Phishingová kampaň zasáhla Česko. NÚKIB už hlásí desítky obětí

novinky.cz/clanek/internet-a-pc-bezpecnost-podvodnik-utoci-v-cesku-40494441

Lenka Zoulová, Miloslav Fišer

Internetoví podvodníci často rozesílají e-maily, které vyvolávají dojem, že pocházejí od důvěryhodné firmy, banky, úřadu nebo webové stránky. Pomocí těchto zpráv se útočníci snaží vylákat citlivé informace, které se týkají například bankovních kont. Tato data následně využívají k odčerpání financí z účtu postiženého. Přesně tak fungují phishingové podvody.

Na takovéto phishingové zprávy už dávno nenarazíme pouze v nevyžádaných e-mailech, ale také v reklamách na různých pochybných webech či v podvodných nabídkách na sociálních sítích.

Rozsáhlá útočná kampaň

Při phishingových útocích zneužívají hackeři známé značky pravidelně. Tak rozsáhlá kampaň podvodných e-mailů, jakou nyní bezpečnostní experti zachytili, patří ale k těm historicky největším.

Kolik let prožijí Češi ve zdraví? Je to výrazně méně než průměrný věk dožití

Seznam Native

„Útočníci využívají důvěryhodnost známých firem jako Amazon a Microsoft, aby oklamali oběti, a rovněž zneužívají jména vládních institucí v jednotlivých zemích. Falešné e-maily, které rozesílají, se tváří, že pocházejí od těchto firem nebo vládních kyberbezpečnostních agentur," stojí v nejnovějším varování kyberbezpečnostního úřadu.

Podle něj jsou problémem především „sofistikované odkazy a přílohy", které phishingové zprávy obsahují. „Ty mají za cíl kompromitovat bezpečnost zařízení uživatelů. Cílem útoků jsou

podle ukrajinského CERT-UA především vládní a armádní organizace, avšak také soukromé společnosti napříč různými sektory," konstatoval NÚKIB.

Právě zahraniční partneři, tedy i zmiňovaný ukrajinský tým CERT-UA, upozornili české bezpečnostní experty na probíhající phishingovou kampaň již ve středu. Kampaň totiž nezasáhla pouze naši domovinu, ale také další země. V tuzemsku jsou evidovány již vyšší desítky případů, kdy byly phishingové útoky úspěšné.

Bezpečnostní experti přitom předpokládají, že počet postižených ještě poroste. Jaké konkrétní firmy či organizace byly útokem zasaženy, však NÚKIB neuvedl. Otazník tak zatím visí i nad tím, zda se kybernetičtí nájezdníci zmocnili nějakých citlivých dat.

Podvodné domény

Zvláštní pozornost si zaslouží fakt, že útočníci vytvořili celou řadu podvodných domén, které napodobují české vládní instituce. „Tyto domény jsou koncipovány tak, aby působily důvěryhodně, a jejich formát často odpovídá například adresám jako ‚nukib-gov.cloud'," varovali bezpečnostní experti.

V seznamu identifikovaných škodlivých domén se podle nich objevují také instituce jako Ministerstvo vnitra, vláda ČR, Policie České republiky a další klíčové státní orgány. Tato skutečnost představuje pro kybernetickou bezpečnost země mimořádné riziko, neboť mnoho uživatelů by mohlo být snadno oklamáno zdánlivě autentickými odkazy.

„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," poradili pracovníci kyberbezpečnostního úřadu.

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

Podvodníci si hrají na novináře

Uživatelé by se měli mít na pozoru před různými investičními podvody, ve kterých útočníci zneužívají jméno zpravodajského serveru Novinky.cz. Na snadné výdělky lákají podvodníci zpravidla v souvislosti se známými osobnostmi. V posledních měsících se objevily například falešné články s prezidentem Petrem Pavlem či moderátorem Janem Krausem.

Jde nicméně o typický phishingový podvod, kdy se útočníci snaží pod vidinou snadného zisku z lidí vylákat peníze. Podvod je to ale poměrně propracovaný, všechny odkazy ve falešném článku vedou na další podvodný web.

Aby důvěřivce kyberzločinci co nejvíce zmátli, nechtějí po něm v některých případech vyplňovat okamžitě čísla kreditních karet ani odesílat žádné peníze. Vše začíná registrací na dané platformě, načež uživatele bude kontaktovat správce platformy. Teprve s jeho pomocí jsou pak z důvěřivců vylákány peníze. Nemusí ho přitom kontaktovat pouze e-mailem, ale klidně i telefonicky.

Poradíme, na co si dát pozor a jak nesednout podvodníkům na lep, a to v dříve uveřejněném článku.

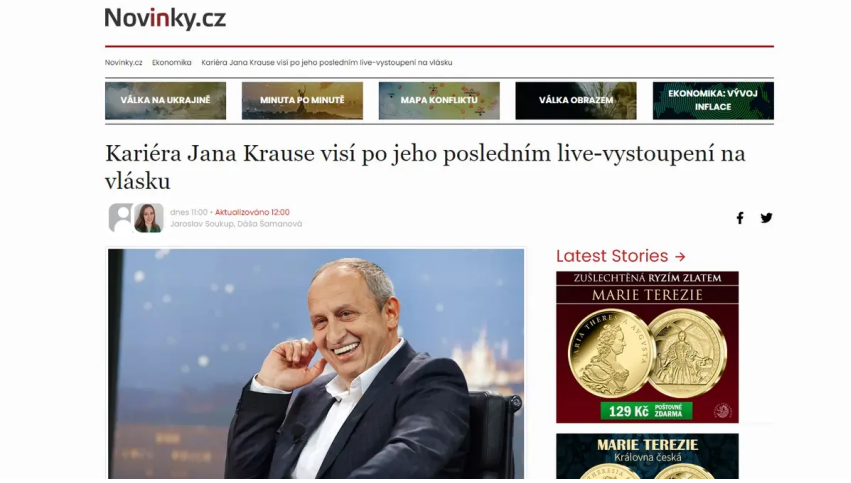

Foto: Novinky

+4

Vězeňská služba, soudy i ministerstvo spravedlnosti. Hackeři zaútočili na cíle v Česku

Bezpečnost