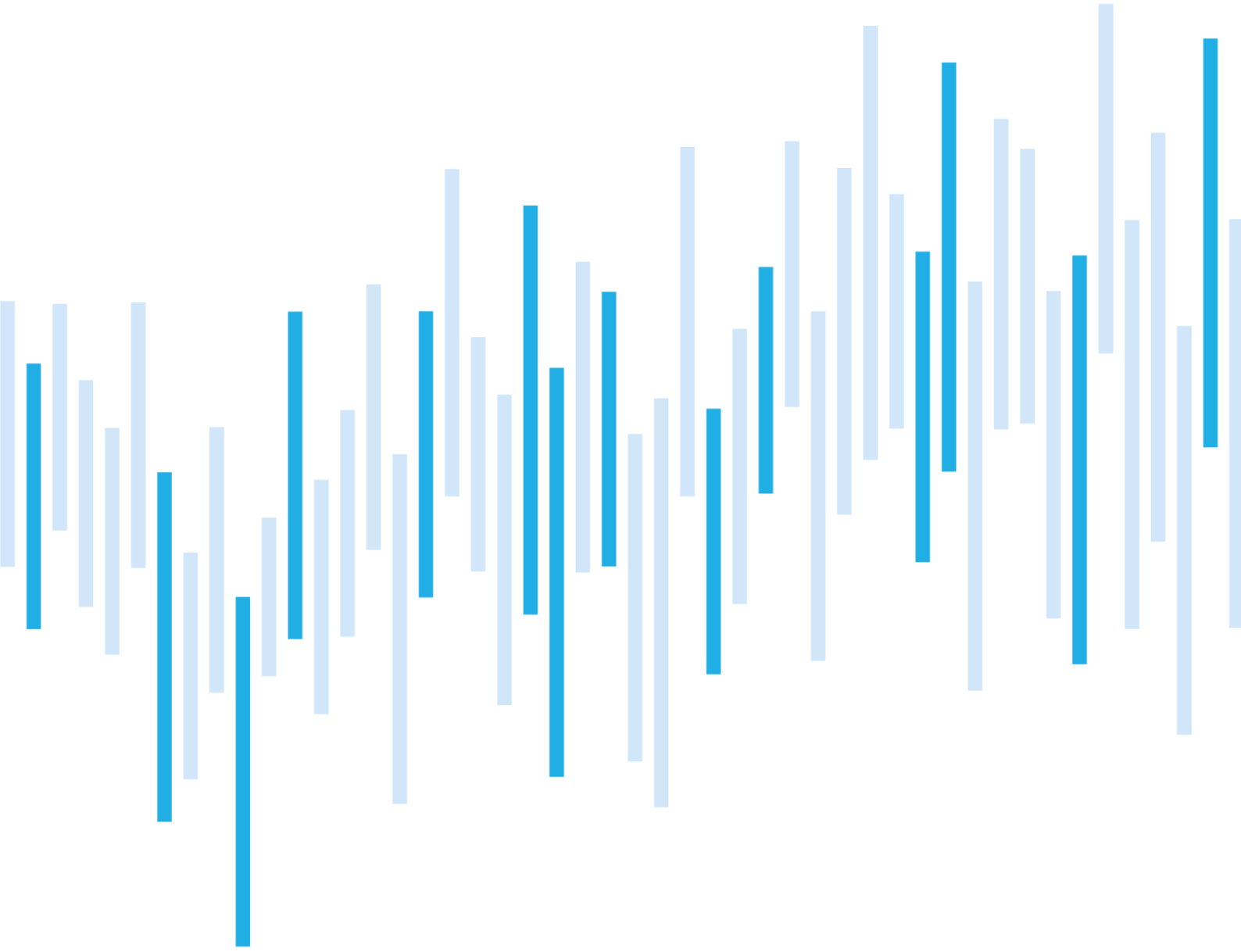
# Kybernetické incidenty pohledem NÚKIB

## ÚNOR 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

## Shrnutí měsíce

Počet kybernetických incidentů se po lednovém nárůstu způsobeném DDoS útoky vrátil do průměrných hodnot posledních 12 měsíců.

Pozornost NÚKIB se v únoru upřela na phishingovou kampaň, kterou mezi incidenty neevidujeme. Kampaň mířila na české a evropské diplomatické cíle a jejím velmi pravděpodobným záměrem byla kybernetická špionáž. Nemáme v tuto chvíli informace o tom, že by útočníci byli úspěšní a některý ze svých cílů kompromitovali. Pravděpodobný původ aktéra a výběr cílů ale ukazuje, že jeho aktivity nemůžeme podceňovat.

Analytici RecordedFuture tuto kampaň spojují s aktérem, jehož operační postupy, motivace a cíle se překrývají s předchozími aktivitami skupiny APT29 (také známé jako Nobelium nebo CozyBear). APT29 je velice pokročilý kyberšpionážní aktér, který operuje pod záštitou ruské Služby vnější rozvědky (SVR).

V reportu rozebíráme průběh útoku a podrobněji se zaměřujeme na techniku HTML Smuggling, kterou útočníci v této phishingové kampani použili. Je to technika, která je velmi obtížně detekovatelná, a tudíž i obrana proti ní samotné je obtížná. APT29 ji do svých kampaní zahrnuje už téměř dva roky.

## Obsah

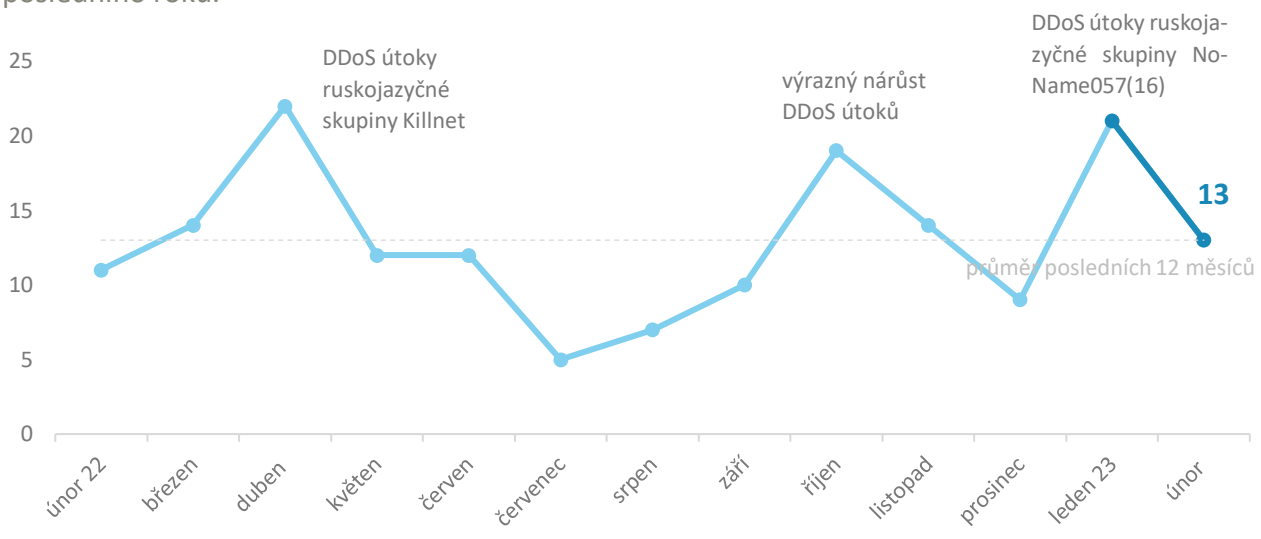


Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

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

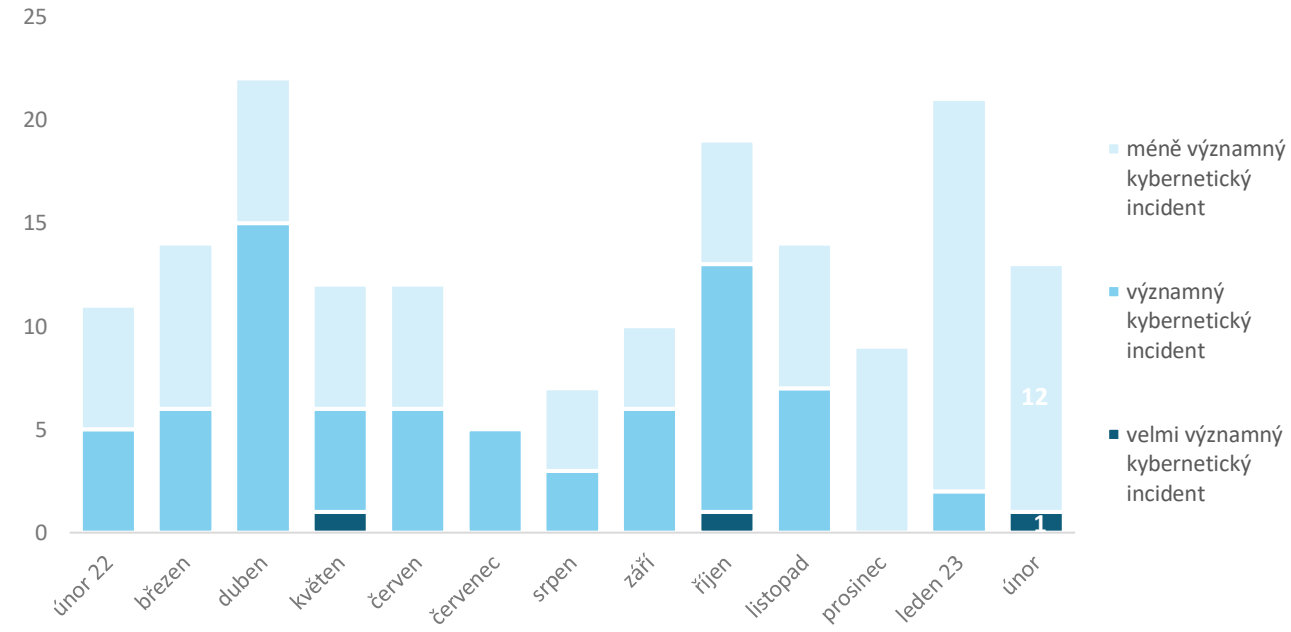
## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet kybernetických incidentů, které NÚKIB v únoru řešil, se po minulém měsíci vrátil na průměr posledního roku. [1]




## Závažnost řešených kybernetických incidentů[2]

NÚKIB po čtyřech měsících opět řešil velmi významný kybernetický incident. DDoS útok proti českému ministerstvu mu způsobil nedostupnost systémů kritické infrastruktury a výpadky služeb výrazně zasáhly do jeho činnosti. Odehrály se v několika vlnách, trvaly vždy v řádu hodin a dotkly se více jak milionu uživatelů.

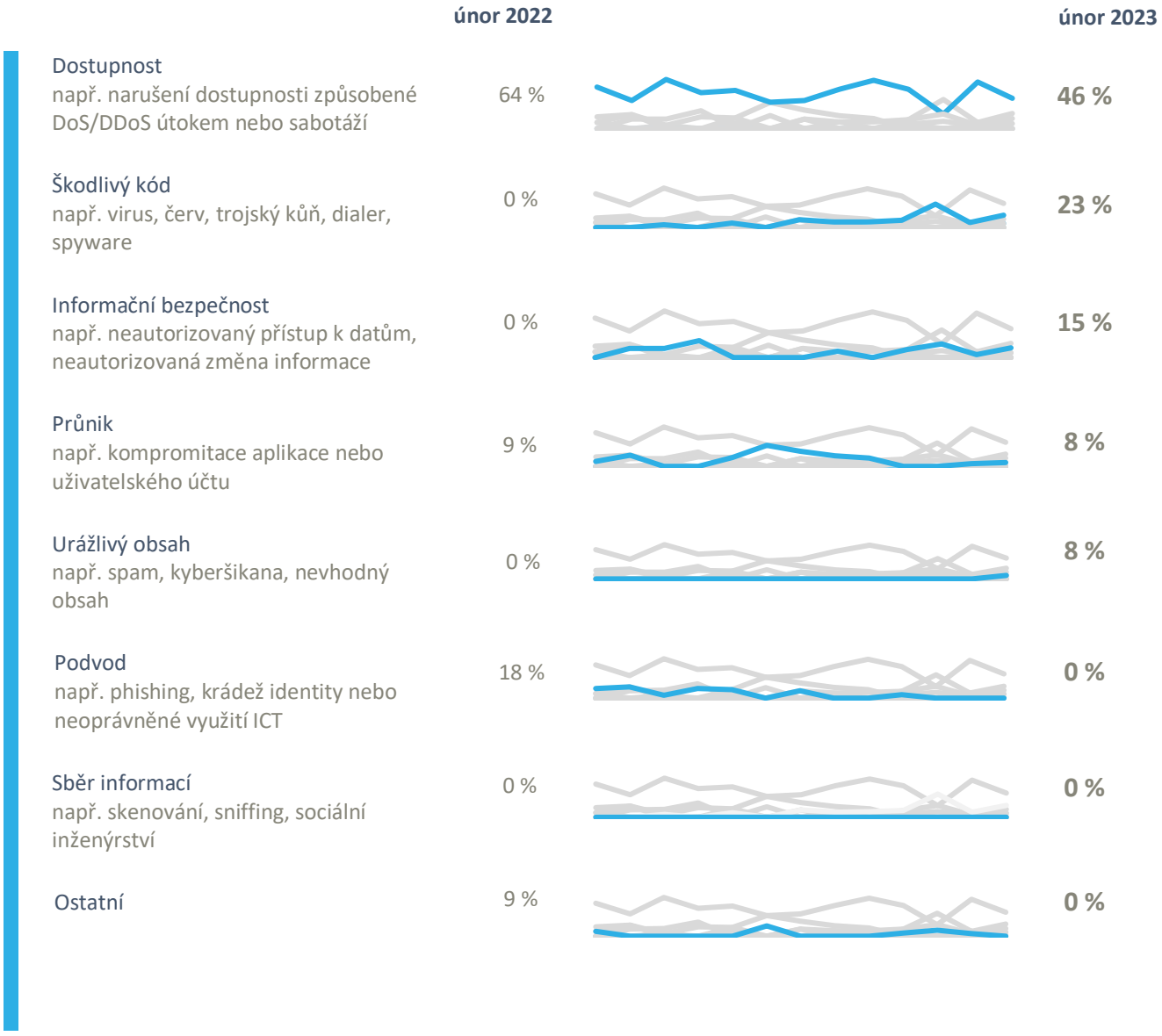



[1] Sedm incidentů NÚKIB evidoval u povinných osob dle zákona o kybernetické bezpečnosti. Zbývajících šest incidentů se týkalo neregulovaných subjektů.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

## Klasifikace incidentů nahlášených NÚKIB[3]

NÚKIB únorové incidenty zařadil do čtyř kategorií:

- Nejčastěji evidovaným typem incidentu byly incidenty, které vyústily v nedostupnost služeb. Nicméně vyjma jednoho DDoS útoku to byly incidenty způsobené výpadky služeb a technickými chybami;
- V kategorii škodlivý kód NÚKIB v únoru zaregistroval tři incidenty. Ve všech případech se jednalo o ransomwarové útoky, jeden z nich ale povinná osoba nahlásila s více jak ročním zpožděním;
- Ve dvou incidentech byla narušena bezpečnost informací. Útočníci se dostaly na server oběti, ze kterého následně stáhli data;
- Poslední dva incidenty NÚKIB klasifikoval jako průnik a urážlivý obsah. V druhém případě útočníci kompromitovali e-mailovou schránku oběti a rozeslali z ní víc jak tisíc zpráv se spamem.




[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

NÚKIB v únoru zachytil a analyzoval phishingovou kampaň, která mířila na české a evropské diplomatické cíle. Kampaň je závažná především kvůli pravděpodobnému původu útočníků, výběru jejich cílů a vysoké pravděpodobnosti, že ve svých aktivitách budou pokračovat i v následujících měsících. Podrobně se jí věnujeme v poslední kapitole tohoto reportu.

### Malware

NÚKIB v únoru podrobně analyzoval malware GraphicalNeutrino, který útočníci použili ve své phishingové kyberšpionážní kampani popsané v poslední kapitole. Některé z atributů GraphicalNeutrino se překrývají s malwarem EnvyScout, který skupina APT29 nasazovala ve svých phishingových kampaních minulý rok.

### Zranitelnosti

Zranitelnosti VMware ESXi, které jsou ve velkém zneužívány v ostatních evropských zemích, se objevily ve dvou incidentech. Ve srovnání s evropskými zeměmi, kde jsou tyto zranitelnosti masivně zneužívány, jsou ale čísla českých obětí relativně nízká.

### Ransomware

Počet kybernetických incidentů způsobených ransomwarem, které NÚKIB v únoru řešil, byl srovnatelný s předchozími deseti měsíci. Skupina ESXiArgs v únoru zasáhla dva nepovinné subjekty. Zneužitím zranitelnosti VMware ESXi jim zašifrovala virtuální servery.

### Útoky na dostupnost

Po lednové vlně DDoS útok NÚKIB tento měsíc řešil jediný. Svou nebývalou závažností se ale zařadil mezi velmi významné incidenty.

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

## Technika měsíce: HTML Smuggling

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V rámci reportu se tentokrát zaměřujeme na techniku T1027.006: HTML Smuggling. Útočníci ji použili v rámci své únorové phishingové kampaně proti českým i zahraničním diplomatickým cílům. Celé kampani se podrobněji věnujeme v následující kapitole.

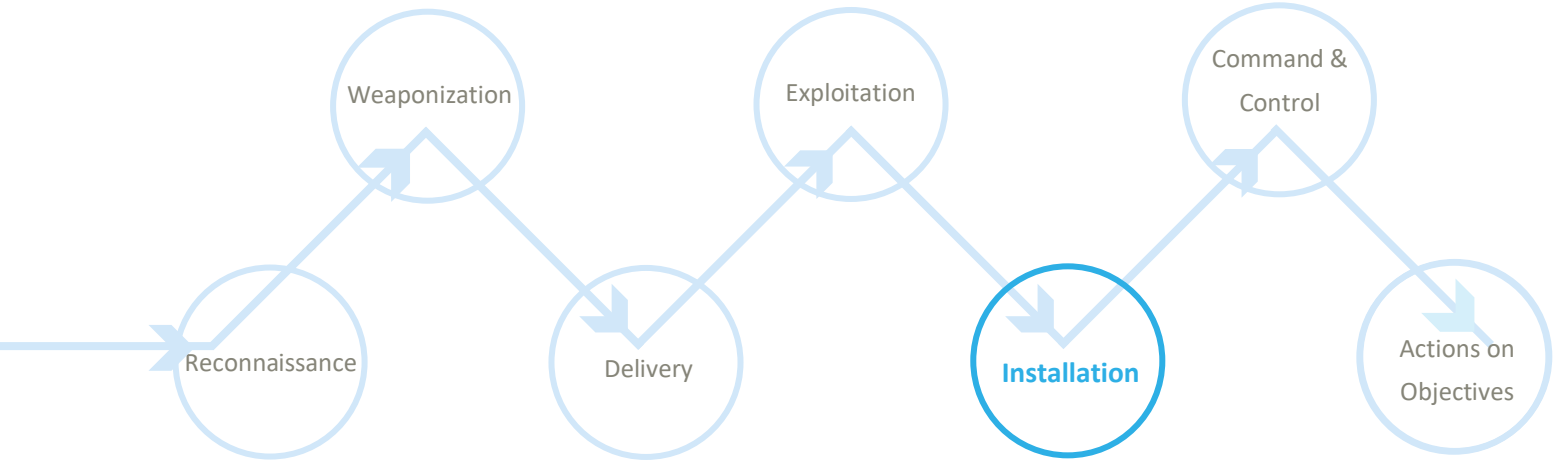
**HTML Smuggling:** HTML Smuggling je technika, kterou útočníci používají, aby se vyhnuli detekci ve chvíli, kde se malware začne stahovat do počítače. Pro obránce je to většinou příležitost k odhalení a zastavení probíhajícího útoku. Mohou totiž stahující se malware identifikovat v síťovém provozu nebo na webovém aplikačním firewallu. HTML Smugglingem se útočníci snaží toto riziko odhalení snížit. Technika funguje následovně:

> Když navštívíte nějakou webovou stránku, Váš prohlížeč nejdříve načte HTML kód a teprve poté zobrazí obsah dané stránky. Útočníci do HTML kódu „propašují“ svůj škodlivý kód, který vypadá zdánlivě neškodně. To, co některé bezpečnostní prvky vidí, je pouze neškodný HTML nebo JavaScript provoz, který navíc může být dále obfuskován, aby zakryl svůj pravý účel. Škodlivé soubory se rozbalí až ve chvíli, kdy je HTML soubor nahrán na koncové zařízení oběti. Protože se škodlivý soubor nestahuje přes síť, ale rozbalí se až za firewallem, je hůře detekovatelný.

**MITRE ID: T1027.006**

**Mitigace:** Jelikož je technika HTML Smuggling obtížně detekovatelná, je komplikovaná i její mitigace. Obrana proti ní vyžaduje několik vrstev ochrany. Útočníci techniku HTML Smuggling často používají ve svých phishingových kampaních. Z pohledu obránců je proto nejlepší útok zastavit hned na jeho počátku, tedy aby se e-mail vůbec nedostal k uživateli. Pokud e-mail propadne, uživatel ho otevře a přes odkaz se dostane na nakaženou webovou stránku, ze které se přes HTML Smuggling začne stahovat malware, jeho spuštění by měly zabránit bezpečnostní kontroly na koncových zařízeních jako např. antiviry nebo EDR platformy.

Znázornění techniky T1027.006 v kill chainu ukazujícím, v jaké fázi útoku kybernetičtí aktéři techniku používají:

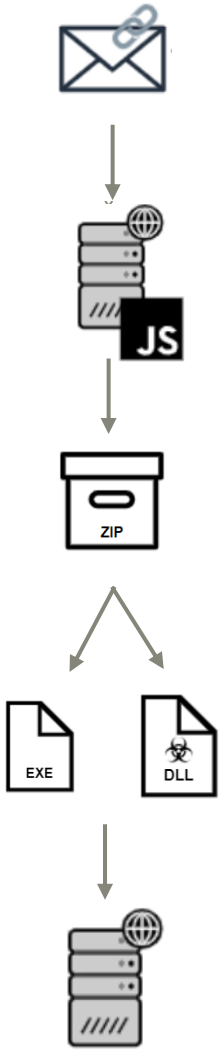


## Zaměřeno na hrozbu: Kyberšpionážní kampaň proti diplomatickým cílům

NÚKIB v únoru analyzoval phishingovou kyberšpionážní kampaň, která mířila na české a evropské diplomatické cíle. Útočníci vystupovali jako zaměstnanci českého Ministerstva zahraničních věcí (MZV), phishingové e-maily psali pod jeho hlavičkou a zneužívali tematiku schůzek velvyslanců. NÚKIB v tuto chvíli nemá informace o tom, že by útočníci byli úspěšní a některý ze systémů kompromitovali. Nicméně pravděpodobný původ aktéra a výběr jeho cílů ukazuje, že jeho aktivity nemůžeme podceňovat.

Podle analytiků z RecordedFuture za kampaní stojí aktér, jehož operační postupy, motivace a cíle se překrývají s předchozími aktivitami skupiny APT29 (také známé jako Nobelium nebo CozyBear). APT29 je velice pokročilý kyberšpionážní aktér, který operuje pod záštitou ruské Služby vnější rozvědky (SVR).

Na základě jednoho z phishingových e-mailů NÚKIB analyzoval, jak útoky únorové kampaně probíhaly:[5]




1. Kampaň začala phishingovým e-mailem. Útočníci se vydávali za zaměstnance českého MZV a tvrdili, že chtějí naplánovat schůzky velvyslanců. Součástí e-mailů byl odkaz na údajný rozvrh českého velvyslance.

2. Odkaz vedl webovou stránku, na které bylo logo českého MZV a silně obfuskovaný JavaScript.

3. Jakmile oběť na webovou stránku vstoupila, JavaScript ihned zahájil stahování ZIP archivu. Útočníci využili techniku HTML Smuggling, kterou přibližujeme v předchozí kapitole. Tuto techniku používali i při svých kampaních v loňském roce.

4. ZIP archiv obsahoval dva soubory, jeden s příponou .exe a druhý .dll. DLL soubor byl skrytý, a tudíž ho uživatel ve složce po rozbalení neviděl. Soubor .exe do sebe po spuštění naimportoval skrytý DLL soubor, což byl malware GraphicalNeutrino.

5. Malware GraphicalNeutrino si vytvořil persistenci v zařízení oběti a začal kontaktovat legitimní službu Notion. Na základě poznatků z předchozích kampaní je velmi pravděpodobné, že útočník by službu Notion dál zneužíval pro komunikaci s řídícím serverem a stáhl by další fázi malwaru. V době psaní analýzy byl ale autentizační token do Notion už neplatný a NÚKIB proto nemohl útok analyzovat až do konce.

[5] Infection chain obsahuje pouze informace, které se již dříve objevily v otevřených zdrojích. Ostatní technická zjištění záměrně vynecháváme a sdílíme je neveřejnými kanály s našimi domácími a zahraničními partnery.

Je velmi pravděpodobné, že APT29 bude ve svých aktivitách proti českým i evropským cílům pokračovat i v budoucnu. Velmi podobné špionážní kampaně totiž vede minimálně od začátku roku 2022. Časový rámec a výběr cílů z diplomatických kruhů tak naznačuje, že APT29 usiluje o získání informací týkajících se NATO/EU, případně konfliktu na Ukrajině. Dokud válka trvá, bude velmi pravděpodobně trvat i zájem ruských skupin o citlivé informace s ní spojené.

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