Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 18. LISTOPADU 2021
SITUAČNÍ PŘEHLED

ZNEUŽÍVÁNÍ ZRANITELNOSTI PROXYSHELL PRO POTŘEBY DORUČOVÁNÍ MALWARU: NÚKIB DETEKUJE VÍCE NEŽ 450 ZRANITELNÝCH SERVERŮ V ČR. MITIGACE V PODOBĚ PATCHOVÁNÍ ZRANITELNOSTÍ POSTUPUJE POMALU

SHRNUTÍ

- **NÚKIB od začátku listopadu detekuje vlnu zneužívání zranitelnosti ProxyShell pro potřeby sofistikovaného doručování phishingových zpráv, které obsahují malware. ProxyShell je soubor trojice zranitelností, jejichž zneužití umožňuje kompromitovat službu Microsoft Exchange Server. Tato série zranitelností se poprvé objevila už v srpnu 2021, ale nyní NÚKIB eviduje její aktivní zneužívaní.**
- **Incident nahlásilo několik subjektů, avšak vzhledem ke značné rozšířenosti MS Exchange Server je pravděpodobné (55-70 %), že počet kompromitací bude mnohem vyšší. Ke dni 18. listopadu bylo v ČR zranitelných celkem 454 serverů, což od 5. listopadu (detekováno 595 zranitelných serverů), kdy NÚKIB vydal webové upozornění, představuje jenom malý pokles. Nadále jde o vážnou hrozbu nejen pro povinné osoby dle zákona o kybernetické bezpečnosti, ale také pro velkou část českých uživatelů.**
- **Útočníci zneužitím zranitelnosti ProxyShell získávají kontrolu nad servery, načež si stahují obsah mailboxů a navazují na legitimní komunikaci. Ze schránek jsou poté rozesílány phishingové e-maily, které eventuálně vedou k instalaci malwarů SquirrelWaffle, QakBot či DanaBot. Ty poté slouží jako prostředky pro rozmístění ransomwarů (např. Conti) či dalších škodlivých programů.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací získaných v rámci činnosti NÚKIB ke dni 18. listopadu 2021.

NÚKIB od začátku listopadu 2021 detekuje vlnu zneužívání zranitelnosti ProxyShell pro potřeby sofistikovaného doručení phishingových zpráv, které obsahují malware. Několik subjektů již nahlásilo incident, ale vzhledem k celkovému počtu uživatelů služby Microsoft Exchange Server je pravděpodobné (55-70 %), že celkový počet obětí bude vyšší.

Série zranitelností ProxyShell se poprvé objevila už letos v srpnu. NÚKIB na ni v létě upozorňoval, ale až nyní eviduje její aktivní zneužívání. Pravděpodobně (55–70 %) je to způsobeno aktivitami útočníků na darkwebu, přičemž nyní nabízený skript usnadňuje akce proti cíli. Skript se na neveřejných fórech nabízí již od října a objevil se též při incidentech hlášených NÚKIB.

BOX 1: ProxyShell

Společně s ProxyLogon a ProxyOracle se jedná o součást série zranitelností, které cílí na službu MS Exchange Server. ProxyShell je soubor trojice zranitelností (CVE-2021-34473, CVE-2021-34523 a CVE-2021-31207), jejichž zneužití umožní převzít kontrolu nad servery.

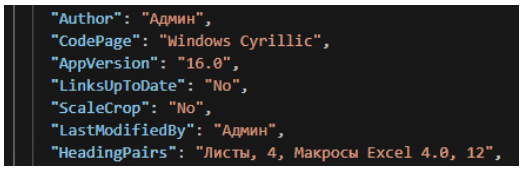
ÚTOČNÍCI NAVAZUJÍ NA LEGITIMNÍ KOMUNIKACI: KAMPAŇ ZATÍM NELZE PŘISUZOVAT KONKRÉTNÍM AKTÉRŮM

Útočníci při současné kampani získají kontrolu nad servery MS Exchange Server zneužitím zranitelnosti ProxyShell. Následně si stáhnou obsah mailboxů, navazují na předchozí legitimní komunikaci a ze schránek odesílají zprávy obsahující malware. Napadení uživatelé po prokliku stáhnou excelový dokument, který obsahuje makra.

Spuštění maker vede k instalaci malwarů SquirrelWaffle (loader pro další malwary), QakBot (loader pro ransomwary – např. Conti) či DanaBot (banking trojan). Vzhledem k tomu, že jsou zprávy odesílány z legitimních serverů, snižuje se možnost záchytu antispamem a nepomohou ani ochranné technologie (např. SPF, DKIM a DMARC).

NÚKIB v tuto chvíli nemá dostatek informací, aby probíhající kampaň přisoudil konkrétním aktérům. Podle zjištění Úřadu však byly škodlivé excelové dokumenty vytvořeny v ruské verzi programu. Toto zjištění však samo o sobě k atribuci nestačí a nelze vyloučit (25-50 %) útok pod falešnou vlajkou (false flag), kdy útočníci záměrně napodobují jiné aktéry.

Obrázek 1: Metadata souboru v ruské verzi



Zdroj: Interní zdroje NÚKIB

Podle interní threat intelligence platformy probíhá kampaň minimálně od září 2021. Zneužívání tzv. e-mailových řetězců se podobá kampani Emotet, ve které útočníci také navazovali na předchozí legitimní konverzaci svých obětí.

NÚKIB DETEKUJE V ČR VÍCE NEŽ 450 ZRANITELNÝCH SERVERŮ

Ke dni 18. listopadu bylo v ČR zranitelných 454 serverů. Přestože dne 5. listopadu, kdy NÚKIB na stávající kampaň upozornil, bylo zranitelných 595 serverů, jedná se pouze o pomalý proces mitigace. Zranitelné jsou mimo jiné systémy, jež se nacházejí v rozsazích zákonem regulovaných poskytovatelů internetových služeb (ISP).

ROZSÁHLOST KAMPANĚ DETEKUJE TAKÉ MEZINÁRODNÍ KOMUNITA

Dle informací partnerů si stávající kampaně všímají také další státy EU. V některých případech již byly detekovány záchyty ransomwaru. NÚKIB využívá pro komunikaci s partnery zvláštní kanály a situaci nadále monitoruje.

MITIGACE: JE POTŘEBA BEZODKLADNĚ PROVÉST AKTUALIZACI ČI REINSTALOVAT KOMPROMITOVANÉ SERVERY

NÚKIB vyzývá k aktualizaci na nejnovější kumulativní update. Dále je doporučeno, aby došlo k aktualizaci též v případě, kdy server není přímo přístupný z internetu, jelikož spuštěním malwaru obdrženého zvenčí může dojít ke zneužití zevnitř sítě.

Lucemburský CIRCL upozornil, že jediným postupem, jak zajistit kompletní opravu a mitigovat situaci, je reinstalace všech kompromitovaných serverů. Ve všech případech je doporučeno provést proces incident response, včetně auditu systému. Pokud došlo k laterálnímu pohybu uvnitř systému, tak existuje vysoké riziko, že aktér nasadí ransomware, případně exfiltruje data.

PŘÍLOHA 1: MITRE ATT&CK

NÚKIB v rámci jednoho detekovaného incidentu identifikoval také některé techniky, taktiky a procedury (TTPs). Přestože se nejedná o všechny TTPs využívané v rámci kampaně cílící proti MS Exchange Server, tak zavedení mitigačních postupů vůči nim výrazně snižuje pravděpodobnost kompromitace. Útočníci využívají následující techniky:

Obrázek 3: Detekované techniky (incident vůči nejmenovanému subjektu)

Initial access (19 items)	Execution (45 items)	Persistence (119 items)	Privilege escalation (103 items)	Defense evasion (177 items)	Credential access (57 items)	Discovery (42 items)	Lateral movement (27 items)	Collection (38 items)	Command and control (46 items)	Exfiltration (18 items)	Impact (26 items)
Exploit Public-Facing Application	Malicious Link	Valid Accounts	Valid Accounts	File Deletion	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	Local Email Collection	Application Layer Protocol	Automated Exfiltration	Data Manipulation
Phishing	Python	.bash_profile and .bashrc	.bash_profile and .bashrc	Indicator Removal on Host	ARP Cache Poisoning	Application Window Discovery	Component Object Model and Distributed COM	ARP Cache Poisoning	Asymmetric Cryptography	Data Transfer Size Limits	Account Access Removal
Valid Accounts	AppleScript	Accessibility Features	Abuse Elevation Control Mechanism	Valid Accounts	AS-REP Roasting	Browser Bookmark Discovery	Distributed Component Object Model	Adversary-in-the-Middle	Bidirectional Communication	Exfiltration Over Alternative Protocol	Application Exhaustion Flood

Zdroj: Interní zdroje NÚKIB

- **Exploit Public-Facing Application (T1190)**

Popis: Útočníci využívají slabiny v programech/systémech, které jsou přístupné z internetu. V případě stávající kampaně se jedná o MS Exchange Server ve verzích 2013, 2016 a 2019.

Mitigace: Application Isolation and Sandboxing (M1048), Exploit Protection (M1050), Network Segmentation (M1030), Privileged Account Management (M1026), Update Software (M1051), Vulnerability Scanning (M1016)

- **Phishing (T1566)**

Popis: Útočníci posílají phishingové zprávy, aby se dostali do systémů obětí. V případě stávající kampaně jsou phishingové zprávy odesílány jako součást tzv. e-mailových řetězců, kdy navazují na legitimní komunikaci mezi uživateli. Většina zpráv je anglicky, nicméně objevily se již i méně kvalitní české překlady.

Mitigace: Antivirus/Antimalware (M1049), Network Intrusion Prevention (M1031), Restrict Web-Based Content (M1021), Software Configuration (M1054), User Training (M1017)

- **Valid Accounts (T1078)**

Popis: Útočníci zneužívají přístupy k existujícím legitimním účtům, aby získali počáteční přístup či persistenci, eskalovali oprávnění nebo se vyhnuli obraně. Během stávající kampaně jsou využity e-mailové účty na kompromitovaných serverech služby MS Exchange Server.

Mitigace: Application Developer Guidance (M1013), Password Policies (M1027), Privileged Account Management (M1026), User Training (M1017)

- **User Execution: Malicious Link (T1204.001)**

Popis: Útočník spoléhá na uživatelovo kliknutí na škodlivý odkaz, aby došlo ke spuštění škodlivého kódu. Během nynější kampaně vede škodlivý odkaz ke stažení infikovaných excelových dokumentů.

Mitigace: Network Intrusion Prevention (M1031), Restrict Web-Based Content (M1021), User Training (M1017)

- **Command and Scripting Interpreter: Python (T1059.006)**

Popis: Útočníci zneužívají příkazy a skripty v jazyce Python pro provedení útoku.

Mitigace: Antivirus/Antimalware (M1049), Audit (M1047), Execution Prevention (M1038), Limit Software Installation (M1033)

- **Indicator Removal on Host: File Deletion (T1070.004)**

Popis: Útočníci mohou mazat soubory zanechané v systému aktivitami v rámci intruze.

Mitigace: N/A

- **Indicator Removal on Host (T1070)**

Popis: Útočníci mohou mazat či pozměnit generované artefakty v systému, včetně logů nebo zachycených souborů (např. malware v karanténě). V kontextu kampaně jde především o mazání zpráv ze složky odeslané pošty.

Mitigace: Encrypt Sensitive Information (M1041), Remote Data Storage (M1029), Restrict File and Directory Permissions (M1022)

- **Email Collection: Local Email Collection (T1114.001)**

Popis: Útočníci mohou cílit na uživatelské e-maily, aby sbírali citlivé informace. V rámci stávající kampaně je podobným způsobem navazováno na legitimní komunikaci prostřednictvím e-mailového klienta.

Mitigace: Encrypt Sensitive Information (M1041)

- **Data Manipulation (T1565)**

Popis: Útočníci mohou vkládat, mazat a manipulovat data pro potřebu manipulace či skrývání svých aktivit.

Mitigace: Encrypt Sensitive Information (M1041), Network Segmentation (M1030), Remote Data Storage (M1029), Restrict File and Directory Permissions (M1022)

PŘÍLOHA 2: KILL CHAIN

NÚKIB vytvořil tzv. kill chain, který detailně mapuje postup kompromitace. Ten se skládá celkem ze sedmi fází, jimiž jsou průzkum (Reconnaissance), weaponizace (Weaponization), doručení (Delivery), zneužití (Exploitation), instalace (Installation), C2 (Command and Control) a akce proti cíli (Actions on Objectives). Blíže k rámci: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Vyhledání serverů MS Exchange zranitelných na CVE-2021-34473, CVE-2021-34523 a CVE-2021-31207, které jsou přístupné z internetu. Toto útočník může zjistit například pomocí nástroje Shodan či aktivním skenováním.

Od konce října 2021 jsou na neveřejných fórech nabídky prodeje speciálně upraveného skriptu ke zneužívání zranitelností ProxyShell. Skript podle popisu může získat přístup k e-mailové schránce libovolného uživatele na zranitelném serveru, stáhnout její obsah a následně jménem oběti automatizovaně rozesílat zprávy navázané na původní vlákno legitimní konverzace. Skript též komplikuje detekci, neboť neukládá tyto zprávy mezi odeslanou poštu.

Ke spuštění daného skriptu a zneužití serveru postačuje útočníkovi pouze veřejná IP adresa či znalost e-mailové adresy uživatele.

Zneužitím zranitelnosti získá útočník přístup k e-mailové schránce uživatele a celému obsahu zpráv.

Na zajištěné zprávy a konverzace ze schránek naváže útočník vlastními podvrženými zprávami, které obsahují odkazy na stažení první fáze malwaru. Tou je XLS dokument, jenž obsahuje dropper ve formě VBA makra. To po spuštění stáhne a nainstaluje na systém příjemce QakBot, DanaBot nebo SquirrelWaffle. Jelikož jsou zprávy rozesílány přímo z napadeného serveru a ze schránky legitimního účtu, tak jsou antispam i technologie SPF, DKIM a DMARC neefektivní.

SquirrelWaffle po napadení sbírá informace o systému a posléze data odesílá na řídící server v obfuskované podobě pomocí HTTP požadavku. Server na základě získaných informací zašle zpět instrukce, například ke stažení dalších nástrojů.

Pomocí phishingu posílaného z legitimního účtu dochází k šíření malwaru jak uvnitř napadené organizace, tak směrem ven. Infekce malwarem QakBot, DanaBot nebo SquirrelWaffle následně vede k instalaci dalšího malwaru či ransomwaru v závislosti na záměrech útočníka.

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách 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 %*