

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **122** ze dne **23.10.2025**

PDF je oblíbeným formátem uživatelů, ale i kyberzločinců

Bezpečnostní agentura Cisco Talos upozorňuje na rostoucí počet phishingových kampaní, které zneužívají zdánlivě neškodné PDF soubory. Útočníci do nich vkládají loga a názvy známých značek a falešné QR kódy nebo podvržená telefonní čísla. Snaží se nalákat oběti na podvodné webové stránky nebo je donutit kontaktovat falešné zákaznické centrum. Zneužívají tak nejen důvěru uživatelů v renomované technologické společnosti, ale také obcházejí zabezpečení firemních zařízení.

"Na PDF dokumenty si lidé zvykli jako na standardní kanál pro komunikaci od firem, bank nebo státu. Vnímají je jako bezpečné a důvěryhodné. Právě této důvěry kyberzločinci nyní systematicky zneužívají pro phishingové útoky," komentuje kyberbezpečnostní expert Cisco Milan Habrcetl nejnovější zjištění agentury Cisco Talos. "Útočníci s oblibou kombinují zejména PDF soubory a QR kódy. Tato technika jim umožňuje maskovat škodlivý obsah a ztěžuje jeho detekci tradičními e-mailovými filtry. Obranou je nejen robustnější kybernetické zabezpečení, ale především vzdělávání zaměstnanců uvnitř firem."

Phishingové útoky stojí na získání důvěry prostřednictvím kradené identity. Často si přitom "půjčují" identitu globálních značek, ale i lokálních firem s velkým počtem zákazníků. Cílem je přesvědčit příjemce, aby v podvrženém dokumentu kliknul na škodlivý odkaz, naskenoval QR kód, nebo zavolal na podvodné telefonní číslo.

Princip útoku je relativně jednoduchý. Hackeři se vydávají za zástupce globální společnosti a pošlou email s PDF souborem, který vizuálně i obsahově odpovídá zneužité firmě. Součástí je falešný QR kód s přesměrováním na phishingové stránky, často chráněné CAPTCHA kódy pro zvýšení důvěryhodnosti. Útočníci navíc někdy vkládají škodlivé odkazy do anotací, poznámek nebo formulářových polí, kde nejsou při strojové kontrole na první pohled viditelné. V takovém případě QR kód odkazuje na legitimní stránku zneužité společnosti, aby posílil důvěryhodnost, zatímco přiložená poznámka obsahuje skutečný phishingový odkaz.

Celosvětově nejčastěji zneužívanými jmény jsou velcí technologičtí hráči jako Microsoft, Adobe nebo Paypal. Experti Cisco Talos například zadrželi phishingový e-mail, který lákal na "zvýšení výplaty" a obsahoval QR kód směřující na falešnou stránku Microsoftu. Jindy se oběť setkala s PDF souborem s logem Adobe. Ten lákal na podvrženou stránku napodobující Dropbox. U nás máme bohaté zkušenosti s masivními podvodnými kampaněmi zneužívajícími identitu České pošty a logistických firem.

"QR kódy představují obzvláště rafinovanou techniku, protože obcházejí textovou analýzu e-mailových filtrů. Celé tělo podvodného e-mailu může být vloženo do PDF přílohy, což ztěžuje detekci tradičními bezpečnostními nástroji. Bez pokročilé analýzy pomocí optického rozpoznávání znaků tyto útoky snadno proklouznou," varuje Habrcetl.

Alarmující je také nárůst takzvaných TOAD útoků (Telephone-Oriented Attack Delivery), kdy PDF dokumenty obsahují telefonní číslo a žádost, aby příjemce telefonicky vyřešil "neodkladnou" záležitost. Útočník se následně vydává za zákaznickou podporu a pod záminkou pomoci získá citlivé údaje nebo oběť navede k instalaci škodlivého softwaru.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **122** ze dne **23.10.2025**

Experti na kyberbezpečnost odhalili, že útočníci často využívají VoIP služby pro zachování anonymity. Navíc stejná telefonní čísla používají opakovaně po několik dní. Tento přístup jim umožňuje vybudovat důvěryhodnou "značku" a efektivně manipulovat s více oběťmi současně.

Podle odborníků Cisco se proto firmy mají chránit nejen robustním kybernetickým zabezpečením, ale také osvětou a vzděláváním svých zaměstnanců. "Zneužití důvěry v zavedené značky, zejména prostřednictvím známých formátů jako PDF nebo skrze telefonickou komunikaci, ukazuje na stále vyšší úroveň vynalézavosti phishingových útočníků. Na straně firem proti nim musí stát nejen dobré kybernetické zabezpečení, ale také zaměstnanci, kteří přemýšlejí," uzavírá Habrcetl.

Zdroj: AV centrum ČR