New Chameleon Android Banking Trojan Variant Bypasses Biometric Authentication

Cybersecurity researchers have discovered an updated version of an Android banking malware called Chameleon that has expanded its targeting to include users in the U.K. and Italy.  
"Representing a restructured and enhanced iteration of its predecessor, this evolved Chameleon variant excels in executing Device Takeover (DTO) using the accessibility service, all while expanding its targeted region," Dutch mobile security firm ThreatFabric said in a report shared with The Hacker News.  
Chameleon was previously documented by Cyble in April 2023, noting that it had been used to single out users in Australia and Poland since at least January. Like other banking malware, it's known to abuse its permissions to Android's accessibility service to harvest sensitive data and conduct overlay attacks.  
The rogue apps were hosted on phishing pages and found to impersonate genuine institutions in the countries, such as the Australian Taxation Office (ATO) and a cryptocurrency trading platform called CoinSpot, in an attempt to lend them a veil of credibility.  
The latest findings from ThreatFabric show that the banking trojan is now being delivered via Zombinder, an off-the-shelf dropper-as-a-service (DaaS) that's sold to other threat actors and which can be used to "bind" malicious payloads to legitimate apps.  
 UPCOMING WEBINAR Beat AI-Powered Threats with Zero Trust - Webinar for Security Professionals Traditional security measures won't cut it in today's world. It's time for Zero Trust Security. Secure your data like never before. Join Now   
Although the offering was suspected to have been shut down earlier this year, it resurfaced last month, advertising capabilities to bypass the 'Restricted Settings' feature in Android to install malware on devices and obtain access to accessibility service.  
Both the malicious artifacts distributing Chameleon masquerade as the Google Chrome web browser. Their package names are listed below -  
  
Z72645c414ce232f45.Z35aad4dde2ff09b48  
com.busy.lady  
  
A notable feature of the enhanced variant is its ability to conduct Device Takeover (DTO) fraud, which leverages the accessibility service to perform unauthorized actions on the victim's behalf.  
  
But in order to trick users into enabling the setting, the malware checks the Android version on the installed device and if it's found to be Android 13 or later, prompts the user to turn it on.  
"Upon receiving confirmation of Android 13 Restricted Settings being present on the infected device, the banking trojan initiates the loading of an HTML page," ThreatFabric explained. "The page is guiding users through a manual step-by-step process to enable the accessibility service on Android 13 and higher."  
Another new addition is the use of Android APIs to disrupt the biometric operations of the targeted device by covertly transitioning the lock screen authentication mechanism to a PIN so as to allow the malware to "unlock the device at will" using the accessibility service.  
  
"The emergence of the new Chameleon banking trojan is another example of the sophisticated and adaptive threat landscape within the Android ecosystem," the company said. "Evolving from its earlier iteration, this variant demonstrates increased resilience and advanced new features."  
The development comes as Zimperium revealed that 29 malware families – 10 of them new – targeted 1,800 banking applications across 61 countries over the past year. The new active families include Nexus, Godfather, PixPirate, Saderat, Hook, PixBankBot, Xenomorph v3, Vultur, BrasDex, and GoatRAT.  
The U.S. top countries targeted comprise the U.S. (109 bank apps), the U.K. (48), Italy (44), Australia (34), Turkey (32), France (30), Spain (29), Portugal (27), Germany (23), Canada (17), and Brazil (11). The most targeted financial services apps are PhonePe (India), WeChat, Bank of America, Well Fargo, (U.S.), Binance (Malta), Barclays (U.K.), QNB Finansbank (Turkey), and CaixaBank (Spain).  
"Traditional banking applications remain the prime target, with a staggering 1103 apps – accounting for 61% of the targets – while the emerging FinTech and Trading apps are now in the crosshairs, making up the remaining 39%," the company said.

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