

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **121** ze dne **14.10.2025**

Za nárůstem ransomwaru stojí phishing a sociální inženýrství

Ransomware zůstává podle zprávy Acronis Cyberthreats Report za první pololetí 2025 hlavní hrozbou pro velké a střední podniky. Ransomwarevé skupiny navíc stále častěji využívají k automatizaci svých aktivit umělou inteligenci – phishing tvořil 25 % všech útoků a 52 % útoků zaměřených na MSP, což představuje nárůst o 22 % ve srovnání s 1. pololetím roku 2024.

Pololetní zpráva pokrývá globální hrozby, které detekovala Acronis Threat Research Unit (TRU) s pomocí senzorů Acronis na koncových zařízeních Windows od ledna do května 2025. Na základě dat z více než milionu unikátních koncových bodů rozmístěných po celém světě zpráva také zahrnuje statistiky hrozeb zaměřené na operační systémy Windows, vzhledem k jejich převaze oproti MacOS a Linuxu.

"Zatímco finální zbraní kyberzločinců je stále ransomware, způsob, jakým ho doručují, se mění," řekl Gerald Beuchelt, CISO ve společnosti Acronis. "I ti nejméně sofistikovaní útočníci mají dnes přístup k pokročilým funkcím umělé inteligence, generují útoky sociálního inženýrství a automatizují své aktivity s minimálním úsilím. Výsledkem je, že organizace, MSP, ISP poskytovatelé a další subjekty jsou neustále vystaveny sofistikovaným útokům, včetně stále pokročilejšího deep fake obsahu, a stačí jedna chyba, aby byla ohrožena celá budoucnost organizace. Abychom v tomto prostředí hrozeb přežili a vyhnuli se škodlivým ransomwarovým útokům, je nezbytná komplexní strategie kybernetické ochrany, která zahrnuje pokročilé funkce detekce, reakce a obnovy."

Mezi hlavní zjištění zprávy Acronis Cyberthreats Report H1 2025 patří:

- Ransomware je stále na špici: počet veřejně známých obětí ransomwaru vzrostl za měřené období téměř o 70 % ve srovnání s roky 2023 a 2024. Nejaktivnější ransomwarové skupiny jsou Cl0p, Akira a Qlin.
- AI podporuje nárůst sociálního inženýrství: ransomwarové gangy stále častěji využívají AI, což se odráží v jejich zvolených vektorech hrozeb – počet případů sociálního inženýrství a BEC útoků vzrostly v období od ledna 2025 do května 2025 o 20 % ve srovnání se stejným obdobím v roce 2024, pravděpodobně kvůli nárůstu využívání AI k vytváření přesvědčivých podvrhů. Malware byl objeven v 1,47 % e-mailových záloh v Microsoft 365.
- MSP pod palbou phishingových a BEC útoků: zatímco celkový počet útoků zaměřených na MSP (poskytovatele řízených služeb) během měřeného období poklesl, povaha útoků se výrazně změnila; phishing tvořil 52 % všech útoků zaměřených na MSP, zatímco v roce 2024 to bylo 30 %, zatímco útoky pomocí protokolu RDP (Remote Desktop Protocol) téměř vymizely.
- Ne všechny phishingové útoky jsou stejné: zatímco phishing je oblíbenou zbraní útočníků, ti se stále více zaměřují na aplikace pro spolupráci a vyhýbají se jednoduchým BEC kampaním. Téměř 25 % útoků v aplikacích pro spolupráci využívalo deep fake obsah generovaný umělou inteligencí nebo automatizované exploity.
- Výrobní firmy v hledáčku: nejčastějším terčem ransomwarových gangů bylo odvětví

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **121** ze dne **14.10.2025**

výroby, když představovalo 15 % všech zaznamenaných případů v 1. čtvrtletí 2025. Oblíbenými cíli byly také retail, potraviny a nápoje (12 %), a telekomunikace a média (10 %).

Další informace naleznete naleznete v kompletní zprávě Acronis H1 2025 Cyberthreats Report.

Zdroj: AV centrum ČR