The Tale of the Pija-Droid Firefinch

medium.com/@paul.k.burbage/the-tale-of-the-pija-droid-firefinch-4d304fde5ca2

Paul Burbage December 27, 2019

Paul Burbage

Dec 27, 2019

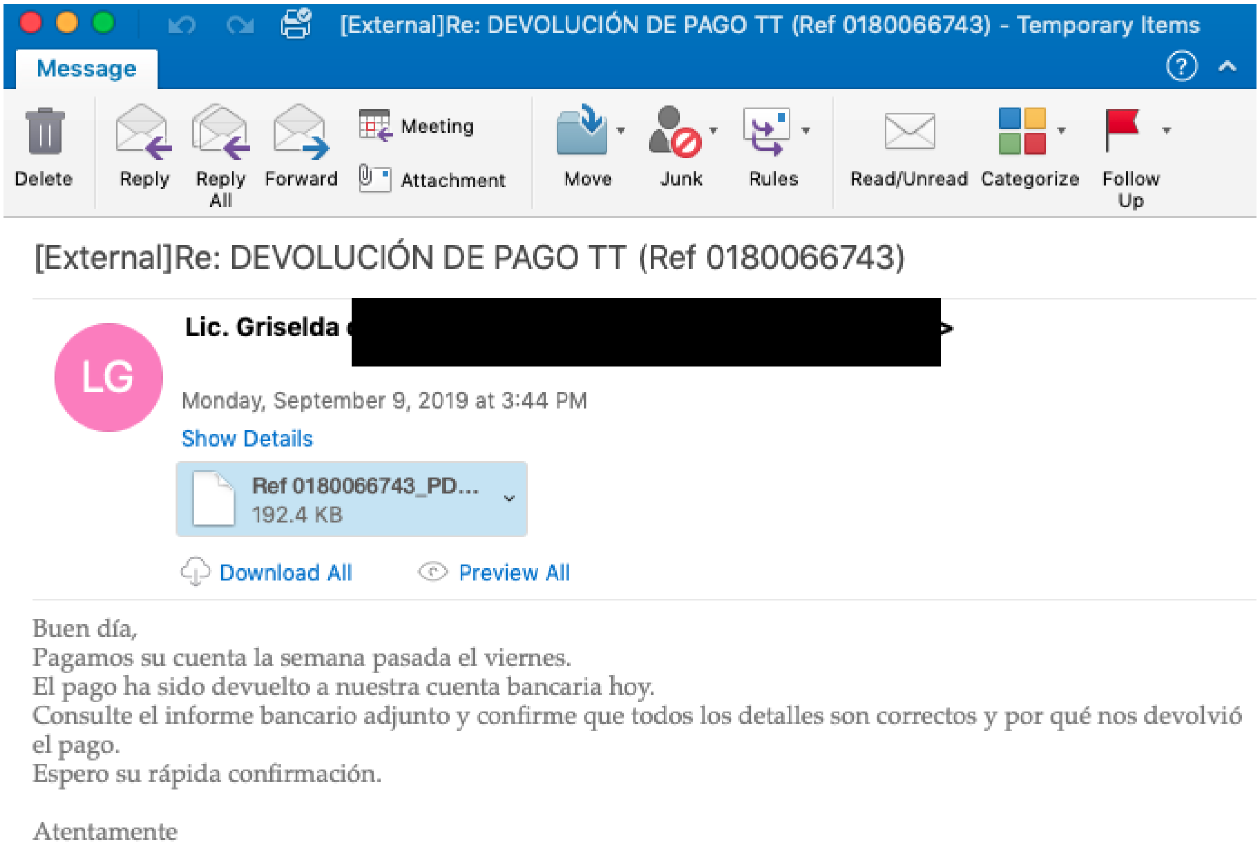
·

2 min read

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.



[External]Re: DEVOLUCIÓN DE PAGO TT (Ref 0180066743)

LG

Lic. Griselda [redacted]

Monday, September 9, 2019 at 3:44 PM

Ref 0180066743_PD...
192.4 KB

Buen día,
Pagamos su cuenta la semana pasada el viernes.
El pago ha sido devuelto a nuestra cuenta bancaria hoy.
Consulte el informe bancario adjunto y confirme que todos los detalles son correctos y por qué nos devolvió el pago.
Espero su rápida confirmación.

Atentamente

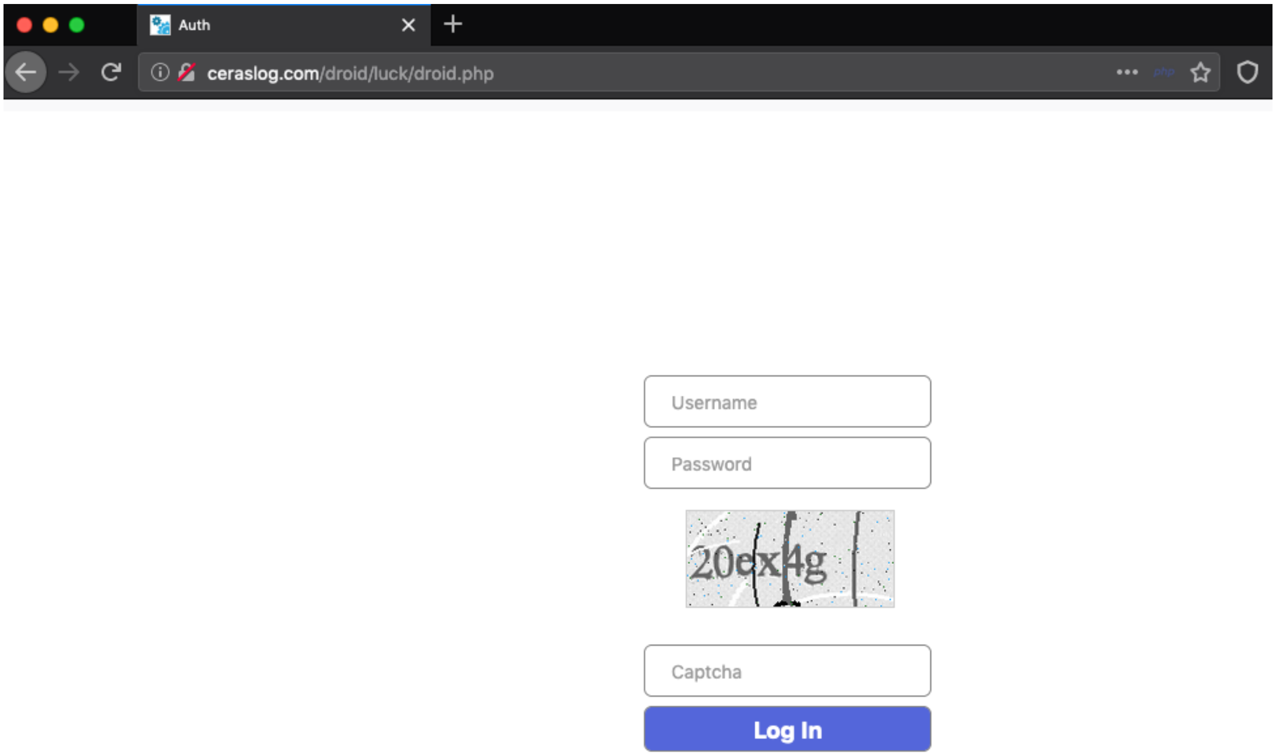
Typical malicious email containing Spanish language.
At MalBeacon.com, we beacon malware adversaries while they are administering botnets, revealing quite a bit of information on attackers. We derived this adversary's name using the following paradigm:

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.

MalBeacon Attribution Intelligence

Beacons indicate that this adversary uses a Windows 10 64 bit Operating System and prefers the Chrome browser when administering their botnet. Based on source IP addresses captured in MalBeacon and enriched in Comox, we can ascertain that this actor is based in Kuje, Nigeria. This actor seems to at times also use TunnelBear VPN software to mask their location. Researchers with access to MalBeacon can track this actor via the tag "pija2pnirb5s17824soa7j7oc3".

The actor is currently using the Lokibot C2 at:
hxxp://ceraslog[.]com/droid/luck/droid.php



The current Lokibot C2 admin login screen used by this adversary.

Lokibot C2 Admin URLs used by this adversary:

hXXp://ceraslog[.]com/droid/luck/droid.php
hXXp://ebdro[.]website/yteu/hff/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://www.pricknpuss[.]website/eby/iop/rt/wer/dj/hid/jkdk/nsijf/nbdfif/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://www.4ku[.]wtf/droid/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://www.loider[.]asia/droid/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://www.botkill[.]asia/droid/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://layol[.]club/droid/five/PvqDq929BSx_A_D_M1n_a.php
hXXps://www.forek[.]asia/droid/Panel/PvqDq929BSx_A_D_M1n_a.php
hXXp://shinican-com[.]tk/droid/five/PvqDq929BSx_A_D_M1n_a.php
hXXp://ccloneforty[.]com/droid/five/PvqDq929BSx_A_D_M1n_a.php

Indicators of Compromise (SHA256)

```
0043f5ca4a46823af3542c5ac95371c6c9c4a01e83d4bef9c8e3a36ec1bf3498
00aad8d16cfbd660318d6e20cb265ff083c1257f38aa6768bf4c4a658c764423
0d7085765464873df26536ee39c324a4e335c97b6308e80f7cb2ffa07e4c6fa5
0ff4de59d91253519bbdabb7a065530a8c3387a191dd666a44dd559e388d7343
11814efcaaba2ec462f1089fda3fbf225fde9edd9786453a11831bda3b7a5a12
14a9714bffe73d3c84876cd2d56539208ccb8ea66dea94e93d65fdc0d170c77c
1b27ecca734a5860a537e25ec025fb949f9b1100fa28d830cb821ed7105e9e7e
1cf3d28a15e45d1a802b04ec0fe74c22747a83f2cb72a0e1a00404192630fb15
232517ade42a92bfd2d00b15c1e59a1f1faf63d2df0cf3534f1566e589638ce4
240fddca13fa1d2567a9e36fe593608d4189f747f128451f843c03a20e38e3d0
2665ef458e4b2cad69e73f2f479a62c83fc1ebb88efba88af3da578d1e5c25f4
2a937cf6b90d4acaa1a7e3ee80bfab552fea34d947c6b3ae9f9f8ba3b3eaa271
2afeecedec480c0ad712a2af0e85967c480735de39758aed220d56a52320f993
3047df68205bff5d71a94d96de2be5813f437990a7b335c81a43b74953eaedb0
3275f6c72c4ef644f54525a823641e0627baf6276a4c44cc1f636903689d2cb6
34bccb20d722f16f8e0beb2067d57903c67ba903b254b07b923a2997aee2a5d6
362763ef9b5d5819e56ecb2c59e7012d8b68d848ccefd3aa4ac0083209f48df0
39e0f4aa3105bd890e3e881699c1d465e2cbd0bb25cbad93a268eebcb5a31ef3
3e5c1b4e262edaf5519c8868371e9d40ba9e5c53000f20a304717bc836cca106
434fe7457fc30a3fa0a1d02783ca87758ca4168cf77d577b0977e7f85417c2b0
4360f8e5bc2c553303c945fbe41512b22e74b8a73bf231ca148700383bf8b4b5
459888b5d39b3383b7dcc28e3708419247d05932d6727317f71b556e08e25146
47fc733d045215367e55c033926c8ebf7ccaa70de65ed9c1175e2e7e45bb688d
499ee4fa0baa4ab69af45b8d873f39d952b2c297f74611c7853b714bd64d5396
4ad53f1c33c4b03e7641a110a6369ae8690ac8ab279c7493744ff11a51462f2a
4d9437684c3931d89a6061b6546ad346c610df634e2c724107d1c982951ad890
4e4ab09a743c3546fb2bb593e120adc565855195227b6418c455a5febada5d59
4e545b2b8c24c54bc995358ad8a7d7fb3947b6e934aed9283f81d72423fcbf5f
4f89855df9703cedbbb838ba7514d4231adb5e5c5b156ec3611eb1abeabe73af
577b5fe65bf87041d37924c28fc9d56563ae7228098cf1dc0cd7e1c645d223b0
5b64f0fbbaad1956c5706e4d258ed1464265704aebc8584116b447cde07990f3
629d22dae05f6b3ae5a60bab42d01869778bae06c18f05370fcccc9a326b1b8a
685856c81793497e40a6aa2ef3ebf4b28875e1832034fdbea7877ac20e9d8662
6977c44579162e2baa1b5d09d5081b917a9201ce7d60b31a37b395a90c118375
720e3427dfadb672905b964c16545c11d25cec4448e74ed227c3235dae26452b
756b135dd77c66a04c6168469f79db53dfe0a66872f84e46bca8a4254bdca0a3
759f962fa803f47bdefded199db215b277e07085b33617cdcc4d119364f44cb6
75e370ff4264717e567afec35762420aa8a1f05dfc996b3cee5f141b1ceedef7
7a47ca97c5dc9999f5b03a5b95a26a647636cf06fa2a3efb9a9223a30098edf7
7a8c32bf14c7635fe32ae623799d2d06480109febff1138e86e677897e798cea
8173917e7132ed1348a9d6a5fea3561605175a2e045c4326211b42df54f435ae
87ff2c79088fc998dcdd5880bdce133239aca5aca03152afb7a7abf621b53920
88613a050c82915d7320fa31a3a088a32ce3e0fe7eba50b27c6099bf8a99d6c4
8a34e21916780732b486ef0afc97e1a5e9f698da8a277071b923d78c55e60d6e
8c8fd26b1af69801f3ae5e96d6bcff4a3f839d704d3b9113a636d45d7b804bbc
8e44a9f77507cad9b0a2de5c9187644342f72e2e8ac289de26d13587e905ece6
9746c1c179e4287f09dc8f5e1bc0fbbf69e14f5acf734e7c6ac8a78d6a000b58
```

```
97853f50eec181948f77569bd1561dc643be4f02a834491947abd087b2ded40b
9ae13a6f8779b6d1e00d1c4182fff0b77c384f6a0ec16bccb6abbaedafd9adc6
9c2ce445b8ca7f4e13887f6dca0d263e8f015849ca12bf70c505c2beb9c96260
9c472a1cc1da194394702daef4b067898b113718a014b69ee558a1866dccbc49
9c4c156cf2ce58e5ab251d55e69b02a9b5efe461a2811b63c86504e608590b38
9f0f090995c6a65e557f4c876f3bd553383ed6053b707944c9916fe5069695e4
9f3b785dd8658fee11fd41904ef7fcec5bbcb17735f93092b683a0b67f32c905
a27b91fc840a1951b89dbb74112f98cc8b9a84bfbbc248ea461234c70c5a8210
a80551fc478bc4b2551d5d7b3ad8472005f7b1b7e5c3e5061b83c5f0efe1e3d6
acf57c992f09e871910529f05cfac9174101dd97edee96d31c76ca8de8a65a91
ad0b6f3f5d023aef90443aada57f4108c16bef6f08c9feea0d77dae93dcd8cae
b0eb1044c8a010429954acdc9fd525d59ccf45de8bfb3a6264ba72f63a420047
b2c6f30ae6e965eb7c27b9788ae894ec070887c985534a2ca62e220e01dc5600
b79c026b5204357412c1b35ef60800a7de693f6f99e36857d39111f0791f4831
b8453e39884796df95bce782057f53d2f48f6a898fb9629d804fca2003fc5e76
bd27666f9c54a424fb6536307a5cc8abd4d63baf016630f766727fafdde75a56
cb3a23752fc8531d9176f0c604952dbccce19753d590b433c545c2aa37cca074
cf03b352eacb8a639e486b680c73d912186775734bd298727e27498a75c56b7c
d3b7c954fa844c97005c645d2ec35ef9095875e1900f97dce25695fdf36ca7c3
d5e2822a4b24de3e07d1218beb7459248aa55eb87541b5b146fe6f6e4658447f
db3036805f9a6853f9110529c4f579ca77b49dbd868f6c4c74073e9711d84186
e39cc7043d80cb695c4317bb1b81872ea24f322f9bbde2b90aa9941f516b4246
ebab97bcebd45d84306b1b9e4d8cf23c624f7259a5aef39b5cf7929d81f28e0d
ebd8b770d20aad3f6d64986c1da6e5ee56f358e1d995bad520c779b8354cceb4
f03bf2e44be15864979b9ff5e6c76ca6c981b32a28af4d171ed17f49e330cc54
f080fc7dfd4adea68e3e40d1de6cef1fa7b027d56b393c658c633dfac936d4bd
f0cebdbc95fb3905ce2625542ed890a3d8b0b7dfdfd466176c1729e9f18dc536
f487ee1cba84db7c95f14a6e60cde89b6a3f02f3f7402d7cc40d0e3727930b5b
f6147a2d4337c768797ff828bffde6474cee9219b01e6749080f1c2c6bee4a33
f9900639f429246816188889e4ebd25986729c9bc19303201cbdc6cbf947c1ab
fb31b8db39898f91047d094d00f4d1b2dc9cdc88edfd3b65fb2dbb11774f06f4
87282a3b391f65a2d0f554e45b48a06b1cf0b8be721d488e6410669342d390bf
98eb0692b796ac0d5dc763bb0af2ed4ed4a820d3d95f027f8c55cc5a32f090e1
cfa7d63eb0f70f0938f15acbab1d08a2f32df7332ca6601c3c2cff21861d90df
6f3fd35f1da12cfc3e4e9c0a3a0a90ff93a033175fe93d01cb957ed38f8594a9
da68b6c865d3adea4a7a5656cbb85ce4866edd492dce22e61ee7516d012064a1
8008a8bc04360de923f469ef67d59b397c6f3e61af6ad7b1df2cbb11fb6666b6
282ce86ad7a47775e94213715aca8b6cb812b1b3308c0bdcff94eb8f7f3f5c28
f0eaa8e3e4f7228e4532dc65cc5d707165ec36f9d02c6e2e5c73cf5ea317a8c8
bfabb027d7cac6f2660dcbff2284769e539da2ec15d7f3f807f5b77ed643508b
e49383ce48b70513b62d28a772a0b53be9d0e4bf4e9e24bc6ffc0374c1f4a9d6
4a1060acaafabe0df9fb41003a810fbe02c1832bea3712dc6cf502985a86d57a
546f44da14f0ba3f9c596b859228d6516009abc3a5e6abfbecf1af281c830bb4
a8ecc3adf1be445d6d45438b2eb1e7259ec2fe8cd625b5b64def18c0b2be44be
10f014c0c2b1555c69c3b1f2f4997cea5a3995db018d1fddc6a89c6657086d5b
10f014c0c2b1555c69c3b1f2f4997cea5a3995db018d1fddc6a89c6657086d5b
4db4803af2045f028ae2f55c3a10de627f8ed8307d3e9c8aa6d4e0b3ffc8ed5d
```

> a8ecc3adf1be445d6d45438b2eb1e7259ec2fe8cd625b5b64def18c0b2be44be
> 2651541eaf14d22b00651d480f5599a9a2f03321795b5af4f64635606e1b268d
> c04979a234e729c9ffaf92fda55623408b4a3ad4bc0ade601806368557818776
> 1f99b6353b6d6e86bbf93ea30c14494e59db26d770125220d0aa0be7b25b3b08