Komentář ESET: Rok 2025 bude ve znamení hrozeb pro platformu iOS a phishingových útoků generovaných AI

19.12.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Experti společnosti ESET reflektují vývoj hrozeb v letošním roce a nabízí výhled do aktuálních kyberbezpečnostních témat pro nadcházející měsíce roku 2025.

„Již v letošním roce jsme zaznamenali nárůst spamů, podvodných a phisingových kampaní generovaných za použití nástrojů umělé inteligence. V kontextu očekávaných geopolitických změn v roce 2025 předpokládáme možné rozvolnění pravidel pro sociální média a technologické společnosti. Tato změna může vést k dalšímu nárůstu a zhoršení kvality obsahu spolu s dalším růstem nevyžádaných zpráv a dalších podvodných aktivit," říká Juraj Jánošík, vedoucí oddělení automatizovaných systémů a inteligentních řešení společnosti ESET.

„Nekvalitní obsah generovaný umělou inteligencí může sloužit také jako lákadlo pro zranitelné uživatele sociálních médií, kteří by se následně mohli stát terčem dezinformačních kampaní. Mohou být také manipulováni k tomu, aby se sami stali jejich aktivními šiřiteli. Tato taktika by mohla částečně automatizovat činnost obsahových a trollích farem, které v současnosti využívají nepřátelské státy a skupiny," pokračuje Jánošík.

„Předpokládáme, že útočníci mohou využít nedávný pokrok v oblasti malých open-source GPT modelů a trénovat je na datech z odcizených účtů na sociálních sítích. To by jim potenciálně umožnilo napodobovat styly komunikace a vydávat se za oběti v různých situacích, jako jsou případy nouze v rodinách nebo milostné podvody. Tím by se tyto podvodné aktivity staly uvěřitelnějšími," varuje Jánošík.

„V roce 2025 také předpokládáme nárůst počtu falešných nebo duplicitních účtů celebrit a dalších veřejně známých osobností na sociálních sítích. Tyto podvodné profily budou využívat deepfake videa a další obsah generovaný pomocí nástrojů umělé inteligence, aby vypadaly legitimně a důvěryhodně. Tím se zvýší význam nástrojů pro ověřování pravosti, jako jsou odznaky Ověřeno na sociálních sítích," doplňuje Jánošík z ESETu.

„V roce 2024 jsme analyzovali útoky využívající nový způsob kompromitace mobilních zařízení se systémy Android a iOS. Útočníci v něm využívají progresivní webové aplikace (PWA) a WebAPK k obejití tradičních bezpečnostních opatření. Jejich cílem je podvodem přimět uživatele k instalaci škodlivých aplikací, které kradou bankovní přihlašovací údaje. Tyto aplikace napodobují legitimní bankovní aplikace a umožňují útočníkům získat přihlašovací údaje, hesla a dvoufaktorové autentizační kódy. Ty útočníci následně použijí k získání neoprávněného přístupu k účtům obětí," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Vzhledem k tomu, že kyberzločinci pokračují v inovacích, je pravděpodobné, že používání PWA a WebAPK ke škodlivým účelům bude narůstat i v roce 2025. Tyto technologie poskytují útočníkům pohodlný a účinný prostředek k šíření podvodných aplikací, aniž by potřebovali schválení v oficiálních obchodech s aplikacemi. Multiplatformní povaha PWA také umožňuje útočníkům cílit na širší publikum, díky čemuž jsou tyto typy útoků univerzálnější a je možné je škálovat," vysvětluje Jirkal.

„Na základě útoků využívajících PWA a WebAPK očekáváme v roce 2025 nárůst hrozeb zaměřených na platformu iOS. Přísné zásady obchodu App Store odjakživa ztěžují šíření škodlivých aplikací, což vede uživatele k přesvědčení, že jejich zařízení se systémem iOS jsou ze své podstaty bezpečnější. Hrozby se však mohou šířit i alternativními cestami. Jejich zdrojem mohou být škodlivé webové stránky, phishingové útoky, nebezpečné přílohy e-mailů, taktiky sociálního inženýrství a škodlivé reklamy umístěné ve vyhledávačích, na sociálních sítích a na webových stránkách. Žádný z těchto způsobů šíření přitom nepodléhá kontrole aplikací obchodu App Store. Společnost Apple se na druhou stranu samozřejmě snaží reagovat na nové hrozby a aktualizovat svá bezpečnostní opatření," doplňuje Jirkal.

„Pravděpodobně se zvýší také počet mobilního i nemobilního škodlivého kódu, který využívá open-source sadu pro vývoj softwaru Flutter (SDK). Flutter je určen pro vytváření multiplatformních aplikací, zjednodušuje jejich vývoj a útočníci jej mohou také využít k efektivnějšímu vytváření a šíření malwaru a trojských koní. Například některé aplikace typu SpyLoan již doplněk SDK využívaly. Útočníci využívají Flutter také jako nástroj, který komplikuje snahy odhalit škodlivé kódy. Zda se využití Flutteru pro tyto účely v roce 2025 zvýší, bude záviset na různých faktorech, včetně toho, zda se kyberzločinci naučí programovací jazyk Dart. Důležité je poznamenat, že kyberbezpečnostní komunita aktivně vytváří nové nástroje a techniky pro rozbor a pochopení složitostí aplikací Flutter," uzavírá Jirkal z ESETu.

„V roce 2024 se gang útočníků RansomHub etabloval jako vedoucí skupina na ransomwarovém trhu a nahradil rozbitý gang LockBit. Očekáváme, že RansomHub si tuto pozici udrží i v roce 2025. Prostředí RaaS (Ransomware-as-a-Service) je však velmi konkurenční a gangy zde často přicházejí s inovacemi a změnami svých partnerských programů. Snaží se přilákat více partnerů a zvýšit tak ziskovost. Pokud se ukáže, že někteří z konkurentů jsou ziskovější, zkušení partneři mohou velmi dobře upravit svá spojenectví. Alarmujícím trendem roku 2024 byl celosvětový rapidní růst útoků na sektor zdravotnictví. Pozorujeme to nyní i na konci roku. Je tak bohužel možné, že tento trend bude pokračovat i v příštím roce," předpovídá Jakub Souček, vedoucí pražského výzkumného týmu společnosti ESET.

„Škodlivé kódy, které se snaží vypnout bezpečnostní řešení, se staly běžnou součástí útoků ransomwarem. V roce 2025 očekáváme, že nejpokročilejší skupiny tento typ nástrojů ještě více zdokonalí. Budou tak stále sofistikovanější, lépe skryté, a tudíž hůře odhalitelné. Tento trend ukazuje, že bezpečnostní nástroje, jako je EDR, jsou kyberzločincům trnem v oku a budou se je usilovně snažit odstranit nebo alespoň vypnout," myslí si Souček.

„Většina nováčků, kteří se pokusí vydobýt si své místo v ekosystému RaaS, bude nejspíše kódovat své šifrovací nástroje v jazyce Rust nebo Go, jak je to trendem u zavedených skupin. Díky tomu totiž útočníci dokáží na jedno kliknutí zařídit, aby škodlivý kód fungoval v různých operačních systémech," uzavírá Souček z ESETu.

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 výzkumná a 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.

Lucie Mudráková

Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/komentar-eset-rok-2025-bude-ve-znameni-hrozeb-pro-platformu-ios-a-phishingovych-utoku-generovanych-ai