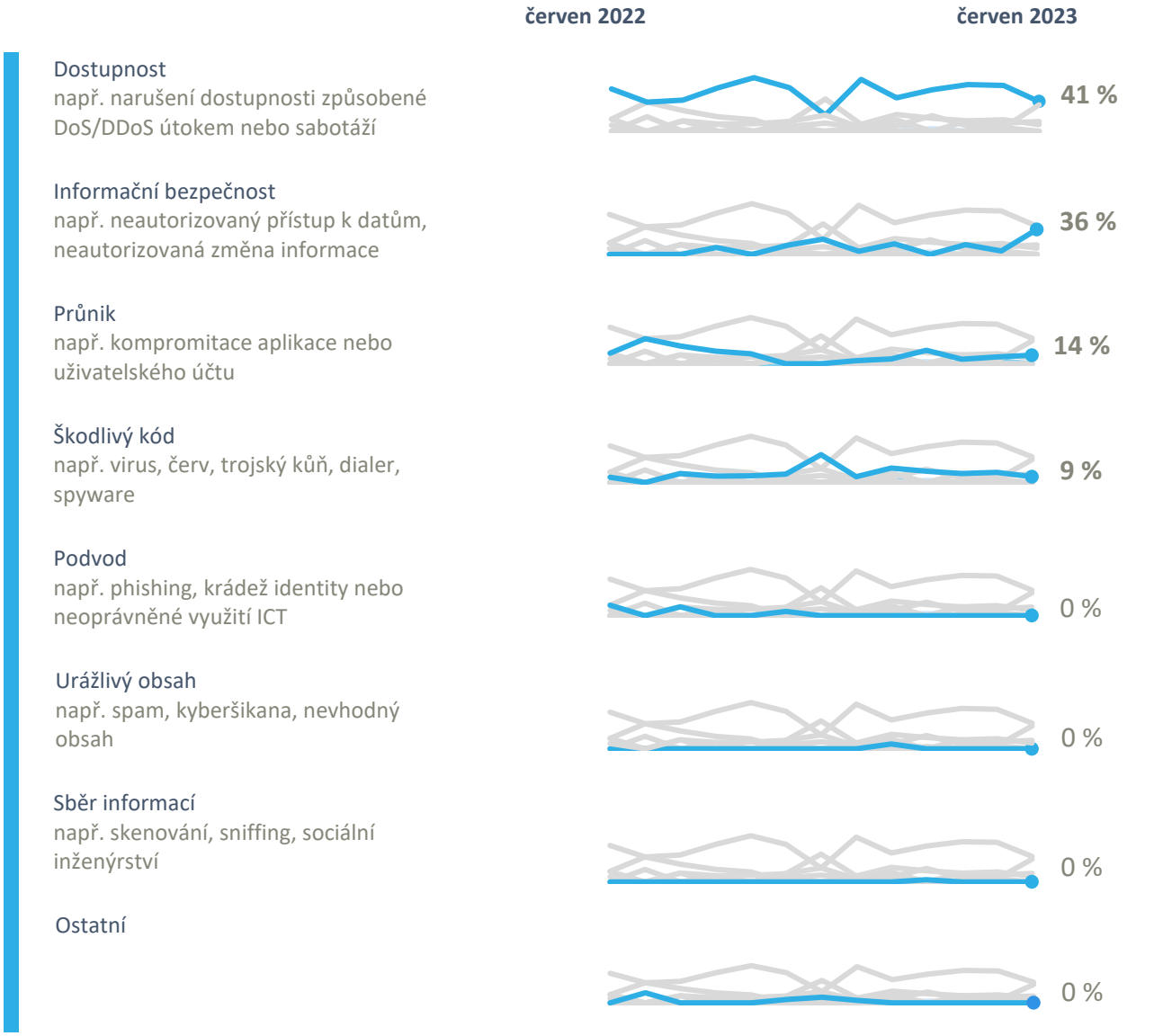

[1] 16 incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývajících šest incidentů nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

## Klasifikace incidentů nahlášených NÚKIB[3]

NÚKIB v červnu opět nejčastěji evidoval omezení dostupnosti služeb, a to především v důsledku DDoS útoků. Nicméně tentokrát jejich procentuální zastoupení v kybernetických incidentech oproti posledním šesti měsícům kleslo. Je to dáno mimo jiné i nárůstem ransomwarových útoků, kterých bylo šest a které jsme evidovali jako narušení informační bezpečnosti.

Vedle toho NÚKIB řešil incidenty v těchto dvou kategoriích:

- Ve třech případech „průniku“ došlo k odcizení přihlašovacích údajů do různých systémů a databází, následkem čehož k nim útočníci získali krátkodobý přístup.
- Dva incidenty, ve kterých byl na uživatelských stanicích nalezen malware, klasifikoval jako škodlivý kód.




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

# Trendy v kybernetické bezpečnosti za červen pohledem NÚKIB[4]

## Phishing, spear-phishing a sociální inženýrství

Po několika měsících, kdy NÚKIB intenzivně řešil phishingové kampaně proti českým strategickým cílům, se situace v červnu uklidnila. NÚKIB evidoval případ spear-phishingu proti české společnosti z obranného průmyslu, ke kompromitaci ale nedošlo. Další, ne příliš propracovaný phishing, pak mířil na jednu z českých univerzit.

## Malware

Phishingová příloha v jednom z červnových incidentů spustila po jejím otevření škodlivý kód, který začal stahovat soubor ve formátu .zip ze škodlivé domény. Na základě informací o URL se pravděpodobně (55-75 %) jedná o malware QakBot, který by v následném kroku do systému uživatele pravděpodobně stáhl ransomware. QakBot ale zachytila technologie EDR (Endpoint Detection and Response) a stažený soubor umístila do karantény.

## Zranitelnosti

Ransomwary, které v červnu útočily na české cíle, ve svých útocích jako vektor útoku často zneužívá zranitelnosti. Ransomware PLAY pro kompromitaci sítí zneužívá např. zranitelnosti FortiOS (CVE-2018-13379, CVE-2020-12812) a MS Exchange (CVE-2022-41080, CVE-2022-41082). Tyto a další kritické zranitelnosti, které jsou aktuálně zneužívány ransomwarovými aktéry v ČR i ve světě, jsme identifikovali v našem upozornění na webových stránkách NÚKIB a doporučujeme si ověřit, zda zranitelné aplikace nevyužíváte.

## Ransomware

Ačkoliv je ransomware stálou hrozbou a NÚKIB se jím od roku 2018 zabývá téměř každý měsíc, v červnu se aktivity kyberzločineckých aktérů proti českým cílům zintenzivnily. NÚKIB řešil šest případů ransomwarových útoků, z toho dva měly závažné dopady na fungování napadených organizací.

Nejvíce se na nárůstu ransomwarových útoků podepsal ransomware PLAY, kterému se blíže věnujeme v poslední kapitole. Kromě něj pak také aktéři útočili pomocí ransomwarů BlackBasta a LockBit.

## Útoky na dostupnost

Červen byl s osmi DDoS útoky srovnatelný s předchozím měsícem. Pokračovala DDoS kampaň vedená prozatím neznámým útočníkem, která míří výhradně na české vládní instituce. Útoky začaly v únoru tohoto roku a každý měsíc cílily na DNS servery institucí ve snaze je zahltit. Na rozdíl od hacktivistických kampaní se k nim ale žádný aktér nehlásí.

Pokračovaly také DDoS útoky hacktivistické skupiny NoName057(016).

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

## Technika měsíce: Exploit Public-Facing Application

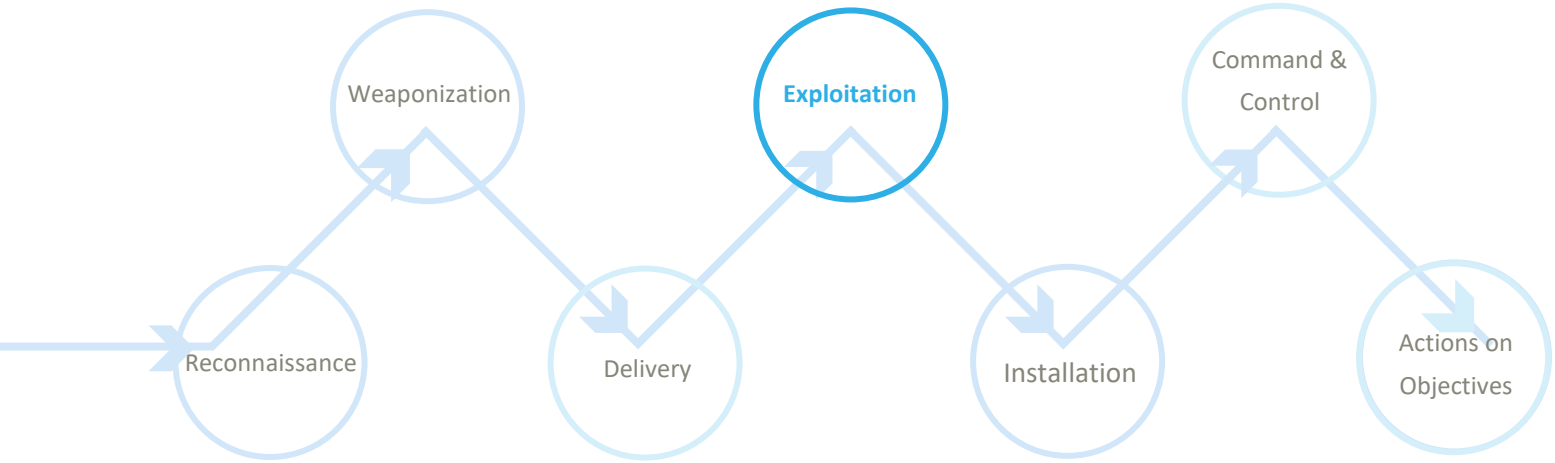
Ransomware PLAY, který útočí na české cíle, se do sítí svých obětí mimo jiné dostává zneužíváním zranitelností. V MITRE ATT&CK matici tato technika odpovídá Exploit Public-Facing Application. Zranitelnosti, které ransomware Play prokazatelně zneužívá, jsou zranitelnosti FortiOS a Microsoft Exchange.

**Exploit Public-Facing Application** je technika, kterou útočníci zneužívají slabých míst v systémech otevřených do internetu. Takovým systémem může být webový nebo e-mailový server či aplikace pro vzdálenou správu dat. Pokud si útočníci všimnou nevhodného nastavení zabezpečení ze strany oběti nebo chyby, kterou udělal výrobce při psaní programu, mohou toho zneužít a skrze takto zranitelné systémy se dostat do sítí oběti. Úspěšná kompromitace může mít za následek krádež dat nebo jejich zašifrování a následné vydírání.

**MITRE ID: T1190**

**Mitigace:** Organizace mohou zmírnit riziko zneužití této techniky tím, že do internetu otevřou jen služby nezbytně nutné k provozu. Také je potřeba pravidelně instalovat aktualizace operačních systémů a aplikací a zároveň vedení protokolů pro správu těchto aktualizací. Toto opatření znesnadní aktérům zneužívání zranitelností softwaru. Pro služby vzdáleného přístupu (VPN, RDP, SSH) doporučujeme používat vícefaktorovou autentizaci (MFA). Používání MFA na všech účtech, zejména na účtech VPN, webmailu a účtech s přístupem ke kritickým systémům, ztíží útočníkům laterální pohyb uvnitř sítě.

Znázornění T1190 v kill chainu ukazujícím, v jaké fázi útoku kybernetičtí aktéři techniku používají:

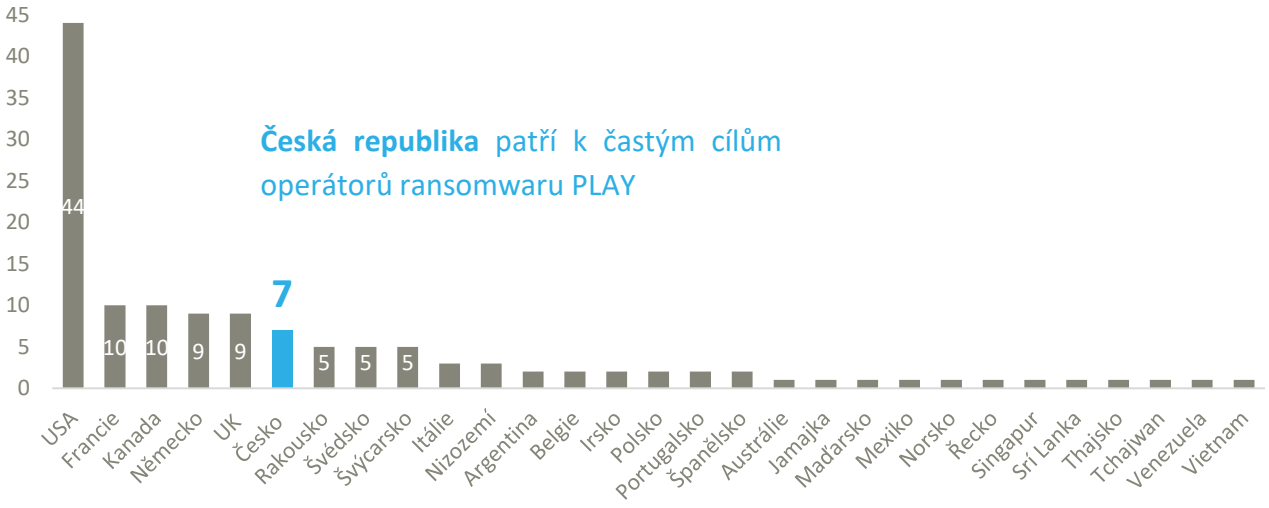


## Zaměřeno na hrozbu: Operátoři ransomwaru PLAY míří na české cíle

NÚKIB v průběhu června evidoval v českém kyberprostoru zvýšenou aktivitu kyberzločineckých skupin. Nejvýrazněji se na tomto nárůstu podílel ransomware PLAY. Z šesti červnových ransomwarových útoků, kterými se NÚKIB zabýval, měl tři z nich na svědomí právě PLAY. Jak ukazuje graf níže, operátoři ransomwaru PLAY zařadili Českou republiku vysoko na seznam cílů.

Ransomware PLAY je aktivní minimálně od června 2022 a počet jeho obětí rychle roste. Za rok působení má na kontě přes sto obětí. Operátoři ransomwaru na svých darkwebových stránkách zveřejnili informace o téměř 150 obětech, včetně sedmi z České republiky. Jsou to organizace z dopravního, energetického i obranného průmyslu, které jsou důležité pro chod státu.

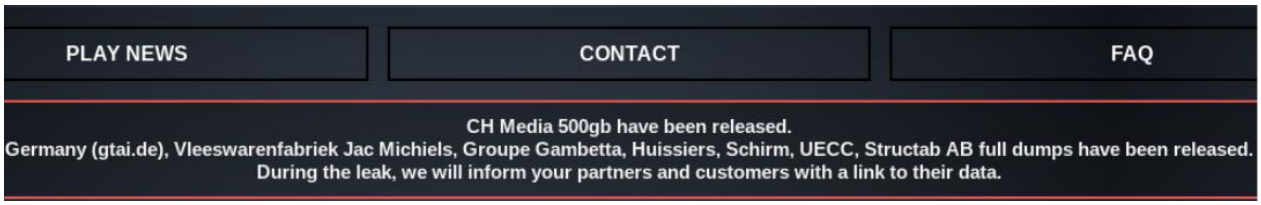
Graf 1: Geografické rozložení obětí ransomwaru PLAY[5]




Skupina je charakteristická využíváním tzv. **přerušovaného šifrování** (intermittent encryption), které zašifruje jen dílčí bloky cílových souborů. Tato metoda umožňuje šifrovat výrazně vyšší rychlostí (nižší stovky MB/s) a zároveň komplikuje detekci.

Operátoři PLAY využívají **tzv. trojího vydírání**, kdy kromě zašifrování a hrozby zveřejnění dat obětem ještě vyhrožují kontaktováním jejich zákazníků, aby je motivovali k platbě.

Obr 1: Příklad trojího vydírání operátorů ransomwaru PLAY (screenshot ze dne 13.06.2023)




Je pravděpodobné (55–70 %), že útočníci budou ve svých aktivitách proti českým cílům pokračovat i v následujících měsících. Upozornění na zvýšené riziko ransomwarových útoků, které NÚKIB 20. června 2023 publikoval na svých webových stránkách, je tak stále aktuální.

[5] Data jsou aktuální k 11. červnu 2023

## 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+STRICT | Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta. |
| 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: 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. |