



SI EL CIBERCRIMEN FUERA UN PAÍS

ESTRATEGIA

Gestión de los Riesgos

Cultura Cibersegura

4 Pilares

PILARES DE LA CIBERSEGURIDAD

PREDICCIÓN

PREVENCIÓN

DETECCIÓN

RESPUESTA

Nuestras Alianzas



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.**



Nuevos Servicios

NV CIBERDEFENSA | SOC

NV AWARENESS



Nuevas oficinas en el Distrito Tecnológico

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



Renovamos nuestra imagen



NEXTVISION

Ciberseguridad Inteligente



NEXTVISION

Ciberseguridad Inteligente



Threat Intelligence Realized.



Luis Núñez



luis.nunez@intsights.com



+52 1 55 5452 3842

Fundadores

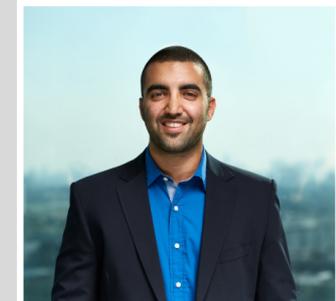
- Junio 2015
- Veteranos de las unidades de inteligencia y ciberseguridad militar israelí de elite.
- Alto conocimiento de comportamiento, colaboración y pensamiento de los hackers.



GUY NIZAN
CEO & Co-Founder



ALON ARVATZ
CPO & Co-Founder



GAL BEN DAVID
CTO & Co-Founder

Inversores

Series C

\$40m (total)

Blackstone



wipro ventures



Crecimiento



210% YoY ARR



140+ Clientes



2 Patentes





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?

CLEAR, DEEP & DARK WEB

Clear Web

4 % de contenido WWW

- Navegable
- Redes Sociales



Dark Web

1 % del contenido

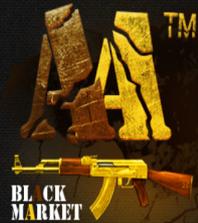
- No navegable con la mayoría de los motores de búsqueda
- TOR, IRCs, BitTorrent, foros de chakeo, C2s y más
- *Aquí se planean ataques, se venden herramientas, se intercambia información y se vende y actualiza malware.*

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.

Qué se sabe acerca de la Dark Web?



Desert Eagle 357 Mag GOLD
TIGER STRIPE

Features:
Manufacturer: Magnum Research



Remi

This rifle was
submitted for



(28 GRAMS) Critical x AK47 - TOP-SHELF WEED!! SUPER HIGH & FLAVOR!! AAA+++ INDOOR GROWN



28g
1lbs

Decommissioned Soviet submarine



Buy now

FULL ESCROW !!!

The girl is brought to the place you choose

To have a slave girl contact slavegirls@secmail.pro

Hire for 15 days: 1490€/1590\$

Hire for 30 days: 2790€/2980\$

The slave girl will fulfill ALL your wishes 24/7 for the specified period of time

Sharon, age: 16, from Hungary

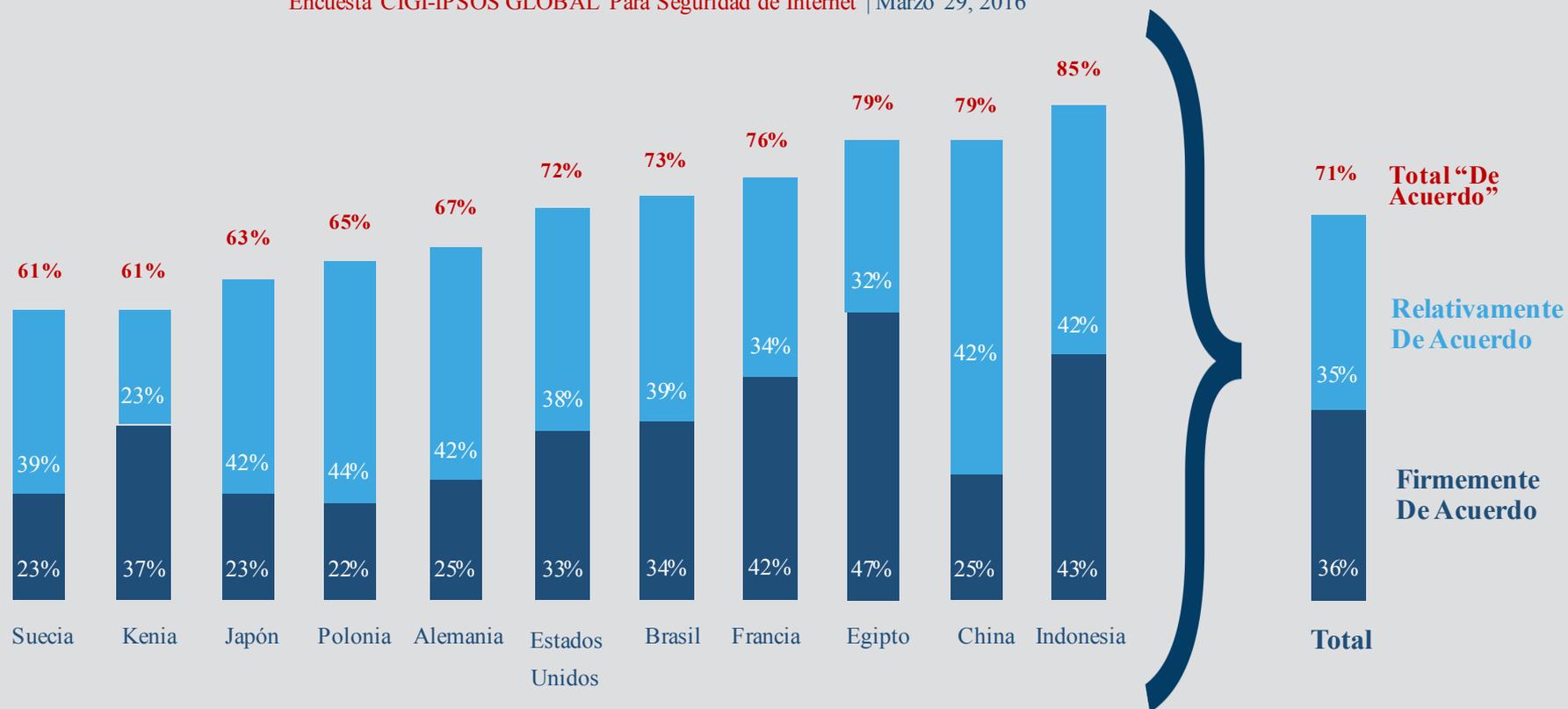
Currently Available



Reputación de la Dark Web

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

Encuesta CIGI-IPSOS GLOBAL Para Seguridad de Internet | Marzo 29, 2016

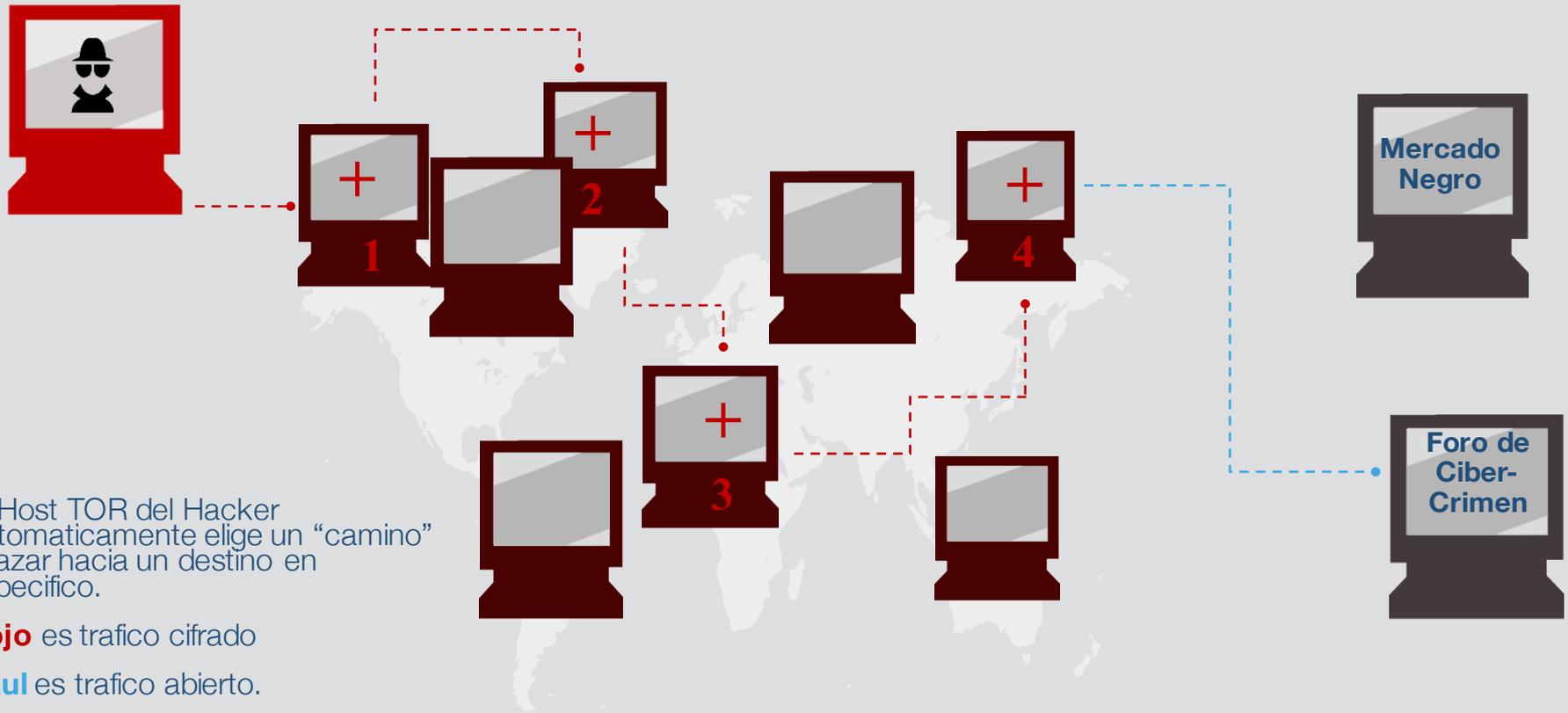


La Ventaja Principal de los Hackers

La Anonimidad



Cómo Funciona TOR



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

Puedes Ser Quien Quieras...

The image shows a collage of forum-related content. At the top left is a profile for 'sync', an Administrator with 45823 posts, dated 26 December 2012. The main content is a forum post by 'Alexendem' from 17 September 2015, featuring a picture of Joker and a green text overlay: 'Pm me if you want to buy any account' and 'Skype:greenbug01'. Below this is a profile for 'alechanow', a 2nd LVL member since Dec 2015, with a picture of Stalin. To the right of the 'alechanow' profile is a 'Community Stats' table:

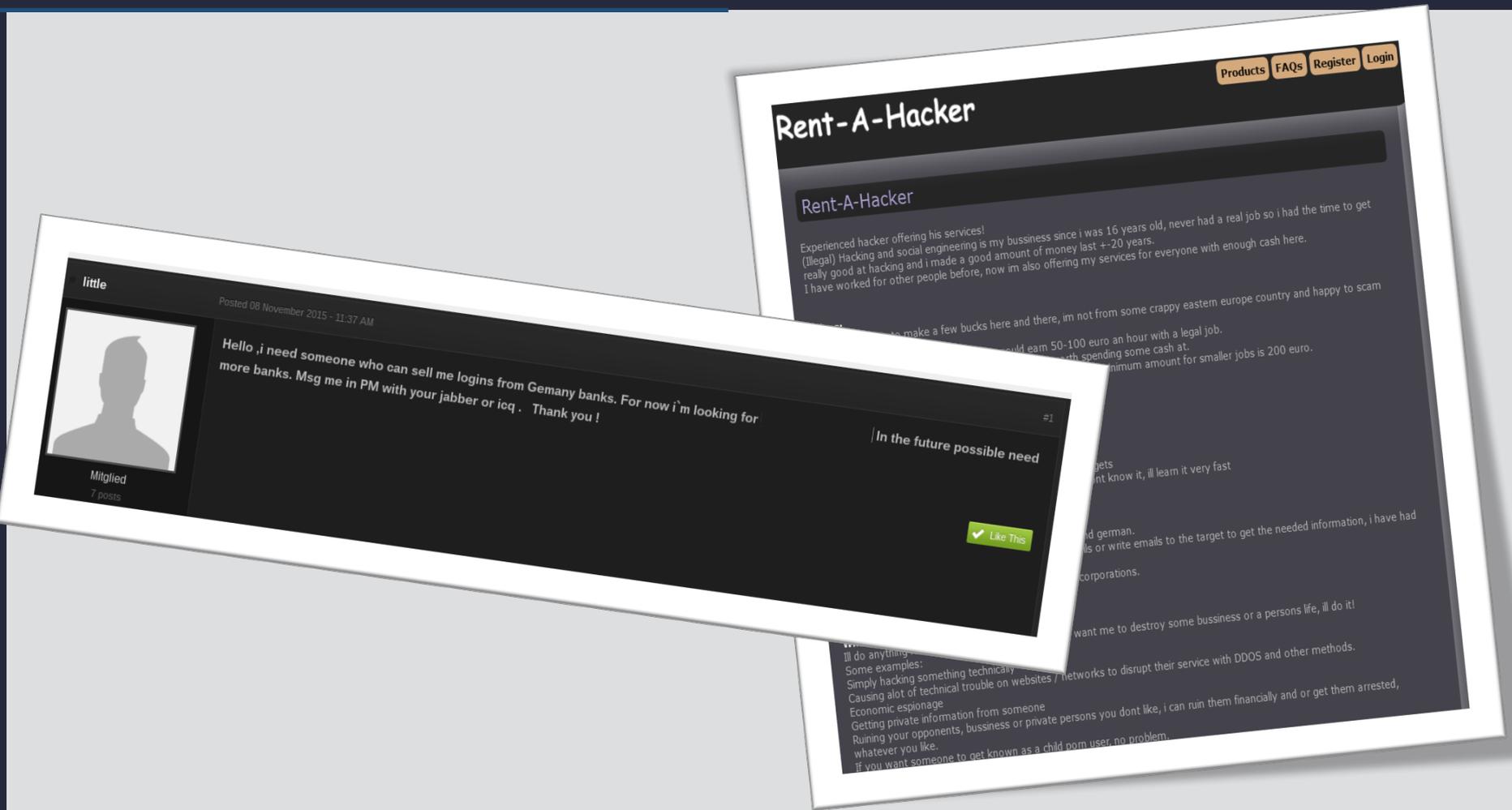
Community Stats	
Group	2nd LVL
Active Posts	355
Profile Views	699
Age	Age Unknown
Birthday	Birthday Unknown

Below the stats is a 'Contact Information' section. To the right of the 'alechanow' profile is a large black box containing several lines of green text: 'Ist alles gut an gekommen. am 6.1 bestellt und heute Morgen im Briefkasten, also eine Versandzeit von 2 Tagen. Blüten wie oben schon gesagt nicht perfekt.', 'Finde die Farben ein wenig zu blass, beim vergleich mit einem echten sieht man deutlichen unterschied.', 'Bei einem ist nach aufsprühen von Haarspray die Farbe verlaufen. was aber evtl daran liegen kann, das mein Kollege ein wenig zu viel drauf gemacht hat, ich war nicht dabei, wollte es aber erwähnen.', 'Ich möchte nichts schlecht reden, aber ich habe schon wesentlich bessere gesehen.', 'Das positive ist, das sie sich ziemlich gut an fühlen, und die Farben mit Haarspray intensiver werden.', and 'Wenn ich das Bild vom Vorposter nochmal vorziehen kann; <http://www.directupl...cc5a7f5.jpg.htm>'. At the bottom right of the collage is the IntSights logo and the text 'Proprietary and Confidential. IntSights Cyber Intelligence Ltd. © 2017. All rights reserved.'

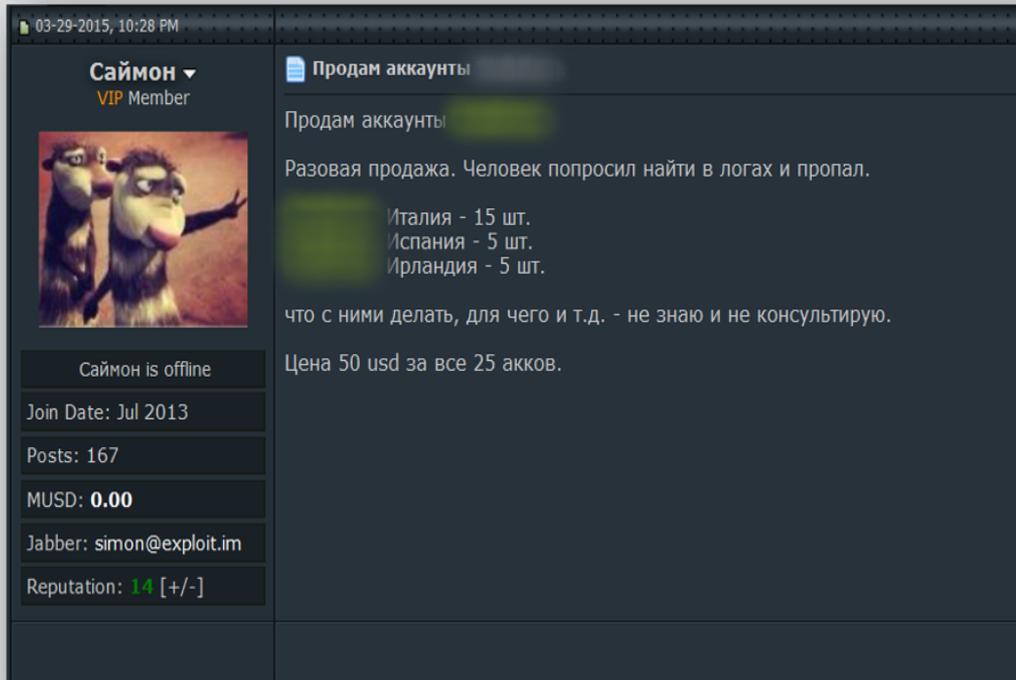
2

Qué tipo de actividad ocurre
en la Dark Web?

Central de Actividad Criminal



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

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

Contacts of [redacted].com

ORGANIZATION DETAILS

Host [redacted].com

Name [redacted]

Contacts **1,664**

Documents **694**

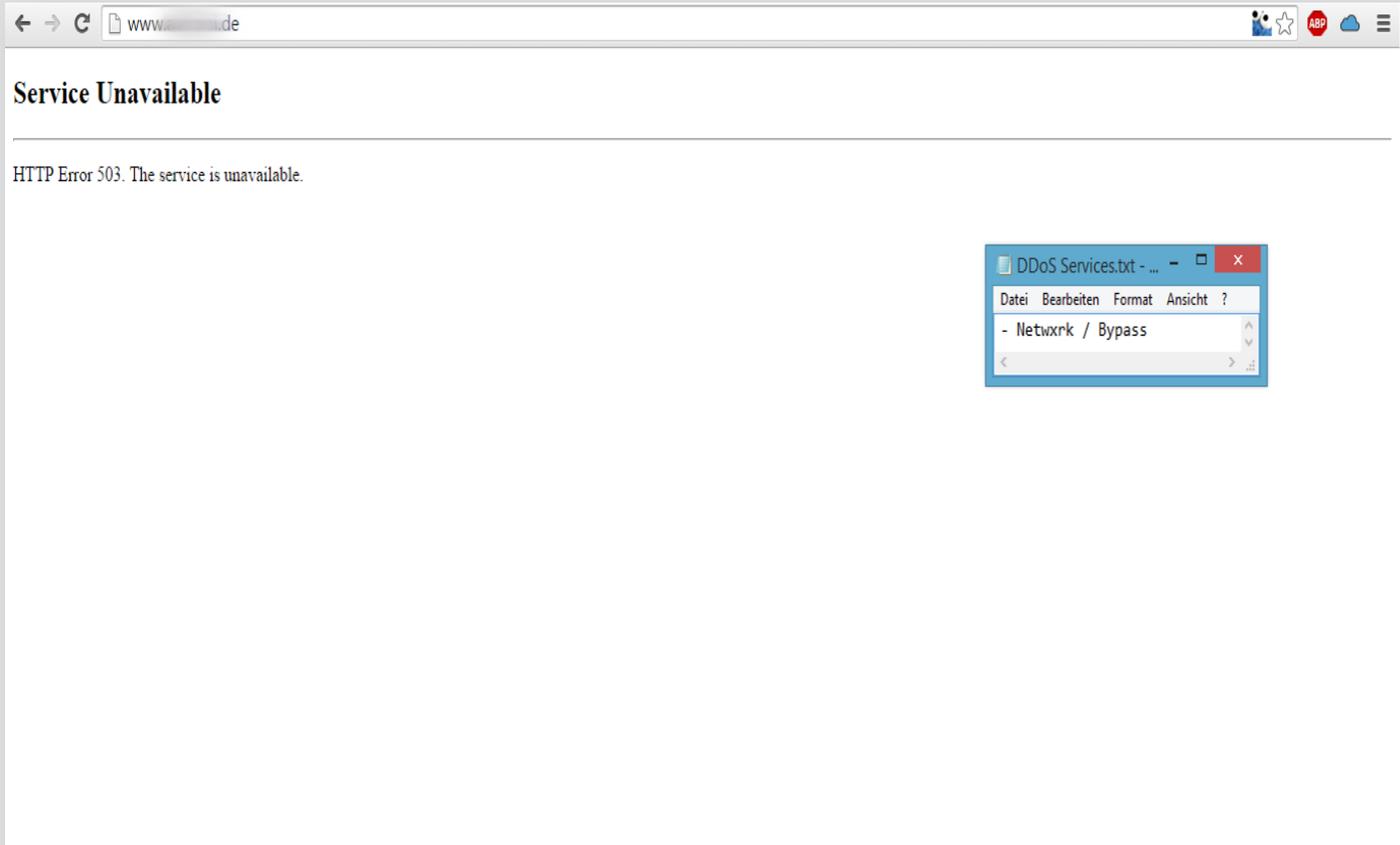
Related **12,208** organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.

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	j*****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

Qué se Vende en la Dark Web?



Mercados en la Dark Web

Is there trust among crooks?

(14:16:05) hack3r133t@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) hack3r133t@jabb3r.org : Yo también estoy allí

(14:18:17) hack3r133t@jabb3r.org : Te recomiendo 8chan

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

(14:19:16) hack3r133t@jabb3r.org : 8ch.net/baphomet/res/104638.html

(14:19:46) hack3r133t@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) hack3r133t@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



ThinkingForward | User Profile

 ThinkingForward(50130) Vendor Level 1 Trust Level 8

Positive feedback (last 12 months): 89%
[How is the feedback score calculated?]

Member since: March 18, 2015
Contracts: 0 in progress, 0 complete

View Store
Send Message
Favorite
Blacklist
FE Allowed

Seller Feedback Ratings (last 12 months) **Buyer Statistics** (since join date)

	1 month	6 months	12 months		Since join
Positive	463	3113	4536	Total disputes / orders	0 / 43
Neutral	25	144	264	Total spendings	...
Negative	83	496	411	Feedback left	8 (37.5% positive)
				Last online	Mar 31, 2016

Detailed seller ratings:

	Stealth	Quality	Value for price
	★★★★★	★★★★★	★★★★★

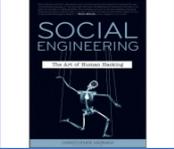
Not USA CC Please Replace
always a+ just know what you are doing
4/5 is AU CC. Terrible. Never buy again
Best seller on ABI!
Best seller on ABI!

About Positive Feedback Neutral Feedback Negative Feedback Feedback Left PGP

3

¿Cómo Aprovechar la Dark Web para Seguridad Proactiva?

“Ladrón que roba a ladrón”

Motive	Targeting	Development	Infrastructure	Recon	Attack
					
					
					

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]:crazydaze63
combo 176k.txt:razrok@[REDACTED]:rizzorat
combo 176k.txt:Smith.Justin218@[REDACTED]:justinsmith
combo 176k.txt:wziewitz@[REDACTED]:walker99
combo 176k.txt:coolspoofo@[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]:hobo
combo 176k.txt:ivanhogan@[REDACTED]:redgreen
```

Cuentas de Banco a la Venta

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

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:

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary

Address [17vHnkXwYaSRipEWNWwNgPvC51ZBswy](#)
Hash 160 [4bfaef88b8e34299a511911c0f050c238a1225c4](#)
Tools [Related Tags - Unspent Outputs](#)

Transactions

No. Transactions 2
Total Received **0.011 BTC**
Final Balance **0.011 BTC**



[Request Payment](#) [Donation Button](#)

Transactions (Oldest First)

[Filter](#)

Transaction ID	Amount	Date
7ae02235a79681f1a7d7575ee66709e922f54e0c704bab1ec0d415079d3ef1d	0.011 BTC	2017-09-09 11:56:52
1AzR9XkaXlaxo9DKBSDmndZAu3LlgasqnEm	0.011 BTC	



[17vHnkXwYaSRipEWNWwNgPvC51ZBswy](#)

0.011 BTC

0.011 BTC

- 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

¡Gracias!

¿Preguntas?





NEXTVISION

Ciberseguridad Inteligente

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

nextvision.com

