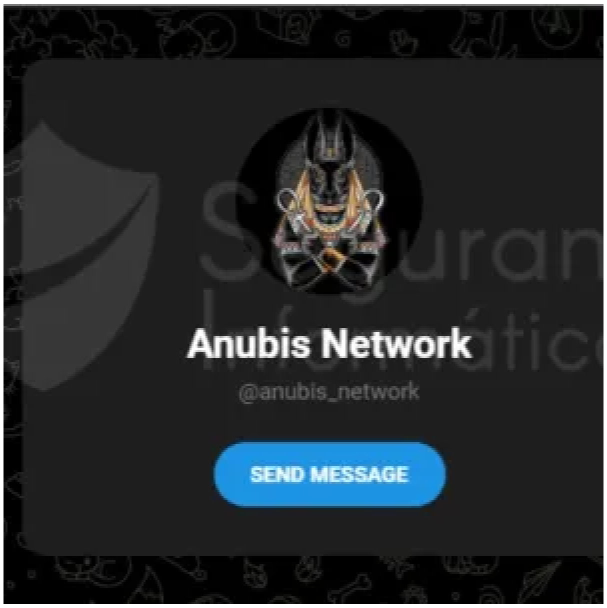
Anubis Networks is back with new C2 server

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

July 11, 2022



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.

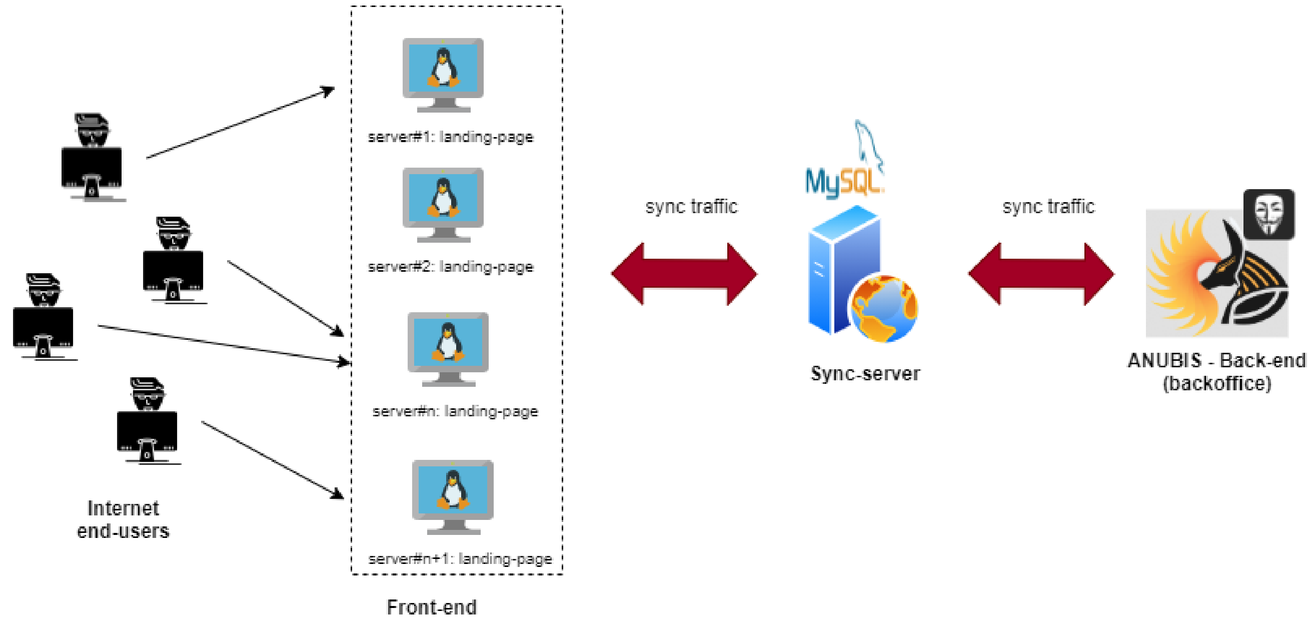
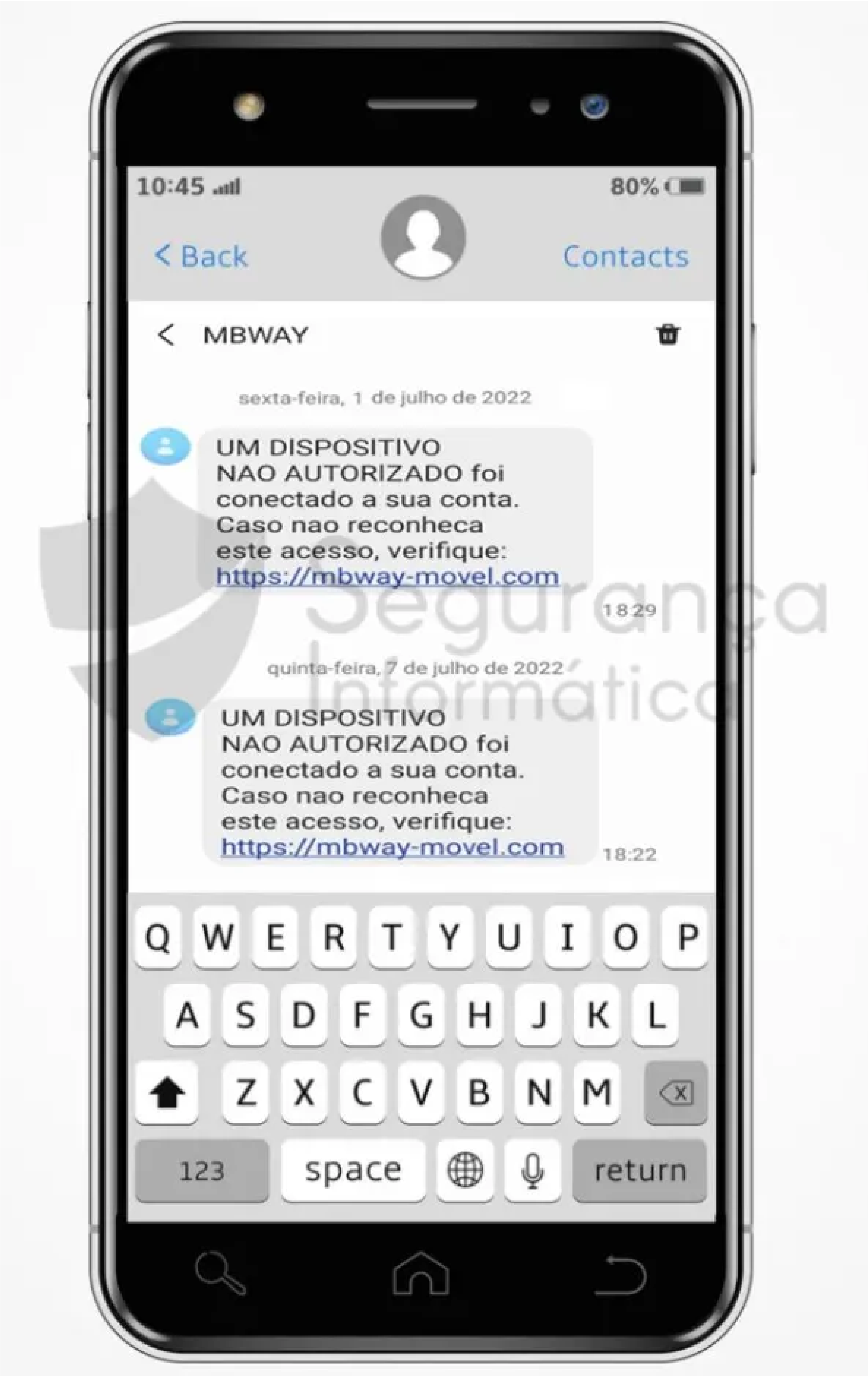


Figure 1: *High-level diagram of the ANUBIS phishing network and its components (2020).*

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.



sexta-feira, 1 de julho de 2022

UM DISPOSITIVO
NAO AUTORIZADO foi
conectado a sua conta.
Caso nao reconheca
este acesso, verifique:
https://mbway-movel.com

18:29

quinta-feira, 7 de julho de 2022

UM DISPOSITIVO
NAO AUTORIZADO foi
conectado a sua conta.
Caso nao reconheca
este acesso, verifique:
https://mbway-movel.com

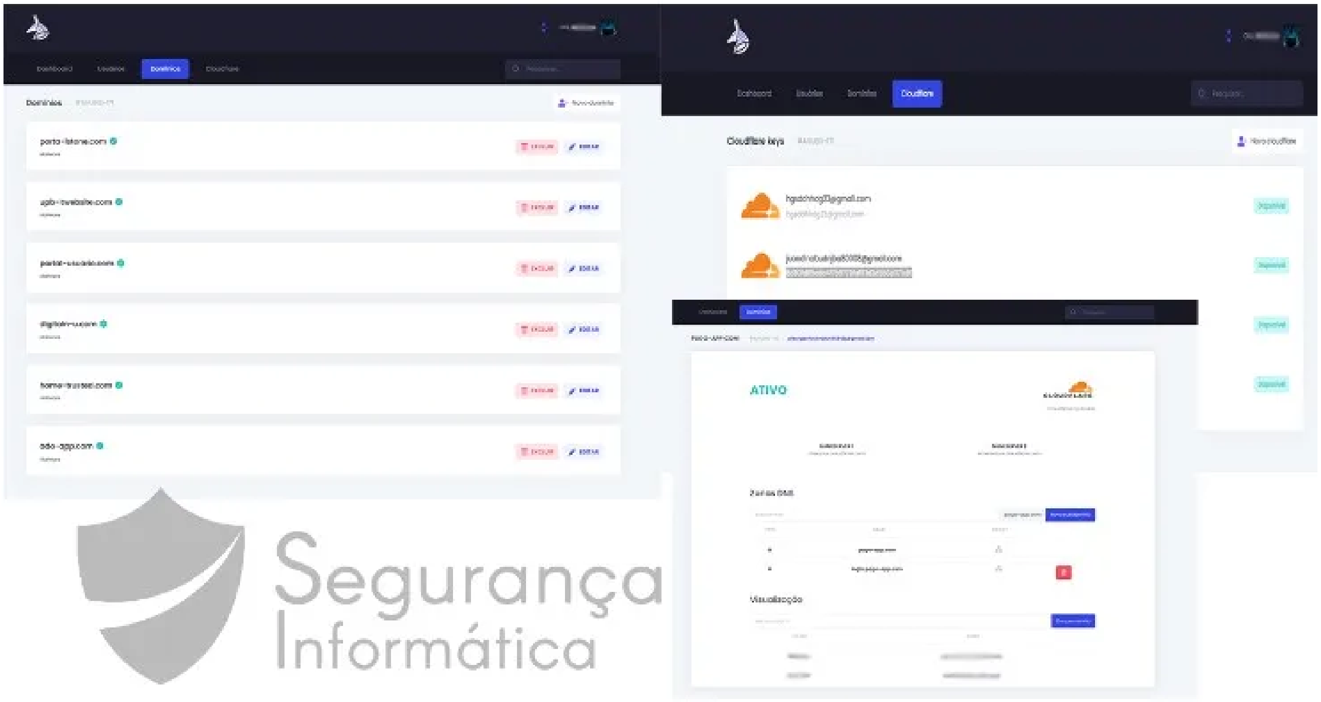
18:22

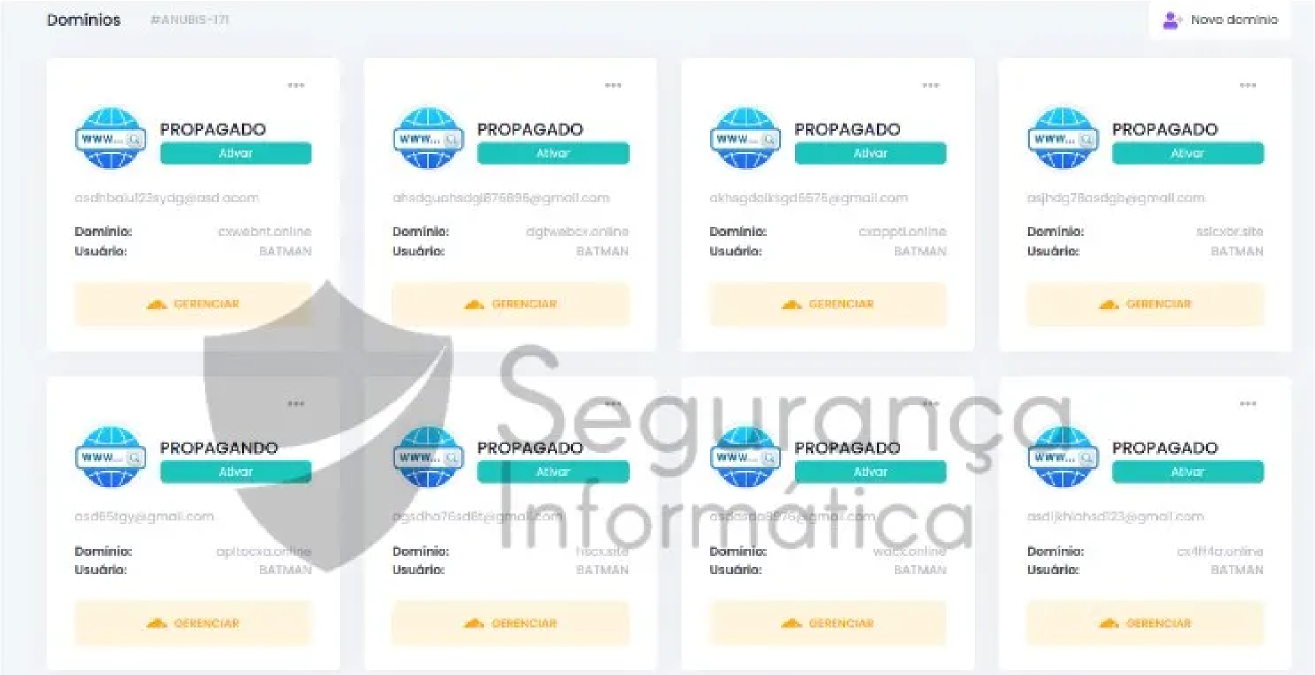
***Figure 2:** Example of SMS sent during the social engineering wave.*

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.





Domínios #ANUBIS-171

Novo domínio

PROPAGADO
Ativar
asdhbalu123sydg@asd.acom
Domínio: cxwebnt.online
Usuário: BATMAN
GERENCIAR

PROPAGADO
Ativar
ahsdguahsdgl876895@gmail.com
Domínio: dgtwebcx.online
Usuário: BATMAN
GERENCIAR

PROPAGADO
Ativar
akhsgdalksgd6575@gmail.com
Domínio: cxappt.online
Usuário: BATMAN
GERENCIAR

PROPAGADO
Ativar
asjhdg78asdgb@gmail.com
Domínio: sslcxbr.site
Usuário: BATMAN
GERENCIAR

PROPAGANDO
Ativar
asd65tgy@gmail.com
Domínio: apltocxa.online
Usuário: BATMAN
GERENCIAR

PROPAGADO
Ativar
agsdha76sd6t@gmail.com
Domínio: fracx.site
Usuário: BATMAN
GERENCIAR

PROPAGADO
Ativar
asdasda8976@gmail.com
Domínio: wacc.online
Usuário: BATMAN
GERENCIAR

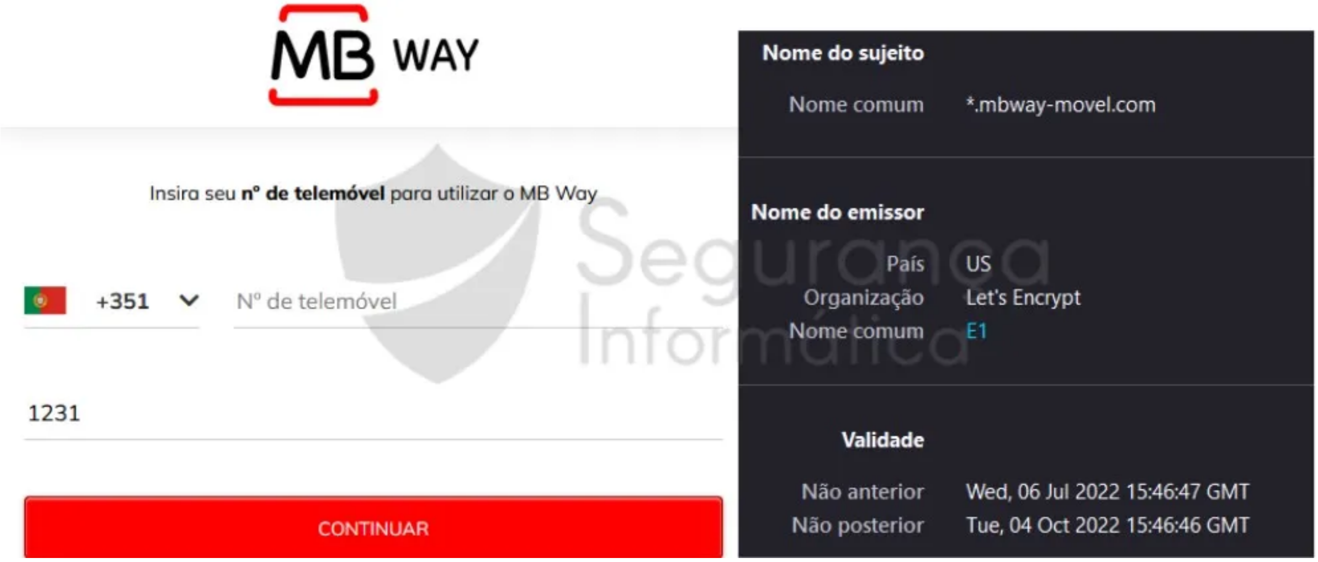
PROPAGADO
Ativar
asdljkhiahsd123@gmail.com
Domínio: cx4ff4a.online
Usuário: BATMAN
GERENCIAR

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.



MB WAY

Insira seu **nº de telemóvel** para utilizar o MB Way

+351 Nº de telemóvel

1231

CONTINUAR

Nome do sujeito

Nome comum *.mbway-movel.com

Nome do emissor

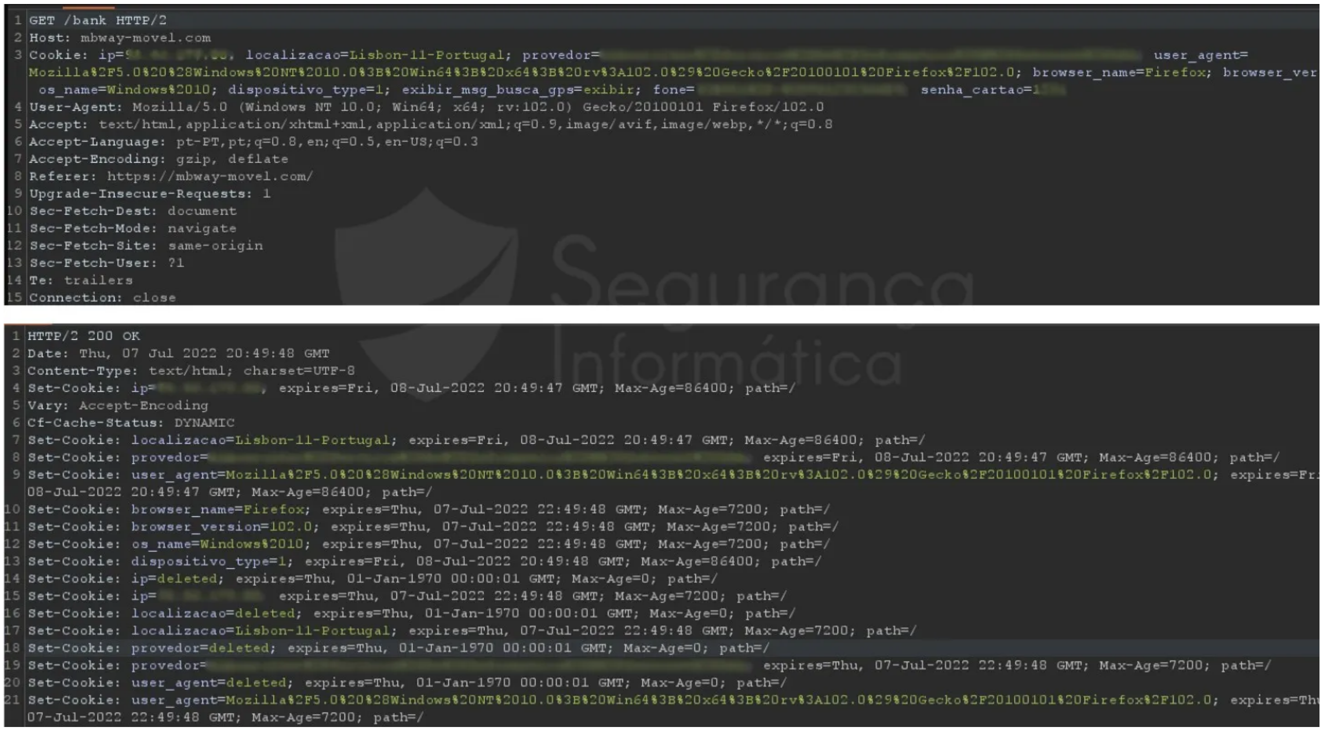
País US
Organização Let's Encrypt
Nome comum E1

Validade

Não anterior Wed, 06 Jul 2022 15:46:47 GMT
Não posterior Tue, 04 Oct 2022 15:46:46 GMT

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.

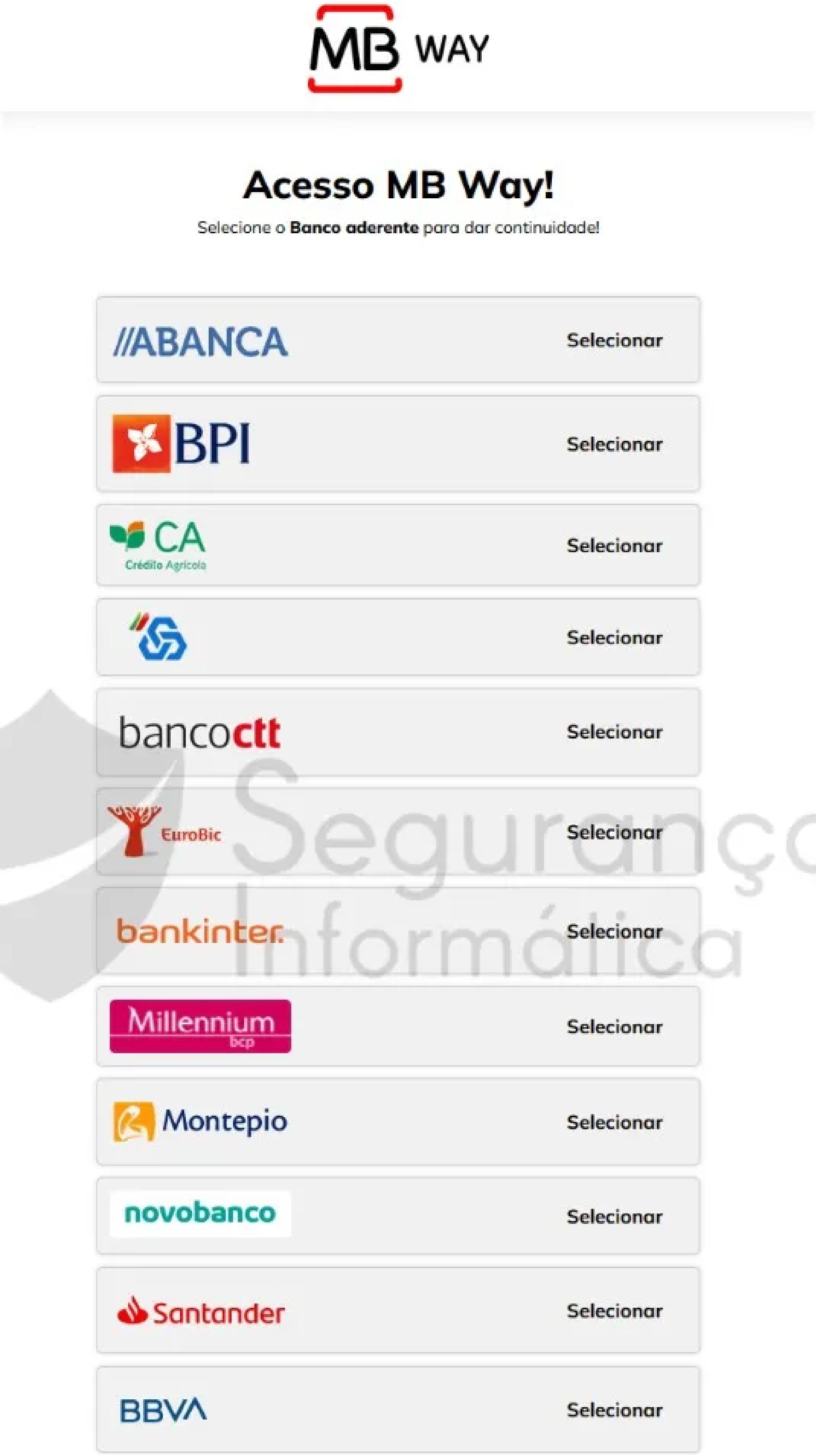


```
GET /bank HTTP/2
Host: mbway-movel.com
Cookie: ip=[redacted] localizacao=Lisbon-11-Portugal; provedor=[redacted] user_agent=
Mozilla%2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%3B%20rv%3A102.0%29%20Gecko%2F20100101%20Firefox%2F102.0; browser_name=Firefox; browser_ver
 os_name=Windows%2010; dispositivo_type=1; exibir_msg_busca_gps=exibir; fone=[redacted] senha_cartao=[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://mbway-movel.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/2 200 OK
Date: Thu, 07 Jul 2022 20:49:48 GMT
Content-Type: text/html; charset=UTF-8
Set-Cookie: ip=[redacted] expires=Fri, 08-Jul-2022 20:49:47 GMT; Max-Age=86400; path=/
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Set-Cookie: localizacao=Lisbon-11-Portugal; expires=Fri, 08-Jul-2022 20:49:47 GMT; Max-Age=86400; path=/
Set-Cookie: provedor=[redacted] expires=Fri, 08-Jul-2022 20:49:47 GMT; Max-Age=86400; path=/
Set-Cookie: user_agent=Mozilla%2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%3B%20rv%3A102.0%29%20Gecko%2F20100101%20Firefox%2F102.0; expires=Fr
08-Jul-2022 20:49:47 GMT; Max-Age=86400; path=/
Set-Cookie: browser_name=Firefox; expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: browser_version=102.0; expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: os_name=Windows%2010; expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: dispositivo_type=1; expires=Fri, 08-Jul-2022 20:49:48 GMT; Max-Age=86400; path=/
Set-Cookie: ip=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: ip=[redacted] expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: localizacao=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: localizacao=Lisbon-11-Portugal; expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: provedor=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: provedor=[redacted] expires=Thu, 07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
Set-Cookie: user_agent=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: user_agent=Mozilla%2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%3B%20rv%3A102.0%29%20Gecko%2F20100101%20Firefox%2F102.0; expires=Thu
07-Jul-2022 22:49:48 GMT; Max-Age=7200; path=/
```

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.

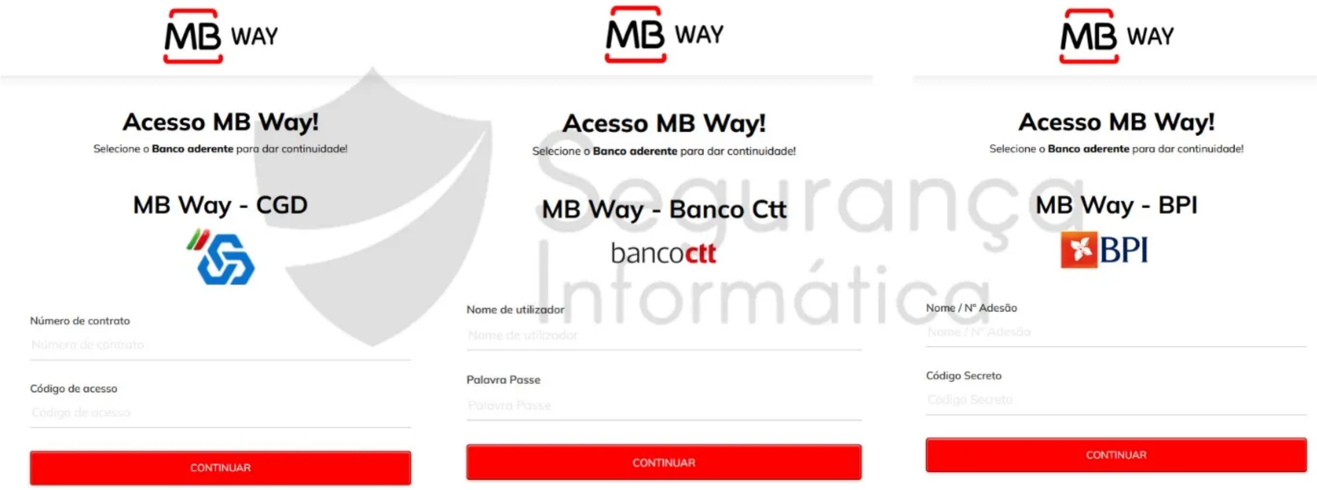


Acesso MB Way!

Selecione o **Banco aderente** para dar continuidade!

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

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



MB WAY

Acesso MB Way!

Selecione o **Banco aderente** para dar continuidade!

MB Way - CGD

Número de contrato

Número de contrato

Código de acesso

Código de acesso

CONTINUAR

MB WAY

Acesso MB Way!

Selecione o **Banco aderente** para dar continuidade!

MB Way - Banco Ctt

bancoctt

Nome de utilizador

Nome de utilizador

Palavra Passe

Palavra Passe

CONTINUAR

MB WAY

Acesso MB Way!

Selecione o **Banco aderente** para dar continuidade!

MB Way - BPI

BPI

Nome / Nº Adesão

Nome / Nº Adesão

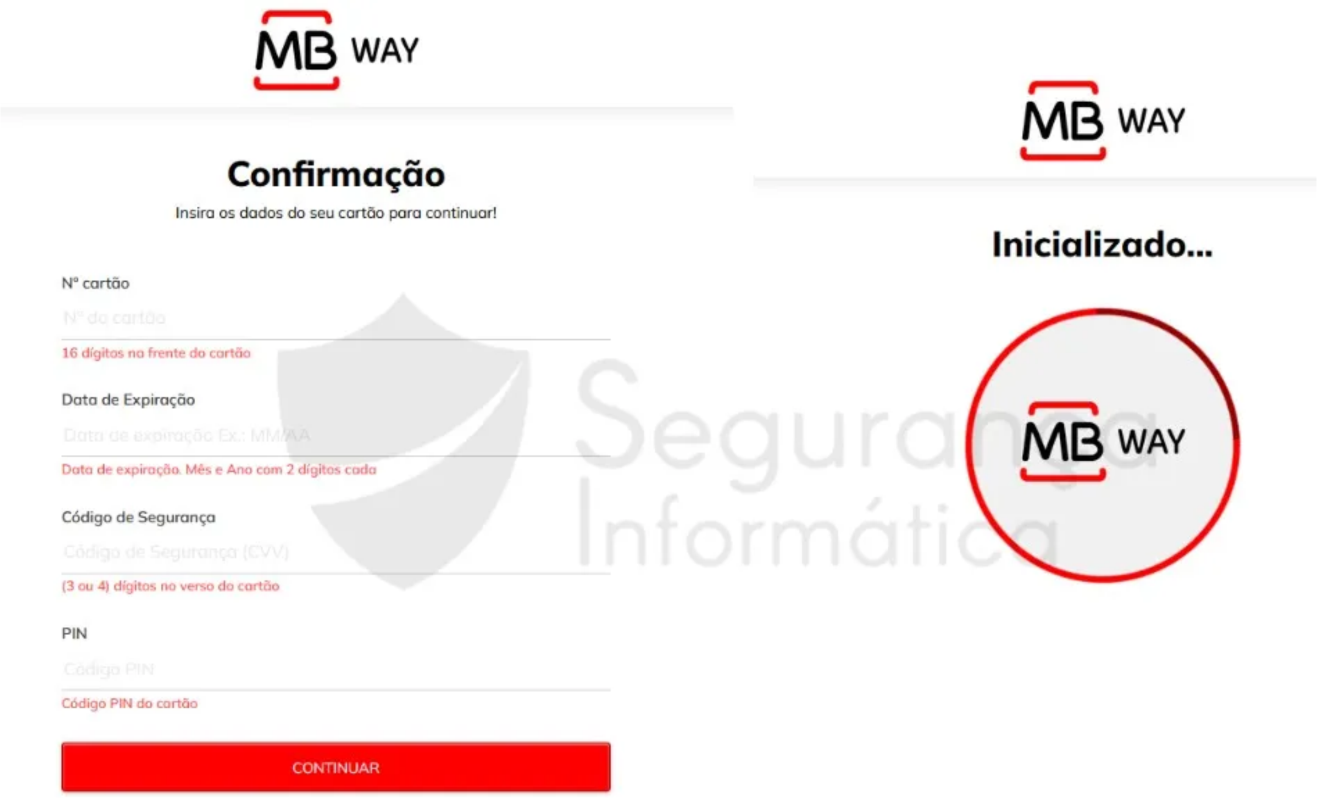
Código Secreto

Código Secreto

CONTINUAR

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*.



MB WAY

Confirmação

Insira os dados do seu cartão para continuar!

Nº cartão

Nº do cartão

16 dígitos na frente do cartão

Data de Expiração

Data de expiração Ex.: MM/AA

Data de expiração. Mês e Ano com 2 dígitos cada

Código de Segurança

Código de Segurança (CVV)

(3 ou 4) dígitos no verso do cartão

PIN

Código PIN

Código PIN do cartão

CONTINUAR

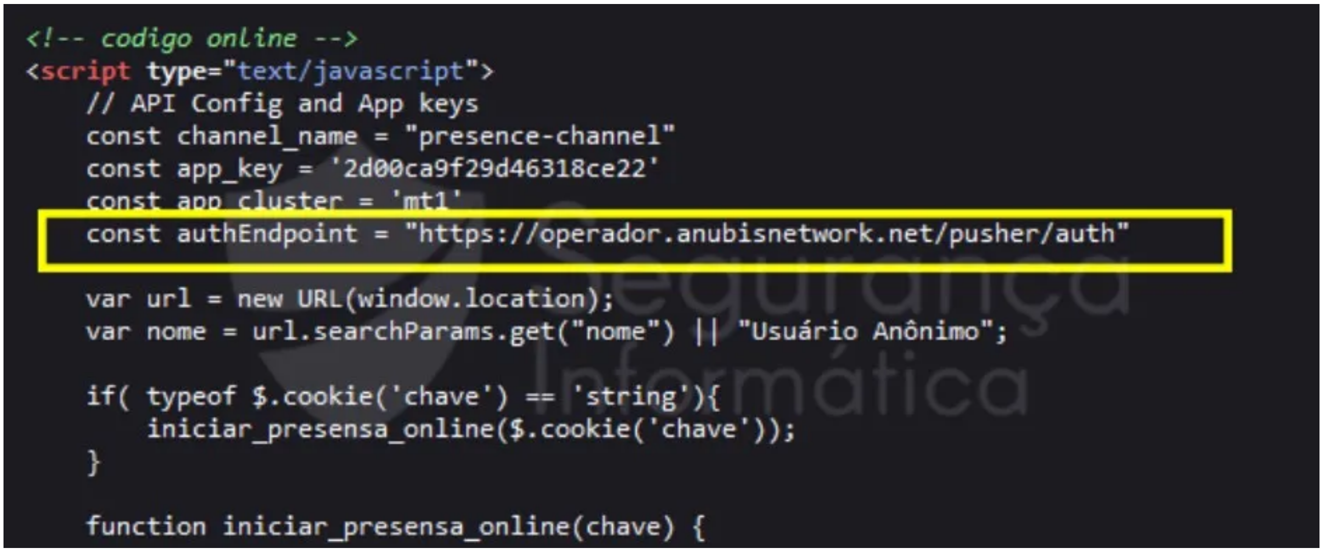
MB WAY

Inicializado...

Figure 8: *Additional information requested by criminals.*

Anubis Network C2 Panel

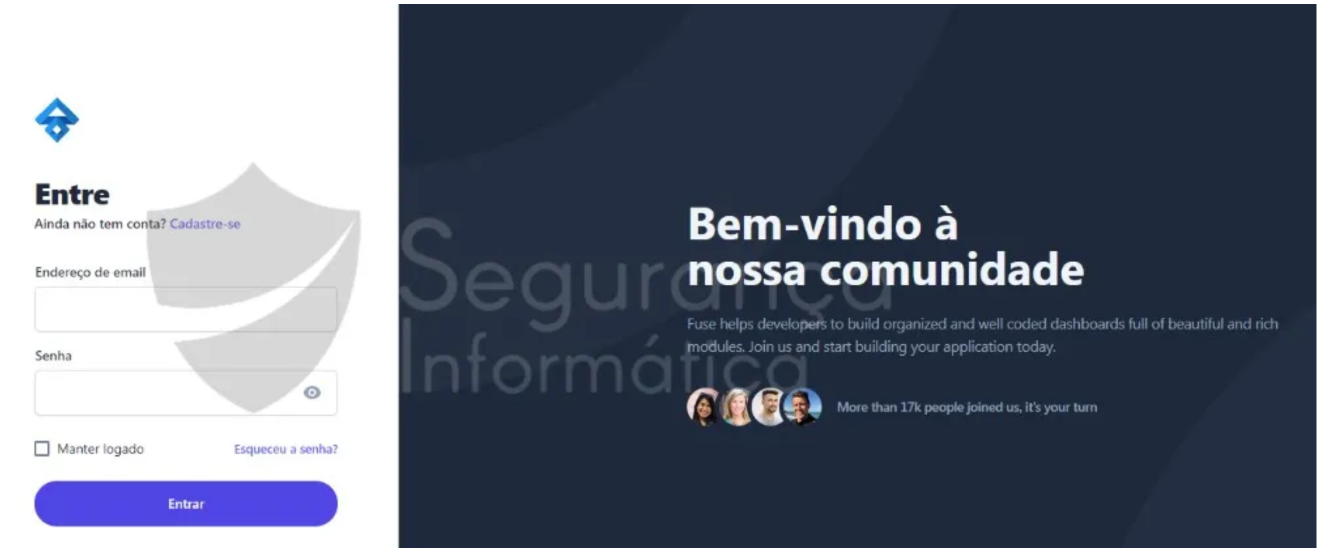
By analyzing the landing page source code, the URL of the C2 server can be obtained.



```
<!-- codigo online -->
<script type="text/javascript">
    // API Config and App keys
    const channel_name = "presence-channel"
    const app_key = '2d00ca9f29d46318ce22'
    const app_cluster = 'mt1'
    const authEndpoint = "https://operador.anubisnetwork.net/pusher/auth"

    var url = new URL(window.location);
    var nome = url.searchParams.get("nome") || "Usuário Anônimo";

    if( typeof $.cookie('chave') == 'string'){
        iniciar_presensa_online($.cookie('chave'));
    }

    function iniciar_presensa_online(chave) {
```

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.



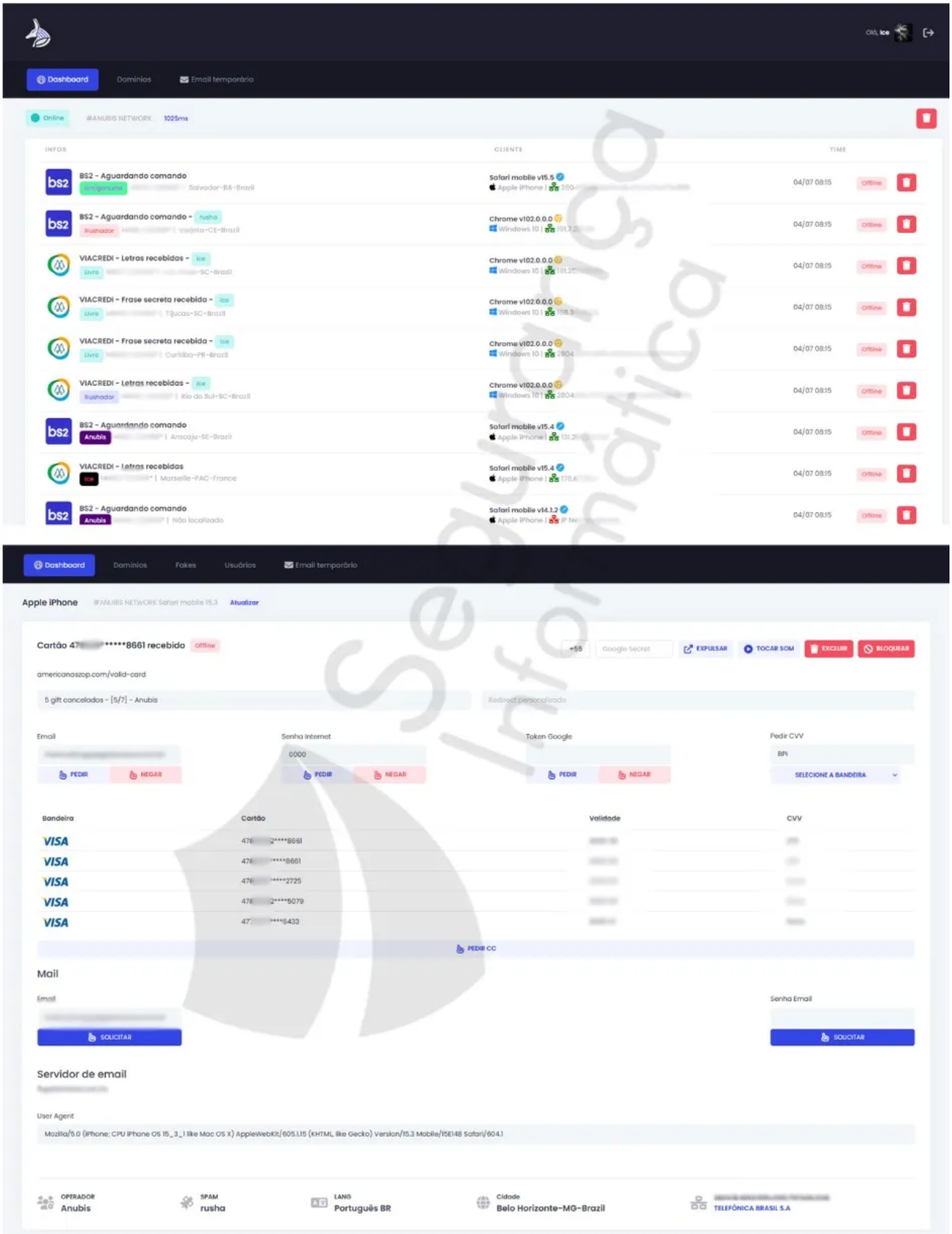
Bem-vindo à nossa comunidade

Fuse helps developers to build organized and well coded dashboards full of beautiful and rich modules. Join us and start building your application today.

More than 17k people joined us, it's your turn

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.



INFOS	CLIENTE	TIME	
BS2 - Aguardando comando amigorusha [redacted] Salvador-BA-Brazil	Safari mobile v15.5 Apple iPhone | 280-[redacted]	04/07 08:15	Offline
BS2 - Aguardando comando - rusha Rushador [redacted] | [redacted]-CE-Brazil	Chrome v102.0.0.0 Windows 10 | 191.7.2[redacted]	04/07 08:15	Offline
VIACREDI - Letras recebidas - ice Livre [redacted]-SC-Brazil	Chrome v102.0.0.0 Windows 10 | 191.25[redacted]	04/07 08:15	Offline
VIACREDI - Frase secreta recebida - ice Livre [redacted] | Tijucas-SC-Brazil	Chrome v102.0.0.0 Windows 10 | 168.9[redacted]	04/07 08:15	Offline
VIACREDI - Frase secreta recebida - ice Livre [redacted] | Curitiba-PR-Brazil	Chrome v102.0.0.0 Windows 10 | 2804[redacted]	04/07 08:15	Offline
VIACREDI - Letras recebidas - ice Rushador [redacted] | Rio do Sul-SC-Brazil	Chrome v102.0.0.0 Windows 10 | 2804[redacted]	04/07 08:15	Offline
BS2 - Aguardando comando Anubis [redacted] | Aracaju-SE-Brazil	Safari mobile v15.4 Apple iPhone | 131.2[redacted]	04/07 08:15	Offline
VIACREDI - Letras recebidas ice [redacted]* | Marseille-PAC-France	Safari mobile v15.4 Apple iPhone | 176.6[redacted]	04/07 08:15	Offline
BS2 - Aguardando comando Anubis [redacted] | Não localizado	Safari mobile v14.1.2 Apple iPhone | IP N[redacted]	04/07 08:15	Offline

Apple iPhone #ANUBIS NETWORK Safari mobile 15.3 Atualizar

Cartão 47[redacted]*****8661 recebido Offline

americanaszop.com/valid-card

5 gift cancelados - [5/7] - Anubis

Email: [redacted]

Senha Internet: 0000

Token Google:

Pedir CVV: BPI

Bandeira	Cartão	Validade	CVV
VISA	47[redacted]2****8661	[redacted]	[redacted]
VISA	47[redacted]****8661	[redacted]	[redacted]
VISA	47[redacted]****2725	[redacted]	[redacted]
VISA	47[redacted]2****5079	[redacted]	[redacted]
VISA	47[redacted]****6433	[redacted]	[redacted]

Mail

Email: [redacted]

Senha Email:

Servidor de email

[redacted]

User Agent

Mozilla/5.0 (iPhone; CPU iPhone OS 15_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.3 Mobile/15E148 Safari/604.1

OPERADOR: Anubis

SPAM: rusha

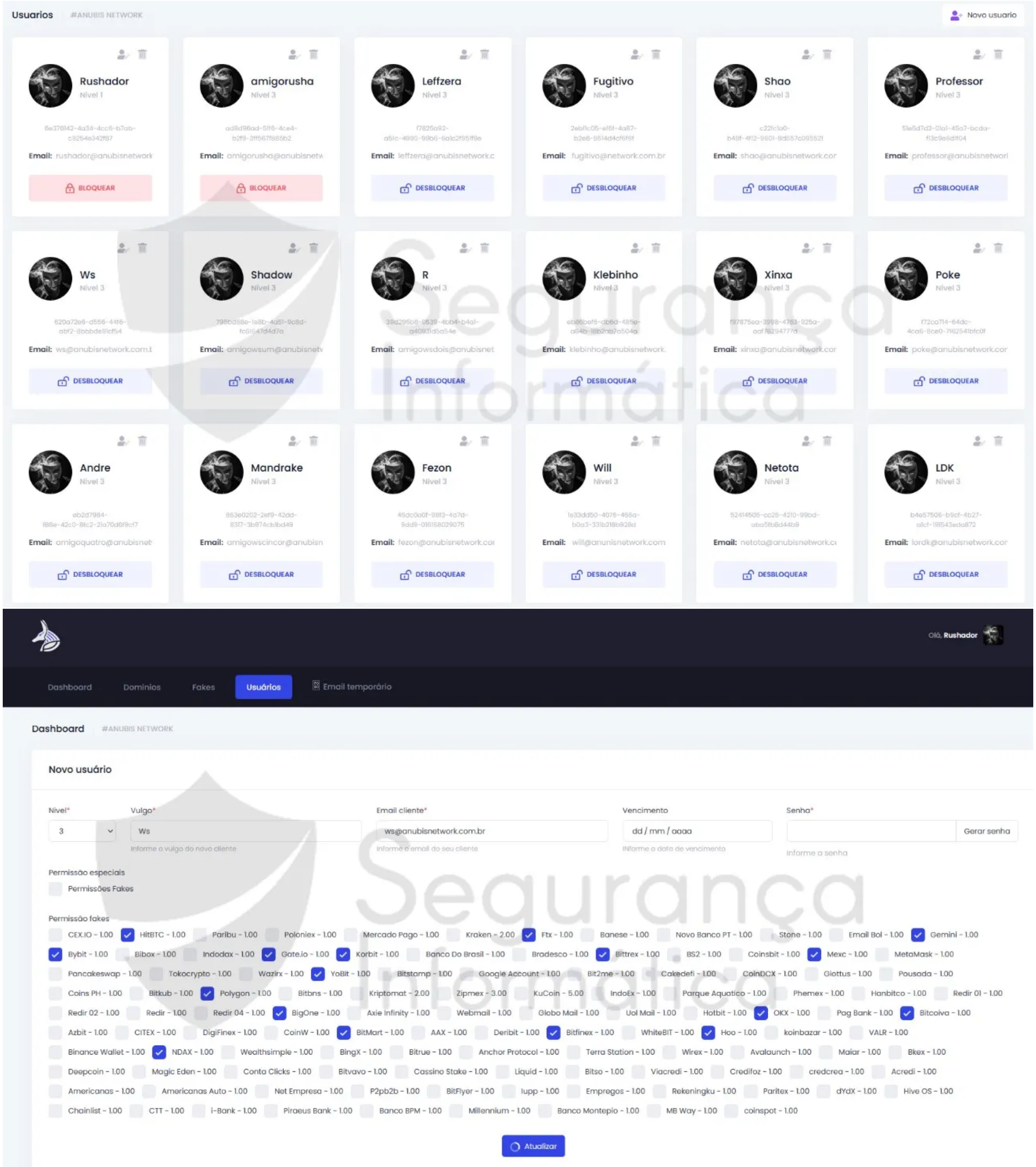
LANG: Português BR

Cidade: Belo Horizonte-MG-Brazil

[redacted] TELEFÔNICA BRASIL S.A

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.



Usuarios #ANUBIS NETWORK

Novo usuario

Rushador
Nivel 1
6e376142-4a34-4cc6-b7ab-c9254e342f87
Email: rushador@anubisnetwork
BLOQUEAR

amigorusha
Nivel 3
ad8d96ad-5ff6-4ce4-b2f9-3ff567f885b2
Email: amigorusha@anubisnetw
BLOQUEAR

Leffzera
Nivel 3
f7825a92-a5lc-4990-99b6-6a1c2f95ff9e
Email: leffzera@anubisnetwork.c
DESBLOQUEAR

Fugitivo
Nivel 3
2ebf1c05-ef6f-4a87-b2e8-8514d4cf6f6f
Email: fugitivo@network.com.br
DESBLOQUEAR

Shao
Nivel 3
c22fc1a0-b49f-4f12-9601-8d557c095521
Email: shao@anubisnetwork.cor
DESBLOQUEAR

Professor
Nivel 3
51e5d7d2-01a1-45a7-bcda-f13c9e6d1f04
Email: professor@anubisnetworl
DESBLOQUEAR

Ws
Nivel 3
620a72e6-d556-44f6-abf2-8bbbde91cf54
Email: ws@anubisnetwork.com.t
DESBLOQUEAR

Shadow
Nivel 3
795bd88e-1e8b-4a51-9c8d-fc61647d4d7a
Email: amigowsum@anubisnetv
DESBLOQUEAR

R
Nivel 3
39d296b8-0639-4bb4-b4a1-a40931d5a54e
Email: amigowsdois@anubisnet
DESBLOQUEAR

Klebinho
Nivel 3
eb86bef6-db6d-485e-a64b-18b2ab7a504a
Email: klebinho@anubisnetwork.
DESBLOQUEAR

Xinxa
Nivel 3
f97875ea-3998-4763-925a-aaf76294777d
Email: xinxa@anubisnetwork.cor
DESBLOQUEAR

Poke
Nivel 3
f72ca714-64dc-4ca6-8ce0-7162541bfc0f
Email: poke@anubisnetwork.cor
DESBLOQUEAR

Andre
Nivel 3
eb2d7984-f86e-42c0-8fc2-21a70d6f9cf7
Email: amigoquatro@anubisnet
DESBLOQUEAR

Mandrake
Nivel 3
863e0202-2ef9-42dd-8317-3b974cb1bd49
Email: amigowscincor@anubisn
DESBLOQUEAR

Fezon
Nivel 3
45dc0a0f-98f3-4a7d-9dd9-016168029075
Email: fezon@anubisnetwork.coı
DESBLOQUEAR

Will
Nivel 3
1e33dd50-4076-466a-b0a3-331b218b928d
Email: will@anunisnetwork.com
DESBLOQUEAR

Netota
Nivel 3
52414505-cc26-4210-99bd-aba5fb8d44b9
Email: netota@anubisnetwork.cı
DESBLOQUEAR

LDK
Nivel 3
b4e57506-b9cf-4b27-a1cf-191543eda872
Email: lordk@anubisnetwork.cor
DESBLOQUEAR

Dashboard #ANUBIS NETWORK

Novo usuário

Nivel*: 3
Vulgo*: Ws
Informe o vulgo do novo cliente
Email cliente*: ws@anubisnetwork.com.br
Informe o email do seu cliente
Vencimento: dd / mm / aaaa
INforme a data de vencimento
Senha*: Gerar senha
Informe a senha

Permissão especiais
□ Permissões Fakes

Permissão fakes
□ CEX.IO - 1.00 ☑ HitBTC - 1.00 □ Paribu - 1.00 □ Poloniex - 1.00 □ Mercado Pago - 1.00 □ Kraken - 2.00 ☑ Ftx - 1.00 □ Banese - 1.00 □ Novo Banco PT - 1.00 □ Stone - 1.00 □ Email Bol - 1.00 ☑ Gemini - 1.00
☑ Bybit - 1.00 □ Bibox - 1.00 □ Indodax - 1.00 ☑ Gate.io - 1.00 ☑ Korbit - 1.00 □ Banco Do Brasil - 1.00 □ Bradesco - 1.00 ☑ Bittrex - 1.00 □ BS2 - 1.00 □ Coinsbit - 1.00 ☑ Mexc - 1.00 □ MetaMask - 1.00
□ Pancakeswap - 1.00 □ Tokocrypto - 1.00 □ Wazirx - 1.00 ☑ YoBit - 1.00 □ Bitstamp - 1.00 □ Google Account - 1.00 □ Bit2me - 1.00 □ Cakedefi - 1.00 □ CoinDCX - 1.00 □ Giottus - 1.00 □ Pousada - 1.00
□ Coins PH - 1.00 □ Bitkub - 1.00 ☑ Polygon - 1.00 □ Bitbns - 1.00 □ Kriptomat - 2.00 □ Zipmex - 3.00 □ KuCoin - 5.00 □ IndoEx - 1.00 □ Parque Aquatico - 1.00 □ Phemex - 1.00 □ Hanbitco - 1.00 □ Redir 01 - 1.00
□ Redir 02 - 1.00 □ Redir - 1.00 □ Redir 04 - 1.00 ☑ BigOne - 1.00 □ Axie Infinity - 1.00 □ Webmail - 1.00 □ Globo Mail - 1.00 □ Uol Mail - 1.00 □ Hotbit - 1.00 ☑ OKX - 1.00 □ Pag Bank - 1.00 ☑ Bitcoiva - 1.00
□ Azbit - 1.00 □ CITEX - 1.00 □ DigiFinex - 1.00 □ CoinW - 1.00 ☑ BitMart - 1.00 □ AAX - 1.00 □ Deribit - 1.00 ☑ Bitfinex - 1.00 □ WhiteBIT - 1.00 ☑ Hoo - 1.00 □ koinbazar - 1.00 □ VALR - 1.00
□ Binance Wallet - 1.00 ☑ NDAX - 1.00 □ Wealthsimple - 1.00 □ BingX - 1.00 □ Bitrue - 1.00 □ Anchor Protocol - 1.00 □ Terra Station - 1.00 □ Wirex - 1.00 □ Avalaunch - 1.00 □ Maiar - 1.00 □ Bkex - 1.00
□ Deepcoin - 1.00 □ Magic Eden - 1.00 □ Conta Clicks - 1.00 □ Bitvavo - 1.00 □ Cassino Stake - 1.00 □ Liquid - 1.00 □ Bitso - 1.00 □ Viacredi - 1.00 □ Credifoz - 1.00 □ credcrea - 1.00 □ Acredi - 1.00
□ Americanas - 1.00 □ Americanas Auto - 1.00 □ Net Empresa - 1.00 □ P2pb2b - 1.00 □ BitFlyer - 1.00 □ Iupp - 1.00 □ Empregos - 1.00 □ Rekeningku - 1.00 □ Paritex - 1.00 □ dYdX - 1.00 □ Hive OS - 1.00
□ Chainlist - 1.00 □ CTT - 1.00 □ i-Bank - 1.00 □ Piraeus Bank - 1.00 □ Banco BPM - 1.00 □ Millennium - 1.00 □ Banco Montepio - 1.00 □ MB Way - 1.00 □ coinspot - 1.00

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

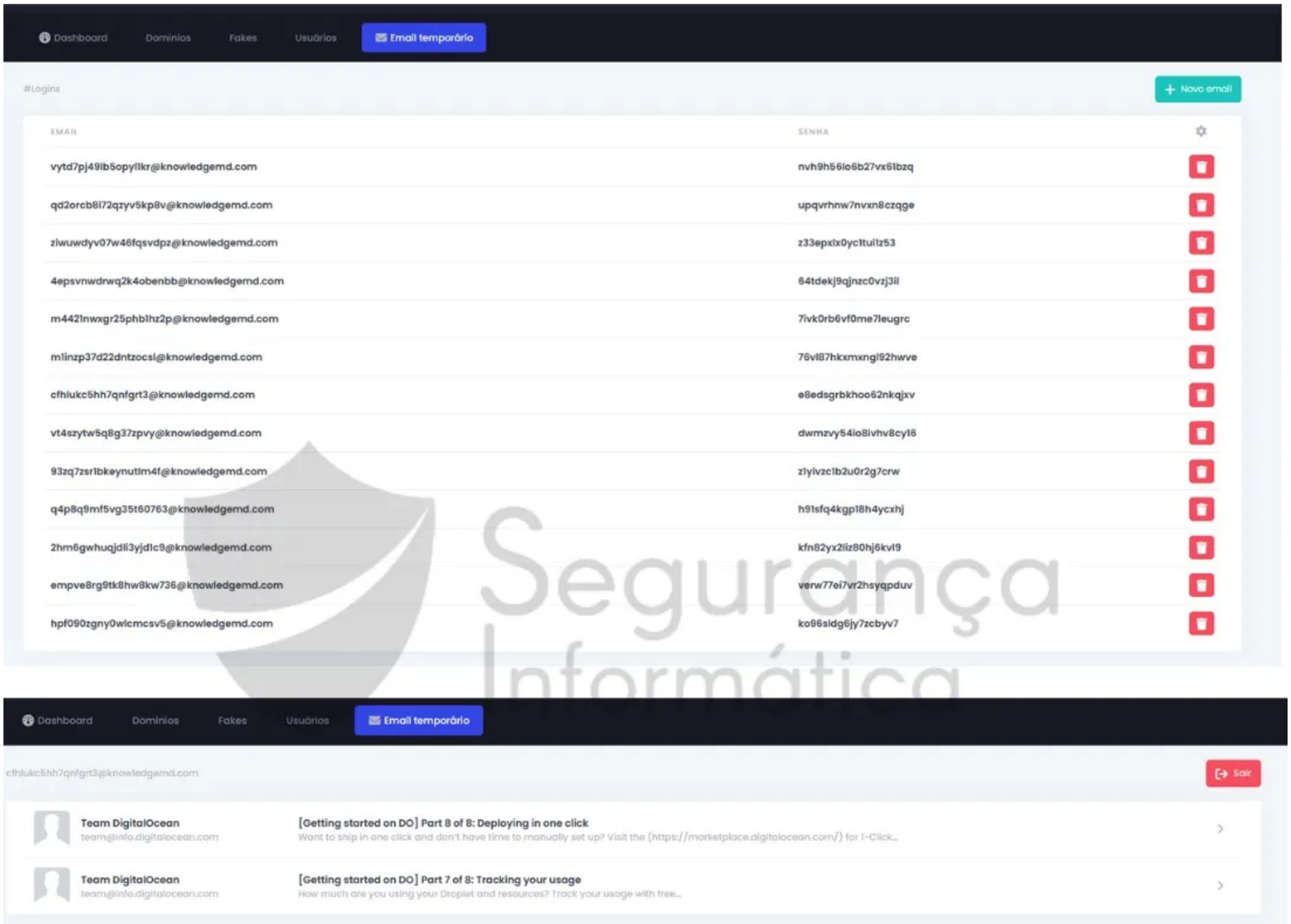
According to the MySQL database that supports the system, there are 77 operators in the system – which represents the business and operational volume of this malicious scheme.

- 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.



#Logins

EMAIL	SENHA
vytd7pj49ib5opyllkr@knowledgemd.com	nvh9h56lo6b27vx6lbzq
qd2orcb8i72qzyv5kp8v@knowledgemd.com	upqvrhnw7nvxn8czqge
ziwuwdyv07w46fqsvdpz@knowledgemd.com	z33epxlx0yc1tui1z53
4epsvnwdrwq2k4obenbb@knowledgemd.com	64tdekj9qjnzc0vzj3il
m442lnwxgr25phblhz2p@knowledgemd.com	7ivk0rb6vf0me7leugrc
mlinzp37d22dntzocsl@knowledgemd.com	76vl87hkxmxngl92hwve
cfhlukc5hh7qnfgrt3@knowledgemd.com	e8edsgrbkhoo62nkqjxv
vt4szytw5q8g37zpvy@knowledgemd.com	dwmzvy54io8ivhv8cy16
93zq7zsrlbkeynutlm4f@knowledgemd.com	zlyivzclb2u0r2g7crw
q4p8q9mf5vg35t60763@knowledgemd.com	h91sfq4kgp18h4ycxhj
2hm6gwhuqjdli3yjd1c9@knowledgemd.com	kfn82yx2liz80hj6kvl9
empve8rg9tk8hw8kw736@knowledgemd.com	verw77ei7vr2hsyqpduv
hpf090zgny0wlcmcsv5@knowledgemd.com	ko96sldg6jy7zcbyv7

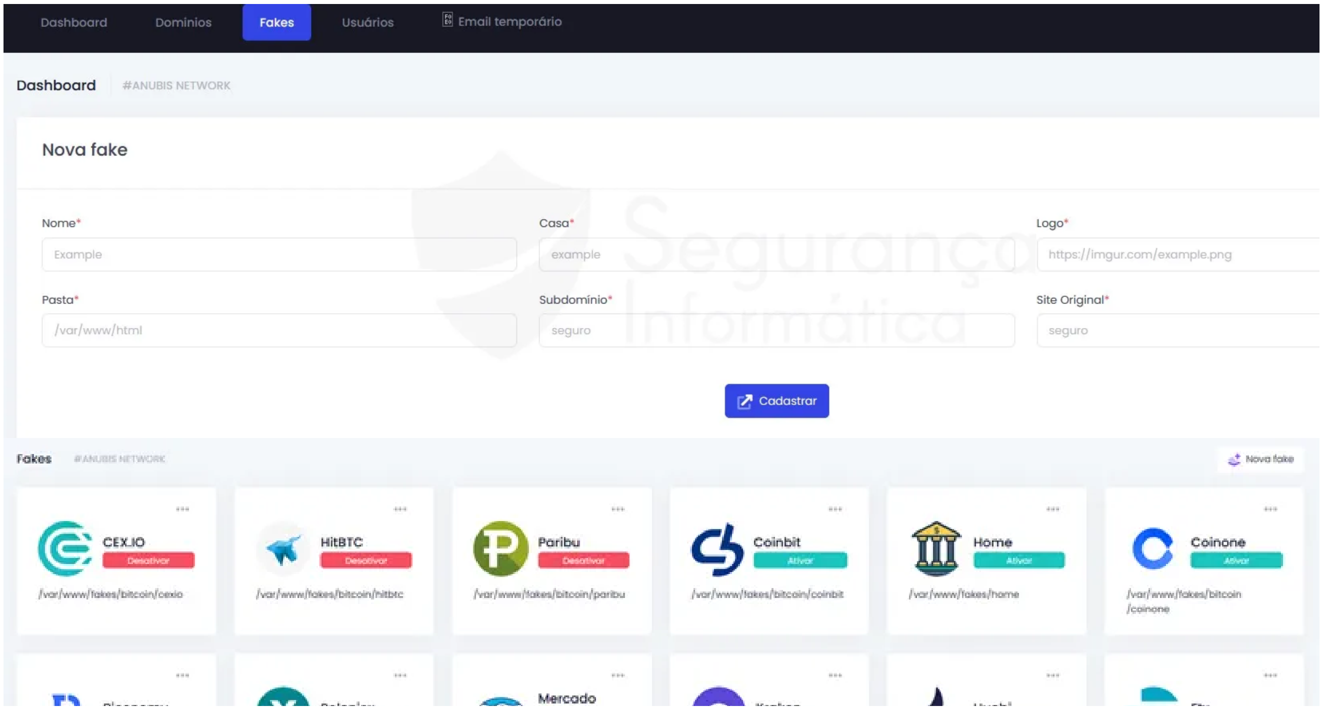
cfhlukc5hh7qnfgrt3@knowledgemd.com

Team DigitalOcean
team@info.digitalocean.com
[Getting started on DO] Part 8 of 8: Deploying in one click
Want to ship in one click and don't have time to manually set up? Visit the (https://marketplace.digitalocean.com/) for 1-Click...

Team DigitalOcean
team@info.digitalocean.com
[Getting started on DO] Part 7 of 8: Tracking your usage
How much are you using your Droplet and resources? Track your usage with free...

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.



Dashboard #ANUBIS NETWORK

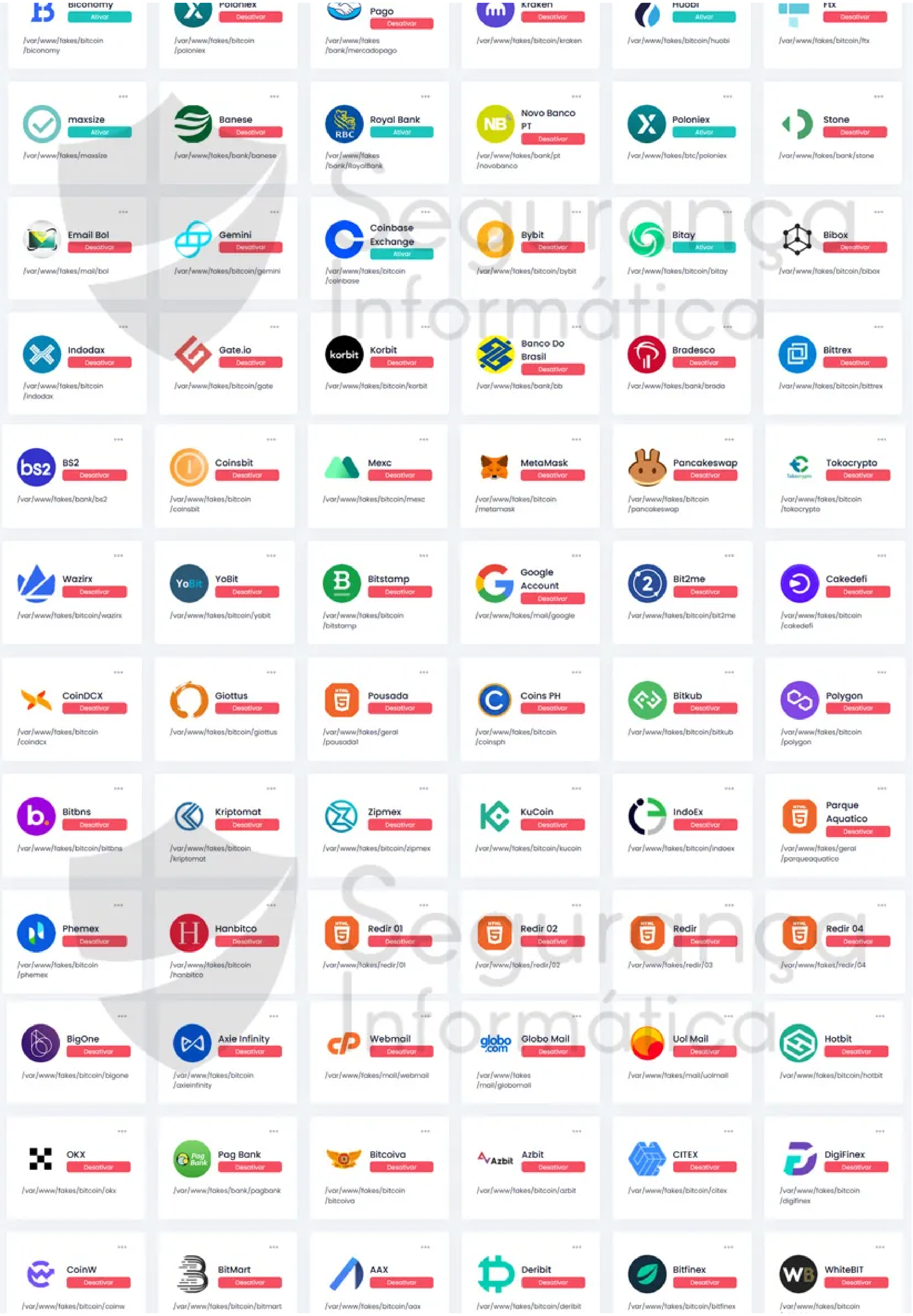
Nova fake

Nome* Example
Casa* example
Logo* https://imgur.com/example.png
Pasta* /var/www/html
Subdominio* seguro
Site Original* seguro

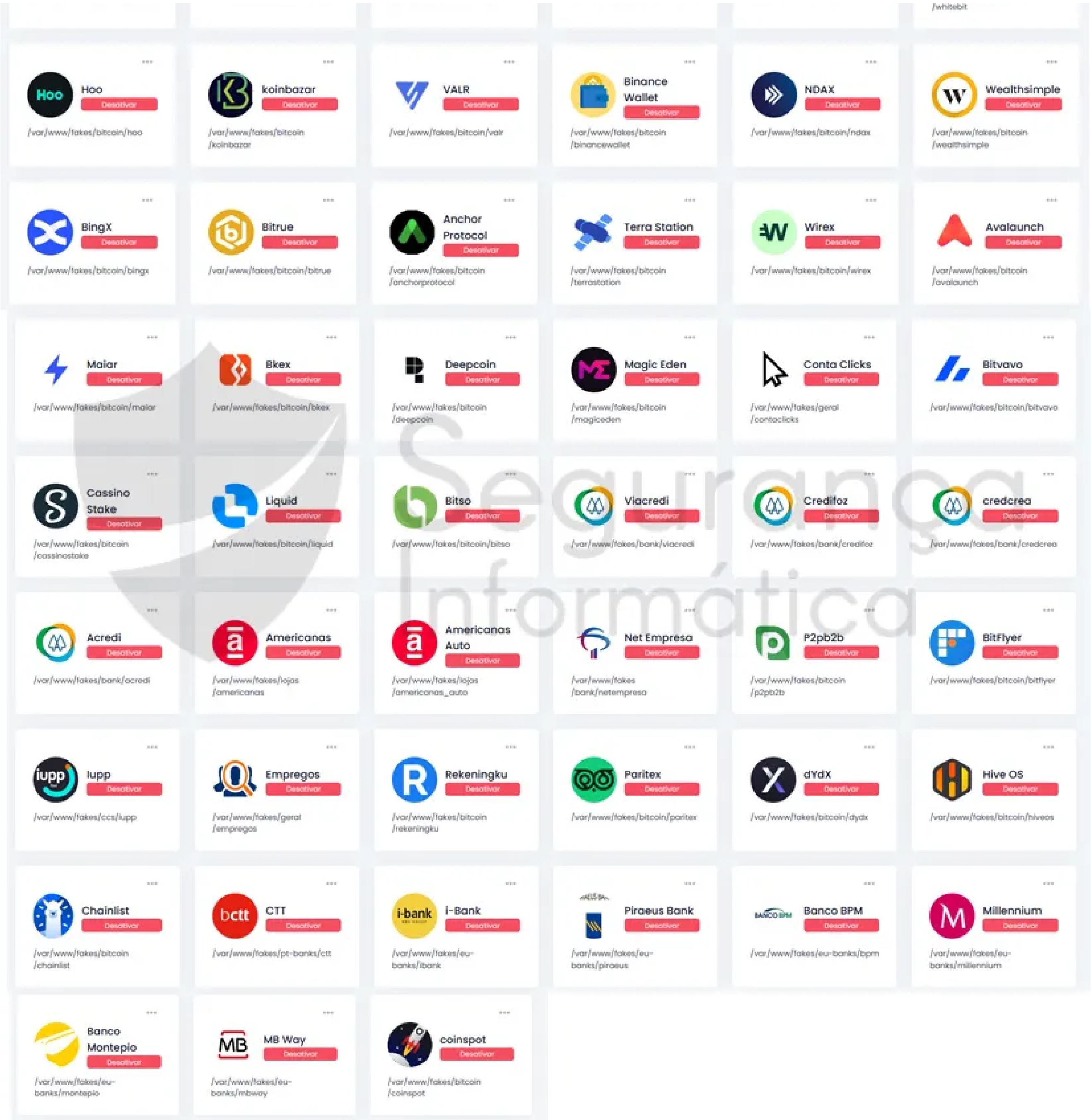
Fakes #ANUBIS NETWORK

CEX.IO — Desativar — /var/www/fakes/bitcoin/cexio
HitBTC — Desativar — /var/www/fakes/bitcoin/hitbtc
Paribu — Desativar — /var/www/fakes/bitcoin/paribu
Coinbit — Ativar — /var/www/fakes/bitcoin/coinbit
Home — Ativar — /var/www/fakes/home
Coinone — Ativar — /var/www/fakes/bitcoin/coinone

Mercado



Biconomy Ativar /var/www/fakes/bitcoin/biconomy	Poloniex Desativar /var/www/fakes/bitcoin/poloniex	Pago Desativar /var/www/fakes/bank/mercadopago	Kraken Desativar /var/www/fakes/bitcoin/kraken	Huobi Ativar /var/www/fakes/bitcoin/huobi	Ftx Desativar /var/www/fakes/bitcoin/ftx
maxsize Ativar /var/www/fakes/maxsize	Banese Desativar /var/www/fakes/bank/banese	Royal Bank Ativar /var/www/fakes/bank/RoyalBank	Novo Banco PT Desativar /var/www/fakes/bank/pt/novobanco	Poloniex Ativar /var/www/fakes/btc/poloniex	Stone Desativar /var/www/fakes/bank/stone
Email Bol Desativar /var/www/fakes/mail/bol	Gemini Desativar /var/www/fakes/bitcoin/gemini	Coinbase Exchange Ativar /var/www/fakes/bitcoin/coinbase	Bybit Desativar /var/www/fakes/bitcoin/bybit	Bitay Ativar /var/www/fakes/bitcoin/bitay	Bibox Desativar /var/www/fakes/bitcoin/bibox
Indodax Desativar /var/www/fakes/bitcoin/indodax	Gate.io Desativar /var/www/fakes/bitcoin/gate	Korbit Desativar /var/www/fakes/bitcoin/korbit	Banco Do Brasil Desativar /var/www/fakes/bank/bb	Bradesco Desativar /var/www/fakes/bank/brada	Bittrex Desativar /var/www/fakes/bitcoin/bittrex
BS2 Desativar /var/www/fakes/bank/bs2	Coinsbit Desativar /var/www/fakes/bitcoin/coinsbit	Mexc Desativar /var/www/fakes/bitcoin/mexc	MetaMask Desativar /var/www/fakes/bitcoin/metamask	Pancakeswap Desativar /var/www/fakes/bitcoin/pancakeswap	Tokocrypto Desativar /var/www/fakes/bitcoin/tokocrypto
Wazirx Desativar /var/www/fakes/bitcoin/wazirx	YoBit Desativar /var/www/fakes/bitcoin/yobit	Bitstamp Desativar /var/www/fakes/bitcoin/bitstamp	Google Account Desativar /var/www/fakes/mail/google	Bit2me Desativar /var/www/fakes/bitcoin/bit2me	Cakedefi Desativar /var/www/fakes/bitcoin/cakedefi
CoinDCX Desativar /var/www/fakes/bitcoin/coindcx	Giottus Desativar /var/www/fakes/bitcoin/giottus	Pousada Desativar /var/www/fakes/geral/pousadal	Coins PH Desativar /var/www/fakes/bitcoin/coinsph	Bitkub Desativar /var/www/fakes/bitcoin/bitkub	Polygon Desativar /var/www/fakes/bitcoin/polygon
Bitbns Desativar /var/www/fakes/bitcoin/bitbns	Kriptomat Desativar /var/www/fakes/bitcoin/kriptomat	Zipmex Desativar /var/www/fakes/bitcoin/zipmex	KuCoin Desativar /var/www/fakes/bitcoin/kucoin	IndoEx Desativar /var/www/fakes/bitcoin/indoex	Parque Aquatico Desativar /var/www/fakes/geral/parqueaquatico
Phemex Desativar /var/www/fakes/bitcoin/phemex	Hanbitco Desativar /var/www/fakes/bitcoin/hanbitco	Redir 01 Desativar /var/www/fakes/redir/01	Redir 02 Desativar /var/www/fakes/redir/02	Redir Desativar /var/www/fakes/redir/03	Redir 04 Desativar /var/www/fakes/redir/04
BigOne Desativar /var/www/fakes/bitcoin/bigone	Axie Infinity Desativar /var/www/fakes/bitcoin/axieinfinity	Webmail Desativar /var/www/fakes/mail/webmail	Globo Mail Desativar /var/www/fakes/mail/globomail	Uol Mail Desativar /var/www/fakes/mail/uolmail	Hotbit Desativar /var/www/fakes/bitcoin/hotbit
OKX Desativar /var/www/fakes/bitcoin/okx	Pag Bank Desativar /var/www/fakes/bank/pagbank	Bitcoiva Desativar /var/www/fakes/bitcoin/bitcoiva	Azbit Desativar /var/www/fakes/bitcoin/azbit	CITEX Desativar /var/www/fakes/bitcoin/citex	DigiFinex Desativar /var/www/fakes/bitcoin/digifinex
CoinW Desativar /var/www/fakes/bitcoin/coinw	BitMart Desativar /var/www/fakes/bitcoin/bitmart	AAX Desativar /var/www/fakes/bitcoin/aax	Deribit Desativar /var/www/fakes/bitcoin/deribit	Bitfinex Desativar /var/www/fakes/bitcoin/bitfinex	WhiteBIT Desativar /var/www/fakes/bitcoin



/whitebit

Hoo
/var/www/fakes/bitcoin/hoo

koinbazar
/var/www/fakes/bitcoin/koinbazar

VALR
/var/www/fakes/bitcoin/valr

Binance Wallet
/var/www/fakes/bitcoin/binancewallet

NDAX
/var/www/fakes/bitcoin/ndax

Wealthsimple
/var/www/fakes/bitcoin/wealthsimple

BingX
/var/www/fakes/bitcoin/bingx

Bitrue
/var/www/fakes/bitcoin/bitrue

Anchor Protocol
/var/www/fakes/bitcoin/anchorprotocol

Terra Station
/var/www/fakes/bitcoin/terrastation

Wirex
/var/www/fakes/bitcoin/wirex

Avalaunch
/var/www/fakes/bitcoin/avalaunch

Maiar
/var/www/fakes/bitcoin/maiar

Bkex
/var/www/fakes/bitcoin/bkex

Deepcoin
/var/www/fakes/bitcoin/deepcoin

Magic Eden
/var/www/fakes/bitcoin/magiceden

Conta Clicks
/var/www/fakes/geral/contaclicks

Bitvavo
/var/www/fakes/bitcoin/bitvavo

Cassino Stake
/var/www/fakes/bitcoin/cassinostake

Liquid
/var/www/fakes/bitcoin/liquid

Bitso
/var/www/fakes/bitcoin/bitso

Viacredi
/var/www/fakes/bank/viacredi

Credifoz
/var/www/fakes/bank/credifoz

credcrea
/var/www/fakes/bank/credcrea

Acredi
/var/www/fakes/bank/acredi

Americanas
/var/www/fakes/lojas/americanas

Americanas Auto
/var/www/fakes/lojas/americanas_auto

Net Empresa
/var/www/fakes/bank/netempresa

P2pb2b
/var/www/fakes/bitcoin/p2pb2b

BitFlyer
/var/www/fakes/bitcoin/bitflyer

Iupp
/var/www/fakes/ccs/iupp

Empregos
/var/www/fakes/geral/empregos

Rekeningku
/var/www/fakes/bitcoin/rekeningku

Paritex
/var/www/fakes/bitcoin/paritex

dYdX
/var/www/fakes/bitcoin/dydx

Hive OS
/var/www/fakes/bitcoin/hiveos

Chainlist
/var/www/fakes/bitcoin/chainlist

CTT
/var/www/fakes/pt-banks/ctt

i-Bank
/var/www/fakes/eu-banks/ibank

Piraeus Bank
/var/www/fakes/eu-banks/piraeus

Banco BPM
/var/www/fakes/eu-banks/bpm

Millennium
/var/www/fakes/eu-banks/millennium

Banco Montepio
/var/www/fakes/eu-banks/montepio

MB Way
/var/www/fakes/eu-banks/mbway

coinspot
/var/www/fakes/bitcoin/coinspot

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.

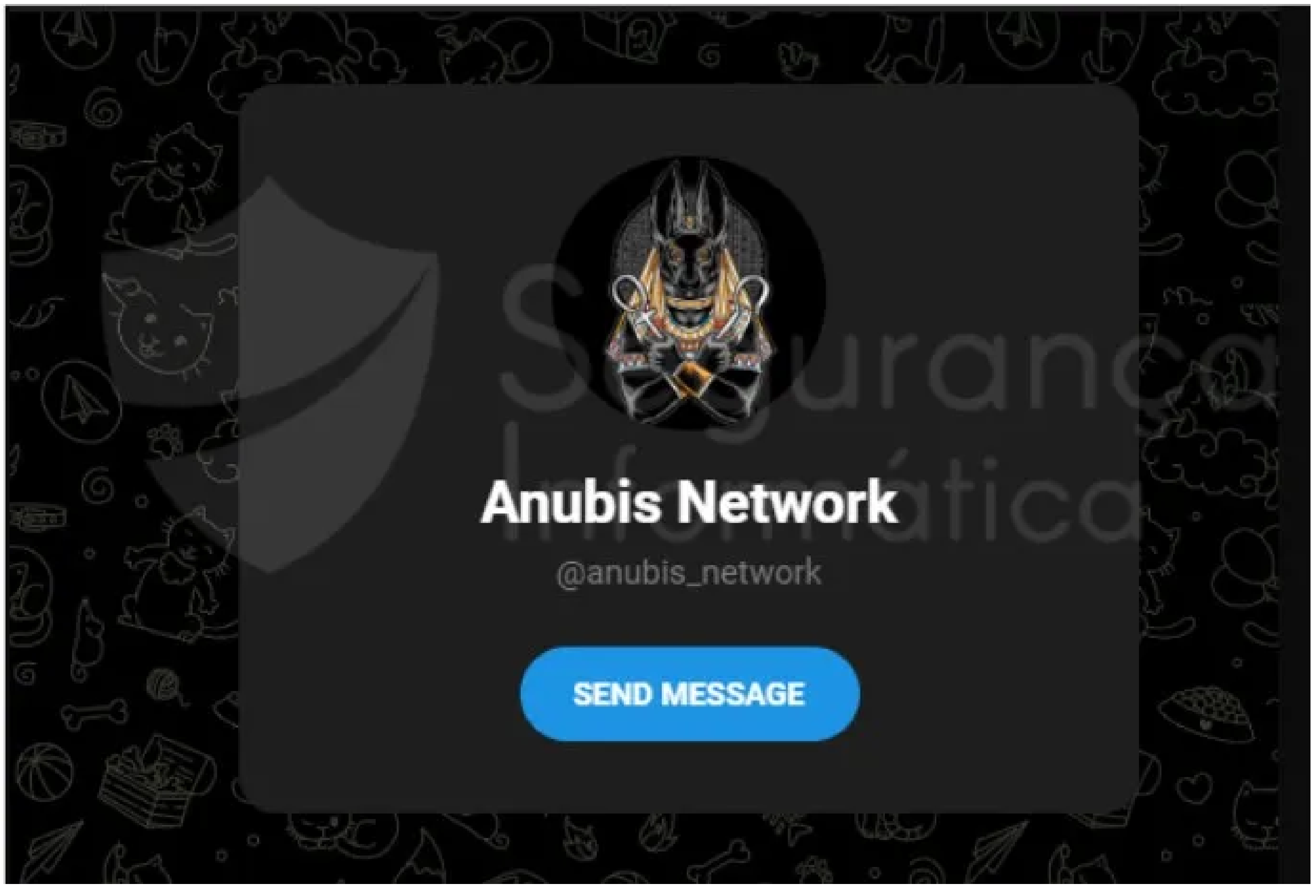
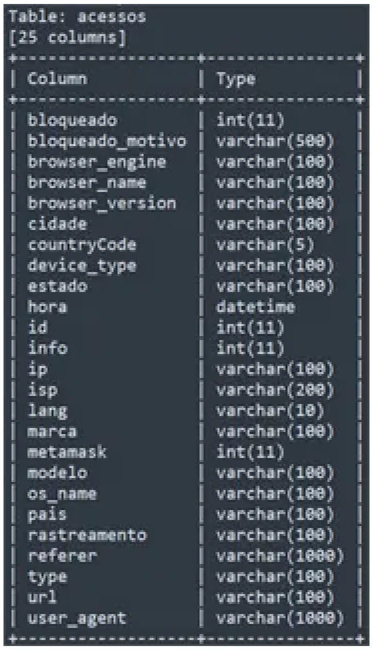


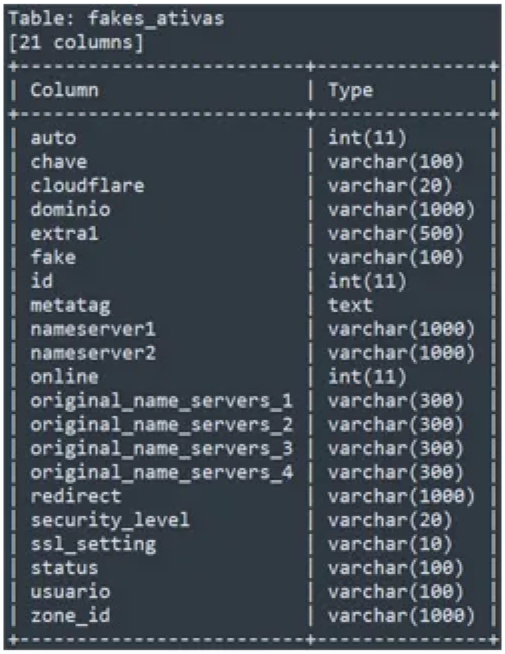
Figure 14: *Telegram channel created as a technical support channel.*

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.

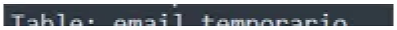


```
Table: acessos
[25 columns]
+------------------+---------------+
| Column           | Type          |
+------------------+---------------+
| bloqueado        | int(11)       |
| bloqueado_motivo | varchar(500)  |
| browser_engine   | varchar(100)  |
| browser_name     | varchar(100)  |
| browser_version  | varchar(100)  |
| cidade           | varchar(100)  |
| countryCode      | varchar(5)    |
| device_type      | varchar(100)  |
| estado           | varchar(100)  |
| hora             | datetime      |
| id               | int(11)       |
| info             | int(11)       |
| ip               | varchar(100)  |
| isp              | varchar(200)  |
| lang             | varchar(10)   |
| marca            | varchar(100)  |
| metamask         | int(11)       |
| modelo           | varchar(100)  |
| os_name          | varchar(100)  |
| pais             | varchar(100)  |
| rastreamento     | varchar(100)  |
| referer          | varchar(1000) |
| type             | varchar(100)  |
| url              | varchar(100)  |
| user_agent       | varchar(1000) |
+------------------+---------------+
```

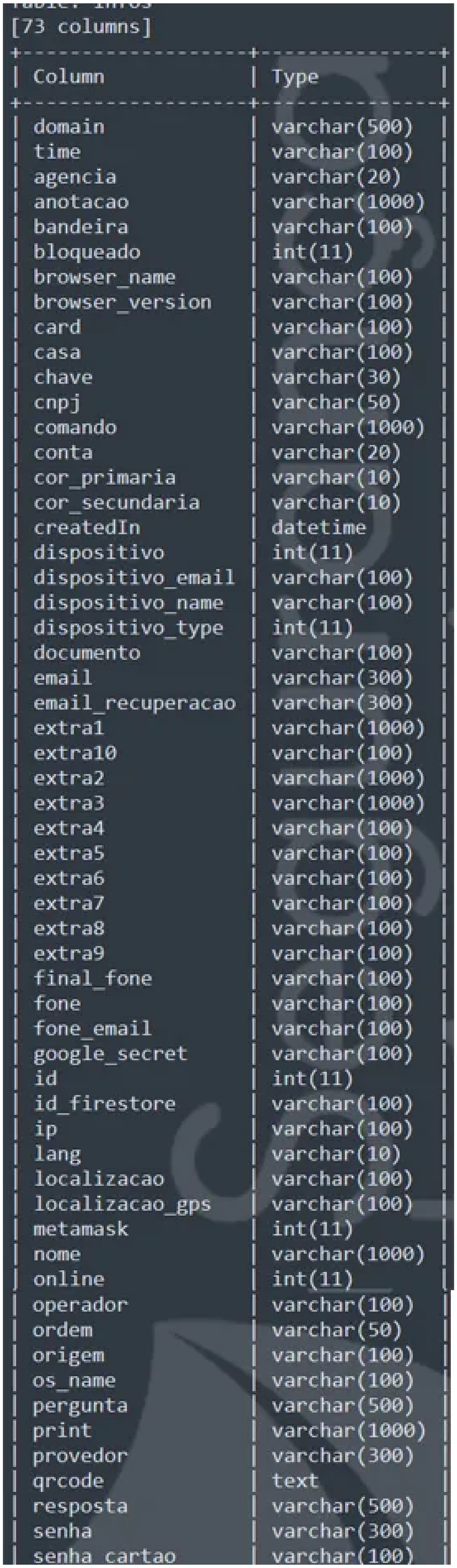


```
Table: fakes_ativas
[21 columns]
+-------------------------+---------------+
| Column                  | Type          |
+-------------------------+---------------+
| auto                    | int(11)       |
| chave                   | varchar(100)  |
| cloudflare              | varchar(20)   |
| dominio                 | varchar(1000) |
| extra1                  | varchar(500)  |
| fake                    | varchar(100)  |
| id                      | int(11)       |
| metatag                 | text          |
| nameserver1             | varchar(1000) |
| nameserver2             | varchar(1000) |
| online                  | int(11)       |
| original_name_servers_1 | varchar(300)  |
| original_name_servers_2 | varchar(300)  |
| original_name_servers_3 | varchar(300)  |
| original_name_servers_4 | varchar(300)  |
| redirect                | varchar(1000) |
| security_level          | varchar(20)   |
| ssl_setting             | varchar(10)   |
| status                  | varchar(100)  |
| usuario                 | varchar(100)  |
| zone_id                 | varchar(1000) |
+-------------------------+---------------+
```

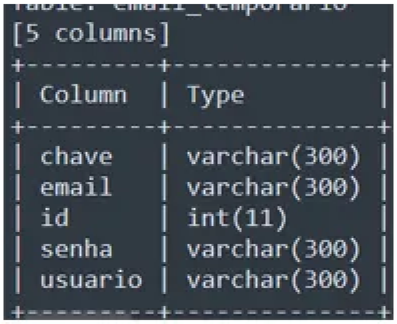
```
Table: infos
```



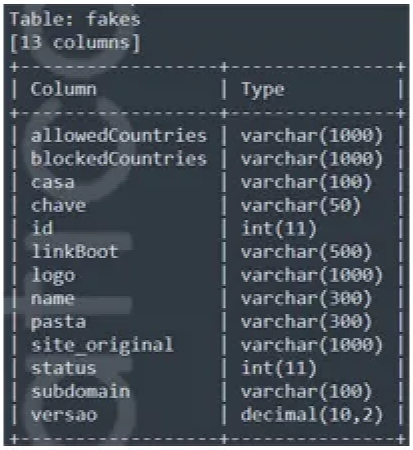
```
Table: email_temporario
```



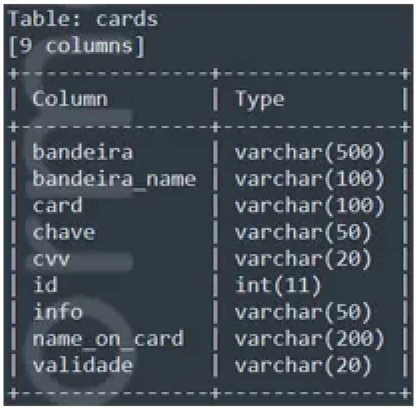
```
Table: infos
[73 columns]
+-------------------+---------------+
| Column            | Type          |
+-------------------+---------------+
| domain            | varchar(500)  |
| time              | varchar(100)  |
| agencia           | varchar(20)   |
| anotacao          | varchar(1000) |
| bandeira          | varchar(100)  |
| bloqueado         | int(11)       |
| browser_name      | varchar(100)  |
| browser_version   | varchar(100)  |
| card              | varchar(100)  |
| casa              | varchar(100)  |
| chave             | varchar(30)   |
| cnpj              | varchar(50)   |
| comando           | varchar(1000) |
| conta             | varchar(20)   |
| cor_primaria      | varchar(10)   |
| cor_secundaria    | varchar(10)   |
| createdIn         | datetime      |
| dispositivo       | int(11)       |
| dispositivo_email | varchar(100)  |
| dispositivo_name  | varchar(100)  |
| dispositivo_type  | int(11)       |
| documento         | varchar(100)  |
| email             | varchar(300)  |
| email_recuperacao | varchar(300)  |
| extra1            | varchar(1000) |
| extra10           | varchar(100)  |
| extra2            | varchar(1000) |
| extra3            | varchar(1000) |
| extra4            | varchar(100)  |
| extra5            | varchar(100)  |
| extra6            | varchar(100)  |
| extra7            | varchar(100)  |
| extra8            | varchar(100)  |
| extra9            | varchar(100)  |
| final_fone        | varchar(100)  |
| fone              | varchar(100)  |
| fone_email        | varchar(100)  |
| google_secret     | varchar(100)  |
| id                | int(11)       |
| id_firestore      | varchar(100)  |
| ip                | varchar(100)  |
| lang              | varchar(10)   |
| localizacao       | varchar(100)  |
| localizacao_gps   | varchar(100)  |
| metamask          | int(11)       |
| nome              | varchar(1000) |
| online            | int(11)       |
| operador          | varchar(100)  |
| ordem             | varchar(50)   |
| origem            | varchar(100)  |
| os_name           | varchar(100)  |
| pergunta          | varchar(500)  |
| print             | varchar(1000) |
| provedor          | varchar(300)  |
| qrcode            | text          |
| resposta          | varchar(500)  |
| senha             | varchar(300)  |
| senha_cartao      | varchar(100)  |
```



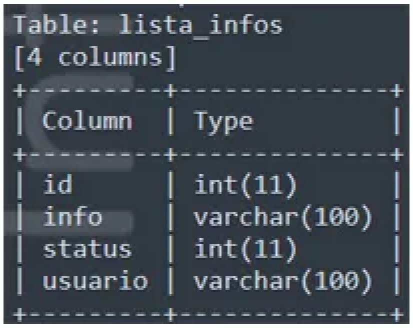
```
Table: email_temporario
[5 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| chave   | varchar(300) |
| email   | varchar(300) |
| id      | int(11)      |
| senha   | varchar(300) |
| usuario | varchar(300) |
+---------+--------------+
```



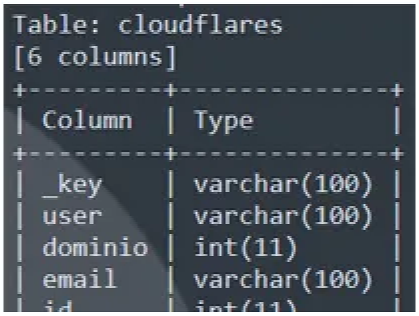
```
Table: fakes
[13 columns]
+-------------------+---------------+
| Column            | Type          |
+-------------------+---------------+
| allowedCountries  | varchar(1000) |
| blockedCountries  | varchar(1000) |
| casa              | varchar(100)  |
| chave             | varchar(50)   |
| id                | int(11)       |
| linkBoot          | varchar(500)  |
| logo              | varchar(1000) |
| name              | varchar(300)  |
| pasta             | varchar(300)  |
| site_original     | varchar(1000) |
| status            | int(11)       |
| subdomain         | varchar(100)  |
| versao            | decimal(10,2) |
+-------------------+---------------+
```



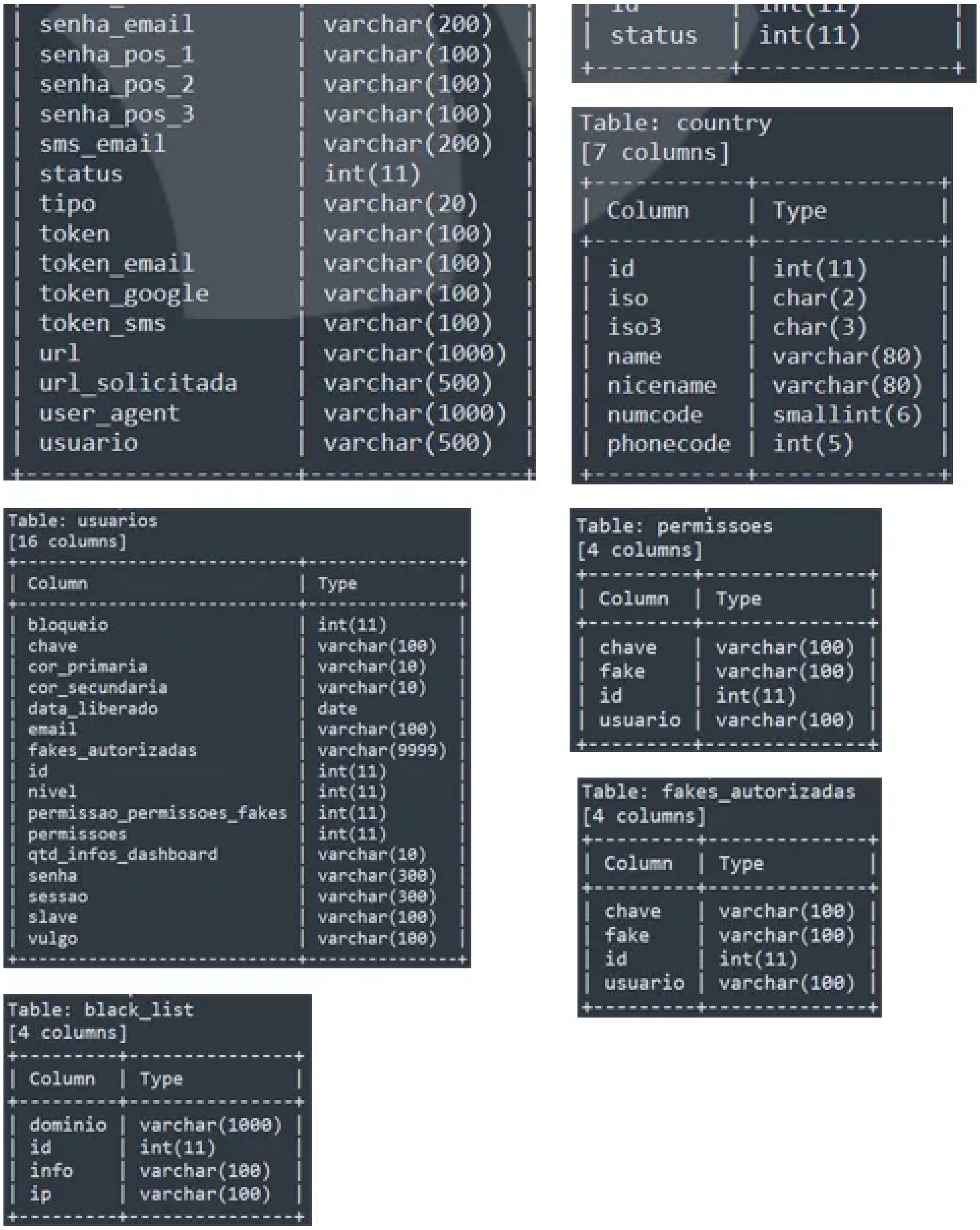
```
Table: cards
[9 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| bandeira      | varchar(500) |
| bandeira_name | varchar(100) |
| card          | varchar(100) |
| chave         | varchar(50)  |
| cvv           | varchar(20)  |
| id            | int(11)      |
| info          | varchar(50)  |
| name_on_card  | varchar(200) |
| validade      | varchar(20)  |
+---------------+--------------+
```



```
Table: lista_infos
[4 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| id      | int(11)      |
| info    | varchar(100) |
| status  | int(11)      |
| usuario | varchar(100) |
+---------+--------------+
```



```
Table: cloudflares
[6 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| _key    | varchar(100) |
| user    | varchar(100) |
| dominio | int(11)      |
| email   | varchar(100) |
| id      | int(11)      |
```



```
| senha_email        | varchar(200)  |
| senha_pos_1        | varchar(100)  |
| senha_pos_2        | varchar(100)  |
| senha_pos_3        | varchar(100)  |
| sms_email          | varchar(200)  |
| status             | int(11)       |
| tipo               | varchar(20)   |
| token              | varchar(100)  |
| token_email        | varchar(100)  |
| token_google       | varchar(100)  |
| token_sms          | varchar(100)  |
| url                | varchar(1000) |
| url_solicitada     | varchar(500)  |
| user_agent         | varchar(1000) |
| usuario            | varchar(500)  |
+--------------------+---------------+
```

```
Table: usuarios
[16 columns]
+----------------------------+---------------+
| Column                     | Type          |
+----------------------------+---------------+
| bloqueio                   | int(11)       |
| chave                      | varchar(100)  |
| cor_primaria               | varchar(10)   |
| cor_secundaria             | varchar(10)   |
| data_liberado              | date          |
| email                      | varchar(100)  |
| fakes_autorizadas          | varchar(9999) |
| id                         | int(11)       |
| nivel                      | int(11)       |
| permissao_permissoes_fakes | int(11)       |
| permissoes                 | int(11)       |
| qtd_infos_dashboard        | varchar(10)   |
| senha                      | varchar(300)  |
| sessao                     | varchar(300)  |
| slave                      | varchar(100)  |
| vulgo                      | varchar(100)  |
+----------------------------+---------------+
```

```
Table: black_list
[4 columns]
+---------+---------------+
| Column  | Type          |
+---------+---------------+
| dominio | varchar(1000) |
| id      | int(11)       |
| info    | varchar(100)  |
| ip      | varchar(100)  |
+---------+---------------+
```

```
| id        | int(11)       |
| status    | int(11)       |
+-----------+---------------+
```

```
Table: country
[7 columns]
+-----------+--------------+
| Column    | Type         |
+-----------+--------------+
| id        | int(11)      |
| iso       | char(2)      |
| iso3      | char(3)      |
| name      | varchar(80)  |
| nicename  | varchar(80)  |
| numcode   | smallint(6)  |
| phonecode | int(5)       |
+-----------+--------------+
```

```
Table: permissoes
[4 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| chave   | varchar(100) |
| fake    | varchar(100) |
| id      | int(11)      |
| usuario | varchar(100) |
+---------+--------------+
```

```
Table: fakes_autorizadas
[4 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| chave   | varchar(100) |
| fake    | varchar(100) |
| id      | int(11)      |
| usuario | varchar(100) |
+---------+--------------+
```

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

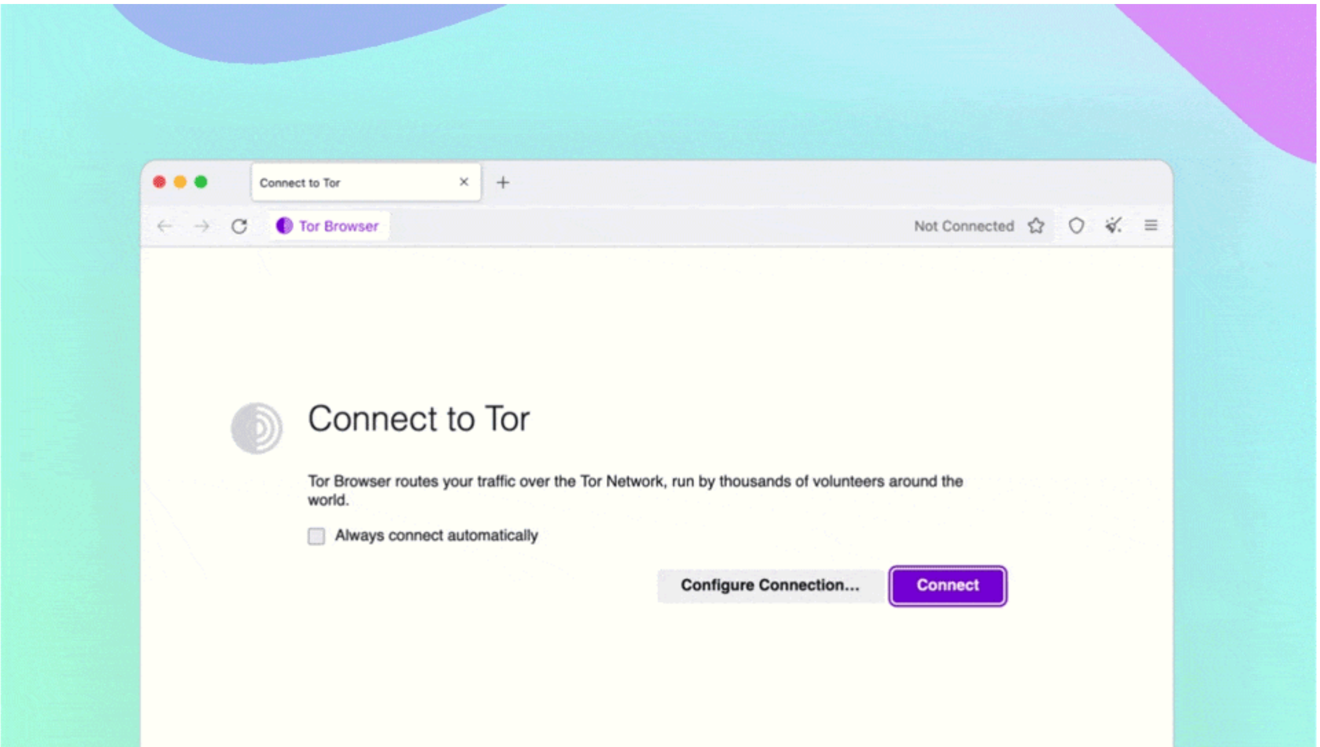
About the author: Pedro Tavarez

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.

Pierluigi Paganini

(SecurityAffairs – hacking, Anubis)

You might also like



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

Tor Browser 11.5 is optimized to automatically bypass censorship

July 18, 2022 By Pierluigi Paganini

A massive cyberattack hit Albania

July 18, 2022 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA