Upozorňujeme na zneužívání identit Amazon, Microsoft a českých institucí

24.10.2024 - | Národní úřad pro kybernetickou a informační bezpečnost

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:

Seznam domén zneužívajících identitu českých vládních institucí:

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.

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