



Evolución del malware bancario y ataques dirigidos a usuarios en España

Josep Albors

Responsable de Investigación y Concienciación
ESET España

BackSwap: Troyano bancario con objetivos españoles

The background is a dark, teal-toned digital landscape. On the left, several bright blue, glowing lines curve upwards and outwards, resembling data streams or network connections. On the right, a close-up, angled view of a computer keyboard is visible, with many keys illuminated by a blue light, suggesting a digital or cyber environment.

Evolución de BackSwap

Proyecto anterior:

- Troyano bancario convencional

Proyecto inicial:

- Robo de datos del portapapeles
- Cuentas bancarias y carteras de criptomonedas como objetivos

Proyecto principal:

- Inyecciones web en sistemas de pago y exchanges de criptomonedas
- Inyecciones web en usuarios de banca online

Características recientes:

- Recopilación de datos introducidos en formularios a través del portapapeles

BackSwap malware finds innovative ways to empty bank accounts

ESET researchers have discovered a piece of banking malware that employs a new technique to bypass dedicated browser protection measures



Michal Poslušný 25 May 2018 - 12:58PM

BackSwap malware campaign evolution

Posted 15 July, 2019 In [Sin categoría](#) | [0 comentarios](#).



BackSwap malware campaign evolution

This article will explain in detail the follow-up that the S21sec Threat Intelligence team has carried out since the BackSwap malware was discovered by ESET in May 2018, as well as the different campaigns that the group behind BackSwap has carried out towards financial institutions from different countries, cryptocurrency exchanges, and its new evolution after a few months of inactivity.

Affectation to Spanish financial firms

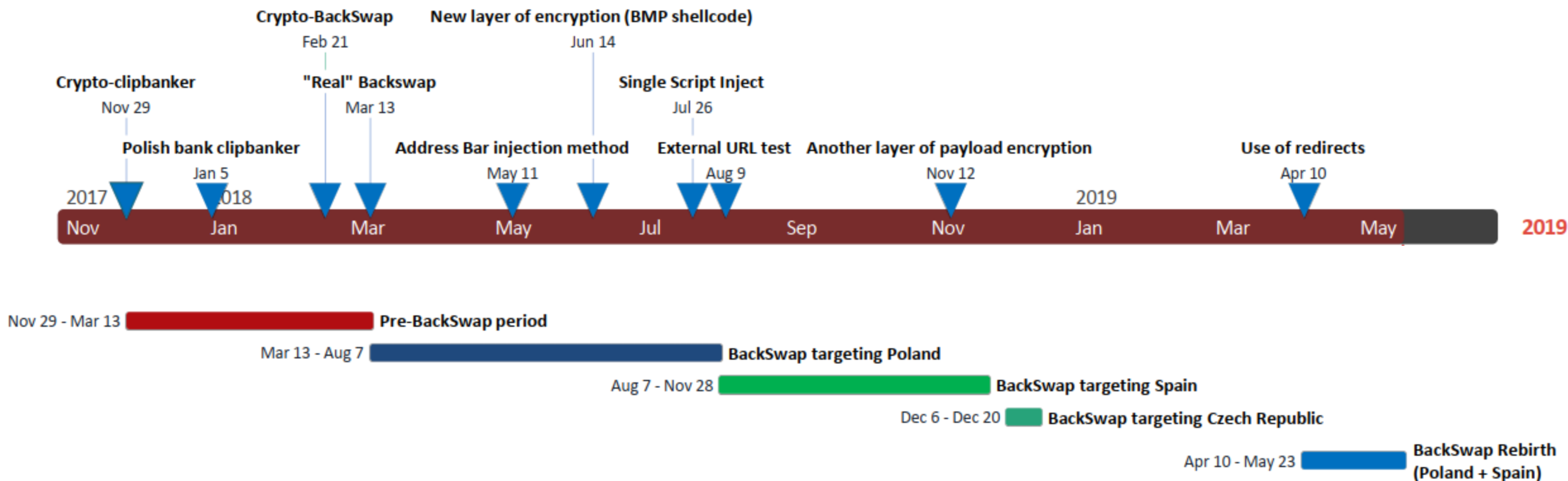




Michal
Poslušný



Peter
Kálnai



BackSwap afectando a España

Primera campaña
Agosto - Diciembre 2018

Aplicaciones legítimas modificadas



7zFM



Dbgview



WinRAR



wingraph32



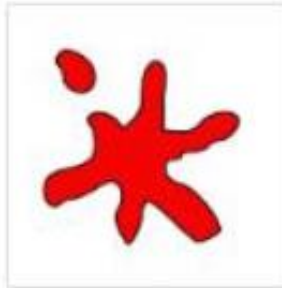
irfanview32



Intel Graphics



steam



ollydbg



SQLmon



FlashFXP



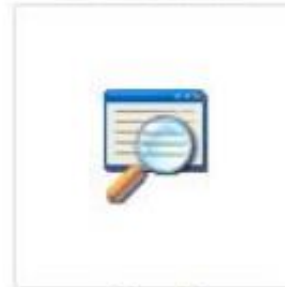
SeaMonkey



FileZilla



cdshot



ZoomIt



Rootkitrevealer



Steganos



ConEmu



Disk2vhd



Driver Update



Dxdiag



Kaspersky Antivirus
19.0



Notepad++

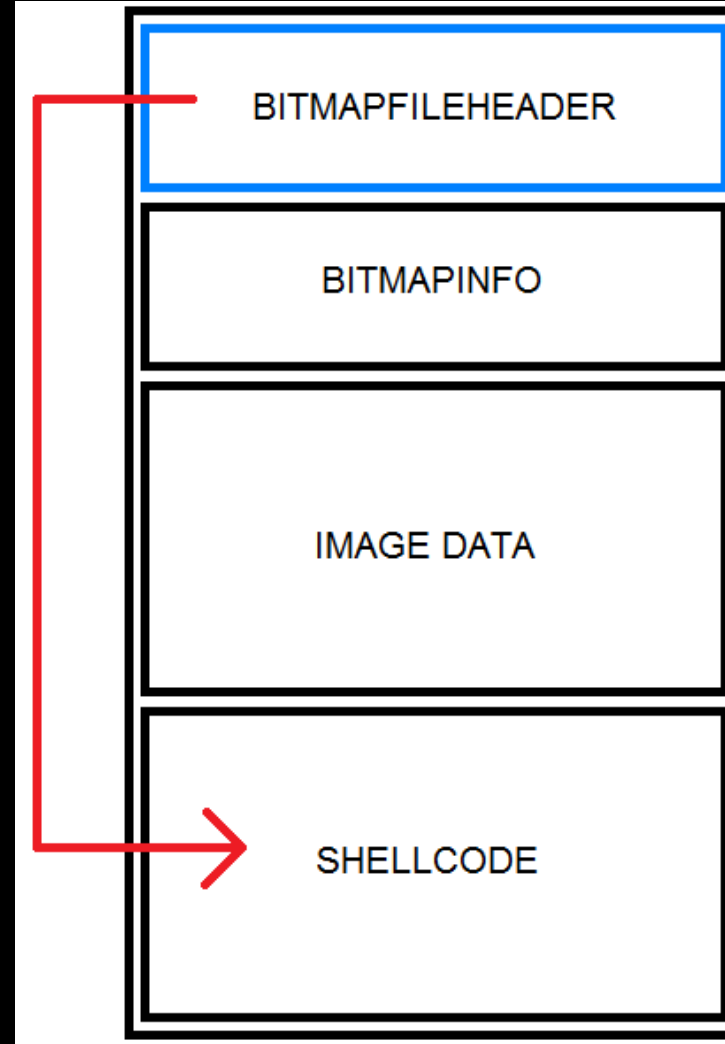
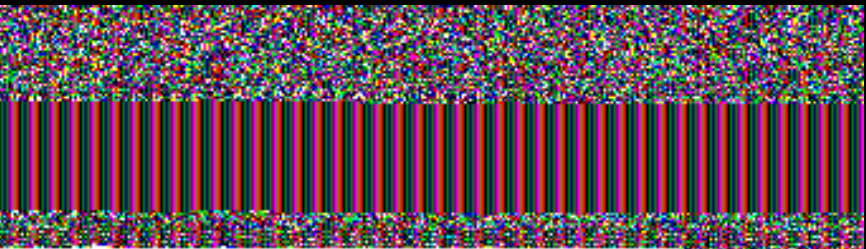


TPVCGateway



WinObj

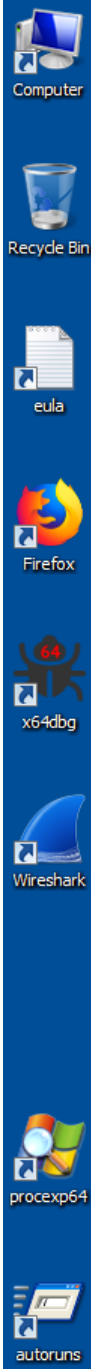
Shellcode en imágenes BMP



42 4D	bftype	db	'BM'
E9 8C 6D 00	bfsiz	dd	6D8CE9h
00 00	bfrserved1	dw	0
00 00	bfrserved2	dw	0
76 00 00 00	bfoffbits	dd	76h

42	bftype:	inc	edx
4D		dec	ebp

E9 8C 6D 00 00	bfsiz:	jmp	loc_1C6D93
00			
00	bfrserved2	db	0
00		db	0
76	bfoffbits	db	76h ; v
00		db	0
00		db	0
00		db	0



```
Administrator: Command Prompt - BackSwapInjectEmulator.exe webinject_BBVA.js
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>cd c:\tools

c:\tools>BackSwapInjectEmulator.exe
Please provide valid arguments
Usage: [script_path] [inject_url (optional)]

c:\tools>BackSwapInjectEmulator.exe webinject_BBVA.js
```

```
*new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
[Icons]
new 1 x
1
length: 0 lines: 1 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

Google

← → ↻ https://www.google.com

Gmail Images

Google

Google Search

I'm Feeling Lucky

Google offered in: [čeština](#)

Czechia

Advertising

Business

About

Privacy Te



```
Administrator: Command Prompt - BackSwapInjectEmulator.exe webinject_BBVA.js
c:\tools>BackSwapInjectEmulator.exe
Please provide valid arguments
Usage: [script_path] [inject_url (optional)]

c:\tools>BackSwapInjectEmulator.exe webinject_BBVA.js
URL Accessed: https://www.google.com/?gws_rd=ssl
```

```
*new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1 x
1
length: 0 lines: 1 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

Google

← → ↻ 🔒 https://www.google.com/?gws_rd=ssl ☆ 👤 ⋮

Gmail Images

Google

Google Search I'm Feeling Lucky

Google offered in: čeština

🛡️

A privacy reminder from Google

REMIND ME LATER

Czechia

Advertising Business About

Privacy



```
Administrator: Command Prompt - BackSwapInjectEmulator.exe webinject_BBVA.js
URL Accessed: https://www.google.com
URL Accessed: https://www.google.com
URL Accessed: https://www.google.com
URL Accessed: https://www.google.com
URL Accessed: https://w
URL Accessed: https://ww
URL Accessed: https://www.
URL Accessed: https://www.b
URL Accessed: https://www.bb
URL Accessed: https://www.bbva
URL Accessed: https://www.bbvan
URL Accessed: https://www.bbvanet
```

```
*new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1 x
1
length: 0 lines: 1 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

Google

← → ↻

https://www.bbvanet

<https://www.bbvanet>

<https://www.bbvanet.com.co>

https://www.bbvanet - Google Search

<https://www.bbvanetcash.com>

<https://www.bbvanetcash.com.co>

<https://www.bbvanetoffice.com>

Google

Google Search I'm Feeling Lucky

Google offered in: čeština

A privacy reminder from Google [REMIND ME LATER](#)

Czechia

Advertising Business About Privacy

Administrator: Command Prompt

```
URL Accessed: https://www.bbvanetcash.com
URL Accessed: https://www.bbvanetcash.com
URL Accessed: https://www.bbvanetcash.com
URL Accessed: https://www.bbvanetcash.com/local_kyop/login
URL Accessed: https://www.bbvanetcash.com/local_kyop/KYOPS
tml
Valid URL detected - injecting...
Injected!

c:\tools>BackSwapInjectEmulator.exe webinject_BBVA.js
URL Accessed: https://www.bbvanetcash.com/local_kyop/KYOPS
tml
Valid URL detected - injecting...
Injected!

c:\tools>
```

*new 1 - Notepad++ [Administrator]

```
cmd: %UID%&E=12349877&U=Victim&P=Hidden&D=
```

length: 41 lines: 1 ln: 1 col: 42 sel: 0 | 0

Windows (CR, LF) UTF-8 INS

rundll32.exe syssetup.SetupOo

For Windows 8, 8.1 and 10, you will NOT

Computer

Recycle Bin

eula

Firefox

x64dbg

Wireshark

procexp64

Procomon

autoruns

Process Hacker 2

BBVA Net cash

https://www.bbvanetcash.com/local_kyop/KYOPSolicitarCredenciales.html

Save password?

Username Victim

Password *****

Save Never

BBVA | Net cash

Atención al cliente | Catálogo de servicios | Demo | Español ▾

Acceso

Los datos introducidos son incorrectos, inténtelo de nuevo

Código de empresa

Usuario

Contraseña

☒ Recordar código de empresa y usuario

¿Olvidó su contraseña?

BBVA One View

Descubre cómo funciona

(Servicio de información de cuentas y otros productos financieros para clientes de BBVA)

Date	Targets	Attacker's Account number(s)	Hashes
2018-08-07	https://*bancopopular.es/eai_logon/GbpInternetLogonEAI/gbplogo* https://www.caixabank.es/particular* https://oi.bankia.es/es/logi* https://www.bankia.es/es/particulare* https://www.bankia.es/oficina/particulares/#/cuentas/transferecias/paso* https://www.bbva.es/particulares/index.js* https://web.bbva.es/index.html* https://www.bancsabadell.com/cs/Satellite/SabAtl* https://www.bancsabadell.com/txbs/TRExternalTransferIIPP.init.b* https://particulares.gruposantander.es/SUPFPA_ENS/BtoChannelDriver.ssobto?dse_operationName=NavLogin* https://particulares.gruposantander.es/CE_VOperativa_SANINT_ENS/BtoChannelDriver.ssobto?dse_operationName=OP_VentanaOperativa_INT*	Jose Maria  ES76210025  0640	72191DEEBAEC3E104 85FA55D3987C204698C2D91 4F329BED66C1BEE24 A2BE0765679F1C2C03AD10C 2D2807E21070ACA6F 9891EAB946B20C7D2FFD15C

Colaboración con Policía Nacional y Guardia Civil



2018-10-18

bancsabadell.com/cs/Satellite/SabAt
*particulares.gruposantander.es/SUPFP
A_ENS*NavLogin*
*particulares.gruposantander.es/CE_VO
perativa_SANINT_ENS/BtoChannelDriv
er.ssobto?dse_operationName=OP_Ven
tanaOperativa_INT*
*bbvanetcash.com/local_kyop/KYOPSoli
citarCredenciales.htm*
*oficinaempresas.bankia.es/es/login.htm
*
*caixabank.es*particulares_*htm*
*caixabank.es*empresas_*htm*
*caixabank.es*agrobank*htm*
*caixabank.es*negocios_*htm*
*caixabank.es*businessbank_*htm*
*gruposantander.es*empresas*home*
https://loc*.caixabank.es/GPeticones;W
ebLogicSession=*
https://www.bbvanetcash.com/SESKYO
P/kyop_mult_web_pub/index-new.htm*

2000|6500
Fiko
ES52305861
[REDACTED]
943

2000|6500
Ghink
ES87203863
[REDACTED]
230

35F22209623ECEA6B51
2AC97A20ED48364B57
24E

BackSwap afectando a España

Segunda campaña
Abril - Mayo 2019



Jorge Rodriguez
@JR0driguezB



Peter Kalnai @pkalnai · Apr 12
Turns out the new [#BackSwap](#) is also still targeting Spain. (The hash request of the sample via DM.)



5 8 8



Creation Time	1992-06-19 22:22:17
First Submission	2019-05-02 17:02:47
Last Submission	2019-05-02 17:02:47
Last Analysis	2019-05-03 09:42:10

BackSwap: Esquema de la actividad criminal

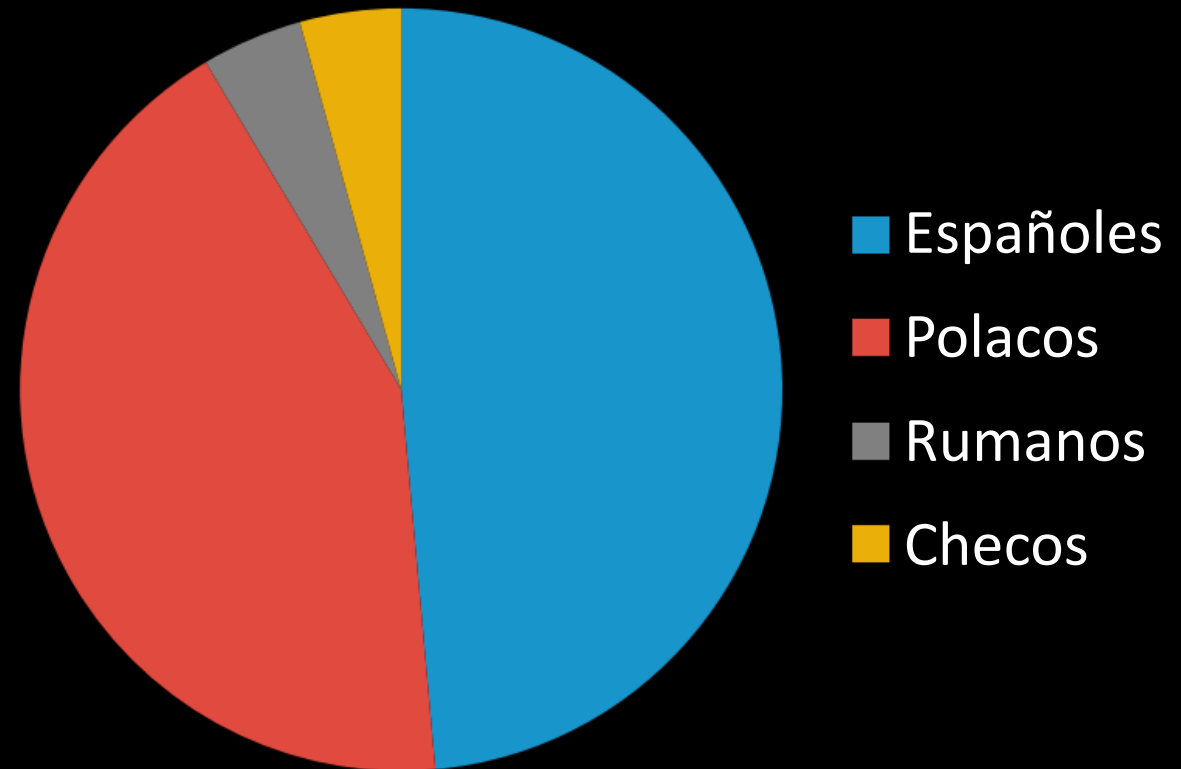
Nacionalidad de las mulas

Alrededor de 70 cuentas bancarias recopiladas

Cooperación con las fuerzas de seguridad de los países afectados

Comunicación directa con los bancos afectados para bloquear las cuentas

Prevención de una elevada cantidad de operaciones fraudulentas



Trojanos y falsas apps bancarias en Android

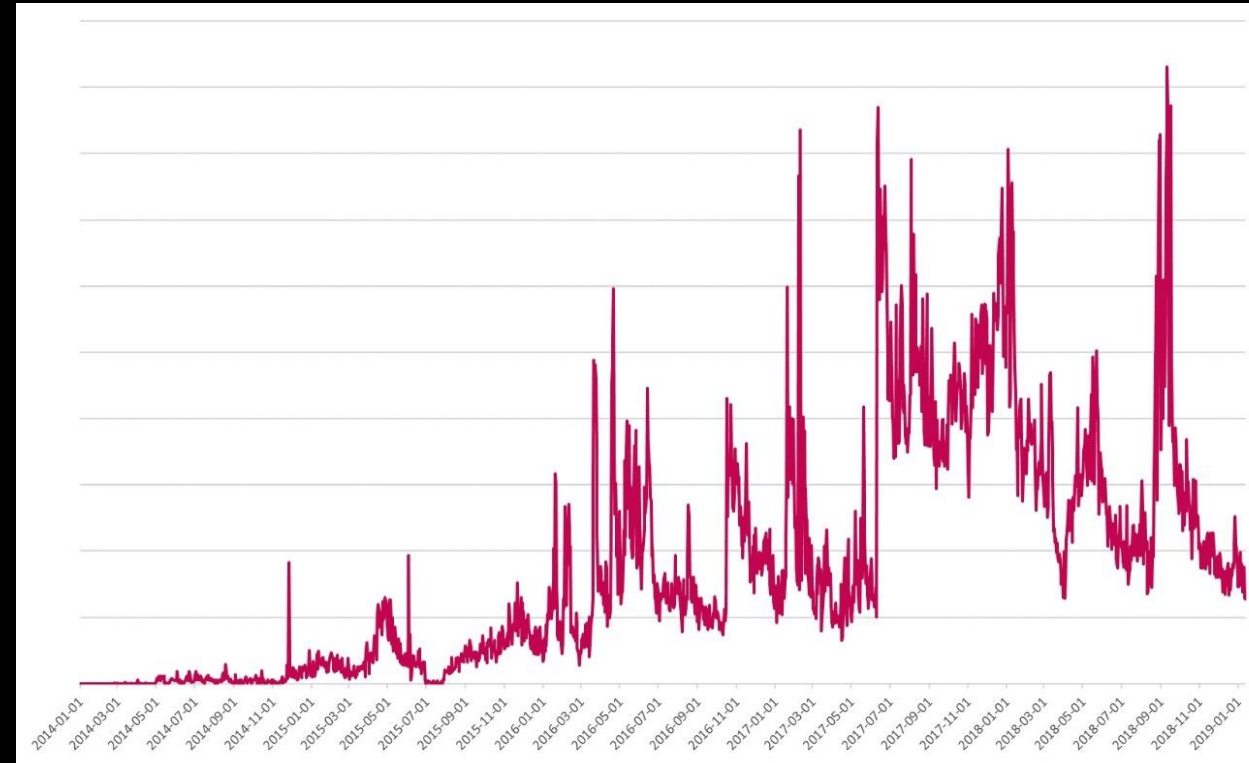
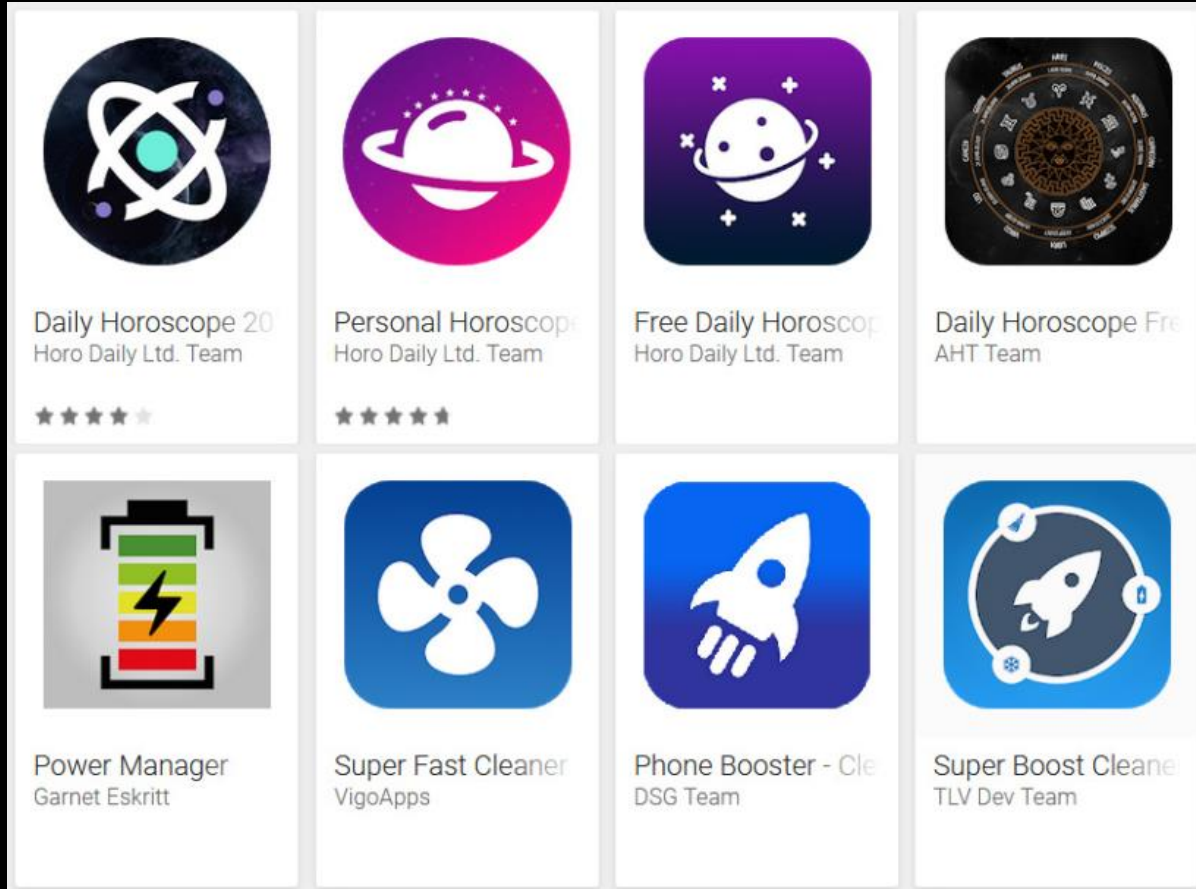
The background of the image is a complex, futuristic digital environment. It features a dark blue color palette with glowing cyan and white lines and points. The scene is composed of various geometric shapes, including cubes, spheres, and elongated rectangular blocks, some of which are arranged in a grid-like pattern. The overall effect is one of a high-tech, data-driven space, possibly representing a digital city or a complex network. The lighting is soft and ambient, with the glowing elements providing the primary source of illumination.

Malware bancario en Android

Troyanos vs. Apps bancarias



Lukas
Stefanko



Busca las diferencias

08:15

Łączenie aplikacji IKO z kontem

PKO Bank Polski Inteligo

Numer klienta albo przyjazny login ?

☐ Został mi udostępniony [Regulamin](#) w formacie PDF.

Więcej

Falso

Dalej

08:18

Łączenie aplikacji IKO z kontem

PKO Bank Polski Inteligo

Numer klienta albo przyjazny login ?

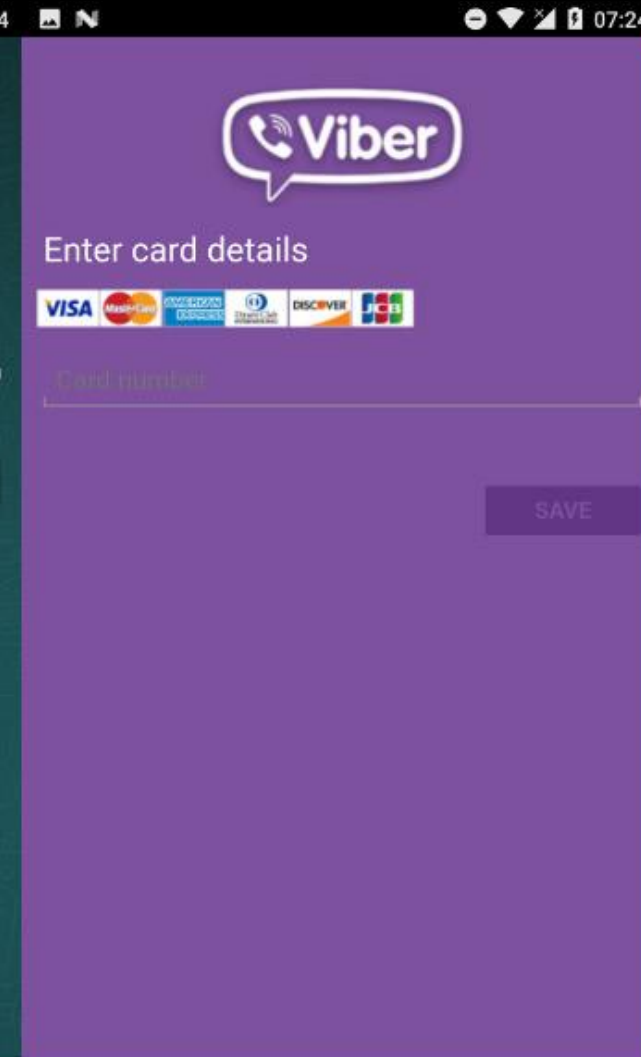
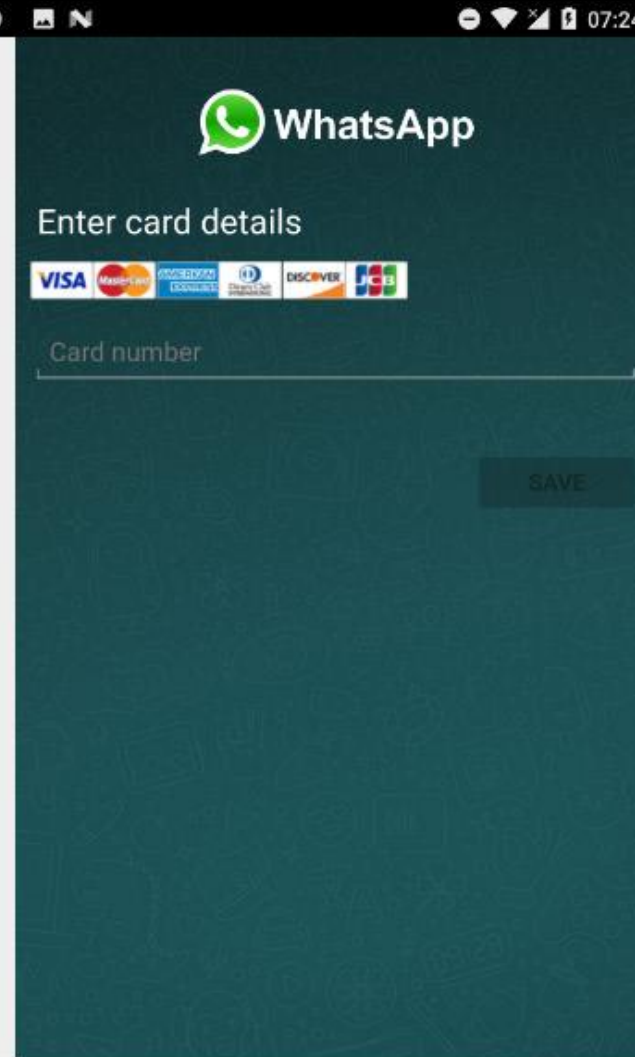
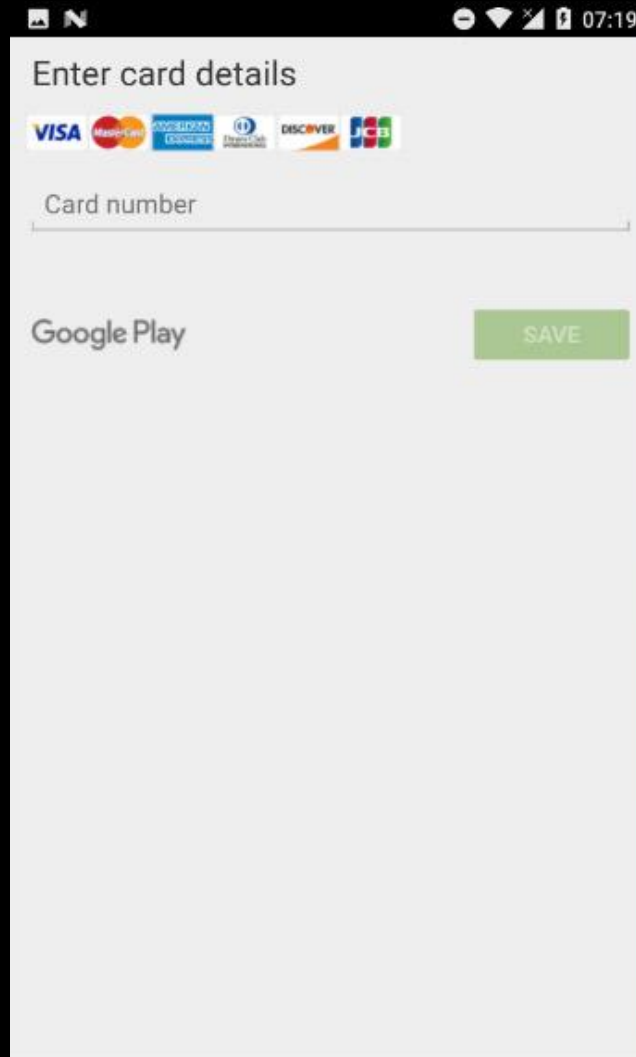
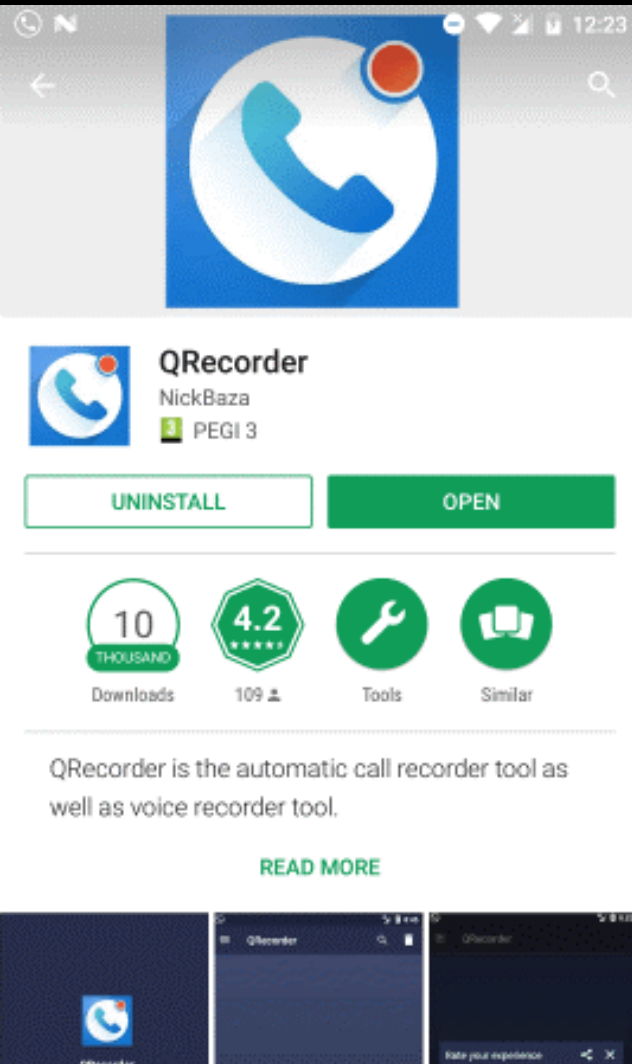
☐ Został mi udostępniony [Regulamin](#) w formacie PDF.

Więcej

Verdadero

Dalej

Pantallas superpuestas fraudulentas



Activate device administrator?



System update

The GNU General Public License is a free, copyleft license for software and other kinds of works. The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

Activating administrator will allow Good Weather to perform the following operations:

- **Change the screen-unlock password**
Change the screen-unlock password.
- **Lock the screen**
Control how and when the screen locks.

CANCEL

ACTIVATE



Google Service

Off



The Services are provided by Google Inc. ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

You must follow any policies made available to you within the Services.

Don't misuse our Services. For example, don't interfere with our Services or try to access them using a method other than the interface and the instructions that we provide. You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations. We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

Using our Services does not give you ownership of any intellectual property rights in our Services or the content you access. You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law. These terms do not grant you the right to use any branding or logos used in our Services. Don't remove, obscure, or alter any legal notices displayed in or



Google Service

Use Google Service?

Google Service needs to:

- **Observe your actions**
Receive notifications when you're interacting with an app.
- **Retrieve window content**
Inspect the content of a window you're interacting with.
- **Turn on Explore by Touch**
Tapped items will be spoken aloud and the screen can be explored using gestures.
- **Turn on enhanced web accessibility**
Scripts may be installed to make app content more accessible.
- **Perform gestures**
Can tap, swipe, pinch, and perform other gestures.

CANCEL

OK

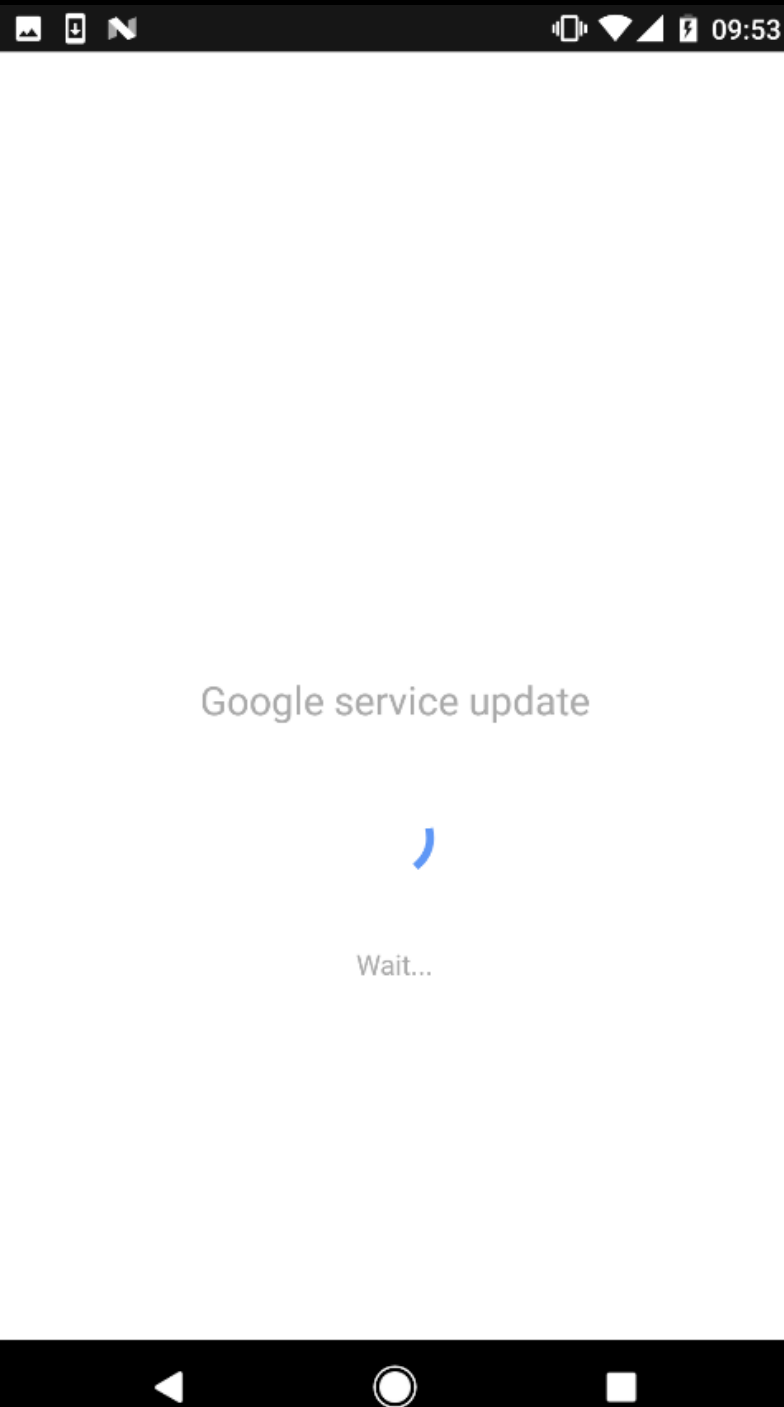
Técnicas de ocultación



Signal, Wi-Fi, and battery status icons. 100% battery, 07:04.

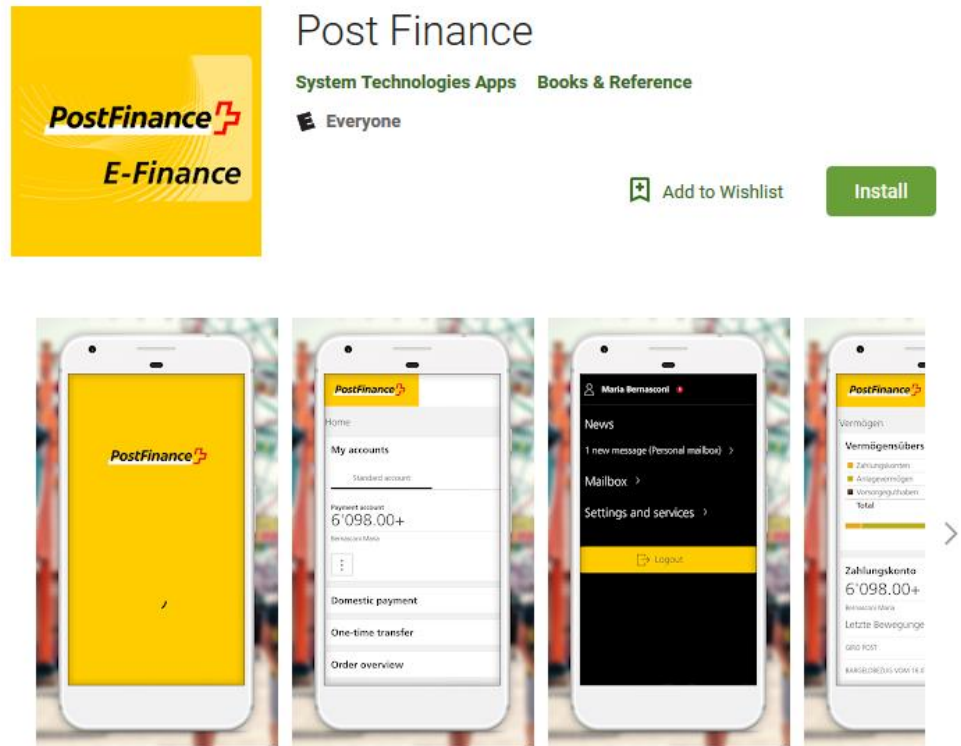
The installed application is incompatible with your phone and has now been removed!

OK



No command.

Aplicaciones bancarias fraudulentas



Have your banking transactions under control in just a few seconds.

You can find the most important information and functions in the Post Finance easily: Check the balance of your accounts and the latest account transactions quickly and easily, transfer small amounts to your friends' mobile numbers.

An overview of the practical functions

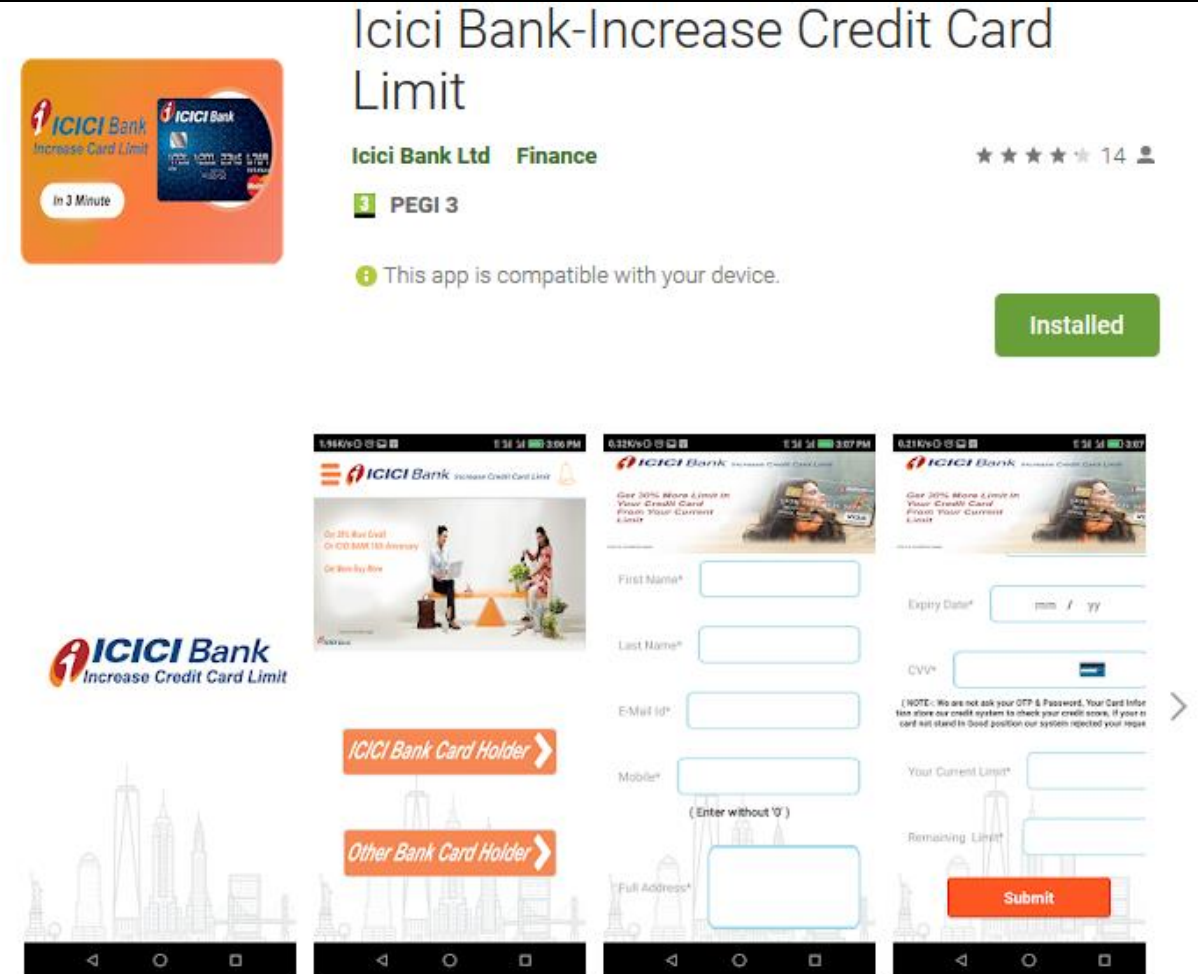
Check your account balance and transactions:

Call up your balance and the most recent transactions on your payment and savings accounts.

E-finance – full access with standard login or via Mobile ID

With Mobile e-finance, you can carry out your financial transactions wherever and whenever you want directly via the app: access all your accounts, transactions, payments, transfers and more.

E-trading and stock exchange – access to the securities custody account



Increase Your Credit Card Limit Up to 30% More.

Secure Your Credit Card

Limit Increase In 3 minute

We Working on this and adding more feature

Aplicaciones bancarias fraudulentas



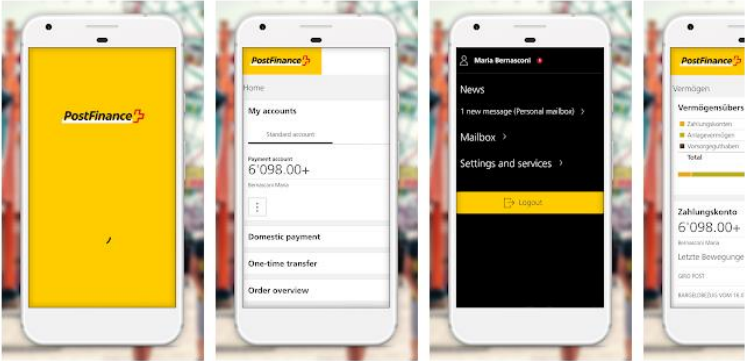
Post Finance

System Technologies Apps Books & Reference

Everyone

Add to Wishlist

Install



Have your banking transactions under control in just a few seconds.
You can find the most important information and functions in the Post Finance easily: Check the balance of your accounts and the latest account transactions quickly and easily, transfer small amounts to your friends' mobile numbers.

An overview of the practical functions
Check your account balance and transactions:
Call up your balance and the most recent transactions on your payment and savings accounts.

E-finance – full access with standard login or via Mobile ID
With Mobile e-finance, you can carry out your financial transactions wherever and whenever you want directly via the app: access all your accounts, transactions, payments, transfers and more.

E-trading and stock exchange – access to the securities custody account



REGISTER

AUTHORIZE

Please provide additional information so we can ensure that this request is being made by you

Card number

Card expiry (MM/YY)

CVV/CVC Code

SecureCode

VERIFY

Congratulations!

Your registration have been completed
Soon we will send you your details for authorization via SMS. After login you'll be prompted to set new password

Ginp: Banca online española como objetivo



Tatyana Shishkova @ Botconf
@sh1shk0va

New Android banking Trojan family **#Ginp** targeting Spain 🇪🇸 and UK 🇬🇧. Latest versions imitate Adobe Flash Player and decrypt payload from assets. Abuses Accessibility Service, sets itself as default SMS app, gets phishing injects from C&C server. (1/2)

[Traducir Tweet](#)

```
else if(w3.equals("DISABLE_CC_GRABBER")) {
    this.c.a("DISABLE_INJECT", Integer.valueOf(0));
    c.a(this, j.a("TXT_C_6"), j.a("TXT_37"));
    c.b(this, j.a("TXT_37"));
}
else if(w3.equals("DISABLE_CC_GRABBER")) {
    this.c.a("DISABLE_INJECT", Integer.valueOf(1));
    c.a(this, j.a("TXT_C_6"), j.a("TXT_38"));
    c.b(this, j.a("TXT_38"));
}
else if(w3.equals("ENABLE_EXTENDED_INJECT")) {
    this.c.a("EXTENDED_INJECTION", Integer.valueOf(1));
    c.b(this, j.a("TXT_35"));
}
else if(w3.equals("DISABLE_EXTENDED_INJECT")) {
    this.c.a("EXTENDED_INJECTION", Integer.valueOf(0));
    c.b(this, j.a("TXT_34"));
}
else if(w3.equals("START_DEBUG")) {
    this.c.a("DEBUG_TO_API", Integer.valueOf(1));
}
else if(w3.equals("STOP_DEBUG")) {
    this.c.a("DEBUG_TO_API", Integer.valueOf(0));
}
else if(w3.equals("START_PERMISSIONS")) {
    this.c();
}
else if(w3.equals("GET_APPS")) {
    this.d();
}
else if(w3.equals("GET_PACKAGE_NAME")) {
    c.b(this, j.a("TXT_11") + this.getPackageName());
}
else if(w3.equals("GET_CONTACTS")) {
    this.e();
}
else if(w3.equals("SEND_BULK_SMS")) {
    String v0_9 = v1_1.getString("MSG");
    String v1_2 = v1_1.getString("NUMBERS");
    c.a(this, j.a("TXT_C_6"), "MSG: " + v0_9 + ", NUMS: " + v1_2);
    this.b(v0_9, v1_2);
}
```

Enter card details



Card number

Google Play

SAVE

1:31 p. m. · 23 oct. 2019 · [Twitter Web Client](#)

← Adobe Flash Player

Off

No description provided.

Use Adobe Flash Player?

Adobe Flash Player needs to:

- **Observe your actions**
Receive notifications when you're interacting with an app.
- **Retrieve window content**
Inspect the content of a window you're interacting with.

CANCEL

OK

Enter card details



Card number

MM/YY

CVC

Google Play

SAVE

Ginp: Overlay attack

Buenos días

NIF

Número de documento

Clave de acceso

☐ Recordar usuario en este dispositivo

ENTRAR

Recupera tu clave de acceso

Verifica tu identidad

Introduzca su datos tarjeta

Número de tarjeta

Fecha de caducidad de tarjeta

01 / 2019

Código CVV

Continuar

BBVA

Verifica tu identidad

NIF, NIE, Tarjeta o Pasaporte *

Clave de acceso *

¿Has olvidado tu clave de acceso?

Iniciar sesión

Hazte cliente

Soy cliente sin usuario online

BBVA

Verifica tu identidad

Introduzca su datos tarjeta

Número de tarjeta *

Mes de vencimiento de la tarjeta *

Año de vencimiento de la tarjeta *

Código CVV *

Continuar

k

ACCESO A BANCA MÓVIL

NIF/Usuario

Clave

Recordar usuario ☒

Recordar usuario implica que este dispositivo recibirá notificaciones dirigidas al usuario vinculado. Puedes configurarlo desde 'Ajustes'.

Entrar

¿Has olvidado tu clave?

k

Introduzca su datos tarjeta

Número de tarjeta

Mes de vencimiento de la tarjeta

Año de vencimiento de la tarjeta

Código CVV

Entrar

Bankia

Accede con tus datos

Nº de documento

Clave de acceso

Recordar mis datos

Entrar

¿Tienes problemas para acceder?

Bankia

Introduzca su datos tarjeta

Número de tarjeta

Mes de vencimiento de la tarjeta

Año de vencimiento de la tarjeta

Código CVV

Continuar

Acceso clientes

Usuario

Contraseña

☐ Recordar usuario

Reactivar claves

ENTRAR

Verifica tu identidad

Número de tarjeta

01 / 2019

Código CVV

CONTINUAR

CaixaBank

¡Buenos días!

Identificador

Contraseña

¿Has olvidado tus datos de acceso?

Entrar

Acceder con huella

Verifica tu identidad

Introduzca su datos tarjeta

Número de tarjeta

Fecha de caducidad de tarjeta

01 / 2019

Código CVV

Continuar

EVO

BIENVENIDO A EVO BANCO MÓVIL

NIF/NIE

Contraseña

¿Problemas para acceder?

CONTINUAR

Emergencia

¿Tarjetas perdidas o robadas?

EVO

VERIFICA TU IDENTIDAD

INTRODUZCA SU DATOS TARJETA

Número de tarjeta

Mes de vencimiento de la tarjeta

Año de vencimiento de la tarjeta

Código CVV

CONTINUAR

The background is a dark, teal-colored digital landscape. It features a central perspective view of a path or road that recedes into the distance. The path is composed of many small, glowing white and light blue dots, creating a sense of depth and movement. The path is flanked by dark, textured surfaces that also appear to be composed of similar dots. The overall effect is a futuristic, high-tech environment.

Conclusiones

Conclusiones

Constante evolución de las técnicas usadas por los troyanos bancarios

Los delincuentes ponen el foco en dispositivos de escritorio y móviles por igual

Las técnicas menos avanzadas también consiguen buenos resultados

Tendencia en continuo crecimiento especialmente en dispositivos Android





ENJOY SAFER TECHNOLOGY™

Gracias por la atención

@JosepAlbors

