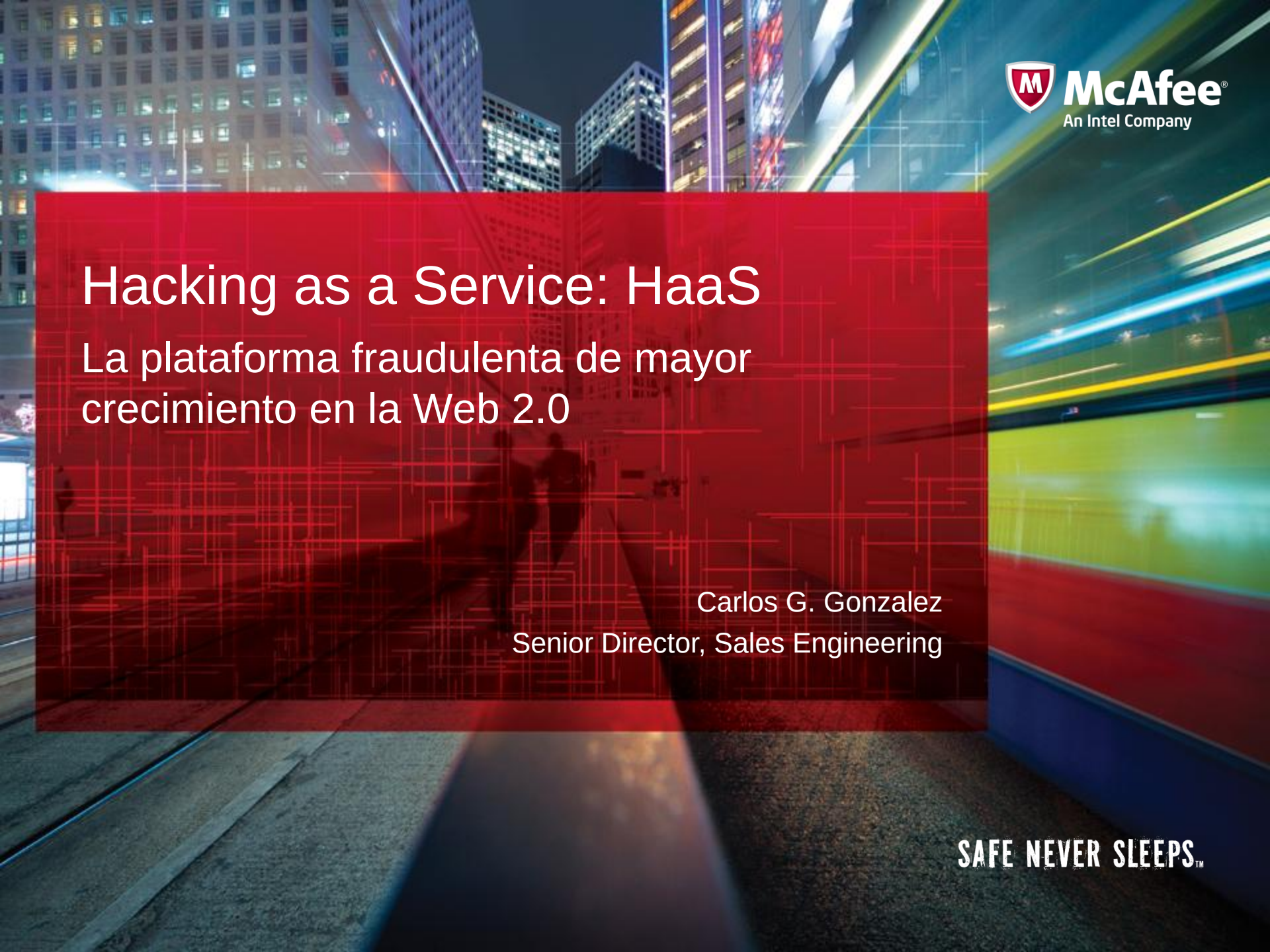


Hacking as a Service: HaaS

La plataforma fraudulenta de mayor crecimiento en la Web 2.0

Carlos G. Gonzalez
Senior Director, Sales Engineering

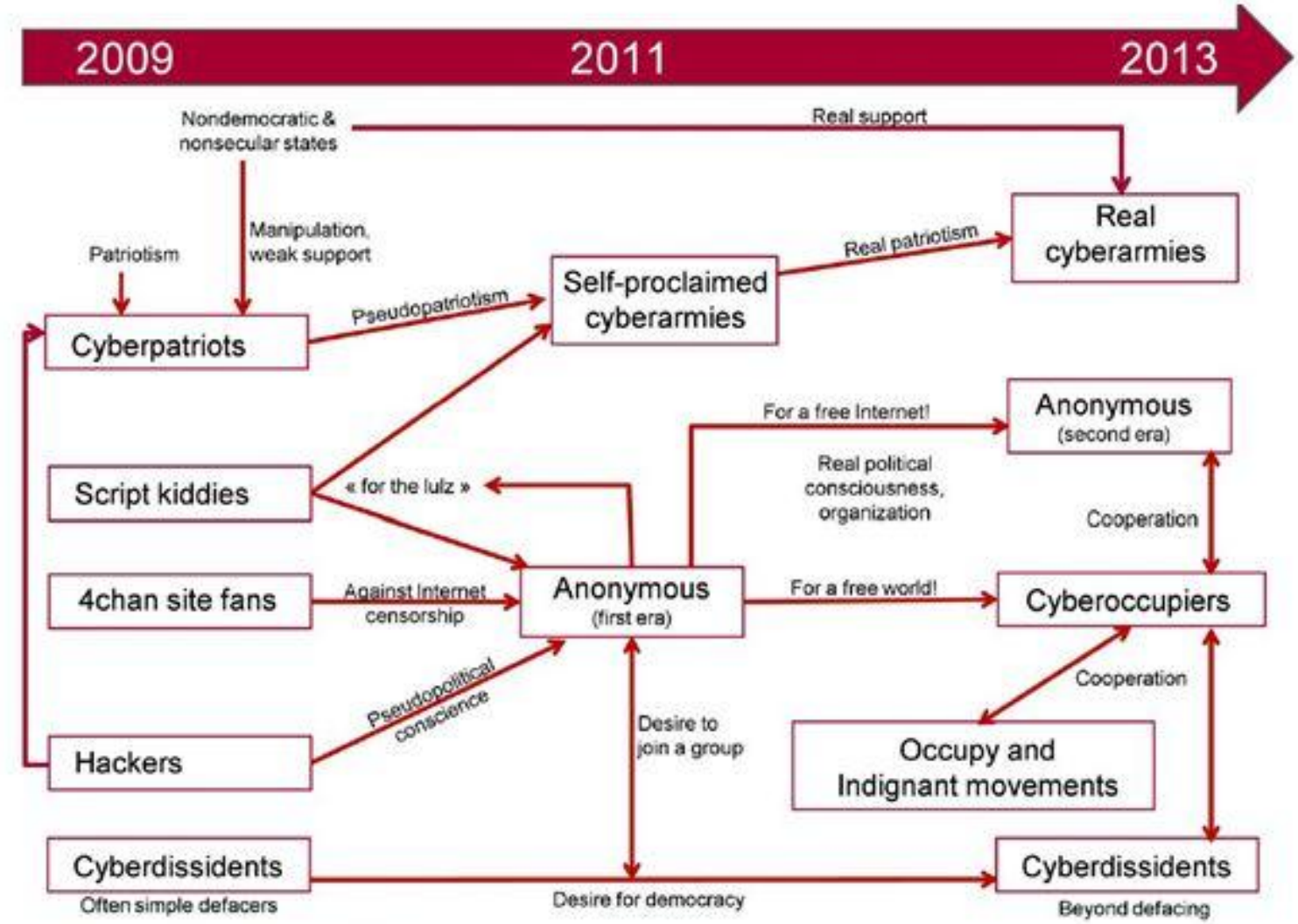
SAFE NEVER SLEEPS™

Hacking-as-a-Service: HaaS

- **InfoSecurity (15 Nov, 2012):**
  - **“HaaS: Un grupo rentando accesos a servidores de empresas Fortune 500, como Cisco, toman ventajas de claves débiles para entregar accesos fáciles. A pesar de su descubrimiento hace tres de semanas, el servicio parece tener mucha fuerza, el ultimo conteo fue de casi 17,000 computadores globalmente.”**

Hacking-as-a-Service: Un patrón alarmante

- **McAfee en su reporte de predicción de amenazas para el 2013, dice que la demanda por los servicios de hacking de los criminales ciberneticos aumentaran.**
  - **“Por mucho tiempo, los criminales cibernéticos han participado en foros públicos para discutir y hacer negocios con otros criminales. En estas reuniones, no soto venden el software sino que también se venden los servicios. Criminales cibernéticos profesionales, ven estos como una perdida de tiempo y confidencialidad (cada trato necesita contacto directo con el cliente quien pudiese ser un agente en cubierto), y una perdida de dinero (el comprador trata de negociar un precio mas bajo),“**
  - **“Por estas razones, el numero de invitaciones privada a foros criminales que tienen costos de registro y garantías han aumentado.”**



Possible evolution of the hacktivist movement

Hacking-as-a-Service o Crimeware-as-a-Service

- Compuestos por
  - Exploit Packs (Paquetes de Exploits)
  - Botnets
  - Proxies as a service
  - Spam
  - DDoS as a Service
  - Bullet Proof Hosting
  - Fake Pharma
- Recent past
  - Prices for crimeware as a Service (oldies)

Exploit packs

Un exploit pack (o BEP - Browser Exploit Pack) es un toolkit que automatiza la explotación de vulnerabilidades en el lado del cliente. Es generalmente entregado como un paquete de archivos exploit de PHP y HTML (incluyendo JAVA, PDF, Navegadores, Adobe Flash Player, etc.) diseñado para atacar el SO, browser y otras aplicaciones en el lado del cliente.

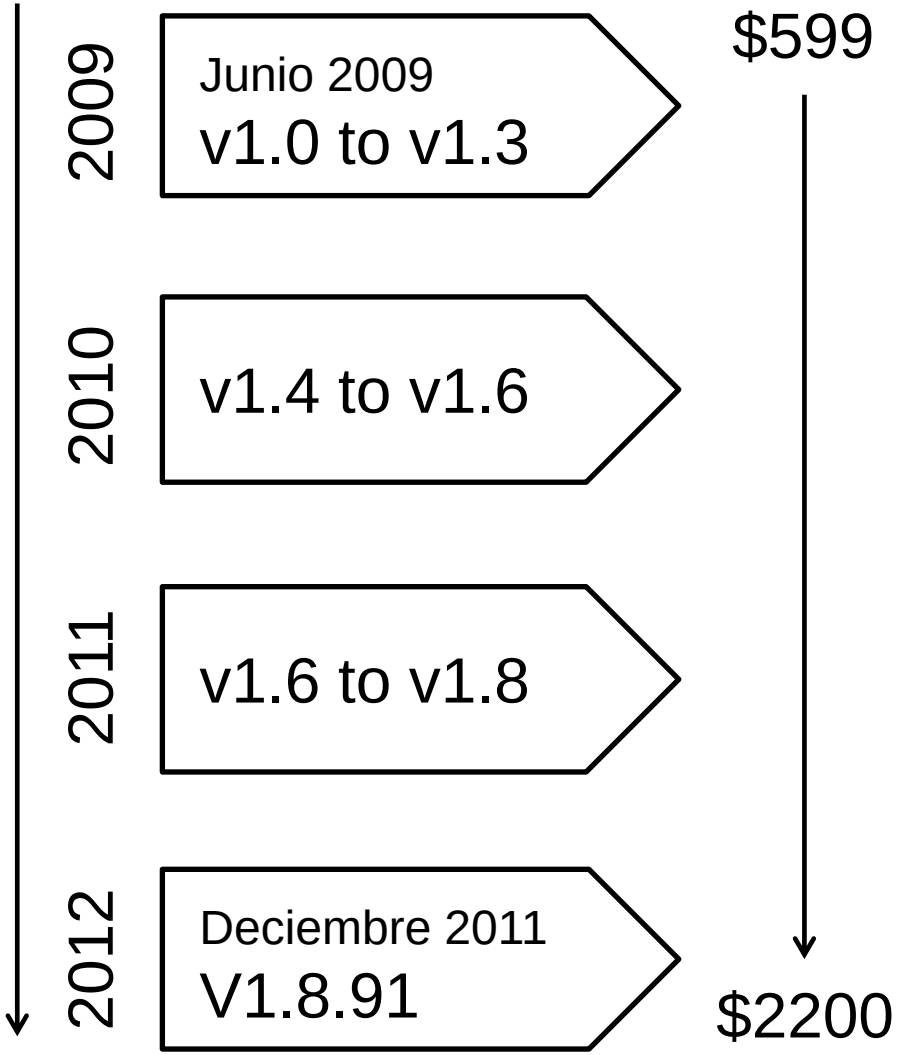
Kahu Security (http://www.kahusecurity.com/2012/wild-wild-west-062012/)

Eleonore Exploit Pack de Exmanoize

Eleonore es un paquete de código malicioso ofrecido a la venta en el mercado negro desde el 2009. Contiene una colección de exploits los cuales pueden ser usados para alterar paginas web. Cuando ejecutado, si la pagina es visitada por un sistema vulnerable, la carga del exploit es ejecutada. El paquete también provee la habilidad de control y comando para administrar los sistemas comprometidos.

Hacking-as-a-Service o Crimeware-as-a-Service

Eleonore Exploit Pack de ExManoize



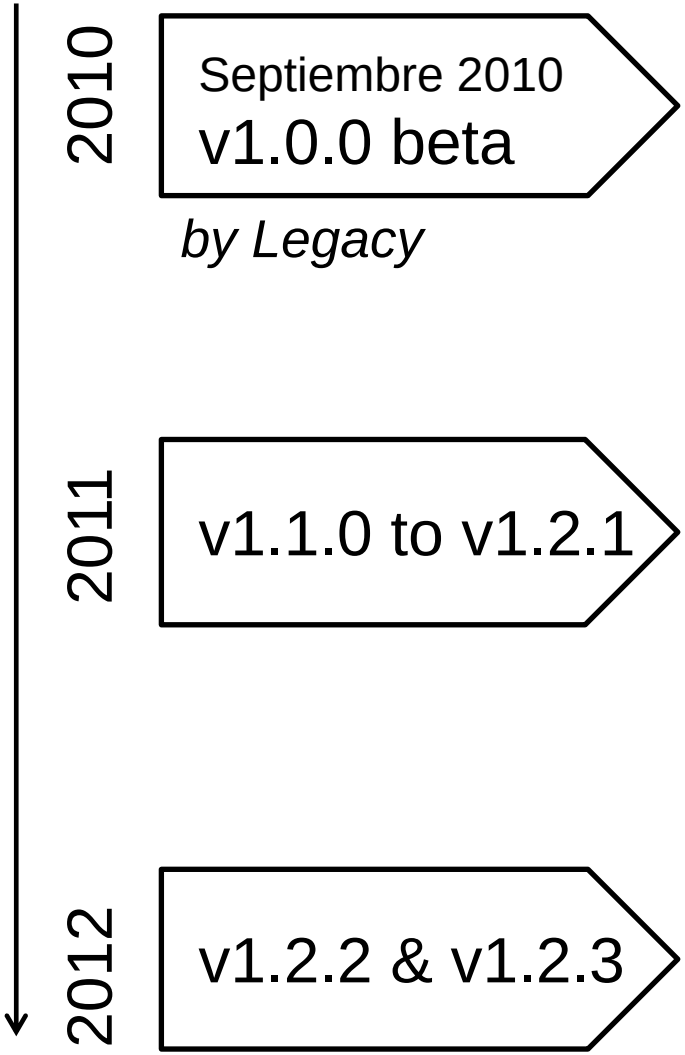
Цена последней версии 1.2:
> Стоимость самой связки = 700$
> Чистки от AB = 50$
> ребилд на другой домен = 50$
* Связка с привязкой к домену.
*** для первых 3х покупателей, цена связки 600$**

The price for the latest version 1.6.x:
> Cost of the bundle itself = $2000
> Cleaning from AB = from $50
> Rebuild to other domain = $50
> Updates = from $100
* Bundle with binding to a domain or IP

The price of last version 1.8.91 :
> Cost of the sheaf = 2200$
> Cleanings from antivirus = от 50$
> Domain change free of charge, change ip = 50$
> Updates = от 100$
* Sheaf with a binding to the domain or IP .

Crimeware as a Service

Black Hole Exploit Pack de Paunch



En las Noticias…

- Abril 6, 2011: Sitio Web USPS.gov infectado con Blackhole Exploit Kit;
- Mayo 13, 2011: Visitantes a Geek.com atacados por Blackhole Exploit Kit;
- Ago. 28 to 31, 2011: Investigadores detectan miles de sitios WordPress infectados con Black Hole;
- Nov. 2, 2011: Blackhole Exploit Kit ataca el sitio WampServer;
- Feb. 12, 2012:Cryptome Infectado con el ToolKit Blackhole;
- Mayo 31, 2012: Links en el sitio web de TSA en los EEUU llevan al Blackhole exploit kit.

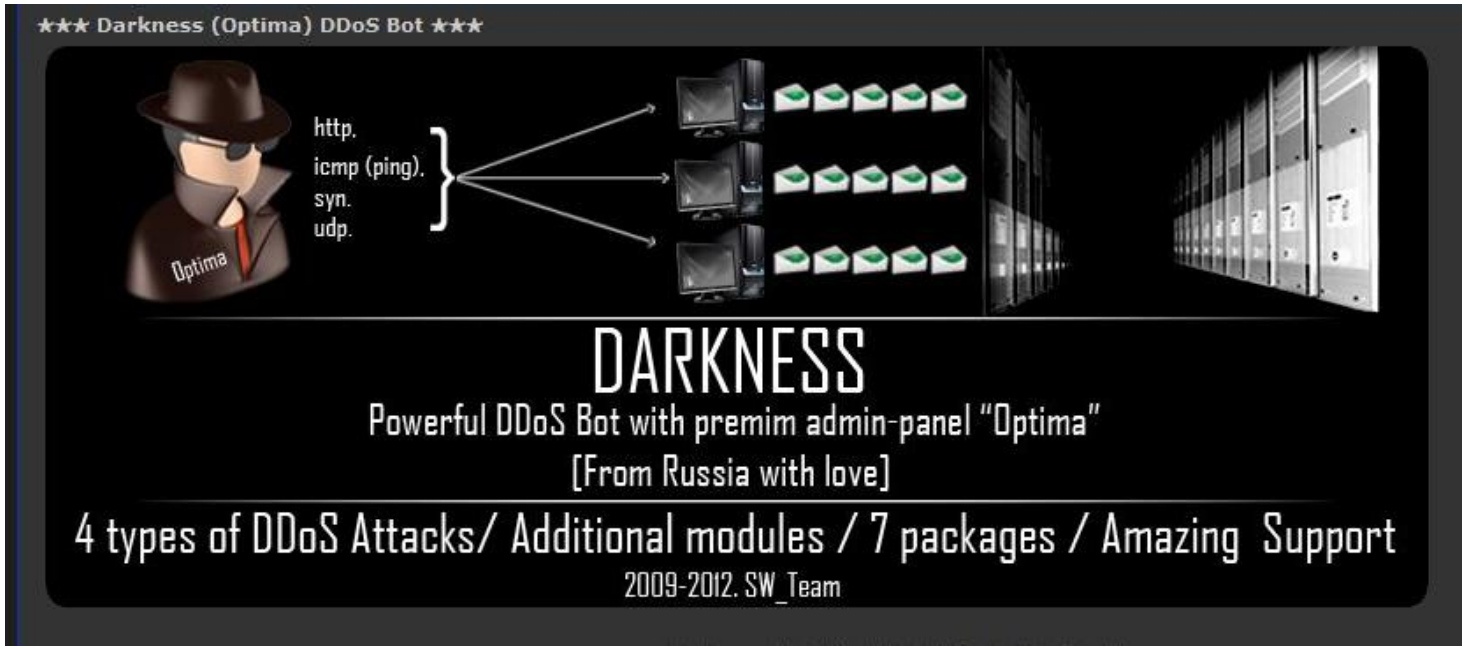
Crimeware as a Service – 2012

Exploit Toolkits	Description
LinuQ (July 2011)	Between bot and exploit pack, this package is designed to compromise linux servers. In its public version, it should use 4 PMA vulnerabilities (CVE-2009-1148/1151) $200 (public version) - $1,500 (with private exploit)
Bleeding Life V3 (August 2011)	A kit with 10 exploits. Price for new buyers: $1,000. A $250 discount is offered for previous buyers
Phoenix Exploit Kit 3.1 (March 2012)	The V3 version included the Java Rhino exploit (CVE-2011-3544). This latest includes Java Atomic (CVE-2012-0507). $2,200 (single domain) - $2,700 (multithreaded domain)
BlackHole Exploit Kit 1.2.1 (November 2011 – Russia))	It also includes Java Rhino (CVE-2011-3544). Annual license: $1,500 – 1 week renting on Blackhole servers: $200
Eleonore V1.8.91 (December 2011 - Russia)	This update includes Java Rhino (CVE-2011-3544) and 5 other 2011 exploits. $2,200
Zhi Zhu (February 2012 - China)	Five exploits of which WMP MIDI (CVE-2012-0003).
Gong Da Pack (February 2012 - China)	Three exploits of which WMP MIDI (CVE-2012-0003).

Crimeware as a Service

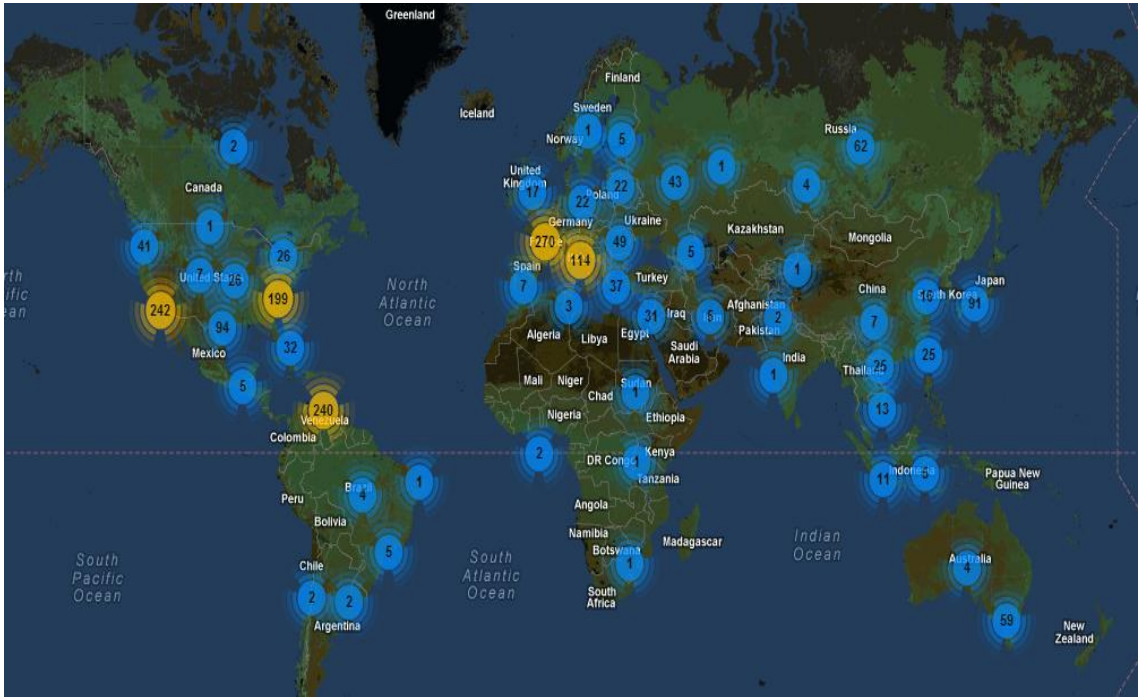
Botnets

Una red de bots es una red infectada de computadores bajo control remoto por un cibercriminal en línea. El usa esta red para enviar spam, lanzar ataques de Denegación de Servicio o distribuir código malicioso financiero. El puede alquilar esta red a otro criminal.



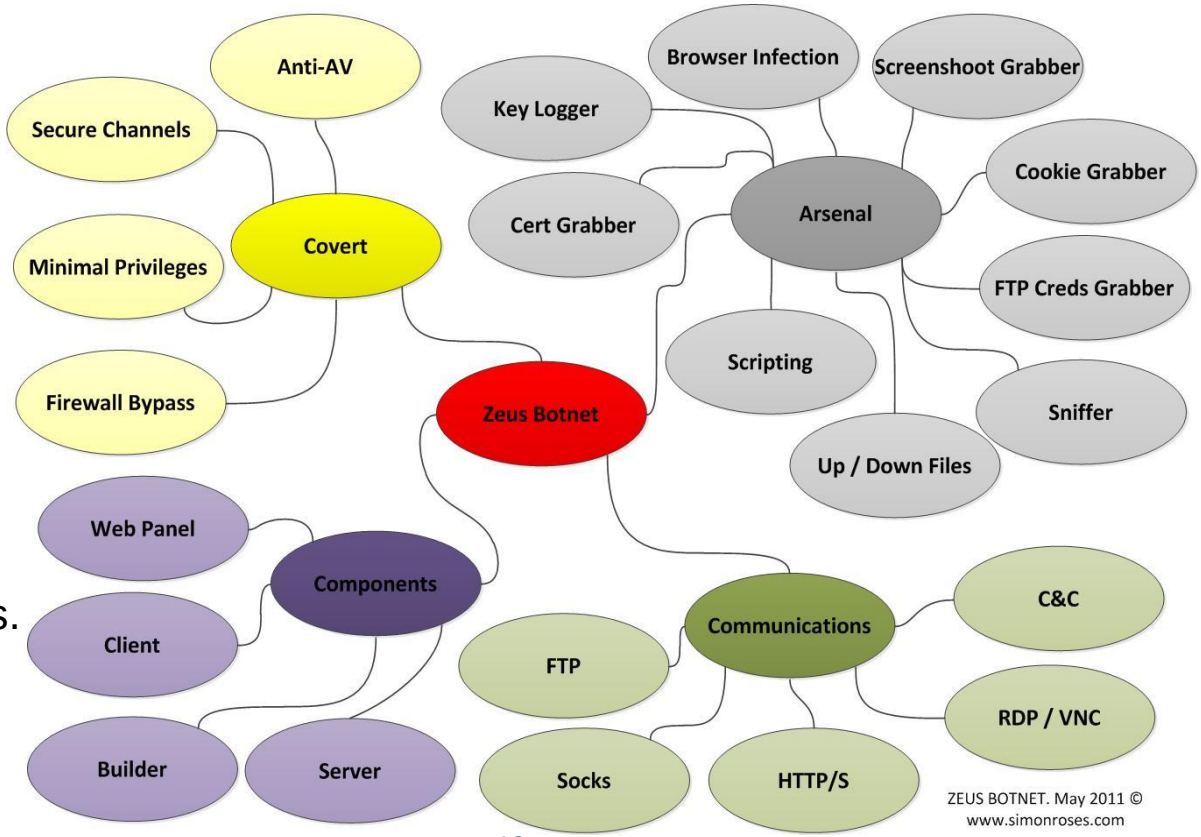
Actividad Global de BOTNETs

- McAfee monitorea la actividad de botnets y sus servidores de control mientras se plagan por el Internet. Los sistemas protegidos por las soluciones McAfee al igual que los dispositivos de seguridad de redes envían información al McAfee Global Threat Intelligence (GTI) en la nube, y junto con la amplia colección de binarios de código malicioso e investigación proactiva, McAfee tiene una visión clara de las amenazas globales de botnet



Crimeware as a Service

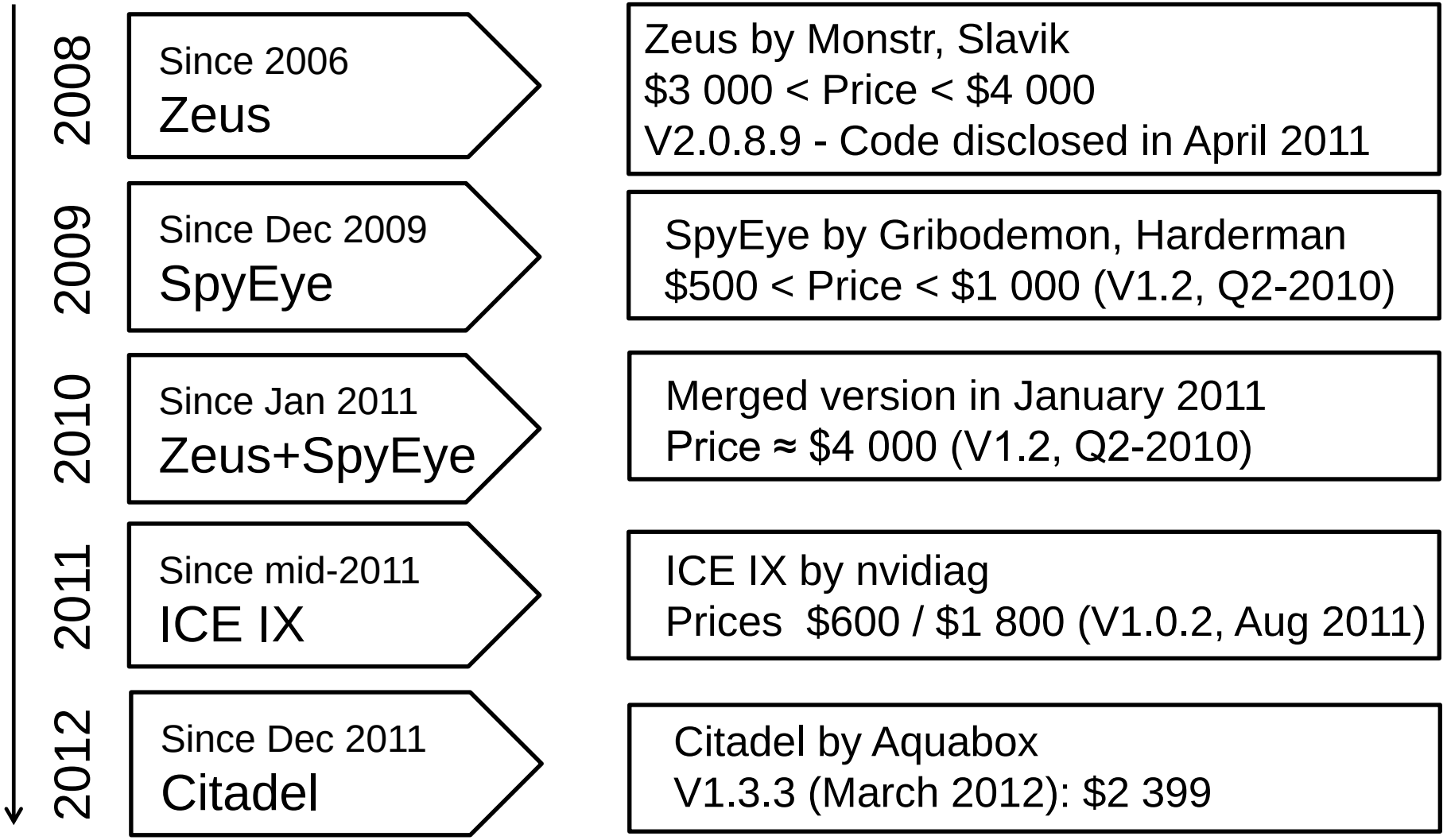
Ciencia de Zeus: Zeus y sus sucesores, SpyEye, ICE IX y Citadel son primeramente usados para robar credenciales financieras en line. Disponibles para la venta, Estos contienen un constructor que puede generar un bot ejecutable asociado a un administrador.



Panel usado para administrar información acerca del botnet y tareas que deben ser realizadas. Pueden ser completadas por módulos opcionales para maximizar su poder malicioso

Crimeware as a Service

Zeus lineage



Crimeware as a Service – 2012

Botnet (Command & Control Toolkits)	Description
Darkness by SVAS/Noncenz (DDOS bot)	DDOS bot From $450 to $999 according to the package - Sources - ~3500-5000$
Citadel	Zeus/SpyEye variant. Financial botnet. Bot builder + admin panel - $2399 + a $125 monthly “rent” (December 2011 price) Automatic update facilities for antivirus evasion - $395. Each update is charged $15
THOR by TheGrimReap3r	Multipurpose P2P botnet. $8000 for the package without modules. Discount of $1500 for the first 5 buyers (March 2012 price). Expected modules under development are: advanced botkiller, DDoS, formgrabber, keylogger/password stealer and mass mailer.
Carberp	Financial botnet Loader + grabbers + all the basic functionality (except for the fact that below) - $2500 (March 2012 price) Anything above + Backconnect 500 connections + IE/FF inject - $5000 Anything above + Hidden browser (similar to VNC) - $8000

Proxies as a Service

Awmprowy.net

En Septiembre 2011, Brian Krebs analizo algunas actividades asociadas al botnet TDSS y particularmente a awmprowy.net. Estos proxies de servicios se presentaron como “Los proxies anónimos mas rápidos”. Antes que este mercado subterráneo desapareciera logramos obtener algunos precios.

Proxies HTTP/SOCKS (http, https, socks4, socks5)				
	Semi Annual	**Mensual/ Limitado**	**Mensual/ Ilimitado**	**Ilimitado-90 Dias**
Costo (Sin e-mail)	65$	95$	195$	500$
Costo (Con e-mail)	-	350$	550$	1400$
Numero de IPs para poder accederlo	Each user gets full access to the whole base on private HTTP/SOCKS (that is why many proxies get to the blacklists)			
Numero of procesos	350		unlimited	

Proxies as a Service

Awmprowy.net

Exclusive/individual proxies (for anonymous browsing, ICQ and FTP; for online-games like casino, poker and roulette. These proxies are given in one hands only)			
	Exclusive-100	**Exclusive-200**	**Exclusive-500**
Amount proxy	100	200	500
Amount of changes in the list per day	50	100	200
Automatic substitution of "dead" proxies by choosing a priority country	ALL RU US/CA		
Cost **Week** **2 weeks** **30 days**	90$ 160$ 290$	160$ 290$ 550$	300$ 550$ 1000$
	Individual-5	**Individual-15**	**Individual-30**
Proxy simultaneously	5	15	30
Amount of changes in the list per day	30	50	100
Cost **2 weeks** **30 days**	40$ 60$	60$ 100$	100$ 160$

Proxies as a Service

Awmprowy.net

Personal proxies (They are browser proxies to anonymously access porno sites, entertainment resources for online casinos, payment systems and other sites that block access for certain countries)			
	Day	Two weeks	Monthly
Cost (traffic unlimited)	3$	15$	25$
Number of IPs to access from	1	3	3
Duration	day	14 days	30 days

Private HTTP proxies (to profit from a static IP from the country you need. To improve performance in mailing campaign)					
	Elementary	Advanced	Professional	Unlimited	Unlimited-90
Cost per month	35$	50$	60$	95$	240$
Term	month				90 days
Number of IPs to access from	1	2	3	3	3
Number of threads per account	100	200	400	unlimited	

Spam – Listas de Correos

Pais	Precios (Todos en US$)
Alemania	1 000 000 direcciones: $25 3 000 000 direcciones: $50 5 000 000 direcciones: $100 8 000 000 direcciones: $200
Turquia	1 000 000 direcciones: $50
Portugal	150 000 direcciones: $25
Australia	1 000 000 direcciones: $25 3 000 000 direcciones: $50 5 000 000 direcciones: $100
Inglatera	1 500 000 direcciones: $100

Pais	Precios (Todos en US$)
Rusia	400 000 direcciones èn St Petersburg: $25 1 000 000 direcciones: $25 3 000 000 direcciones: $50 5 000 000 direcciones: $100 8 000 000 direcciones: $200
EEUU	1 000 000 direcciones: $25 3 000 000 direcciones: $50 5 000 000 direcciones: $100 10 000 000 direcciones: $300
Ukrania	2 000 000 direcciones: $40

Spam – Relay de SMTP

Log in

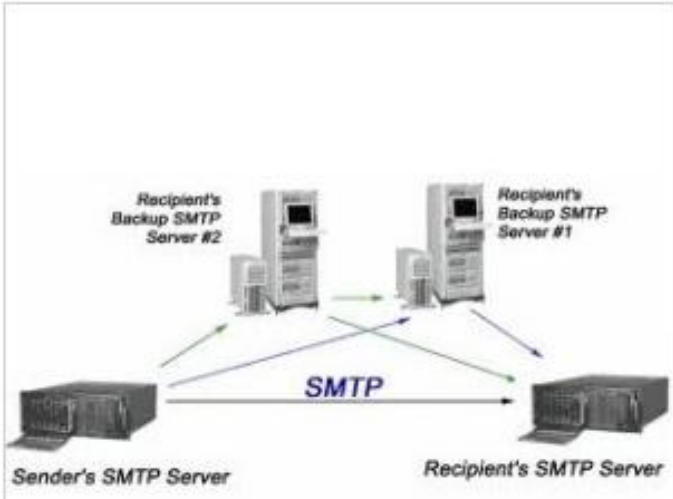
+1

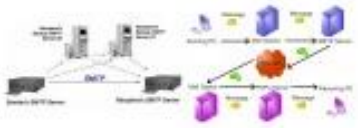
Home > Smtp Relay Server > Smtp Relay Server for 30 000 000 emails

CATEGORIES

- 2012 Business Email List
- ⊞2012 Country Email List
- 2012 Domain Email Lists
- 2012 Email List
- 2012 General Global Email Lists
- 2012 Men's Email Lists
- 2012 Targeted Email List
- 2012 Woman Email List
- Discounted Price
- Email Marketing Campaigns
- Mass Email Software
- **Smtp Relay Server**

SMTP RELAY SERVER FOR 30 000 000 EMAILS





Smtp Relay Server for 30 000 000 emails for the one month

PRICE LOWERED!

$13,340.25 tax incl.

~~$14,822.50 tax incl.~~

(price reduced by 10 %)

Quantity : 1

Availability: 999 items in stock

Add to cart

Add to my wishlist

PayPal
Click here to pay

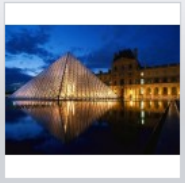
Spam – Base de Datos de Correos Electrónicos

FRANCE EMAIL DATABASE *4 products*

sort by --

France Email Database 1 million Available
France Email Database 1 million
PRICE LOWERED!
$495.49
Add to cart
View

France Email Database 5 million Available
France Email Database 5 million
ON SALE!
$931.70
Add to cart
View



France Email Database 10 Millions Available
France Email Database 10 Millions
PRICE LOWERED!
$1,257.79
Add to cart
View

France Email Database 20 Millions Available
France Email Database 20 Millions
PRICE LOWERED!
$2,210.67
Add to cart
View

USA STATES EMAIL DATABASES *33 products*

sort by --

USA Florida State Email Database... Available
USA Florida State Email Database (10 million emails)
PRICE LOWERED!
$876.64
Add to cart
View

USA Delaware States Email... Available
USA Delaware State Email Database (3 million emails)
PRICE LOWERED!
$419.26
Add to cart
View

USA Maine States Email Database... Available
USA Maine State Email Database (3 million emails)
PRICE LOWERED!
$419.26
Add to cart
View

USA Nevada State Email Database... Available
USA Nevada State Email Database (3 million emails)
PRICE LOWERED!
$724.18
Add to cart
View

Spam – Base de Datos de Correos Electrónicos

Ebay Email Database
Ebay Email Database (1 Million)
Available
PRICE LOWERED!
$266.80
Add to cart
View

Yahoo Email Database
Yahoo Email Database (5 Millions)
Available
PRICE LOWERED!
$343.03
Add to cart
View

Hotmail Email Database
Hotmail Email Database (3 Million)
Available
PRICE LOWERED!
$245.02
Add to cart
View

AOL Email Database
AOL Email Database (5 Millions)
Available
PRICE LOWERED!
$266.80
Add to cart
View

Gmail Email Database
Gmail Email Database (5 Millions)
Available
PRICE LOWERED!
$343.03
Add to cart
View

MSN Email Database
MSN Email Database (5 Millions)
Available
PRICE LOWERED!
$343.03
Add to cart
View

USA DOCTOR EMAIL DATABASE

USA Doctor email Database (0.7 Million)

PRICE LOWERED!
$114.34 tax incl.
~~$127.05 tax incl.~~
(price reduced by 10 %)
Quantity : 1
Availability: 999 items in stock
Add to cart
Add to my wishlist

PayPal
Click here to pay

2012 WOMAN EMAIL LIST *1 product*

sort by --

Woman's Interest Email Database
Woman's Interest Email Database (16.2 Millions)
Available
ON SALE!
$1,312.85
Add to cart
View

DDoS como Servicio

Gwapo

$5 / por hour
$120 / por day
$2,500 por month

Crimeware as a Service

Darkness

El bot Darkness (Optima) es un DDoS que se hizo popular en el 2011. Es capaz de lanzar ataques HTTP, ICMP, y TCP a máxima velocidad, mientras que se mantiene relativamente anónimo en su operación.

10-th version.

Packages:

- Minimum: DDoS Bot, no free updates, no modules = $450
- Standart: DDoS Bot, 1 month free updates, password grabber module = $499
- Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = $570
- Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = $650
- Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = $699
- Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = $825
- Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = $999

Other:
- ReBuild (URLs changing) – $35.
- Sources - ~3500-5000$, discuss individually
- New features - discuss individually.
- Web-Panel reinstalling (1st time is free) - $50

Source McAfee – Enero 2012

Bullet Proof Hosting

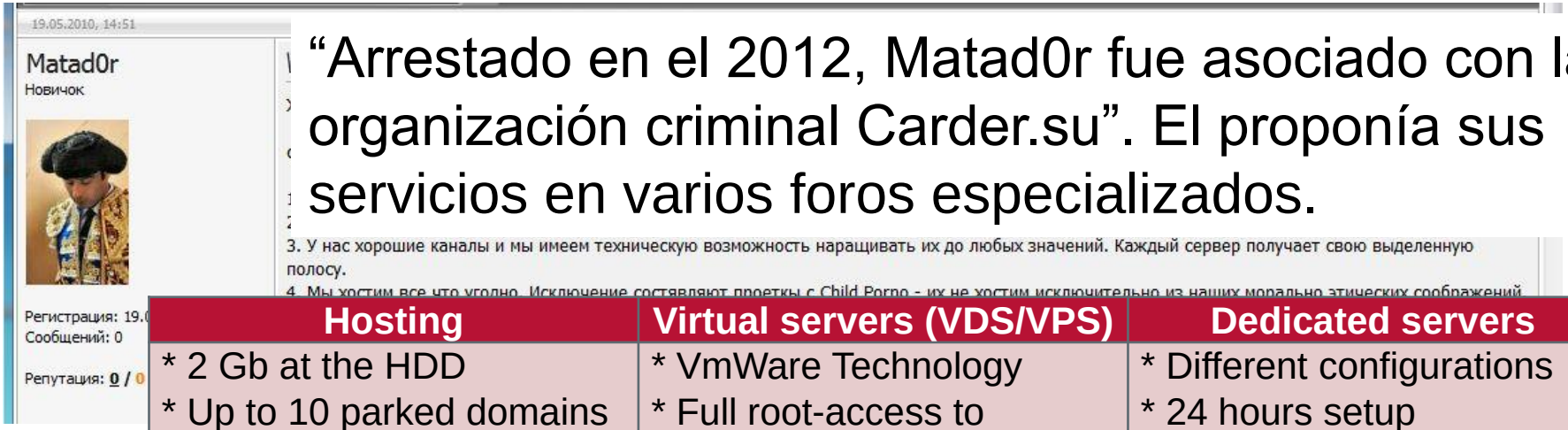
Proveedores conocidos como "bulletproof hosting" son aquellos que con conocimiento proveen servicios de web y hosting a cibercriminales intentando ignorar las quejas y no toman acciones contra el uso malicioso de sus servicios.

Según Wikipedia, Las Noticias dijeron:

- Russian Business Network (or RBN), bajado en Nov 2007
- Atrivo/Intercage, bajado en Sep. 2008
- McColo, bajado en Nov. 2008
- 3FN, bajado por la FTC en Jun. 2009
- Real Host, bajado en Agosto 2009
- Group Vertical, bajado en Oct 2009
- Riccom, bajado en Dic. 2009
- Troyak, bajado en Mar. 2010
- Proxiez, bajado en Mayo 2010
- Voze Networks, bajado en Feb. 2011

Bullet Proof Hosting

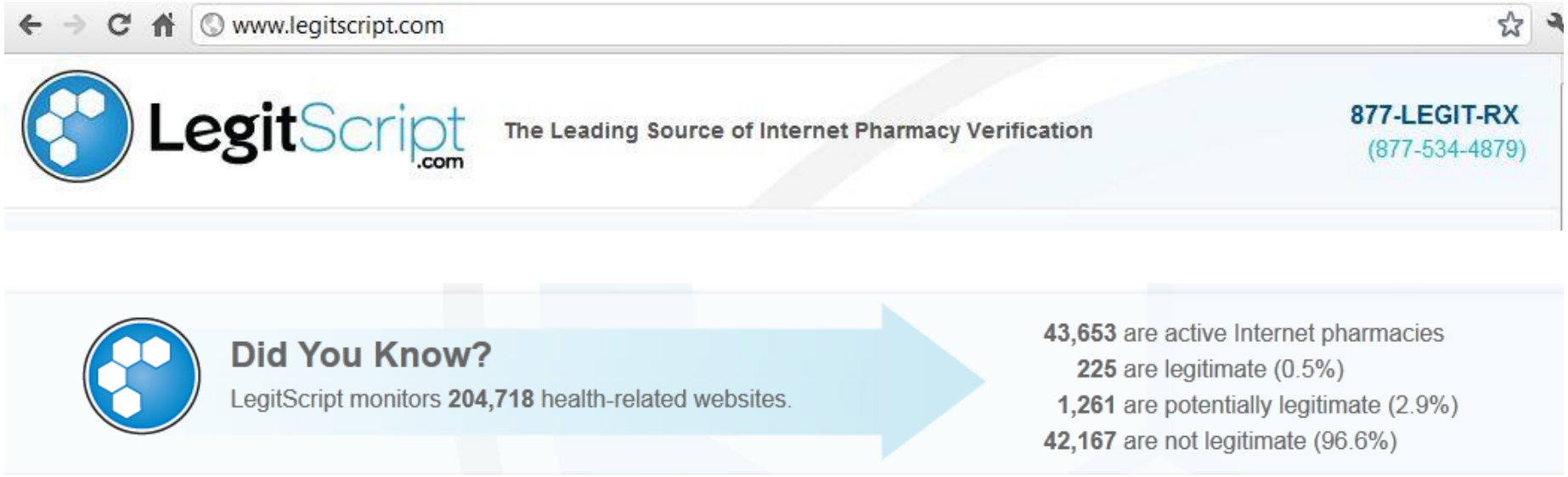
Matad0r



"Arrestado en el 2012, Matad0r fue asociado con la organización criminal Carder.su". El proponía sus servicios en varios foros especializados.

Hosting	Virtual servers (VDS/VPS)	Dedicated servers
* 2 Gb at the HDD * Up to 10 parked domains * Dedicated DNS servers * Hosting control panels * Unlimited Traffic * Necessary modules and soft for free **50$ per month**	* VmWare Technology * Full root-access to servers * Up to 25% CPU Xeon * From 1 GB RAM * From 30 GB HDD * Unlimited traffic * Free setup/resetup * Full software set * Additional IP addresses if necessary **150$ per month**	* Different configurations * 24 hours setup * Unlimited traffic * Free setup/resetup * Any OS for free (including Windows) * Additional IP addresses if necessary **400$ per month**

Fake Phama


www.legitscript.com
LegitScript.com
The Leading Source of Internet Pharmacy Verification
877-LEGIT-RX
(877-534-4879)
Did You Know?
LegitScript monitors 204,718 health-related websites.
43,653 are active Internet pharmacies
225 are legitimate (0.5%)
1,261 are potentially legitimate (2.9%)
42,167 are not legitimate (96.6%)

Fake Phama

EvaPharmacy

El grupo de Internet conocido como EvaPharmacy es circulo de “medicinas” basado en crimen y mentira. Deliberadamente engañan a los potenciales clientes a “Comprar medicina de primera línea de farmacias localizadas en los EEUU”. En algunos casos se hacen pasar por “CVS Pharmacy”, una cadena de farmacias reconocida en los EEUU. Ninguno de los sitios web requiere una receta; todos venden medicinas falsas o prohibidas que importan legalmente de sitios como India, conocido como un sitio donde se consiguen medicinas ilegales.

Fake Phama

Affiliate Program	orders/month	*Spamalytics* single order	*Spamalytics* rev/month	Min product price single order	Min product price rev/month	Basket-weighted average single order	Basket-weighted average rev/month
33drugs	9,862	$100	$980,000	$45.00	$440,000	$57.25	$560,000
4RX	8,001	$100	$800,000	$34.50	$280,000	$95.00	$760,000
EuroSoft	22,776	N/A	N/A	$26.50	$600,000	$84.50	$1,900,000
EvaPharmacy	26,962	$100	$2,700,000	$50.50	$1,300,000	$90.00	$2,400,000
GlavMed	17,933	$100	$1,800,000	$54.00	$970,000	$57.00	$1,000,000
Online Pharmacy	5,856	$100	$590,000	$37.00	$220,000	$58.00	$340,000
Pharmacy Express	7,933	$100	$790,000	$51.00	$410,000	$58.75	$460,000
Royal Software	13,483	N/A	N/A	$55.25	$750,000	$133.75	$1,800,000
Rx–Promotion	6,924	$100	$690,000	$45.00	$310,000	$57.25	$400,000
SoftSales	1,491	N/A	N/A	$20.00	$30,000	$134.50	$200,000

Table 4: Estimated monthly order volume, average purchase price, and monthly revenue (in dollars) per affiliate program using three different per-order price approximations.

"En esta tabla podemos ver que GlavMed y EvaPharmacy tienen ganancias en exceso de un Millon de dólares y todas las demás menos 2, ganan mas de 400 Mil dólares por mes.

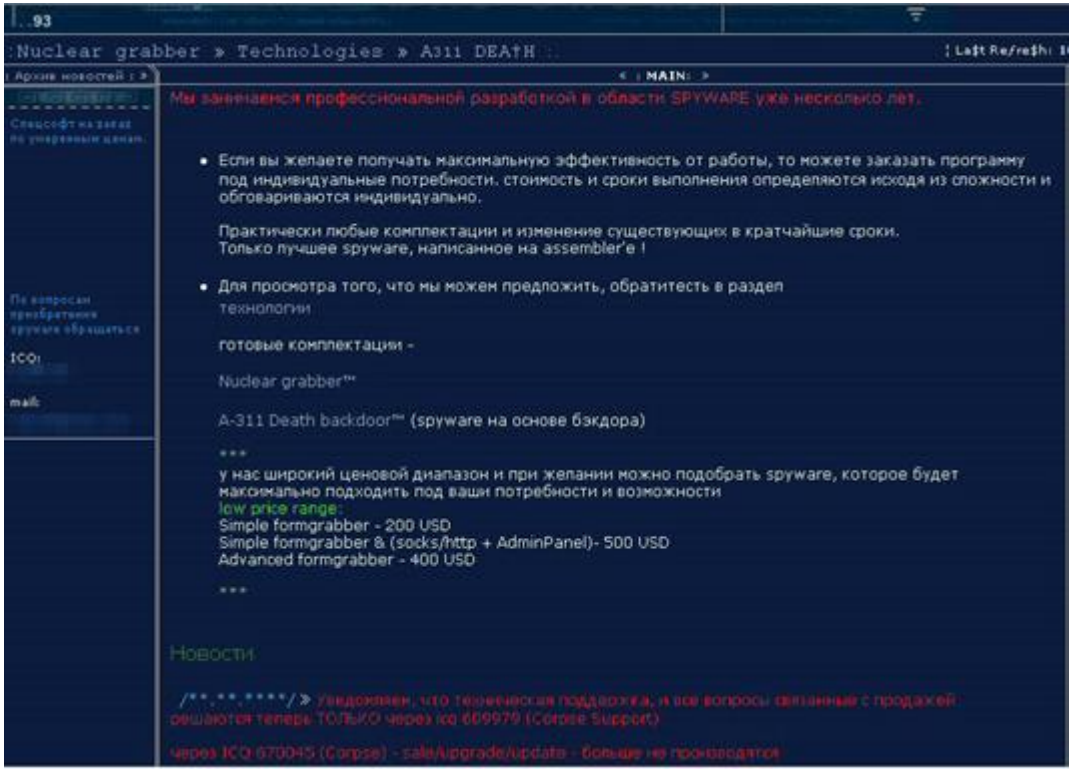
Fuente: http://cseweb.ucsd.edu/~savage/papers/UsenixSec11-SMTM.pdf

Recent Past

- Prices for crimeware as a service (oldies)
  - 2007
  - 2008/2009
  - 2009
  - 2009/2010
  - 2010
  - 2010/2011

Crimeware as a Service – 2007

The "Infection Kit" year



Crimeware/Author	Prices Encountered
FTP Checker	$15
IcePack (IDT Group)	$40 to $400
Limbo V1.7 (December 2006)	1,000 wmz (see note)
MPack (DreamCoders Team) V0.99 (Aug. 2007)	$700
Nuclear Grabber (Corpse) V5 (Feb. 2007)	$3,000 (October 2005) $100 (July 2007)
Pinch (Coban2k for the original version) V2.99 (Mar. 2007)	$30 Update: $5 Management help tool: $100
Power Grabber (privat.inattack.ru) v1.8 (March 2007)	$700 + $30 for anti-virus protection.
Web-Attacker (inet-lux.com)	$25 to $300 (July 2006) Approx. $17

Note: wmz is the symbol for one of the electronic money units used by WebMoney (1$US = 1wmz).

Crimeware as a Service – 2008/2009

Crimeware (Seller or Author)	Description	Prices Encountered
FirePack (Diel)	Web Exploitation Malware Kit Nota: a Chinese version exists	$3000 (February 2008) $300 (April 2007)
Zeus & Zeus Sploit-Pack (magicz)	The ZeuS trojan is able to inject code into login webpage of financial organization to ask personal data and divert them to a remote location. In addition to listening in on the submission of forms in the browser, it can take screenshots of the victim's machine, or control it remotely, or add additional pages to a website and monitor it, or steal passwords that have been stored by popular programs.	$3000 for Zeus (January 2009) $700 for Zeus Sploit-Pack (Jan 2009)
Adrenaline, an update of Nuclear Grabber (Corpse)	Universal kit for creating tools to capture targeted banking data. Able to intercept and retransmit authentic transactions on the fly between the bank and its client.	$3000
PolySploit, an update of NeoSploit (Grabarz)	Web Exploitation Malware Kit, statistical engine, enhanced configuration capability, exploitation package , enhanced support and online forum for customers.	100 €
El fiesta	Web Based and PDF-Exploit Pack used to launch attacks and monitor them.	$850 (December 2008)
Turkojan RAT (AlienSoftware)	A Remote Access Tool made in Turkey.	Bronze edition: $99 (July 2008) Silver edition: $179 Gold edition: $249
Sploit25	Browser vulnerability test kit with IE6, IE7 & PDF exploits	PRO vers: 2500WMZ (nov. 2008) Lite version: 1500 WMZ

Carding – 2008/2009

Service	Description	Prices Encountered
Dump CC's with CVV	Format: FULL NAME | COMPANY | ADDRESS | ADDRESS 2 | CITY | ZIPCODE | PHONE | COUNTRY | CC TYPE | NAME ON CARD | CC NUMBER | EXPIRATION DATE | CVV	United States 2$ Canada 4$ United Kingdom 4$ Australia 7$ Europe 8$ Asia 8$
Full Info	Format: IP | PAYPAL LOGIN | PAYPAL PASSWORD | CC TYPE | CC NUMBER | EXPIRATION DATE | CVV | NAME ON CARD | BANK NAME | FIRST NAME | LAST NAME | ADDRESS | ADDRESS2 | CITY | STATE | ZIPCODE | PHONE | DOB | MMN | SSN	United States 15$ Canada 35$ United Kingdom 25$ Australia 30$ France 25$ Germany 30$ Italy 30$
Custom Projects	Credit cards, full info or bank logins from any bank or institution with the information the customer request	1000$ upfront and 4000$ when project is ready
In bulk	100 Dumps EU Credit Classic - $5500 (201 code) 100 Dumps EU Credit Classic - $6500 (101 code) 100 Dumps EU Credit Gold/Platinum - $7500 (201 code) 100 Dumps EU Credit Gold/Platinum - $8500 (101 code) 1000 Dumps USA Credit Classic - $5000 1000 Dumps USA Credit Gold/Plat - $10000	

Crimeware as a Service – 2008/2009

Service	Description	Prices Encountered
Proxy Rental	Botnet networks on a “Per use” (on a monthly basis) or “daily rates” (on a daily basis, over a month) plans.	Daily Limit 50, Qty per Month 1500: $95 Per Use Plan, Qty per Month 1000: $69.95
Web Injection Shop	HTML injection codes designed to steal information from customers of dozens of financial institutions worldwide. Each HTML injection is specifically tailored to match each bank’s specific website design.	Each between $10 and $30
Spam facilities	Spamming tools, mailing lists, etc.	5000/7000 email per minutes, over 1 million emails per day: $2000 per month
Botnet management	HTTP Command & Control facilities for ZeuS malware.	$50 per month
Flooding/ DDoS	Complete paralysis of your competitor by flooding • his stationary or mobile phone • his web site • his Live Box	$80 per 24h ; 1 hour: $20 ; 1 day: $100 Large projects: $200 $20
Vulnerable Computers	If you have a malware, they have the vulnerable computers! They install for you your malware on them.	For 1000 computers: Asia: 12$ Europe: 40$ In the US: 140$ In GB: 220$ In IT: 150$ In DE: 170$ In PL: 150$ In BR: 150$ In CA: 200$ Others: ~250$
Bulletproof hosting	Guarantee of staying online, no matter what types of complaints (or how many) the ISP receives about that individual’s actions.	$650 per month

Crimeware as a Service – 2009

Crimeware (Seller or Author)	Description	Prices Encountered
CRUM Cryptor Polymorphic	Tool dedicated to encrypt malware like Zeus or Pinch3 before their spreading.	$100 (V2 - May 2009) $200 (V2.6) $300 (V3.3 – December 2009)
Zeus & Zeus Sploit-Pack	The ZeuS trojan is able to inject code into login webpage of financial organization to ask personal data and divert them to a remote location. In addition to listening in on the submission of forms in the browser, it can take screenshots of the victim's machine, or control it remotely, or add additional pages to a website and monitor it, or steal passwords that have been stored by popular programs.	Between $3000 and $6000 for a private version of a Zeus creator kit . We saw a complete version proposed at $14,000 (December 2009). $700 for Zeus Sploit-Pack (Jan 2009) Backdoored and old versions between $25 and $800.
Eleonore Exploit Pack	Exploit pack	$700 (V1.3.2 –December 2009) (or $1500 with no binding domain)
Unique Pack Sploits	Exploit pack	$600 (V2.1 –October 2009)

Spamming facilities – 2009/2010
Social Networks and E-mail

Social network accounts can be abused in a variety of ways. Creating accounts in forums, for example, helps in sponsoring or spamming. These accounts can be used to send spam, phishing links, links to fake products or services, or even malicious downloads. Prices for providing bogus accounts vary depending on the account quality. The most expensive accounts are usually verified (after a phone text or SMS acknowledgement).

Account Offers	Number of and Prices in US Dollars			
Yahoo	100 : $3 500 : $8	1000 : $15 5000 : 50$	10000 : 100$	
Gmail	Basic:	100 / 20$ 250 / 40$ 500 / 65$ 1000 / 120$	Verified:	100 / 30$ 250 / 75$ 500 / 115$ 1000 / 190$
Hotmail	Basic:	500 / 10$ 1000 / 15$ 5000 / 65$ 10000 / 120$	Verified:	500 / 15$ 1000 / 20$ 5000 / 80$ 10000 / 150$
Twitter MySpace	100 : $15 250 : $35	500 : 65$ 1000 : 100$		
HushMail AOL	500 : $10 1000 : $20	5000 : 90$ 10000 : 160$		

Spamming facilities – 2009/2010
Social Networks and E-mail

Social network accounts can be abused in a variety of ways. Creating accounts in forums, for example, helps in sponsoring or spamming. These accounts can be used to send spam, phishing links, links to fake products or services, or even malicious downloads. Prices for providing bogus accounts vary depending on the account quality. The most expensive accounts are usually verified (after a phone text or SMS acknowledgement).

Account Offers	Number of and Prices in US Dollars		
Facebook	Basic: 100 / 15$ 250 / 35$ 500 / 65$ 1000 / 120$	Multi Pictures: 100 / 22$ 250 / 55$ 500 / 100$ 1000 / 190$	Verified: 20 / 40$ 50 / 100$ 100 / 200$ 250 / 500$
Youtube	Basic: 100 / 12$ 250 / 30$ 500 / 60$ 1000 / 120$	Verified: 100 / 45$ 250 / 100$ 500 / 190$ 1000 / 350$	

Services are also provided should users need to increase the size of their fan clubs or friends list:

Offers	Prices
Facebook likes/fans for a fan page	1000 worldwide fans: 50$
Youtube subscribers and ratings	100 subscribers and ratings: 7$ 200 subscribers and ratings: 16$ 300 subscribers and ratings: 23$ 500 subscribers and ratings: 38$

Crimeware as a Service – 2010

Exploit Toolkits	Description	Prices
Zombie Infection Kit (Q3-2010)	Russian kit containing at least 10 package exploits, of which 2 from 2010.	1000$
Phoenix v2.4 (Q3-2010)	The Phoenix Exploit's Kit (PEK) first appeared in 2007 and was regularly updated. Today, and among the about sixteen exploits, eight are from 2010.	2200$
Crimepack v3.1.3 (Q3-2010)	CrimePack first appeared in 2009. Among 14 exploits, 4 are from 2010:	400$ (V3.0)
Eleonore v1.6 and v1.6.2 (Q4-2010)	A new Eleonore version was proposed in 2010. Today, and among the about ten exploits, six are from 2010.	2000$
Bleeding Life v2 (Q4-2010)		New Buyers: $400.00 Previous v1 Buyers: $250.00
Blackhole v1.0.0 beta (Q4-2010)	New exploit kit developed in Russia with built-in Traffic Direct System, self-defensive module, and advanced statistics widgets	License Annual: $1,500 Half-year: $1,000 3 months: $700

Crimeware as a Service – 2010

Botnet (Command & Control Toolkits)	Description	Prices Encountered
Zeus	The Zeus production is stopped. A new product, a merger with SpyEye is now on the market.	Kit sold between 3000$ & 4000$ Must be accompanied by addons and plug-ins which prices vary from $500 to $10K
SpyEye V 1.2 (April 2010) V1.3.05beta (Jan 2011)	Created by Gribodemon, le V1.0 was put on the criminal market the very last December 2009 days. Serious Zeus outsider in 2010, it finally absorbed its competitor. The last V1.3.05b version is a SpyEye/Zeus merge.	Between 500$ & 1000$ (V1.2) Merged version around 4000$
Golod (alias Go-Load) (September 2010)	Botnet client application including an advanced cryptor. Each client can circumvent the Windows Vista User Account Control and the Windows Host Firewall.	$600 for a basic toolkit Built on a specific single domain, $1,500 for a builder.

Crimeware as a Service – 2010/2011

Name	Comments	Prices (all in US$)
DDoS service	Prices are falling. One year ago prices were generally $20 for one hour and between $100 and $200 for 24hours.	10 minutes for $1 1 hour for $10 2 hours for $15 5 hours for $25 1 day for $50
Install software	If you have a malware, they have the vulnerable computers! They install for you your malware on them. The price is for 1000 installs	Asia: 8$ Europe: 50$ Canada: 100$ Australia: 140$ USA: 160$
Spam service (in millions of emails)	Prices for these services are increasing. In 2007, the same business offered 32 million emails for $1,000.	1M: 100$ 8M: 500$ 3M: 200$ 16M: 900$ 5M: 300$ 32M: 1500$
Socks/Proxy service		1 day: 120$ 1 week: 500$ 2weeks: 950$ 1 month: 1500$

Carding – 2010/2011
Dumps – Prices per Countries

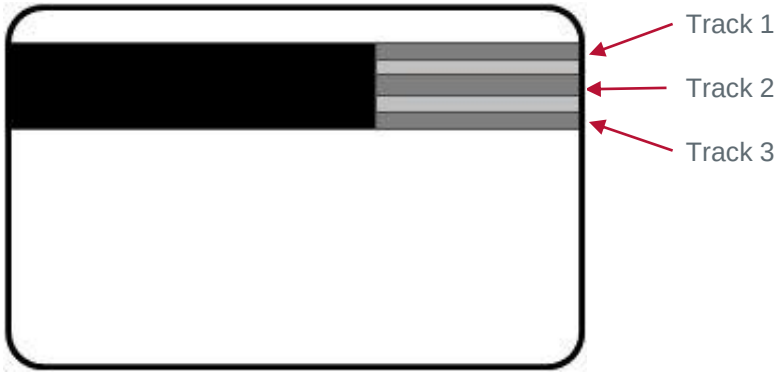
Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)											
	USA			EU			CA, AU			Asia		
Visa Classic	15$	80$		40$	150$		25$	150$		50$	150$	
Master Card Standard		90$			140$			150$			140$	
Visa Gold/Premier	25$	100$	200$	45$	160$	250$	30$	160$		55$	150$	
Visa Platinum	30$	110$		50$	170$		35$	170$		60$	170$	
Business/Corporate	40$	130$		60$	170$		45$	175$		70$	170$	
Purchasing/Signature	50$	120$		70$			55$			80$		
Infinite				130$	190$		60$	200$			190$	
Master Card World		140$										
AMEX	40$			60$			45$			70$		
AMEX Gold	70$			90$			75$			100$		
AMEX Platinum	50$											

"Dump" refers to information electronically copied from the magnetic stripe on the back of credit and debit cards. It references the two tracks of data (Track 1 and Track 2) on the magnetic stripe. Track 1 is alpha-numeric and contains the customer's name and account number. Track 2 is numeric and contains the account number, expiration date, the secure code (known as the CVV), and discretionary institution data. Track 3 is almost never used.

For a same country, prices increase depending on the supply, or not, of the associated PIN, as well as a guarantee of a "good balance.

Carding – 2010/2011
Dumps – Prices per Types

Track	Prices Encountered
Track1 only without PIN	25$
Track1 only without PIN	60$
Track1+ Track2 without PIN	70$
Track1+ Track2 without PIN and good balance	USA: 150$ Europe: 200$
Track1+ Track2 with PIN	120$ - 140$
Track1+ Track2 with PIN and good balance	USA: 200$ Europe: 250$



Carding – 2010/2011
CC with CVV, CC with Fullz info

Credit Card Number with CVV2	Estimate of Prices (Min – Max)									
	USA		EU		CA, AU		ASIA		Middle East	
Random	2$	5$	5$	25$	8$	10$	15$		30$	
With BIN	4$	15$	30$							
With DOB	15$	20$	35$	40$	20$	40$			60$	
With fullz info	10$	60$	12$	80$	50$					
With COB	140$	200$								

"CVV" is the acronym used in the credit card (CC) industry to refer to "Card Verification Value." CVV1 is a unique three-digit value encoded on the magnetic stripe of the card. CVV2 is the three-digit value that is printed on the back of all payment cards.

"random" means auto generated (via software)
"with BIN" means the first six digits refers to an existing bank. If just "random", the CC number, its CVV2 and expiration date can be valid regarding the algorithm, but without bank connection.
"with DOB" means date of birth of the CC owner is provided.
"with fullz info" means the seller supplies all of the details about the bank cart and its owner (ex: Full Name , Billing Address - CC# - Exp Date - (PIN - SSN - MMN - DOB - CVV2).
"with COB" means the carder provides, in addition to "full info", a login and a password for online access allowing the buyer to change the shipping/billing address or to add a new one.

Carding – 2010/2011
CC with CVV, random

If u buy UK, EU, CA, AU cvv (over 10cc/time) and US cvv (DOB+SSN+MMN) please contact me via Email or ICQ.

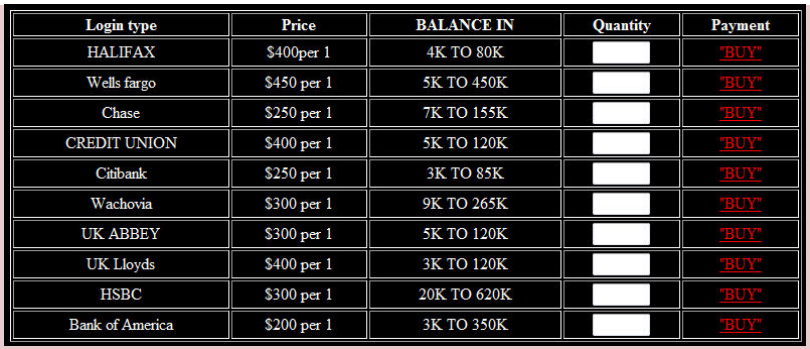
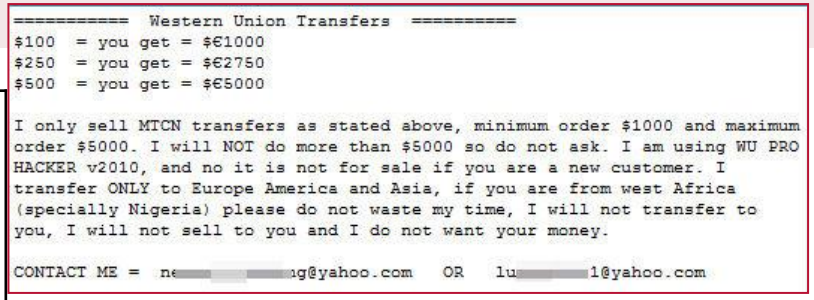
REMEMBER TO PAY THE RIGHT AMOUNT TO GET YOUR PASS CODE TO GET YOUR CC INSTANT

NEW FRESH RANDOM USA UK EU AU CVV

Card type	Price	In stock	Quantity	Payment
Paypal USA	$40per 1	1153		Buy
US Visa Card	$3 per 1	12.000		Buy
US Master Card	$3 per 1	5200		Buy
US Amex Card	$5 per 1	798		Buy
US Discover Card	$5 per 1	420		Buy
CANADA Randon Card(VISA/MC)	$10 per 1	1020		Buy
UK Randon Card(VISA/MC)	$5 per 1	13790		Buy
EU Randon Card(VISA/MC/AMEX)	$15 per 1	7799		Buy
AU Randon Card(VISA/MC)	$10 per 1	7139		Buy

Randon CC format: # Card Number CVV Expire Holders Name Sex State City Zip Address Country Phone Email Card System Card Payment Method Card Type Bank Name Bank Phone Additional Info Check NON VBV

Carding – 2010/2011
Logins, Online Payment Hacking

Login	Prices Encountered	Examples
USA bank with fullz info	2% of balance (55$ - 1000$)	
EU banks with fullz	4-6% of balance (50$ - 1500$)	
Paypal, Moneybookers, Netteler verified	6-20% of balance	
Western Union Transfers (via WU PRO HACKER v2010)	10% from amount	

Login type	Price	BALANCE IN	Quantity	Payment
HALIFAX	$400per 1	4K TO 80K		"BUY"
Wells fargo	$450 per 1	5K TO 450K		"BUY"
Chase	$250 per 1	7K TO 155K		"BUY"
CREDIT UNION	$400 per 1	5K TO 120K		"BUY"
Citibank	$250 per 1	3K TO 85K		"BUY"
Wachovia	$300 per 1	9K TO 265K		"BUY"
UK ABBEY	$300 per 1	5K TO 120K		"BUY"
UK Lloyds	$400 per 1	3K TO 120K		"BUY"
HSBC	$300 per 1	20K TO 620K		"BUY"
Bank of America	$200 per 1	3K TO 350K		"BUY"

Sell paypal UK 1310£ balance with price :100$ Liberty Reserve

PAYPAL GERMANY

Sell paypal GER 3,900€ balance with price :172$ Liberty Reserve

Sell paypal GER 8,000€ balance with price :960$ Liberty Reserve

Sell paypal GER 9,500€ balance with price :998$ Liberty Reserve

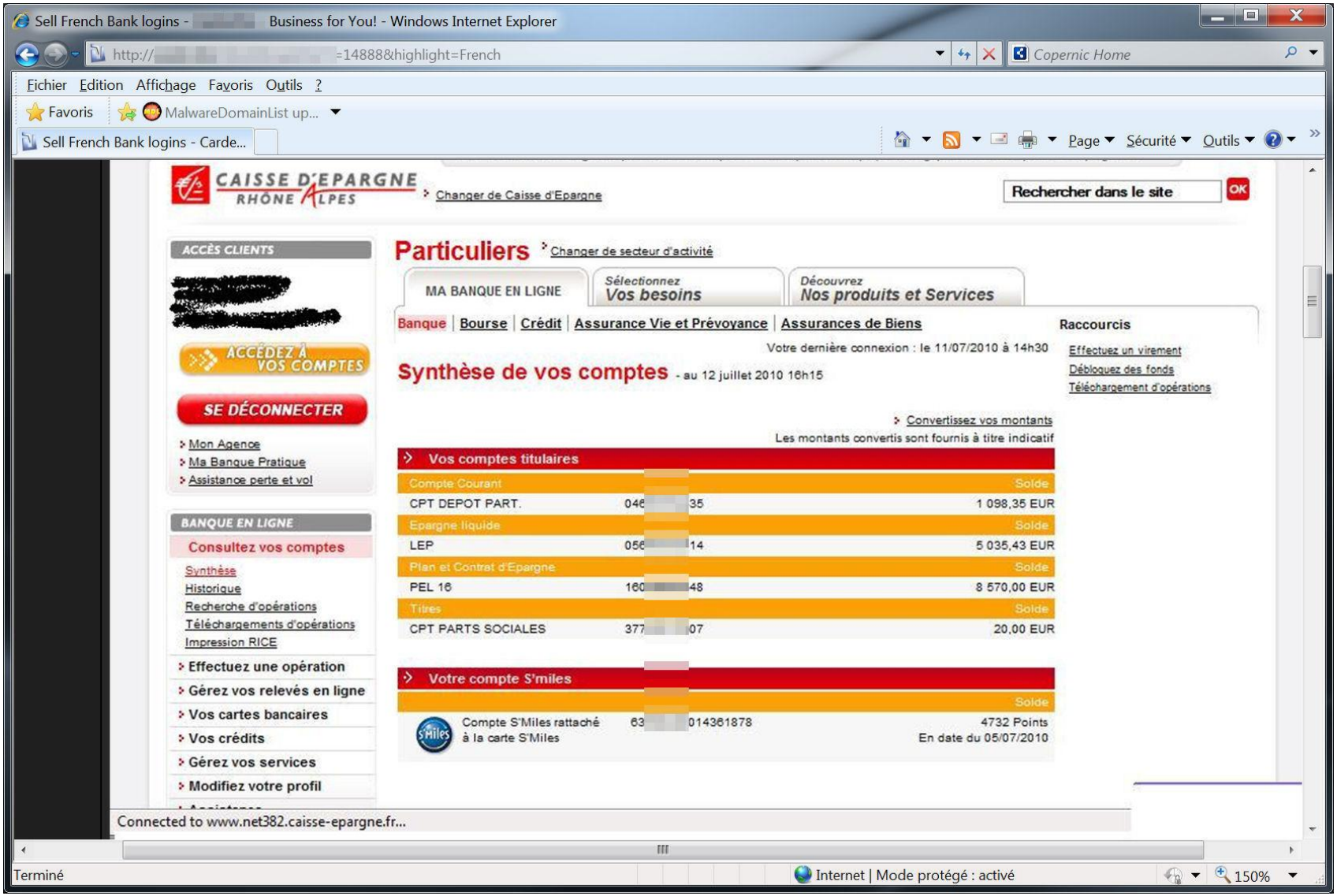
Sell paypal GER 11,780€ balance with price :1018$ Liberty Reserve (bonus : 18 cvv UK)

```
==========  Western Union Transfers  ==========
$100  = you get = $€1000
$250  = you get = $€2750
$500  = you get = $€5000

I only sell MTCN transfers as stated above, minimum order $1000 and maximum
order $5000. I will NOT do more than $5000 so do not ask. I am using WU PRO
HACKER v2010, and no it is not for sale if you are a new customer. I
transfer ONLY to Europe America and Asia, if you are from west Africa
(specially Nigeria) please do not waste my time, I will not transfer to
you, I will not sell to you and I do not want your money.

CONTACT ME =  ne[redacted]g@yahoo.com   OR   lu[redacted]1@yahoo.com
```

Phishing is the most and well-known way to obtain login credentials.
But, to access Paypal, Western Union (WU) or Liberty Reserve databases and terminals, cybercriminals use most confidential tools like **WU PRO HACKER** (see next slide).

"with fullz info" means the seller supplies all of the details about the bank cart and its owner
MTCN = Money Transfer Control Number (Western Union)

Carding – 2010/2011
Logins, Online Payment Hacking



Carding – 2009/2010
Logins, Online Payment Hacking

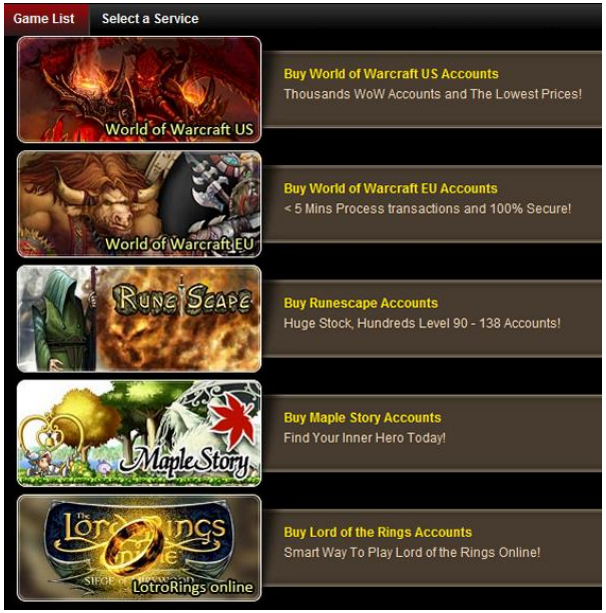
HACKING TOOLS (March – July 2010)	Prices
Apache for E-Gold	150$
Devohack-lr v.7.2 for Liberty Reserve	470$
Libhack-2 for Liberty Reserve	440$
GoldTresor A-4.2 for E-Gold	380$
Liberty Exploit v 1.8 for Liberty Reserve	270$
LR-Crack – 9.0 for Liberty Reserve	250$
PayPal Database Hacker 1.5	150$
Spawn 2.1 for E-Gold	200$
Vampire 3.6 for Liberty Reserve	480$
Western Union Admin Terminal Software	280$
Western Union Buster 2009	250$
Western Union Database Hacker	350$
Western Union Pro Hacker	120$
XPP 3.9 Paypal Hackware	350$
XT-LibertyReserveHack-91	490$

Real tools or fake offers to lure criminal's apprentice ?

To access Paypal, Western Union (WU) or Liberty Reserve databases and terminals, cybercriminals use most confidential tools like WU PRO HACKER.

Carding – 2009/2010
Social Networks and MMORPG

Login	Prices Encountered
One Facebook account with 1000 friends	5$ - 25$
One Facebook account with 500 “profiled” friends	30$
World of Warcraft account with high score	120$ - 200$
Runescape account with high score	40$ - 1200$



500 Facebook Fans - Start NOW!

Budget: $30 - 250 Posted: 21 hours ago Type: Facebook Internet Marketing Leads Social Networking

Email & Mobile Marketing Made Easy! TRY IT FREE emailbrain SMART EMAIL MARKETING
www.EmailBrain.com Ads by Google

**********PLEASE NO BIDS OVER $30! THANK YOU!**********

I need you to get me 500 Facebook fans from Singapore.
Fans MUST be from Singapore ONLY, with the following character;

1. Between 25 and 52 years old.
2. 50% Women and 50% men
3 All profiles should have at least 2 pictures in his/her profile
4. We want profiles at least 6 months OLD.
5. Each profile should have at least 5 friends.

Must be done in a way to prevent Facebook bans.

**********PLEASE NO BIDS OVER $30! THANK YOU!**********

.Payment & Requirements:

* WE WILL NOT MAKE ANY PAYMENT IF THE PAGE IS SUSPENDED WITHIN 10 DAYS OF DELIVERY.
* You will be paid 10 days after project delivery
* Any fans that are suspended in that time period must be replaced or will not be paid for.
* You must not acquire these fans in a way that will get the page banned or suspended.

Please Include When Bidding:

* Price of bid
* Accurate date of completion
* URLS with examples of previous Singapore Facebook fan page work & explanation of how fans will be acquired (general information)

ONLY SERIOUS BIDS PLEASE!
The project has the possibility to expand to our other fan pages

Thank You!

McAfee
An Intel Company
Protegiendonos contra HaaS
Lo que toma para hacernos sentir SEGUROS
SAFE NEVER SLEEPS™

Que toma para ASEGURAR una organización

LO QUE DEMOS SABER…

- Con **Quien** estoy tratando
- Cual es su **Proposito**
- Que **Datos** esta Accesando
- Evaluar el **Riesgo**
- **Monitoreo** Continuo
- Aprendizaje e **Inteligencia**

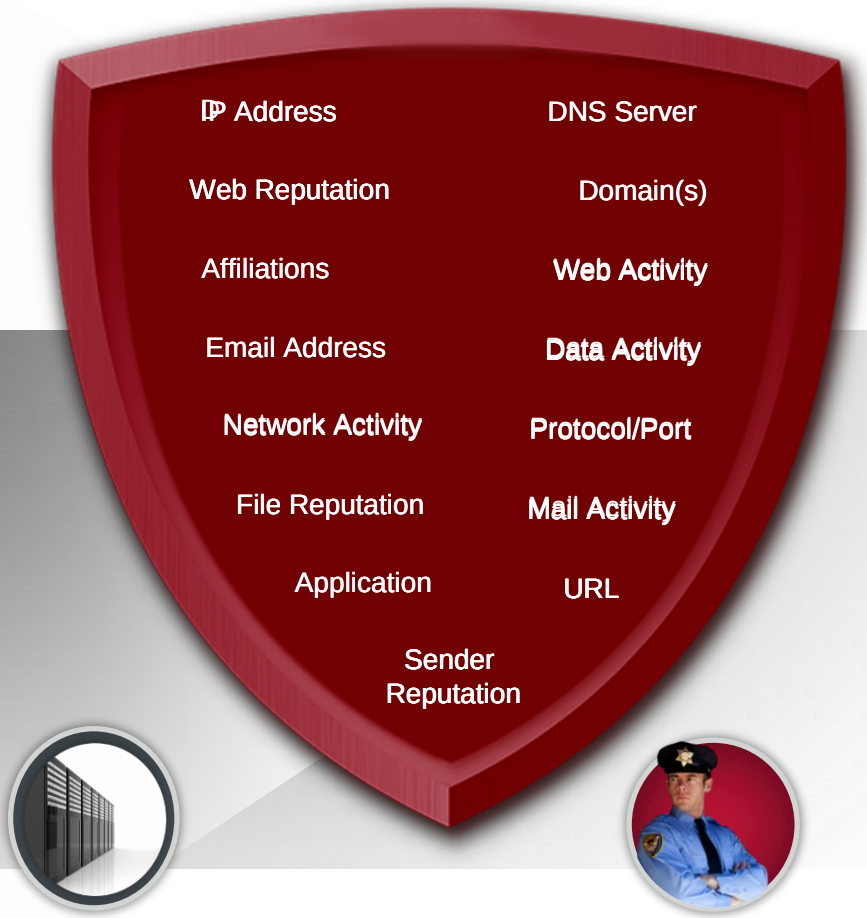
Datacenter

Que toma para ASEGURAR una organización

LO QUE DEMOS SABER…

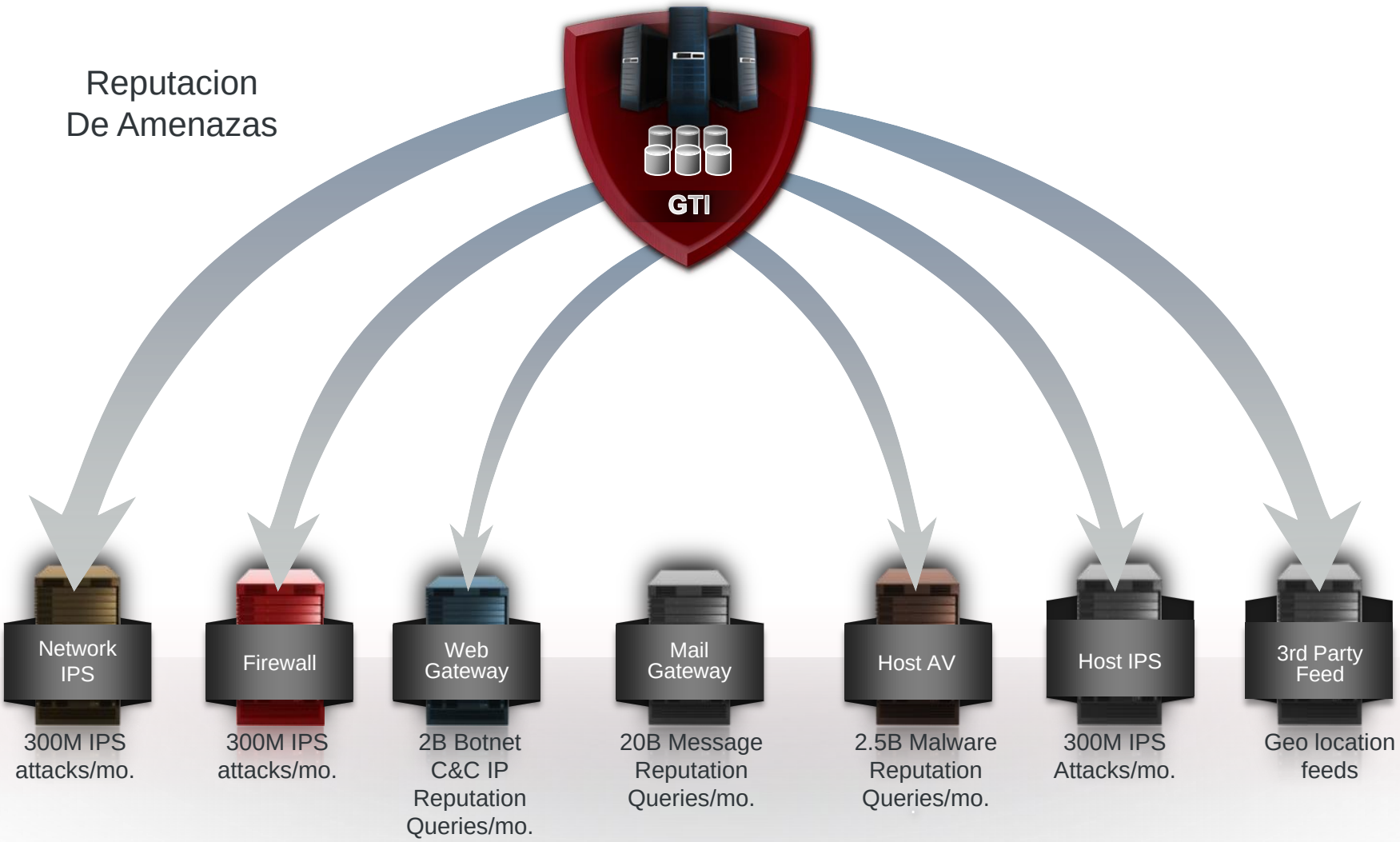
- Con **Quien** estoy tratando
- Cual es su **Propositourpose**
- Que **Datos** esta Accesando
- Evaluar el **Riesgo**
- **Monitoreo** Continuo
- Aprendizaje e **Inteligencia**

LO QUE DEBEMOS EVALUAR…



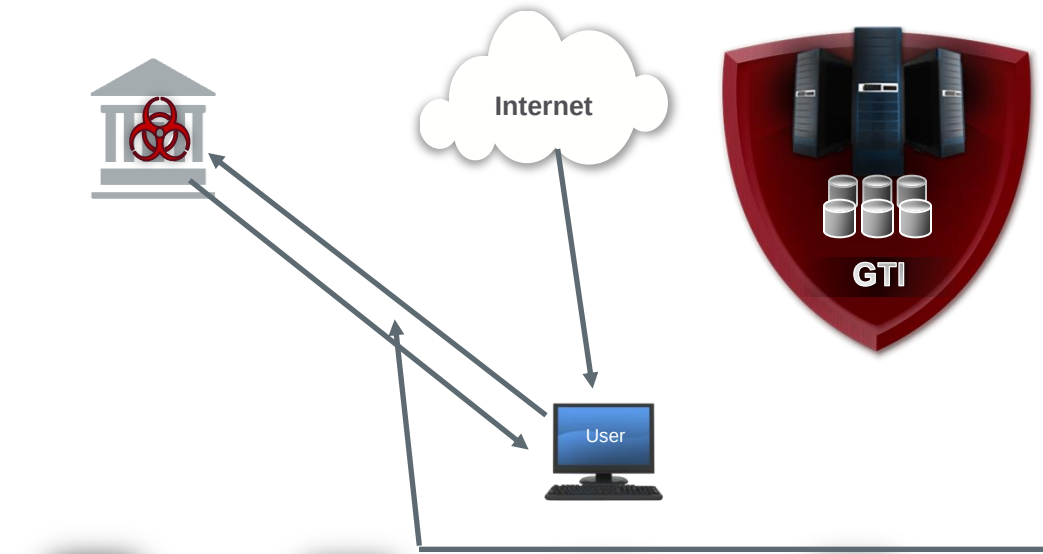
Datacenter

Que toma para ASEGURAR una organizacion
Global Threat Intelligence



Lo que aprendemos de un mensaje SPAM

Global Threat Intelligence



Origen del SPAM?

Links & Codigo Malicioso?

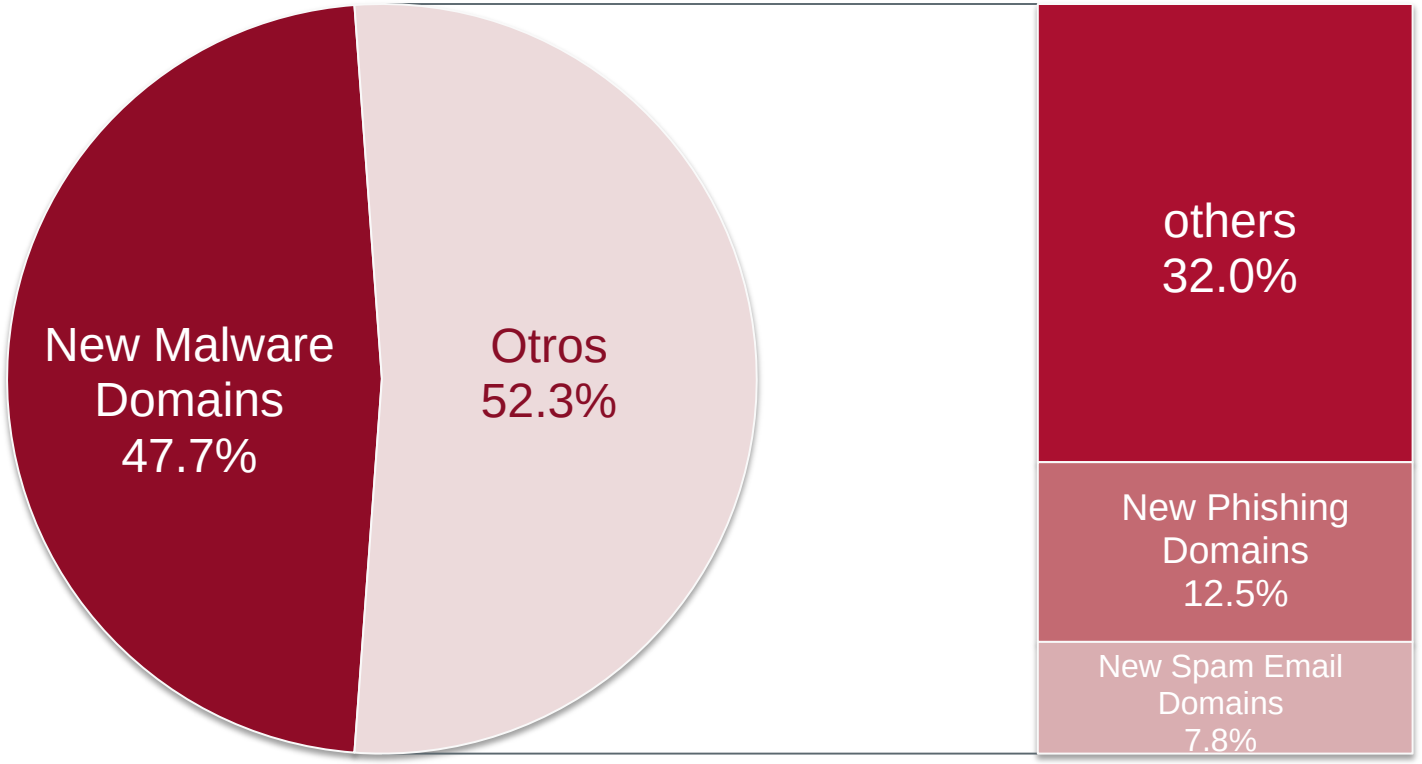
GTI Comparte con el Portafolio

Host IPS Bloquea el Codido

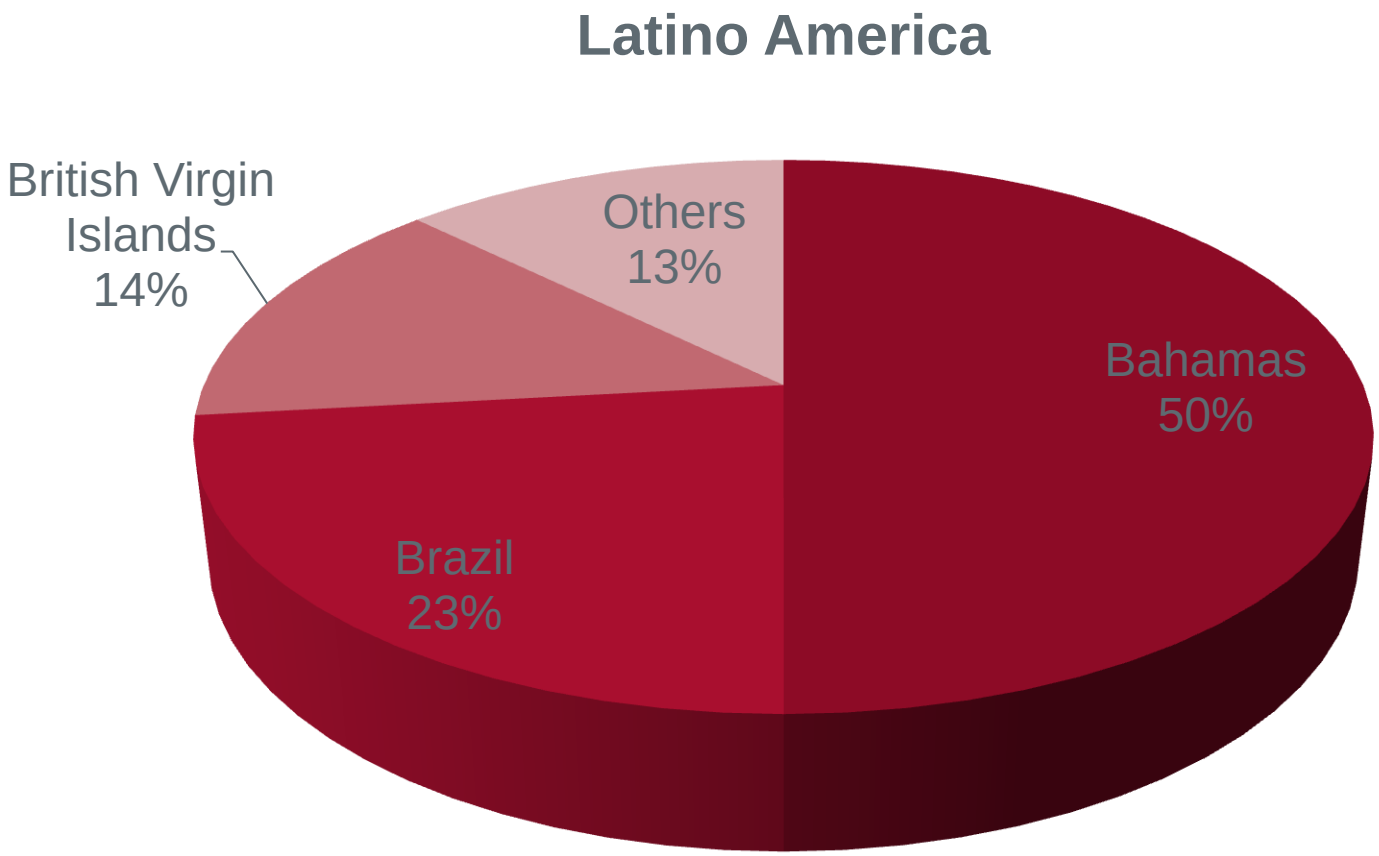
Network IPS	Firewall	Web Gateway	Mail Gateway	Host AV	Host IPS	3rd Party Feed
Dominio Direccion IP Afiliaciones	Dominio Direccion IP	Dominio Direccion IP Localizacion GEO Afiliaciones Links Peligrosos Codigo Malicios	Dominio Direccion IP Localizacion GEO Afiliaciones	Codigo Malicioso	Dominio Direccion IP Localizacion GEO Afiliaciones	Localizacion GEO

Nuevos Dominios Sospechosos

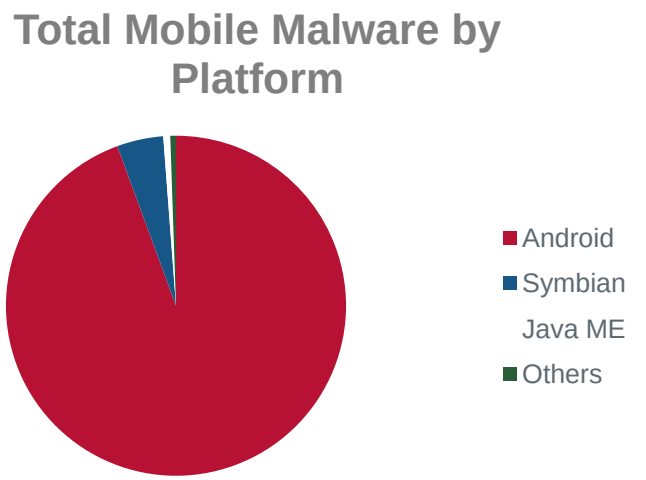
Dominios Sospechoso Nuevos

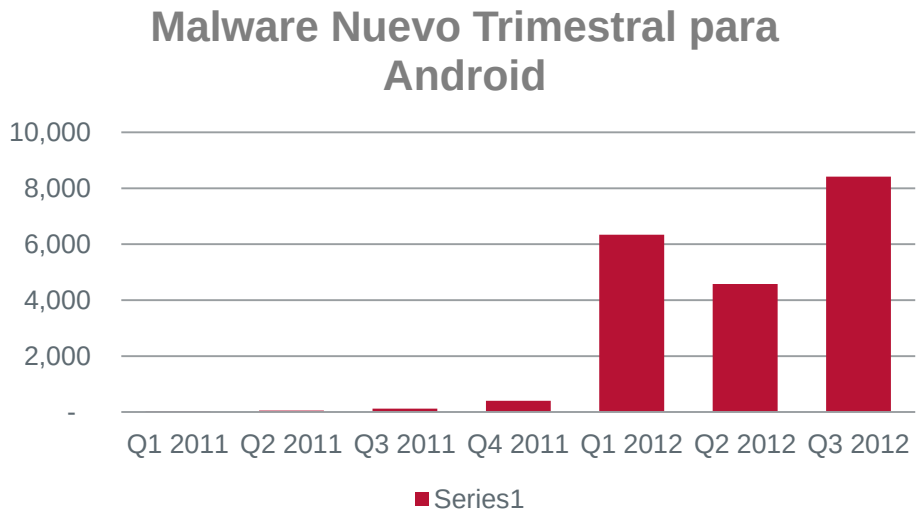


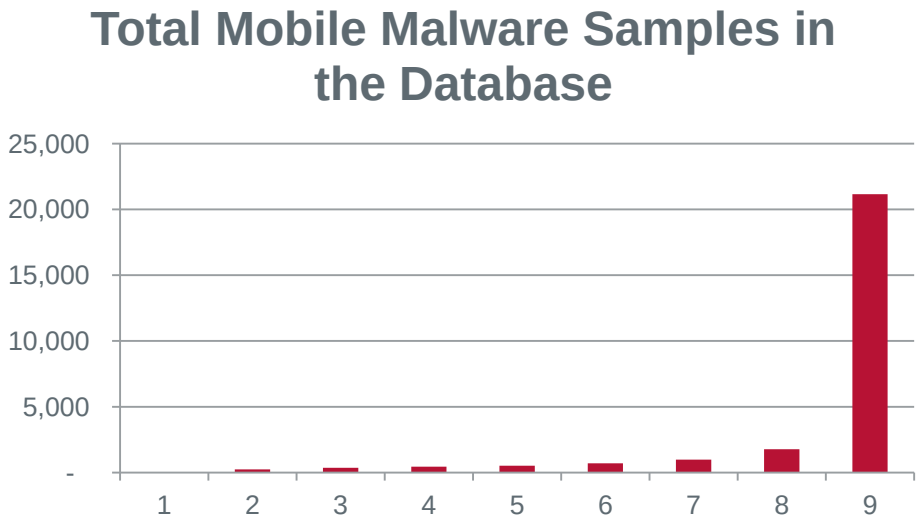
Países con mayor numero de dominios maliciosos



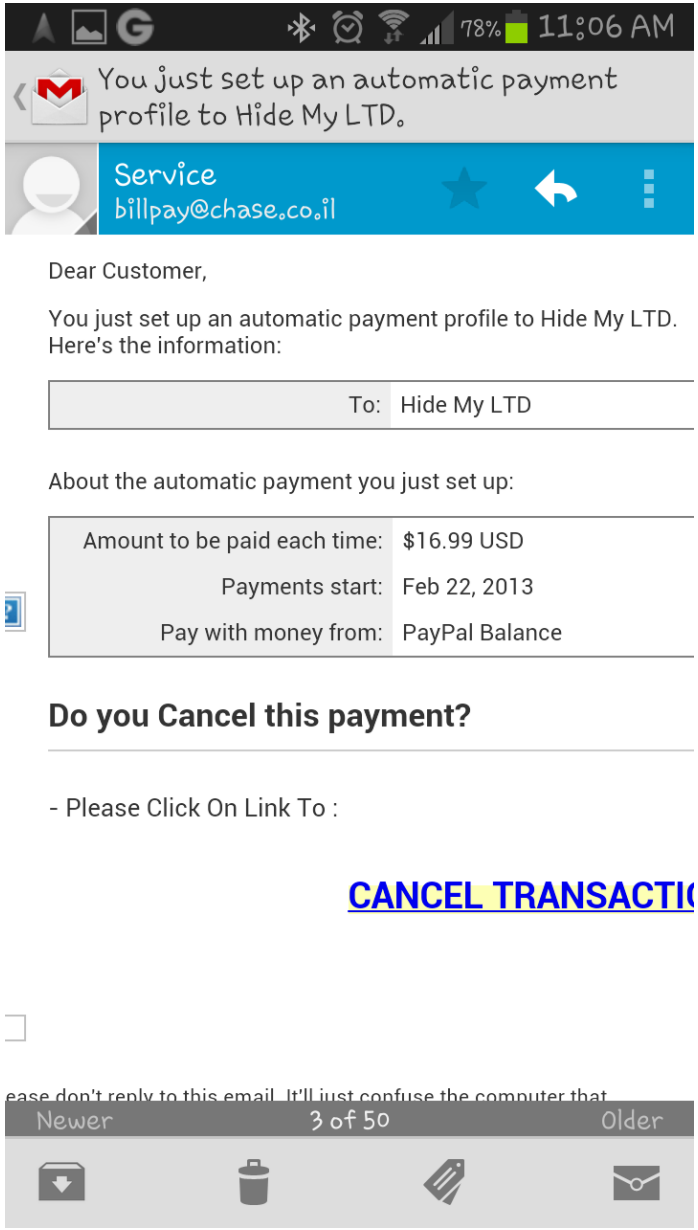
Malware en Plataformas Móviles

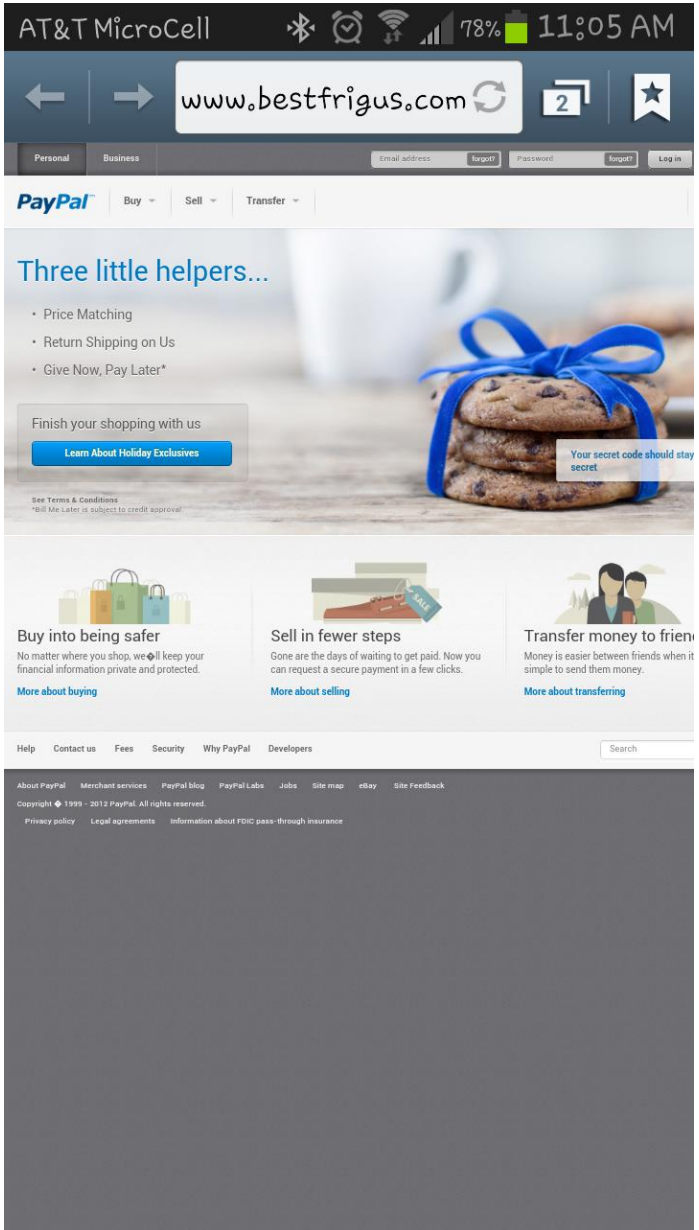






Fresquecito, para esta presentacion…





Gracias!!!

- Preguntas??

- Contacto:

Carlos G Gonzalez
Senior Director – Sales Engineer LTAM
Email: cgonzalez@mcafee.com
Twitter: cgtwitts72
Linkedin: www.linkedin.com/pub/carlos-g-gonzalez/1/a17/217/

McAfee®