Medusa malware ramps up Android SMS phishing attacks

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** February 7, 2022 11:38 AM **0**

The Medusa Android banking Trojan is seeing increased infection rates [illegible]argets more geographic regions to steal online credentials and

Today, researchers at ThreatFabric have published a new report detailing the latest tricks employed by the Medusa malware and how it continues to evolve with new features.

Medusa on the rise

Medusa (aka TangleBot) is not a novel banking trojan, but it has seen increased distribution, with campaigns now targeting North America and Europe using the same distribution service as the notorious FluBot malware.

BleepingComputer previously reported that the Medusa and FluBot trojans had previously used (https://www.bleepingcomputer.com/news/security/android-spyware-spreading-as-antivirus-software-in-japan/) 'duckdns.org,' a free dynamic DNS abused as a delivery mechanism, so this is not the first sign of overlap between the two.

"The samples seen in side-by-side campaigns with Cabassous are identified by the actors themselves with the tags FLUVOICE, FLUFLASH and FLUDHL (possibly as a reference to the corresponding Cabassous/Flubot campaigns)," ThreatFabric explains in their report (https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html#medusa-turkish-delight-with-dangerous-filling).

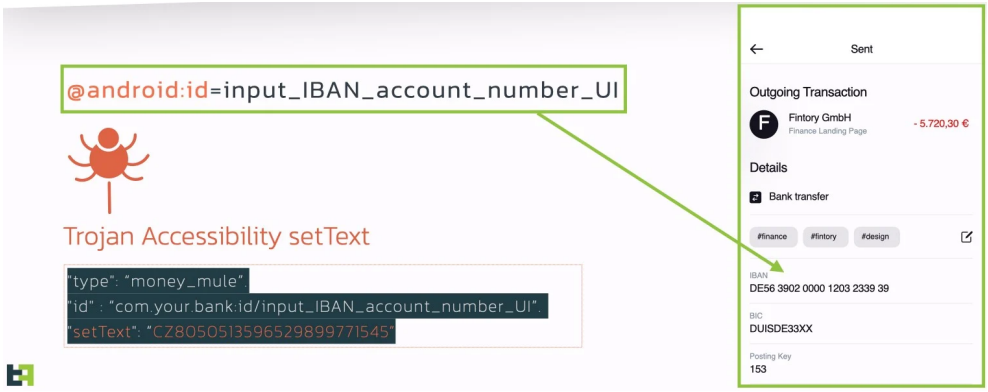
The researchers believe that the Medusa threat actors began using this distribution service after seeing how widely spread and successful FluBot's campaigns had become.

Medusa's main strength lies in its abuse of the Android 'Accessibility' scripting engine, which enables actors to perform various actions as if they were the user.

These actions are:

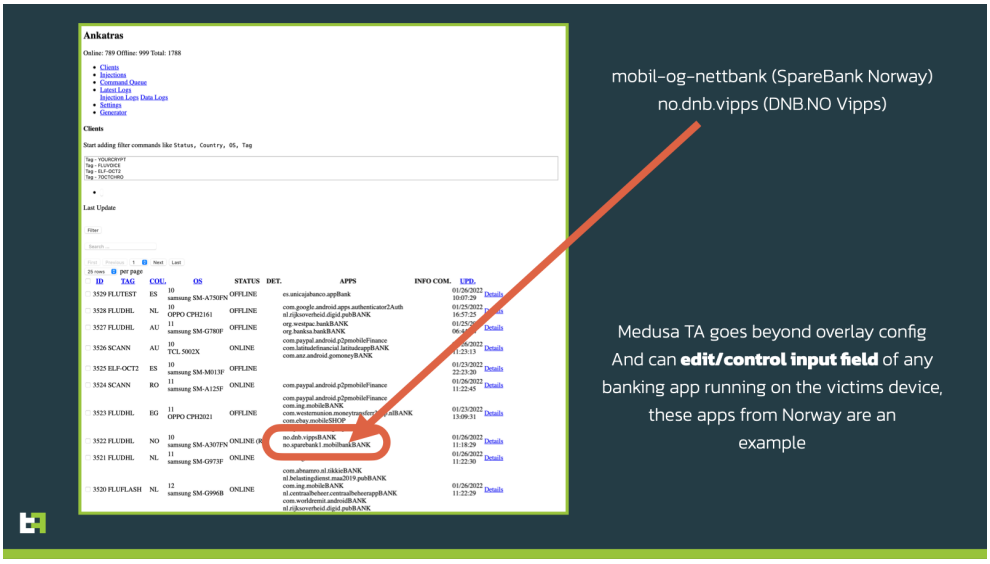
- **home_key** – Performs HOME global action
- **ges** – Executes a specified gesture on the screen of the device
- **fid_click** – Clicks on the UI element with the specified ID
- **sleep** – Sleeps (waits) for the specified number of microseconds
- **recent_key** – Shows overview of the recent apps
- **scrshot_key** – Performs TAKE_SCREENSHOT global action
- **notification_key** – Opens the active notifications
- **lock_key** – Locks the screen
- **back_key** – Performs BACK global action
- **text_click** – Clicks on the UI element that has specified text displayed
- **fill_text** – Not implemented yet

All in all, it's a highly capable banking trojan with keylogging features, live audio and video streaming, remote command execution options, and more.



Manual input field changing
Source: ThreatFabric

ThreatFabric was able to gain access to the malware's backend administration panel and found that its operators can edit any field on any banking app running on the device. This feature allows the malware to target almost any banking platform with fake phishing login forms to steal credentials.



Source: ThreatFabric

The malware is commonly distributed spoofed DHL or Purolator apps, but the researchers also saw packages masquerading as Android Update, Flash Player, Amazon Locker, and Video Player.

Fake DHL APKs containing Medusa or Flubot (Cabassous)

Source: ThreatFabric

These APKs are manually installed by the victims themselves, who receive an SMS message with a URL leading to a site pushing the malicious Android app.

To prevent being infected by these malware infections, always treat strange URLs sent from your contact list as untrustworthy as they may have been sent by malware on the senders' device.

As always, do not, under any circumstance, download APKs from unknown websites, as they invariably lead to malware infections.

Related Articles:

Roaming Mantis Android malware campaign sets sights on Europe (https://www.bleepingcomputer.com/news/security/roaming-mantis-android-malware-campaign-sets-sights-on-europe/)

FluBot malware now targets Europe posing as Flash Player app (https://www.bleepingcomputer.com/news/security/flubot-malware-now-targets-europe-posing-as-flash-player-app/)

Chaes banking trojan hijacks Chrome with malicious extensions (https://www.bleepingcomputer.com/news/security/chaes-banking-trojan-hijacks-chrome-with-malicious-extensions/)

New FluBot and TeaBot campaigns target Android devices worldwide (https://www.bleepingcomputer.com/news/security/new-flubot-and-teabot-campaigns-target-android-devices-worldwide/)

Android banking trojan spreads via fake Google Play Store page (https://www.bleepingcomputer.com/news/security/android-banking-trojan-spreads-via-fake-google-play-store-page/)