ESET: Ve třetím čtvrtletí letošního roku vzrostly případy podvodů s využitím nástroje Telekopí

12.11.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastějším typem podvodů v Česku zůstaly i v období od července do září 2025 falešné zprávy od telekomunikačních služeb, bank či provozovatelů sociálních sítí. S téměř stejným počtem zachycených případů ale těmto podvodům sekundovali také organizovaní útočníci známí z online bazarů a ubytovacích platforem, kteří k přípravě svých útoků využívají nástroj Telekopí (kombinace slov Telegram a kopí neboli také Telekopye). Vyplývá to z analýzy phishingových útoků na Českou republiku od společnosti ESET. Kromě těchto dvou typů kybernetických podvodů pak bezpečnostní experti zachytili nárůst případů, při nichž útočníci využívají k okradení svých obětí komunikační platformu WhatsApp.

Ve třetím čtvrtletí roku 2025 zůstaly nejčastějšími kybernetickými podvody v Česku falešné zprávy od telekomunikačních společností, poskytovatelů sociálních sítí či bank. Bezpečnostní experti z ESETu označují tento typ celosvětově rozšířených phishingových útoků názvem Phishing.Gen.

„Podvody, které sledujeme pod označením Phishing.Gen, jsme zachytili ve velkém počtu případů již letos na jaře. I když se jejich objem výrazně zmenšil, pořád šlo ve třetím kvartálu letošního roku o dominantní typ podvodné aktivity v Česku," říká Ondřej Novotný, kyberbezpečnostní analytik z pražské výzkumné pobočky společnosti ESET. „Tyto útoky sice nejsou výlučně zacílené na české uživatele a uživatelky, ani zprávy v jiném než českém jazyce ale nemusí vzbudit podezření. Řada z nás využívá služby zahraničních poskytovatelů, kteří nám čas od času legitimní zprávu v cizím jazyce zašlou. Cílem těchto útoků jsou naše přihlašovací údaje do různých účtů. Útočníci je pak přeprodávají na černém trhu nebo na jejich základě staví další phishingové kampaně," doplňuje Novotný.

V období od července do září 2025 experti z ESETu opět zaznamenali nárůst podvodů pomocí nástroje Telekopí. Cílem těchto podvodů jsou informace z platebních karet či přihlašovací údaje do internetového bankovnictví, díky kterým útočníci následně okradou své oběti o peníze.

„Ve třetím čtvrtletí jsme opět sledovali nárůst podvodného útoku, při němž útočníci využívají nástroj Telekopí. Ten funguje jako tzv. Telegram bot a umožňuje i méně technicky zdatným útočníkům vytvářet phishingové stránky z přednastavených šablon, generovat QR kódy a falešné screenshoty a rozesílat podvodné e-maily či SMS zprávy," vysvětluje Novotný. „Za útoky stojí poměrně pokročile organizovaná síť útočníků, kteří se už na české uživatele a uživatelky zaměřují cíleně, i když samozřejmě nejsme jedinou zemí, která se s nimi potýká. Cílem útočníků jsou naše peníze – manipulativní komunikací nás během útoku navádějí k zadání údajů k platební kartě či do bankovního účtu na falešných webových stránkách," připomíná Novotný.

Podvody, při nichž útočníci využívají nástroj Telekopí, jsou nejčastější na internetových tržištích, jako je například Vinted, eBay, Facebook Marketplace, Bazoš či Sbazar. Objevují se ale také na populárních platformách pro rezervace ubytování Booking.com a Airbnb. Nástroj Telekopí používají podle informací společnosti ESET desítky podvodných skupin, kdy každá z nich může mít až tisíc členů. Finanční škody spojené s těmito podvody činí již více než 100 milionů korun. Útoky přicházejí nejčastěji od rusky mluvících podvodníků, a to i ze zemí EU. Své oběti nazývají mamuti – v rusky mluvících zemích je to označení pro někoho, kdo se snadno nachytá.

Podvod, při němž útočníci zneužívají komunikační platformu WhatsApp, zachytili bezpečnostní specialisté opět již letos na jaře. Ve třetím čtvrtletí pak počet případů této útočné aktivity vzrostl na více než 10 procent v kontextu všech podvodů v Česku za toto období. Podvod monitorují pod označením Phishing.WhatsApp.A.

„Útočníci v tomto případě necílí tak přímočaře na naše bankovní účty. Zákeřnost tohoto podvodu ale tkví v tom, že o peníze můžeme přijít v domnění, že pomáháme někomu z přátel," říká Novotný. „Nejdříve vám útočníci pošlou zprávu, ve které se vydávají za někoho z vašich kontaktů, a poprosí vás, abyste hlasovali v nějaké soutěži či anketě. Ve zprávě najdete odkaz, který vypadá velmi důvěryhodně, ale zavede vás pouze na falešné webové stránky, kde máte kvůli údajnému zabezpečení zadat ověřovací kód z aplikace WhatsApp. Tím ale předáte útočníkům přístup ke svému účtu," pokračuje Novotný ve vysvětlení podvodného scénáře.

Bezpečnostní experti doporučují věnovat v případě podobných zpráv dostatek času na ověření jejich pravosti. Je totiž možné, že se vaši přátelé a známí, které máte v kontaktech, stali oběťmi stejného podvodu. I zde útočníci v konečném důsledku usilují o to, aby z nás vylákali peníze.

Bezpečnostní experti z ESETu v Česku monitorují stále také případy propracovaného podvodu Nomani, ve kterém útočníci zneužívají jména českých médií a lákají své oběti na manipulativní články se šokujícími titulky. Ačkoli ve třetím čtvrtletí počet případů tohoto podvodu klesl, stále zůstává na hodnotách ze začátku roku. Cílem útočníků je podvedené donutit k zadání kontaktních údajů do falešného formuláře. Podvod následně pokračuje po telefonu jako tzv. vishing.

„Vše to začíná nastraženou clickbaitovou reklamou na sociálních sítích. Jakmile na ni člověk klikne, je přesměrován na webové stránky s falešným článkem a kontaktním formulářem. Článek je psaný tak, aby v nás vyvolal silné emoce, ať už se jedná o strach nebo zvědavost. Pokud zadáme do formuláře své kontaktní údaje, ozve se nám následně někdo z podvodného call centra. Podvod může mít několik rozličných variant. Cílem je nás opět přimět k převedení peněz na účet podvodníků pod záminkou investování," říká Novotný z ESETu.

S ohledem na skutečnost, že v rámci investičních podvodů mohou útočníci k manipulaci využívat i deepfake obsah generovaný pomocí nástrojů umělé inteligence, doporučují experti přistupovat k senzačním reklamám a zprávám skepticky. Když zní něco až příliš senzačně a jednoduše, je v tom pravděpodobně nějaký háček.

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 RESET 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-ve-tretim-ctvrtleti-letosniho-roku-vzrostly-pripady-podvodu-s-vyuzitim-nastroje-telekopi