#ShortAndMalicious — PikaBot and the Matanbuchus connection

medium.com/@DCSO_CyTec/shortandmalicious-pikabot-and-the-matanbuchus-connection-5e302644398

DCSO CyTec Blog February 11, 2023

DCSO CyTec Blog

Feb 10

.

3 min read

Photo by on

Continuing our #ShortAndMalicious series, where we aim to briefly highlight new or otherwise noteworthy malware, a tweet by Unit 42 Intel caught our attention early February 2023:

Thank you Unit 42 for sharing!

Having covered Matanbuchus before, DCSO CyTec jumped in to investigate this new sample, which quickly turned out to be a new malware family instead.

Twitter user Germán Fernández then identified it as “PikaBot/iPikaBot” so we set out to see what’s under the hood.

Blog post authored by and .

What we know

In short, here’s what we know after analyzing the new PikaBot sample:

- It is it was distributed similarly to Qakbot — thank you for pointing out the misunderstanding!)
- It’s a , so the purpose is mainly fetching additional malware (for now)
- It’s split into a loader and a core component
- It features a heavy amount of anti-debug functions… we stopped naming them after identifying the 20th anti-debug function, and it contains some anti-VM functionality in addition
- Traffic consists of exchanging , with the payload encrypted using Base64+AES-CBC
- A lot of configuration is hardcoded (C2 servers, request paths)
- It excludes based on the configured language ID of the infected system

Initial POSTs to the hardcoded C2 feature the following decrypted payload:

```
{    "uuid": "542F70A6000008AC43698032133",    "stream":
"bb_d2@T@dd48940b389148069ffc1db3f2f38c0e",    "os_version": "Win 10.0 19045",
"product_number": 48,    "username": "batman",    "pc_name": "DESKTOP-BATCAVE",
"cpu_name": "Intel(R) Xeon(R) CPU E3-1505M v6 @ 3.00GHz",    "arch": "x86",
"pc_uptime": 1994593,    "gpu_name": "VMware SVGA 3D",    "ram_amount": 4095,
"screen_resolution": "1567x904",    "version": "0.1.7",    "av_software": "unknown",
"domain_name": "",    "domain_controller_name": "unknown",
"domain_controller_address": "unknown"}
```

Noteworthy is the version number reported as **0.1.7** so the malware appears to be in the very early stages of development.

Analysis is still ongoing but commands we have identified so far are as follows:

```
cmd                Run shell commandexe                Fetch and run EXEdll
Fetch and run DLLshellcode          Run shellcodeadditional         Send additional
system info (?)knock_timeout      Change C2 check-in intervaldestroy            Not
implemented yet
```

New devil or new clothes?

Regarding the Matanbuchus connection — without further hard evidence we can’t assess a possible relationship between both malware families.

PikaBot is definitely a new malware family in the early stages of development. Based on previous research of Matanbuchus we’ve noticed some similiarities however:

- Both malware families are written in C/C++
- Both malware families utilize a clear loader/core component split
- Both malware families utilize JSON+Base64+crypto (Matanbuchus: RC4, PikaBot: AES-CBC) for traffic
- Both malware families extensively use hardcoded strings instead of some sort of configuration blob

which might hint towards a possible connection of both malware families.

IoCs

```
SHA256c666aeb7ed75e58b645a2a4d1bc8c9d0a0a076a8a459e33c6dc60d12f4fa0c01
Loader59f42ecde152f78731e54ea27e761bba748c9309a6ad1c2fd17f0e8b90f8aed1    Core
```