New ‘Brokewell’ Android Malware Spread through Fake Browser Updates

Date: 28th April 2024 | Severity: Medium

Summary

The Brokewell Android banking Trojan was first reported by cybersecurity researchers in April 2024. The malware targets the users of financial service and digital authentication applications.

Attack Vectors

- Banking trojan, once installed and launched for the first time, prompts the victim to grant permissions to the accessibility service, which it subsequently uses to automatically grant other permissions and carry out various malicious activities.
- This includes displaying overlay screens on top of targeted apps to pilfer user credentials. It can also steal cookies by launching a WebView and loading the legitimate website, after which the session cookies are intercepted and transmitted to an actor-controlled server.
- The threat actors can also leverage the malware’s remote-control functionality to see what’s displayed on screen in real-time, as well as interact with the device through clicks, swipes, and touches.
- Brokewell infects users by masquerading as legitimate Android applications, such as Google Chrome updates or the Klarna financial service. Once executed, the malware uses overlay techniques, displaying fake login screens to steal user credentials.
- It harvests session cookies by launching its own WebView. Brokewell can also capture the victim’s interaction with the device (taps, swipes, information displayed, text input, and applications opened), collect the device information, geolocation, and call history, and record audio.
- Brokewell is said to be the work of a developer who goes by the name “Baron Samedit Marais” and manages the “Brokewell Cyber Labs” project, which also includes an Android Loader publicly hosted on Gitea.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• d807070973bde0d85f260950dc764e46a0ba486f62da3e62f3b229ca3ea322f1 • 00d35cf5af2431179b24002b3a4c7fb115380ebda496d78849bf3d10055d8a88

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/new-brokewell-android-malware-spread.html
- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/662a58b69edcffc72a6461c4