Globální vývoj kybernetických hrozeb od ESET: Útočníci zneužívají ke krádeži dat falešné AI aplikace

9.7.2024 - Lucie Mudráková | ESET software

Společnost ESET vydala svou nejnovější zprávu ESET Threat Report H1 2024. Zpráva shrnuje globální vývoj kybernetických hrozeb na základě dat z telemetrie a odborného pohledu analytiků společnosti, a to od prosince 2023 do května 2024.

Infostealery, se kterými se útočníci pravidelně zaměřují také na Českou republiku, začaly napodobovat generativní AI nástroje jako Midjourney, Sora nebo Gemini. V oblasti kybernetických hrozeb pro mobilní zařízení se objevil také nový malware GoldPickaxe, který je se svými funkcemi schopný krást data k rozpoznávání obličeje, a tím vytvářet deepfake obsah. Bezpečnostní experti ve zprávě popsali také kybergang využívající malware Balada Injector, který je nechvalně proslulý zneužíváním zranitelností pluginů WordPress. Skupina útočníků v první polovině roku 2024 kompromitovala přes 20 000 webových stránek, včetně webů v České republice. Zpráva se také věnuje vývoji ransomwarových hrozeb, kdy v centru pozornosti stála v posledním půl roce operace Cronos k rozbití ransomwarového gangu LockBit.

„Za sledované období, které pokrývá naše poslední zpráva ESET Threat Report, jsme se setkali s novým chováním infostealerů. S tímto typem škodlivého kódu se pravidelně setkávají i uživatelé v Česku, především v případě operačního systému Windows. Již od loňského roku sledujeme, jak infostealery postupně nepřímo zneužívají nástroje generativní umělé inteligence. Přestože pokračující vývoj těchto modelů doprovází ochranná opatření, která mají zabránit jejich zneužití, kyberzločincům to nezabránilo, aby zneužili jména nástrojů ve svých útocích – jmenovitě šlo například o napodobeniny služeb Midjourney, Sora nebo Gemini. Očekáváme, že tento trend bude pokračovat. Uživatelům proto doporučujeme, aby byli obezřetní při stahování a využívání AI nástrojů a nenechali se zlákat mnohdy výhodnými, ale podvodnými nabídkami, které se objevují na sociálních sítích. Před infostealery a před spywarem je účinnou ochranou bezpečnostní software," říká Jiří Kropáč, vedoucí detekcí hrozeb a výzkumné pobočky společnosti ESET v Brně.

„Z veřejně dostupných údajů na webech informujících o únicích informací vyplývá, že počet útoků ransomwarem v prvním čtvrtletí roku 2024 vzrostl o více než 20 % ve srovnání s prvním čtvrtletím předešlého roku. Ve druhém čtvrtletí jsme pozorovali určitý pokles detekcí, především v důsledku oslabení a rozpadu některých ransomwarových gangů. Zde je na místě zmínit operaci Cronos z letošního února, která vedla k narušení nechvalně proslulého ransomwarového gangu LockBit. Druhá polovina roku 2024 jistě přinese jasnější obrázek o tom, kam se zbylé části a nespokojení partneři dřívějších uskupení přesunuli a s jakými dalšími aktéry uzavřeli nová spojenectví," shrnuje situaci kolem ransomwarových hrozeb Jakub Souček, bezpečnostní expert z pražské výzkumné pobočky společnosti ESET a vedoucí nového pražského týmu, který se na ransomware zaměřuje.

„Ve sledovaném období jsme zachytili také výjimečnou aktivitu gangu využívající Balada Injector, který se specializuje na zneužívání zranitelností ve službě WordPress. Škodlivý JavaScript JS/Agent.RJR jsme sledovali také v České republice. Škodlivé skripty mohou vést až k úplnému převzetí webového serveru," dodává Jiří Kropáč z ESETu.

Skupina stojící za malwarem Balada Injector neblaze proslula zneužíváním zranitelností pluginů

WordPress. V první polovině roku 2024 byla skupina výjimečně aktivní. Podařilo se jí kompromitovat přes 20 000 webových stránek. Detekční technologie společnosti ESET zaznamenaly více než 400 000 případů, kdy gang v rámci svých kampaní převzal kontrolu nad webovými servery obětí.

Vzhledem k tomu, že škodlivé JavaScript kódy mohou vést až k úplnému ovládnutí webového serveru, je podle bezpečnostních expertů důležité nezapomenout z webu při řešení incidentů odstranit všechny zranitelné pluginy a aktualizovat systém jako ochranu před budoucím zneužitím. Balada Injector také do systému obvykle instaluje mechanismy proti odstranění škodlivého kódu (tzv. mechanismy perzistence). Pro zabezpečení systému je tak důležité odstranit i je, a to prostřednictvím kontroly kompromitovaných administrátorských účtů a souborů na daném webovém serveru. Následně experti doporučují změnit také přihlašovací údaje.

Využití nástrojů umělé inteligence bylo během sledovaných šesti měsíců patrné u několika různých typů kybernetických hrozeb. Jednalo se například o hrozby zaměřené na mobilní bankovní služby platformy Android, ať už ve formě „tradičního“ bankovního malwaru nebo tzv. kryptostealerů. Škodlivé kódy zaměřující se na krádeže informací, tzv. infostealery, nyní mohou napodobovat generativní nástroje AI a nový mobilní malware GoldPickaxe dokonce dokáže krást data pro rozpoznávání obličeje a vytvářet deepfake videa, která útočníci používají k ověření podvodných finančních transakcí.

„GoldPickaxe má verze pro Android i iOS a cílí na oběti v jihovýchodní Asii prostřednictvím lokalizovaných škodlivých aplikací. Při bližší analýze této rodiny malwaru jsme objevili, že starší podoba tohoto škodlivého kódu nazvaná GoldDiggerPlus se také zaměřila na oběti v Latinské Americe a Jižní Africe,“ vysvětluje Jiří Kropáč.

V první polovině roku 2024 zneužíval škodlivý kód Rilide Stealer ke zmatení a nalákaní obětí jména generativních AI asistentů, jako je Sora od OpenAI a Gemini od Google. Škodlivý kód Vidar infostealer se zase skrýval za údajnou desktopovou aplikací Midjourney ke generování AI obrázků pro operační systém Windows, přestože v době útoku nebyla tato aplikace oficiálně k dispozici. Ke stažení škodlivého kódu byli uživatelé lákáni také prostřednictvím reklam na Facebooku. Bezpečnostní experti z ESETu počítají s tím, že trend, kdy se škodlivý kód maskuje za známé AI nástroje, aby se dostal do zařízení obětí, bude i nadále pokračovat.

Infostealery byly ve sledovaném období hrozbou i pro fanoušky gamingu, a to především pro herní nadšence, kteří se pohybují mimo oficiální herní ekosystém. Některé cracknuté videohry a nástroje pro podvádění využívané v online multiplayerových hrách (tzv. cheaty) obsahovaly malwary Lumma Stealer a RedLine Stealer. RedLine Stealer na sebe v detekčních datech upozornil několika silnými kampaněmi ve Španělsku, Japonsku a Německu. Jednalo se o tak významné události, že detekce malwaru RedLine Stealer v první polovině roku 2024 překonaly detekce za stejné období roku 2023 o třetinu.

Mezi ransomwarovými skupinami došlo v únoru 2024 k zásadnímu narušení činnosti přední skupiny LockBit, a to v rámci globální policejní operace Cronos pod vedením britské NCA. ESET sice zaznamenal ve sledovaném období dvě významné kampaně tohoto ransomwaru, stály za nimi však skupiny, které využívaly pouze veřejně uniklý builder ransomwaru LockBit. Podle bezpečnostních expertů se LockBit také snaží zachránit svou reputaci například tím, že na svých webových stránkách zveřejňuje až dva roky staré údaje o obětech a vydává je za nové. Cílem je pravděpodobně udržet iluzi, že se policejní operace skupiny nedotkla.

Zpráva ESET Threat Report obsahuje dále informace o více než desetiletém vyšetřování pokročilých globálních kampaní, které využívají malware Ebury. Během let byl malware Ebury nasazen jako backdoor (tzv. zadní vrátka) ke kompromitaci téměř 400 000 serverů Linux, FreeBSD a OpenBSD po

celém světě. Koncem roku 2023 bylo stále kompromitováno více než 100 000 serverů.

Více informací o vývoji kybernetických hrozeb za období od prosince 2023 do května 2024 najdete v celém znění zprávy ESET Threat Report H1 2024.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále 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 řešení od 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/globalni-vyvoj-kybernetickych-hrozeb-od-eset-utocnici-zneuzivaji-ke-kradezi-dat-falesne-ai-aplikace