Kaspersky: trojan Necro na Google Play napadl až 11 milionů obětí

27.9.2024 - | PROTEXT

Možnosti trojského koně Necro

Varianta hrozby Necro, kterou objevili odborníci společnosti Kaspersky, dokáže do infikovaných smartphonů stahovat moduly, které zobrazují reklamy v neviditelných oknech a umožňují na ně kliknout, stahovat spustitelné soubory, instalovat aplikace třetích stran a otevírat libovolné odkazy v neviditelných oknech WebView a tím spouštět kód JavaScriptu. Na základě svých technických parametrů je trojský kůň pravděpodobně také schopen přihlásit uživatele k placeným službám. Stažené moduly navíc útočníkům umožňují přesměrovat internetový provoz přes zařízení oběti. To umožňuje kyberzločincům navštěvovat zakázané servery pomocí zařízení oběti a potenciálně jej využívat jako součást proxy botnetu.

Infikované aplikace na neoficiálních platformách

Odborníci společnosti objevili Necro poprvé v upravené verzi aplikace Spotify Plus. Tvůrci aplikace tvrdili, že je pro zařízení bezpečná a nabízí další funkce, které se v oficiální aplikaci ke streamování hudby nenacházejí. Následně odborníci našli také upravenou verzi aplikace WhatsApp obsahující downloader Necro a poté infikované verze populárních her, včetně Minecraftu, Stumble Guys a Car Parking Multiplayer. Necro byl do těchto aplikací integrován přes neověřený reklamní modul.

Infikované aplikace v Google Play

Kromě platforem třetích stran se Necro rozšířil i do Google Play. Škodlivý downloader byl nalezen v aplikaci Wuta Camera a Max Browser. Podle statistik Google Play přesáhl počet stažení těchto aplikací dohromady 11 milionů. Na této platformě byl Necro distribuován také prostřednictvím neověřeného reklamního modulu. Na základě hlášení Kaspersky Lab společnosti Google byl škodlivý kód z aplikace Wuta Camera odstraněn a aplikace Max Browser byla z obchodu stažena. Uživatelé však stále riskují, že se s Necro setkají na neoficiálních platformách.

"*Uživatelé často stahují neoficiální, upravené aplikace, aby obešli omezení v oficiálních aplikacích nebo získali přístup k dalším bezplatným funkcím. Kyberzločinci tohoto chování využívají a šíří prostřednictvím těchto aplikací malware, protože na platformách třetích stran neexistuje žádná regulace*," komentuje **Dmitrij Kalinin**, odborník na kybernetickou bezpečnost společnosti Kaspersky. "*Za zmínku stojí také to, že verze Necro vložená do těchto aplikací používala techniky steganografie a skrývala svůj payload v obrázcích, aby zůstala neodhalena - což je u mobilního malwaru velmi ojedinělá metoda.*"

Bezpečnostní řešení společnosti Kaspersky chrání před hrozbou Necro a detekují downloader jako Trojan-Downloader.AndroidOS.Necro.f a Trojan-Downloader.AndroidOS.Necro.h, přičemž škodlivé komponenty jsou identifikovány jako Trojan.AndroidOS.Necro.

Další informace o trojanu Necro naleznete na webu Securelist.com.

K ochraně před touto a dalšími kybernetickými hrozbami pro systém Android Kaspersky doporučuje:

[1] *Údaje vycházejí z anonymizovaných statistik produktů Kaspersky za období 26. srpna - 15. září*

2024.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-trojan-necro-na-google-play-napadl-az-11-milionu-obeti/2574622