Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 24. ŘÍJNA 2024

SITUAČNÍ PŘEHLED

NEZNÁMÝ ÚTOČNÍK ZNEUŽÍVÁ IDENTITY SPOLEČNOSTÍ AMAZON, MICROSOFT A ČESKÝCH INSTITUCÍ PRO KOMPROMITACI OBĚTÍ SKRZE NÁSTROJ VZDÁLENÉ SPRÁVY: NÚKIB DOPORUČUJE ZVÝŠENOU OBEZŘETNOST A PROVEDENÍ PREVENTIVNÍCH KROKŮ

SHRNUTÍ

- **Během dne 23. října NÚKIB obdržel informace od partnerů o aktivní phishingové kampani neznámého útočníka. Útoky byly potvrzeny v několika partnerských zemích, včetně vyšších desítek případů v České republice, přičemž celkový rozsah a objem útoků může nadále růst.**
- **Phishingový útok spočívá v zaslání e-mailu s tematikou nastavení služby pro sdílení dat a vzdálené správy společnosti Amazon. Text se taktéž odkazuje na zavedení politiky nulové důvěry (Zero Trust policy). Příloha s různými názvy, vždy však ve formátu .rdp (Remote Desktop Protocol), vede uživatele skrze dialogové okno ke spuštění vzdálené správy mezi jeho zařízením a infrastrukturou útočníka. V rámci dialogového okna je pro navýšení důvěry uvedena škodlivá doména zneužívající názvy vládních institucí v napadené zemi.**
- **Potvrzení vzdálené správy umožní útočníkům přístup k souborům a síťovým zařízením oběti, potenciálně i možnost spouštět programy třetích stran a vlastních skriptů útočníků.**
- **V případě jakéhokoli podezření na kompromitaci či záchyt škodlivého e-mailu neváhejte kontaktovat bezpečnostní tým vaší instituce, případně i přímo NÚKIB na adrese cert.incident@nukib.gov.cz.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací, které jsou veřejně dostupné, byly získány v rámci činnosti NÚKIB či pocházejí od partnerů.

Ukrajinský CERT-UA a několik dalších partnerů NÚKIB 23. října upozornili na phishingovou kampaň s tematikou nastavení služby AWS Secure Data Exchange. **Útočník se přitom vydává za společnosti Amazon, Microsoft a vládní kyberbezpečnostní instituce v napadených zemích.** Podle CERT-UA mají být cílem vládní a armádní instituce, ale i soukromé společnosti v řadě sektorů. **Mezi indikátory kompromitací se objevila i celá řada falešných domén zneužívající identitu českých vládních institucí a ministerstev, včetně NÚKIB.**

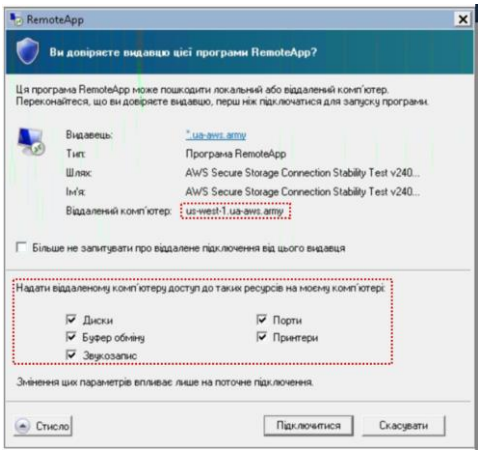
Kampaň je založena na rozesílání phishingových e-mailů, které obecně navádí oběť k otevření škodlivé přílohy ve formátu .rdp (Remote Desktop Protocol). Ta má údajně sloužit k nastavení služby AWS Secure Data Exchange společnosti Amazon pro vzdálenou správu zařízení a odkazuje taktéž na zavádění politiky nulové důvěry (Zero Trust), jakožto bezpečnostního opatření. **Reálně však tento soubor, po potvrzení výzvy v dialogovém oknu, spustí vzdálenou správu mezi kompromitovaným zařízením a infrastrukturou útočníka. Podle dostupných informací kampaň cílí nejen na Českou republiku, ale i celou řadu dalších západních států včetně Ukrajiny.**

Spuštění škodlivého souboru má útočníkům zajistit přístup nejen k uložišti a síťovým zařízením, ale potenciálně i možnost spouštět programy třetích stran či vlastních skriptů. **V případě kompromitace tak útočník získá takřka plnou kontrolu nad napadeným zařízením, které může být využito pro další škodlivé aktivity.**

Mezi indikátory kompromitací se objevila i celá řada domén, které zjevně zneužívají identitu českých vládních institucí, včetně NÚKIB. Objevují se ve formátu nukib-gov[.]cloud. Seznam českých škodlivých domén obsahuje ministerstva, vládu, státní úřady i PČR (viz Box 1). Tyto domény slouží ke zvýšení důvěryhodnosti kampaně, jelikož po otevření souboru je oběť vyzvána k potvrzení navázání vzdálené správy v dialogovém okně (viz Obrázek 1). Jako vzdálené

zařízení se zobrazí právě falešná doména ze seznamu (tj. zaměstnancům NÚKIB by se zobrazila doména nukib-gov[.]cloud). **V současnosti nelze určit, zdali se podobným způsobem snaží útočníci cílit i na jiné než v seznamu domén uvedné organizace, nelze to však vyloučit (25–50 %).**

Obr. 1: Dialogové okno potvrzující navázání vzdálené správy z infrastruktury útočníka



Zdroj: cert.gov.ua

NÚKIB v době psaní analýzy disponuje informacemi o vyšších desítkách případů zacílení českých subjektů. Vzhledem k povaze a počtu zveřejněných falešných domén či potvrzených záchytů kampaně v partnerských zemích je pravděpodobné (55–70 %), že počet útoků bude přibývat.

DOPORUČENÍ A MITIGACE

Obdobně jako CERT-UA i NÚKIB doporučuje sadu kroků, které mohou zamezit případné kompromitaci.

- Blokace .rdp souborů v rámci e-mailové služby
- Omezení práv uživatelů spouštět .rdp soubory
- Nastavení firewallu k omezení možnosti programu mstsc.exe navazovat vzdálený přístup
- Nastavit pravidla, která zabrání uživatelům při použití RDP přesměrování lokálních zdrojů.

Pro zpětné odhalení kompromitace je třeba analyzovat síťový provoz na přiložené IP adresy a názvy domén. Dále též v aktuálním měsíci samostatně analyzovat legitimitu všech odchozích síťových připojení na libovolné IP adresy v internetu na portu 3389/tcp.

NÚKIB doporučuje všem příjemcům této zprávy zvýšenou obezřetnost před e-maily s výše popsanou tematikou. V případě jakéhokoli podezření neváhejte kontaktovat bezpečnostní tým vaší instituce, případně přímo NÚKIB na adrese cert.incidentukib.gov.cz.

Box 1: Seznam domén zneužívajících identitu českých vládních institucí

md-gov[.]cloud

mf-gov[.]cloud

mo-gov[.]cloud

mpo-gov[.]cloud

mpsv-gov[.]cloud

msmt-gov[.]cloud

mv-gov[.]cloud

my-gov[.]cloud

mzd-gov[.]cloud

mze-gov[.]cloud

mzp-gov[.]cloud

mzv-gov[.]cloud

nakit-gov[.]cloud

nbu-gov[.]cloud

nukib-gov[.]cloud

policie-gov[.]cloud

mmr-gov[.]cloud

uohs-gov[.]cloud

uoou-gov[.]cloud

vlada-gov[.]cloud

PŘÍLOHA 2: INDIKÁTORY KOMPROMITACE

Síťové indikátory kompromitace	Typ
yulia.antonenko@townoflakelure.com	e-mail
alexandra.gerst@townoflakelure.com	e-mail
oleksii.myronov@townoflakelure.com	e-mail
ca-central-1.awsplatform[.]online	Doména
ca-west-1.mfa-gov[.]cloud	Doména
central-2-aws.ua-aws[.]army	Doména
eu-central-1-aws.mfa-gov[.]cloud	Doména
eu-central-1.mfa-gov[.]cloud	Doména
eu-central-1.ukrtelecom[.]cloud	Doména
eu-central-2-aws.ua-aws[.]army	Doména
eu-north-1-aws.ua-energy[.]cloud	Doména
eu-north-1-aws.ua-gov[.]cloud	Doména
eu-south-1-aws.mfa-gov[.]cloud	Doména
eu-south-2-aws.mfa-gov[.]cloud	Doména
eu-southeast-1-aws.gov-ua[.]cloud	Doména
eu-southeast-1-aws.govtr[.]cloud	Doména
eu-southeast-1-aws.zero-trust[.]solutions	Doména
us-east-1-aws.mfa-gov[.]cloud	Doména
us-east-2-aws.ua-gov[.]cloud	Doména
us-east-console.awsplatform[.]online	Doména
us-west-1-amazon.ua-energy[.]cloud	Doména

us-west-1.aws-ukraine[.]cloud	Doména
us-west-1.ua-aws[.]army	Doména
us-west-1.ukrtelecom[.]cloud	Doména
us-west-2-aws.mfa-gov[.]cloud	Doména
zero-trust[.]solutions	Doména
ukrtelecom[.]cloud	Doména
awsplatform[.]online	Doména
aws-ukraine[.]cloud	Doména
aws-s3[.]cloud	Doména
aws-meet[.]cloud	Doména
aws-il[.]cloud	Doména
aws-data[.]cloud	Doména
aws-meetings[.]cloud	Doména
aws-secure[.]cloud	Doména
aws-join[.]cloud	Doména
aws-online[.]cloud	Doména
gov-au[.]cloud	Doména
gov-aws[.]cloud	Doména
gov-fi[.]cloud	Doména
gov-gr[.]cloud	Doména
gov-lt[.]cloud	Doména
gov-lv[.]cloud	Doména
gov-pl[.]cloud	Doména

gov-sk[.]cloud	Doména
gov-trust[.]cloud	Doména
gov-ua[.]cloud	Doména
govps[.]cloud	Doména
govtr[.]cloud	Doména
govua[.]cloud	Doména
eru-gov[.]cloud	Doména
feedzai-gov[.]cloud	Doména
md-gov[.]cloud	Doména
mf-gov[.]cloud	Doména
mo-gov[.]cloud	Doména
mpo-gov[.]cloud	Doména
mpsv-gov[.]cloud	Doména
msmt-gov[.]cloud	Doména
mv-gov[.]cloud	Doména
my-gov[.]cloud	Doména
mzd-gov[.]cloud	Doména
mze-gov[.]cloud	Doména
mzp-gov[.]cloud	Doména
mzv-gov[.]cloud	Doména
nakit-gov[.]cloud	Doména
nbu-gov[.]cloud	Doména
nukib-gov[.]cloud	Doména

policie-gov[.]cloud	Doména
mmr-gov[.]cloud	Doména
uohs-gov[.]cloud	Doména
uoou-gov[.]cloud	Doména
vlada-gov[.]cloud	Doména
voa-gov[.]cloud	Doména
mfa-gov[.]cloud	Doména
mfa-gov[.]cloud	Doména
mfa-gov-il[.]cloud	Doména
mfa-gov-il[.]cloud	Doména
mfa-gov-tr[.]cloud	Doména
mfa-gov-tr[.]cloud	Doména
mil-be[.]cloud	Doména
mil-ee[.]cloud	Doména
mil-pl[.]cloud	Doména
mil-pt[.]cloud	Doména
mod-gov-il[.]cloud	Doména
mod-gov-il[.]cloud	Doména
s3-acronis[.]cloud	Doména
s3-army[.]cloud	Doména
s3-atlassian[.]cloud	Doména
s3-aws[.]cloud	Doména
s3-bah[.]cloud	Doména

s3-be[.]cloud	Doména
s3-blackberry[.]cloud	Doména
s3-csis[.]cloud	Doména
s3-de[.]cloud	Doména
s3-dgap[.]cloud	Doména
s3-dk[.]cloud	Doména
s3-dnc[.]cloud	Doména
s3-esa[.]cloud	Doména
s3-fbi[.]cloud	Doména
s3-hudson[.]cloud	Doména
s3-ida[.]cloud	Doména
s3-iri[.]cloud	Doména
s3-knowbe4[.]cloud	Doména
s3-marcus[.]cloud	Doména
s3-monitoring[.]cloud	Doména
s3-nato[.]cloud	Doména
s3-ned[.]cloud	Doména
s3-nsa[.]cloud	Doména
s3-proofpoint[.]cloud	Doména
s3-pt[.]cloud	Doména
s3-rackspace[.]cloud	Doména
s3-rand[.]cloud	Doména
s3-spacex[.]cloud	Doména

s3-state[.]cloud	Doména
s3-stig[.]cloud	Doména
s3-ua[.]cloud	Doména
s3-ucia[.]cloud	Doména
s3-zoho[.]cloud	Doména
ua-aws[.]army	Doména
ua-energy[.]cloud	Doména
ua-gov[.]cloud	Doména
ua-gov[.]cloud	Doména
ua-mil[.]cloud	Doména
ua-sec[.]cloud	Doména
ua-se[.]cloud	Doména
ua-sn[.]cloud	Doména
37.153.155[.]143 (Email)	IP adresa
45.42.142[.]49 (Email)	IP adresa
45.42.142[.]89 (Email)	IP adresa
199.204.86[.]87 (Email)	IP adresa
181.215.148[.]194 (Email)	IP adresa
104.247.120[.]157 (Email)	IP adresa
204.111.198[.]27 (Email)	IP adresa
136.0.0[.]11 (Email)	IP adresa
38.180.110[.]238	IP adresa
179.43.148[.]82	IP adresa

45.11.230[.]105	IP adresa
45.141.58[.]60	IP adresa
95.217.113[.]133	IP adresa
185.187.155[.]74	IP adresa
141.195.117[.]125	IP adresa
185.76.79[.]178	IP adresa
2.58.201[.]112	IP adresa
89.46.234[.]115	IP adresa
84.32.188[.]193	IP adresa
38.180.146[.]210	IP adresa
84.32.188[.]197	IP adresa
45.80.193[.]9	IP adresa
45.67.85[.]40	IP adresa
45.134.111[.]123	IP adresa
84.32.188[.]153	IP adresa
62.72.7[.]213	IP adresa
93.188.163[.]16	IP adresa
23.160.56[.]122	IP adresa
95.156.207[.]121	IP adresa
84.32.188[.]148	IP adresa
166.0.187[.]233	IP adresa
185.216.72[.]196	IP adresa
38.180.146[.]230	IP adresa

84.32.188[.]200	IP adresa
45.11.231[.]8	IP adresa
162.252.175[.]233	IP adresa
13.49.21[.]253	IP adresa
179.43.163[.]18	IP adresa
46.19.141[.]186	IP adresa
193.29.59[.]9	IP adresa
135.181.130[.]232	IP adresa
45.134.110[.]83	IP adresa
185.187.155[.]73	IP adresa
23.160.56[.]100	IP adresa

Host-based indikátory kompromitace	SHA-256 Hash	MD5 Hash
Zero Trust Architecture Configuration.rdp	34c88cd591f73bc47a1a0fe2a4f594f628be98ad2366eeb4e467595115d8505a	a5de73d69c1a7fbae2e71b98d48fe9b5
ZTS Device Compatibility Test.rdp	071276e907f185d9e341d549b198e60741e2c7f8d64dd2ca2c5d88d50b2c6ffc	8bcb741a204c25232a11a7084aa2221f
Device Configuration Verification.rdp	6e6680786fa5b023cf301b6bc5faaa89c86dc34b696f4b078cf22b1b353d5d3c	86f58115c891ce91b7364e5ff0314b31
Zero Trust Architecture Configuration.rdp	31f2cc1157248aec5135147073e49406d057bebf78b3361dd7cbb6e37708fbcc	80b3cad4f70b6ea8924aa13d2730328b
Device Security Requirements Check.rdp	88fd6a36e8a61597dd71755b985e5fcd0b8308b69fc0f4b0fc7960fb80018622	c0da30b71d58e071fc5863381444d9f0
Device Security Requirements Check.rdp	b8327671ebc20db6f09efc4f19bd8c39d9e28c9a37bdd15b2fd62ade208d2e8a	1595266bb78dc1e3d67f929154824c74

Device Configuration Verification.rdp	a5bbb109faefcecba695a84a737f5e47fa418cea39d654bb512a6f4a0b148758	222c83d156a41735c38cc552a7084a86
Zero Trust Architecture Configuration.rdp	5534cc837ba4fa3726322883449b3e97ca3e0d28c0ccf468b868397fdfa44e0b	fa9af43e9bbb55b7512b369084d91f4d
Zero Trust Security Environment Compliance Check.rdp	b9ab481e7a9a92cfa2d53de8e7a3c75287cff6a3374f4202ec16ea9e03d80a0b	281a28800a4ba744bfde7b4aff46f24e
Device Configuration Verification.rdp	18a078a976734c9ec562f5dfa3f5904ef5d37000fb8c1f5bd0dc2dee47203bf9	d37cd2c462af0e0643076b20c5ff561e
AWS IAM Quick Start.rdp	bb4d5a3f7a40c895882b73e1aca8c71ea40cef6c4f6732bec36e6342f6e2487a	e465a4191a93195094a803e5d4703a90
Device Configuration Verification.rdp	ef4bd88ec5e8b401594b22632fd05e401658cf78de681f81409eadf93f412ebd	3f753810430b26b94a172fbf816e7d76
Zero Trust Security Environment Compliance Check.rdp	1cfe29f214d1177b66aec2b0d039fec47dd94c751fa95d34bc5da3bbab02213a	434ffae8cfc3caa370be2e69ffaa95d1
ZTS Device Compatibility Test.rdp	3a2496db64507311f5fbd3aba0228b653f673fc2152a267a1386cbab33798db5	c287c05d91a19796b2649ebebd27394b
AWS IAM Configuration.rdp	984082823dc1f122a1bb505700c25b27332f54942496814dfd0c68de0eba59dc	aabbfd1acd3f3a2212e348f2d6f169fc
Zero Trust Security Environment Compliance Check.rdp	383e63f40aecdd508e1790a8b7535e41b06b3f6984bb417218ca96e554b1164b	b0a0ad4093e781a278541e4b01daa7a8
Device Security Requirements Check.rdp	296d446cb2ad93255c45a2d4b674bbacb6d1581a94cf6bb5e54df5a742502680	a18a1cad9df5b409963601c8e30669e4
ZTS Device Compatibility Test.rdp	129ba064dfd9981575c00419ee9df1c7711679abc974fa4086076ebc3dc964f5	cbbc4903da831b6f1dc39d0c8d3fc413
AWS IAM Quick Start.rdp	f2acb92d0793d066e9414bc9e0369bd3ffa047b40720fe3bd3f2c0875d17a1cb	bd711dc427e17cc724f288cc5c3b0842
AWS IAM Compliance Check.rdp	f357d26265a59e9c356be5a8ddb8d6533d1de222aae969c2ad4dc9c40863bfe8	b38e7e8bba44bc5619b2689024ad9fca
AWS IAM Configuration.rdp	280fbf353fdffefc5a0af40c706377142fff718c7b87bc8b0daab10849f388d0	40f957b756096fa6b80f95334ba92034

Zero Trust Security Environment Compliance Check.rdp	8b45f5a173e8e18b0d5c544f9221d7a1759847c28e62a25210ad8265f07e96d5	db326d934e386059cc56c4e61695128e
Zero Trust Security Environment Compliance Check.rdp	ba4d58f2c5903776fe47c92a0ec3297cc7b9c8fa16b3bf5f40b46242e7092b46	f58cf55b944f5942f1d120d95140b800

ZDROJE

CERT-UA. 2024. RDP configuration files as a means of obtaining remote access to a computer or "Rogue RDP" (CERT-UA#11690). https://cert.gov.ua/article/6281076

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí 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+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
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: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.

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 %*