ESET: Češi se ve druhém čtvrtletí 2025 potýkali s masivní vlnou podvodných zpráv

14.8.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ve druhém čtvrtletí letošního roku se útočníci nejčastěji vydávali za telekomunikační společnosti, poskytovatele sociálních sítí nebo banky. Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET. Útoky v nejčastějších případech nemířily přímo na české uživatele a uživatelky, to jim ale podle bezpečnostních expertů neubíralo na nebezpečnosti – řada z nás využívá služby zahraničních poskytovatelů a komunikace v angličtině tak není neobvyklá. Kromě těchto případů pokračovaly v Česku také podvody na internetových bazarech a upozornil na sebe i podvodný scénář na komunikační platformě WhatsApp.

Zatímco v prvním čtvrtletí letošního roku převládal v Česku kyberpodvod, v rámci kterého chtěli útočníci získat bankovní identitu svých obětí prostřednictvím falešných výzev k uhrazení dopravních pokut, ve druhém čtvrtletí se do popředí dostaly obecné phishingové útoky, které bezpečnostní experti z ESETu monitorují pod názvem Phishing.Gen nebo Agent.BDI. Jedná se o podvodné zprávy, ve kterých se útočníci vydávají za telekomunikační společnosti, poskytovatele sociálních sítí, banky apod. V případě útoků označených jako Phishing.Gen se ve sledovaném období jednalo o 66 % procent všech zachycených případů v České republice.

„Po bližší analýze těchto útoků můžeme potvrdit, že se nejednalo o žádný přesně cílený útok na Českou republiku. Tento typ phishingových zpráv ohrožuje uživatele a uživatelky ve více zemích. Ani potenciální oběti v Česku ale nemusí na první pohled pojmout podezření založené jen na tom, že nám někdo píše v angličtině a chce, abychom někam klikali nebo něco stahovali, protože běžně využíváme služeb řady zahraničních poskytovatelů. Z tohoto pohledu bohužel nejde říct, že by tyto útoky byly v Česku méně nebezpečné," vysvětluje Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET. „Typickou kořistí phishingového útoku jsou naše přihlašovací údaje. Ty buď útočníci prodají na černém trhu nebo rovnou využijí k přípravě dalších útoků, typicky s cílem prolomit naše osobní účty, včetně těch bankovních. Phishing může být ale součástí i pokročilejších útočných praktik, které mohou vyústit až k vpuštění ransomwaru do zařízení a ochromení například celé firmy nebo instituce," doplňuje Novotný.

Na stabilních hodnotách zůstaly ve druhém čtvrtletí také tzv. investiční podvody, které ESET sleduje pod označením Nomani, a to i přes dočasný propad v počtu detekcí v letošním květnu. Útočníci v rámci těchto podvodů nejčastěji lákají na investice do kryptoměn nebo jiných, lukrativních komodit s vidinou rychlého zisku.

I ve druhém čtvrtletí roku 2025 se v Česku objevovaly podvody na internetových bazarech, přestože počet zachycených případů oproti prvnímu kvartálu výrazně poklesl. Bezpečnostní experti z ESETu je detekují pod označením Phishing.Agent.GFH.

„Vzhledem k tomu, že se s podvody na internetových bazarech v Česku setkáváme již několikátým rokem, neměli bychom očekávat, že z našeho prostředí úplně zmizí. Stále také platí známý scénář, kdy se podvodník vydává za kupujícího, oběti zašle odkaz na falešný formulář nebo platební bránu, kam je nutné pro převzetí částky zadat přístupové údaje do online bankovnictví, a to včetně hesla a bezpečnostního kódu z autorizační SMS. S ohledem na to, že se v Česku s těmito podvody stále setkáváme zhruba v desetině všech případů, je na místě připomenout, že by uživatelé neměli nikam zadávat své přihlašovací údaje do bankovních účtů, pokud jsou na straně prodávajícího," říká

Novotný.

V období od dubna do června se lidé v Česku mohli také častěji setkávat s podvodem na chatovací platformě WhatsApp. Cílem podvodníků bylo v těchto případech převzít účet své oběti a pak vylákat peníze z jejích kontaktů.

„Podvod na chatovací platformě WhatsApp funguje jednoduše, přitom je ale velmi efektivní. Podvodná zpráva se nejdříve tváří jako výzva od vašeho známého, abyste hlasovali v nějaké anketě či soutěži. Odkaz ve zprávě vypadá velmi důvěryhodně, vede ale ve skutečnosti pouze na falešnou stránku, kde jsou oběti vyzvány, aby právě kvůli větší bezpečnosti zadaly ověřovací kód ze své aplikace. Tím jej ale jen předají útočníkovi, který tak může získat kontrolu nad jejich účtem. Zde bych rozhodně doporučil ověřit si s tím, kdo vám píše, zda se jedná o reálnou výzvu," dodává Novotný.

Podvodná komunikace na internetu se neustále vyvíjí a útočníci své prověřené strategie neúnavně vylepšují. Dříve například daleko více platilo, že nás na podvod mohla upozornit špatná úroveň češtiny. To bohužel s příchodem stále lepších verzí nástrojů generativní umělé inteligence přestává dle expertů platit. Kam až se může scénář útočníků vyvinout, dokládají také případy podvodu ClickFix, které podle zprávy ESET Threat Report H1 2025 vzrostly v období od prosince 2024 do května 2025 o 500 %. Útočníci v těchto případech zobrazují obětem na webových stránkách falešnou chybu, která je manipuluje k tomu, aby zkopírovaly, vložily a spustily škodlivé příkazy na svém zařízení. Útoky jsou zacíleny na všechny hlavní operační systémy, včetně Windows, Linux a macOS.

„Vždy na uživatele a uživatelky apelujeme, aby manipulativní podvodnou komunikaci nepodceňovali a ke své obezřetnosti a zdravé skepsi přidali i profesionální kyberbezpečnostní ochranu. Phishingové zprávy mohou do zařízení vpustit další závažné škodlivé kódy," říká Novotný z ESETu a dodává: „Útoky ClickFix jsou v současnosti druhou nejčastější podvodnou technikou po phishingu. Pomáhají šířit řadu dalších hrozeb – infostealery, ransomware, trojské koně využívané k získání vzdáleného přístupu, škodlivé kódy určené k těžbě kryptoměn, nástroje pro zneužívání zranitelností nebo škodlivé kódy, které využívají útočníci napojení na státní aktéry. Bezpečnostní software je tak i v případě podvodů na internetu pojistkou, která vás chrání v případě, kdy prostě už ostražitost stačit nebude."

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 kybernetické 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.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-cesi-se-ve-druhem-ctvrtleti-2025-potykali-s-masivni-vlnou-podvodnych-zprav