Kaspersky hlásí přes 340.000 útoků skrz mód WhatsAppu

10.11.2023 - | PROTEXT

Lidé často přecházejí na modifikace svých oblíbených komunikačních aplikací (IM), aby získali další funkce. Některé z těchto modifikací, které jsou vytvářeny třetími stranami, sice vylepšují funkčnost, ale zároveň obsahují skrytý malware. Společnost Kaspersky identifikovala novou modifikaci aplikace WhatsApp, která nabízí přídavné funkce, například plánované zprávy a možnosti přizpůsobení, ale má v sobě také škodlivý spywarový modul.

Upravený soubor klienta WhatsApp obsahuje podezřelé komponenty (službu a přijímač vysílání), které v originální verzi nejsou. Přijímač iniciuje službu a spustí špionážní modul, když je telefon zapnutý nebo se nabíjí. Po aktivaci odešle škodlivý implantát zprávu s údaji o zařízení na server útočníka. Tyto údaje zahrnují IMEI, telefonní číslo, kódy zemí a sítí a další informace. Každých pět minut také přenáší kontakty a údaje o účtu oběti a dokáže dokonce nastavit nahrávání z mikrofonu a provádět exfiltraci souborů z externího úložiště.

Škodlivá verze pronikla do populárních kanálů Telegramu, které jsou zaměřeny převážně na arabsky a ázerbájdžánsky mluvící uživatele, přičemž některé z těchto kanálů se mohou pochlubit téměř dvěma miliony odběratelů. Výzkumníci společnosti Kaspersky proto upozornili na tento problém společnost Telegram. Telemetrie společnosti Kaspersky identifikovala jen během října více než 340 000 útoků s tímto modem, přičemž tato hrozba se objevila relativně nedávno – začala působit v polovině srpna 2023.

Nejvíce útoků bylo zaznamenáno v Ázerbájdžánu, Saúdské Arábii, Jemenu, Turecku a Egyptě. Ačkoli mezi obětmi převažují arabsky a ázerbájdžánsky mluvící uživatelé, zasaženy byly také osoby z USA, Ruska, Velké Británie, Německa a dalších zemí.

Produkty Kaspersky detekují trojského koně pod označením Trojan-Spy.AndroidOS.CanesSpy.

„Lidé přirozeně důvěřují aplikacím z vysoce sledovaných zdrojů, ale podvodníci této důvěry zneužívají. Šíření škodlivých modifikací prostřednictvím oblíbených platforem třetích stran zdůrazňuje důležitost používání oficiálních IM klientů. Pokud však potřebujete nějaké další funkce, které v originálním klientovi nejsou, měli byste před instalací softwaru od třetí strany zvážit použití renomovaného bezpečnostního řešení, které ochrání vaše data před ohrožením. Pro lepší ochranu osobních údajů stahujte aplikace vždy jen z oficiálních obchodů s aplikacemi nebo z oficiálních webových stránek,“ říká Dmitrij **Kalinin**, bezpečnostní expert společnosti Kaspersky.

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-hlasi-pres-340000-utoku-skrz-mod-whatsappu/2438993