

# TERMINALES INTERACTIVOS

Pedro C. aka s4ur0n – TACS 2017

CS³ SECURITY SERVICES
https://cs3group.com



# Whoami

```
class PedroC:
    def __init__(self):
        self.name =  'Pedro Candel'
        self.email =  's4ur0n@s4ur0n.com'
        self.web =    'https://www.s4ur0n.com'
        self.nick =   '@NN2ed_s4ur0n'
        self.role =   'Security Researcher'
        self.work =   [ 'Reversing', 'Malware',
                        'Offensive Security', '...' ]
        self.groups = [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

mlw.re

ENIGMASEC

OWASP
Open Web Application Security Project

© 2017 CS³ Group. Todos los derechos reservados.

# ¿Quiénes somos?

- **Unión** de **profesionales y empresas multidisciplinares** seleccionados cuidadosamente por CS³ Group ofreciendo un conjunto completo e integral de servicios y/o productos de **seguridad informática**
- **Amplia experiencia** con reconocidas trayectorias profesionales nacionales e internacionales de los miembros del grupo CS³
- **Independencia** y **neutralidad** de fabricantes, proveedores y/o distribuidores
- Proyectos realizados con la **máxima calidad**

© 2017 CS³ Group. Todos los derechos reservados.

# ¿Quiénes somos?



Pedro C. aka s4ur0n
CS³ Group Member ID: 3413




Pedro Sánchez
CS³ Group Member ID: 3412



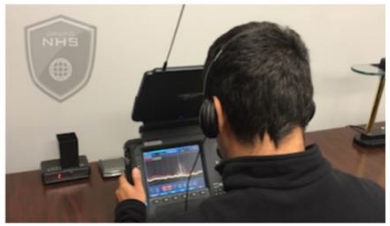

Javi Espejo "qemm" (Raipson)
CS³ Group Member ID: 3417




Igor Lukic (Enigmasec Team)
CS³ Group Member ID: 3414




Tomás Isasia (TIIZSS)
CS³ Group Member ID: 3410




Grupo NHS
CS³ Group Member ID: 3415



cyttek GROUP

Rafael Revert (Cyttek Group)
CS³ Group Member ID: 3416



Mikel Gorraiz "Hackpintero"
CS³ Group Member ID: 3409

IhackLabs
PLATAFORMAS DE TRAINING

iHackLabs
CS³ Group Member ID: 3418



C4T
CS³ Group Member ID: 3513



© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# Portfolio

## Formación en Seguridad

Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

## Hacking Ético

Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

## Análisis de Malware

Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

## Ingeniería Inversa

Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

## Exploiting

Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

## Desarrollo Seguro

Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

## Hardware Hacking

Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

## Seguridad en dispositivos móviles

Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

## Respuesta ante incidentes

Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

## Forense

Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

## DevSecOps

Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

## Intelligence

Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

## SIGINT

Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

## T.S.C.M.

Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

## Telecom

Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

## ATM

Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

## PoS/TPV

Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

## LOPD/GPDR/Cumplimiento

LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

© 2017 CS³ Group. Todos los derechos reservados.

# • Agenda




- Introducción
- Sistemas Operativos de kiosko
- Hacking físico (hardware)
- Hacking lógico (software)
- Hacking remoto (internet)

© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com




# INTRODUCCIÓN

© 2017 CS³ Group. Todos los derechos reservados.

# 1 Introducción

- Retiramos dinero del cajero, hacemos consultas en los hoteles, realizamos reservas en restaurantes, imprimimos tarjetas, jugamos, sacamos tabaco, apostamos en directo… pero detrás hay un ordenador con **una única aplicación**, que suele ser un navegador que permite realizar **sólo acciones limitadas**.
- Es lo que se conoce como **modo kiosko** o a **pantalla completa** desde la que podemos realizar operaciones **sin tener acceso** al resto de aplicaciones o ni mucho menos, al contenido del resto del equipo…

© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 1 Introducción




© 2017 CS³ Group. Todos los derechos reservados.

# 1 Introducción

- Posibilidades de **ampliación**:
  - **Check-in** sin reserva previa
  - Integración con **PMS**: gestión hotelera con sincronización de pagos y reservas
  - **Webcam**
  - Verificación de número de móvil: con **SMS de confirmación** para operaciones realizadas
  - **Firma** de condiciones
  - **Impresión** de documentos: bienvenida, recibos
  - Aplicaciones con **escaner**: Identificación con DNI/pasaporte, QR, ePassport, tickets parking

© 2017 CS³ Group. Todos los derechos reservados.

- **Integración con cerraduras electrónicas**



Banda magnética




Proximidad



chip



Módulo de 20 llaves



Duplicado de llave

© 2017 CS³ Group. Todos los derechos reservados.

# 1 Introducción

- Opciones para **pagos**
  - **Sin** pagos
  - **Con** pagos:
    - Tarjeta de débito/crédito/otras
    - Aceptación y devolución de monedas
    - Aceptación y devolución de billetes

© 2017 CS³ Group. Todos los derechos reservados.

# 1 Introducción

- Revolución **2.0**
  - Emisión de bonos descuento (restaurantes, parques de atracciones, etc.)
  - Tarjeta de fidelización (carga/consulta puntos)
  - Emisión de facturas
  - Impresión de documentos
  - Suscripción a listas de email
  - Precheck-in online y check-out
  - Reservas de otros servicios (golf, spa, etc.)
  - Tienda
  - Encuestas de satisfacción

© 2017 CS³ Group. Todos los derechos reservados.

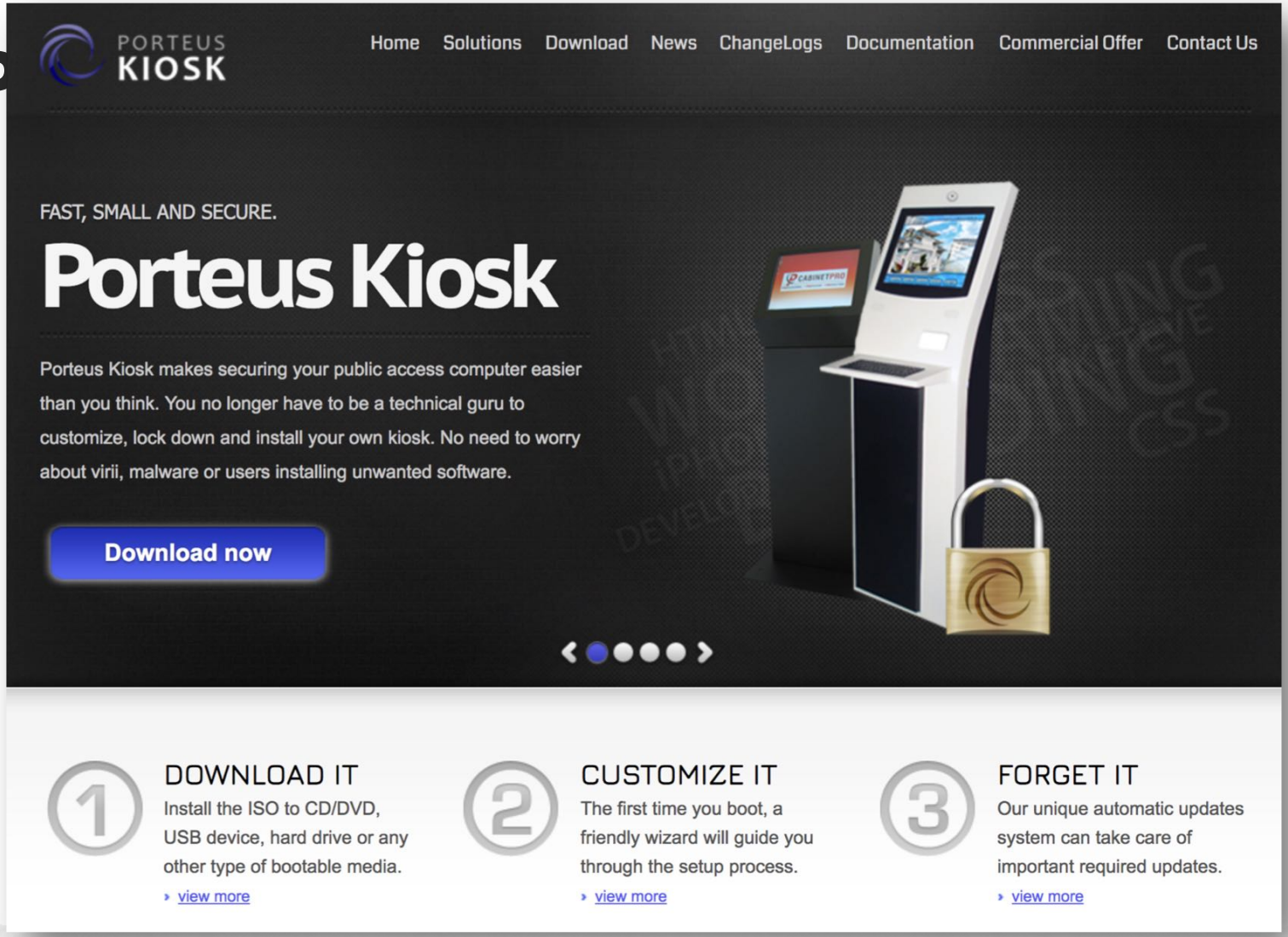
CS³ SECURITY SERVICES
https://cs3group.com




# SS.OO.
# KIOSKO

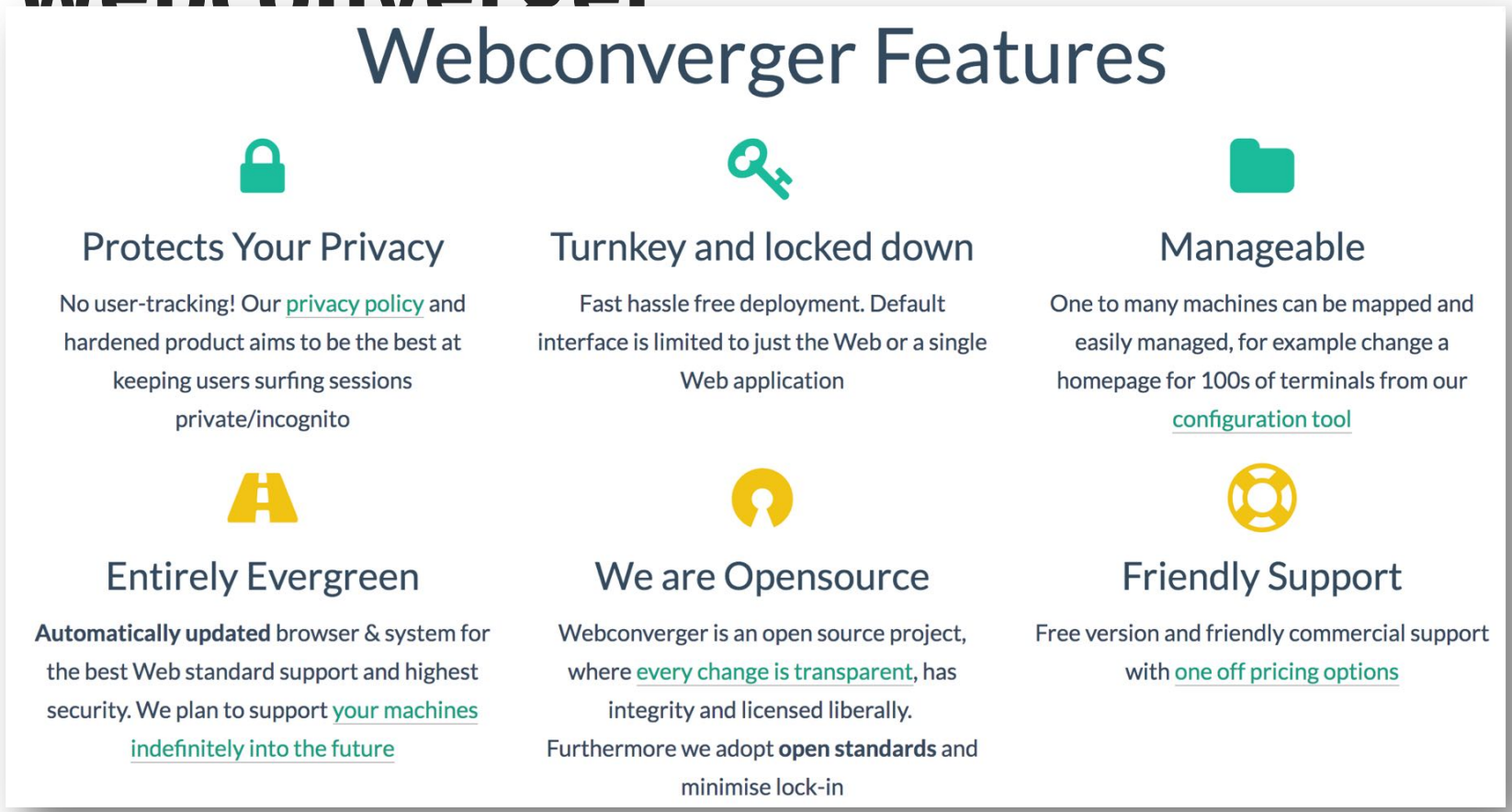
© 2017 CS³ Group. Todos los derechos reservados.

• P




© 2017 CS³ Group. Todos los derechos reservados.

- **Webconverger**




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com




© 2017 CS³ Group. Todos los derechos reservados.

# 3 Hacking físico

- **Puertos de expansión**
  - USB
  - Lector de tarjetas
  - Lectores de códigos de barras / QR:
    `http://malqr.shielder`




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 3 Hacking físico



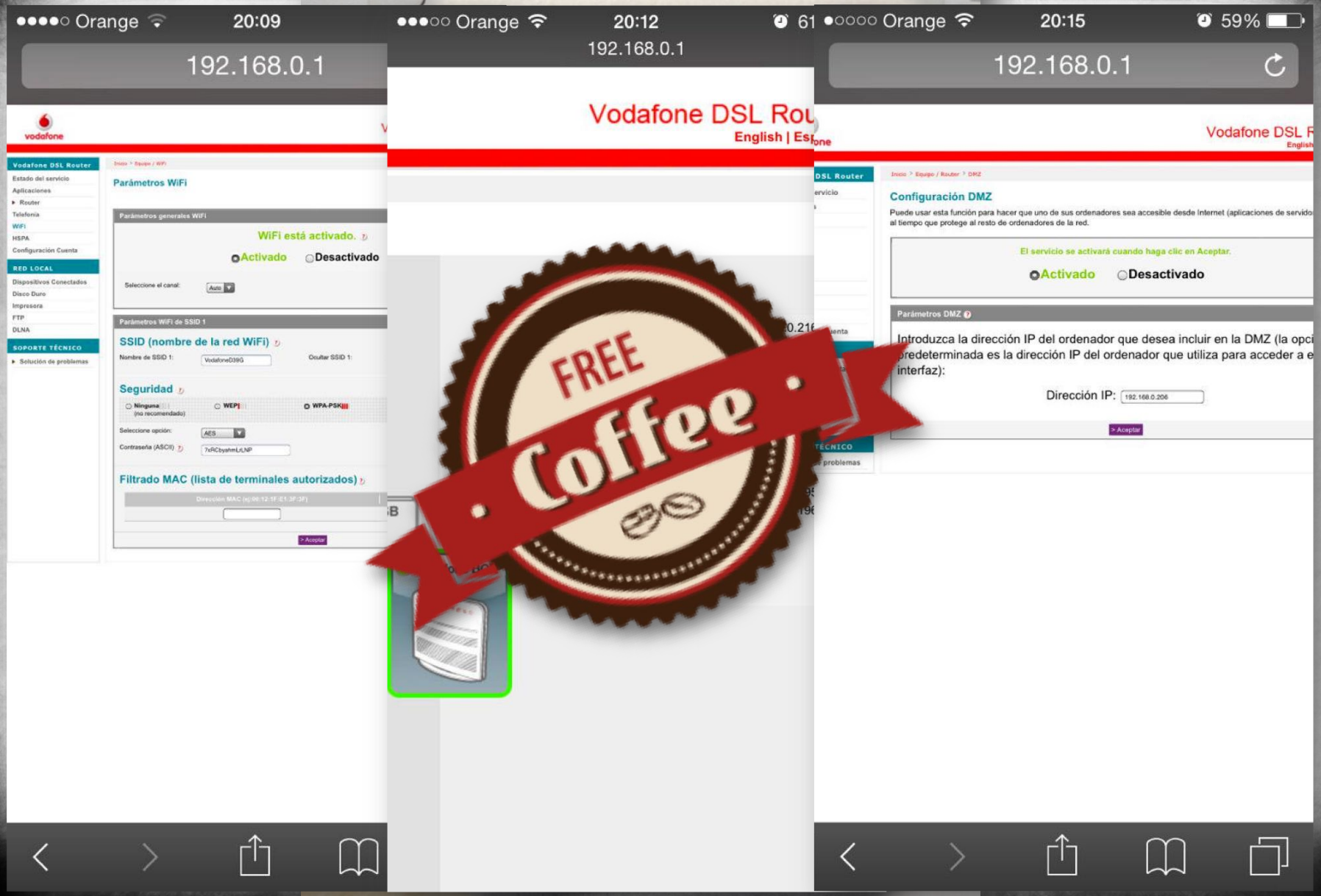




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 3 Hacking físico




© 2017 CS³ Group. Todos los derechos

CS³ SECURITY SERVICES
https://cs3group.com

# 2 Hacking físico

- C
  -




© 2017 CS³ Group. Todos los derechos res

CS³ SECURITY SERVICES
https://cs3group.com




© 2017 CS³ Group. Todos los derechos reservados.

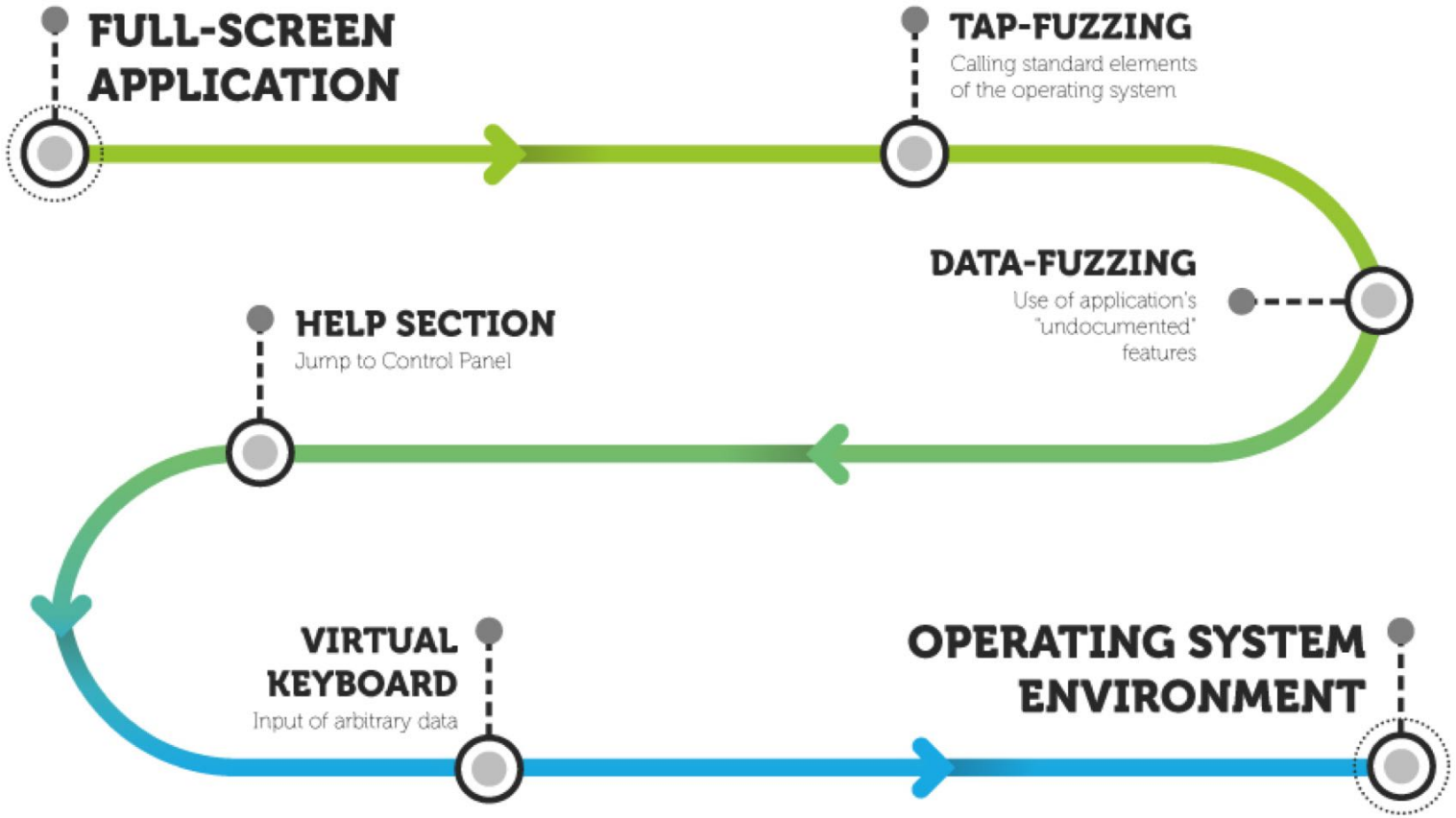
# 4 Hacking lógico

- **Técnicas** para conseguir el **acceso** al **Sistema Operativo**:
  - (1) **Tap** Fuzzing
  - (2) **Data** Fuzzing
  - (3) External **links**

© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

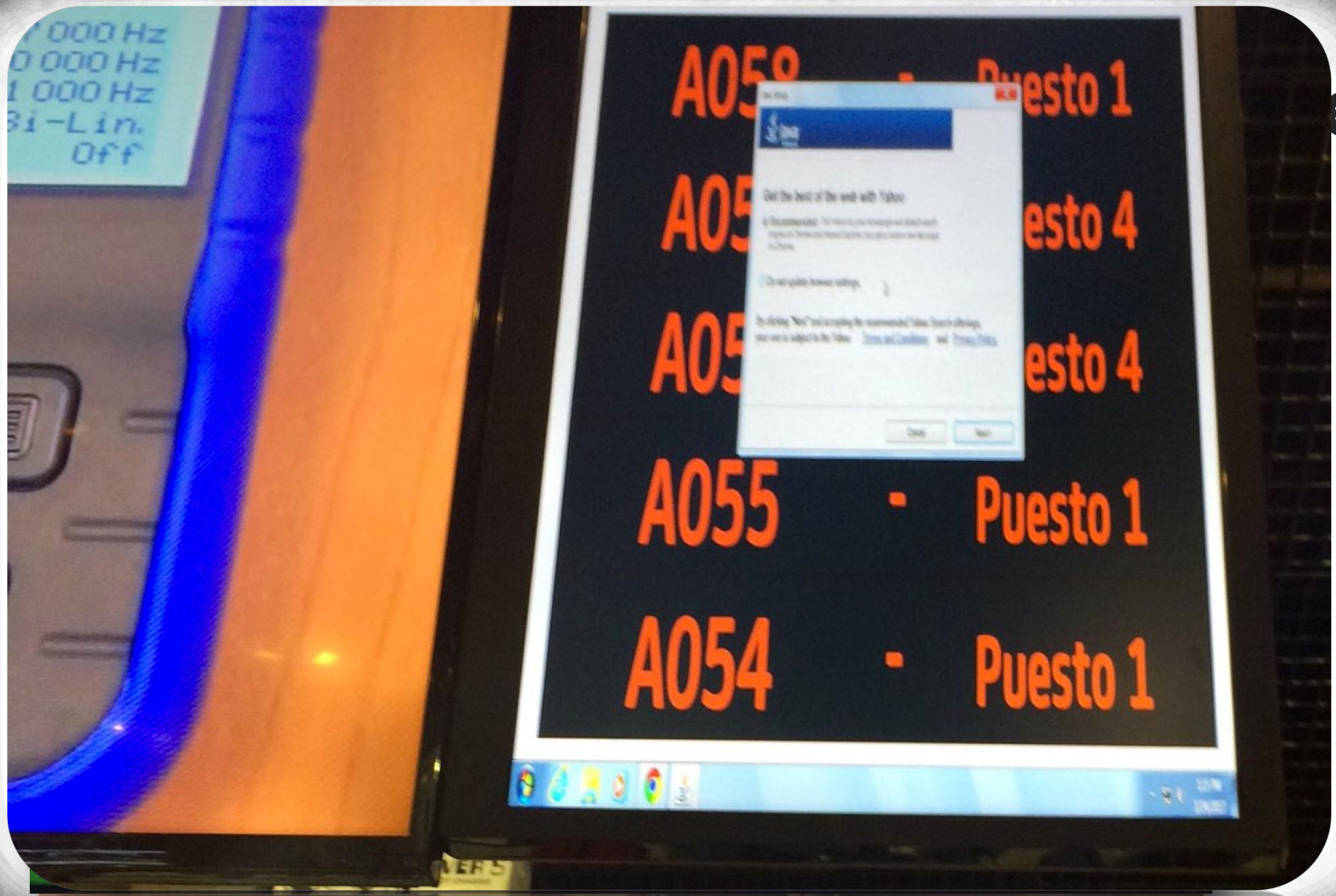
# 4 Hacking lógico




© 2016 AO Kaspersky Lab. All Rights Reserved.

© 2017 CS³ Group. Todos los derechos reservados.

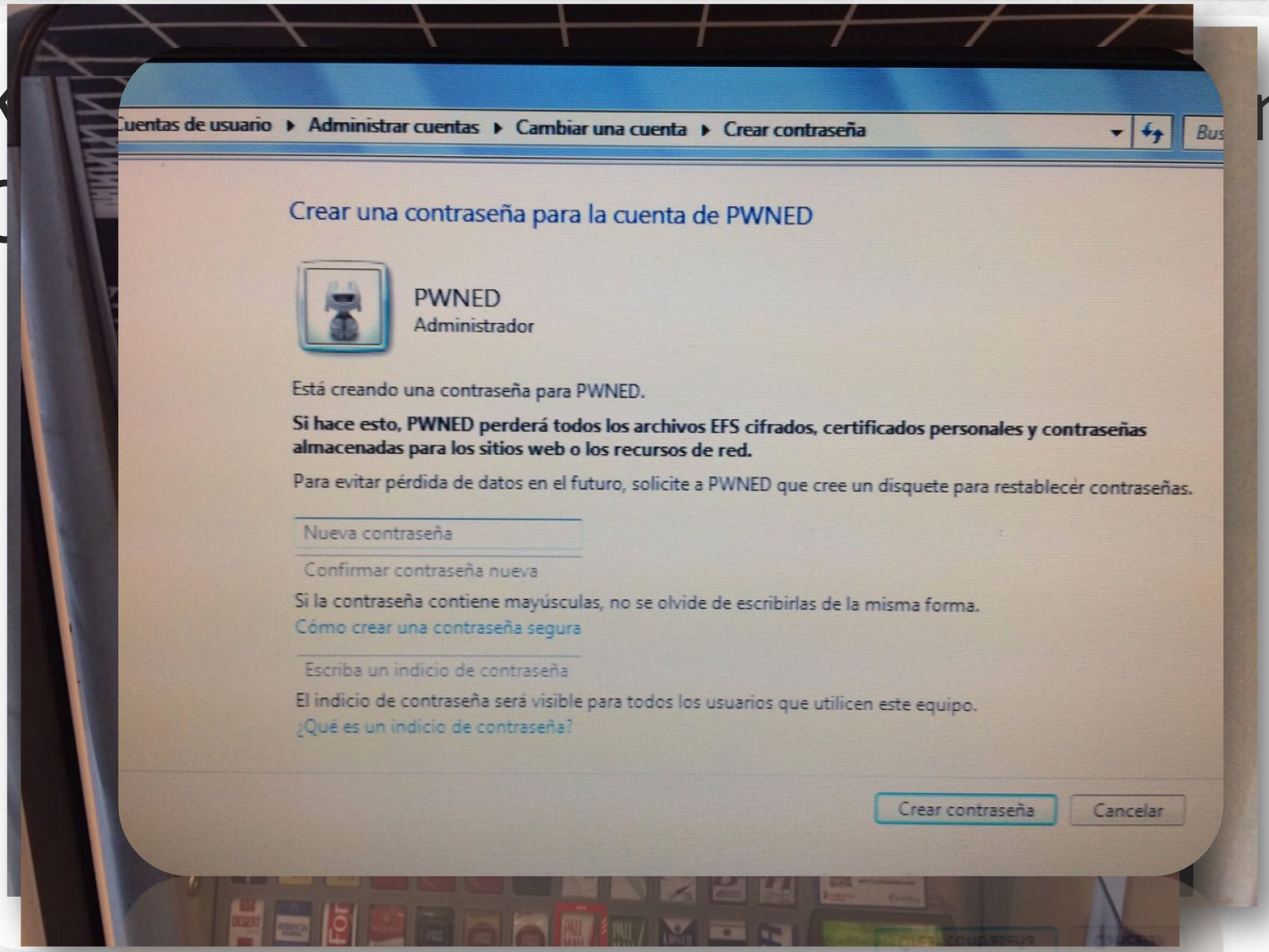
# 4 Hacking lógico




© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico

- K… n
  C…




© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico

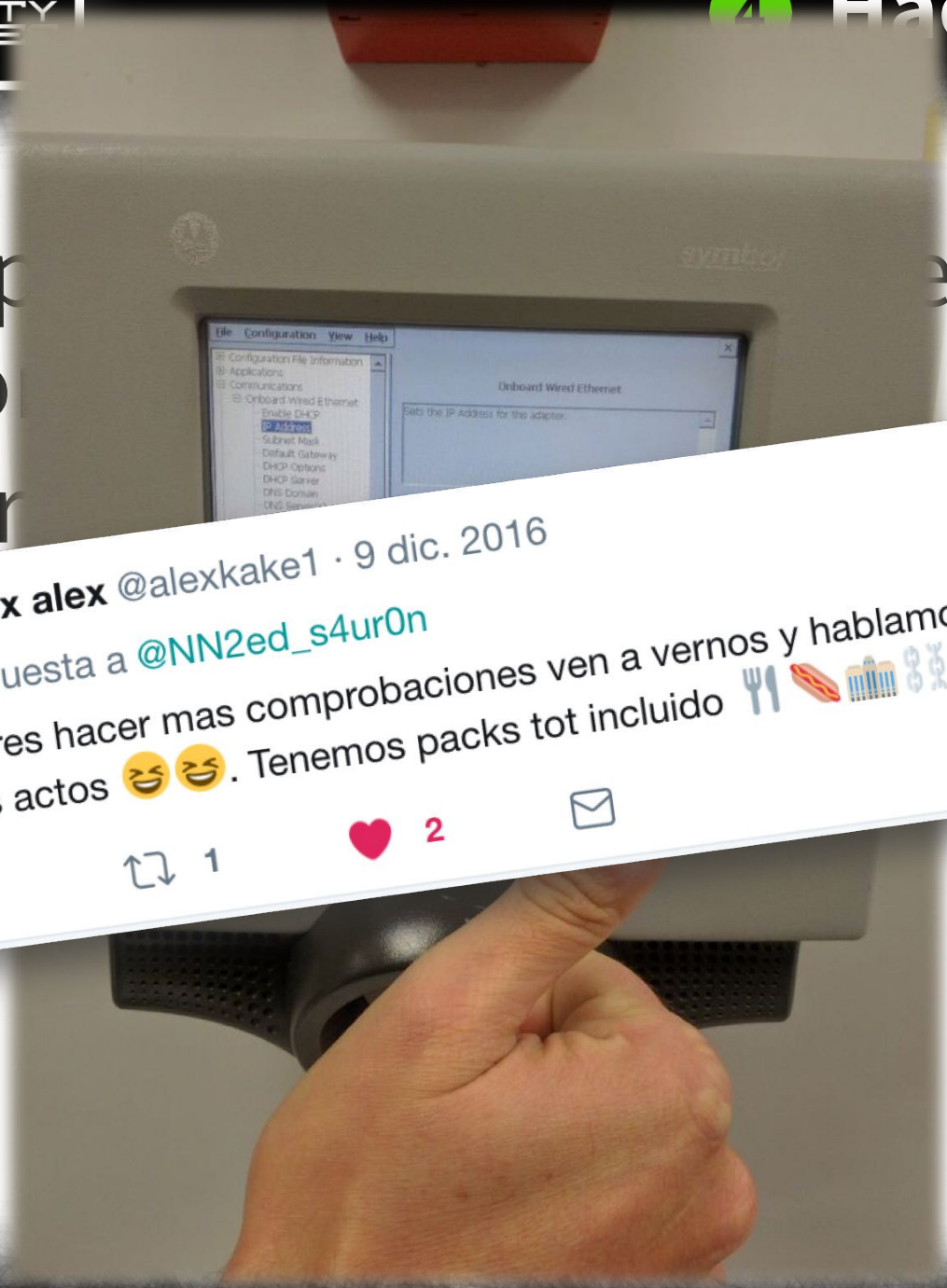
- Ascensor en **Torre Catalunya**



© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico

- Comp … en
  Andro…
  - Per…




**alex alex alex** @alexkake1 · 9 dic. 2016

En respuesta a @NN2ed_s4ur0n

si quieres hacer mas comprobaciones ven a vernos y hablamos del precio de ciertos actos 😆😆. Tenemos packs tot incluido 🍴🌭🏛️🚓😂😂

1 2

© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico

- Kiosko **rápi**




© 2017 CS³ Group. Todos los derechos reservados.

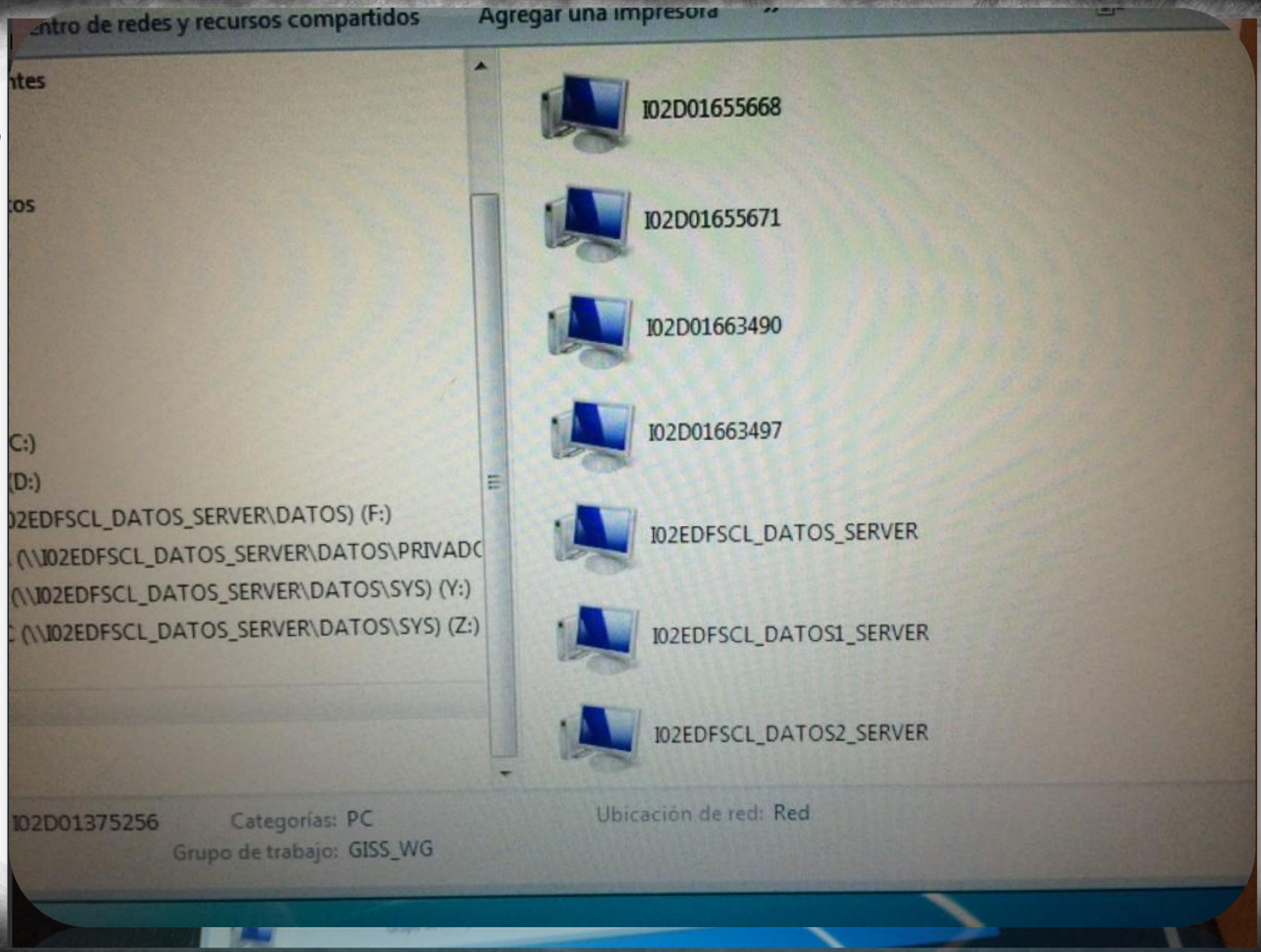
# 4 Hacking lógico

- C




© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico




© 2017 CS³ Group. Todos los derechos reservados.

# 4 Hacking lógico

- Ki n
  la
  -




© 2017 CS³ Group. Todos los derechos reservados.

# Hacking lógico




© 2017 CS³

CS³ SECURITY SERVICES
https://cs3group.com




# REVOLUTION 2.0

© 2017 CS³ Group. Todos los derechos reservados.

# 5 Revolution 2.0

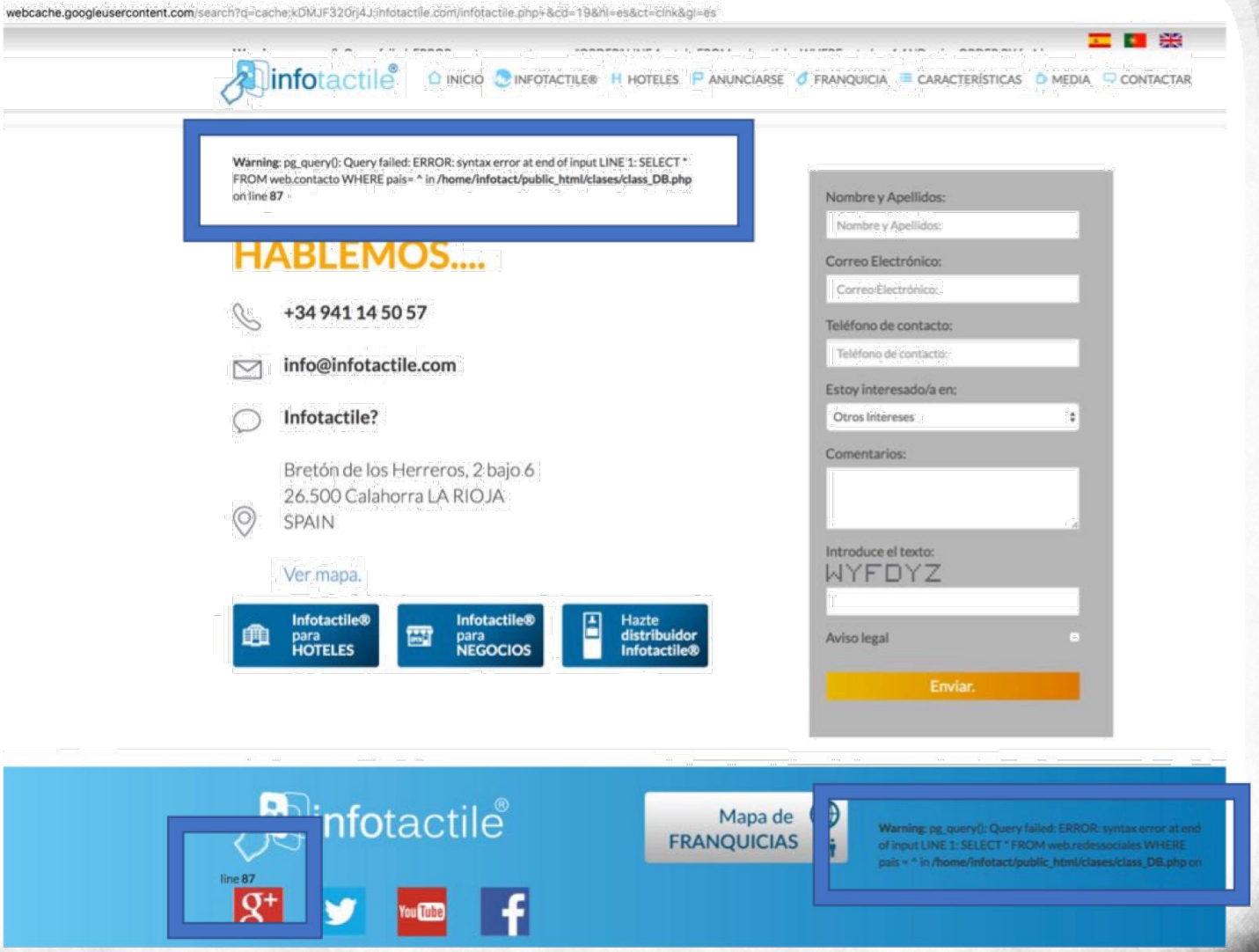
Caso empresa X: donde **todos quieren estar**... **Protegidos**!




© 2017 CS³ Group. Todos los derechos reservados.

# 5 Revolution 2.0

Sencilla **búsqueda en los indexadores públicos** de contenidos…




© 2017 CS³ Group. Todos los derechos reservados.

# 5 Revolution 2.0

Sencilla **búsqueda en los indexadores públicos** de contenidos...

webcache.googleusercontent.com/search?q=cache:taOgz3l-_iwJ:infotactile.com/noticias.php+&cd=24&hl=es&ct=clnk&gl=es

infotactile® INICIO INFOTACTILE® HOTELES ANUNCIARSE FRANQUICIA CARACTERÍSTICAS MEDIA CONTACTAR

Esta es la versión en caché de http://infotactile.com/noticias.php de Google. Se trata de una captura de pantalla de la página tal como esta se mostraba el 17 Ene 2017 13:05:37 GMT.
Es posible que la página haya sufrido modificaciones durante este tiempo. Más información

Versión completa Versión de solo texto Ver origen Sugerencia: para encontrar rápidamente tu término de búsqueda en esta página, pulsa Ctrl+F o ⌘-F (Mac) y utiliza la barra de búsqueda.

Varning: pg_query(): Query failed: ERROR: syntax error at or near "ORDER" LINE 1: ...ticias WHERE estado = 1 AND portada = 1 AND pais= ORDER BY f... ^ in /home/infotact/public_html/clases/class_DB.php on line 87

Noticias

Warning: pg_query(): Query failed: ERROR: syntax error at or near "ORDER" LINE 1: ...ada FROM web.noticias WHERE estado = 1 AND pais= ORDER BY f... ^ in /home/infotact/public_html/clases/class_ on line 87

Warning: pg_query(): Query failed: ERROR: syntax error at or near "ORDER" LINE 1: ...deo FROM web.noticias WHERE estado = 1 AND pais= ORDER BY f... ^ in /home/infotact/public_html/clases/class_DB.php on line 87

INFOTACTILE PRESENTA NOVEDADES PARA TURISMO

12/01/2017
INFOTACTILE INSTALA SU PRIMER DISPOSITIVO DE

23/12/2016
CÓRDOBA YA TIENE 6 DISPOSITIVOS INFOTACTILE

INFOTACTILE PRESENTA NOVEDADES PARA TURISMO Y TICKETING EN FITUR

La marca de dispositivos de información, publicidad y venta de entradas acude, un año más, a FITUR y mostrará ahí sus dispositivos actualizados y nuevas soluciones para mejorar el turismo y la venta de entradas.

Fitur 18-22 Enero 2017 FERIA INTERNACIONAL DE TURISMO




© 2017 CS³ Group. Todos los derechos reservados.

# 5 Revolution 2.0

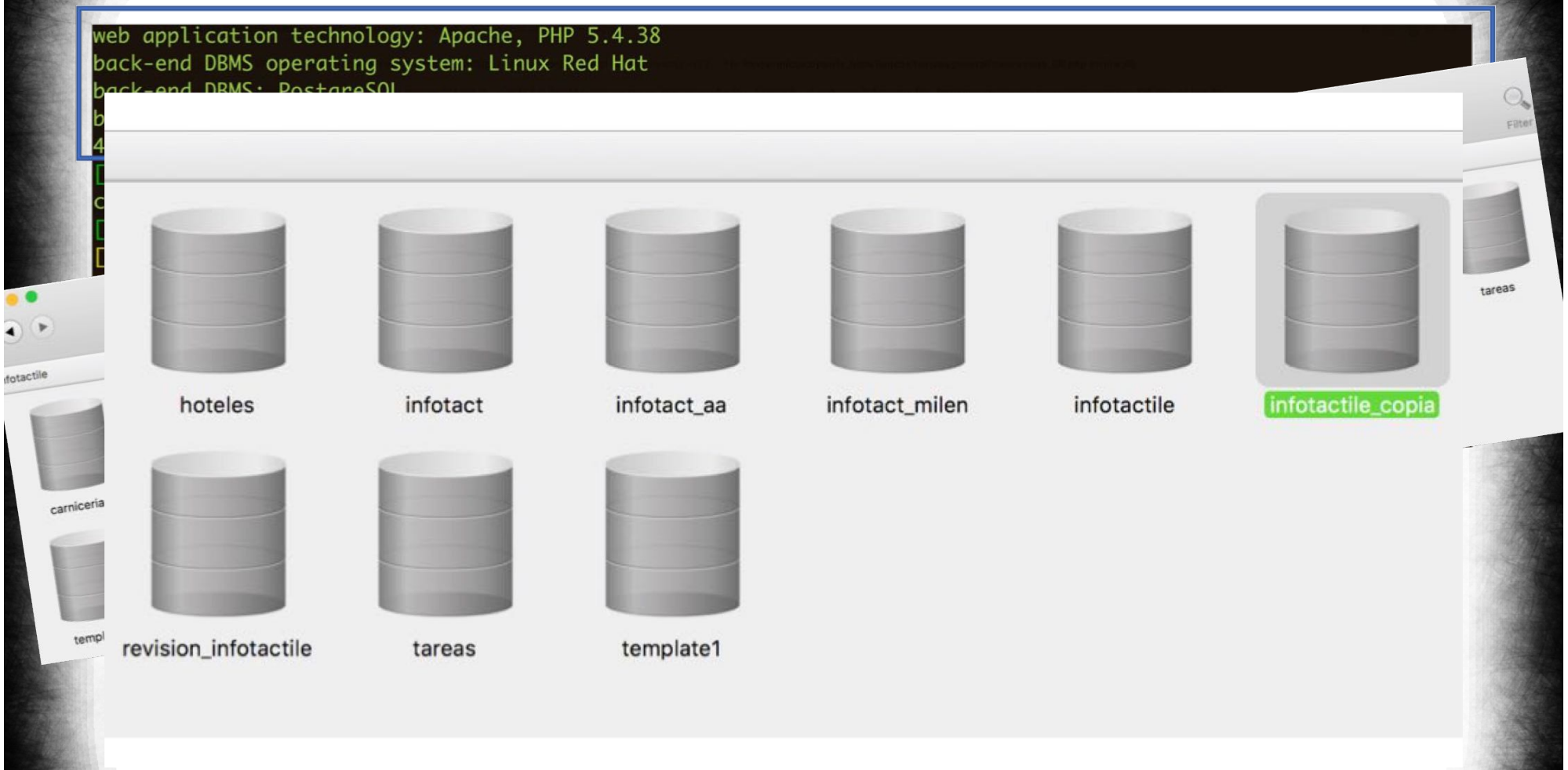
Incluso en **SHODAN** con la exposición de su base de datos...




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

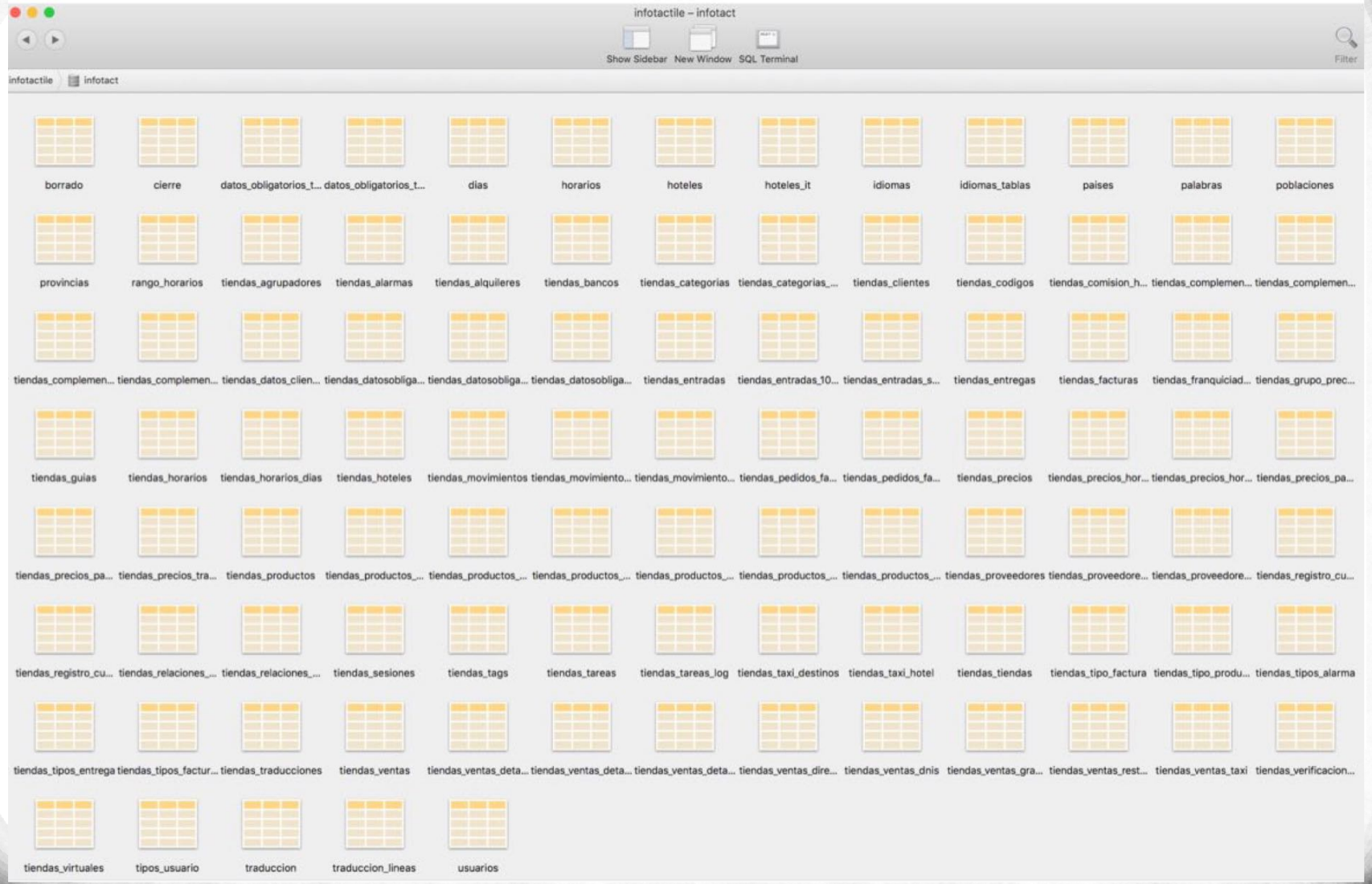
# 5 Revolution 2.0




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0

Revelando datos **confidenciales** sometidos a RLOPD...

infotactile | infotactile | ventas

| id | fecha | cliente | franquiciad | formapago | importe | fxlarma | alarma | cobrocient | cobro | disenoA | facturad | disenoFa | fdisenoA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 2014-02-04 | 189 | 2 | D Bancaria 0182221791020156221 9 | 100 | 2014-06-15 | ✓ | 364 | 100 | ✓ | ✓ | ✓ | NULL |
| 11 | 2014-02-05 | 233 | 2 | D Bancaria 0046501261265385044 8 | 200 | 2014-06-15 | ✓ | 596 | 200 | ✓ | ✓ | ✓ | NULL |
| 12 | 2014-02-06 | 125 | 2 | Contado | 200 | 2014-12-15 | ✓ | 936,56 | 0 | ✓ | ✓ | ✓ | 2014-06-30 |
| 13 | 2014-02-07 | 7 | 2 | D Bancaria 3008006157148502402 8 | 144 | 2014-12-15 | ✓ | 936 | 0 | ✓ | ✓ | ✓ | 2014-06-30 |
| 14 | 2014-02-07 | 21 | 2 | D Bancaria 2100257414020011201 9 | 200 | 2014-03-15 | ✓ | 299 | 200 | ✓ | ✓ | ✓ | NULL |
| 15 | 2014-02-07 | 5 | 2 | D Bancaria 0081039881000148596 2 | 100 | 2014-12-15 | ✓ | 892 | 0 | ✓ | ✓ | ✓ | 2014-06-30 |
| 16 | 2014-02-07 | 217 | 2 | D Bancaria 2085568682050032736 1 | 200 | 2014-06-15 | ✓ | 596 | 200 | ✓ | ✓ | ✓ | NULL |
| 17 | 2014-02-07 | 118 | 2 | Cheque | 200 | 2014-09-15 | ✓ | 596 | 200 | ✓ | ✓ | ✓ | NULL |
| 18 | 2014-02-07 | 9 | 2 | D Bancaria 0182350026020158401 2 | 200 | 2014-06-15 | ✓ | 596 | 0 | ✓ | ✓ | ✓ | 2014-06-30 |
| 19 | 2014-02-07 | 24 | 2 | D Bancaria 3017056976215489072 6 | 200 | 2014-03-15 | ✓ | 299 | 200 | ✓ | ✓ | ✓ | NULL |
| 20 | 2014-02-07 | 6 | 2 | D Bancaria 2996058384327118690 4 | 100 | 2014-12-15 | ✓ | 892 | 100 | ✓ | ✓ | ✓ | NULL |
| 21 | 2014-02-07 | 3 | 2 | D Bancaria 0075057064666001330 | 200 | 2014-03-15 | ✓ | 299 | 200 | ✓ | ✓ | ✓ | NULL |
| 22 | 2014-02-07 | 130 | 2 | D Bancaria 2100144340200025289 | 144,56 | 2014-12-15 | ✓ | 936,56 | 144,56 | ✓ | ✓ | ✓ | NULL |
| 23 | 2014-02-07 | 2 | 2 | Transferencia | 200 | 2014-06-15 | ✓ | 596 | 200 | ✓ | ✓ | ✓ | NULL |
| 24 | 2014-02-07 | 4 | 2 | D Bancaria 2085566280550442579 | 144,56 | 2014-12-15 | ✓ | 936,56 | 144,56 | ✓ | ✓ | ✓ | NULL |
| 25 | 2014-02-07 | 8 | 2 | D Bancaria 0049175044231001060 7 | 140 | 2014-12-15 | ✓ | 932 | 140 | ✓ | ✓ | ✓ | NULL |
| 29 | 2014-02-07 | 71 | 2 | D Bancaria 0075014107060014710 7 | 200 | 2014-03-15 | ✓ | 398 | 200 | ✓ | ✓ | ✓ | NULL |
| 30 | 2014-02-07 | 312 | 2 | D Bancaria ES8000496684102118033 | 200 | 2015-01-15 | ✓ | 902 | 200 | ✓ | ✓ | ✓ | NULL |
| 35 | 2014-02-13 | 178 | 2 | D Bancaria 3008016389175502282 7 | 200 | 2014-08-15 | ✓ | 596 | 200 | ✓ | ✓ | ✓ | NULL |
| 40 | 2014-02-17 | 121 | 2 | D Bancaria | 200 | 2014-08-15 | ✓ | 596,56 | 200 | ✓ | ✓ | ✓ | 2014-06-30 |

© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0

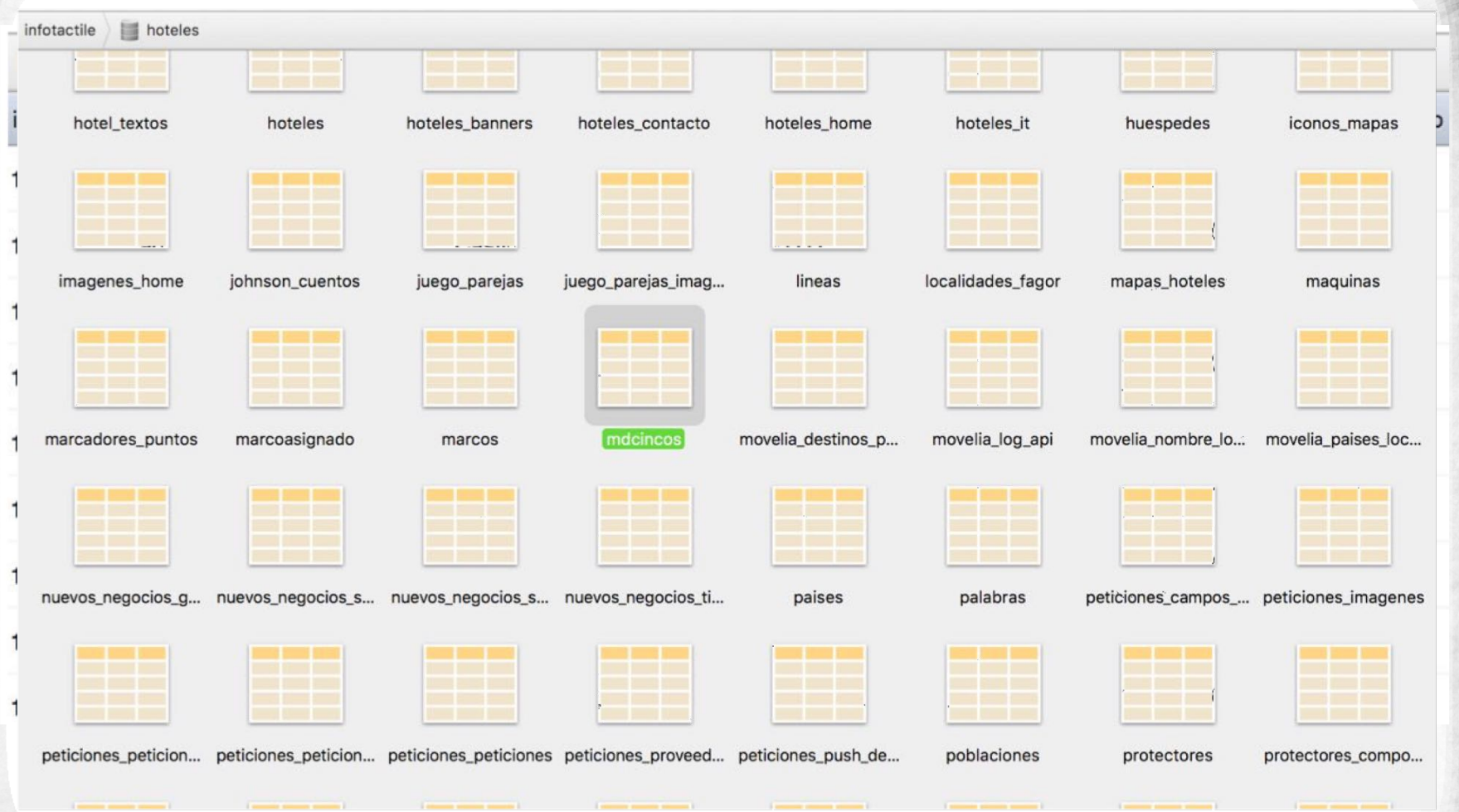
infotactile › hoteles › peticiones_push_devices

| id | gcm_regid | name | idterminal | fecha | usuario | pass |
|---|---|---|---|---|---|---|
| 24 | APA91bF5dASJzKThqiz3PASanVhwSAz296ZJ9DqmRYjsD_yu6DpPoVjg4M5ONVDUcTvY11yRZ... | HTC One | b1bbd7924901188d | 2014-10-22 12:10:18 | apple | apple |
| 25 | APA91bGN-a3pSjaicyQbTUixOvWy2hgh7Pi1zwL0Wvtaezjf... | DARKMOON | b9db9c22c2bb48 | 2014-10-22 17:33:08 | Leti | Leti |
| 26 | APA91bG3Cayw1qZSXJNBc3fN5E99V__gqw4RPLyhN9BodWxEwXIEm_AmPp4XgFC2M0yurd2... | LG-D802 | 74f0011f18de64a3 | 2014-10-23 09:43:44 | Leti | Leti |
| 31 | APA91bHtWY_yVyTUe0U_UJzzsGKkA6yg_QNaa6qb1tnNd2JHxYf58wFz9tkObRXVxrL5l9nO23W... | Nexus 5 | 2946ff43148ed010 | 2014-10-24 10:23:11 | NULL | NULL |
| 32 | APA91bFoxOv-IR0BovbLPNx0SUEFatsGW2dLoMbZaPC10Qc... | C6833 | 8f99444efe0b0de4 | 2014-10-24 17:37:45 | apple | apple |
| 33 | APA91bHi4ElvtqdteFg_wRvxJkUHAMPtRy81IjczlR2u0Xhs2vT-snrxP43RJlrliTttTUuFqUrduMoDz... | LG-E400 | aaee40c14f3a6dd1 | 2014-10-30 14:22:29 | NULL | NULL |
| 34 | APA91bGM0Qw1a2U5pQR1XpDLJcQEedJvt9szBxHzL9l1XMwzf39mbjXW_cH7Mk9RPd2ghoXV... | GT-I9505 | f20a2db1f798d260 | 2014-11-04 13:36:12 | demoinfo | demoinfo |
| 35 | APA91bHqgTCfyu0VYTPp9xrF_F9NeiLpvRy04CVZP0jOnKTIZBpdkachqKc3PsavySFU2zMlF_s... | LG-D855 | 70e0412075a824e5 | 2014-11-05 10:32:11 | NULL | NULL |
| 36 | APA91bEN726AxUXPdVuNGwngxFgWryvtD3NbxTSoRkvw8GMK2xDBnuSSA0Bmb4BuSGtiljjQC... | Coolpad 8297W | e433b3e3fada9601 | 2014-11-06 18:12:05 | dorado | caballos |
| 37 | APA91bFILhxpWUVCprwg_a0jPicA_NaXbmTcV7ydeBD0g3fzjc1IDoRaySg41Bw2p_S--AMCCsx-... | GT-I8730 | 24c495f54cbcc357 | 2014-11-09 19:15:14 | NULL | NULL |
| 38 | APA91bF63e_JLcj8e5aGKnWKkmp2jT8oJnrILzq2emgESpIBKVoGEmVQUlQDHDwTFYg9JZpg5u... | FIZZ | 4ca48cce3060b7db | 2014-11-10 18:06:43 | demoinfo | demoinfo |
| 39 | APA91bEXJuZ8KVw-zfHYAT81V_tJH-mwCxbz8hE98y5Uknhi2IfvSyf-P5uJUG5_vQdS... | A500 | 5551a69a7f442774 | 2014-11-10 23:20:16 | NULL | NULL |
| 54 | 88b3bd788e1f7ac6625b36f9eedd0591d0da5c3c4e97ca3ffeb95f5a614b9207 | IOS_iPad4,1 | ADD03288-0430-4B0B-A98E-0C3D71A8C1D8 | 2014-11-19 11:12:53 | apple | apple |
| 55 | 285ca1bb119078c9d4f0091988ac9a5f97eafc061d5b1cf7e91374621a89fdce | IOS_iPhone5,2 | 2B7D7D71-4F6C-4C3C-9ED2-1A80E42FADC3 | 2014-11-19 11:32:39 | demoinfo | demoinfo |
| 56 | APA91bEdPJiTqE6l_antPfYa7G0twIFnvl-cjS9WFDbkgo6Fe-PtYCCaoWTsdWW_UCu7So... | C6833 | 8f99444efe0b0de4 | 2014-11-19 13:20:20 | demoinfo | demoinfo |
| 57 | APA91bGDyINEkBgLcTK4qbhgmBSk4-O-9S99pEeoSlvwXJn9bTvuPK0Bdjk3_p8xPbY... | JY-G3 | 59becb558dc5c23e | 2014-11-19 13:22:32 | demoinfo | demoinfo |
| 58 | 9ad2fbd3deb95688d183c95d71b340e86d6f45e7632b562ed240a81d4d089bc6 | IOS_iPhone5,2 | D0B84373-98BD-4417-99F7-5040AD70312A | 2014-11-24 16:00:38 | NULL | NULL |
| 59 | f56768d5cbd65587cd9105b2a6926e9e02e158ffe92d01c2c6f580593ac0b2b8 | IOS_iPhone4,1 | 073D71F6-56BB-4D11-9262-EFFE84F3B8DE | 2014-11-27 10:48:23 | demoinfo | demoinfo |
| 60 | ed856ddca9bc800d9702505fa3faed909501a449ffc1b4fb82978ecc29303dcf | IOS_iPhone7,2 | F0054306-F868-4BBF-A23E-8B280DE86810 | 2014-12-01 13:52:44 | NULL | NULL |
| 61 | 658ac03d830ddec4579be2f0fdad62e4e28b48250c830366aed6b28e65306406 | IOS_iPhone6,1 | C3DEE76C-C6B0-4903-AC96-88BA0847D6EB | 2014-12-03 05:11:28 | NULL | NULL |
| 62 | 77c6da77e2689568b4d9cd2c8f2cbc777b6eace73f8806e42a4e9b377b29b620 | IOS_iPad2,2 | 23B2338B-6839-4868-95EA-75451039F0CB | 2014-12-17 23:29:52 | NULL | NULL |
| 63 | 1525b11c10903decf80e131ea59e1c37a4453af46e47617fc2dc09eaf30cad62 | IOS_iPad4,2 | BA3F1A9A-0EB8-4715-84BD-B93845CF7EF9 | 2014-12-23 21:58:55 | NULL | NULL |
| 64 | APA91bHX1n-IseRk8dGlzp1UwRCy1qxft21FY3lC4uGqiSC2N... | GT-I9105P | 594ed341e514a9d5 | 2015-01-18 16:00:37 | NULL | NULL |
| 65 | ff4f80880926eac1f21ab71b14abdf1bd31e4f6a6f5c2c5681d684f7e0afd17d | IOS_iPad2,2 | A67A05D8-855C-403D-9988-992E340A17DD | 2015-01-18 17:39:58 | NULL | NULL |

© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0

infotactile › hoteles › wifis

| id | hotel | inicio | fin | texto |
|---|---|---|---|---|
| 111 | 322 | 20[redacted]25 | 2[redacted]9-30 | Aquí iría su clave y las especificaciones que quiera poner |
| 132 | 307 | 20[redacted]10 | 2[redacted]0-26 | ALDEA BAR RECEPCION FREE. PASWORD: aldeacbosch09 |
| 142 | 388 | 20[redacted]23 | 2[redacted]7-12 | EXPOBCN5683 |
| 146 | 153 | 20[redacted]25 | 2[redacted]5-31 | CONTRASEÑA: 0906196000 |
| 147 | 137 | 20[redacted]25 | 2[redacted]6-25 | Contraseña: FREE |
| 150 | 330 | 20[redacted]09 | 2[redacted]7-01 | NETWORK: MUNIA PASSWORD: f984285580 NETWORK: HOTEL... |
| 152 | 277 | 20[redacted]06 | 2[redacted]8-30 | Usuario: granhotel Contraseña: 2020oviedo |
| 153 | 296 | 20[redacted]23 | 2[redacted]2-31 | CONTRASEÑA: lbbsal2015 |
| 157 | 439 | 20[redacted]29 | 2[redacted]2-31 | NETWORK: HOTEL ISABEL - USER: isabel - PASSWORD: 7islas2014 |
| 161 | 438 | 20[redacted]09 | 2[redacted]0-31 | ORIENTE36093 |
| 162 | 308 | 20[redacted]09 | 2[redacted]0-31 | DUNAS983759A |
| 165 | 440 | 20[redacted]07 | 2[redacted]2-31 | Wifi Network: parque Password: HotPar75... |
| 167 | 123 | 20[redacted]01 | 2[redacted]4-30 | WIFI GRATIS |
| 170 | 512 | 20[redacted]23 | 2[redacted]2-31 | RED Ilunion Suites Madrid Password 63da54dn8g |
| 173 | 439 | 20[redacted]12 | 2[redacted]2-31 | NETWORK: HOTEL ISABEL - USER: isabel - PASSWORD: 7islas2014 |
| 175 | 308 | 20[redacted]14 | 2[redacted]1-31 | DUNASwifi |
| 176 | 522 | 20[redacted]14 | 2[redacted]2-28 | WIFI CLAVE123 |
| 184 | 515 | 20[redacted]01 | 2[redacted]2-31 | USERNAME: teide PASSWORD: 3718... |
| 186 | 296 | 20[redacted]14 | 2[redacted]2-31 | CONTRASEÑA: lbbsal2015 |
| 190 | 66 | 20[redacted]10 | 2[redacted]4-03 | ¿Qué tienes pensado para Semana Santa? Descubre la oferta del Hotel Silken Indautxu: 15... |
| 192 | 387 | 20[redacted]18 | 2[redacted]1-01 | NETWORK: costaadeje PASSWORD: 7islas2014 |

© 2017 CS³ Group. Todos los derechos reservados.

# 5 Revolution 2.0




© 2017 CS³ Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

# 5 Revolution 2.0

Enviado - s4ur0n 19:15

**s4ur0n**
Vulnerabilidad en vuestros sistemas con un riesgo muy alto
Para: administracion@publipan.net Cc: eGarante
Seguridad: Firmado (s4ur0n@s4ur0n.com)

añadir...

Se ha encontrado un evento en este correo: 4 de febrero de 2017

Buenas tardes:

Quería comentaros que he visto vuestros paneles de información en un hotel este fin de semana y me parecen geniales, muy logrados y acertados, además de ser muy cómodos para el usuario.

Me dedico desde muchos años a la seguridad informática y he visto algunos fallos en vuestros sistemas que podrían presentar un riesgo y una exposición de datos muy alta y me gustaría poder comentarlos con alguna persona de vuestra empresa o responsable de desarrollo, ya que son principalmente de código.

Sin embargo, cuando busqué vuestra información en google, tras una pequeña búsqueda, se delata que existen varias vulnerabilidades en vuestro código y en la BB.DD que potencialmente podrían exponer incluso el contendio completo de todas vuestras BB.DD. sin mayor problema y sus contenidos. Hay algunas referencias como simplemente buscando en google "error site:infotactile.com" que ya revelan información sensible de vuestras conexiones e incluso la cadena de consulta empleada para recuperar los datos.

Principalmente, hay SQL Injection (https://www.owasp.org/index.php/Top_10_2013-A1-Injection) que permiten revelar el nombre del usuario y BBDD que emplea vuestro sistema, por lo que una simple conexión al servidor sin más, entraría en todo vuestro sistema ya que no se encuentra identificado por ningún tipo de password y está expuesto públicamente en Internet sin mayor protección.

El dominio afectado por las vulnerabilidades es en "infotactile.com" que referencia a 37.187.153.126 y se encuentra listado también en shodan (buscador de servicios) con el puerto 5432 expuesto públicamente en Internet (https://www.shodan.io/host/37.187.153.126).

Un usuario malicioso, simplemente conociendo la información del usuario con el que se conecta a vuestra BBDD y el nombre de la BBDD (ambos datos salen en simples consultas) al no tener autenticación ninguna, podría entrar sin más y tener acceso a todo, incluso para poder borrar/modificar/añadir datos que supongo que serán sensibles e incluso pueden afectar a clientes vuestros que podrían incluso denunciar que sus datos no han sido tratados conforme al Reglamento de Protección de Datos.

Además, dado que también al parecer el dominio "publipan.net" es prácticamente igual en contenido, podría ser que los mismos fallos de seguridad se encontrasen también en el mismo.

Entendiendo que nuestra responsabilidad moral debe ser comunicaros responsablemente las vulnerabilidades que a veces vemos, quedo a vuestra disposición para cualquier cosa que queráis comentar y/o poderos ayudar a solucionar estas vulnerabilidades lo más rápido posible. Para evitar malentendidos, comentaros que esto lo hago de forma completamente altruista, ya que me parece lógico avisaros que un ciberdelincuente podría aprovecharse de la información que contenga o perjudicar gravemente a vuestra empresa.

Muchas gracias por vuestra atención.

Un saludo,

Pedro C. aka s4ur0n
GPG 0x42386475 | s4ur0n
http://s4ur0n.com
@NN2ed_s4ur0n

© 2017 CS³ Group. Todos los derechos reservados.

# GRACIAS



CS³ SECURITY SERVICES
https://cs3group.com

**© 2017 CS³ GROUP. Todos los derechos reservados.**

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.