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.  
„Reprezentując restrukturyzowaną i ulepszoną iterację swojego poprzednika, ten rozwinięty wariant kameleon wyróżnia się w realizacji przejęcia urządzeń (DTO) przy użyciu usługi dostępności, a jednocześnie rozszerzając swój ukierunkowany region” - powiedziała holenderska firma zajmująca się ochroną mobilną ThreatFabric.  
Chameleon został wcześniej udokumentowany przez Cyble w kwietniu 2023 r., Zauważając, że był używany do wyróżnienia użytkowników w Australii i Polsce od co najmniej stycznia.Podobnie jak inne złośliwe oprogramowanie bankowe, wiadomo, że nadużywa swoich uprawnień do usługi dostępności Androida w celu zebrania wrażliwych danych i przeprowadzania ataków nakładek.  
Rogue aplikacje zawierające wcześniejszą wersję były gospodarzem stron phishingowych i stwierdzono, że podszywa się pod oryginalne instytucje w krajach, takie jak Australian Taxation Office (ATO) i platforma handlu kryptowalutami o nazwie Coinspot, w celu pożyczenia im wiarygodności.  
Najnowsze ustalenia z ThreeadFabric Show, że trojan bankowy jest teraz dostarczany za pośrednictwem Zombinder, gotowego kroplowania-as-usługi (DAAS), który jest sprzedawany innym podmiotom zagrożeniowym i który można wykorzystać do „wiązania” złośliwych ładunkówdo legalnych aplikacji.  
 Nadchodzące seminarium internetowe pokonało zagrożenia związane z AI z Zero Trust - seminarium internetowe dla specjalistów ds. Bezpieczeństwa tradycyjne środki bezpieczeństwa nie zmniejszą go w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.Dołącz teraz  
Chociaż podejrzewano, że oferta została zamknięta na początku tego roku, powtórzyła się w zeszłym miesiącu, możliwości reklamowe w celu ominięcia funkcji „ograniczonych ustawień” w Android w celu zainstalowania złośliwego oprogramowania na urządzeniach i uzyskania dostępu do usługi dostępności.  
Oba złośliwe artefakty dystrybuujące maskaradę kameleon jako przeglądarka internetowa Google Chrome.Ich nazwy pakietów są wymienione poniżej -  
  
Z72645C414CE232F45.Z35AAD4DDE2FF09B48  
com.busy.lady  
  
Godną uwagi cechą ulepszonego wariantu jest jego zdolność do przeprowadzania oszustwa przejęcia urządzeń (DTO), która wykorzystuje usługę dostępności do wykonywania nieautoryzowanych działań w imieniu ofiary.  
  
Ale aby oszukać użytkowników, aby umożliwić ustawienie, złośliwe oprogramowanie sprawdza wersję Androida na zainstalowanym urządzeniu, a jeśli okaże się, że jest Android 13 lub nowszy, zachęca użytkownika do włączenia go.  
„Po otrzymaniu potwierdzenia systemu Androida 13 ograniczonych ustawień na zainfekowanym urządzeniu, trojan bankowy inicjuje ładowanie strony HTML”, wyjaśnił ThreatFabric.„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 z Androidem do zakłócenia operacji biometrycznych docelowego urządzenia poprzez potajemne przejście mechanizmu uwierzytelniania ekranu blokady na PIN, aby umożliwić złośliwemu oprogramowaniu „odblokowanie urządzenia w woli” przy użyciu usługi dostępności.  
  
„Pojawienie się nowego trojana bankowego Chameleon jest kolejnym przykładem wyrafinowanego i adaptacyjnego krajobrazu zagrożenia w ekosystemie Androida” - powiedziała firma.„Ewoluując od wcześniejszej iteracji, ten wariant pokazuje zwiększoną odporność i zaawansowane nowe funkcje”.  
Rozwój pojawia się, gdy Zimperium ujawniło, że 29 rodzin złośliwego oprogramowania - 10 nowych - w ciągu ostatniego roku miało na celu 1800 aplikacji bankowych w 61 krajach.Nowe aktywne rodziny to Nexus, Ojciec chrzestny, Pixpirate, Saderat, Hook, Pixbankbot, Xenomorph V3, Vultur, Brasdex i Goatrat.  
Krajowe kraje USA obejmują USA (109 aplikacji bankowych), Wielka Brytania (48), Włochy (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).  
„Tradycyjne aplikacje bankowe pozostają głównym celem, z oszałamiającymi 1103 aplikacjami - stanowiącym 61% celów - podczas gdy wschodzące aplikacje fintech i handlowe znajdują się teraz w celownikach, co stanowi pozostałe 39%” - powiedziała firma.

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