Globální vývoj kyberhrozeb od ESET: Kyberútočníci díky AI zlepšují své útoky

9.7.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Bezpečnostní experti ze společnosti ESET zveřejnili zprávu ESET Threat Report, která pokrývá globální vývoj kyberhrozeb za období od prosince 2025 do května 2026.

- Technika sociálního inženýrství, ClickFix, ve které útočníci využívají falešné chybové hlášky pro celou řadu IT problémů, se nově objevuje i na webových stránkách s radami pro práci s AI, v rozšířeních prohlížečů a pracovním prostředí, kde je nutné ověření pro přístup do cloudu.
- Quishing, phishing prostřednictvím QR kódů, dosáhl v datech společnosti ESET za sledované období rekordních hodnot.
- Společnost ESET analyzovala také téměř 900 000 AI skillů, malých funkčních komponent, které využívají AI agenti. Identifikovala desítky tisíc podezřelých a tisíce škodlivých vzorků. Umělá inteligence se navíc začíná objevovat i v malwaru.
- Ani v případě ransomwaru se situace neuklidňuje. Útočníci nadále využívají tzv. EDR killery, nástroje určené k deaktivaci bezpečnostního softwaru během ransomwarových útoků.

Praha, 9. července 2026 — Bezpečnostní experti ze společnosti ESET zveřejnili zprávu o globálních kybernetických hrozbách Threat Report za období od prosince 2025 do května 2026. První polovina roku 2026 ukázala, jak útočníci nadále zvyšují efektivitu a škálovatelnost svých operací a stále významnější roli hraje v tomto vývoji umělá inteligence (AI). Společnost ESET analyzovala téměř 900 000 AI skillů (dovedností) – malých funkčních komponent využívaných AI agenty. Identifikovala desítky tisíc podezřelých a tisíce jednoznačně škodlivých vzorků. Umělá inteligence se navíc začíná objevovat přímo v malwaru: v únoru letošního roku experti varovali před škodlivým kódem PromptSpy, první známým malwarem pro platformu Android, který využívá generativní AI.

„Útočníci se nespoléhají na zcela nové metody a nástroje, ale rychle přizpůsobují osvědčené techniky novým platformám, technologiím a chování uživatelů. Počet AI skillů v tomto novém ekosystému aktuálně rychle roste, čímž se dále rozšiřuje útočný prostor," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně. „Na druhou stranu případ malwaru PromptSpy ukazuje, jak by mohly být budoucí hrozby flexibilnější, i když ochranná opatření proti zneužití, která jsou součástí velkých jazykových modelů, pravděpodobně zpomalují jejich zavádění," dodává Kropáč.

Nebezpečné AI skilly

AI skilly jsou malá rozšíření nebo sady instrukcí. AI agentům určují, jak mají vykonávat konkrétní úkoly, včetně toho, jaké služby či nástroje použít a k jakým datům přistupovat. Ve zprávě ESET popisuje škodlivé AI skilly využívající útočné nástroje třetích stran, jako jsou Mimikatz nebo Impacket, i podezřelé skilly se schopností se samy modifikovat, které jsou navržené pro vytváření mechanismů perzistence (souborů JSON) a nástrojů pro vlastní modifikaci (kód v jazyce Python).

Výše popsané skutečnosti mohou vést k nepředvídatelnému chování AI agentů nebo k jejich zneužití. Experti ve zprávě popisují také neškodné, avšak problematické AI skilly. Jedná se například o dovednosti, které jsou propagovány jako bezpečnostní skenery, ale vytvářejí falešný pocit bezpečí, protože implementují pouze základní kontrolní mechanismy připomínající antivirové nástroje z 90. let, nebo se omezují na ověřování reputace hashů, URL adres a IP adres prostřednictvím služby VirusTotal.

Proměna podvodů ClickFix

Technika sociálního inženýrství ClickFix, ve které útočníci využívají chybové hlášky, se mezitím rozšířila daleko za hranice podvodných výzev CAPTCHA. Nově se objevuje také na stránkách, které nabízejí nápovědu pro práci s AI nástroji, v rozšířeních internetových prohlížečů či při ověřování přístupu do cloudového prostředí.

Případ AI-fix ukazuje, jak útočníci zneužívají důvěru uživatelů v generativní AI. Vkládají kompromitované řetězce ClickFix do obsahu vygenerovaného nástroji umělé inteligence. Na webových stránkách, které zneužívají domény předních poskytovatelů AI služeb, tak útočníci nabízí uživatelům a uživatelkám řešení neexistujících problémů.

ConsentFix zase představuje posun směrem ke krádežím tokenů. Kombinuje útok ClickFix se zneužitím autorizace OAuth. Tím útočníkům umožňuje převzít cloudové účty bez nutnosti krádeže přihlašovacích údajů. Útočníci tak často dokážou obejít vícefázové ověřování (MFA) a spoléhají se výhradně na legitimní přihlašovací procesy. Detekce této techniky se v systémech společnosti ESET mezi druhým pololetím roku 2025 a prvním pololetím roku 2026 více než zdvojnásobily, což potvrzuje její trvalé využívání a další vývoj.

Podvržené QR kódy

V reakci na změny v chování uživatelů se vyvíjejí i phishingové kampaně. Phishing prostřednictvím QR kódů, známý také jako quishing, dosáhl v telemetrii společnosti ESET rekordních hodnot. Útočníci vkládají škodlivé odkazy do QR kódů, aby obešli kontrolní mechanismy. Zneužívají přitom důvěru, kterou mnoho lidí k těmto čtvercovým kódům chová. Přibližně 11 % všech phishingových e-mailů, které byly detekovány v prvním pololetí roku 2026, obsahovalo QR kódy. Kyberbezpečnostní analytici tyto hrozby nejčastěji zaznamenali ve Spojených státech (19 % detekcí), ve Španělsku (17 %) a Mexiku (6 %).

EDR killery

Globální prostředí ransomwaru nevykazovalo během sledovaného období žádné známky útlumu. Útočníci nadále využívají takzvané EDR killery – nástroje určené k vypnutí bezpečnostního softwaru během útoků. Bezpečnostní experti z ESETu zdokumentovali více než 100 různých EDR killerů používaných v reálných útocích a pravidelně se objevují jejich nové varianty.

Počet ransomwarových útoků v prvním pololetí roku 2026 dále rostl, avšak počet obětí ochotných zaplatit výkupné klesl na historické minimum. Tento klesající trend potvrdily také další tři kyberbezpečnostní zprávy, podle nichž výkupné zaplatilo pouze 14 až 28 % napadených organizací.

Více informací

Více informací včetně grafů a komentářů kyberbezpečnostních expertů ze společnosti ESET najdete v celém znění zprávy ESET Threat Report H1 2026.

O společnosti ESET

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

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.

Kontakt pro media:

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-kyber utocnici-diky-ai-zlepsuji-sve-utoky