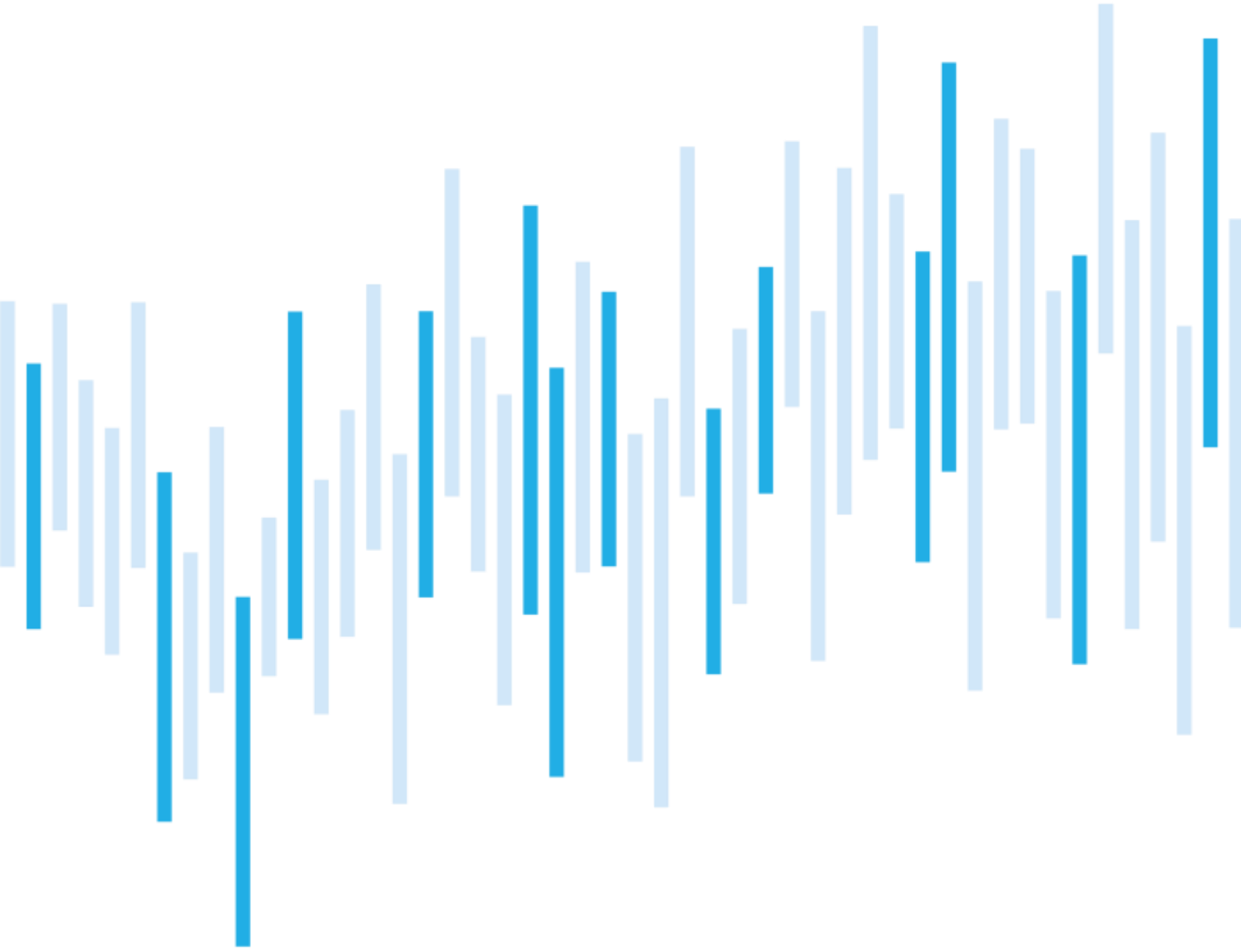
Kybernetické incidenty pohledem NÚKIB

ČERVEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se během června držel na podprůměrných hodnotách. Jde o každoroční trend, kdy během léta NÚKIB eviduje nižší počet incidentů. Přesto však byla závažnost často relativně vysoká.

V červnu výrazně převažovaly útoky proti regulovaným subjektům, nicméně nelze definovat sektor, který by byl zasažen významněji než ostatní.

V červnu se NÚKIB zaměřil na CZ PRES jakožto událost zvláštního významu. ČR na začátku července převzala na půl roku předsednictví v Radě EU, přičemž kybernetická bezpečnost patří mezi jeho hlavní priority. Nelze však pomíjet, že CZ PRES představuje lákavý cíl pro útočníky, především s ohledem na možnost špionáže, nasazení ransomwaru/wiperu nebo snahy o krátkodobou paralýzu výkonu skrze DDoS útoky.

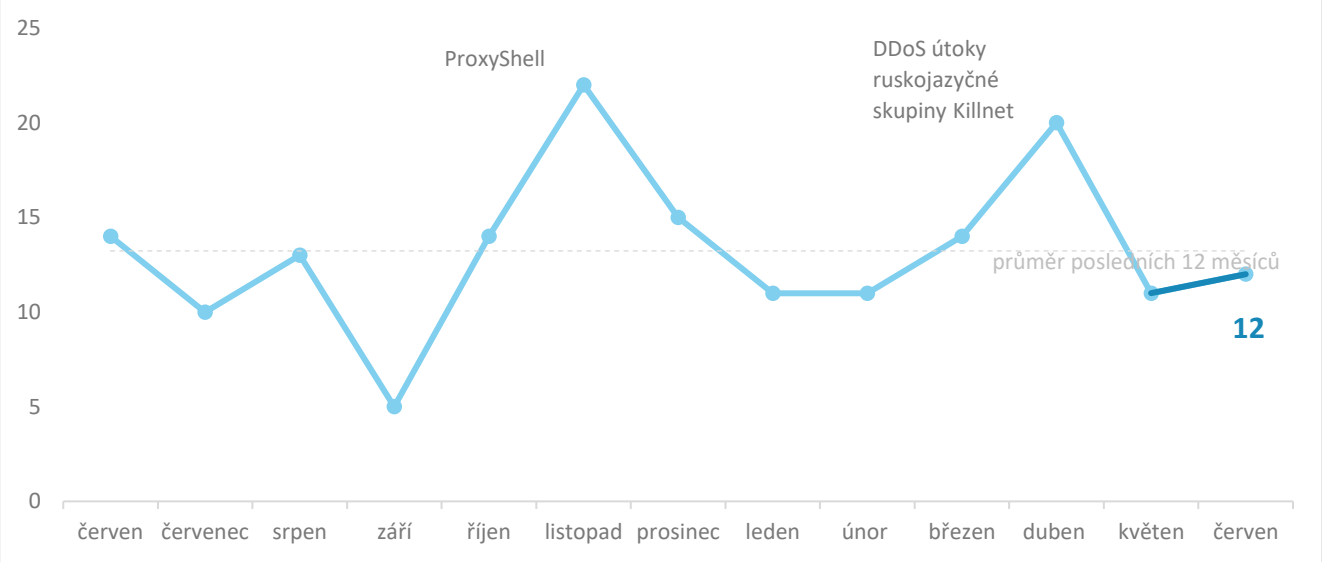
Obsah

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

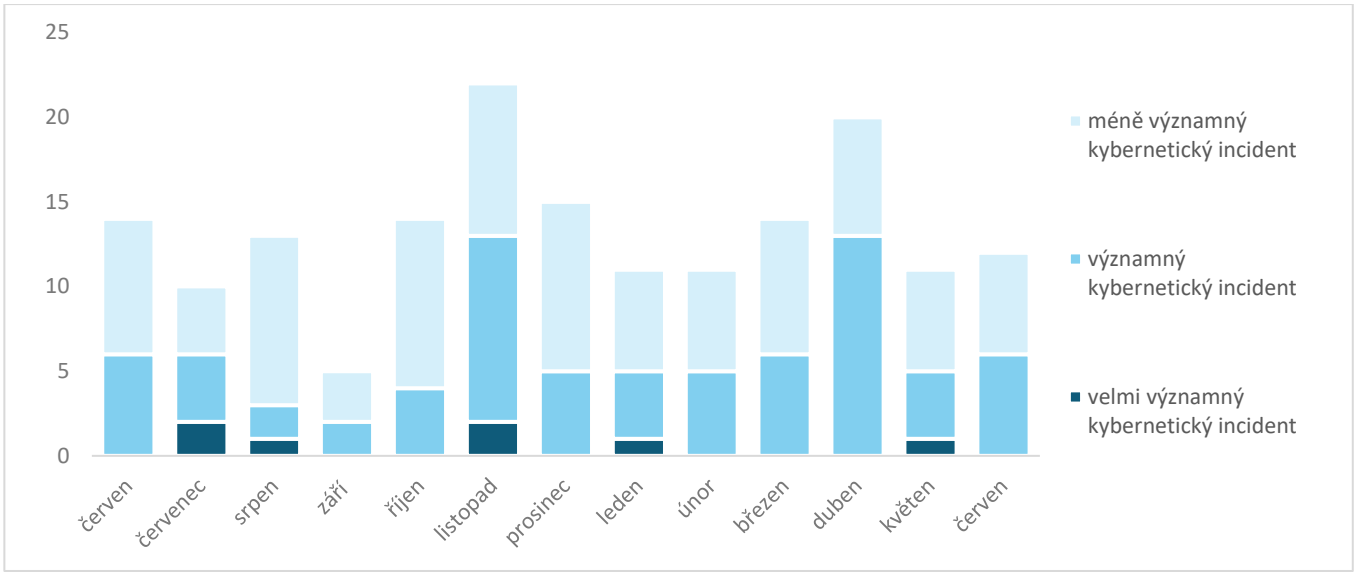
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet incidentů se v měsíci červnu držel na průměrné úrovni. Během letních měsíců obvykle NÚKIB eviduje nižší počet incidentů.[1]



Závažnost řešených kybernetických incidentů[2]

Během měsíce června se incidenty téměř rovnoměrně rozdělily na méně významné a významné. Oproti minulému měsíci nedošlo k velmi významnému incidentu.

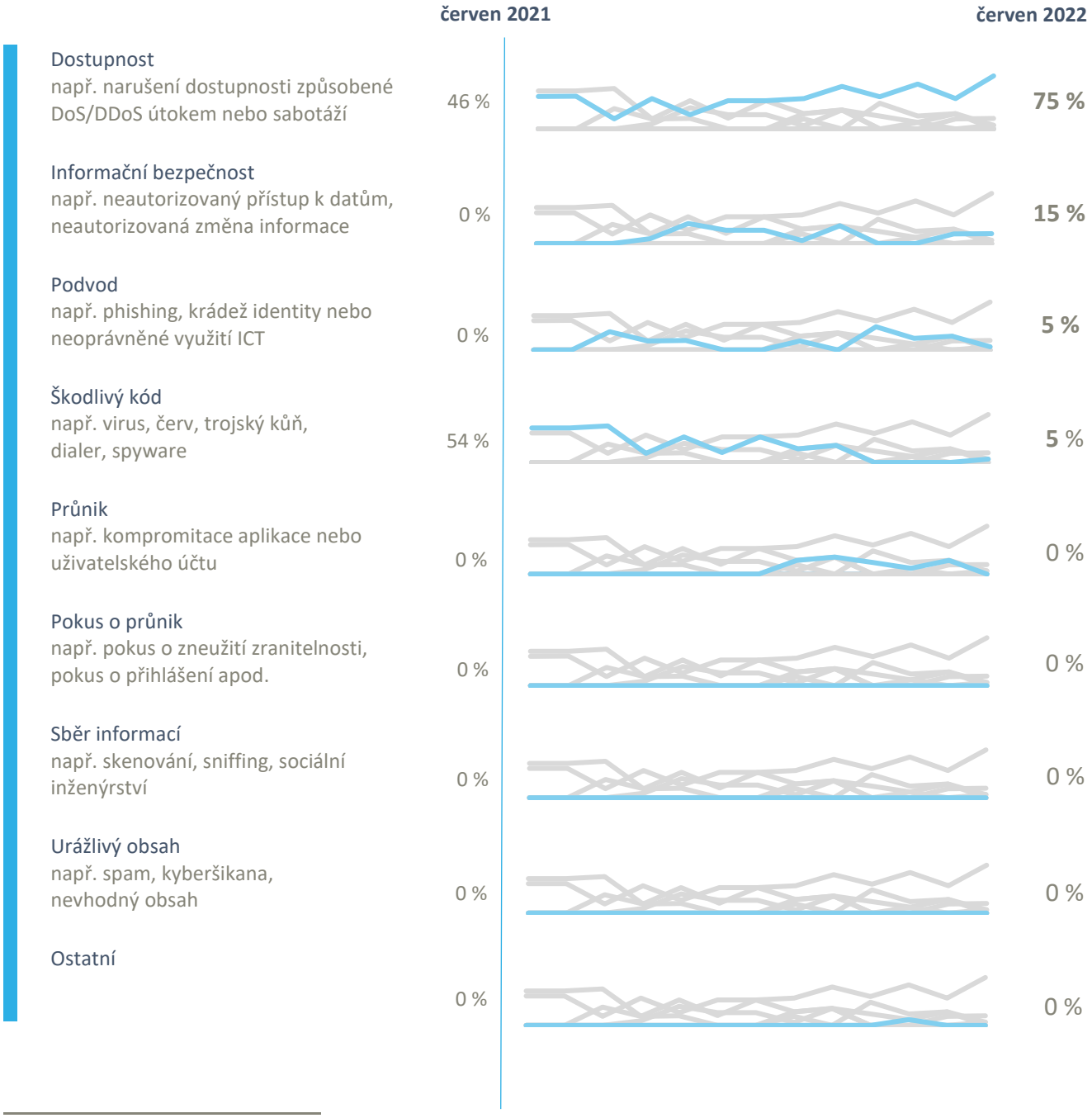


[1] 10 incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých 2 incidentech NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Červnové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Pokračovala převaha incidentů spjatých s dostupností, nicméně vyjma dvou případů se jednalo o technické chyby, kdy došlo k výpadkům systému. V jednom případě šlo o ransomware. Nejzajímavějším případem bylo přeřezání optické kabeláže, jež vyústilo ve výpadek systémů jednoho subjektu.
- Došlo také k několika incidentům, které jsou klasifikovány jako průnik. Nejednalo se nicméně o závažné incidenty.
- V případě incidentu typu podvod došlo k phishingovému útoku proti jedné státní instituci, jejíž zaměstnanci obdrželi e-mail obsahující zprávu v češtině se srbochorvatským podpisem. Phishing byl odeslán ze schránky patřící telekomunikační společnosti s původem v Bosně a Hercegovině.
- NÚKIB taktéž evidoval incident typu 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

Phishing či pokusy o něj mají permanentní trend. Nejzajímavějším červnovým případem byl incident, během kterého pracovníci jedné státní instituce obdrželi e-mail psaný relativně dobrou češtinou, ale obsahující podpis v srbochorvatštině. Zpráva byla odeslána z velmi pravděpodobně kompromitované schránky, která patří telekomunikační společnosti, jež sídlí v Bosně a Hercegovině.

Malware

Poté co Microsoft zamezil spouštění maker v základní konfiguraci kancelářského balíku Office je patrný pokles používání této techniky ve phishingových kampaních šířících např. Emotet, AgentTesla či Qakbot. V reakci se tyto rodiny malwaru objevují v nových variantách a zneužívají k doručení zejména LNK soubory.

NÚKIB také zachytil spear-phishingovou kampaň šířící malware PlugX. Žádný z hlášených případů nicméně nevyústil k incident.

Zranitelnosti

V červnu se objevila nová kritická zranitelnost CVE-2022-26134, která se týká produktů od Atlassian, jmenovitě Confluence Server a Data Center. Útočník může provést vzdálené spuštění kódu (RCE), což má potenciálně devastující dopady pro oběť. Pokud je zranitelnost úspěšně zneužita, tak útočník může nasadit backdoor, ransomware či stealer, který oběti odcizí data.

Ransomware

Přestože podíl ransomwaru na celkovém počtu všech incidentů byl v červnu minimální, trend vyděračských útoků pokračoval.

Útoky na dostupnost

Podobně jako v předchozím měsíci nezpůsobil žádný incident DDoS útok. Přesto docházelo k narušení dostupnosti kvůli technickým chybám.

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

Technika měsíce: Spear-Phishing Attachment

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V tomto měsíci jsme se zaměřili na spear-phishingové přílohy, které v kampaních využívá většina APT a kyberkriminálních skupin.

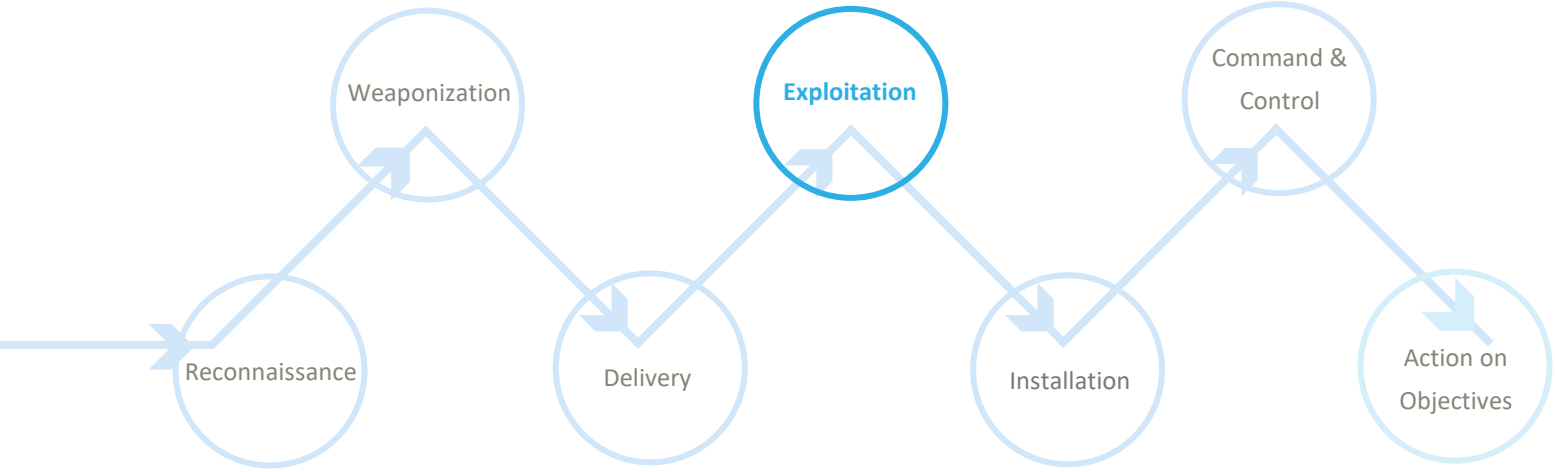
MITRE ID: T1566.001

Jelikož Microsoft v aktuálních verzích kancelářského balíku zavedl již v základní konfiguraci blokaci spouštění maker v souborech stažených z internetu, začala řada rodin malwaru v reakci měnit své techniky doručení.

Nyní nejrozšířenější technikou ke spuštění malwaru ze strany uživatele je pomocí souboru zástupce (.LNK). Ten běžně slouží k odkazům na soubory, v parametru odkazu lze ale nastavit i širší funkcionalitu. Obvyklé použití ze strany útočníka spočívá v zamaskování pomocí dvojí přípony a ikony upravené jako PDF nebo Word dokument, případně jako instalátor legitimního programu, který uživatel spustí. Nejčastější metodou je nastavení zástupce ke spuštění PowerShell nebo příkazové řádky k přímému vykonání příkazů, například ke stažení malwaru z internetu a jeho spuštění přímo v paměti. Této techniky hojně využívají např. trojany Emotet nebo Ursnif.

Mitigace: Detekce a blokace LNK souborů v přílohách e-mailu, nastavení logování příkazové řádky a PowerShell a důsledná kontrola skutečného typu souboru uživatelem.

Znázornění techniky T1566.001 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na událost: CZ PRES

ČR se dne 1. července 2022 ujala podruhé v historii předsednictví Rady EU, přičemž kybernetická bezpečnost patří spolu s posílením evropských obranných kapacit mezi pět hlavních priorit tzv. CZ PRES. Vyjma bezpečnosti kybernetického prostoru v rámci předsednických priorit je pak důležité taktéž zajištění kyberbezpečnosti samotné půlroční události.

NÚKIB si stanovil pro CZ PRES tyto priority:

1) Návrh nařízení pro vysokou společnou úroveň kybernetické bezpečnosti unijních orgánů, agentur a institucí

2) Návrh regulace bezpečnosti ICT produktů a souvisejících služeb

3) Kybernetická bezpečnost dodavatelského řetězce ICT

Obr 1: Úvodní stránka webu CZ PRES

Nelze vyloučit, že nastavenou agendu ovlivní ruská agrese vůči Ukrajině a možné hrozby z ní plynoucí. Nejvážnějšími hrozbami jsou kyberšpionáž zaměřená na zisk citlivých dat z informačních či komunikačních systémů využívaných pro potřeby CZ PRES, wiperové/ransomwarové útoky a DDoS útoky, jež by vyústily v nedostupnost kritických systémů, či zneužití kyberprostoru pro provádění informačních operací (tzv. cyber-enabled operations).

Kyberšpionáž: Je třeba brát v potaz, že během předsednictví se výrazně zvyšuje objem a citlivost předávaných informací. Pro útočníky jde o jedinečnou příležitost získat cenné poznatky, které se týkají politik a procesů EU.

Wiper/ransomware: Rozsáhlý útok pomocí wiperu či ransomwaru by potenciálně mohl způsobit nedostupnost dlouhodobějšího rázu.

DDoS: Oproti wiperu a ransomwaru způsobují DDoS útoky primárně krátkodobou nedostupnost, která navíc obvykle nemá vážné následky. S tímto typem útoků má ČR čerstvé zkušenosti, když se v dubnu tuzemské subjekty staly obětí ruskojazyčné skupiny Killnet.

Informační operace: Kyberprostor lze využít pro šíření dezinformací, například přes kompromitované legitimní účty a webové stránky. Hlavním důsledkem je především reputační újma.

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.