Globální vývoj kyberhrozeb od ESET: Útočníci nutí uživatele opravovat neexistující chyby, šíří tak řadu kyberhrozeb

9.7.2025 - | ESET software

Společnost ESET vydala svou nejnovější zprávu ESET Threat Report H1 2025. Zpráva shrnuje globální vývoj kybernetických hrozeb na základě dat z telemetrie a odborného pohledu analytiků společnosti, a to od prosince 2024 do května 2025. Na scéně kyberzločinu se podle bezpečnostních expertů objevil nový podvodný útok ClickFix, který byl ve sledovaném období druhým nejčastějším typem útoku pomocí technik sociálního inženýrství, a to hned po phishingu. Zpráva nabízí také pohled na vývoj infostealerů, které jsou dlouhodobě přítomné i v Česku, v oblasti ransomwaru či na platformě Android.

Mezi nejvýraznější útoky patřil ve sledovaném období ClickFix, jehož případy vzrostly podle telemetrie společnosti ESET o více než 500 % ve srovnání s druhou polovinou roku 2024. Díky tomu se stal jednou z nejrychleji rostoucích kyberhrozeb. V první polovině roku 2025 tvořil téměř 8 % všech zablokovaných útoků, a je nyní po phishingu druhým nejčastějším vektorem útoku v rámci technik sociálního inženýrství.

Útoky ClickFix 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.

„Útoky ClickFix jsou vstupní branou pro další hrozby, jejichž seznam se každým dnem rozšiřuje. Útoky umožňují šířit infostealery, ransomware, trojské koně využívané k získání vzdáleného přístupu, škodlivé kódy určené k těžbě kryptoměn, nástroje pro zneužívání zranitelností, a dokonce i vlastní malware napojený na státní aktéry," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

K výrazným změnám došlo v první polovině roku 2025 mezi infostealery. Zatímco infostealer Agent Tesla mizí z předních míst detekcí, SnakeStealer neboli Snake Keylogger se dostal do popředí a stal se nejčastěji detekovaným infostealerem v telemetrii ESET za sledované období. Dokáže zaznamenávat stisky kláves, odcizit uložené přihlašovací údaje, pořizovat snímky obrazovky a sbírat data ze schránky.

Ve sledovaném období přispěli experti z ESETu také k rozsáhlým operacím k narušení činnosti dvou významných hrozeb typu malware-as-a-service – malware rodin Lumma Stealer a Danabot.

„Před těmito operacemi byla aktivita malwaru Lumma Stealer v první polovině roku 2025 o 21 % vyšší než ve druhé polovině roku 2024, zatímco aktivita v případě malwaru Danabot vzrostla dokonce o 52 %. To dokládá, že se jednalo o velmi aktivní hrozby, a operace k narušení jejich činnosti byly o to důležitější," doplňuje Kropáč.

Ransomwarová scéna se ve sledovaném období propadala do chaosu, přičemž spory mezi konkurenčními gangy ovlivnily i hlavní hráče, včetně největšího aktéra v rámci služby ransomware-as-a-service – gang RansomHub.

Kromě externího tlaku vyvíjeného policejními složkami zaútočil na infrastrukturu svých rivalů i gang

DragonForce. To mimo jiné přispělo právě k destrukci gangu RansomHub. Kdo bude jeho nástupcem zatím není dle bezpečnostních expertů jasné. Ostatní ransomwarové gangy se snaží přilákat někdejší partnery RansomHubu pod svá křídla. Kromě toho došlo i k několika únikům interních dat ransomwarových gangů, především dominantního Black Basta. Tento gang se již z takové ztráty důvěryhodnosti mezi svými partnery nevzpamatoval.

V případě platformy Android vzrostly detekce adwaru o 160 %, a to především kvůli nové, sofistikované hrozbě s názvem Kaleidoscope. Tento škodlivý kód je využíván k šíření škodlivých klonů aplikací, které uživatele po stažení bombardují reklamami a zhoršují výkon zařízení. Zároveň více než pětatřicetkrát vzrostly podvody založené na technologii NFC, a to díky phishingovým kampaním a vynalézavým způsobům přenosu dat. Ačkoli celkové počty případů zůstávají relativně nízké, jejich nárůst ukazuje, jak rychle kyberzločinci vyvíjejí své postupy a že se nadále zaměřují na zneužívání technologie NFC.

Výzkum společnosti ESET, který se týká nástroje GhostTap, ukazuje, jak tento nástroj krade údaje z platebních karet. Útočníci následně mohou nahrát karty obětí do svých digitálních peněženek a provádět bezkontaktní platby po celém světě. Organizované „podvodné farmy" používají k rozšíření těchto podvodů více telefonů. SuperCard X je pak další, jednoduchý nástroj typu malware-as-a-service, který také útočníkům umožnuje krást data přes NFC. Vypadá jako neškodná aplikace, ale po instalaci na zařízení oběti v reálném čase tiše zachytává a přenáší údaje z karty.

„Od nových technik sociálního inženýrství přes sofistikované mobilní hrozby až po zásadní narušení rodin infostealerů – první polovina roku 2025 rozhodně nebyla klidným obdobím ve světě kyberbezpečnosti," shrnuje Jiří Kropáč z ESETu.

Více informací o vývoji kybernetických hrozeb za období od prosince 2024 do května 2025 najdete v celém znění zprávy ESET Threat Report H1 2025.

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.

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/globalni-vyvoj-kyberhrozeb-od-eset-utocnici-nuti-uzivatele-opravovat-neexistujici-chyby-siri-tak-radu-kyberhrozeb