Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 28. LEDNA 2022

ANALÝZA HROZBY

UPOZORNĚNÍ NA ZVÝŠENÉ RIZIKO KYBERŠPIONÁŽNÍCH ČI RANSOMWAROVÝCH ÚTOKŮ PROTI ČESKÉ REPUBLICE

SHRNUTÍ

- **V důsledku stávající geopolitické situace ve východní Evropě, především na Ukrajině, existuje zvýšené riziko zejména kyberšpionážních či ransomwarových útoků proti České republice a tuzemským subjektům.**
- **Tyto aktivity mohou mít podobu kyberšpionážních operací ze strany cizí moci, destruktivních útoků směřovaných vůči narušení důvěrnosti a dostupnosti dat (ransomware či datový wiper) provedených kyberkriminálními aktéry a dezinformačních operací, které jsou podpořeny aktivitami v kyberprostoru (tzv. cyber-enabled operations).**
- **Mezi subjekty, u kterých existuje vyšší pravděpodobnost, že budou čelit kyberútoku, patří zejména strategické státní instituce, média a kritická informační infrastruktura. Ohroženy však mohou být také další typy subjektů.**
- **Vzhledem ke zvýšenému riziku útoků doporučujeme věnovat pozornost 19 technikám útoku a dále 14 nejčastěji zneužívaným zranitelnostem, jejichž přehled (včetně mitigace a detekce) je součástí analýzy.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

V DŮSLEDKU GEOPOLITICKÉ SITUACE VE VÝCHODNÍ EVROPĚ SE MOHOU STUPŇOVAT KYBERÚTOKY PROTI ČESKÉ REPUBLICE

Od podzimu 2021 se zvyšuje geopolitické napětí ve východní Evropě, především na hranicích Ukrajiny a Ruska, popř. východních hranicích zemí NATO/EU (Litva, Lotyšsko a Polsko). **Jednou z domén, kde se stupňují škodlivé aktivity je kyberprostor.** Zde probíhají nejenom operace státem zaštítěných skupin s kyberšpionážními či destruktivními motivacemi, ale i kyberkriminálních skupin nasazujících primárně ransomware. **V případě trvající eskalace je pravděpodobné, že se zvýší riziko kyberútoků proti ČR.**

Ukrajina se stala v první polovině ledna obětí datového wiperu, jenž se maskoval jako ransomware. Navzdory neznámým obětem je velmi pravděpodobné, že útok mohl usilovat o paralýzu strategických institucí po vzoru předchozích kampaní NotPetya a BadRabbit. Vyjma toho byla Ukrajina zacílena defacementem (nahrazení originálního obsahu webových stránek obsahem vytvořeným útočníkem).[1] Kyjev se navíc společně s Vilniusem, Rigou a Varšavou stává dlouhodobě cílem dezinformační kampaně Ghostwriter, jejíž významnou komponentu představují akce v kyberprostoru (tzv. cyber-enabled operations).

Na základě analýzy byly vyhodnoceny jako zvláště ohrožené strategické státní instituce, média a kritická informační infrastruktura, kdy riziko jejich zacílení roste s pokračující eskalací. Strategické instituce státu, zejména ty zodpovědné za obranu státu a zahraniční politiku, jsou zranitelné především vůči kyberšpionáži. V případě médií je z krátkodobého hlediska vyšší pravděpodobnost DDoS útoků a defacementu, primárně s ohledem na možnou komplexní kampaň zahrnující také informační operace. Kritická infrastruktura (např. energetika) je zranitelná vzhledem k pokročilým schopnostem některých aktérů provádět destruktivní útoky vůči průmyslovým řídicím systémům (ICS). **Paralýza daných sektorů výrazně snižuje efektivní schopnost se bránit ve fyzické doméně a může eventuálně vést k celospolečenským dopadům.** Specifickou kategorii představují ransomwarové útoky, jejichž obětí mohou být primárně energetika, průmysl, výzkum a zdravotnictví.

NEJČASTĚJŠÍ TECHNIKY VYUŽÍVANÉ ŠKODLIVÝMI AKTÉRY V KYBERPROSTORU

NÚKIB na základě historických dat, vlastních zdrojů a informací bezpečnostní komunity identifikoval 13 technik (TTPs) podle MITRE ATT&CK, které se nejčastěji objevovaly v letech 2020-2021. Vyjma toho bylo dodatečně identifikováno šest technik často využívaných škodlivými aktéry v kyberprostoru.[2] Informace o nich lze posléze využít ke zvýšení odolnosti organizace před kybernetickými útoky. Odkaz u každé techniky obsahuje taktéž doporučení k mitigaci možných útoků využívajících konkrétní techniku. NÚKIB doporučuje technikám a mitigaci proti nim věnovat pozornost. Níže jsou uvedeny pouze techniky patřící mezi nejvyužívanější, avšak je třeba brát v potaz, že útočníci obvykle používají širokou paletu nástrojů.

Technika	Informace
T1059 (Command and Scripting Interpreter)	Zneužití příkazové řádky ke spuštění škodlivého kódu.
T1218 (Signed Binary Proxy Execution)	Zneužití legitimních binárních souborů k proxy spuštění škodlivého kódu.
T1543 (Create or Modify System Process)	Zneužití možnosti vytvořit nebo upravit procesy na úrovni operačního systému k opakovanému spuštění škodlivého kódu.
T1053 (Scheduled Task/Job)	Zneužití plánování úloh k prvotnímu či opakujícímu se spuštění škodlivého kódu.
T1003 (OS Credential Dumping)	Pokus o vypsání přihlašovacích údajů kvůli získání údajů k účtu z OS a softwaru.
T1055 (Process Injection)	Vložení škodlivého kódu do legitimního procesu, a to zejména kvůli vyhnutí se odhalení.
T1027 (Obfuscated Files or Information)	Snaha ztížit detekci či analýzu škodlivého souboru zašifrováním nebo zaheslováním.
T1105 (Ingress Tool Transfer)	Přesunutí nástrojů či dalších souborů útočníkem z externího do kompromitovaného systému.
T1569 (System Services)	Zneužití legitimních systémových služeb nebo daemonů ke spuštění škodlivého kódu či programu.
T1036 (Masquerading)	Snaha upravit škodlivý kód a soubory, aby je bezpečnostní nástroje považovaly za legitimní nebo neškodné.
T1486 (Data Encrypted for Impact)	Zašifrování dat na cílovém systému pomocí ransomwaru.
T1082 (System Information Discovery)	Pokus o zisk detailních informací o OS a hardwaru.
T1497 (Virtualization/Sandbox Evasion)	Prostředky využité pro detekci a vyhnutí se virtualizačnímu či analytickému prostředí.
T1566 (Phishing)	Phishingové e-maily, jež mohou obsahovat škodlivou přílohu v podobě odkazu či přiloženého dokumentu.
T1078 (Valid Accounts)	Zneužití legitimních uživatelských účtů, které útočník napadl (např. znalost či krádež přihlašovacích údajů).

T1190 (Exploit Public-Facing Application)	Zneužití zranitelností aplikací či programů otevřených do sítě Internet.
T1133 (External Remote Services)	Zneužití vzdálených služeb (např. VPN) k získání prvotního přístupu.
T1595 (Active Scanning)	Aktivní skenování IP rozsahů a zranitelných systémů.
T1110 (Brute Force)	Využívání hrubé síly za účelem získání přístupu k účtům, když hesla nejsou známá nebo jsou získány jejich hashe.

NEJČASTĚJŠÍ ZRANITELNOSTI ZNEUŽÍVANÉ ŠKODLIVÝMI AKTÉRY V KYBERPROSTORU

NÚKIB na základě historických dat, vlastních zdrojů a informací bezpečnostní komunity identifikoval 14 nejčastějších zranitelností, jež jsou využívány ze strany vybraných aktérů. **Pokud subjekt provozuje některý ze zranitelných systémů, tak důrazně doporučujeme kontrolu jeho verze a případnou aktualizaci.**

Zranitelnost	Zranitelný systém
CVE-2018-13379	FortiGate VPN
CVE-2019-1653	Cisco
CVE-2019-2725	Oracle WebLogic Server
CVE-2019-7609	Kibana
CVE-2019-9670	Zimbra
CVE-2019-10149	Exim Simple Mail Transfer Protocol
CVE-2019-11510	Pulse Secure
CVE-2019-19781	Citrix
CVE-2020-0688	Microsoft Exchange
CVE-2020-4006	VMware
CVE-2020-5902	F5 Big-IP
CVE-2020-14882	Oracle WebLogic
CVE-2021-26855	Microsoft Exchange
CVE-2021-44228	Apache Log4j

DOPORUČENÍ

Vzhledem ke zvýšenému riziku útoků proti ČR a tuzemským subjektům doporučuje NÚKIB zvýšenou ostražitost před vybranými technikami a konkrétními zranitelnostmi.

NÚKIB doporučuje věnovat pozornost 19 zmíněným technikám a mitigaci proti nim, především pokud je organizace součástí některého z rizikových sektorů. Pokud organizace provozuje některý ze zranitelných systémů, tak důrazně doporučujeme kontrolu jeho verze a případnou aktualizaci.

Některé státem zaštítěné skupiny či kyberkriminální aktéři zneužívají nyní široce rozšířenou zranitelnost Log4Shell (CVE-2021-44228). NÚKIB v prosinci 2021 vydal reaktivní opatření, jež kvůli mitigaci zranitelnosti ukládá specifické úkony regulovaným subjektům. Vzhledem k možným dopadům Log4Shell doporučujeme úkony definované opatřením aplikovat i neregulovaným subjektům.

Další podpůrné materiály naleznete na webu NÚKIB, včetně dokumentu Jak se bránit útoku ransomwarem.

ZDROJE

[1] NÚKIB. 2022. Komentář GovCERT.CZ k napadení webů ukrajinské vlády a doporučení k zabezpečení. https://www.nukib.cz/cs/infoservis/hrozby/1789-komentar-govcert-cz-k-napadeni-webu-ukrajinske-vlady-a-doporuceni-k-zabezpeceni/

[2] Seznam kombinuje nejčastější techniky za rok 2020 dle Red Canary (viz https://redcanary.com/threat-detection-report/techniques/) a dále v období od října 2020 do října 2021 dle reportu Picus Security (viz https://www.picussecurity.com/picus-the-red-report-21). Oba reporty předkládají 13 nejčastějších technik, které doplňuje šest dalších významných technik na základě dat NÚKIB či partnerských organizací.

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách http://www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **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.
Oranžová **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.
Zelená **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.
Bílá **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.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

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 %*