Téměř 90 % kyberhrozeb spočívá v manipulaci člověkem

14.5.2024 - | Avast Software

Podle Avastu, lídra v oblasti digitálního zabezpečení a ochrany soukromí a značky společnosti Gen™ (NASDAQ: GEN), bude v roce 2024 většinu kyberhrozeb, kterým budou jednotlivci čelit, představovat sociální inženýrství, tedy manipulace s lidmi. Z nejnovější čtvrtletní zprávy Avast Threat Report, která se zabývá hrozbami od ledna do března 2024, vyplývá, že podvody, phishing a malvertising představují 90 % všech hrozeb na mobilních zařízeních a 87 % hrozeb na počítačích. Výzkumníci hrozeb navíc objevili výrazný nárůst podvodů využívajících sofistikované taktiky jako jsou technologie deepfake, synchronizace hlasu pomocí umělé inteligence nebo krádeže účtů na YouTube a dalších sociálních sítích k šíření podvodného obsahu.

„V prvním čtvrtletí roku 2024 jsme zaznamenali historicky nejvyšší kyberbezpečností riziko, což znamená tu nejvyšší pravděpodobnost, že se člověk stane cílem kybernetického útoku," říká Jakub Křoustek, ředitel výzkumu malwaru ve společnosti Gen. „Bohužel, lidé jsou nejslabším článkem digitálního bezpečnostního řetězce a kyberzločinci to vědí. Využívají emoce a touhu po vědění, aby pronikli do lidských životů a zařízení a získali z nich peníze."

I když jsou všechny sociální sítě přirozeným líhništěm podvodů, významným kanálem pro kriminalitu se stal především YouTube. Podle telemetrických údajů Avastu byly v roce 2023 před hrozbami na YouTube ochráněny 4 miliony unikátních uživatelů a v lednu až březnu 2024 dalších přibližně 500 tisíc.

Automatizované reklamní systémy v kombinaci s obsahem vytvářeným uživateli představují pro kyberzločince bránu, která umožňuje obejít běžná bezpečnostní opatření. YouTube se tak stává účinným kanálem pro šíření phishingu a malwaru. K významným hrozbám na této platformě patří nástroje pro krádež přihlašovacích údajů, jako jsou Lumma a Redline, odkazy na phishingové a podvodné stránky (landing pages) a škodlivý software maskovaný jako legitimní aplikace nebo aktualizace.

Podvodníci také ve velké míře využívají jako lákadlo na své podvody videa. A jde o videa všeho druhu, od již existujících záběrů po propracovaný deepfake. Jedna z nejrozšířenějších technik spočívá ve využívání známých osobností a významných medializovaných událostí k přilákání velkého množství diváků. Tyto kampaně často využívají deepfaky, které vznikají převzetím oficiálních videí, jež pomocí umělé inteligence synchronizují s nově vytvořeným hlasem. Tato videa plynule kombinují pozměněný zvuk s existujícím obrazem, takže necvičené oko jen obtížně pozná, že se nejedná o autentický obsah.

Kromě toho slouží YouTube jako kanál pro distribuční systémy (TDS), které přesměrovávají uživatele na škodlivé stránky a podporují nejrůznější scamy, od rozdávání falešných bonusů až po investiční podvody.

Mezi nejčastější podvodné taktiky na YouTube patří:

Za rostoucím počtem podvodů stojí i kyberzločinci využívající nové obchodní příležitosti: model malware jako služba (Malware-as-a-Service, MaaS). Prostřednictvím tohoto modelu podnikání mohou organizované zločinecké skupiny najímat menší zločince, kteří si chtějí rychle vydělat peníze

distribucí malwaru pod záštitou skupiny. Tito zločinci si mohou malware jednorázově zakoupit, předplatit si ho jako službu nebo se i partnersky podílet na zisku v rámci provize.

Nejčastějším malwarem využívaným v modelu MaaS jsou programy pro krádež přihlašovacích údajů, které stále hledají nové distribuční kanály. Například DarkGate se údajně šíříprostřednictvím phishingu v Microsoft Teams. Lumma Stealer, další nástroj pro krádež přihlašovacích údajů na modelu MaaS, se stále šíří prostřednictvímcracknutého softwaru sdíleného na YouTube, přičemž k oklamání obětí využívá falešné návody. To jen podtrhuje, že tyto malwarové kmeny – ani jejich tvůrci – nikdy nepromeškají příležitost využít sociální inženýrství k dalšímu šíření.

Další informace a celou zprávu o hrozbách Avast Threat Report za 1. čtvrtletí 2024 najdete na https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/.

https://press.avast.com/cs-cz/temer-90-kyberhrozeb-spociva-v-manipulaci-clovekem