

# Lampion trojan disseminated in Portugal using COVID-19 template

[seguranca-informatica.pt/lampion-trojan-disseminated-in-portugal-using-covid-19-template/](https://seguranca-informatica.pt/lampion-trojan-disseminated-in-portugal-using-covid-19-template/)

February 10, 2021

**The fresh release of the Latin American Lampion trojan was updated with a new C2 address. Lampion trojan disseminated in Portugal using COVID-19 template.**

In the last few days, a new release of the Latin American Lampion trojan was released in Portugal using a template related to COVID-19. This trojan has been distributed in Portugal in different ways, but this time the pandemic situation and the ongoing vaccination process is the reason behind this campaign to drop the beast in the wild.

In detail, the threat is impersonating the domain “*min-saude.pt*” and the link to the zip file is also distributed in the email body.

Comunicado-Covid19-Min-Saude-VRC-03-02-21-210.zip

Ariane.Tabosa.Belo.863@covid19.min-saude.pt sent you 1 file(s) (109.56 KB) via pCloud Transfer

Files (109.56 KB)

– Comunicado-Covid19-Min-Saude-VRC-03-02-21-210.zip

"Bom dia, Exmo.(a). Senhor(a) [redacted] Vimos, pela presente, informar que o Serviço Nacional de Saúde seleccionou-lhe para o - Plano de Vacinação contra a COVID-19 - Primeira Fase - Seguem em anexo todos os dados e informações necessárias seguindo o calendário de distribuição das vacinas. Seu número de adesão:7M4M76C. A Vacina não dispensa medidas de protecção da COVID-19 .Dep. de Comunicação SNS - Ariane Tabosa Belo. 04/02/2021 09:42:57."

pCloud Transfer

Files are ready to download

1 file

Comunicado-Covid19-Min-Saude-VRC-03-02-21-210.zip	109.6 KB
---	----------

DOWNLOAD

Compartilhar Download Inscreva-se

Selecione uma pasta ou arquivo para ver as opções

Nome do Arquivo	Tamanho	Modificado
<input type="checkbox"/> Comunicado-Covid19-Min-Saude-VRC-03-02-21-210.zip	109.6 KB	04/02/2021

1 itens

The *modus operandi* is the same as observed in **previous releases**, only the addresses of the DLLs used during the side-loading process and C2 server geolocalized in Russia have been changed.

## DLLs used during the DLL side-loading process downloaded from Google storage

```
encrypted_string="n\s^[j]jef9ig0`%Y%|ipjweWh+WM]2[W$}MeRee]8bc[{W<f6_$iH$iYLe]c|%  
[email_protected];h/w*]M[o(g&c(_'P%=FZ#R(I#1'8/'$dZtb^b0g"  
decrypted_string="hxxps://storage.googleapis.]com/mystorage2021/P-2-19.dll"
```

```
encrypted_string="iP/^*j6jvfpiV00%A%*i;j+eLh(W\K[N$0];e.ep]&br[gW+f/_)ik$+Y&excs%=cJc  
decrypted_string="hxxps://storage.googleapis.]com/mystorage2021/0.zip"
```

When the malware is executed, it communicates with the C2 server and the browser overlay process begins every time a target home banking portal is accessed on the victim side.

```
0x4e7e210 (22): <|AppClip|>
<br />0x4e7e344 (38): Server Mandou====> <br />0x4e7e37c (36): <|FECHAR_RECORTE|>
<br />0x4e7e3b0 (72): Server manda====> Fecahando Recorte!
<br />0x4e7e408 (30): <|ALINHA_TELA|>
<br />0x4e7e434 (34): ServRecebeu====> <br />0x4e7e474 (8): ><|>
<br />0x4e7e4b4 (40): ClienteRecebeu====> <br />0x4e7e500 (44): Erro Encontrado====>
```

```
0x4e71f98 (28): banco montepio
0x4e71fc4 (16): montepio
0x4e71ff8 (26): millenniumbcp
0x4e72034 (18): Santander
0x4e72054 (14): BPI Net
0x4e72070 (18): Banco BPI
0x4e720a4 (24): Caixadirecta
0x4e720cc (42): Caixadirecta Empresas
0x4e72118 (20): NOVO BANCO
0x4e72150 (14): EuroBic
0x4e72186 (16): Credito Agricola
0x4e721b0 (20): Login Page
0x4e721d4 (22): CA Empresas
0x4e7220c (18): Bankinter
0x4e72240 (38): navegador exclusivo
0x4e74abc (14): TravaBB
0x4e74ada (32): Banco do Brasil
0x4e74b08 (16): Traazure
0x4e74b2a (32): Caixa Economica
0x4e74b58 (20): Travsantos
0x4e74b7e (20): Santander
0x4e74ba0 (14): Travsic
0x4e74bbe (14): Sicred
0x4e74bdc (14): Travite
0x4e74bfa (8): Ita
0x4e74c14 (18): Travdesco
0x4e74c36 (18): Bradesco
0x4e74c58 (22): BANRITRAVAR
0x4e74c7e (18): Banrisul
0x4e74ca0 (20): TravaBitco
0x4e74cc6 (32): Mercado Bitcoin
0x4e74cf4 (14): Travcit
0x4e74d12 (18): Citibank
0x4e74d34 (18): Travorigs
0x4e74d56 (30): Banco Original
0x4e74d84 (18): SICTRAVAR
0x4e74da6 (14): Sicoob
```

## Communication process

---

```

0x64d637c (246): <|Info|><|>Microsoft Windows 10 Home (64)bit<|><|><|>
<<|@[email_protected]|DESKTOP-xxxxxxx - xxxx|Microsoft Windows 10 Home
(64)bit||MP|N
0x64d6474 (108): 0|210X|..|FF|#####00000000|5.188.9.28||@[email_protected].
0x64d64fc (360):
##35977722363232BA77922081E8A8B11D252207F6A#####173E26057E4840ABCD03FFE2D3BAC

0x64d667c (364):
##35977722363232BA77922081E8A8B11D252207F#####A0053CCA9187D90E173E26057E4840

0x64dc5cc (264):
##35977722363232BA77922081E8A8B11D252207F#####90E173E26057E4840ABCD0##
0x64dc6ec (260):
44A46F92B11004144D5DFA2DF86AAF66#####C8690B55C83A03225F22BBC12B17BDD3AD94E

```

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host
22	UDP						
23	TCP		5.188.9.28	51959	9171	DESKTOP-...	

```

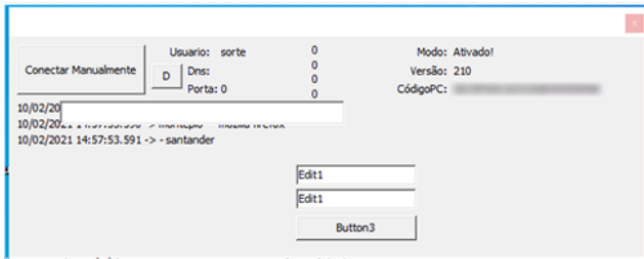
##7313373: 1FC6009A8B7BECEEE85##
##3394352: 0FD54#####23744367173335C380884
##3597772: 22081E8A8B11D252207F6A8607780#####9A22F334746F16F5F1EEDB5
##7093714: D1B4DADE9##
##2022170: 3327DD3DB##
##7694841: C6115FECE##
##2786424: 3F9F22389##
##6329835: F47169721##
##4351289: 0C18F85C3##
##2113954: 038A87926E0#####30534655527137AB02D0195B813D##
##9577334: E18C39AC2##
##3487903: 2DCF34266##
##8453245: 962E61548##
##7138130: C7051D320##

```

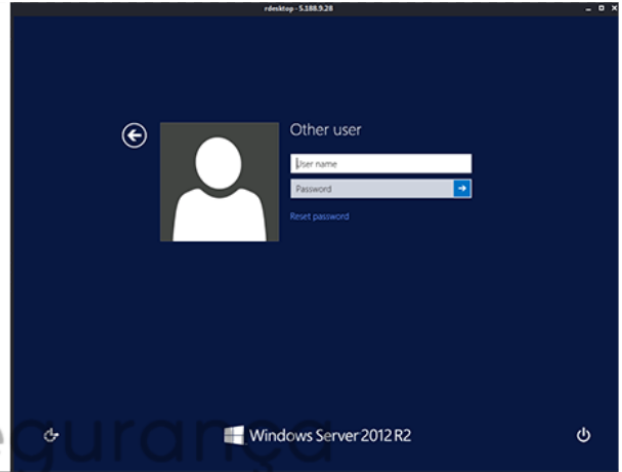


## C2 server geolocated in Russia

C2: 5.188.9.]28



0x64e4d54 (74): No NOVO BANCO a privacidade e a prote  
 0x64e4da2 (166): o dos dados pessoais dos seus clientes e dos demais  
 titulares de dados pessoais s  
 0x64e4e4a (538): o fundamentais. Saiba como tratamos os seus dados, com quem  
 os partilhamos, durante quanto tempo os conservamos, bem como as formas de entrar em  
 contacto com o NOVO BANCO e de exercer os seus direitos.  
 O NOVO BANCO apenas recolhe e trata os dados pessoais neces  
 0x64e5066 (64): rios para lhe prestar um  
 servi  
 0x64e50a8 (84): o de qualidade e o mais personalizado poss  
 0x64e50fe (44): vel, enquanto Institui  
 0x64e512e (14): o de Cr  
 0x64e513e (34): dito,  
 Intermedi  
 0x64e5162 (104): rio Financeiro e Mediador de Seguros. O NOVO BANCO n



**5.188.9.28** View Raw Data

self signed

Country	Russia
Organization	Petersburg Internet Network Hosting
ISP	Petersburg Internet Network Hosting
Last Update	2021-02-01T15:10:23.595186
ASN	AS34665

**Ports**

135 3389 5985

**Services**

**135** Microsoft RPC Endpoint Mapper  
 tcp  
 ms-portmap-tcp  
 DCE/RPC Endpoint Mapper  
 Max Count: 500  
 Actual Count: 267  
 Number of Entries: 267

## Banking overlay windows

<p><b>Millennium</b> bcp</p> <p><b>Atualização do módulo de Segurança</b></p> <p><b>Trusteer</b> an IBM Company</p> <p>Estimado cliente:</p> <p>O módulo de segurança é um sistema de proteção que, durante a execução de transações eletrônicas, atua como escudo para o seu computador contra ataques de programas maliciosos na internet.</p> <ul style="list-style-type: none"> <li>✓ 1: Configurações iniciais</li> <li>✓ 2: Ambiente de configuração</li> <li>✓ 3: Verificando instalações anteriores</li> <li>✓ 4: Preparação de atualizações do módulo de segurança</li> <li>⌚ 5: Instalando a atualização do componente de segurança</li> </ul> <p>A atualização pode levar alguns minutos para ser concluída. Para garantir sua segurança durante o processo, alguns dados serão solicitados.</p> <p><b>AVISO: Não desligue ou desconecte o computador até que a atualização esteja concluída, caso contrário, poderá danificar os arquivos do sistema.</b></p>	<p><b>CA</b> Crédito Agrícola</p> <p><b>Atualização do módulo de Segurança</b></p> <p><b>Trusteer</b> an IBM Company</p> <p>Estimado cliente:</p> <p>O módulo de segurança é um sistema de proteção que, durante a execução de transações eletrônicas, atua como escudo para o seu computador contra ataques de programas maliciosos na internet.</p> <ul style="list-style-type: none"> <li>✓ 1: Configurações iniciais</li> <li>✓ 2: Ambiente de configuração</li> <li>✓ 3: Verificando instalações anteriores</li> <li>✓ 4: Preparação de atualizações do módulo de segurança</li> <li>⌚ 5: Instalando a atualização do componente de segurança</li> </ul> <p>A atualização pode levar alguns minutos para ser concluída. Para garantir sua segurança durante o processo, alguns dados serão solicitados.</p> <p><b>AVISO: Não desligue ou desconecte o computador até que a atualização esteja concluída, caso contrário, poderá danificar os arquivos do sistema.</b></p>
<p><b>Banco Montepio</b></p> <p><b>Atualização do módulo de Segurança</b></p> <p><b>Trusteer</b> an IBM Company</p> <p>Estimado cliente:</p> <p>O módulo de segurança é um sistema de proteção que, durante a execução de transações eletrônicas, atua como escudo para o seu computador contra ataques de programas maliciosos na internet.</p> <ul style="list-style-type: none"> <li>✓ 1: Configurações iniciais</li> <li>✓ 2: Ambiente de configuração</li> <li>✓ 3: Verificando instalações anteriores</li> <li>✓ 4: Preparação de atualizações do módulo de segurança</li> <li>⌚ 5: Instalando a atualização do componente de segurança</li> </ul> <p>A atualização pode levar alguns minutos para ser concluída. Para garantir sua segurança durante o processo, alguns dados serão solicitados.</p> <p><b>AVISO: Não desligue ou desconecte o computador até que a atualização esteja concluída, caso contrário, poderá danificar os arquivos do sistema.</b></p>	<p><b>NOVO BANCO</b></p> <p><b>Atualização do módulo de Segurança</b></p> <p><b>Trusteer</b> an IBM Company</p> <p>Estimado cliente:</p> <p>O módulo de segurança é um sistema de proteção que, durante a execução de transações eletrônicas, atua como escudo para o seu computador contra ataques de programas maliciosos na internet.</p> <ul style="list-style-type: none"> <li>✓ 1: Configurações iniciais</li> <li>✓ 2: Ambiente de configuração</li> <li>✓ 3: Verificando instalações anteriores</li> <li>✓ 4: Preparação de atualizações do módulo de segurança</li> <li>⌚ 5: Instalando a atualização do componente de segurança</li> </ul> <p>A atualização pode levar alguns minutos para ser concluída. Para garantir sua segurança durante o processo, alguns dados serão solicitados.</p> <p><b>AVISO: Não desligue ou desconecte o computador até que a atualização esteja concluída, caso contrário, poderá danificar os arquivos do sistema.</b></p>

## Indicators of Compromise (IOCs)

sample: A0217751E21918083A8B9A6DD3916EDD

<https://app.any.run/tasks/d3d7faf4-1d88-449a-812b-d34714ecf924/>

Zip file: [https://transfer.pcloud.com/download.html?](https://transfer.pcloud.com/download.html?code=5Z3YkhXZI6WMHp985xzZaomKZG0Mp6DsTf9jKump5wPGz1VLzHrJV&label=Transfer%20-%20files%20sent%20(to%20recipient)#)

[code=5Z3YkhXZI6WMHp985xzZaomKZG0Mp6DsTf9jKump5wPGz1VLzHrJV&label=Transfer%20-%20files%20sent%20\(to%20recipient\)#](https://transfer.pcloud.com/download.html?code=5Z3YkhXZI6WMHp985xzZaomKZG0Mp6DsTf9jKump5wPGz1VLzHrJV&label=Transfer%20-%20files%20sent%20(to%20recipient)#)

DLLs:

<https://storage.googleapis.com/mystorage2021/0.zip>

<https://storage.googleapis.com/mystorage2021/P-2-19.dll>

C2 server - RUSSIA - :

5.188.9.]28



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](http://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](#).