Kaspersky hlásí za rok 2024 téměř 900 milionů pokusů o phishing

21.2.2025 - | PROTEXT

Bezpečnostní řešení společnosti Kaspersky zablokovala v roce 2024 více než 893 miliony pokusů o phishing – to je 26% nárůst oproti roku 2023, kdy jich bylo celkem téměř 710 milionů. Nárůst těchto pokusů (znázorněný v grafu) mezi květnem a červencem je tradičně spojen s obdobím dovolených, kdy se podvodníci často pokoušejí nalákat cestování chtivé jedince na podvody zahrnující falešné rezervace letenek a hotelů, klamavé balíčky zájezdů a nabídky příliš dobré na to, aby byly pravdivé.

• Společnost Kaspersky zablokovala v roce 2024 ve srovnání s předchozím rokem celosvětově o 26 % více pokusů o phishing. Kyberzločinci pokračovali ve využívání známých značek, jako je Booking, Airbnb, TikTok a Telegram, aby ukradli přihlašovací údaje nebo instalovali malware.

• Uživatelé navíc čelili více než 125 milionům útoků prostřednictvím škodlivých příloh e-mailů.

• Každý druhý e-mail ve firemních schránkách byl spam.

Odborníci pozorovali řadu phishingových a podvodných schémat zaměřených na krádež dat, peněz a instalaci škodlivého softwaru. V roce 2024 kyberzločinci často napodobovali webové stránky známých značek, jako je Booking, Airbnb, TikTok, Telegram a další. Jedna probíhající kampaň se například zaměřuje na uživatele TikTok Shopu. Podvodníci vytvořili falešné přihlašovací stránky určené k odcizení přihlašovacích údajů prodejců. Kromě toho vydělávali na trendových zprávách a organizovali podvodná schémata týkající se žhavých témat, například kryptoměnové hry Hamster Kombat a peněženky TON.

Podvodné programy se v roce 2024 snažily těžit také z falešných obrázků celebrit a propagace rozdávání fiktivních hodnotných cen fanouškům, které ale nikdy nedostali. Tento trend přetrvává i v roce 2025.

„Základní mechanismy phishingu a podvodů zůstávají stejné, útočníci však neustále zdokonalují svoje finty a maskování. Vydělávají na trendových zprávách, medializovaných tématech nebo kombinují propagaci značek více společností na jedné phishingové stránce, aby zvýšili efektivitu svých kampaní. Ve vytváření velmi přesvědčivých falešných webových stránek jim přitom pomáhají nástroje řízené umělou inteligencí, takže je obtížnější tyto podvody odhalit. Neustále zdokonalované taktiky představují rostoucí riziko nejen pro zabezpečení financí, ale i pro ochranu osobní identity. Kvůli tomu nebyla ostražitost a používání robustních řešení kybernetické bezpečnosti nikdy důležitější,“ říká **Olga Svistunova**, bezpečnostní expertka společnosti Kaspersky.

Spam a škodlivé e-mailové kampaně

Podle údajů společnosti Kaspersky se jednotlivci i firemní uživatelé setkali v roce 2024 se škodlivými e-mailovými přílohami více než 125 milionkrát.

Odborníci pozorovali, že kyberzločinci používali v e-mailových kampaních zaměřených na firmy různé taktiky. Ty zahrnovaly zasílání e-mailů s heslem chráněnými archivy, které obsahovaly škodlivý

obsah a SVG obrázky maskované jako neškodná grafika, a mnoho dalších schémat. Útočníci lákali oběti ke klikání na škodlivý obsah prostřednictvím falešných soudních obsílek, fiktivních kontraktů, padělaných oficiálních oznámení apod.

Téměř každý druhý e-mail ve firemní poštovní schránce (47 % celosvětového provozu) byl spam, což představuje nárůst o 1,27 procentního bodu oproti předchozímu roku. I když spam zahrnuje různé e-mailové hrozby, včetně výše uvedených, není vždy škodlivý a obsahuje většinou nevyžádané reklamy. Odborníci poznamenávají, že trendy firemního spamu za poslední rok výrazně zahrnují reklamy na AI řešení, související webináře, online propagační služby, nabídky na zvýšení počtu příznivců na sociálních sítích a mnoho dalších.

Chcete-li se dozvědět více o prostředí spamu a phishingových hrozeb, navštivte stránky Securelist.com.

Abyste se nestali obětí phishingu, scamu nebo škodlivých zpráv, odborníci společnosti Kaspersky doporučují:

• Otevírejte e-maily a klikejte na odkazy pouze v případě, že jste si jisti, že můžete odesílateli důvěřovat.

• Pokud je odesílatel legitimní, ale obsah zprávy se zdá být podivný, vyplatí se ověřit si ho pomocí alternativních komunikačních prostředků.

• Při podezření na podvodnou stránku zkontrolujte správnost zápisu její webové adresy (URL). Podvržená adresa může například obsahovat změny, které jsou na první pohled těžko rozpoznatelné, například 1 místo I nebo 0 místo O.

• Při surfování na webu používejte osvědčená bezpečnostní řešení. Díky přístupu k mezinárodním zdrojům informací o hrozbách jsou tato řešení schopna odhalit a zablokovat spamové a phishingové kampaně.

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-hlasi-za-rok-2024-temer-900-milionu-pokusu-o-phishing/2637404