Kyberzločinci spojují útok na jednotlivce s masovými kampaněmi

12.7.2024 - | PROTEXT

Cílený phishing se zaměřuje na konkrétní osoby nebo malé skupiny. Využívají k tomu e-maily, které napodobují styl a obsah legitimní komunikace od důvěryhodných subjektů. Jsou pečlivě vytvořeny tak, aby se obešly bezpečnostní filtry, a často neobsahují žádné technické chyby. Masové phishingové kampaně naopak rozhodí širokou síť a rozesílají obecné zprávy mnoha příjemcům. Jsou neosobní, nekonkrétní a často obsahují chyby v textu i designu.

Koncem roku 2023 výzkumníci společnosti Kaspersky zaznamenali statistickou anomálii, která svědčila o kombinaci taktiky cíleného spear phishingu a hromadného phishingu. Některé detekované e-maily byly příliš agresivní na spear phishing, ale příliš sofistikované na hromadný phishing. V jednom případě phishingový e-mail z oblasti lidských zdrojů oslovil příjemce jménem a odkazoval na jeho společnost, avšak propojený phishingový formulář byl jen obecným falešným přihlášením do aplikace Outlook, což je typickým znakem hromadného phishingu.

„Podvodná e-mailová zpráva využívající ghost spoofing: jméno odesílatele obsahuje e-mailovou adresu personálního týmu, čímž se e-mailu dodá zdání pravosti.“

Další kampaň využívala tzv. „ghost spoofing“, kdy se v názvu odesílatele objeví skutečná firemní e-mailová adresa, aniž by se změnila skutečná doména. Tato technika, která je obvykle využívaná při cílených útocích, byla použita při hromadném phishingu a dodávala mu zdání autenticity, ale po kliknutí na odkaz vedla k obecnému phishingovému formuláři.

V období od března do května 2024 společnost Kaspersky zjistila výrazný nárůst počtu hybridních phishingových e-mailů. Tento nárůst naznačuje, že útočníci využívají pokročilé technologie ke snížení nákladů a úsilí na personalizaci masových útoků. Nástroje poháněné umělou inteligencí nyní dokážou vytvořit dostatečně přesvědčivý text e-mailu, opravit překlepy a vylepšit design, díky čemuž jsou účinnější a hůře odhalitelné.

„Útočníci ve svých hromadných kampaních stále častěji používají metody a technologie spear phishingu, což vede k personalizovanějším e-mailům a rozšiřuje se škála technologií a taktik podvodného jednání. Přestože se jedná o hromadné e-mailové kampaně, představují tyto útoky významnou hrozbu. V boji proti této neustále se rozvíjející hrozbě je nezbytné zavést bezpečnostní opatření, která drží krok s technologickým vývojem a využívají kombinaci moderních postupů a služeb,“ komentuje **Roman Dedenok** ze společnosti Kaspersky.

Další informace naleznete na webu Securelist.

Aby byla vaše data chráněna před phishingovými útoky a úniky, doporučují odborníci společnosti Kaspersky následující:

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

https://www.ceskenoviny.cz/tiskove/zpravy/kyberzlocinci-spojuji-utok-na-jednotlivce-s-masovymi-kampanemi/2542885