The Tale of the Pija-Droid Firefinch

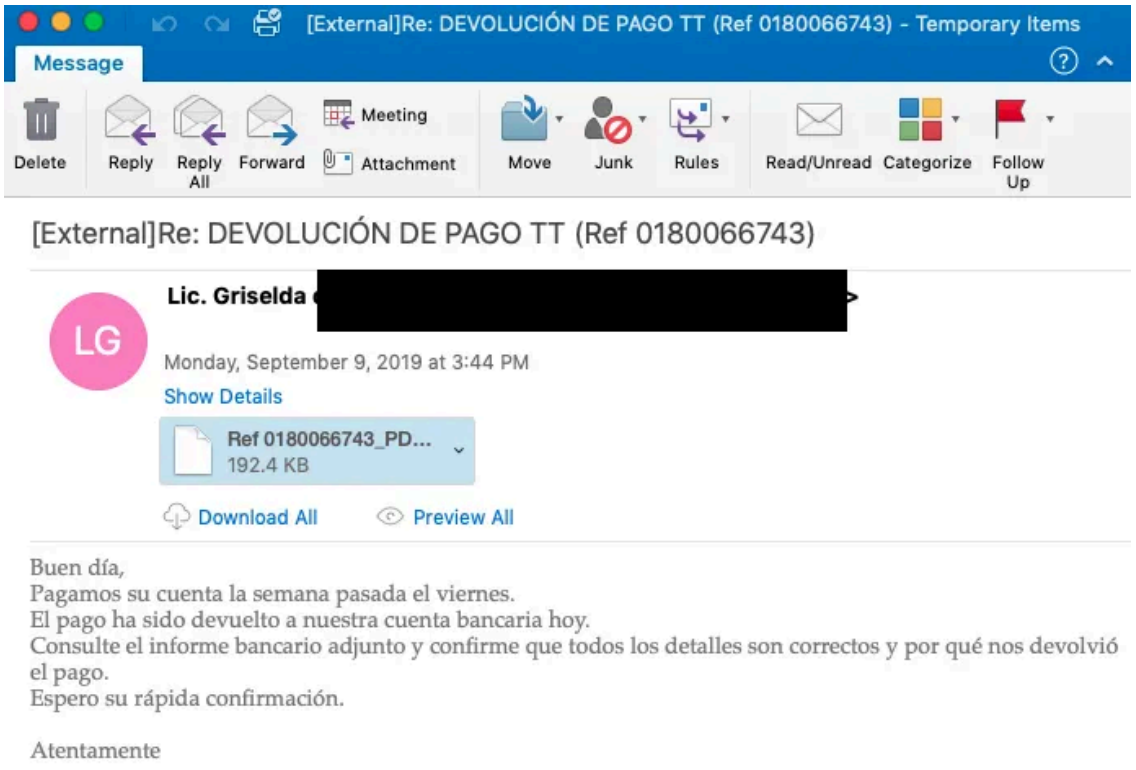
By Paul Burbage

Published: 2019-12-27 · Archived: 2026-04-05 14:31:05 UTC

From the illuminating malware adversaries series.

One thing that I've learned from investigating malware adversaries for over a decade is that they enjoy reusing nicknames. An adversary that I have been tracking since February 2019 likes to use the moniker "Droid" in their Lokibot command-and-control (C2) addresses. So begins the story of the "Pija-Droid Firefinch".

The Pija-Droid Firefinch is a frequent flyer of **Lokibot** malware — an infostealer once marketed in Russian underground forums but nowadays freely available by any ne'er-do-wells brazen enough to infect computers. It appears that this malware actor mainly targets Spanish speaking communities based on language used in their malspam lures. The malicious email attachments are usually obscure file archive formats, perhaps utilized to circumvent AV scanners.



Typical malicious email containing Spanish language.

At MalBeacon.com, we beacon malware adversaries while they are administering botnets, revealing quite a bit of information on attackers. We derived this adversary's name using the following paradigm:

Pija = The Spanish word for “prick”. Spanish is also the preferred malspam language used by the attacker.
Droid = Our adversary’s moniker and a common directory found in their C2 URLs.
Firefinch = A bird native to Nigeria and our attacker’s location.
