Ginp - A malware patchwork borrowing from Anubis

Published: 2024-10-01 · Archived: 2026-04-05 17:57:01 UTC

Intro

ThreatFabric analysts have recently investigated an interesting new strain of banking malware. The malware was first spotted by Tatyana Shishkova from Kaspersky by end October 2019, but actually dates back to June 2019. It is still under active development, with at least 5 different versions of the Trojan released within the last 5 months (June - November 2019).

What makes Ginp stand out is that it was built from scratch being expanded through regular updates, the last of which including code copied from the infamous Anubis banking Trojan, indicating that its author is cherry-picking the most relevant functionality for its malware. In addition, its original target list is extremely narrow and seems to be focused on Spanish banks. Last but not least, all the overlay screens (injects) for the banks include two steps; first stealing the victim's login credentials, then their credit card details. Although multi-step overlays are not something new, their usage is generally limited to avoid raising suspicion.

Evolution

The initial version of the malware dates back to early June 2019, masquerading as a "Google Play Verificator" app. At that time, Ginp was a simple SMS stealer whose purpose was only to send a copy of incoming and outgoing SMS messages to the C2 server.

A couple of months later, in August 2019, a new version was released with additional banking-specific features. This and following versions were masquerading as fake "Adobe Flash Player" apps. The malware was able to perform overlay attacks and become the default SMS app through the abuse of the Accessibility Service. The overlay consisted of a generic credit card grabber targeting social and utility apps, such as Google Play, Facebook, WhatsApp, Chrome, Skype, Instagram and Twitter.

Although early versions had some basic code and string obfuscation, protection of the third version of the malware was enhanced with the use of payload obfuscation. The capabilities remained unchanged, but a new endpoint was added to the Trojan C2 allowing it to handle the generic card grabber overlay and specific target overlays (banking apps) separately. In addition, the credit card grabber target list was expanded with Snapchat and Viber.

In the third version spotted in the wild, the author introduced parts of the source code of the infamous Anubis Trojan (which was leaked earlier in 2019). This change came hand in hand with a new overlay target list, no longer targeting social apps, but focusing on banking instead. A remarkable fact is that all the targeted apps relate to Spanish banks, including targets never seen before in any other Android banking Trojan. The 24 target apps belong to 7 different Spanish banks: Caixa bank, Bankinter, Bankia, BBVA, EVO Banco, Kutxabank and Santander. The specific apps can be found in the target list in the appendix.

The most recent version of Ginp (at the time of writing) was detected at the end of November 2019. This version has some small modifications which seems to be unused, as the malware behaviour is the same as the previous version. The author has introduced the capability to grant the app the device admin permission. Additionally new endpoint was added that seems related to downloading a module for the malware, probably with new features or configuration.

How it works

When the malware is first started on the device it will begin by removing its icon from the app drawer, hiding from the end user. In the second step it asks the victim for the Accessibility Service privilege as visible in following screenshot:
