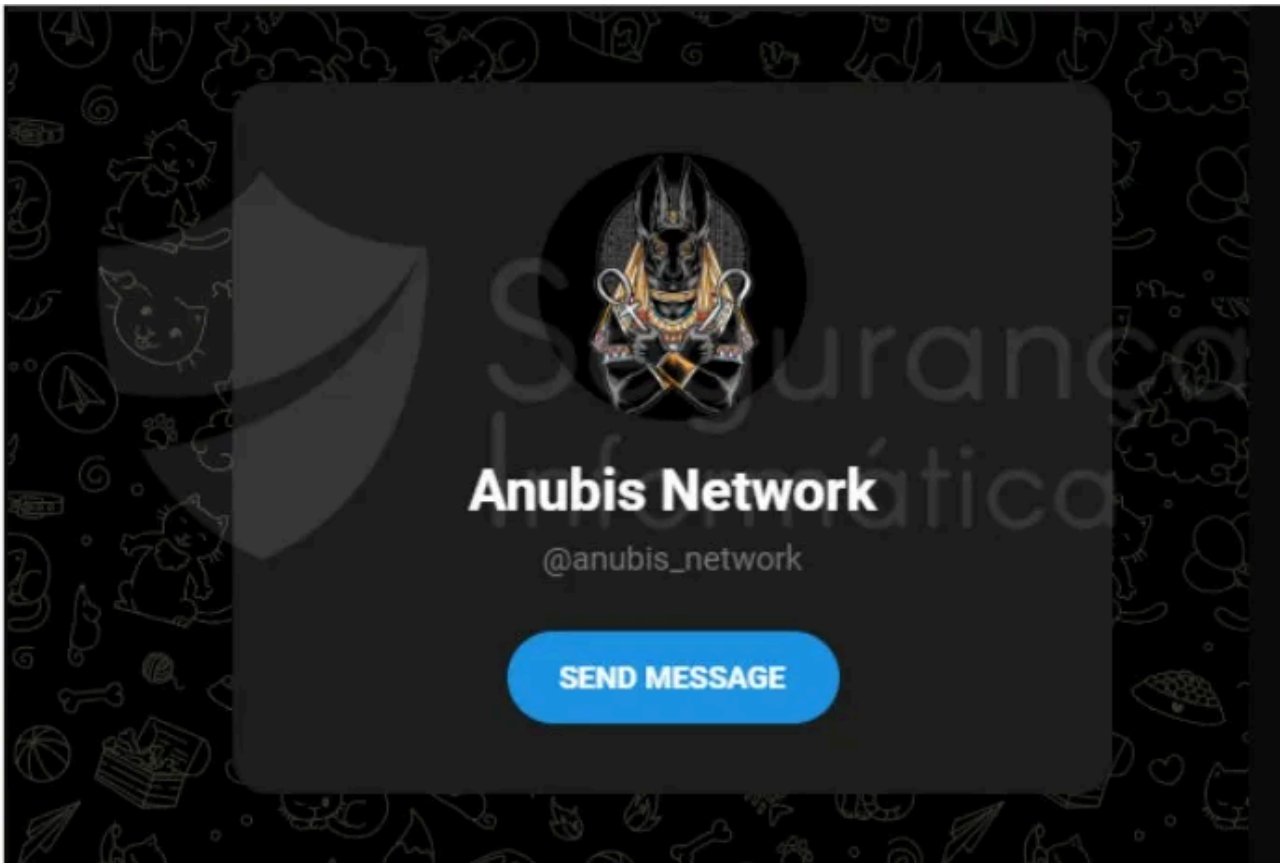
Anubis Networks is back with new C2 server

By Pierluigi Paganini

Published: 2022-07-11 · Archived: 2026-04-05 23:03:22 UTC



A large-scale phishing campaign leveraging the Anubis Network is targeting Brazil and Portugal since March 2022.

A large-scale phishing campaign is targeting Internet-end users in Brazil and Portugal since March 2022. Anubis Network is a C2 portal developed to control fake portals and aims to steal credentials to fully access the real systems.

This C2 server is controlled by a group of operators that come from the previous analysis in 2022, the various brands being divided among the operators of the group (in a call center *modus operandi*).

This campaign is **highlighted by Segurança Informática in 2020**, and the high-level diagram of this new campaign can be observed below.

Figure 1: *High-level diagram of the ANUBIS phishing network and its components (2020).*

In detail, this fresh campaign is composed of three crucial operating components:

- **the delivery vehicle to propagate the landing page in the wild; usually carried out through smishing (SMS) and phishing (email)**
- **a malicious landing page hosted on a cloud server, composed of a user interface and layout very similar to the real system**
- **an operation back-end that allows criminals to manage the details of users who have fallen into the trap.**

Figure 2 presents an example of an SMS sent to Internet end-users during the ANUBIS social engineering wave. The image is related to an ongoing campaign in Portugal impersonating a specific organization to steal banking credentials.

Figure 2: *Example of SMS sent during the social engineering wave.*

SMSs are sent based on a list created by the C2 owner, namely: **1kk-rusha-01.txt**.

Fake domains hosted automatically on Cloudflare CDN

The ANUBIS network phishing campaigns are masked through the Cloudflare CDN. Operators can easily make this configuration through an interface that uses the CloudFlare API for configuring new DNS zones.

Figure 3: *Feature of adding new domains and configuring them behind the Cloudflare CDN via the ANUBIS back office portal.*

The Phishing template

One of the last campaigns disseminated by criminals is impersonating a popular service in Portugal with the goal of stealing credentials of home banking portals.

After clicking on the link distributed via smishing, the victims are redirected to a specific landing page that collects the mobile phone number and the associated code (PIN). As observed, criminals are using the Let's Encrypt CA to create valid HTTPs certificates.

Figure 4: *Phishing template of ANUBIS Network campaign.*

After clicking on "**CONTINUAR**", a new page is presented. Additional data from the victim are requested by the server-side and added to session cookies.

Figure 5: *Additional details about the victims are stored on the session cookies.*

As observed, 12 target banks operating in Portugal are listed in this specific campaign.

Figure 6: *Target banks present on the Anubis Network campaign in Portugal.*

In the next step, credentials to access the target portals are requested.

Figure 7: *Credentials to access the real systems are requested.*

Additional details related to credit cards are also requested by criminals. A specific loading page is then presented, and ANUBIS operators can request other details via the C2 portal in a call center *modus operandi*.

Figure 8: *Additional information requested by criminals.*

Anubis Network C2 Panel

By analyzing the landing page source code, the URL of the C2 server can be obtained.

Figure 9: *Endpoint of the Anubis Network C2 server present on the source code.*

As observed, the C2 login page is linked to a legitimate system in order to confuse threat analysts.

Figure 10: *Login page of Anubis Network C2 server.*

The features observed inside the C2 server are very similar to the analysis performed in 2020. Operators can control all the infection flow by requesting additional details and accessing the real system in the background.

Figure 10: *Internal pages where Anubis Network operators can control all the malicious flow.*

In detail, global administrators are capable of adding users to specific target organizations as observed below.

Figure 11: *Anubis Network operators and permissions page with the target organizations.*

According to the MySQL database that supports the system, there are 77 operators in the system – which represents the business and operational volume of this malicious scheme.

- admin@anubisnetwork.com
- amigoquatro@anubisnetwork.com
- amigorusha@anubisnetwork.com.br
- amigowscincor@anubisnetwork.com
- amigowsdois@anubisnetwork.com.br
- amigowsum@anubisnetwork.com.br
- anubis@anubisnetwork.com
- aprendiz@anubisnetwork.net
- azzouzmarzuk@anubisnetwork.net
- banzeiro@anubisnetwork.net
- batman@anubisnetwork.com
- bicudo@anubisnetwork.com
- bigj@anubisnetwork.net
- Bk_Delas@anubisnetwork.com
- buchuda@anubisnetwork.net
- ceiffador@networkanubis.online
- dimitri@anubisnetwork.com
- dk@anubisnetwork.com
- el@anubisnetwork.com
- elpablito@anubisnetwork.net
- estranho@anubisnetwork.one
- fezon@anubisnetwork.com
- frost@anubisnetwork.com
- fugitivo@network.com.br
- gringo@anubisnetwork.net
- ice@anubisnetwork.com
- jreis@anubisnetwork.com
- junim@anubisnetwork.com
- katatal@anubisnetwork.com
- kingg@anubisnetwork.com
- klebinho@anubisnetwork.com
- knabzdg@anubisnetwork.com
- lbooy@anubisnetwork.com
- leffzera@anubisnetwork.com.br
- lobinho@anubisnetwork.net
- lordk@anubisnetwork.com
- magao@anubisnetwork.com
- malware@anubisnetwork.com
- mandrake@anubisnetwork.com
- maxter@anubisnetwork.one
- mirror@anubisnetwork.com
- mk@anubisnetwork.com

- netota@anubisnetwork.com
- nivel3@anubisnetwork.com
- operador@anubisnetwork.com
- papoko@networkanubis.online
- plasma@anubisnetwork.com
- poke@anubisnetwork.com
- pppp@anubisnetwork.com.br
- ppppe@anubisnetwork.com
- professor@anubisnetwork.com.br
- r0bust0@anubisnetwork.com
- redir@redir.com
- reynan@anubisnetwork.com.br
- ricaria@anubisnetwork.com
- rk@anubisnetwork.com
- rodrigues@anubisnetwork.net
- rushador@anubisnetwork.com
- rushadorr@anubisnetwork.com
- savior@anubisnetwork.com.br
- shao@anubisnetwork.com.br
- skull@anubisnetwork.com
- skulll@anubisnetwork.com
- stealth@anubisnetwork.com
- stealth@anubisnetwork.net
- sujo@anubisnetwork.net
- tiocris@anubisnetwork.com
- trakino@anubisnetwork.com
- traks@anubisnetwork.com
- velhodick@anubisnetwork.net
- will@anunisnetwork.com
- ws@anubisnetwork.com.br
- wyzgoi@anubisnetwork.net
- x0rg@anubisnetwork.com
- xinxa@anubisnetwork.com
- zeus@anubisnetwork.net
- zezinho@anubisnetwork.com

An interesting feature also implemented in this new version of the C2 portal is the **email temp**. By using this feature, criminals can create new domains and use internal emails to manage all the processes.

Figure 12: *Anubis Network email temp feature.*

The landing pages presented to the victims and specific data can be configured on the Anubis Network administrative portal. The path of the folder and the target brand can be observed on this specific page.

Figure 13: *Target organizations of Anubis Network C2 server – Jully 2022.*

Since the malicious network is made up of many people, a channel on Telegram was created in order to provide technical support to operators in the performance of their duties.

Figure 14: *Telegram channel created as a technical support channel.*

The MySQL database

The heart of the ANUBIS network is a MySQL database. This database is used for data synchronization between all components of the malicious ecosystem and maintains everything up-to-date each second.

Figure 15: *Database schema of the ANUBIS phishing network.*

Additional details, including final thoughts and Indicators of Compromise (IoCs) are available in the original analysis published by the Pedro Tavares

https://seguranca-informatica.pt/anubis-networks-is-back-with-new-c2-server/#.Ysv53XZBy5d

About the author: Pedro Tavarez

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker, Malware Analyst and also a Security Evangelist. He is also a founding member and Pentester at CSIRT.UBI and founder of the security computer blog seguranca–informatica.pt.

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner="9"]	[adrotate banner="12"]

Pierluigi Paganini

(SecurityAffairs – hacking, Anubis)

[adrotate banner="5"]

[adrotate banner="13"]

Source: https://securityaffairs.co/wordpress/133115/hacking/anubis-networks-new-c2.html