V letošním roce lze očekávat útoky za použití AI, růst hrozeb pro Android i pokračující útoky ransomwarem

8.1.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Bezpečností experti z českých poboček společnosti ESET komentují vývoj hrozeb ve druhé polovině roku 2023 a nabízejí výhled v aktuálních kyberbezpečnostních tématech pro následující měsíce roku 2024.

„Rok 2023 byl rokem, kdy kyberzločinci začali naplno využívat generativní umělou inteligenci ke zlepšování svých útočných kampaní, zejména pokud jde o vytváření obsahu pro různé online podvody, phishing nebo jinou manipulaci s uživateli. Očekáváme, že v roce 2024 se tento trend zrychlí a AI se stane ústředním prvkem ve vytváření útoků tzv. sociálního inženýrství,“ říká Vladimíra Žáčková, specialistka kybernetické bezpečnosti společnosti ESET.

„Ve druhé polovině roku 2023 společnost ESET také zablokovala více než 650 000 pokusů o přístup ke škodlivým doménám, jejichž názvy obsahovaly řetězec chatgpt nebo podobný text odkazující na chatbota ChatGPT nebo na stránky, které zdánlivě nabízely služby společnosti OpenAI. Nerostly tak pouze útoky za využití nástrojů umělé inteligence, ale také případy podvodů a phishingu zneužívající přímo jméno konkrétního nástroje,“ dodává Žáčková.

„Dalšími oblastmi, kde by nástroje umělé inteligence mohly mít značný dopad, jsou dezinformační a deepfake kampaně používané z politických, ideologických nebo jiných důvodů. To dokládají i příklady z minulého roku jako deepfake audio zveřejněné den před slovenskými parlamentními volbami nebo množství falešných videí šířících se prostřednictvím sociálních médií v souvislosti s aktuální válkou Izraele proti Hamásu,“ uzavírá Žáčková z ESETu.

„Ve druhé polovině roku 2023 jsme zaznamenali u systému Android výrazný nárůst případů spywaru, a to globálně o 89 %. Nárůst připisujeme především přítomnosti malwaru SpinOk. Tento škodlivý kód je distribuován jako sada pro vývoj softwaru a nachází se v různých, i legitimních aplikacích pro systém Android. Mohou se s ním setkat i čeští uživatelé, protože malware SpinOk pravidelně detekujeme také na platformě Android v Česku, a to od loňského června,“ vysvětluje Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

„V letošním roce očekáváme v případě platformy Android také neustálý nárůst adwaru, clickerů a skrytých aplikací, jejichž autoři vydělávají peníze zobrazováním velkého množství reklam uživatelům. Tento přístup funguje, protože mnoho uživatelů nechce za aplikace platit a místo toho volí neoficiální verze zdarma, které jsou ale zpravidla součástí většího balíčku obsahujícího škodlivý kód. S takovými aplikacemi se mohou uživatelé nejčastěji setkat v obchodech třetích stran,“ říká Kropáč a dodává: *„Očekáváme, že autoři škodlivého kódu mohou využívat nástroje umělé inteligence ke zlepšení jazykové kvality a důvěryhodnosti svých škodlivých aplikací a obsahu. Jejich distribuce bude také snazší a rychlejší vzhledem ke generativním schopnostem AI modelů, které mohou vytvářet nové webové stránky.“*

„Obzvláště znepokojivá je také například forma digitální lichvy v podobě škodlivých aplikací, které označujeme termínem SpyLoan a u kterých jsme zaznamenali alarmující meziroční nárůst o 285 %. Podvodné aplikace nabízejí uživatelům půjčky s vysokým úrokem a shromažďují osobní a citlivé informace, které odesílají na servery útočníků. Ti pak tyto údaje využívají k obtěžování a vydírání

uživatelů, kteří včas neplatí splátky. Ačkoli se aplikace převážně šíří prostřednictvím online tržišť třetích stran, v některých případech byly staženy také z Google Play a mohou se zde znovu objevit i v roce 2024. Dále předpokládáme, že se tyto aplikace rozšíří i mimo region Střední a Jižní Ameriky a jihovýchodní Asie, kde jsou aktuálně nejrozšířenější,“ uzavírá Kropáč z ESETu.

„Vyděračský software neboli ransomware je stále jednou z největších hrozeb pro firmy. V uplynulém roce byl opět aktivnější než v roce 2022, a to skoro dvojnásobně. Podle dostupných zjištění vzniká mnoho nových variant ransomwaru na základě již dříve uniklých zdrojových kódů předchozích variant. Mnohdy tak nové varianty vytváří i amatérští útočníci. Zároveň to ale pomáhá i nám, obráncům, abychom dokázali pokrýt širší škálu všech variant ransomwaru, včetně těch právě nově vznikajících, s pomocí obecnější sady pravidel a detekcí,“ vysvětluje Jakub Souček, bezpečnostní expert z pražské výzkumné pobočky společnosti ESET.

„Na základě veřejných informací a incidentů, které jsme analyzovali, vzrostly v minulém roce také požadavky na výkupné. Je ovšem obtížné posoudit, zda to bylo způsobeno snahou útočníků o co největší zisk nebo menší ochotou obětí platit, což útočníky mohlo nutit hledat velké příjmy. Je také možné, že vývoj požadované výše výkupného ovlivnila vysoká inflace,“ doplňuje Souček.

„V roce 2024 očekáváme, že většina stávajících trendů v útocích ransomwarem bude pokračovat. Útočníci budou stále aktivnější a agresivnější ve svých požadavcích na výkupné. Současné přední ransomwarové gangy se také budou soustředit na zapojení dalších kyberzločinců do svých stávajících útočných kampaní, proto neočekáváme, že by se v letošním roce objevilo větší množství nových významnějších ransomwarových skupin jako jejich nově vznikajících konkurentů,“ dodává Souček z ESETu.

Další technické informace naleznete například v kompletní zprávě ESET Threat Report H2 2023, která mapuje globální vývoj kybernetických hrozeb za období od června 2023 do listopadu 2023 a shrnuje nejvýznamnější odhalení bezpečnostních expertů společnosti ESET.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky připravuje také podcast True Positive nebo online magazín o IT bezpečnosti pro firmy Digital Security Guide.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete také na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/komentar-eset-v-letosnim-roce-lze-ocekavat-utoky-za-pouziti-ai-rust-hrozeb-pro-android-i-pokracujici