Chameleon Android Banking Trojan Variant Bypasses Biometric Authentication

Badacze cyberbezpieczeństwa odkryli zaktualizowaną wersję złośliwego oprogramowania bankowego z Androidem o nazwie Chameleon, która rozszerzyła celowanie o użytkowników w Wielkiej Brytanii i Włoch.) Korzystając z Usługi Dostępności, wszystko, jednocześnie rozszerzając swój ukierunkowany region „Holenderska firma zajmująca się ochroną mobilną Threerzefabric w raporcie udostępnionym Hacker News.Chameleon został wcześniej udokumentowany przez Cyble w kwietniu 2023 r.Australia i Polska od co najmniej stycznia.Podobnie jak inne złośliwe oprogramowanie bankowe, wiadomo, że nadużywa swoich uprawnień do usługi dostępności Androida w celu zbioru wrażliwych danych i przeprowadzania ataków nakładek. Aplikacje nieuczciwe zawierające wcześniejszą wersję były hostowane na stronach phishingBiuro Podatków (ATO) i platforma handlu kryptowalutami o nazwie Coinspot, próbując nadać im zasłonę wiarygodności. Najnowsze ustalenia z zagrożenia pokazują, że trojan bankowy jest teraz dostarczany za pośrednictwem Zombinder, niewielkiej kropli.-Service (DAAS), który jest sprzedawany innym podmiotom zagrożonym i które można wykorzystać do „wiązania” złośliwych ładunków do legalnych aplikacji. Tradycyjne środki bezpieczeństwa nie zmniejszą tego w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.Chociaż podejrzewano, że oferta została zamknięta na początku tego roku, powtórzyła się w zeszłym miesiącu, możliwości reklamowe, aby ominąć funkcję „Ograniczone ustawienia” w Android w celu zainstalowania złośliwego oprogramowania na urządzeniach i uzyskania dostępu do usługi dostępnościMaskarada jako przeglądarka internetowa Google Chrome.Ich nazwy pakietów są wymienione poniżej -Godną uwagi cechą ulepszonego wariantu jest jego zdolność do przeprowadzania oszustw związanych z przejęciem urządzeń (DTO), która wykorzystuje usługę dostępności do wykonywania nieautoryzowanych działań w imieniu ofiary, ale w celu oszczędzania użytkowników, aby umożliwić ustawienie Ustawienia, złośliwe oprogramowanie sprawdza wersję Androida na zainstalowanym urządzeniu, a jeśli okaże się, że jest to Android 13 lub nowszy, zachęca użytkownika do włączenia go. ”Po otrzymaniu potwierdzenia systemu Android 13 obecnych na zainfekowanym urządzeniu, Trojan bankowy inicjujeŁadowanie strony HTML, „wyjaśnił Threerzefabric.„Strona prowadzi użytkowników poprzez ręczny proces krok po kroku, aby umożliwić usługę dostępności na Androida 13 i wyższej.” Kolejnym nowym dodatkiem jest użycie interfejsów API Androida w celu zakłócenia operacji biometrycznych docelowego urządzenia poprzez potajemne przejście blokadyMechanizm uwierzytelniania ekranu do PIN, aby umożliwić złośliwemu oprogramowaniu „odblokowanie urządzenia w Will„ Korzystanie z usługi dostępności ”. Pojawienie się nowego trojana bankowego Chameleon jest kolejnym przykładem wyrafinowanego i adaptacyjnego krajobrazu zagrożenia w ekosystemie Androida”Firma powiedziała.„Ewoluując od wcześniejszej iteracji, ten wariant pokazuje zwiększoną odporność i zaawansowane nowe cechy.” Rozwój pojawia się, gdy Zimperium ujawniło, że 29 rodzin złośliwego oprogramowania - 10 nowych - w ciągu ostatniego roku miało miejsce na 1800 zastosowań bankowych w 61 krajach.Nowe aktywne rodziny to Nexus, Ojciec chrzestny, Pixpirate, Saderat, Hook, Pixbankbot, Xenomorph V3, Vultur, Brasdex i Goatrat. Kraje najlepszych w USA obejmują amerykańskie (109 aplikacji bankowych), Wielka Brytania (48), Włosze (44), Australia (34), Turcja (32), Francja (30), Hiszpania (29), Portugalia (27), Niemcy (23), Kanada (17) i Brazylia (11).Najbardziej ukierunkowane aplikacje usług finansowych to Phonepe (Indie), WeChat, Bank of America, Well Fargo, (U.S.), Binance (Malta), Barclays (Wielka Brytania), QNB Finansbank (Turcja) i Caixabank (Hiszpania). ”Tradycyjna bankowość.Aplikacje pozostają głównym celem, z oszałamiającymi 1103 aplikacjami - stanowiącym 61% celów - podczas gdy nowe aplikacje fintech i handlowe znajdują się teraz na celowniku, co stanowi pozostałe 39% ” - powiedziała firma.

Link: <https://thehackernews.com/2023/12/new-chameleon-android-banking-trojan.html>