TLP: WHITE

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 20. DUBNA 2021

UPOZORNĚNÍ NA ZVÝŠENÉ RIZIKO KYBERNETICKÝCH ÚTOKŮ PROTI ČESKÉ REPUBLICE

SHRNUTÍ

- **V důsledku aktuálního dění nelze vyloučit nárůst počtu kybernetických útoků směřujících vůči České republice, jejím zájmům, organizacím, které v ČR sídlí, případně dalším subjektům významným pro ČR.**
- **Tyto aktivity mohou mít podobu špionážních kybernetických operací, případně se může jednat i o destruktivní útoky v podobě sabotáží průmyslových systémů a útoků prostřednictvím ransomwaru/wiperu (malware, který nenávratně smaže data). Mezi subjekty, u kterých existuje vyšší pravděpodobnost, že budou čelit kybernetickému útoku, patří zejména vládní instituce, ozbrojené síly a firmy v sektoru energetiky a průmyslu. Ohroženy však mohou být i subjekty z dalších sektorů.**
- **Vzhledem ke zvýšenému riziku útoků NÚKIB doporučuje věnovat pozornost 23 technikám útoku a 17 nejčastěji zneužívaným zranitelnostem, jejichž přehled tvoří přílohu tohoto dokumentu.**

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.

TYPY ÚTOKŮ, K NIMŽ MŮŽE DOJÍT

- **Špionážní kybernetické operace;**
- **destruktivní útoky v podobě sabotáží průmyslových systémů;**
- **útoky prostřednictvím ransomwaru/wiperu (malware, který nenávratně smaže data);**
- **další typy útoků na důvěrnost a integritu dat (konkrétně například zneužití informací z e-mailové komunikace získaných kybernetickou špionáží k dezinformačním kampaním).**

ZVLÁŠTĚ OHROŽENÉ SEKTORY A SYSTÉMY

- **Vládní sektor, u něhož hrozí zneužití dat získaných špionáží v dezinformačních operacích;**
- **významné podniky, u nichž hrozí útoky prostřednictvím ransomwaru/wiperu;**
- **kritická informační infrastruktura, významné informační systémy a systémy poskytovatelů základní služby dle zákona o kybernetické bezpečnosti (hrozí všechny typy útoků);**
- **webové stránky (v krátkodobém horizontu je vyšší pravděpodobnost útoků typu DDoS a defacementu webových stránek médií a státních institucí);**
- **výzkum a vývoj;**
- **finanční sektor.**

NEJČASTĚJŠÍ TECHNIKY VYUŽÍVANÉ KYBERNETICKÝMI AKTÉRY

NÚKIB na základě historických dat, vlastních zdrojů a informací bezpečnostní komunity identifikoval 23 aktuálně nejpoužívanějších technik. Informace o těchto technikách lze využít ke zvýšení odolnosti organizace před kybernetickými útoky. Odkaz u každé z technik obsahuje i doporučení k mitigaci případných kybernetických útoků. Doporučujeme těmto technikám a jejich mitigaci věnovat pozornost, zejména pokud je organizace součástí některého z rizikových sektorů, viz výše. Níže jsou uvedeny pouze techniky, které patří mezi nejvyužívanější. Je třeba brát v potaz, že APT skupiny používají širokou paletu nástrojů a níže uvedené jsou pouze ty nejfrekventovanější.

Číslo techniky	Název techniky	Informace o technice	Odkaz s informacemi o mitigaci a detekci
T1566	Phishing	Phishingové e-maily, které mohou obsahovat škodlivou v přílohu v podobě odkazu nebo přiloženého dokumentu.	Odkaz MITRE
T1078	Valid Accounts	Zneužití legitimních uživatelských účtů, které útočník kompromitoval (např. znalostí či krádeží přihlašovacích údajů).	Odkaz MITRE
T1190	Exploit Public-Facing Application	Zneužití zranitelností aplikací či programů otevřených do sítě Internet (webové stránky, SQL databáze, SMB, SSH apod.).	Odkaz MITRE
T1133	External Remote Services	Zneužití vzdálených služeb (VPN, Citrix apod.) k získání prvotnímu přístupu k síti.	Odkaz MITRE
T1195	Supply Chain Compromise	Zneužití produktu třetí strany (softwarové aktualizace, manipulace zdrojového kódu apod.) ke kompromitaci cílového systému.	Odkaz MITRE
T1212	Exploitation for Credential Access	Zneužití zranitelnosti softwaru ke sběru přihlašovacích údajů.	Odkaz MITRE
T1606.002	Forge Web Credentials: SAML Tokens	Zfalšování SAML tokenů s libovolnými autorizacemi či životností. Zfalšované tokeny umožnují útočníkovi autentizaci ve službách využívající SAML 2.0 jako SSO (single sign-on) mechanismus.	Odkaz MITRE
T1059	Command and Scripting Interpreter	Zneužití příkazové řádky (zejména příkazová řádka Windows a PowerShell) ke spuštění škodlivého kódu.	Odkaz MITRE
T1569	System Services	Zneužití legitimních systémových služeb, nebo daemonů ke spuštění škodlivého kódu nebo programu.	Odkaz MITRE
T1543	Create or Modify System Process	Zneužití možnosti vytvořit, nebo upravit procesy na úrovni systému (zejména ve Windows) k opakovanému spuštění škodlivého kódu.	Odkaz MITRE

T1053	Scheduled Task/Job	Zneužití plánování úloh (zejména Windows Task Scheduler) k prvotnímu, nebo opakujícímu se spouštění škodlivého kódu.	Odkaz MITRE
T1055	Process Injection	Vložení škodlivého kódu do legitimního procesu, zejména ve snaze vyhnout se odhalení.	Odkaz MITRE
T1218	Signed Binary Proxy Execution	Zneužití legitimních binárních souborů (zejména mshta.exe a rundll32.exe) k proxy spuštění škodlivého kódu.	Odkaz MITRE
T1218.005	Mshta	Zneužití Windows nástroje Mshta.exe k proxy spuštění škodlivých .hta souborů, javaskriptů nebo VBS skriptů.	Odkaz MITRE
T1218.011	Rundll32	Zneužití Rundll32.exe k proxy spuštění škodlivého kódu, zejména ve formátu DLL.	Odkaz MITRE
T1027	Obfuscated Files or Information	Snaha ztížit detekci/analýzu škodlivého souboru jeho zašifrováním, zaheslováním apod.	Odkaz MITRE
T1036	Masquerading	Snaha upravit škodlivý kód a soubory tak, aby je bezpečnostní nástroje považovaly za legitimní nebo neškodné.	Odkaz MITRE
T1003	OS Credential Dumping	Pokus o vypsání přihlašovacích údajů kvůli získání údajů k účtu z operačního systému a softwaru.	Odkaz MITRE
T1003.001	LSASS Memory	Pokus o zisk a zneužití přihlašovacích údajů uložených v procesové paměti LSASS.	Odkaz MITRE
T1497	Virtualization/Sandbox Evasion	Prostředky využité pro detekci a vyhnutí se virtualizačním a analytickým prostředím.	Odkaz MITRE
T1082	System Information Discovery	Pokus o zisk detailních informací o operačním systému a hardwaru.	Odkaz MITRE
T1105	Ingress Tool Transfer	Přesunutí nástrojů nebo dalších souborů útočníkem z externího do kompromitovaného systému.	Odkaz MITRE
T1219	Remote Access Software	Zneužití legitimní desktopové podpory a softwaru pro vzdálený přístup kvůli vytvoření interaktivního C2 kanálu pro zacílení systémů uvnitř sítí.	Odkaz MITRE

NEJČASTĚJŠÍ ZRANITELNOSTI ZNEUŽÍVANÉ KYBERNETICKÝMI AKTÉRY

NÚKIB identifikoval 17 nejčastějších zranitelností, které byly a nadále jsou využívány některými APT skupinami. Nejedná se o konečný seznam zneužívaných zranitelností. **Pokud organizace provozuje některý ze zranitelných systémů, důrazně doporučujeme kontrolu jeho verze a jeho případnou aktualizaci.**

Zranitelnost	Zranitelný systém	Komentář	Odkaz
CVE-2019-0604	Microsoft SharePoint	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0604
CVE-2019-11510	Pulse Connect Secure (PCS) VPN	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510
CVE-2020-1472	Netlogon	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472
CVE-2017-8759	Microsoft .NET Framework	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8759
CVE-2019-1132	Windows (Win32k)	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1132
CVE-2018-4878	Adobe Flash Player	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4878
CVE-2018-20250	WinRAR	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20250
CVE-2018-13379	Fortinet FortiGate VPN	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379
CVE-2019-9670	Synacor Zimbra Collaboration Suite	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9670
CVE-2019-19781	Citrix Application Delivery Controller and Gateway	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781
CVE-2020-4006	VMware Workspace ONE Access	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4006

CVE-2018-0802	Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, aMicrosoft Office 2016 (Equation Editor)	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0802
CVE-2018-0798	Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 a Microsoft Office 2016 (Equation Editor)	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0798
CVE-2017-11882	Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, a Microsoft Office 2016	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882
CVE-2017-0199	Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199
CVE-2019-0708	Remote Desktop Services	**Podle nástroje Shodan je zranitelnost aktivní na 712 zařízeních v ČR.**	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
CVE-2019-10149	Exim (Mail Transfer Agent)	**Podle nástroje Shodan je zranitelnost aktivní na 74 zařízeních v ČR.**	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10149

DOPORUČENÍ

Vzhledem ke zvýšenému riziku útoků doporučujeme ostražitost před konkrétními technikami kybernetických útoků a zneužití konkrétních zranitelností. NÚKIB doporučuje věnovat pozornost 23 výše uvedeným technikám a jejich mitigaci, zejména pokud je organizace součástí některého z rizikových sektorů, viz výše.

Pokud organizace provozuje některý ze zranitelných systémů, důrazně doporučujeme kontrolu jeho verze a jeho případnou aktualizaci.

Další podpůrné materiály naleznete na webu NÚKIB včetně dokumentu „Jak se bránit útoku ransomwarem“ nebo aktuální informace o hrozbách a zranitelnostech.

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.us-cert.gov/tlp). 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 použita jinou osobou než konkrétní osobou na straně příjemce, které byla informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým lze tuto informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit po dohodě s původcem informace.
Oranžová TLP: AMBER	Informace může být sdílena pouze mezi pracovníky příjemce, kteří mají 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, nebudou-li výslovně stanoveny další osoby, kterým ji lze poskytnout.
Zelená TLP: GREEN	Informace může být sdílená v rámci příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály. Příjemce při předání musí zajistit důvěrnost komunikace informace. Příjemce nesmí informaci poskytnout veřejně, může ji však při splnění a zajištění stejných podmínek ochrany předat dalším partnerským subjektům příjemce.
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.