



Fraud as a Service

Gabriel Bergel

Gabriel Bergel



- Cursando Magister de Ciberseguridad Universidad Camilo José Cela
- CISSP, C|CISO, CISM, CBCP, ISO 27001 LA
- 15 años de experiencia, Consultor, JP, ISO, CISO, Rockstar.
- CSA en Eleven Paths / Director de Estrategia (CSO) en Dreamlab Technologies
- Profesor de Seguridad de la Información en UNAB
- Fundador y Organizador de 8.8 Computer Security Conference
- Vicepresidente del Capítulo de (ISC)2 y Director Académico del Capítulo de ISSA
- Miembro de LAAC de (ISC)2
- Coordinador del Centro de CiberSeguridad Industrial (CCI)
- Relator de Charlas de Seguridad en Colegios



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

Agenda



**Introducción FAAS –
Sector Financiero (DBIR 2016)**

Cibercrimen en Sector Financiero

**Contramedidas de la Industria
Desafíos**

**Recomendaciones
Conclusiones**



Introducción

FAAS SECTOR FINANCIERO



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

FAAS

Sólo es necesario tener
un PC, conexión a
internet, Tor y Bitcoins



Servicios garantizados,
postventa, soporte,
devolución del dinero



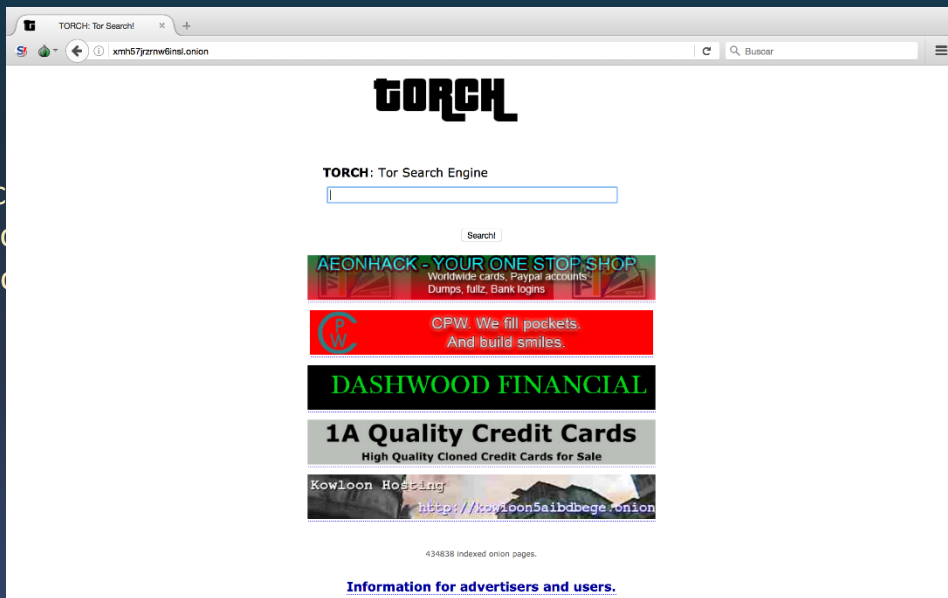
Cibercrimen
Organizado
“Ellos si comparten la
información”



FAAS

Sólo es necesario
un PC, conexión a
internet, Tor

no
o
orden la
h"



Sólo es necesario
un PC, conexión a
internet, y tener la

“necesidad”

A1 Quality Credit Cards

2222ppcgy2amp23.onion

Buscar

1A Quality Credit Cards Store

Hi there, I'm selling cloned credit cards with PIN code, ready for using at ATM. The cards are mostly VISA and MasterCard; they work worldwide. Cards are discreetly mailed worldwide using priority mail. We are the only ones with English attention.

Our Prices

!!! Free Express Shipping !!!

Free express shipping within 48-72 hours for every order

- 1 card with **\$1000** guaranteed and up to **\$2000** - 0.20 BTC
- 1 card with **\$2000** guaranteed and up to **\$3000** - 0.25 BTC
- 1 card with **\$3000** guaranteed and up to **\$4000** - 0.30 BTC
- 1 card with **\$4000** guaranteed and up to **\$5000** - 0.35 BTC
- 1 card with **\$5000** guaranteed and up to **\$6000** - 0.40 BTC

- 1 card with **€1000** guaranteed and up to **€2000** - 0.20 BTC
- 1 card with **€2000** guaranteed and up to **€3000** - 0.25 BTC
- 1 card with **€3000** guaranteed and up to **€4000** - 0.30 BTC
- 1 card with **€4000** guaranteed and up to **€5000** - 0.35 BTC
- 1 card with **€5000** guaranteed and up to **€6000** - 0.40 BTC

All our Goods are 100% Verified
I will give a great deal on orders of more than 1 card



Sólo es necesario
un PC, conexión a
internet, T

no
o
ten la
h"

A1 Quality Credit Cards
2222ppclgy2amp23.onion

About Us

We are a small dedicated team of hackers, we operate botnets and install card readers at atm's to get credit card details. We sell the most demanded products on the deepweb, we have specialized and have over 6 years experience in this field.

We sell cards from the USA and from the EU.

We not make all the withdraws for ourselves for the risk.

All the cards come with PINs and instructions. You can use them at any ATM worldwide.

If you want your name embossed on the card let us know



Contact/Order

How do I order?

To fully understand what our customer needs, we process all the orders by e-mail

To place an order, just send us an e-mail containing the following:

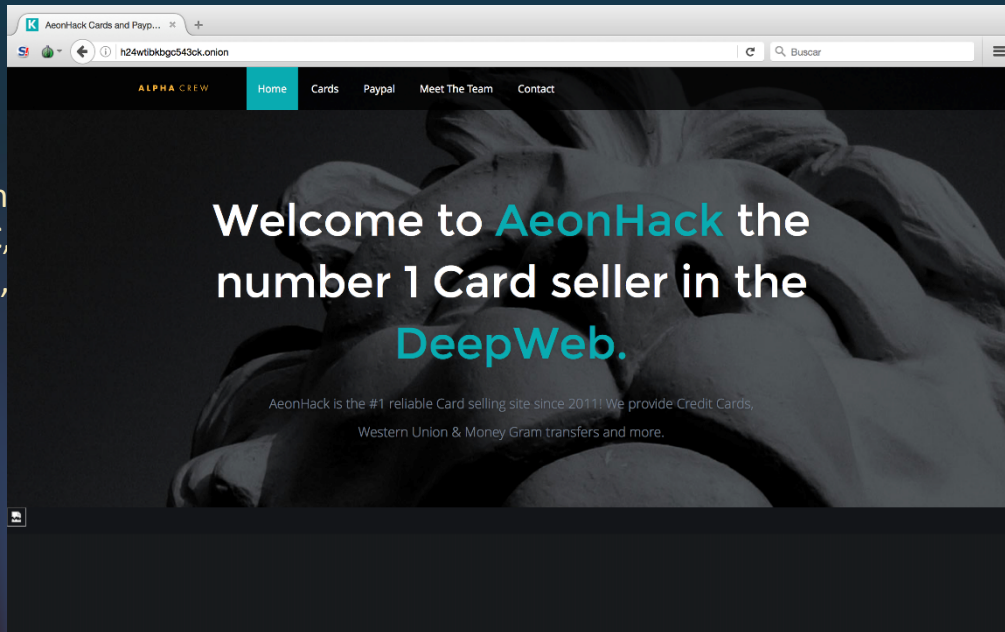
- 1 - The type of card you need (VISA or MasterCard)
- 2 - How many cards you need
- 3 - The name you want embossed on the card/s (optional)

You can Contact Us at **1Acards@sigaint.org**



FAAS

Sólo es n
un PC,
internet,

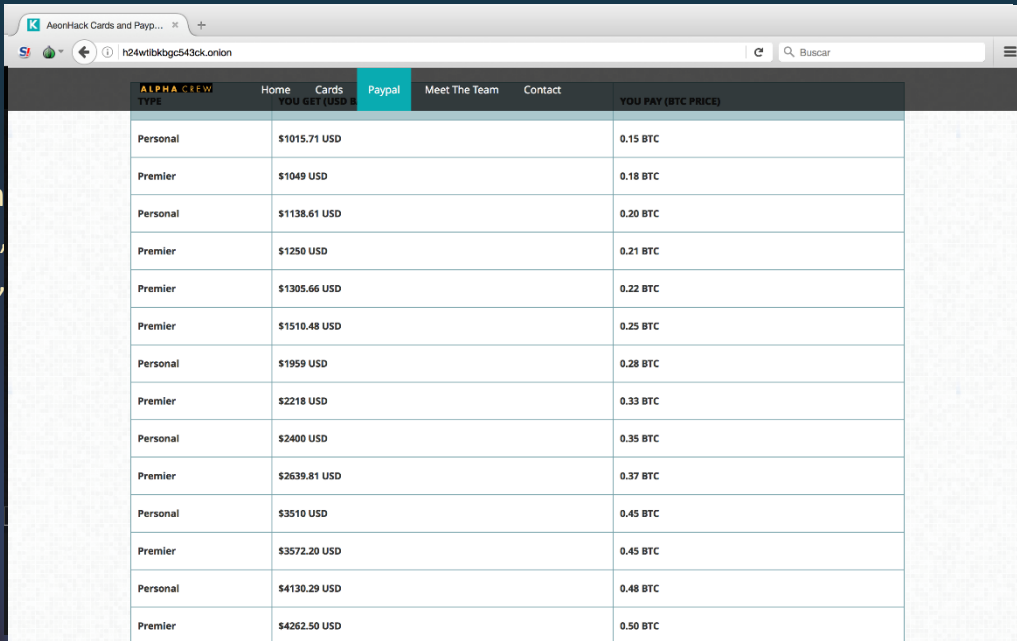


en la



FAAS

Sólo es n
un PC,
internet,



The screenshot shows a web browser window with the address bar displaying "h24wtlkbkgc543ck.onion". The page title is "AeonHack Cards and Pay...". The browser's address bar includes a search icon and the text "Buscar". The page content features a table with the following structure:

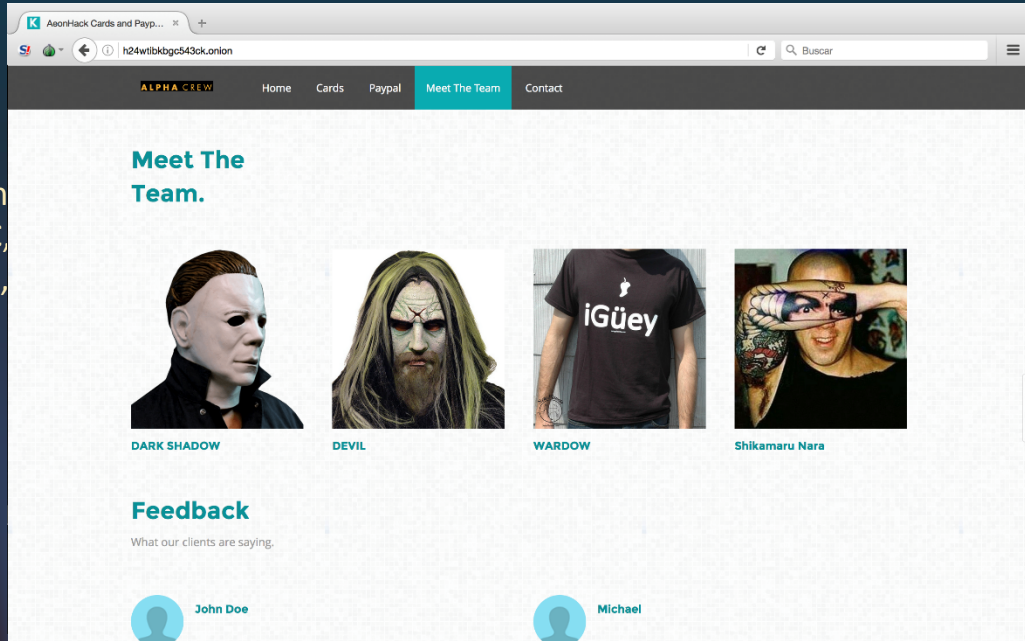
ALPHA KREW TYPE	Home Cards YOU GET (USD)	Paypal	Meet The Team	Contact	YOU PAY (BTC PRICE)
Personal	\$1015.71 USD				0.15 BTC
Premier	\$1049 USD				0.18 BTC
Personal	\$1138.61 USD				0.20 BTC
Premier	\$1250 USD				0.21 BTC
Premier	\$1305.66 USD				0.22 BTC
Premier	\$1510.48 USD				0.25 BTC
Personal	\$1959 USD				0.28 BTC
Premier	\$2218 USD				0.33 BTC
Personal	\$2400 USD				0.35 BTC
Premier	\$2639.81 USD				0.37 BTC
Personal	\$3510 USD				0.45 BTC
Premier	\$3572.20 USD				0.45 BTC
Personal	\$4130.29 USD				0.48 BTC
Premier	\$4262.50 USD				0.50 BTC

n la



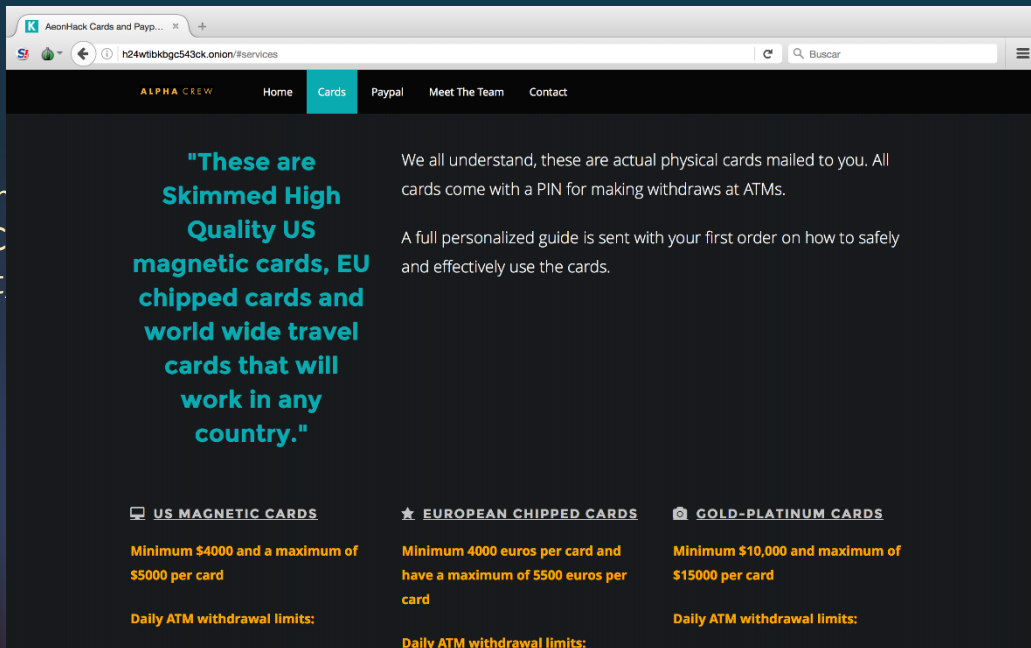
Sólo es n
un PC,
internet,

n la



FAAS

Sólo es necesario
un PC o un
internet



The screenshot shows a web browser displaying the Alpha Crew website. The browser's address bar shows a URL starting with 'h24wtibkbgc543ck.onion//services'. The website has a dark theme with a navigation bar at the top containing 'ALPHA CREW', 'Home', 'Cards' (highlighted in teal), 'Paypal', 'Meet The Team', and 'Contact'. The main content area features a large teal quote: "These are Skimmed High Quality US magnetic cards, EU chipped cards and world wide travel cards that will work in any country." To the right of the quote, there is explanatory text: "We all understand, these are actual physical cards mailed to you. All cards come with a PIN for making withdrawals at ATMs." and "A full personalized guide is sent with your first order on how to safely and effectively use the cards." Below this, there are three columns of card options, each with an icon and a title: a laptop icon for 'US MAGNETIC CARDS', a star icon for 'EUROPEAN CHIPPED CARDS', and a camera icon for 'GOLD-PLATINUM CARDS'. Each column lists minimum and maximum values and mentions 'Daily ATM withdrawal limits:'.

"These are Skimmed High Quality US magnetic cards, EU chipped cards and world wide travel cards that will work in any country."

We all understand, these are actual physical cards mailed to you. All cards come with a PIN for making withdrawals at ATMs.

A full personalized guide is sent with your first order on how to safely and effectively use the cards.

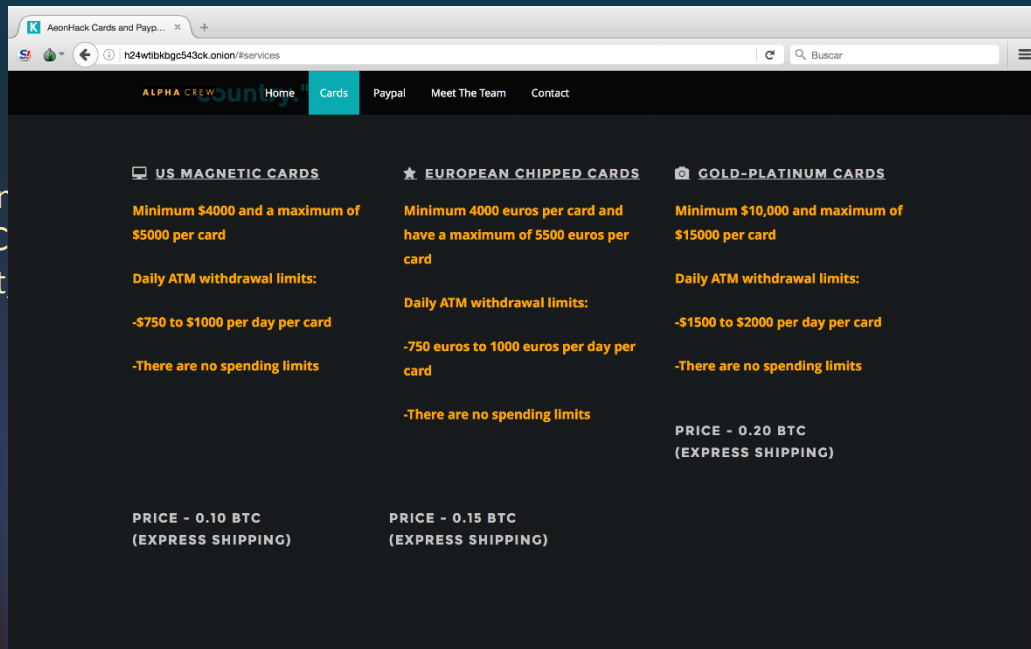
 <u>US MAGNETIC CARDS</u>	 <u>EUROPEAN CHIPPED CARDS</u>	 <u>GOLD-PLATINUM CARDS</u>
Minimum \$4000 and a maximum of \$5000 per card	Minimum 4000 euros per card and have a maximum of 5500 euros per card	Minimum \$10,000 and maximum of \$15000 per card
Daily ATM withdrawal limits:	Daily ATM withdrawal limits:	Daily ATM withdrawal limits:

la



FAAS

Sólo es necesario
un PC
internet



The screenshot shows a web browser displaying the Alpha Crew website. The browser's address bar shows the URL `h24wtibkbgc543ck.onion//services`. The website has a dark theme with a navigation bar at the top containing links for Home, Cards, Paypal, Meet The Team, and Contact. The main content area is divided into three columns, each representing a different card type:

US MAGNETIC CARDS	★ EUROPEAN CHIPPED CARDS	📷 GOLD-PLATINUM CARDS
Minimum \$4000 and a maximum of \$5000 per card	Minimum 4000 euros per card and have a maximum of 5500 euros per card	Minimum \$10,000 and maximum of \$15000 per card
Daily ATM withdrawal limits:	Daily ATM withdrawal limits:	Daily ATM withdrawal limits:
- \$750 to \$1000 per day per card	- 750 euros to 1000 euros per day per card	- \$1500 to \$2000 per day per card
- There are no spending limits	- There are no spending limits	- There are no spending limits
PRICE - 0.10 BTC (EXPRESS SHIPPING)	PRICE - 0.15 BTC (EXPRESS SHIPPING)	PRICE - 0.20 BTC (EXPRESS SHIPPING)

h la



FAAS

Sólo es n
un PC
internet

TORCH search results for: atm ...

Search for: atm malware Search Extended

Search for atm malware. Search results: atm : 3314, malware : 1647. Results 1-10 of 109. Search took 0.868 seconds

Sort by: relevancy | last modified date | title

STOCK INSIDER KNOWLOON Hosting Services Jorah serves over 50,000 queries a day Jorah serves over 50,000 queries a day Jorah serves over 50,000 queries a day Jorah serves over 50,000 queries a day

1. [Oniondir - Hacking](#) [0.243%]
... 2.0 Learn To Hack Terminals And **ATM**'s Or Work For Us! :) Our blackmarket ... 01:53:02 100% up (last 7 days) **Malware** as Service 0
0 I make custom Windows **malware** for some BTC, see the site for more ...
 - <http://autwvp2nmbqkfq.onion/?cat=5> - 19673 bytes [text/html] - Tue, 24 May 2016, 08:51:01 BST
[Cached copy]
2. [Oniondir](#) [0.243%]
... 1.0 Learn To Hack Terminals And **ATM**'s Or Work For Us! :) Our blackmarket ... 16:50:05 100% up (last 7 days) **Malware** as Service 0
0 I make custom Windows **malware** for some BTC, see the site for more ...
 - <http://autwvp2nmbqkfq.onion/?cat=5&p=0> - 19673 bytes [text/html] - Sun, 01 May 2016, 09:19:02 BST
[Cached copy]
3. [Oniondir](#) [0.243%]
... 1.0 Learn To Hack Terminals And **ATM**'s Or Work For Us! :) Our blackmarket ... 21:30:03 100% up (last 7 days) **Malware** as Service 0
0 I make custom Windows **malware** for some BTC, see the site for more ...
 - <http://autwvp2nmbqkfq.onion/index.php?cat=5> - 20320 bytes [text/html] - Thu, 05 May 2016, 18:37:29 BST
[Cached copy]
4. [CC guru is a scammer - Hidden Answers](#) [0.236%]
... (9) Darknet Markets (710) Hacking/ **Malware**/ Tech (2,793) Erotica (492) Financial ... To mount this simply put in on a real **ATM**'s
buttons and wait for a victim. ... not only about stealing cc data at the **ATM**, it also includes POS machines and ...
 - <http://answerstothetech.onion/83172/cc-g...> - 193741 bytes [text/html] - Wed, 18 May 2016, 14:46:37 BST
[Cached copy]
5. [CC guru is a scammer - Hidden Answers](#) [0.236%]



FAAS

Sólo es n
un PC
internet

C'thulu Resume

UK Guns and Ammo Store - ...

+

cthuluuap7ch47k.onion

Buscar

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000
Cripple Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$12,000	\$24,000	\$48,000
Uglify	\$18,000	\$36,000	\$72,000
Two Hands	\$24,000	\$48,000	\$96,000
Paralyse	\$30,000	\$60,000	\$120,000
Rape	Low Rank	Medium Rank	Family Members
Regular	\$7,000	\$14,000	\$28,000
Under age	\$21,000	\$42,000	\$84,000
Bombing	Low Rank	Medium Rank	Family Members
Simple	\$5,000	\$10,000	\$20,000
Complex	\$10,000	\$20,000	\$40,000
Besting	Low Rank	Medium Rank	Family Members
Simple	\$3,000	\$9,000	\$18,000

We need:

Name,
Country and City,
Clear and recent picture of target,
And any other information you can provide will speed things up.

Contact:

Mai: BM-2cVbNcn18dhfcefaX73USLq4dYTIxW7U@bitmessage.ch
PGP/GPG Encryption: [Download Key](#)



Sólo es
un PC
internet



Debit Card

@NeedADebitCard

Please quit posting pictures of your debit cards, people.

Joined May 2012

 Tweet to Debit Card

 7 Followers you know



 Photos and videos

TWEETS
192

FOLLOWERS
18.1K

Tweets

Tweets & replies

Media



Debit Card Retweeted



@Yellowschoolbus · Aug 17

My new debit card!! Blue looks good



1.1K

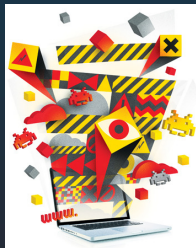


808



Sector Financiero (Fuente DBIR 2016)

3 -> 9 patrones de ataques= 88%



48%



Dridex



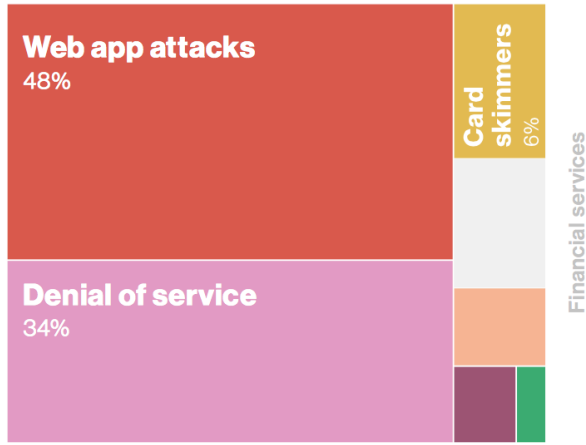
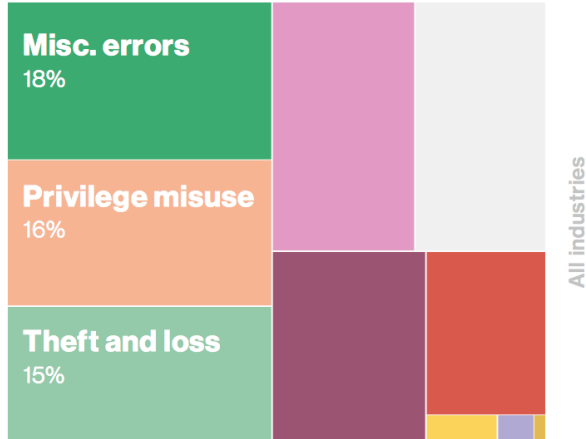
34%



6%

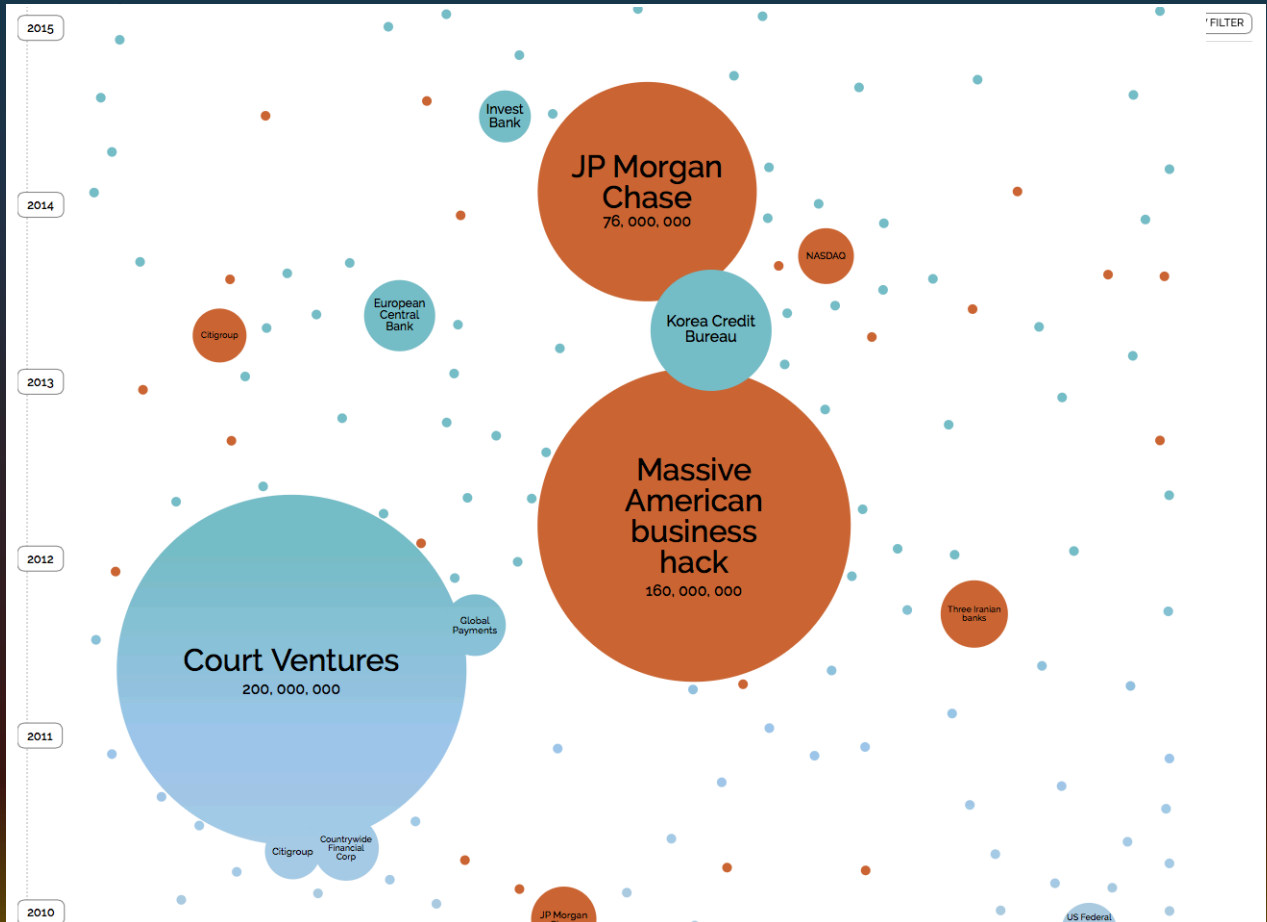
High Lights

- 89% de las brechas tenía un motivo económico o espionaje.
- 63% de las violaciones confirmadas involucraban autenticación débil, o por defecto o contraseñas robadas.
- 30% de los mensajes de phishing se abrieron en 2015 y el 12% de los objetivos hace clic en el archivo adjunto malicioso o enlace.
- 85% del trafico exitoso de exploit era a partir de los 10 principales vulnerabilidades. El otro 15% cubrió 900 vulnerabilidades.



Brechas Mundiales

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



CIBERCRIMEN SECTOR FINANCIERO



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

BANCA / INSTITUCIONES FINANCIERAS

27/05/2015

Transbank acusa intentos de ciberataque para colapsar el sistema

Fuentes al interior de la entidad encargada de Webpay afirman que ésta es la razón detrás de un servicio que en determinados lapsos puede ser más lento.



Tran
cola
Fuente
detrás

FISCALÍA CENTRO NORTE LLEVA INVESTIGACIÓN

Sabotaje informático al BCI: roban \$ 1.000 millones de las cuentas de la Sofofa y las multinacionales DHL y Salfa

28

COMENTARIOS

Jorge Molina Sanhueza | 15 Octubre, 2015

Tags: **BCI**, **Chilean News**, **dhl**, **fiscalía**, **salfa**, **seguridad**, **Sofofa**, **ssabotaje informatico**

Fotos: The Clinic



EL MERCURIO NACIONAL

C

SANTIAGO DE CHILE, DOMINGO 7 DE FEBRERO DE 2016

nacional@mercurio.cl

Alerta policial especialmente en regiones por período de vacaciones:

Clonación de tarjetas bancarias se duplica en el último año y delito sigue al alza

En 2014 se registraron 14.282 denuncias, mientras que en 2015 hubo 28.066, es decir, un incremento del 97%. Bandas especializadas operan por medio de bases de datos.

CATALINA YOB ÁLVAREZ

El lunes 18 de enero, una mujer de 61 años, de iniciales M.P.M.K., concurrió a una estación de servicio de Vitacura donde solicitó \$10 mil en combustible.

El bombero del local olvidó controlar el precio de los litros y detuvo el contador al llegar a los \$32 mil. Debido a esto, la cliente, quien reside en la misma comuna y pretendía pagar en efectivo, tuvo que hacer uso de su tarjeta de débito del Banco Bice.

Dos días después, recibió una llamada de la entidad bancaria, alertándola por una "actividad extraña" en sus movimientos financieros. Habían sido retirados \$900 mil desde diversos cajeros ubicados en la provincia de San Antonio. Al bloquear su



La clonación de tarjetas es un delito que se está extendiendo rápidamente a las regiones del país, según expertos del NSJ.

1.364
denuncias fueron realizadas en enero de 2015, mientras que en el mismo mes de este año, se registraron 2.112. Es decir, hubo un alza de 56% en este tipo de acusaciones.

107
detenidos por este tipo de ilícito hubo en 2015. En 2014 la cifra llegó a 73.

11
personas fueron detenidas en enero del año pasado tras ser acusadas de uso fraudulento de tarjetas bancarias. Mientras que en 2016 ya suman 16 los imputados.

Fache se percató de un retiro indebido de su cuenta al revisar los últimos giros en la página web del Banco Estado. Doscientos mil pesos habían sido extraídos desde un cajero. El hecho le despertó sospecha, porque durante la semana solo utilizó su tarjeta Cuenta RUT en un cajero automático y en un local de Maipencillo.

Luego de bloquearla y pre-

producido al menos cinco casos de clonación en la misma Región de Valparaíso.

Al respecto, el mayor Morales indica que antiguamente las bandas no solían movilizarse fuera de la capital, pero que hoy —y con mayor razón durante las vacaciones de verano— han ido modificando los lugares donde deciden realizar este tipo de ilícitos.

Carabineros describe el fenó-

Sorpréndete con grandes ofertas en **CyberMonday**

Lo quiero

movistar
Elige todo

Aumentan denuncias y reclamos por clonación de tarjetas en primera parte del año

Con el objetivo de informar y disminuir estos delitos, el Servicio Nacional del Consumidor junto a la PDI dieron inicio a la campaña "Tarjeta Segura".

21 de Julio de 2016 | 12:07 | Por Fernanda Fernández, Emol



Un 27% aumentaron los reclamos en el Sernac por delitos de clonación de tarjetas de crédito.

Sernac



RECOMENDADOS DEL EDITOR



GUÍA: Todo lo que hay que saber de la elección en EE.UU.

104 comentarios



PENSIONES: Qué han dicho Piñera, Guillier y Lagos

216 comentarios



UNIVERSIDADES: ¿Por qué las con gratuidad dejaron de recibir \$30 mil millones?

79 comentarios

27/05/2015

C

nacional@mercurio.cl

uplica alza

107
etenedos
or este tipo
ilícito hubo
n 2015. En
D14 la cifra
legó a 73.

11
personas fueron
detenidas en enero
del año pasado tras
ser acusadas de uso
fraudulento de tarjetas
bancarias. Mientras
que en 2016 ya suman
16 los imputados.

producido al menos cinco casos
de clonación en la misma Región
de Valparaíso.

Al respecto, el mayor Morales
indica que antiguamente las ban-
das no solían movilizarse fuera
de la capital, pero que hoy —y
con mayor razón durante las va-
caciones de verano— han ido
modificando los lugares donde
deciden realizar este tipo de ilíc-
tos.

Carabineros describe el fenó-

Nacional

Compartir



27/05/2015

Sernac y PDI revelaron nuevos métodos de clonación de tarjetas de crédito

Autor: **Marié Scarpa**

Aumentar primera p

Con el objetivo d
inicio a la campa

21 de Julio de 2016 | T

La campaña se lanzó para entregar recomendaciones a los consumidores frente a un delito que ya acumuló 1.400 reclamos en el Servicio durante el primer semestre de 2016.

Tarjeta Segura

Previene la clonación



000 4367 87463 3111

3464

VALIDA HASTA 04/24

En 2014 se i
un increme

CATALINA YOB ÁLVAREZ

El lunes 18 de enero de 61 años, de inicial concurrencia a una estación de Vitacura de \$10 mil en combustil

El bombero del 1 controló el precio de detuvo el contador a \$32 mil. Debido a esto quien reside en la man y pretendía pagar tuvo que hacer uso de débito del Banco

Dos días después, llamada de la entidad alertándola por una "extraña" en sus movimientos financieros. Habían dos \$900 mil desde jeros ubicados en la de San Antonio. Al

Un 27% aumentar

C

nacional@mercurio.cl

plica
za

7
idos
tipo
hubo
5. En
cifra
73.

11
personas fueron
detenidas en enero
del año pasado tras
ser acusadas de uso
fraudulento de tarjetas
bancarias. Mientras
que en 2016 ya suman
16 los imputados.

roducido al menos cinco casos de clonación en la misma Región de Valparaíso.

Al respecto, el mayor Morales indica que antiguamente las banderolas no solían movilizarse fuera de la capital, pero que hoy —y con mayor razón durante las vacaciones de verano— han ido modificando los lugares donde suceden este tipo de ilícitos.

Carabineros describe el fenómeno

Eje MANUAL DE USO DE TARJETAS DE CRÉDITO



En el caso de los cajeros, la recomendación para el usuario es **fijarse en el lector de tarjetas, pues en esta zona se ubican habitualmente los "skimmers" o dispositivos utilizados para clonarlos.**

También se deben mirar las ranuras de las salidas de dinero y el teclado, pues allí se podrían encontrar otras amenazas que favorecerían a los delincuentes que quisieran suplantar identidades y hacer uso de las cuentas.

En el caso de las máquinas para realizar pagos, los criminales **suelen reemplazarlas por una que clona tarjetas o también, mediante un "skimmers" adulterado, almacenan datos digitalmente.**

Entre otras sugerencias para el consumidor, están:

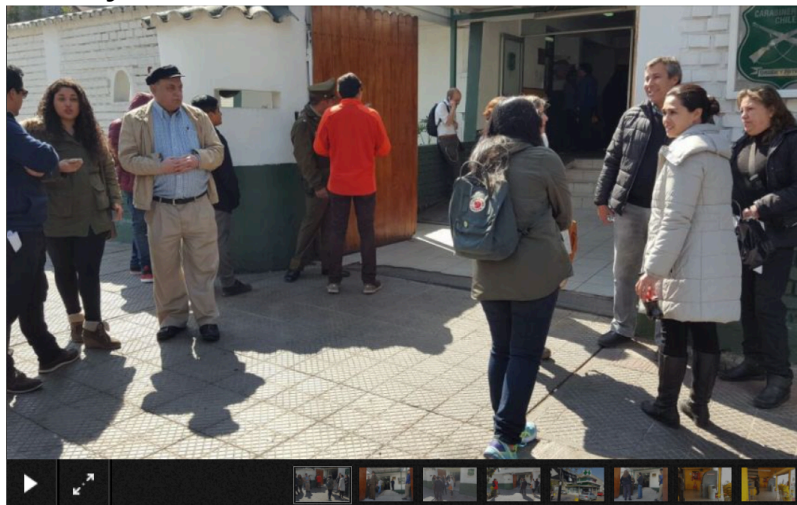
- Evitar ocupar cajeros en lugares aislados o con personas desconocidas cerca. 
- No pedir consejos a desconocidos ni aceptar recomendaciones. 
- Ante cualquier elemento extraño en el cajero, no hacer la operación y comunicárselo al banco.
- Revisar el entorno del cajero en busca de micro cámaras ocultas apuntando el teclado.
- Tapar siempre el teclado con su otra mano cuando digite su clave secreta.
- Cambiar su clave frecuentemente y usar códigos alfanuméricos difíciles de adivinar. Estos debe memorizarlos. 
- Tener a mano el número de teléfono para bloquear la tarjeta. 

que clona tarjetas o también, mediante un “skimmers” adulterado, almacenan datos digitalmente.

Eje MANUAL DE U Más de 200 afectados por clonación masiva de tarjetas en Providencia

Entre otras suger

- Evitar oc
- No pedir
- Ante cua al banco.
- Revisar e teclado.



s cerca.

comunicárselo

tando el

reta.

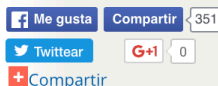
es de adivinar.

an datos

- Tapar sie
- Cambiar Estos del
- Tener a r

ACTUALIZADO : 2 Septiembre
PUBLICADO : 2 Septiembre

NATHALY LEPE



RELACIONADOS



Según comentaron las víctimas a Publimetro, la mayoría de los afectados por el fraude trabajan en el cuadrante de Eliodoro Yáñez, Valenzuela Castillo y Manuel Montt de dicha comuna.

Más de 200 personas habían llegado hasta el medio día de este viernes hasta la 19ª Comisaría de Carabineros de Providencia, ubicada en calle Miguel Claro, para estampar una denuncia luego de detectar que sus tarjetas bancarias habían sido clonadas.

Los afectados, en muchos casos compañeros de trabajo no daban crédito por la gran cantidad de personas que se encontraban en el recinto policial en su misma situación.

En más de algún caso, las personas afectadas sólo notaron que habían sido víctimas de la estafa cuando sus cuentas ya estaban en cero.

que clona tarj
digitalmente.

Eje MA

que
dig

12 de Octubre de 2016 | 06:30 | Emol



[El Mercurio \(archivo\)](#)

Raspberry Pi, el cual es usado para fines educativos o proyectos de robótica y que tiene muy bajo costo: en tiendas chilenas cuesta alrededor de \$40 mil, señala ["El Mercurio"](#).



RECOMENDADOS DEL EDITOR



GUÍA: Todo lo que hay que saber de la elección en EE.UU.

unicárselo



PENSIONES: Qué han dicho Piñera, Guillier y Lagos

UNIVERSIDADES: ¿Por qué las con gratuidad dejaron de recibir \$30 mil millones?

e adivinar.

NOTICIAS MÁS COMENTADAS



T13



TELE13 RADIO



ELECCIONES EN EEUU

PRESIDENCIALES 2017

REAJUSTE SECTOR PÚBLICO

CYBERMONDAY

TORNEO DE APERTURA 2016

IN

sura



DONDE UN CHEF VE SU ARTE, NOSOTROS VEMOS CRECER.
SURA, ahorra con productos de inversión.



T13

CLONACIÓN EN CAJEROS VÍA WIFI

21:06

f teletrece



@t13



www.t13.cl



21:36 hrs. Miércoles 12 Octubre 2016

Carabineros descubre nueva tecnología para clonar tarjetas bancarias

Los cajeros son alterados con mini computadores que son conectados al sistema operativo del dispensador. Y no solo eso, la información obtenida puede ser exportada vía Wi Fi.

árselo

inar.

Eje MA Detectan moderno dispositivo que clona tarjetas y permite robar datos a distancia

Entre

Luego del allanamiento al departamento de una banda colombiana especializada, Carabineros advierte que ha habido tres intentos para instalar este mecanismo en el país, pero que fueron frustrados.

12 de Octubre de 2016 | 06:30 | Elmol



El Mercurio (archivo)

SANTIAGO.- El OS-9 de Carabineros desbarató una banda de ocho ciudadanos colombianos que clonaba tarjetas en distintos cajeros automáticos de la Región Metropolitana.

En el allanamiento realizado a un departamento en la calle San Diego —aparte de tarjetas clonadas, lectores de bandas magnéticas y otros elementos— se incautó un minicomputador llamado Raspberry Pi, el cual es usado para fines educacionales o proyectos de robótica y que tiene muy bajo costo: en tiendas chilenas cuesta alrededor de \$40 mil, señala ["El Mercurio"](#).



RECOMENDADOS DEL EDITOR



GUÍA: Todo lo que hay que saber de la elección en EE.UU.

104 comentarios



PENSIONES: Qué han dicho Piñera, Guillier y Lagos

216 comentarios



UNIVERSIDADES: ¿Por qué las con gratuidad dejaron de recibir \$30 mil millones?

79 comentarios

NOTICIAS MÁS COMENTADAS



ca.

unicárselo

lo el

e adivinar.

atos



21:22

INÉDITO SISTEMA DE CLONACIÓN DE TARJETAS

f teletrece

@t13

www.t13.cl

21:22 hrs. Martes 25 Octubre 2016

El nuevo método de clonación de tarjetas que afecta a Chile

Un grupo de delincuentes búlgaros trajo la inédita fórmula, que hace inútiles las principales recomendaciones para detectar fraudes.

Los cajeros son alterados con mini computadores que son conectados al sistema operativo del dispensador. Y no solo eso, la información obtenida puede ser exportada vía Wi Fi.

NACIONAL

"Caja mágica": PDI descubre un nuevo método de clonación en cajeros

25

OCTUBRE
2016

POR 24HORAS.CL TVN

Para cometer estos actos, los delincuentes se coluden con un técnico de cajeros automáticos. El trabajador instala una caja que roba la información de los plásticos.

Twitter

+ Compartir

0

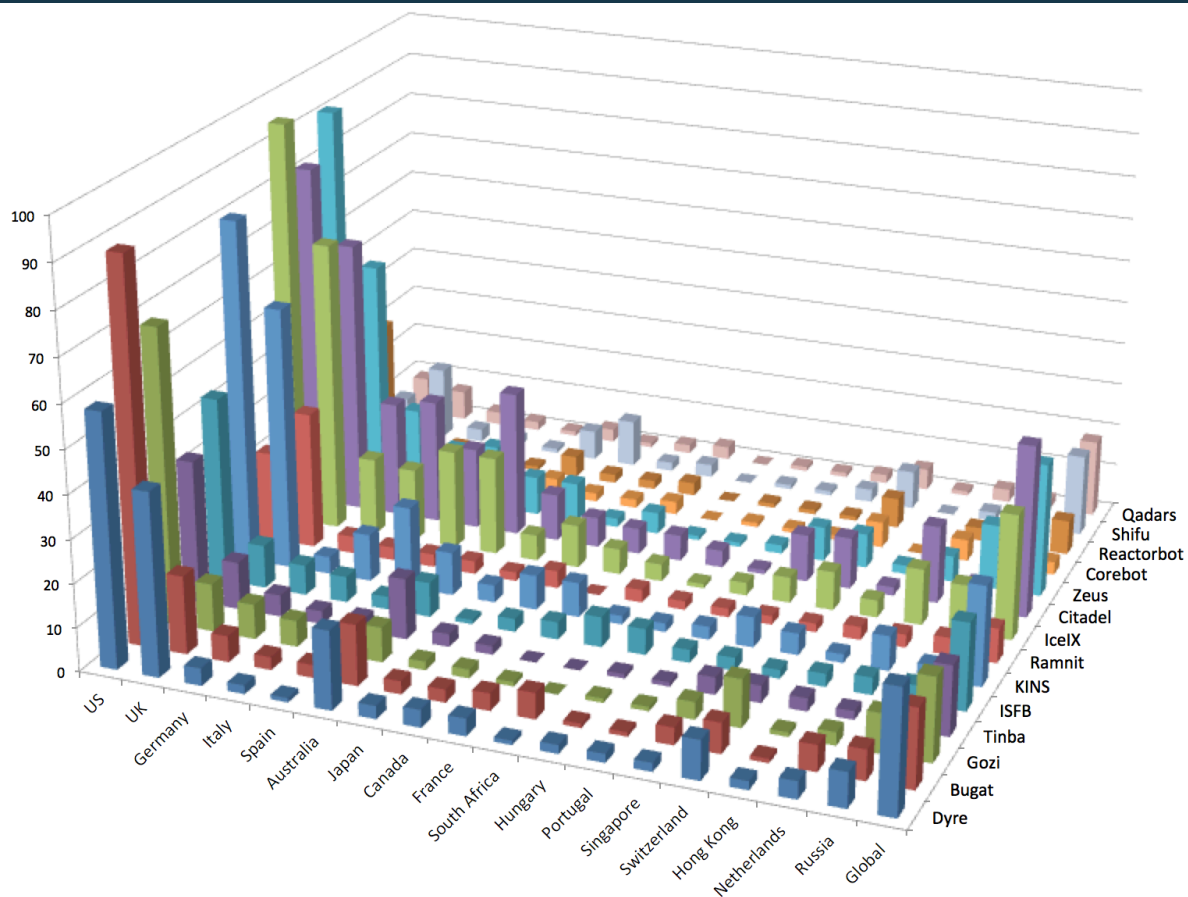
f Compartir

1.322



"CAJA MÁGICA": PDI DESCUBRE UN NUEVO MÉTODO DE CLONACIÓN EN CAJEROS

Malware Bancario



How the Carbanak cybergang stole \$1bn

A targeted attack on a bank

1. Infection

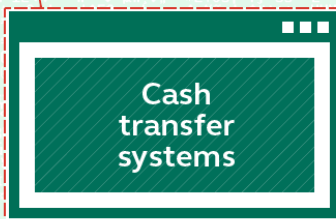


100s of machines infected
in search of the admin PC



2. Harvesting Intelligence

Intercepting the clerks' screens



3. Mimicking the staff

How the money was stolen

Online-banking

Money was transferred to fraudsters' accounts

E-payment systems

Money was transferred to banks in China and the US

Inflating account balances

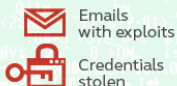
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs

Orders to dispense cash at a pre-determined time

How the Carbanak A targeted attack

1. Infection

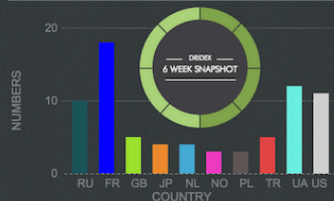


100s of machines infected
in search of the admin PC



© 2015 Kaspersky Lab

DRIDEX



DISTRIBUTION

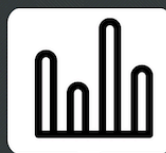


France has offered the greatest support to Dridex in terms of C2s and compromised servers, this is supported by way of a referral fee on carder & malware forums

DELIVERY



45% .DOC



35% .XLS



20% .PDF

CONTENT

INVOICE



REMITTANCE



PAYMENT



bn

the staff

ey was stolen

anking

ransferred
accounts

systems

ransferred
ia and the US

unt balances

were pocketed
t transaction

g ATMs

nse cash at a
ined time

KASPERSKY

Ataques Web

Esto es cuando los atacantes utilizan credenciales robadas o explotan vulnerabilidades en aplicaciones Web, a menudo sistemas de gestión de contenidos (CMS) o plataformas de comercio electrónico.



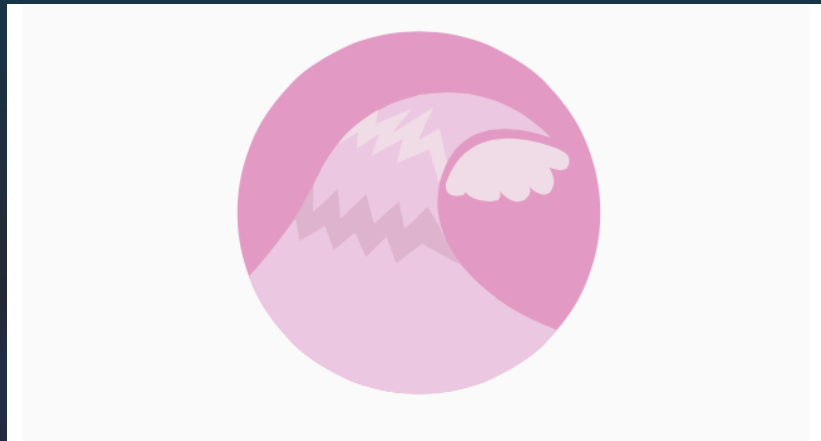
¿Qué se puede hacer?

- Utilice la autenticación de dos factores.
- Parche con prontitud.
- Control de todas las entradas en los formularios.



Denegacion de Servicio (DOS)

Los ataques DoS son un técnica maliciosa de interrupción de servicios. Utilizan por lo general redes de bots con el objetivo de inundar el canal de datos o hacer colapsar algún dispositivo en la ruta de los servicios en línea.



¿Qué se puede hacer?

- Aislar los activos.
- Tener un plan de mitigación.
- Analisis de Gaps.



Skimmers de Sistemas de Pago



CARTOONSTOCK
.com

Search ID: wda0349

"Él pregunta si alguien sabe como
Instalar un skimmer"

Skimmers de Sistemas de Pago

skimmers de tarjetas de pago utilizan un "skimmer" físico en un cajero automático, terminal punto de venta (POS) o bomba de gas/bencina para leer los datos de la banda magnética de la tarjeta cuando se paga.

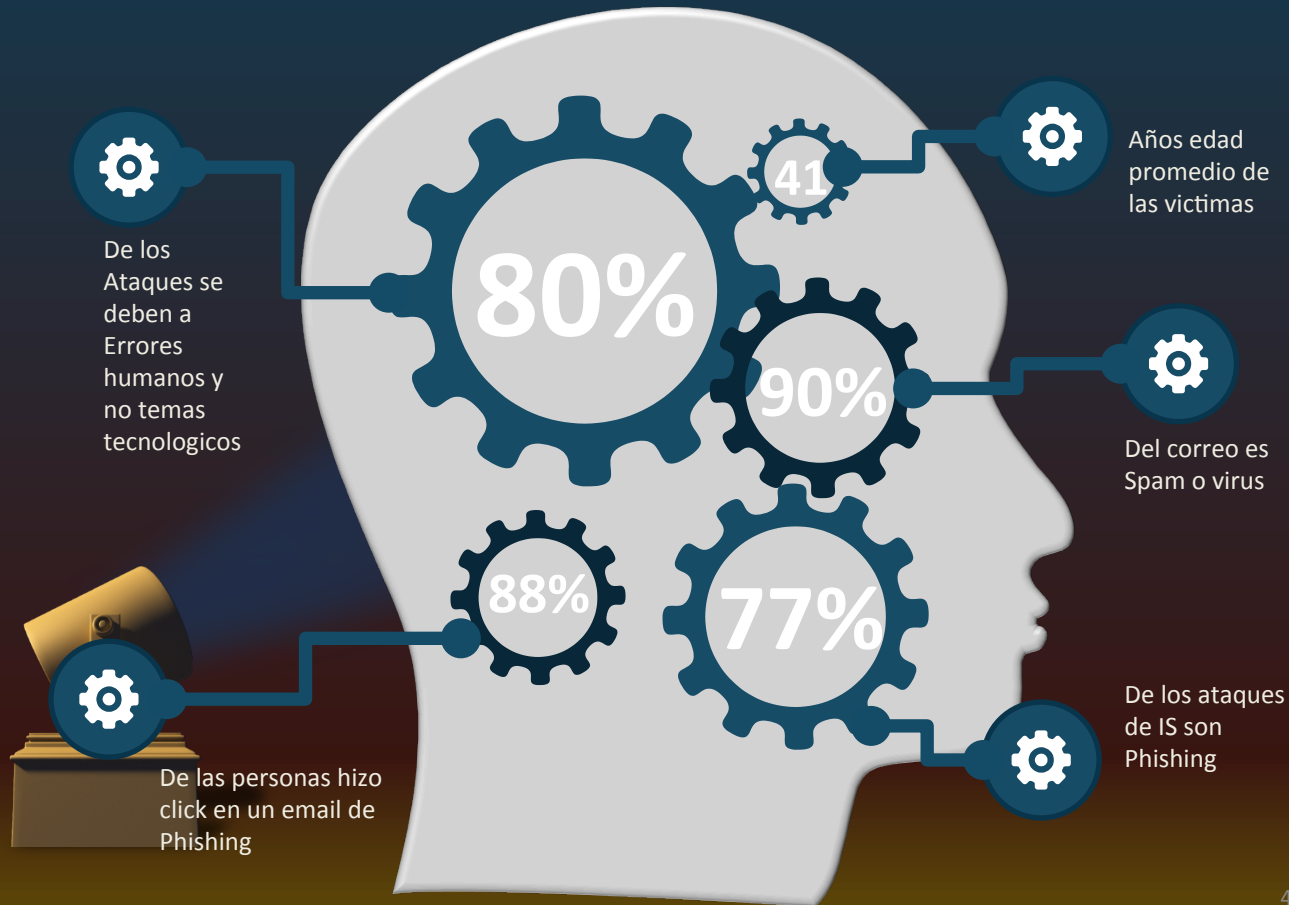


¿Qué se puede hacer?

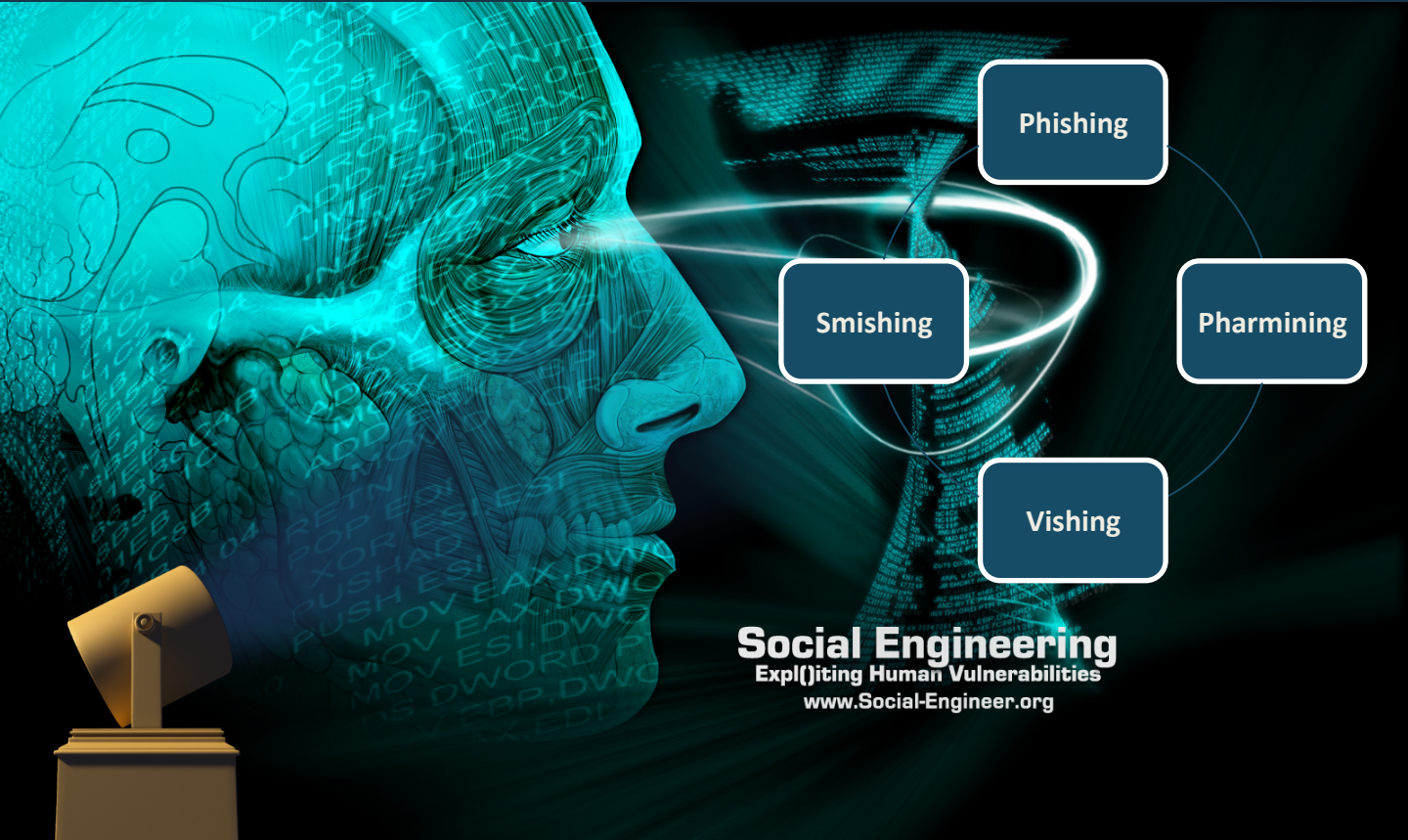
- Monitorear los terminales de pago.
- Considere reemplazar los cajeros automáticos.
- Use controles a prueba de manipulaciones (tamper).



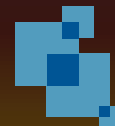
Factor Humano



Ingeniería Social



Cibercrimen **Modo Presencial**



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

ATM Skimmers

<http://www.cbsnews.com/videos/more-thieves-using-atm-skimmers-to-steal-credit-card-info/>



ATM



ATM



ATM





ATM



ATM

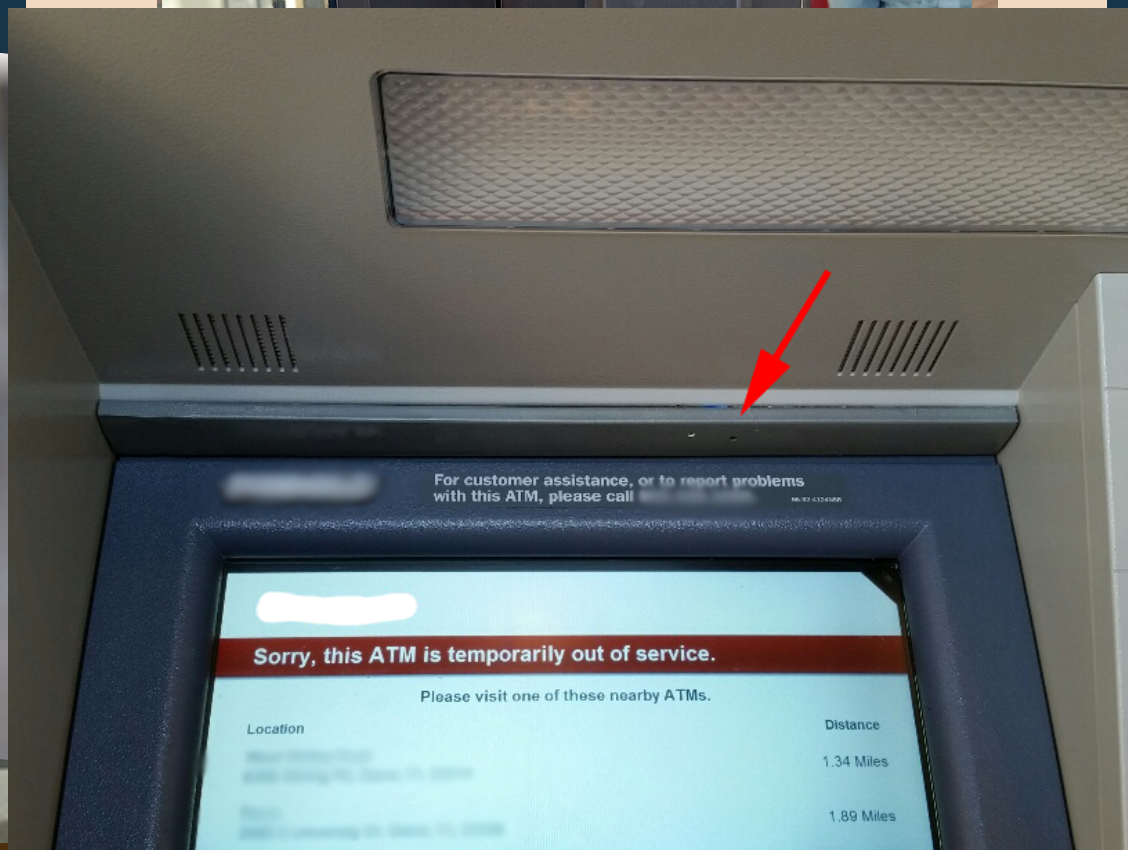


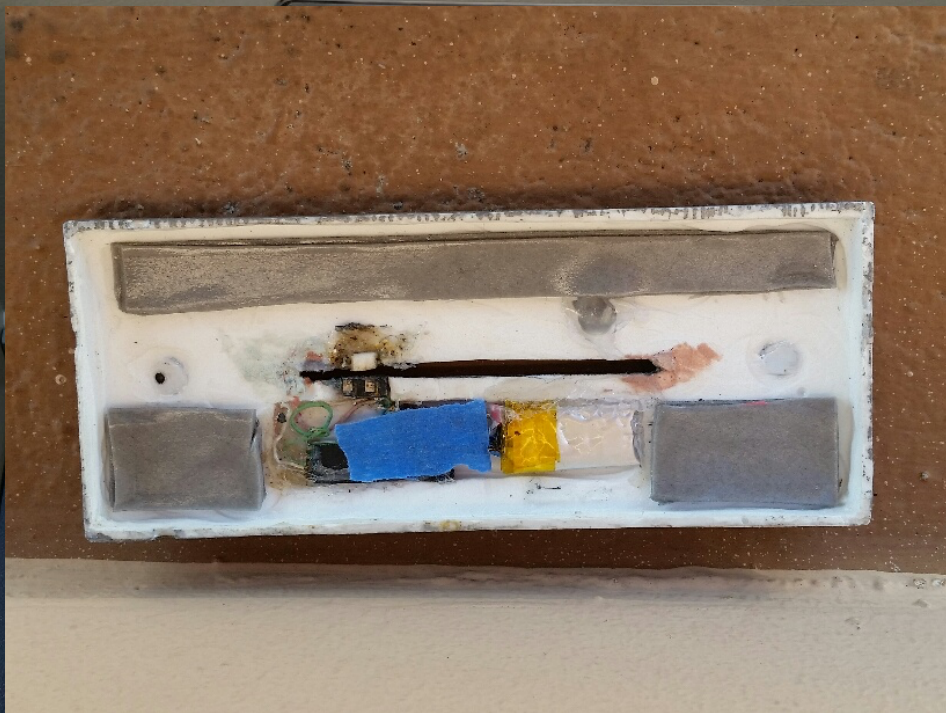
ATM











1.89 Miles









7 Razones de porque es tan Fácil

SOFTWARE INTEGRITY CONTROL

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32> [redacted] status
[redacted]: Disabled
[redacted] on reboot: Disabled

ePO Managed: No
Local CLI access: Recovered

  [fstype]      [status]      [driver status] [volume]
* NTFS        [redacted]      Unattached      C:\

C:\Windows\system32> [redacted]
Enumerating installed products.
[redacted] volume C:\
00:11:26: Total files scanned 99324, [redacted] 42
```



7 Razones de porque es tan Fácil

SOP

M
C
e
L
*
C
E
E

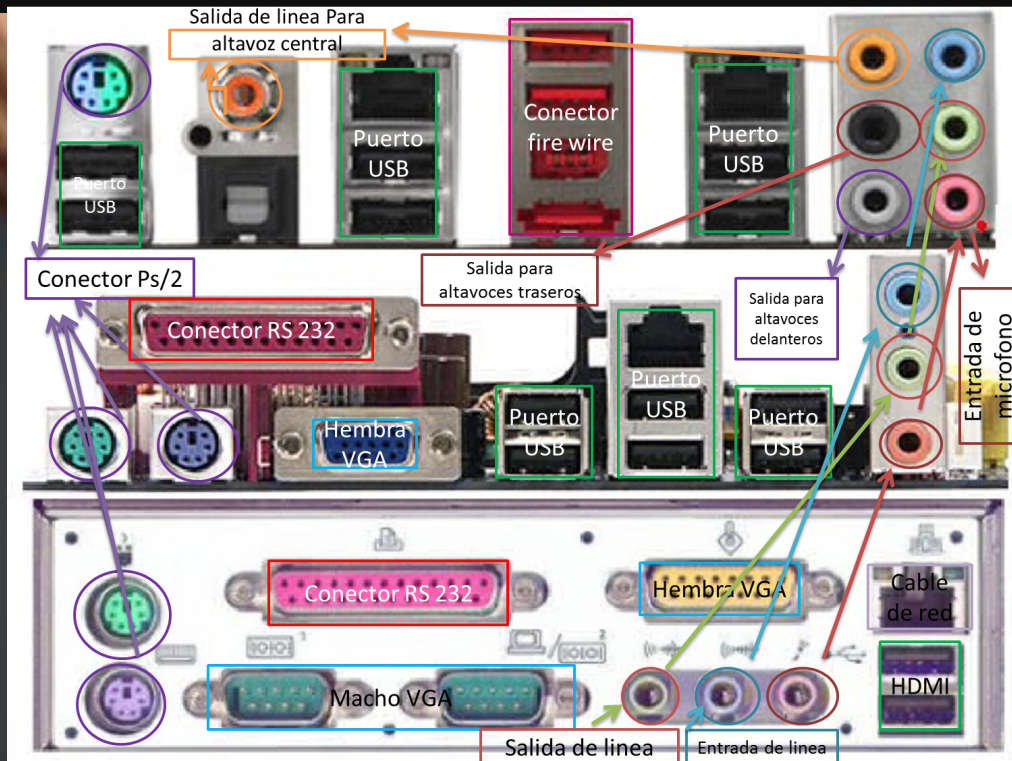


Seguridad

16

7 Razones de porque es tan Fácil

SOF

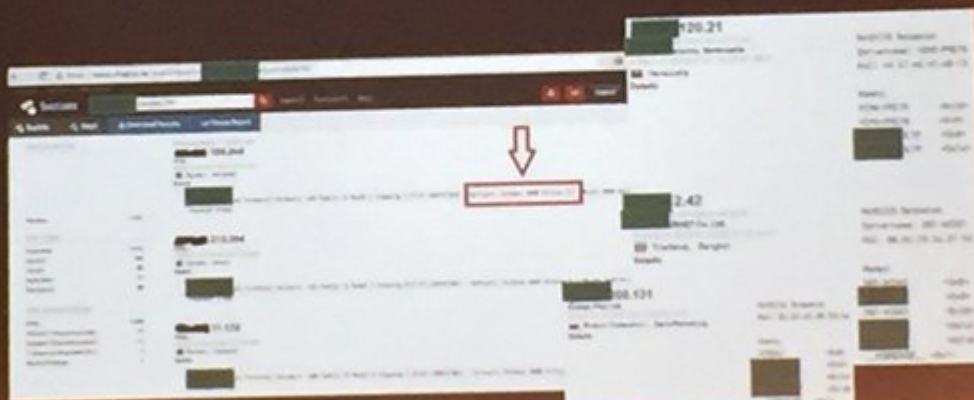


Secur

7 Razones de porque es tan Fácil

SO

LET ME IN: ATMS ON THE INTERNET



Sec

Point Of Sale (POS)

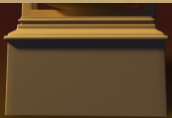
- ✓ 2 marcas principales en Latam: Verifone (USA) e Ingenico (Francia).
- ✓ Sistema Operativo propietario, Linux.
- ✓ Poseen tamper (secuencial y paralelo).
- ✓ Poseen Hardware Security Module (HSM) para llaves de encriptación.
- ✓ Soportan protocolos de encriptación (DES, 3DES, DUKPT).
- ✓ Control de acceso con clave, perfiles.
- ✓ Cumplen con normativa PCI PTS (1.0 - 4.0)



Point Of Sale (POS)



¿Son Seguros?



Modalidades del Fraude

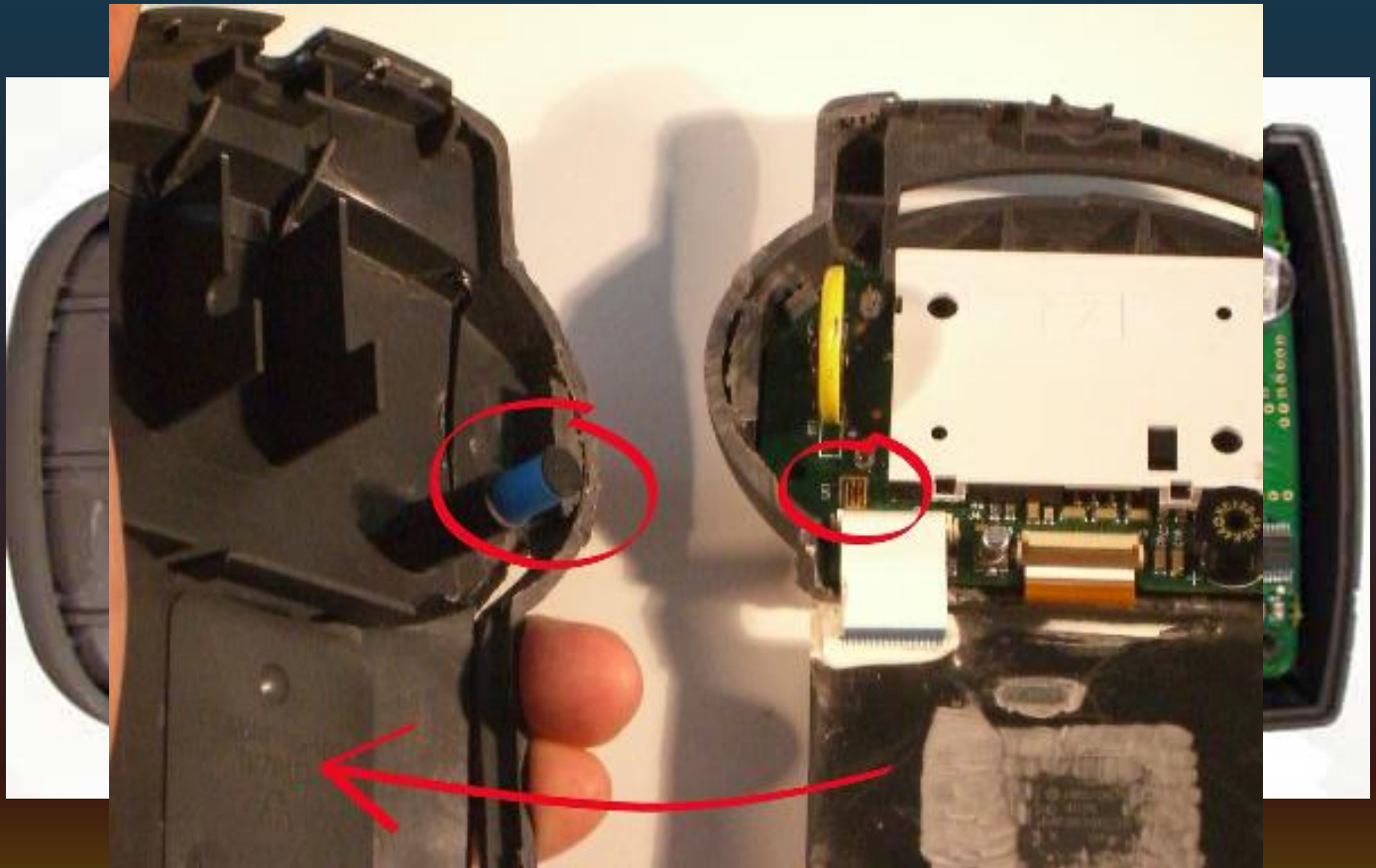
- Skimmer clásico, no depende de la tecnología (pasado de moda).
- Extracción y Copia de la data almacenada en POS (almacenamiento local y no encriptada).
- Evesdropping (Dial Up)
- POS Fantasma o de Palo (software factory, SO no firmado)
- Tampering:
- Circuito integrado (cabezal magnético y Pinpad) + Memoria
- Circuito integrado + Bluetooth (Activo, on demand)
- Circuito integrado + GPRS, GSM



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.





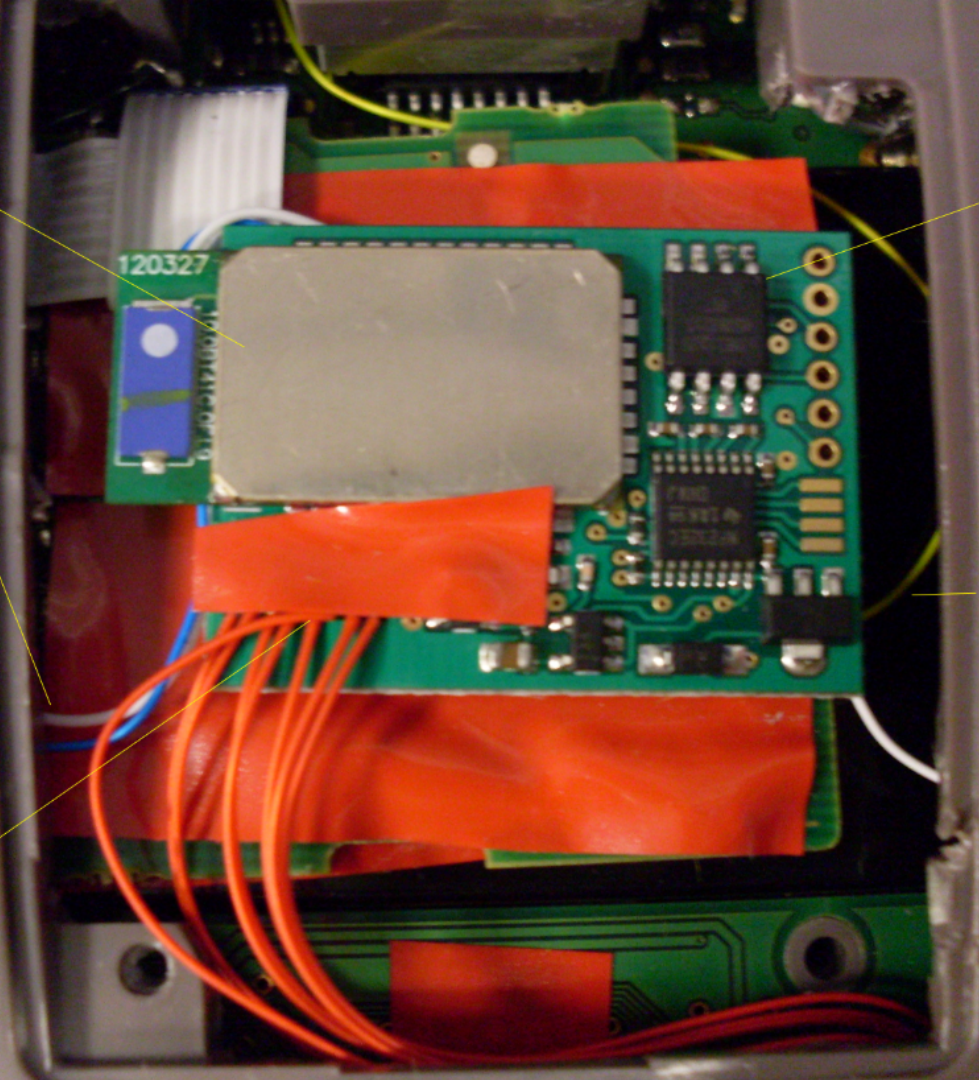
Bluetooth
Module

Memory
module

Blue/White
wires link
module to
card
reader.

Yellow
wires to
power

Orange
wires
connect to
PIN pad.



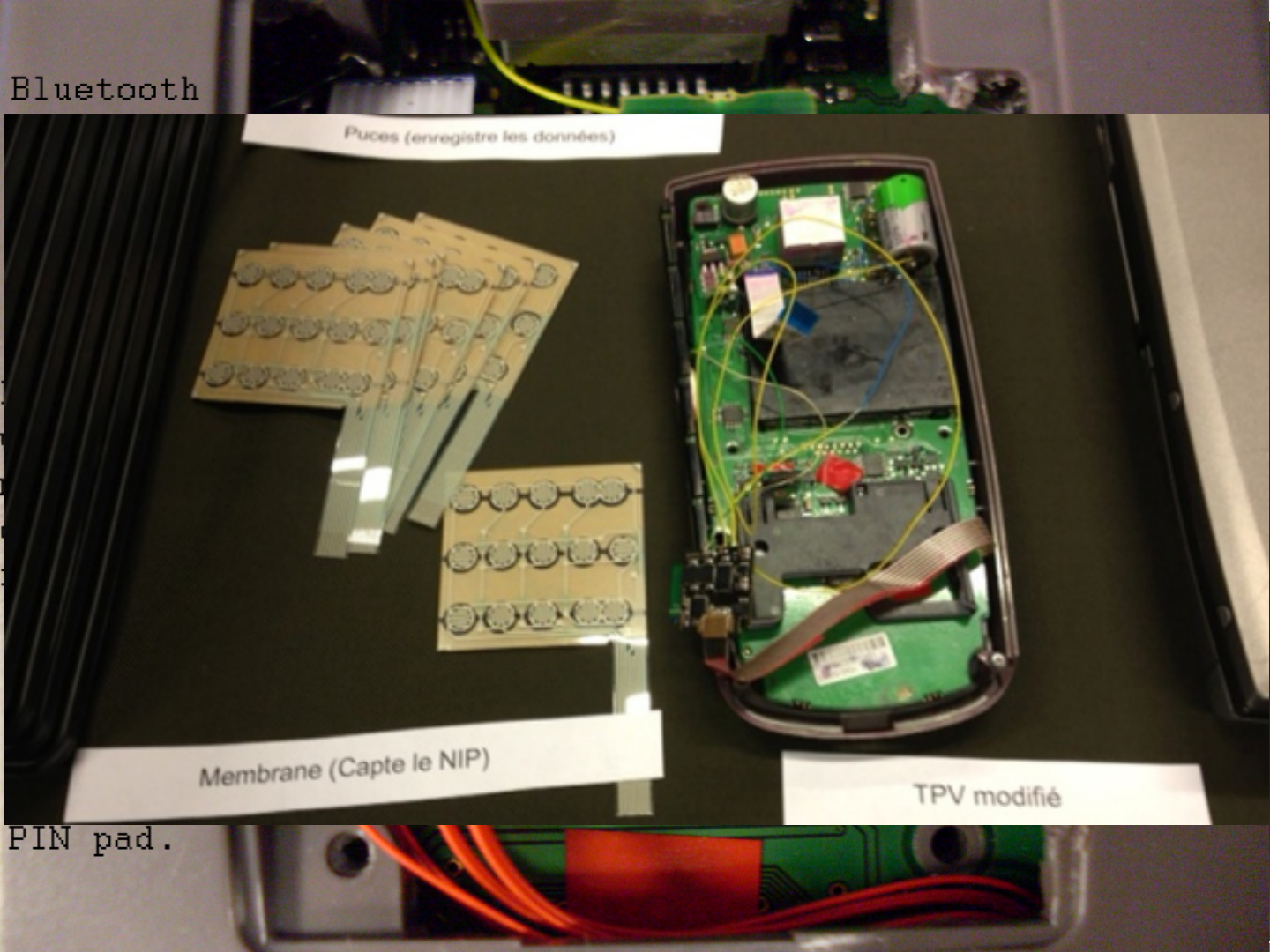
Bluetooth

Puces (enregistre les données)

Membrane (Capte le NIP)

TPV modifié

PIN pad.



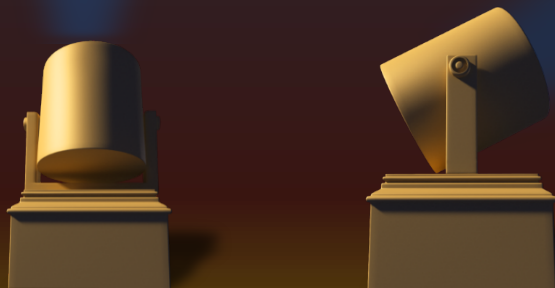
Principales Modelos Adulterados

- VX 510
- VX 670
- VX 680*
- Pinpad VX800
- Pinpad VX810
- Todos PCI PTS 1.0, en proceso de caducación, ya no se pueden comprar mas equipos despues de abril 2014.

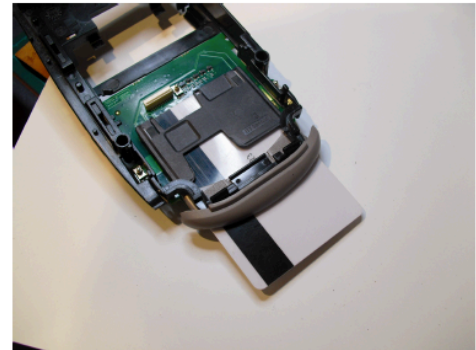
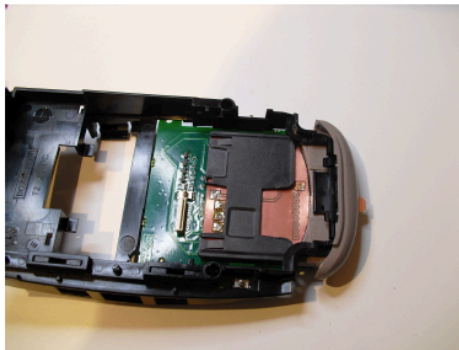
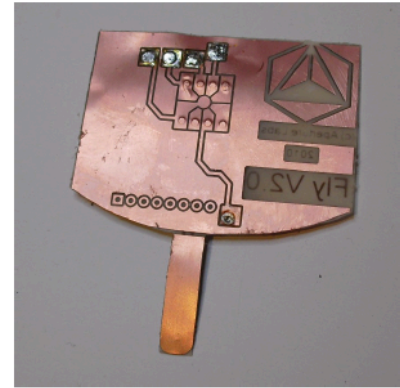
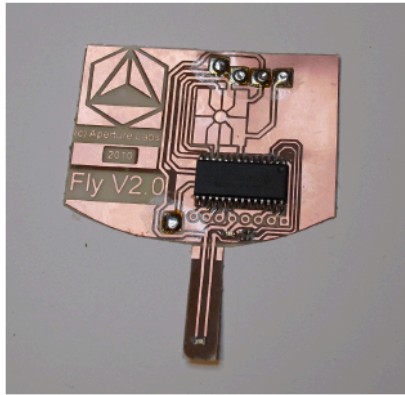
* PCI PTS 3.0



5100
Pinpad 3070



SCHIM



SCHIM





CONTRAMEDIDAS DE LA INDUSTRIA



DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

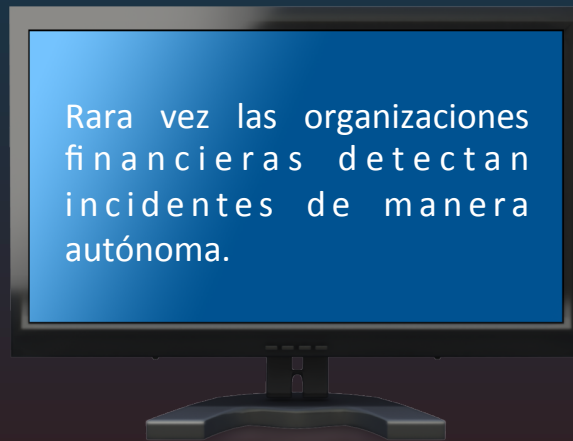


PCI DSS

I'd love to talk about PCI ...no really.

Desafío: Tiempo Id de Incidentes en este Ámbito

- ✓ 54% de los incidentes permaneció sin descubrir durante semanas.
- ✓ 15% permaneció sin descubrir durante meses o más.
- ✓ Sistemas del sector financiero se vieron comprometidos en minutos o menos en el 98% de los casos.
- ✓ Eso sugiere que los atacantes tienen un montón de tiempo para encontrar los datos potencialmente lucrativos que están buscando.



> Lentitud > Impacto

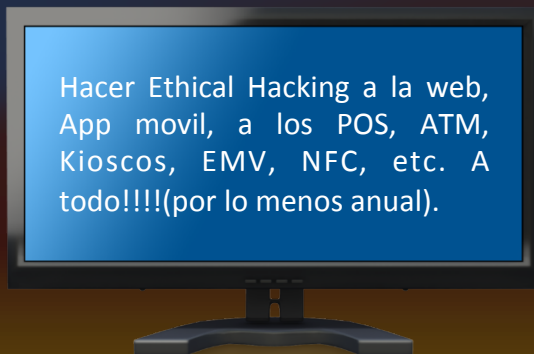


“El tiempo no es relativo...”



Recomendaciones

- Mantener un inventario, Auditar el inventario.
- Clasificar (CID) el inventario y gestionar el riesgo
- Modificar, afinar los sistemas de monitoreo y detección de fraude.
- Incluir al área de Riesgos o Seguridad de la Información en los procesos de compra de nuevas tecnologías y nuevos proyectos
- Cumplir con la normativa legal y exigencias de las marcas.
- Capacitar y sensibilizar a los colaboradores, proveedores sobre estos riesgos.
- “Compartir” la información, investigaciones e incidentes, actuar en bloque, como industria.

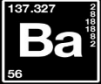


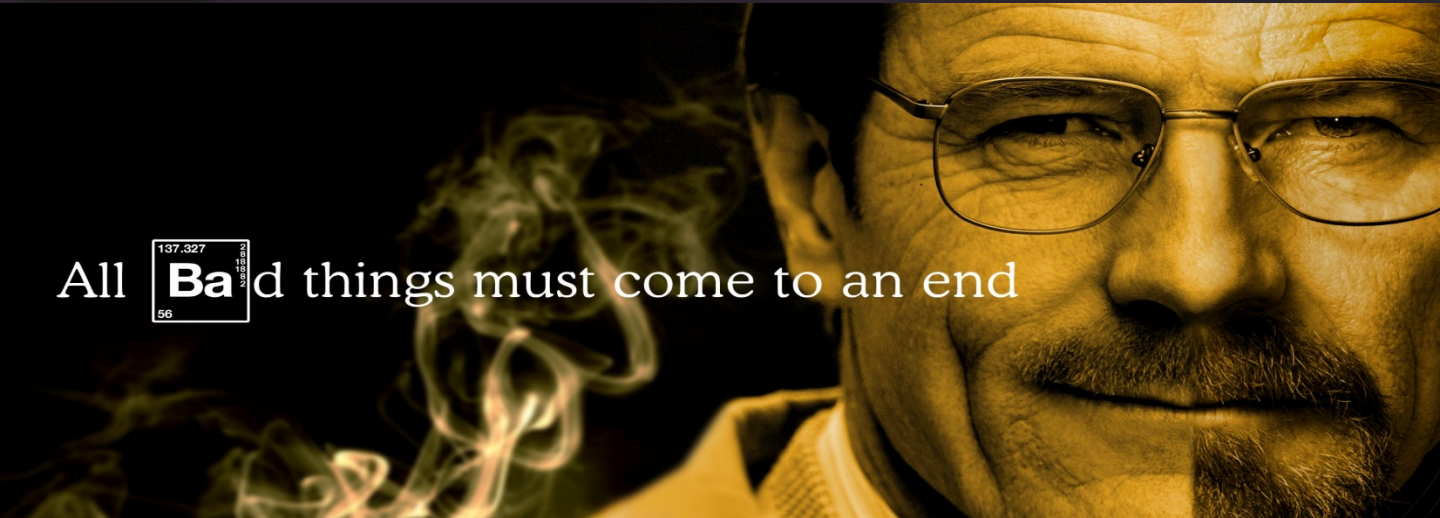
DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

Conclusión

- La tecnología avanza.... avanzan las modalidades de fraude.
- El fraude es parte del negocio financiero, se deben buscar las formas de disminuirlo, no se puede eliminar...
- Se debe aumentar la seguridad asociada a medios de pago, aunque implique mayor complejidad o tiempo
- Es necesario adelantarse a las amenazas, más inteligencia...

All  d things must come to an end



¿Preguntas?
¿Más Información?



Gabriel Bergel

gabriel.bergel@dreamlab.net

@gbergel

