Kaspersky: Ransomware útočí chytřeji a levněji – co očekávat v roce 2025?

9.5.2025 - | PROTEXT

Podle údajů z Kaspersky Security Network jsou z hlediska podílu ransomwarem napadených uživatelů v jednotlivých regionech na předních místech Blízký východ, Asie-Pacifik a Afrika, na konci pak Latinská Amerika, SNS (Společenství nezávislých států) a Evropa. Celosvětově se v letech 2023 až 2024 podíl uživatelů postižených útoky ransomwaru zvýšil o 0,02 % na 0,44 %. Zdánlivě malé procento útoků je pro ransomware typické a vysvětluje se tím, že útočníci tento typ malwaru obvykle nešíří hromadně, ale upřednostňují cíle s vysokou hodnotou, což snižuje celkový počet incidentů.

Den boje proti ransomwaru (Anti-Ransomware Day) byl ustanoven 12. května 2020 organizací INTERPOL ve spolupráci se společností Kaspersky jako připomínka nechvalně známého útoku ransomwaru WannaCry, ke kterému došlo právě 12. května 2017. Účelem Dne boje proti ransomwaru je zvýšit globální povědomí o hrozbách, které ransomware představuje, a propagovat osvědčené postupy, jak těmto útokům předcházet, i jak na ně reagovat.

Evropa je stálým terčem ransomwaru, ale profituje z robustních opatření a předpisů kybernetické bezpečnosti, které některé útočníky odrazují. Častým terčem útoků jsou zdravotnické a vládní systémy, ale rozsah škod omezují dobrá příprava a účinné reakce na incidenty. Diverzifikované ekonomiky a silná obrana činí z tohoto regionu méně vyhledávaný terč ransomwarových útoků, než jsou regiony s rychlým, ale hůře chráněným digitálním růstem.

Aktuální a nově vznikající trendy v oblasti ransomwaru

Při vývoji ransomwaru byly stále častěji používány nástroje s podporou AI, což se ukázalo i v případě ransomwarové skupiny FunkSec, která se objevila koncem roku 2024 a rychle se „proslavila“ tím, že jen v samotném prosinci překonala počtem svých obětí již déle působící skupiny Cl0p nebo RansomHub. Skupina FunkSec, která využívá služby Ransomware-as-a-Service (RaaS), má dvojitou vyděračskou taktiku – kombinuje šifrování dat s exfiltrací a cílí na sektory, jako je vláda, technologie, finance a vzdělávání v Evropě a Asii. Od ostatních se odlišuje tím, že se silně spoléhá na nástroje s podporou AI pro generování kódu ransomwaru, který doplňuje bezchybnými komentáři vytvořenými pravděpodobně pomocí velkých jazykových modelů (LLM), aby zefektivnila vývoj a vyhnula se odhalení. Na rozdíl od typických ransomwarových skupin požadujících milionové částky, volí FunkSec velkoobjemový, nízkonákladový přístup s neobvykle nízkými požadavky na výkupné, což dále zvyšuje úspěšnost jejího inovativní využití AI ke zjednodušení a urychlení operací.

Dominantním prostředkem pro útoky ransomwaru zůstává model RaaS (Ransomware-as-a-Service), což podporuje jejich rozšíření díky snížení znalostní bariéry pro méně technicky zdatné kyberzločince. Platformy RaaS, jako je RansomHub, vzkvétaly v roce 2024 díky nabídce malwaru, technické podpory a partnerských programů, které rozdělovaly výkupné. Tento model umožňuje provádět sofistikované útoky i nekvalifikovaným aktérům, což jen v roce 2024 přispělo ke vzniku několika nových ransomwarových skupin.

V roce 2025 se očekává, že se ransomware bude dále vyvíjet s využíváním nekonvenčních zranitelností, jak předvedl gang Akira, který dokázal pomocí nezabezpečené webové kamery obejít systémy detekce a reakce u koncových bodů a infiltrovat interní sítě. Útočníci se budou pravděpodobně stále častěji zaměřovat na dosud přehlížené potenciální přístupové body, jako jsou

zařízení internetu věcí (IoT), chytré spotřebiče nebo nesprávně nakonfigurovaný hardware na pracovišti, a využívat pro svoje útoky tento rostoucí nástupní prostor vytvářený propojenými systémy. Souběžně s tím, jak organizace posilují tradiční obranu, budou také kyberzločinci zdokonalovat své taktiky a preferovat nenápadný průzkum a opatrný postupný průnik do sítí, aby mohli ransomware nasazovat s větší přesností, což obráncům ztíží včasnou detekci a reakci.

Šíření velkých jazykových modelů (LLM) přizpůsobených pro kyberkriminalitu dále zesílí dosah a dopad ransomwaru. LLM prodávané na dark webu snižují technickou bariéru pro vytváření škodlivého kódu, phishingových kampaní a útoků sociálního inženýrství, což umožňuje i méně zkušeným aktérům vytvářet velmi přesvědčivé návnady nebo automatizovat nasazení ransomwaru. Vývojáři softwaru rychle přecházejí na inovativní programovací nástroje, například RPA (Robotic Process Automation a LowCode, které nabízejí intuitivní vizuální rozhraní s podporou AI a snadné sestavování programů přetahováním částí kódů myší. Můžeme očekávat, že vývojáři ransomwaru budou tyto nástroje používat k automatizaci svých útoků i vývoje nového kódu také, čímž hrozba ransomwaru dále poroste.

Více informací o trendech ransomwaru v roce 2025 najdete ve zprávě na webu Securelist.com.

Společnost Kaspersky vyzývá organizace, aby nejen v Den boje proti ransomwaru dodržovaly tyto osvědčené postupy ochrany:

⇒ Využívejte spolehlivé bezpečnostní řešení renomovaných značek, například oceňovaný Kaspersky.

⇒ Udržujte software na všech používaných zařízeních neustále v aktuálním stavu, abyste zabránili útočníkům zneužít nově objevené zranitelnosti a proniknout do vaší sítě.

⇒ Zaměřte svoji obrannou strategii na detekci metody „lateral movement“ (postupné pronikání útočníka do sítě přes jedno ovládnuté zařízení a získávání kontroly nad dalšími zařízeními) a na exfiltraci vašich dat na internet. Věnujte zvláštní pozornost odchozímu provozu, abyste odhalili připojení kyberzločinců k vaší síti. Používejte offline zálohy dat, se kterými nemohou narušitelé manipulovat. Zajistěte, abyste k nim měli v případě potřeby nebo nouzové situace rychlý přístup.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-ransomware-utoci-chytreji-a-levneji-co-ocekavat-v-roce-2025/2671025