Globální vývoj kyberhrozeb od ESET: Sociální sítě zaplavil nový typ investičního podvodu, jehož součástí je deepfake

14.1.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET vydala svou nejnovější zprávu ESET Threat Report H2 2024. Zpráva shrnuje globální vývoj kybernetických hrozeb na základě dat z telemetrie a odborného pohledu analytiků společnosti, a to od června do listopadu 2024. Během tohoto období výrazně narostl počet investičních podvodů, a to o více než 335 % mezi prvním a druhým pololetím roku 2024. Investiční podvody v popsaném scénáři zaplavují sociální sítě a pomocí nástrojů umělé inteligence zneužívají jména známých osobností či firem. Nejvíce detekcí zachytili experti z ESETu v Japonsku, na Slovensku, v Kanadě, ve Španělsku a v České republice. Zpráva Threat Report H2 2024 se dále věnuje například rostoucím útokům na kryptoměnové peněženky, nástupu infostealeru Formbook či aktuálním proměnám ransomwarové scény.

Investiční podvod, který ESET označuje detekcí HTML/Nomani, se šíří prostřednictvím falešných reklam na sociálních sítích, zejména na platformě Meta. Reklamy zneužívají jména známých osobností či firem a lákají uživatele na pohádkově výhodné investování nebo zázračné doplňky stravy. Častou taktikou při těchto podvodných reklamách jsou videa upravená pomocí umělé inteligence (deepfake), na kterých vystupují známí politici, moderátoři či úspěšní podnikatelé a sdělují informace, které tito lidé ve skutečnosti neřekli. Útočníci pomocí AI napodobili na Slovensku například prezidenta Petra Pellegriniho či generálního ředitele společnosti ESET Richarda Marka. V Česku se mohli uživatelé setkat například s reklamami, na nichž podvodníci zneužili postavu prezidenta Petra Pavla nebo bývalého premiéra Andreje Babiše.

„Jde o poměrně propracovaný podvod, který útočníci realizují na několika úrovních. I když zkušenější uživatelé mohou na první pohled podvod rozeznat, útočníci přesto spoléhají na to, že naletí alespoň malá část zranitelné populace. U osob, které na deepfake videích mluví, si můžeme například všimnout nepřirozeného pohybu rtů. Na menších obrazovkách to ale můžeme snadno přehlédnout. Navíc předpokládáme, že tento podvod bude díky dalšímu vývoji nástrojů umělé inteligence stále důvěryhodnější. Nejlepší prevencí proto zůstává chránit se bezpečnostním softwarem a neustále podrobovat online obsah kritickému myšlení," vysvětluje Ondřej Novotný, výzkumný analytik z pražské pobočky společnosti ESET.

Reklamy často odkazují na důvěryhodně působící, ale falešné zpravodajské portály nebo podvodné stránky, které napodobují legitimní firmy. Falešné weby vybízejí uživatele k vyplnění kontaktních údajů. Po vyplnění formuláře zájemce kontaktuje pracovník telemarketingu, který má za úkol nasměrovat oběť k převodu peněz s počáteční „investicí" 250 eur (přes 6000 Kč). Útočníci mohou oběti nabádat také k tomu, aby si do zařízení stáhly nástroj pro vzdálený přístup nebo aby zažádaly o půjčku.

Nejvíce se tato škodlivá kampaň objevovala v Japonsku a na Slovensku, třetí místo patří Kanadě a následují Španělsko a Česko. Na základě analýzy zachycených případů se experti z ESETu domnívají, že podvodníci pocházejí z rusky mluvících zemí.

Ve sledovaném období došlo také ke změnám v kategorii infostealerů, což jsou škodlivé kódy určené ke krádežím citlivých údajů. Dlouhodobě dominantní spyware Agent Tesla byl „sesazen" jedním ze

svých starších konkurentů, infostealerem Formbook. Tuto změnu zaznamenali bezpečnostní experti také v Česku, kde tyto hrozby pro zařízení s operačním systémem Windows dlouhodobě sledují. Útočníci stále více vyhledávají i škodlivý kód Lumma Stealer. Ve druhém pololetí roku 2024 se objevil v několika významných útočných kampaních. Počet jeho detekcí vzrostl v telemetrii společnosti ESET o 369 %.

V říjnu 2024 došlo za spoluúčasti mezinárodních bezpečnostních organizací k přerušení prodeje známého infostealeru Redline Stealer. Bezpečnostní experti však očekávají, že zánik této malware rodiny povede k tomu, že útočníci tento škodlivý kód postupně nahradí jinou, podobnou službou. Ransomwarová scéna se změnila poté, co byl v další mezinárodní operaci „sesazen" bývalý lídr ransomwarových gangů, LockBit. Vzniklo tak vakuum, které však záhy vyplnili jiní aktéři. Ransomwarový gang RansomHub měl do konce druhého pololetí 2024 na svědomí stovky obětí, čímž se etabloval jako nový dominantní hráč. APT skupiny napojené na Čínu, Severní Koreu a Írán stále častěji využívaly ransomware jako krytí svých aktivit.

Jelikož kryptoměny dosáhly ve druhé polovině roku 2024 rekordních hodnot, údaje z kryptopeněženek byly také jedním z hlavních cílů útočníků. V telemetrii společnosti ESET došlo k nárůstu počtu detekcí cryptostealerů na několika platformách. Nejdramatičtější nárůst zaznamenali bezpečnostní experti na platformě macOS. V rámci této platformy se ve srovnání s prvním pololetím roku 2024 více než zdvojnásobil počet tzv. Password-Stealing Ware – škodlivých kódů zaměřených na přihlašovací údaje do kryptopeněženek. K tomuto nárůstu výrazně přispěl AMOS (známý také jako Atomic Stealer), škodlivý kód určený ke shromažďování a odcizení citlivých údajů ze zařízení Mac. Finanční hrozby pro platformu Android zaměřené na bankovní aplikace i kryptopeněženky vzrostly ve sledovaném období o 20 %.

Více informací o vývoji kybernetických hrozeb za období od června do listopadu 2024 najdete v celém znění zprávy ESET Threat Report H2 2024. Komentáře expertů k vývoji kybernetických hrozeb v následujících měsících roku 2025 najdete zde.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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 anebo v podcastu TruePositive.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

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

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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/globalni-vyvoj-kyberhrozeb-od-eset-socialni-site-zaplavil-novy-typ-investicniho-podvodu-jehoz-soucasti-je-deepfake