SI EL CIBERCRIMEN FUERA UN PAÍS

ESTRATEGIA

- Gestión de los Riesgos
- Cultura Cibersegura
- 4 Pilares

PILARES DE LA CIBERSEGURIDAD

Nuestras Alianzas

NEXTVISION
Ciberseguridad Inteligente

Nos seguimos transformando

- **Para continuar brindando valor a nuestros clientes.**
- **Para combinar la experiencia de 28 años de trayectoria con una mirada innovadora y profesional.**
- **Consolidando un equipo sólido.**

NEXTVISION
Ciberseguridad Inteligente

Nuevos Servicios

NV CIBERDEFENSA | SOC

NV AWARENESS

NEXTVISION
Ciberseguridad Inteligente

Nuevas oficinas en el Distrito Tecnológico

- **Desde Julio de 2018**
- **Integramos el Board del Distrito Tecnológico**

NEXTVISION
Ciberseguridad Inteligente

Renovamos nuestra imagen

NEXTVISION

Ciberseguridad Inteligente

NEXTVISION

Ciberseguridad Inteligente

INTSIGHTS

Threat Intelligence Realized.

Luis Núñez luis.nunez@intsights.com +52 1 55 5452 3842

Fundadores

- Junio 2015
- Veteranos de las unidades de inteligencia y ciberseguridad militar israelí de elite.
- Alto conocimiento de comportamiento, colaboración y pensamiento de los hackers.

GUY NIZAN
CEO & Co-Founder

ALON ARVATZ
CPO & Co-Founder

GAL BEN DAVID
CTO & Co-Founder

Inversores

Series C

$40m (total)

Blackstone

Glilot Capital Partners
Seeds of Intelligence

wipro ventures

ClearSky

BLUMBERG CAPITAL

TOLA CAPITAL

Crecimiento

210% YoY ARR

140+ Clientes

PATENTED

2 Patentes

INTSIGHTS

Tutorial de Dark Web:
Uso de la Dark Web Como Estrategia para Seguridad Proactiva

Luis Núñez
luis.nunez@intsights.com
+52 1 55 5452 3842

Agenda:

- Definición: Qué es la Dark Web?
- Qué ocurre en la Dark Web?
- Cómo utilizar la Dark Web como estrategia de seguridad proactiva?

1

Qué es la Dark Web?

INTSIGHTS

CLEAR, DEEP & DARK WEB

Clear Web

4 % de contenido WWW

– Navegable

– Redes Sociales

Deep Web

95 % del contenido

– No es navegable por la mayoría de los motores de búsqueda

– Está protegido por contraseñas

– Web mail, home banking y video demanda, intranets corporativas y contenido por suscripción, etc.

Dark Web

1 % del contenido

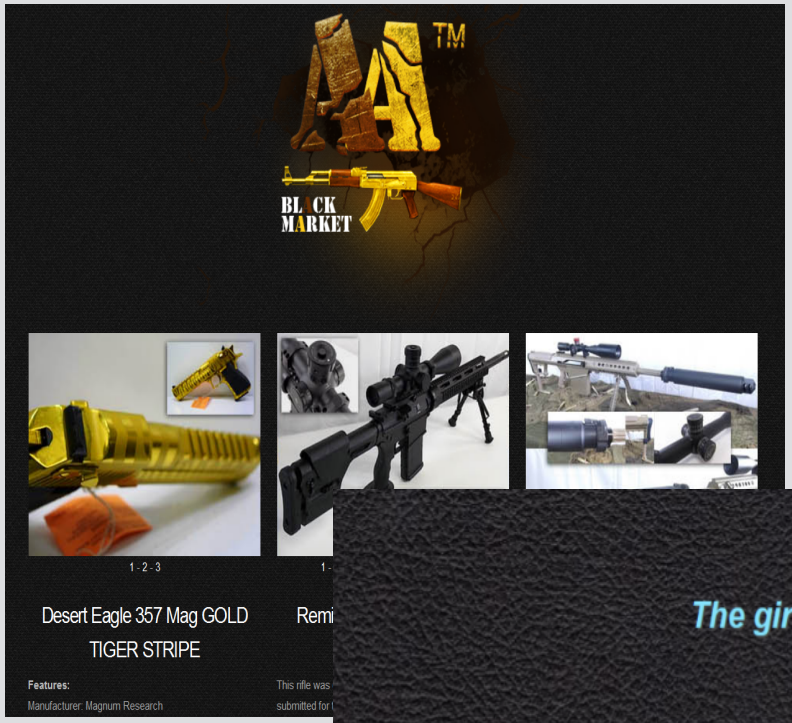
– No navegable con la mayoría de los motores de búsqueda

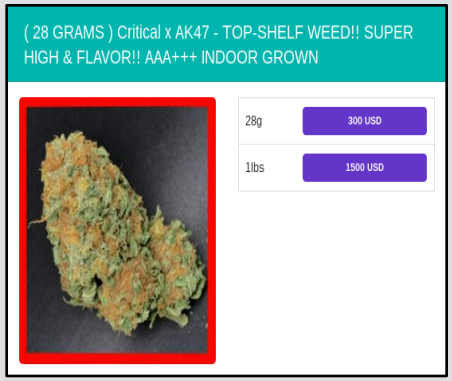
–TOR, IRCs, BitTorrent, foros de chakeo, C2s y más

– ***Aquí se planean ataques, se venden herramientas, se intercambia información y se vende y actualiza malware.***

INTSIGHTS

Qué se sabe acerca de la Dark Web?

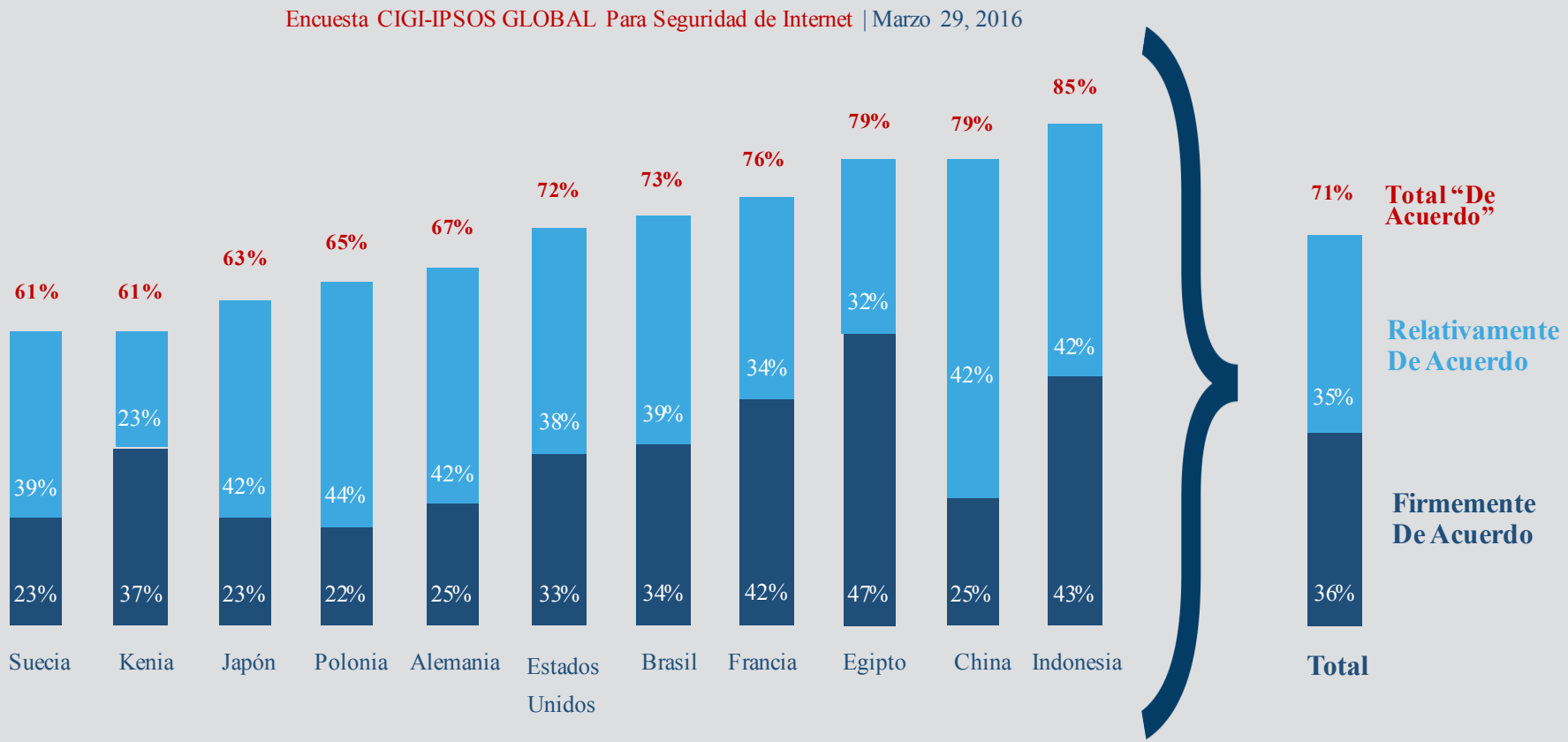




INTSIGHTS

Reputación de la Dark Web

Encuesta: Siete de cada diez personas (71%) opinan que no debe de ser abolido



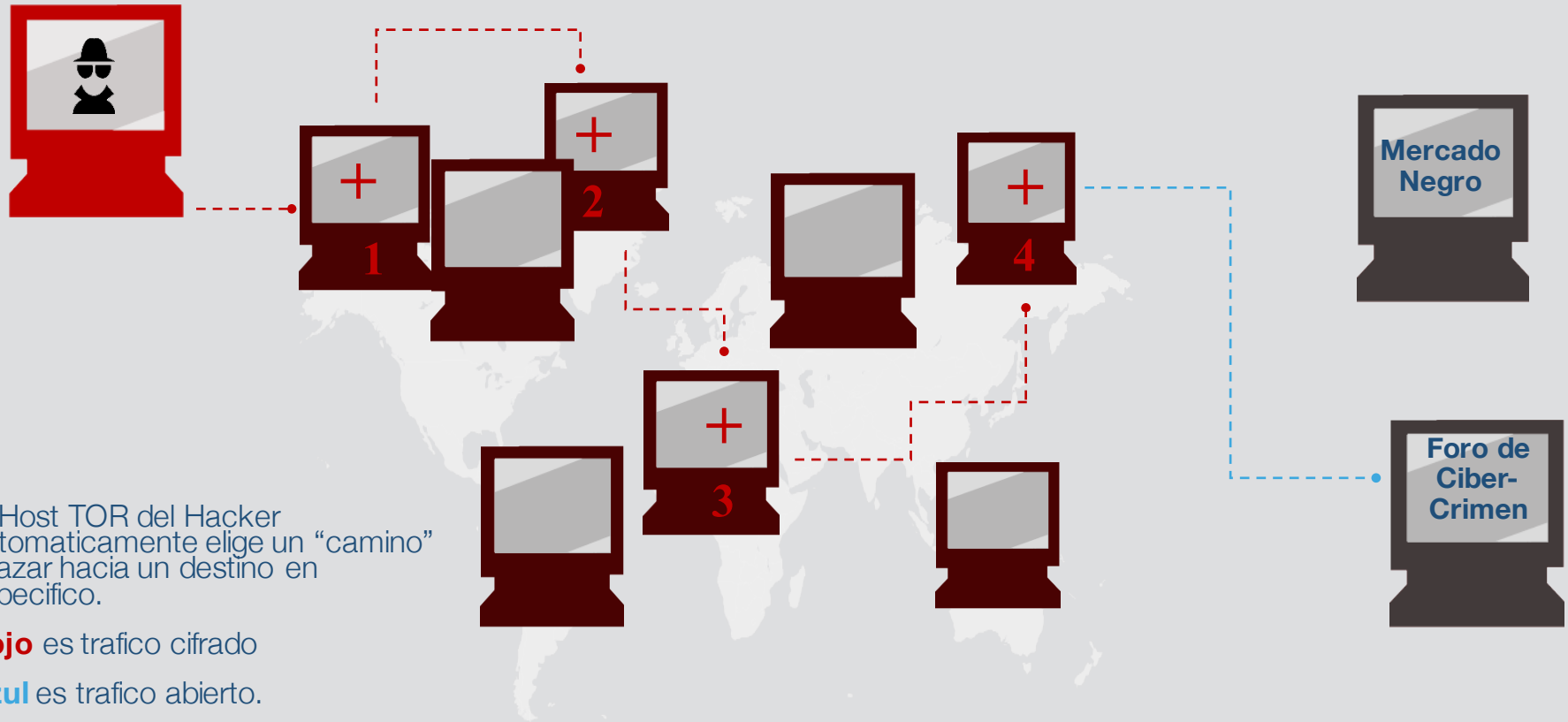
INTSIGHTS

La Ventaja Principal de los Hackers

La Anonimidad

INTSIGHTS

Cómo Funciona TOR



El Host TOR del Hacker automaticamente elige un “camino” al azar hacia un destino en especifico.

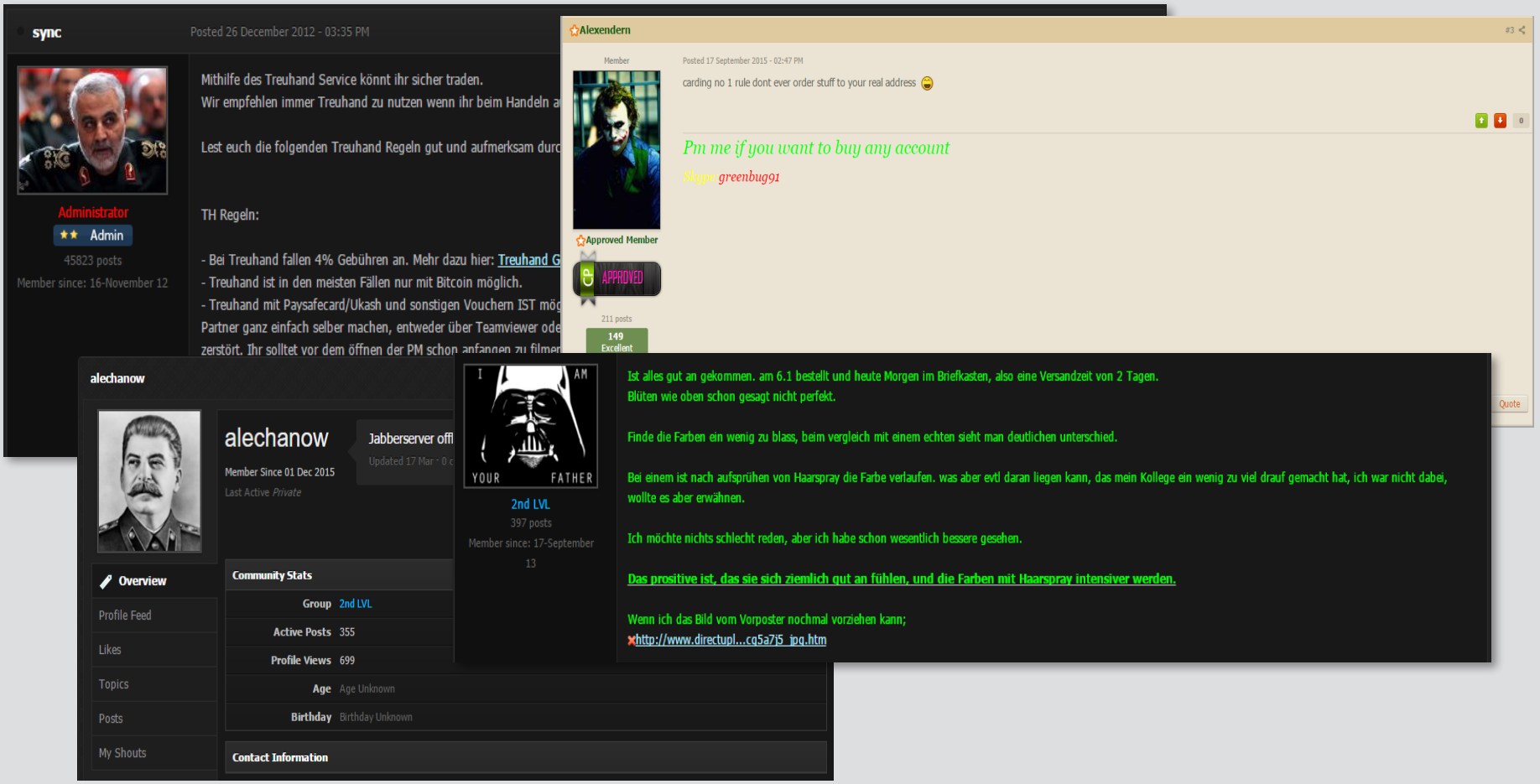
Rojo es trafico cifrado

Azul es trafico abierto.

Monitoreo Entrada/Salida de un “Exit Node” del TOR

INTSIGHTS

Puedes Ser Quien Quieras…



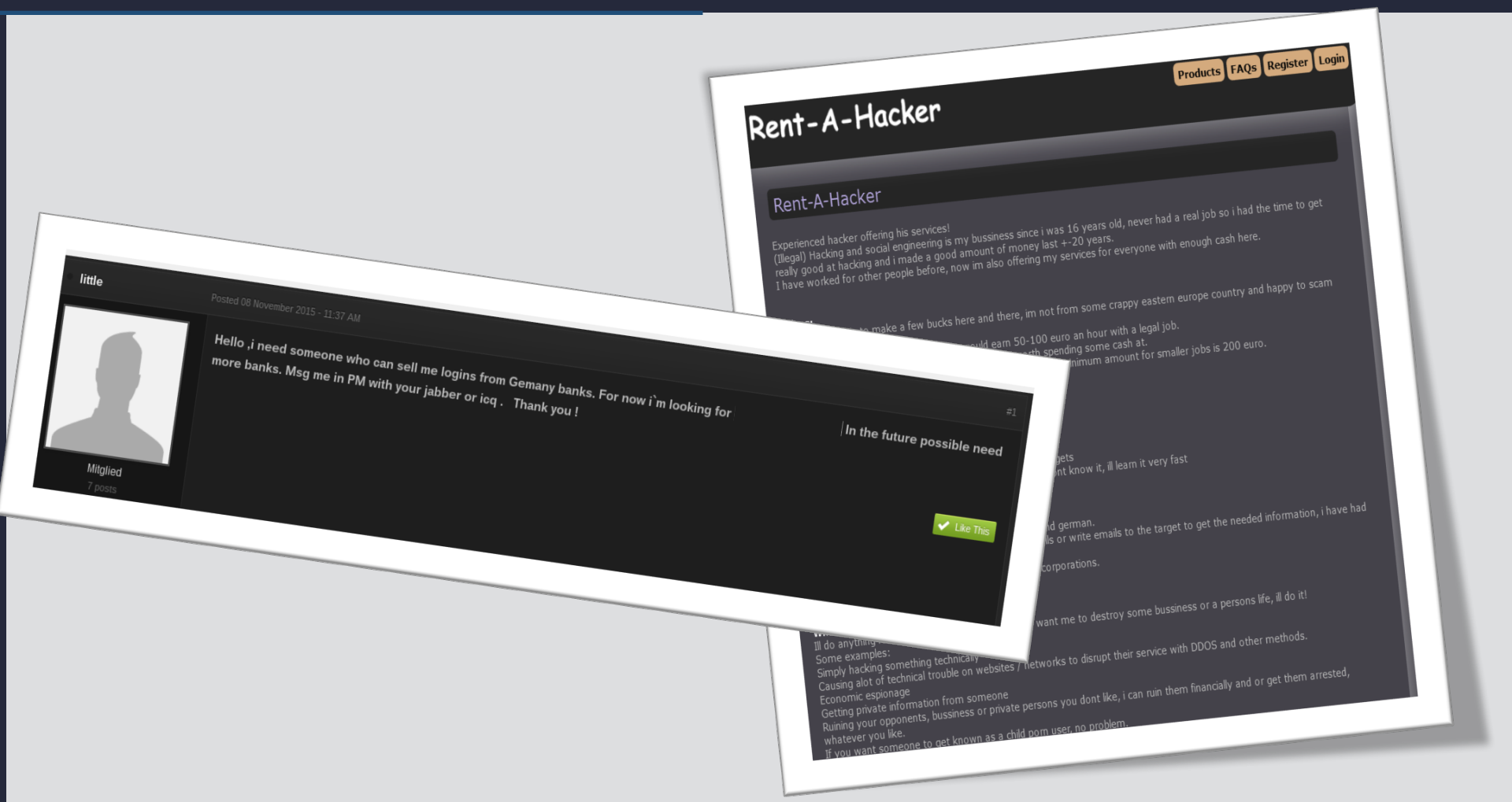
INTSIGHTS

2

Qué tipo de actividad ocurre en la Dark Web?

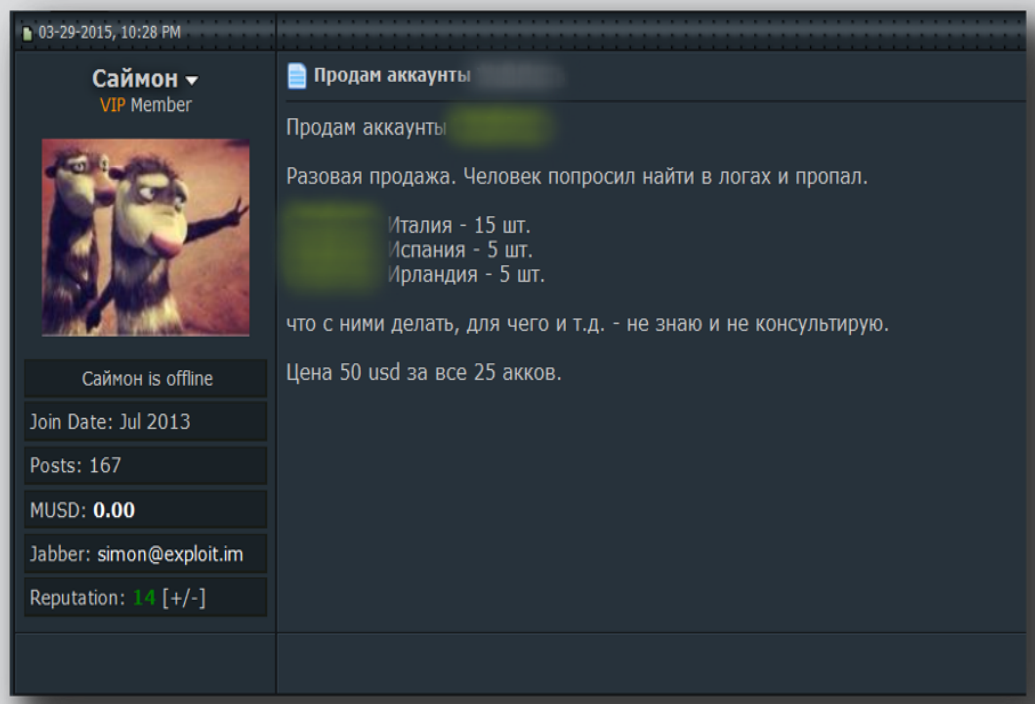
INTSIGHTS

Central de Actividad Criminal



INTSIGHTS

Qué se Vende en la Dark Web?



XXXX Cuentas de Venta

Una sola venta. El hombre pidió encontrar en el registro y desapareció.

XXX Italy - 15 piezas

XXX Spain - 5 piezas

XXX Ireland – 5 piezas.

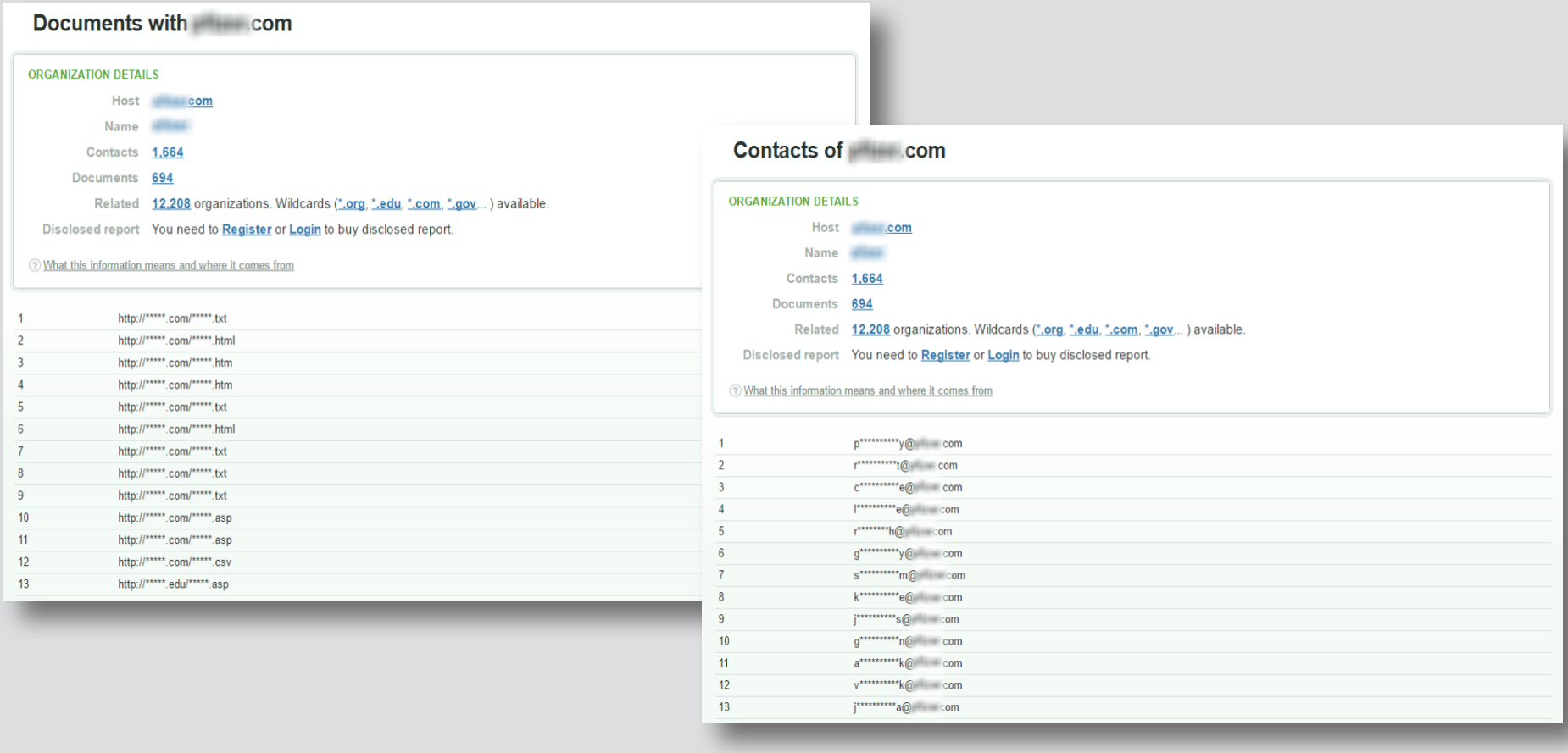
Qué hacer con ellos, para qué, etc.

No lo sé y no brindo asesoramiento al respecto.

Precio 50 USD por los 25 registros

INTSIGHTS

Qué se Vende en la Dark Web?



Documents with [redacted].com

ORGANIZATION DETAILS

Host	[redacted].com
Name	[redacted]
Contacts	1,664
Documents	694
Related	12,208 organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.
Disclosed report	You need to Register or Login to buy disclosed report.

What this information means and where it comes from

1	http://*****.com/*****.txt
2	http://*****.com/*****.html
3	http://*****.com/*****.htm
4	http://*****.com/*****.htm
5	http://*****.com/*****.txt
6	http://*****.com/*****.html
7	http://*****.com/*****.txt
8	http://*****.com/*****.txt
9	http://*****.com/*****.txt
10	http://*****.com/*****.asp
11	http://*****.com/*****.asp
12	http://*****.com/*****.csv
13	http://*****.edu/*****.asp

Contacts of [redacted].com

ORGANIZATION DETAILS

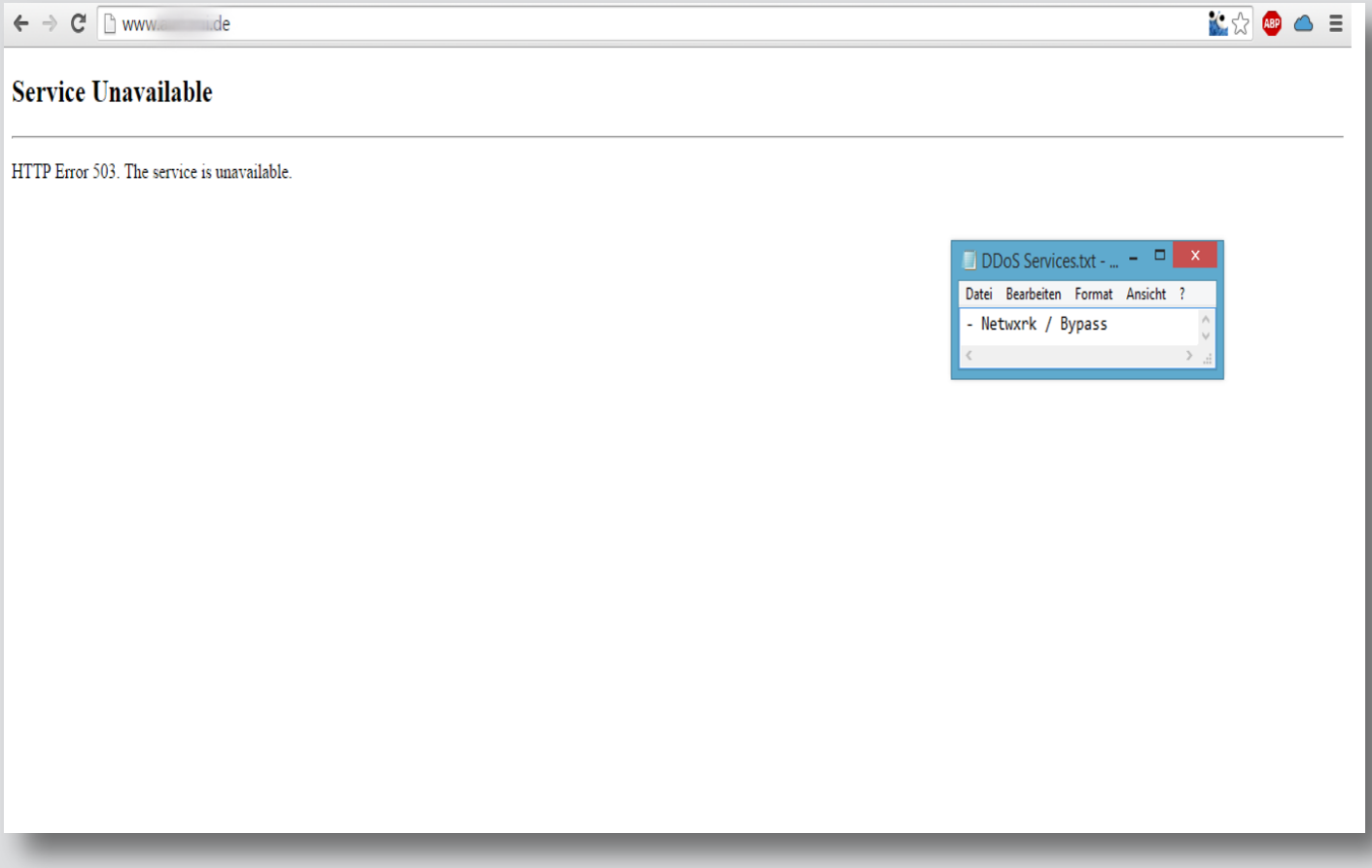
Host	[redacted].com
Name	[redacted]
Contacts	1,664
Documents	694
Related	12,208 organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.
Disclosed report	You need to Register or Login to buy disclosed report.

What this information means and where it comes from

1	p*********y@[redacted].com
2	r*********t@[redacted].com
3	c*********e@[redacted].com
4	l*********e@[redacted].com
5	r********h@[redacted].com
6	g*********y@[redacted].com
7	s*********m@[redacted].com
8	k*********e@[redacted].com
9	j*********s@[redacted].com
10	g*********n@[redacted].com
11	a*********k@[redacted].com
12	v*********k@[redacted].com
13	j*********a@[redacted].com

INTSIGHTS

Qué se Vende en la Dark Web?



INTSIGHTS

Mercados en la Dark Web

Is there trust among crooks?

(14:16:05) hack3rl33t@jabb3r.org: ¿tienes otras fuentes o foros interesantes para recomendar?

(14:17:10) lorenzo@crypt.am: sí

(14:17:18) lorenzo@crypt.am: kick ass es interesante también

(14:17:24) hack3rl33t@jabb3r.org : Yo también estoy allí

(14:18:17) hack3rl33t@jabb3r.org : Te recomiendo 8chan

(14:18:31) lorenzo@crypt.am: Tienes el enclace por favor?

(14:19:16) hack3rl33t@jabb3r.org : 8ch.net/baphomet/res/104638.html

(14:19:46) hack3rl33t@jabb3r.org : Dame una buena fuente, amigo! Quiero algo nuevo jajaja

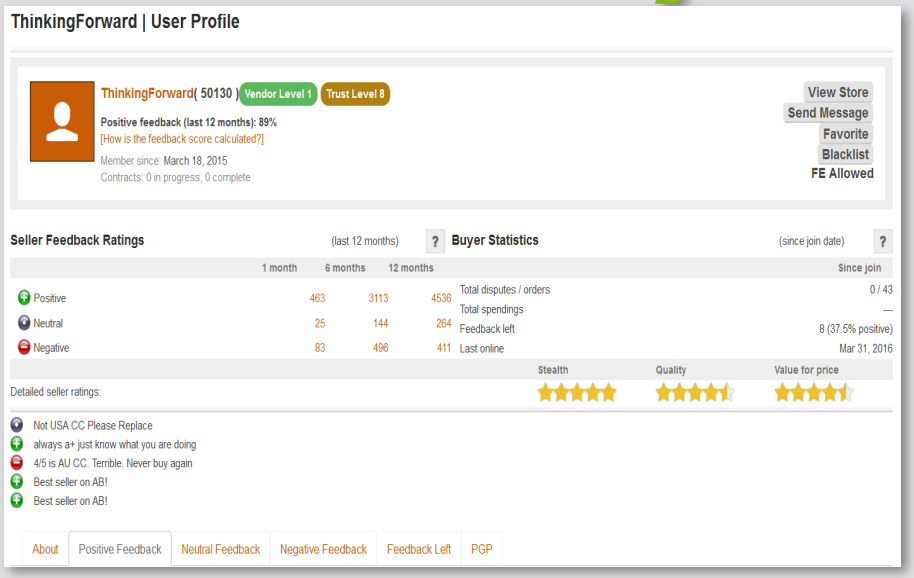
(14:21:05) lorenzo@crypt.am: yo también estoy en varios foros franceses

(14:21:34) lorenzo@crypt.am: Hablas francés?

(14:24:10) hack3rl33t@jabb3r.org : Pasame algunos de esos foros

(14:24:51) lorenzo@crypt.am: http://fdpogivefk34xkbd.onion/

(14:24:56) lorenzo@crypt.am: este es el más interesante

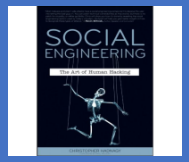
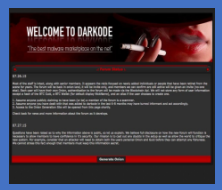


3

¿Cómo Aprovechar la Dark Web para Seguridad Proactiva?

INTSIGHTS

“Ladrón que roba a ladrón”

Motive	Targeting	Development	Infrastructure	Recon	Attack
					
					
					

INTSIGHTS

Visibilidad de Riesgos y Ataques

- Credenciales o cuentas comprometidas a la venta
- Amenazas dentro de la misma organización
- Guías de como crear aplicaciones móviles maliciosas
- Métodos de Hacking a los servicios de negocio
- Vulnerabilidades
- Y la lista sigue…

Credenciales Fugadas

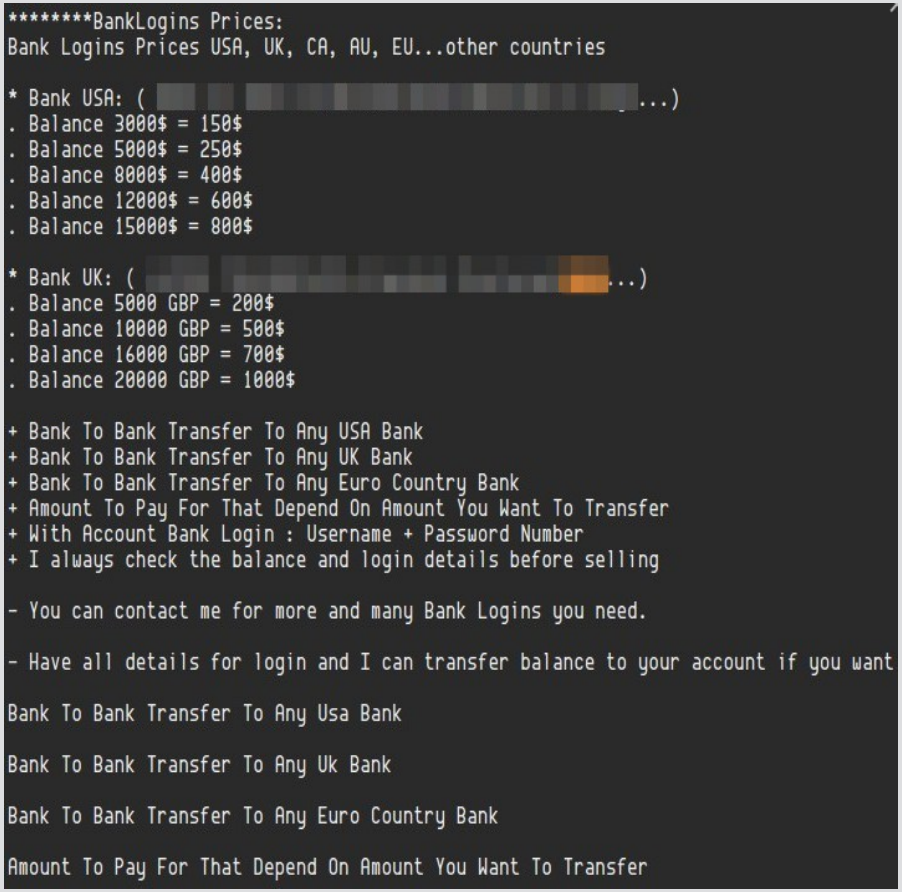
```
combo 176k.txt:john.monsour@[redacted]:13151315
combo 176k.txt:j.reinholdt@[redacted]:polaris
combo 176k.txt:wesman2@[redacted]:hunter
combo 176k.txt:kevin_nguyen@[redacted]:keothai
combo 176k.txt:r.adams@[redacted]:booba8880
combo 176k.txt:GPATES@[redacted]:blackie
combo 176k.txt:darekclark@[redacted]:redmanhomes
combo 176k.txt:dxtremeone@[redacted]:renier
combo 176k.txt:jroot1@[redacted]:721081
combo 176k.txt:ddpound@[redacted]:packers
combo 176k.txt:gooftrooper@[redacted]:killer
combo 176k.txt:zootii@[redacted]:em424242
combo 176k.txt:michaelcville@[redacted]:crazzydaze63
combo 176k.txt:razrok@[redacted]:rizzorat
combo 176k.txt:Smith.Justin218@[redacted]:justinsmith
combo 176k.txt:wziewitz@[redacted]:walker99
combo 176k.txt:coolspoof@[redacted]:reading11
combo 176k.txt:rdales@[redacted]:raichu
combo 176k.txt:88flash88@[redacted]:bbplayer
combo 176k.txt:randi.hess@[redacted]:runningback
combo 176k.txt:jackel_fox@[redacted]:flflf1
combo 176k.txt:jackel_fox@[redacted]:flflf1
combo 176k.txt:longr@[redacted]:hitsquad
combo 176k.txt:rds262@[redacted]:bobo
combo 176k.txt:ivanhogan@[redacted]:redgreen
```

INTSIGHTS

Cuentas de Banco a la Venta

Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Mail access	Seller	Price ($):	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	
[illegible]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5	

Cuentas de Banco a la Venta



```
********BankLogins Prices:
Bank Logins Prices USA, UK, CA, AU, EU...other countries

* Bank USA: (                                                ...)
. Balance 3000$ = 150$
. Balance 5000$ = 250$
. Balance 8000$ = 400$
. Balance 12000$ = 600$
. Balance 15000$ = 800$

* Bank UK: (                                                ...)
. Balance 5000 GBP = 200$
. Balance 10000 GBP = 500$
. Balance 16000 GBP = 700$
. Balance 20000 GBP = 1000$

+ Bank To Bank Transfer To Any USA Bank
+ Bank To Bank Transfer To Any UK Bank
+ Bank To Bank Transfer To Any Euro Country Bank
+ Amount To Pay For That Depend On Amount You Want To Transfer
+ With Account Bank Login : Username + Password Number
+ I always check the balance and login details before selling

- You can contact me for more and many Bank Logins you need.

- Have all details for login and I can transfer balance to your account if you want

Bank To Bank Transfer To Any Usa Bank

Bank To Bank Transfer To Any Uk Bank

Bank To Bank Transfer To Any Euro Country Bank

Amount To Pay For That Depend On Amount You Want To Transfer
```

INTSIGHTS

Caso: Equifax

~~~~~~~~~~~~ Sell Cvv,Cc All Countries and All Kinds ~~~~~~~~~~~~

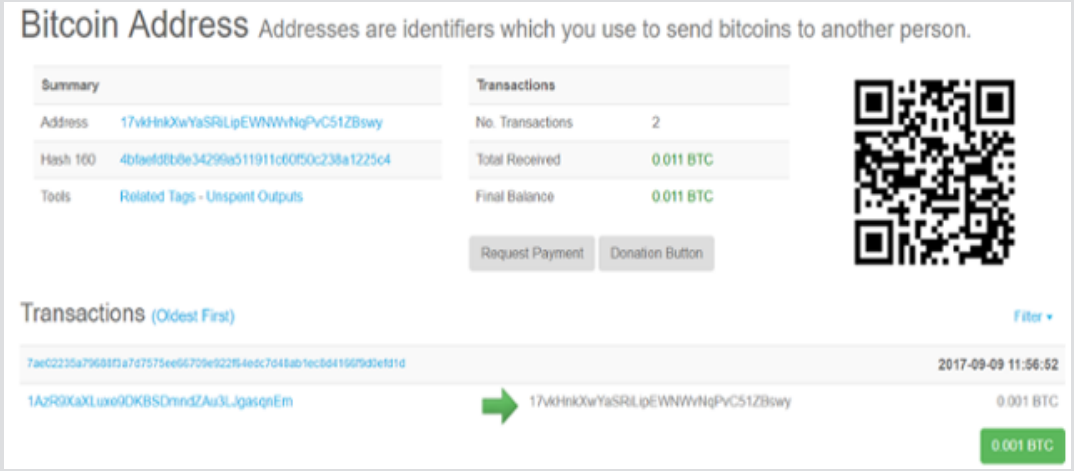
.We always checker Cvv valid 100% before send to customers

Credit Card Usa :
- Cvv Usa normal : $10 per 1
- Cvv Usa Bin : $13 per 1
- Cvv Usa fullz info : $20 per 1

Credit Card Uk :
- Cvv Uk normal : $20 per 1
- Cvv Uk dob : $23 per 1
- Cvv Uk fullz info : $30 per 1

Credit Card Ca :
- Cvv Ca normal : $25 per 1
- Cvv Ca dob : $27 per 1
- Cvv Ca fullz info : $40 per 1

PastHole Hacking Team website:



- De 143 millones de datos fugados, 209.000 contenía información de tarjetas de crédito
- Valor por información personal: $0.2 USD
- Valor tarjetas de credito: $20 USD

Valor total de perdida: (142,791,000 x 0.2) + (209,000 x 20) = 32,738,200 USD

INTSIGHTS
~~~~~~~~~~~~

¡Gracias!

¿Preguntas?

INTSIGHTS

NEXTVISION

Ciberseguridad Inteligente

Avenida Sáenz 17
Piso 4 (C1437DNA)
Distrito Tecnológico
Buenos Aires, Argentina
Tel: +54 (11) 5263 8326

nextvision.com