ESET: Češi se nejčastěji potýkají s útoky na bankovní identitu a falešnými kupujícími na bazarech

2.6.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastějšími phishingovými útoky byly v období od ledna do března 2025 falešné SMS a zprávy v chatovacích aplikacích (Messenger, WhatsApp). Útočníci se tímto způsobem snažili získat přístup k bankovní identitě obětí. Bezpečnostní experti z ESETu zachytili tento typ podvodu ve více než čtvrtině případů všech phishingových útoků na Česko. V pětině případů pak zůstalo rizikem i prodávání zboží na internetových bazarových platformách. Objevily se také podvody zacílené na české bankovní účty a držitele kryptoměn. Rostoucí hrozbou byly i propracované investiční podvody lákající na zbohatnutí nákupem kryptoměn nebo jiných komodit. Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET.

Podle dat společnosti ESET bylo nejvíce případů phishingových podvodů za první čtvrtletí 2025 zachyceno v lednu. Phishing je jednou z technik sociálního inženýrství a útočníci při něm využívají manipulativní komunikaci k získání financí nebo přihlašovacích údajů. Ve sledovaném období převažovaly útoky na bankovní identitu českých občanů a podvodná komunikace na bazarových platformách. Mezi sledovanými škodlivými aktivitami však nechyběly ani podvodné weby s vizuály českých bank nebo falešné kryptoměnové směnárny. Investiční podvody se pak nejvíce objevovaly v březnu.

„Phishingové útoky se staly nedílnou součástí kybernetických rizik, kterým dnes čelíme úplně stejně, jako škodlivým kódům. Podvodná manipulativní komunikace je přitom v mnoha ohledech daleko úspěšnější než klasický útok škodlivým kódem. Proto dnes útočníci phishing zapojují i do složitých kybernetických útoků. Pomáhá jim zkrátka otevřít cestu do zařízení a k financím obětí. Obrana v těchto případech není snadná, ale není ani nemožná. Ideální je kombinovat všeobecnou ostražitost v online světě s moderními ochrannými technologiemi," říká Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET.

Phishingové útoky v Česku měly ve sledovaném období nejčastěji podobu podvodné SMS zprávy nebo zprávy v chatovacích aplikacích, ve které se útočníci snažili přesvědčit své oběti, že mají nezaplacenou pokutu za dopravní přestupek. Bezpečnostní experti tento typ phishingového útoku detekují pod označením Kidnab.

„Jedním z nejčastějších případů podvodné komunikace byla SMS zpráva o dopravním přestupku. Útočníci vyzývali své oběti k urgentnímu uhrazení pokuty, k čemuž jim mělo sloužit vyplnění formuláře přes datovou schránku. Navedli svou oběť na web datových schránek k přihlášení pomocí bankovní identity. Jak webová stránka datové schránky, tak rozhraní bankovní identity ale byly falešné. Cílem útočníků bylo získat přihlašovací údaje napadených uživatelů," vysvětluje Novotný.

Na ústupu zatím nejsou ani známé podvody na internetových bazarech. Tento typ podvodu je v Česku velmi rozšířený již několikátým rokem a čísla z prvního letošního čtvrtletí nasvědčují tomu, že se s ním budeme nadále setkávat. Útočníci k vytvoření podvodu využívají podvržené stránky známých přepravních společností a bezpečnostní experti tento typ útoku označují jako Phishing.Agent.GFH. Další zachycené phishingové útoky pak nejčastěji mířily také na kryptoměny a klasické bankovní účty.

„Na internetových bazarech se stále setkáváme se scénářem, kdy se podvodník vydává za kupujícího. Oběti, která je v tomto případě v pozici prodávajícího, zašle odkaz na falešný formulář nebo platební bránu, která často vypadá jako služba známého dopravce. Podvodník své oběti tvrdí, že částku k zaplacení zboží si může vyzvednout prostřednictvím brány nebo formuláře, pokud tam zadá údaje ke své kartě nebo přístupové údaje do svého online bankovnictví – zpravidla včetně bezpečnostního kódu z autorizační SMS zprávy. Oběť ale v tomto případě jen útočníkovi umožní přístup ke svým penězům," vysvětluje Novotný.

Kromě phishingových útoků, jejichž cílem jsou přístupové údaje k našim bankovním účtům nebo cenným a dobře zpeněžitelným datům, jsou v Česku hojně zastoupeny také investiční podvody. Tento typ hrozby od začátku ledna kontinuálně stoupal po celé první čtvrtletí. Útočníci nejčastěji lákají na investice do kryptoměn nebo jiných, lukrativních komodit s vidinou rychlého zisku. Bezpečnostní experti z ESETu tyto podvody detekují pod názvem Nomani.

„Investiční podvody, které v současnosti sledujeme, začínají většinou tzv. clickbaitovou reklamou na sociálních sítích. Pokud na ni člověk klikne, je přesměrován na webovou stránku, kde bývá falešný článek, který se tváří jako legitimní zpráva od nějakého známého média. Tato zpráva je zpravidla šokující a má za úkol manipulovat emocemi oběti a upoutat její pozornost. Na webové stránce je pak také falešný formulář. Jakmile do něj člověk zadá své údaje, kontaktuje ho následně někdo z podvodného call centra. Podvod může mít také několik dalších variant. Formulář k zadání údajů může být přímo součástí reklamy na sociálních sítích. Útočník může oběť kontaktovat také rovnou na sociálních sítích prostřednictvím chatu a následně v komunikaci pokračovat buď po telefonu nebo e-mailu. Cílem podvodníků je samozřejmě vždy přimět oběť k převodu peněz," popisuje aktuální podvodný scénář Novotný.

Podvodné webové stránky spolehlivě zablokuje kvalitní bezpečnostní software. Dokáže například odhalit tzv. homoglyfy, znaky z jiných abeced. Útočníci je mohou dosazovat do URL adres podvržených webů a lidské oko je neodhalí. Jak však bezpečnostní specialisté upozorňují, velká část obrany před těmito útoky leží v rukou samotných uživatelů a uživatelek. Obzvláště by měli věnovat pozornost příchozí komunikaci a při platbách na internetu.

„Dříve daleko více platilo, že nás na podvod mohla upozornit špatná úroveň češtiny. To bohužel s příchodem stále lepších verzí nástrojů generativní umělé inteligence přestává platit. Dnes útočníci vynakládají velkou část práce na to, aby manipulací zakryli, že jde o podvod. Na co by se ale měli uživatelé určitě zaměřit, je URL adresa webu – jedná se o údaj v horním řádku internetového prohlížeče po otevření stránky z odkazu v SMS zprávě nebo e-mailu. Pokud se tato adresa neshoduje s oficiální doménou služby, o kterou se má jednat – například přípona není .cz nebo obsahuje nějaké divné znaky a čísla – je na místě ověřit si pravost stránky s oficiální zákaznickou podporou," říká Novotný z ESETu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné

šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-cesi-se-nejcasteji-potykaji-s-utoky-na-bankovni-identitu-a-falesnymi-kupujicimi-na-bazarech