

# **MEATEST spol. s r.o.** - sdělení pověření pro ochranu osobních údajů číslo **139** ze dne **7.4.2026**

---

## **AI zrychluje kybernetické útoky. I levné a rychlé nástroje obcházejí současnou obranu**

Nejnovější zpráva HP Threat Insights Report uvádí, že útočníci využívají umělou inteligenci ke škálování a urychlování svých kampaní. Mnozí z nich přitom upřednostňují náklady, rychlost a efektivitu před kvalitou. Přestože jsou tyto AI-asistované útoky často schematické a nenáročné, dokážou proklouznout podnikovou obranou.

Zpráva analyzuje reálné kybernetické útoky a pomáhá organizacím držet krok s nejnovějšími technikami, které kyberzločinci používají k obcházení detekce a průnikům do počítačů. Na základě dat z milionů koncových zařízení s HP Wolf Security identifikoval výzkumný tým HP mimo jiné tyto kampaně:

Skripty typu "vibe-hacking" s přesměrováním na Booking.com: Útočníci využívají AI ke generování hotových infekčních skriptů – tzv. vibe-hackingu – které automatizují doručení malwaru. V jedné z kampaní je ve falešné PDF faktuře vložen odkaz, který nejprve nenápadně stáhne škodlivý soubor z kompromitovaného webu a poté uživatele přesměruje na důvěryhodnou platformu, například Booking.com.

"Flat-pack" malware urychluje tvorbu kampaní: Aktéři hrozeb skládají útoky z levných, běžně dostupných malwarových komponent, pravděpodobně zakoupených na hackerských fórech. Návnady a finální škodlivé kódy se mění, zatímco prostřední skripty a instalátory zůstávají stejné. To umožňuje rychlé sestavení, přizpůsobení i škálování kampaní s minimálním úsilím. Nejde přitom o jedinou skupinu – stejné stavební bloky využívá více nezávislých aktérů.

Malware ukrytý ve falešném instalátoru Teams ("piggyback" útok): Útočníci manipulují výsledky vyhledávání a zneužívají podvodné reklamní kampaně k propagaci podvodných webů vydávajících se za Microsoft Teams. Oběti si stáhnou škodlivý instalační balíček, ve kterém je skrytý malware Oyster Loader "přibalen" k instalaci Teams. Zatímco se legitimní aplikace nainstaluje, infekce probíhá nenápadně na pozadí a útočník získá zadní vrátka do zařízení.

Alex Holland, hlavní výzkumník kybernetických hrozeb v HP Security Lab, komentuje výsledky průzkumu: "Je to klasický projektový trojúhelník – rychlost, kvalita a náklady. Obvykle musíte jeden z těchto faktorů obětovat. Vidíme, že mnoho útočníků optimalizuje především rychlost a náklady, nikoli kvalitu. Umělou inteligenci nepoužívají ke zvyšování úrovně útoků, ale k urychlení práce a snížení námahy. Kampaně jsou často jednoduché, ale nepříjemnou realitou je, že stále fungují."

Zpráva, která analyzuje období říjen–prosinec 2025, ukazuje, že kyberzločinci nadále diverzifikují metody, jak obejít bezpečnostní nástroje založené na detekci.

Alespoň 14 % e-mailových hrozeb identifikovaných pomocí HP Sure Click obešlo jeden nebo více skenerů e-mailových bran.

Spustitelné soubory byly nejčastějším způsobem doručení (37 %), následované soubory .zip (11 %) a .docx (10 %).

Dr. Ian Pratt, ředitel bezpečnosti osobních systémů ve společnosti HP Inc., dodal: "Útoky využívající umělou inteligenci odhalují limity bezpečnostních řešení založených primárně na detekci.

# **MEATEST spol. s r.o.** - sdělení pověření pro ochranu osobních údajů číslo **139** ze dne **7.4.2026**

---

Pokud útočníci dokážou během několika minut generovat a upravovat nové varianty malwaru, obrana postavená na rozpoznávání vzorců nemůže držet krok. Místo snahy zachytit každou variantu by se organizace měly zaměřit na snižování expozice. Izolací vysoce rizikových aktivit v odděleném prostředí (například otevírání nedůvěryhodných příloh nebo klikání na neznámé odkazy) lze zastavit hrozby ještě předtím, než způsobí škodu. A eliminovat celou kategorii rizik."

Data byla shromážděna od zákazníků HP Wolf Security, kteří s tím vyjádřili souhlas, v období říjen–prosinec 2025. Vyšetřování prováděl tým HP Threat Research.

AV centrum ČR