Ransomware v Česku: 100procentní nárůst útoků, tři světové gangy a nová éra sofistikovaných hrozeb

1.4.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

V České republice bylo za první kvartál letošního roku evidováno 12 obětí útoků ransomwarem: jedná se o nárůst 100 % ve srovnání se stejným obdobím loňského roku.

- Na Česko cílí trojice předních gangů v rámci modelu RaaS (Ransomware-as-a-Service): Gentlemen, Akira a Qilin. Poslední dva jmenovaní jsou každý globálně zodpovědný za 10 % analyzovaných útoků.
- Česká republika čelí o 20 % vyššímu počtu kyberútoků, než je evropský průměr.
- Ransomwarové útoky mají za rok 2025 na svědomí celosvětově 6 937 obětí, tj. o 1 700 více než v roce 2024.

Česká republika se v roce 2026 ocitá pod výrazně rostoucím tlakem ransomwarových útoků. Společnost ESET ve svých datech zaznamenala prudký nárůst případů, což potvrzuje i to, že jen v prvním čtvrtletí 2026 bylo na veřejných stránkách ransomwarových skupin evidováno již 12 českých obětí – dvojnásobek oproti stejnému období roku 2025 (6 obětí). Například v roce 2024 dosáhlo Česko stejného čísla až v srpnu. Tuzemská situace odráží alarmující globální trend: podle dat ze zprávy ESET Threat Report H2 2025 měl ransomware v roce 2025 celosvětově na svém kontě 6 937 obětí, čímž překonal celkový součet roku 2024 o více než 1 700 případů.

Trojice předních světových gangů operuje v ČR

Experti společnosti ESET identifikovali tři skupiny, které v současnosti nejaktivněji útočí na české subjekty: Gentlemen, Akira a Qilin. Všechny tři gangy fungují v modelu Ransomware-as-a-Service (RaaS) – samy vyvíjejí malware a distribuují jej rozsáhlé síti partnerů, kteří provádějí útoky po celém světě. Podle dat ze zprávy ESET Threat Report H2 2025 jsou gangy Akira a Qilin globálně každý zodpovědný za přibližně 10 % všech analyzovaných ransomwarových útoků, přičemž Qilin se ve druhém pololetí roku 2025 stal dominantním hráčem na celé ransomwarové scéně po pádu skupiny RansomHub.

Zvláštní pozornost si zaslouží skupina Gentlemen, u níž ESET zaznamenal v prvním čtvrtletí 2026 prudký nárůst aktivity. Tato skupina neustále zdokonaluje svůj arzenál a disponuje rozsáhlou globální sítí partnerů.

„Skupina Gentlemen je jednou z nejaktivnějších ransomwarových organizací současnosti. V prvním čtvrtletí letošního roku jsme zaznamenali její výrazně zvýšenou aktivitu i v české digitální infrastruktuře. Skutečnost, že se tři globálně nejaktivnější RaaS skupiny současně zaměřují na Českou republiku, jasně ukazuje, že naše země je pro útočníky čím dál atraktivnějším cílem. Nejde přitom o sofistikované zero-day útoky – v drtivé většině průniků útočníci zneužívají zcela základní bezpečnostní mezery, které lze relativně snadno odstranit. Slabá hesla, neaktualizované systémy a otevřené RDP porty zůstávají hlavními vstupními body i pro ty nejnebezpečnější gangy," říká Jakub Souček, vedoucí výzkumného týmu v pražské pobočce společnosti ESET.

Útočníci neutralizují bezpečnostní software: EDR killery jako nový standard

Klíčovým trendem, který společnost ESET zaznamenala již koncem loňského roku 2025 a jehož dopad se projevuje i v českém prostředí, je masivní rozšíření tzv. EDR killerů. Jde o specializované nástroje navržené tak, aby deaktivovaly nebo zcela vypnuly bezpečnostní software instalovaný na napadených zařízeních. Jen v posledních třech měsících roku 2025 odhalili bezpečnostní experti z ESETu více než tucet nových nástrojů tohoto druhu, používané mimo jiné i partnery skupin Akira, Gentlemen a Qilin.

Nejrozšířenější metodou nasazení EDR killerů je technika BYOVD (Bring Your Own Vulnerable Driver). Útočník do systému oběti zavede legitimní, ale zranitelný ovladač, přes který poté z úrovně jádra operačního systému narušuje bezpečnostní procesy. Zároveň se šíří případy zneužívání legitimních nástrojů pro vzdálenou správu (RMM), jako jsou AnyDesk, MeshAgent nebo SimpleHelp – jejich nečekaná přítomnost v síti by proto měla okamžitě vyvolat bezpečnostní prověření.

Souběžně s tím útočníci již rutinně využívají tzv. double extortion model: data jsou nejprve exfiltrována a teprve poté zašifrována. Oběť je pak vydírána nejen hrozbou ztráty dat, ale také jejich zveřejněním.

Kdo je v hledáčku gangů: SMB, výrobní a technologické firmy

Ransomwarové gangy se v České republice zaměřují především na malé a střední podniky (SMB). Tento segment je pro útočníky lákavý. Tyto firmy mají zpravidla omezené kapacity v oblasti kybernetické bezpečnosti, dopady výpadku systémů jsou pro provoz závažnější a pravděpodobnost zaplacení výkupného je vyšší. Podle dat ze zprávy ESET Threat Report H2 2025 jsou globálně nejvíce zasaženými odvětvími výroba, stavebnictví, maloobchod, technologie a zdravotnictví – odvětví s vysokou závislostí na nepřetržitém provozu IT systémů.

V Česku převažují oběti z oblasti výroby, technologického sektoru a obchodu. Každá hodina výpadku zde přináší přímé finanční ztráty a zákazníci jsou okamžitě zasaženi. Ransomwarové skupiny s těmito dopady počítají a jsou schopné požadovat i mnohamilionová výkupná.

Jak se bránit: doporučení a konkrétní kroky

Bezpečnostní experti ze společnosti ESET opakovaně potvrzují, že velká většina ransomwarových útoků nevyužívá sofistikované zero-day zranitelnosti. Podle dat ze zprávy ESET Threat Report tvoří hádání hesel více než 42 % všech externích vektorů průniku. Níže uvedenými opatřeními tak mohou firmy zablokovat drtivou většinu reálných útoků:

- Revize politik hesel a zavedení MFA: Slabá nebo opakovaně používaná hesla zůstávají nejčastější vstupní branou pro útoky ransomwarem. Vícefaktorová autentizace (MFA) dokáže naprostou většinu pokusů o průnik zastavit dřív, než dojde k přístupu do systému.
- Audit zařízení vystavených do internetu: Zejména VPN, RDP a exponované správcovské rozhraní. Pokusy o uhádnutí hesel a zneužití zranitelností VPN jsou dlouhodobě mezi třemi nejčastějšími vektory útoků. Veškerá zařízení musí být aktualizována a správně nakonfigurována.
- Pokrytí všech koncových bodů bezpečnostním řešením: Servery pro řízení oprávnění a přihlašování jsou pro útočníky klíčovým cílem – jejich kompromitace znamená fakticky plnou

kontrolu nad celou sítí. Bezpečnostní software musí být nasazen bez výjimky na všech zařízeních.
- Aktivní reakce na bezpečnostní upozornění: Mnoho útoků ponechává v systémech stopy hodiny či dny před zašifrováním. Ignorovaná upozornění jsou promarněnou šancí útok zastavit. Zvláštní pozornost věnujte nečekanému výskytu nástrojů pro vzdálenou správu (AnyDesk, MeshAgent).
- Funkčnost a izolace záloh: Zálohy musí být fyzicky a logicky odděleny od produkční sítě – útočníci cíleně vyhledávají a šifrují či ničí i záložní systémy. Zálohy je nutné pravidelně testovat a ověřovat jejich obnovitelnost.

Se všemi výše uvedenými body dokáže pomoci bezpečnostní řešení od ESET: malé a střední firmy ochrání řešení ESET PROTECT Advanced, které zahrnuje vícevrstvou ochranu koncových zařízení, včetně anti-ransomwarové vrstvy, a cloudovou správu z jedné platformy. Větší organizace pak naleznou maximální ochranu v platformě ESET PROTECT MDR, která přidává pokročilý monitoring 24/7, spravovanou detekci a reakci (MDR) a technologii XDR pro podrobné vyšetřování incidentů.

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.

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/ransomware-vcesku-100procentni-narust-utoku-tri-svetove-gangy-a-nova-era-sofistikovanych-hrozeb