Upozorňujeme na zneužívání identit Amazon, Microsoft a českých institucí

nukib.gov.cz/cs/infoservis/hrozby/2182-upozornujeme-na-zneuzivani-identit-amazon-microsoft-a-ceskych-instituci

Ve středu 23. října Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) obdržel informace od partnerů, včetně ukrajinského CERT-UA, 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. Útočník se přitom vydává za společnosti Amazon, Microsoft a vládní kyberbezpečnostní instituce v napadených zemích. Podle ukrajinského CERT-UA mají být cílem vládní a armádní instituce, ale i soukromé společnosti v řadě sektorů.

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 Policii ČR (úplný seznam níže).

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.

NÚKIB proto doporučuje sadu kroků, které mohou zamezit případné kompromitaci:

- Blokace souborů .rdp 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.

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

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.

Podrobnější informace naleznete zde.