Avast zablokoval v roce 2023 rekordních 10 miliard útoků; Česko sužovaly finanční a seznamovací podvody

12.2.2024 - | Avast Software

Avast, přední značka v oblasti digitální bezpečnosti a ochrany soukromí společnosti Gen™ (NASDAQ: GEN), zablokovala v roce 2023 bezprecedentních 10 miliard útoků, což představuje pozoruhodný meziroční nárůst o 49 procent. V Česku bylo celkem zablokováno kolem 194 milionů útoků, což je o 55 % více než v předchozím roce a jde o historicky nejvyšší hodnotu převyšující světový průměr. Podle nejnovější čtvrtletní zprávy Avast Threat Report, která se zabývá hrozbami v období od října do prosince 2023, představují i nadále více než 75 % všech kyberhrozeb podvody, phishing a malvertising.

Tyto hrozby často přicházejí ve formě škodlivých push notifikací a nových metod umělé inteligence, jako jsou deepfakes. Ty s využitím tváře a hlasu známých osobností lákaly oběti zejména na sofistikované finanční podvody, které se masivně rozmáhaly i v Česku. Uplynulé čtvrtletí bylo také ve znamení nárůstu malwarových útoků využívajících soubory PDF a nových technik, jak zneužít Google ke krádeži informací.

„V posledních třech měsících jsme byli svědky toho, že se kyberzločinci přestali spoléhat pouze na sociální inženýrství a začali využívat důvěryhodná digitální média, ať už se jedná o velmi věrohodná deepfake videa nebo hrozby šířící se prostřednictvím souborů PDF," vysvětluje ředitel výzkumu malwaru Avastu Jakub Křoustek. „Tento trend odráží nejen neustále se měnící metody kyberzločinců, ale také poukazuje na zranitelnosti našeho každodenního digitálního života. Nyní je více než kdy jindy potřeba, aby si lidé ověřovali, s čím se na internetu setkávají, a využívali nástroje, které jim pomohou zůstat v bezpečí."

V posledním čtvrtletí roku 2023 zablokoval Avast více než 10 milionů útoků využívajících soubory PDF, a ochránil tak více než 4 miliony uživatelů po celém světě. Kyberzločinci se na soubory PDF zaměřili až v posledních měsících roku. Výzkumníci Avastu zaznamenali celou škálu hrozeb a podvodů spojených se soubory PDF, od jednoduchých podvodů s loteriemi a seznamkami až po dokumenty obsahující klamavé informace, jako jsou phishingové odkazy směřující na stránky napodobující známé značky jako Netflix nebo Amazon. Výzkumníci také zaznamenali nárůst komplexních kampaní šířících sofistikovanější hrozby, jako jsou nástroje na krádež hesel, např. AgentTesla.

Šíření kyberhrozeb s využitím formátu PDF znamená významný posun v taktice kyberzločinců. Soubory PDF jsou oblíbené pro svou nezávislost na platformě, která umožňuje jejich bezproblémové otevření na jakémkoli zařízení, což z nich dělá dokonalý způsob šíření hrozeb. Přílohy v PDF jsou navíc často ve výchozím nastavení povoleny spamovými filtry, což přidává další možnost zneužití.

I nadále dominovaly webové hrozby, přičemž podvody, phishing a malvertising se celkově umístily na předních místech žebříčku. Rostlo zejména používání škodlivých push notifikací v prohlížeči, které se staly upřednostňovaným nástrojem podvodníků napříč různými doménami, od stránek s obsahem pro dospělé až po podvody s technickou podporou. Populárním druhem podvodů byly také seznamovací podvody, s nimiž se setká zhruba jeden člověk z dvaceti a u nichž patří k nejvíc zasaženým zemím i Česko. V souvislosti s blížícím se Valentýnem se pak očekává ještě další nárůst.

Svou roli zde hraje také umělá inteligence, která kromě způsobů jejich šíření pomáhá zločincům vytvářet věrohodnější podvody. Deepfake videa, zejména ta spojená s investičními podvody, byla v minulém čtvrtletí výrazně sofistikovanější a otestovala schopnost lidí rozlišit mezi skutečným a uměle vytvořeným obsahem. Po sociálních sítích se také stále častěji šíří AI pornografie, která nyní snadno a velice levně může zneužít podobu existujících lidí, jako nejnověji kupříkladu zpěvačky Taylor Swift. Některé země, jako např. Spojené státy americké, už podnikají kroky k tomu, aby se oběti, bez jejichž souhlasu pornografický obsah generovaný za použití umělé inteligence vznikl, mohly bránit právními kroky.

Poslední čtvrtletí roku 2023 přineslo také novou a zajímavou techniku, kterou si rychle osvojily nástroje na krádež informací: zneužití koncového bodu Google OAuth, který slouží k synchronizaci účtů napříč službami Google, k obnovení autentizačních souborů cookies. Tento typ cookies v sobě může nést jedinečný identifikátor, který ověřuje identitu a oprávnění uživatele při přístupu na webové stránky. Pomocí autentizačních cookies mohou kyberzločinci získat přístup k přihlašovacím údajům dotyčného a dalším citlivým datům. Jedním z prvních nástrojů pro krádež informací, který tuto techniku využil, byla Lumma, rychle rostoucí malware jako služba (MaaS), a další ji brzy následovaly.

https://press.avast.com/cs-cz/avast-zablokoval-v-roce-2023-rekordnich-10-miliard-utoku-cesko-suzovaly-financni-a-seznamovaci-podvody