FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Que hay de nuevo en Seguridad de Información

y que podemos hacer para prevenir los riesgos en la industria bancaria

Ing. Giovanni Bautista Pichling Zolezzi
gpichling@asbanc.com.pe
www.giovannipichling.blogspot.com

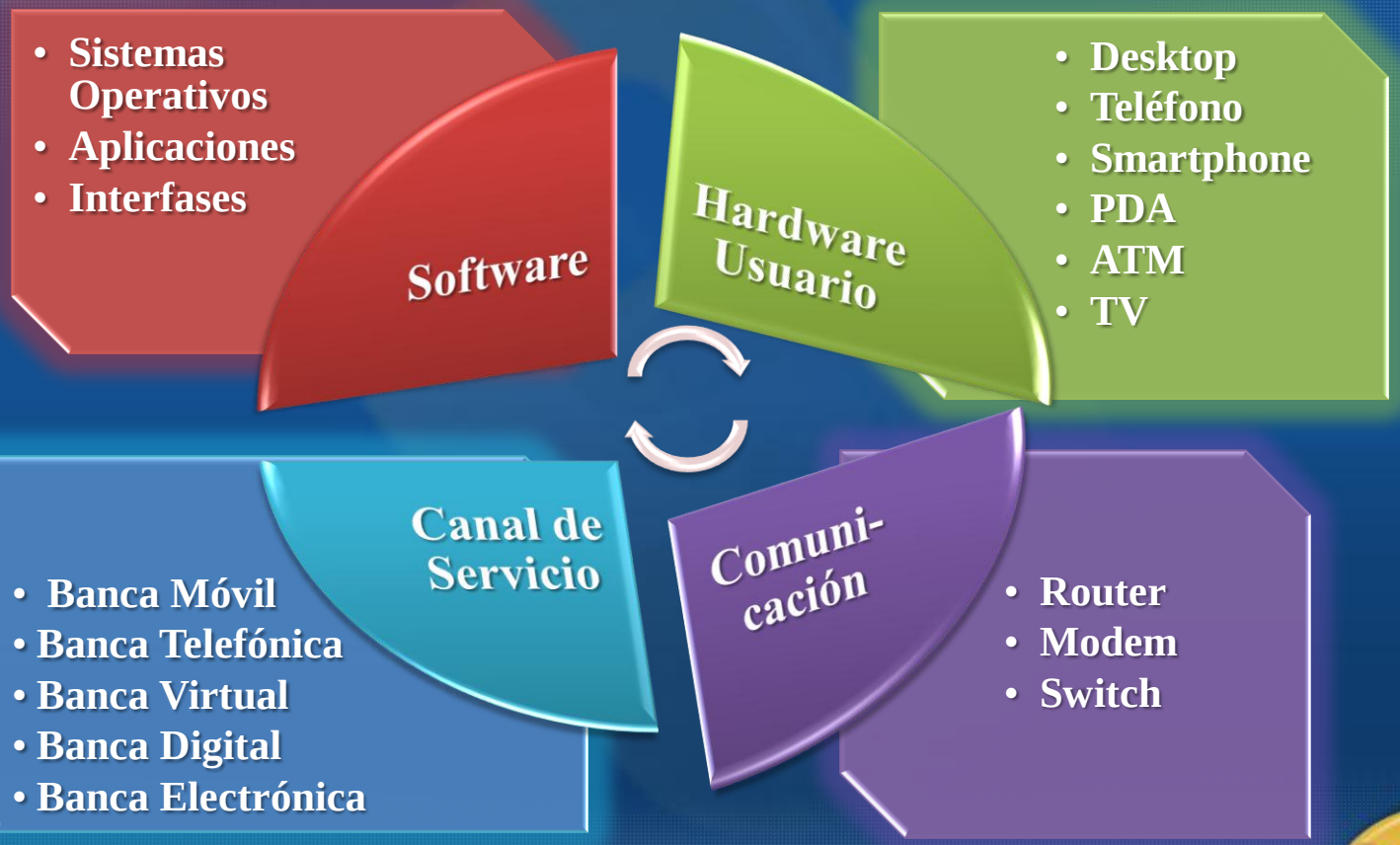
Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Principios que sustentan el Negocio Bancario

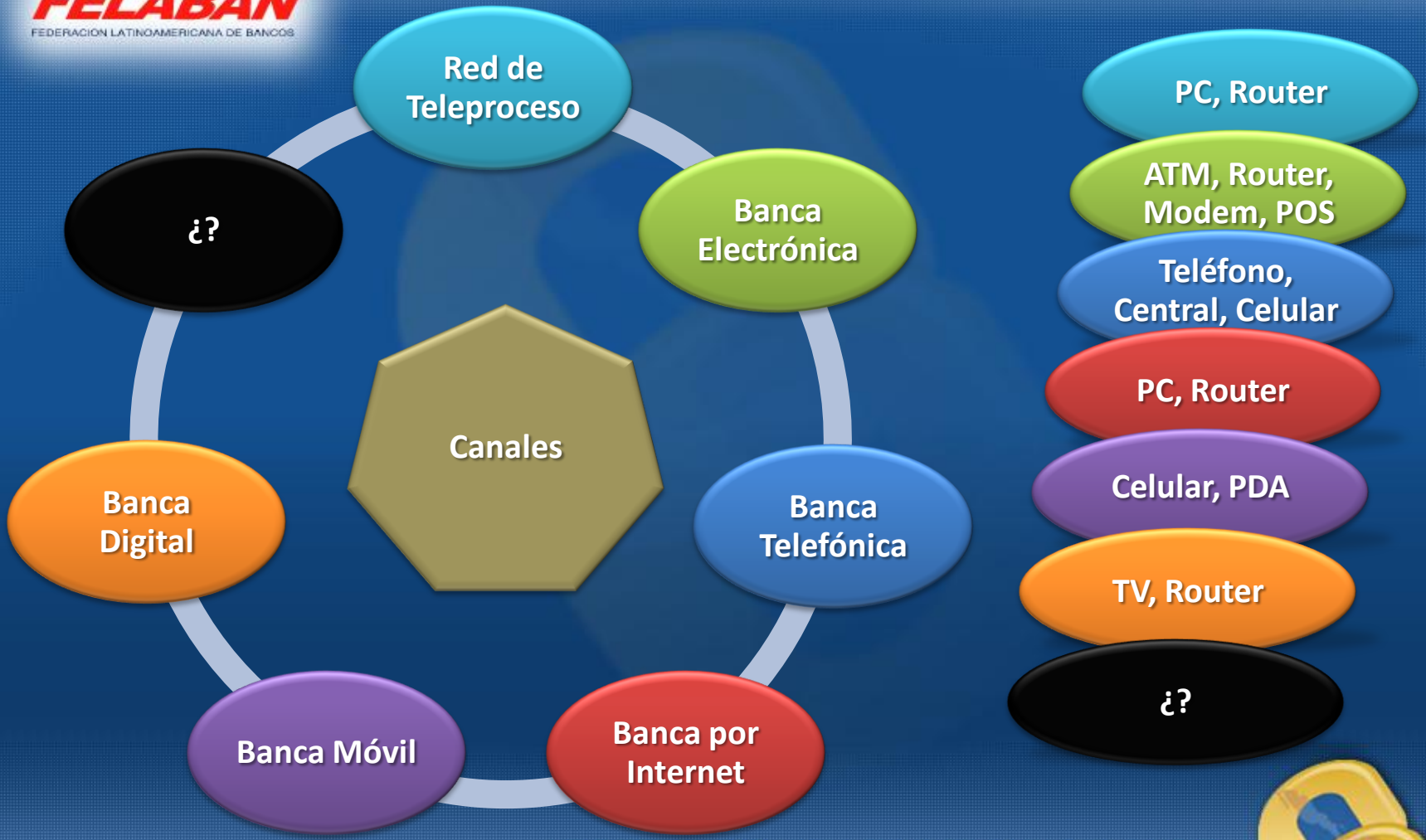
Confianza y Seguridad

Información, el activo más importante

Elementos que Facilitan el acceso a la Información



Tecnología asociada



Estrategia para contrarrestar los Delitos Informáticos

Organizaciones Delincuenciales

Estadísticas

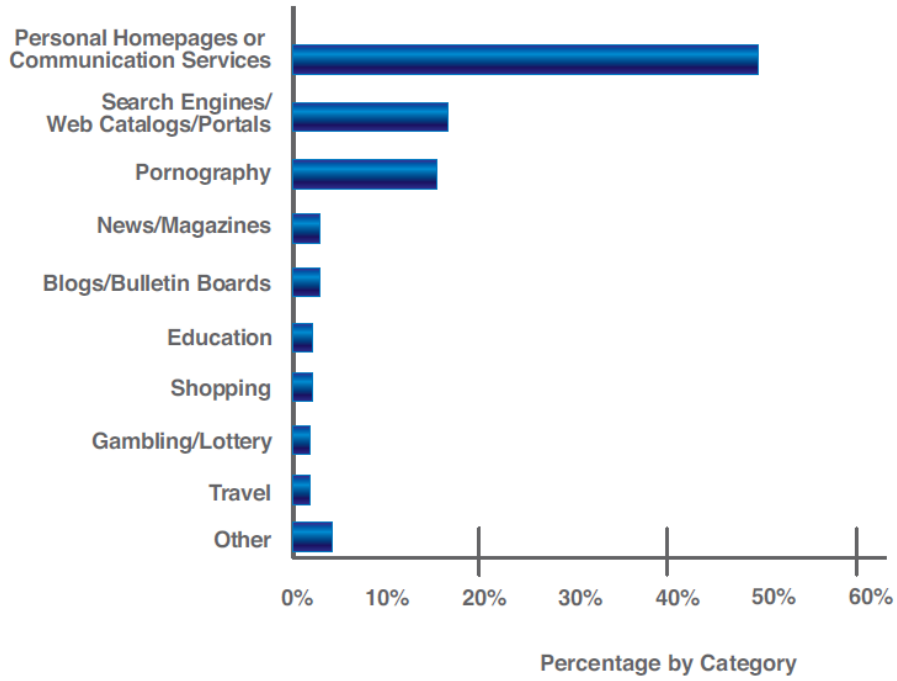


Figure 27: *Top Web Sites Containing at Least One Malicious Link*

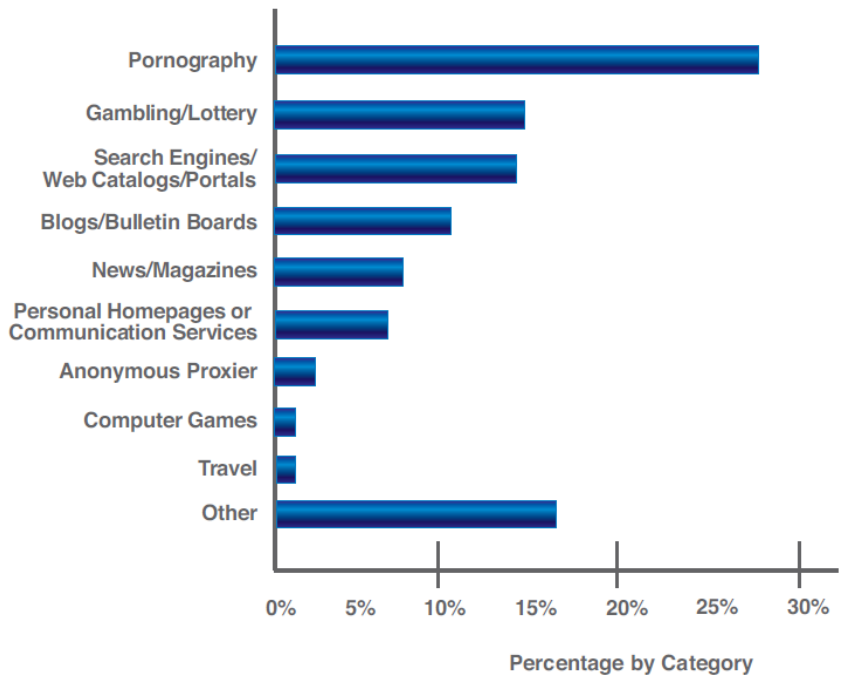


Figure 28: *Top Web Sites Containing Ten or More Malicious Links*

Estadísticas

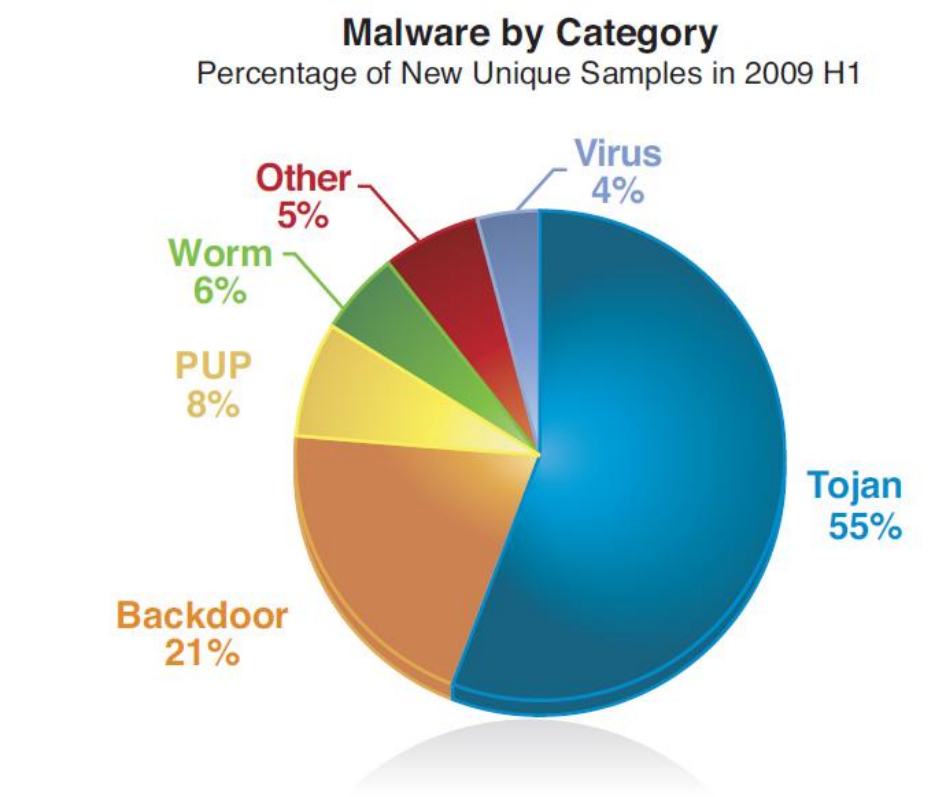


Figure 29: Malware by Category, 2009 H1

Estadísticas

The figure below shows the geographical distribution of malware phone home locations from the samples we collected for the first half of 2009:

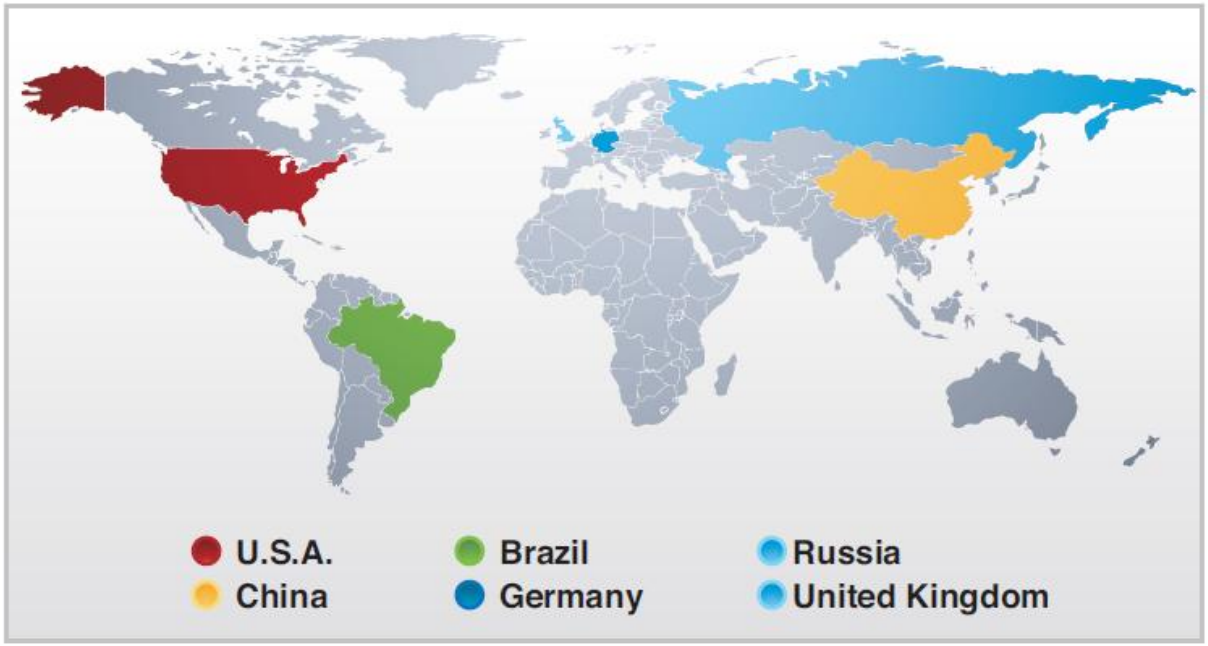


Figure 39: *Phone Home Locations Geographical Distribution (Unique IPs), 2009 H1*

Figure 53: *Geographical Distribution of Spam Senders, 2009 H1*

Estadísticas

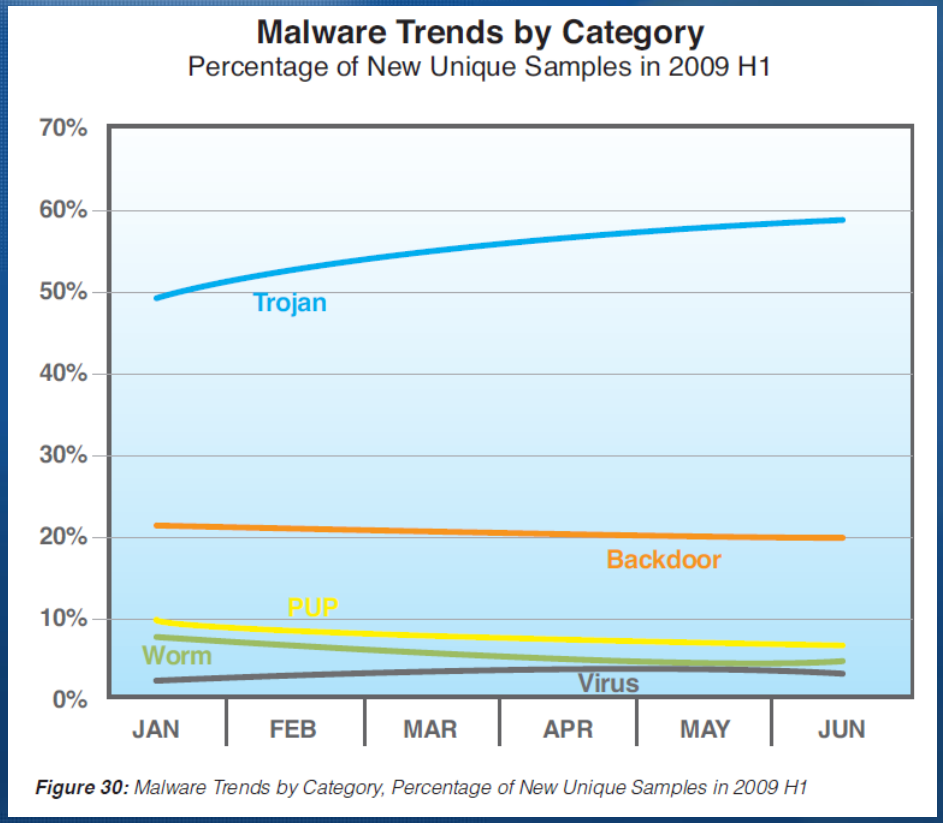


Figure 30: *Malware Trends by Category, Percentage of New Unique Samples in 2009 H1*

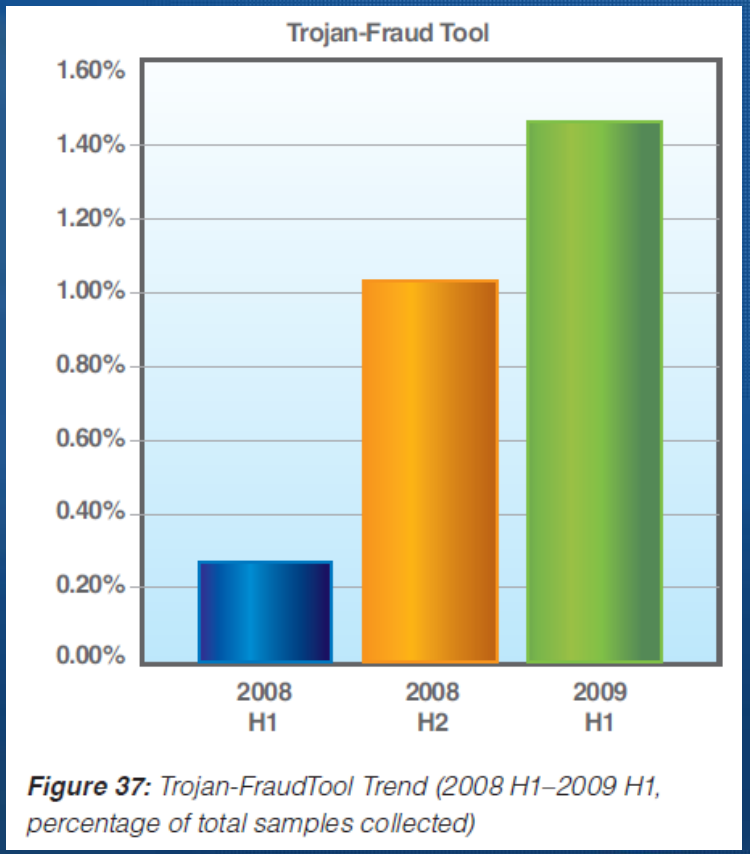


Figure 37: *Trojan-FraudTool Trend (2008 H1–2009 H1, percentage of total samples collected)*

Estadísticas

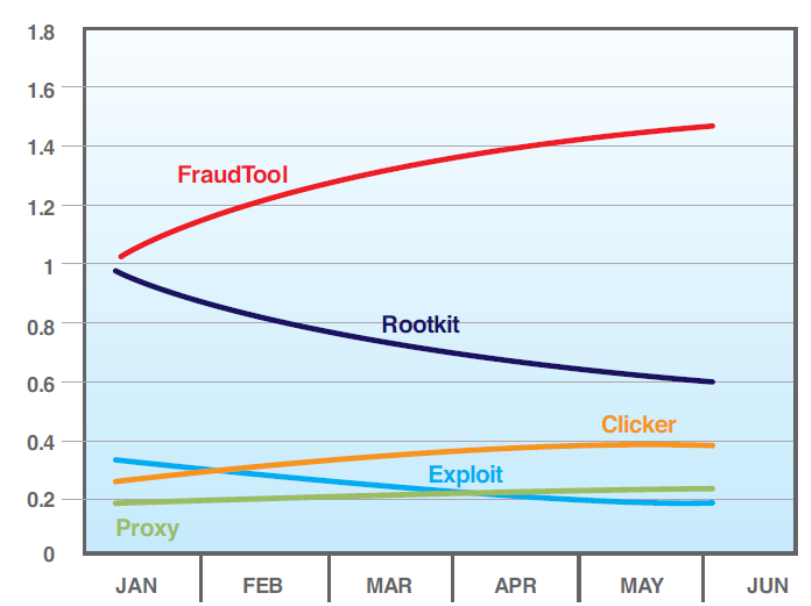


Figure 35: *Trojan Trends, Granular Detail for Other Category, 2009 H1*

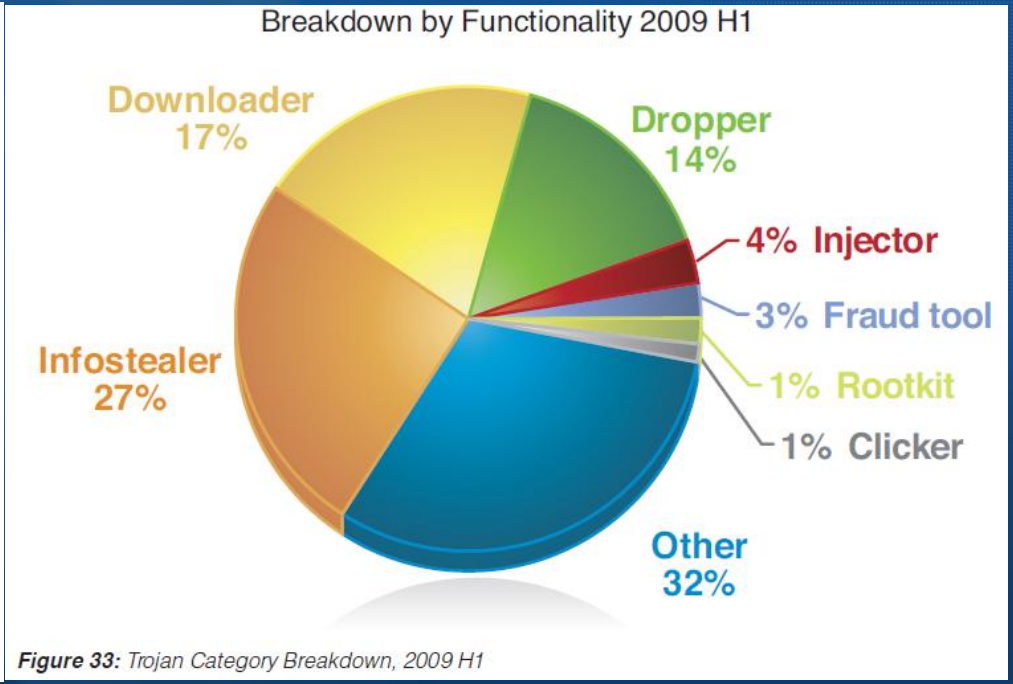


Figure 33: *Trojan Category Breakdown, 2009 H1*

Estadísticas

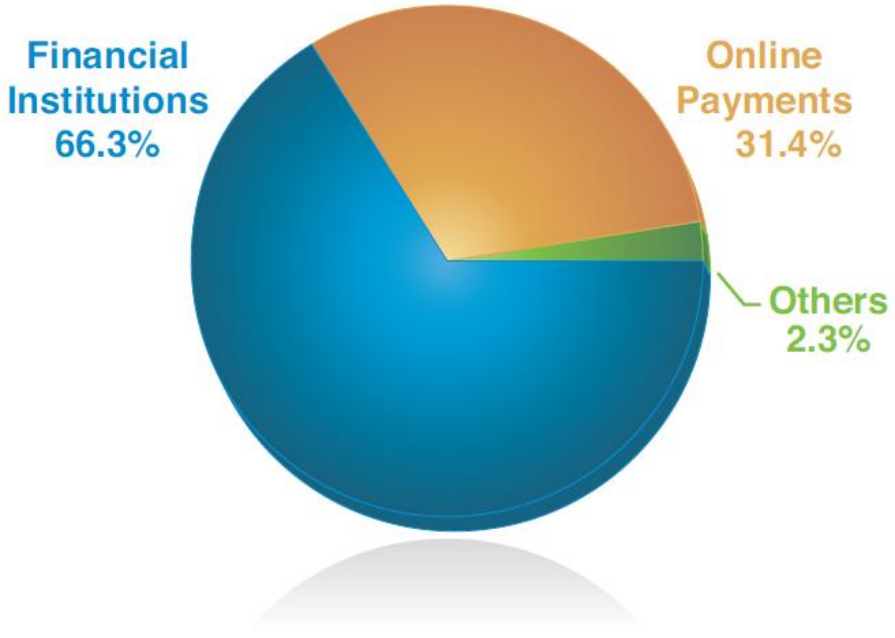


Figure 60: *Phishing Targets by Industry, 2009 H1*

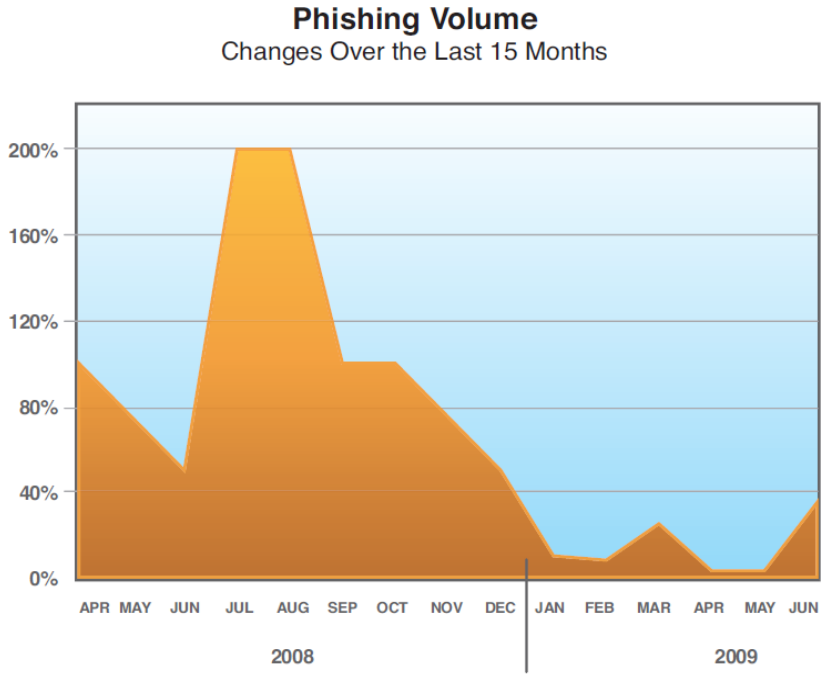


Figure 57: *Phishing Volume, Apr 2008-Jun 2009*

Estadísticas

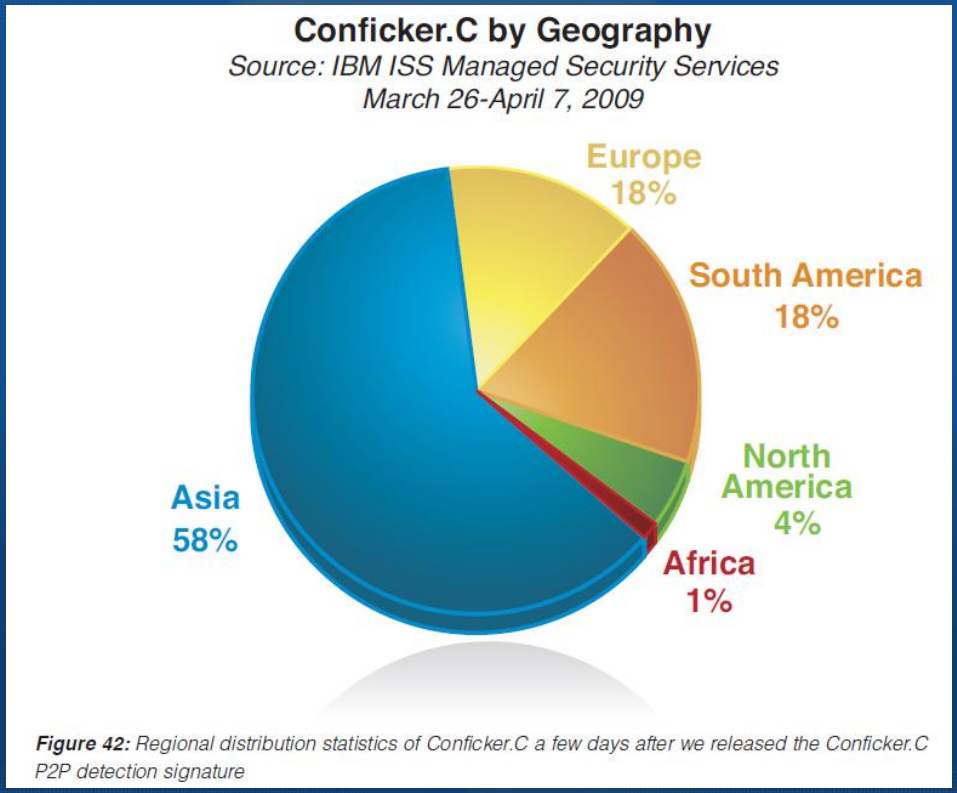
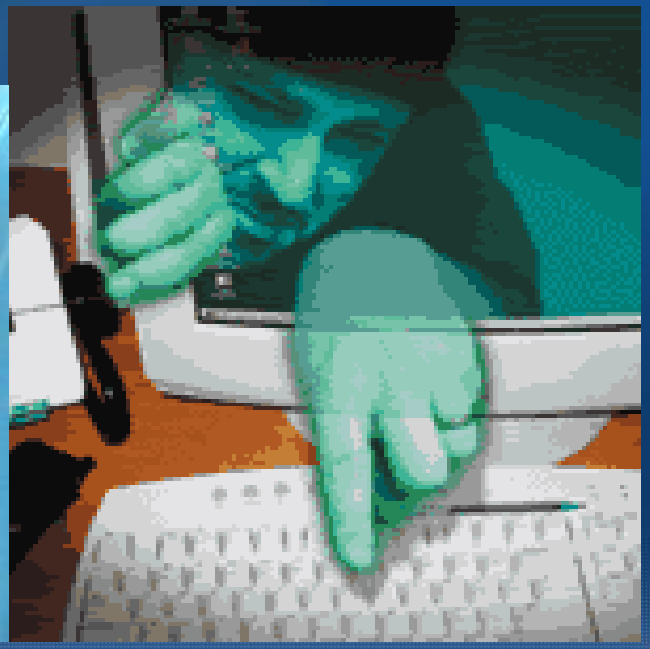


Figure 42: *Regional distribution statistics of Conficker.C a few days after we released the Conficker.C P2P detection signature*

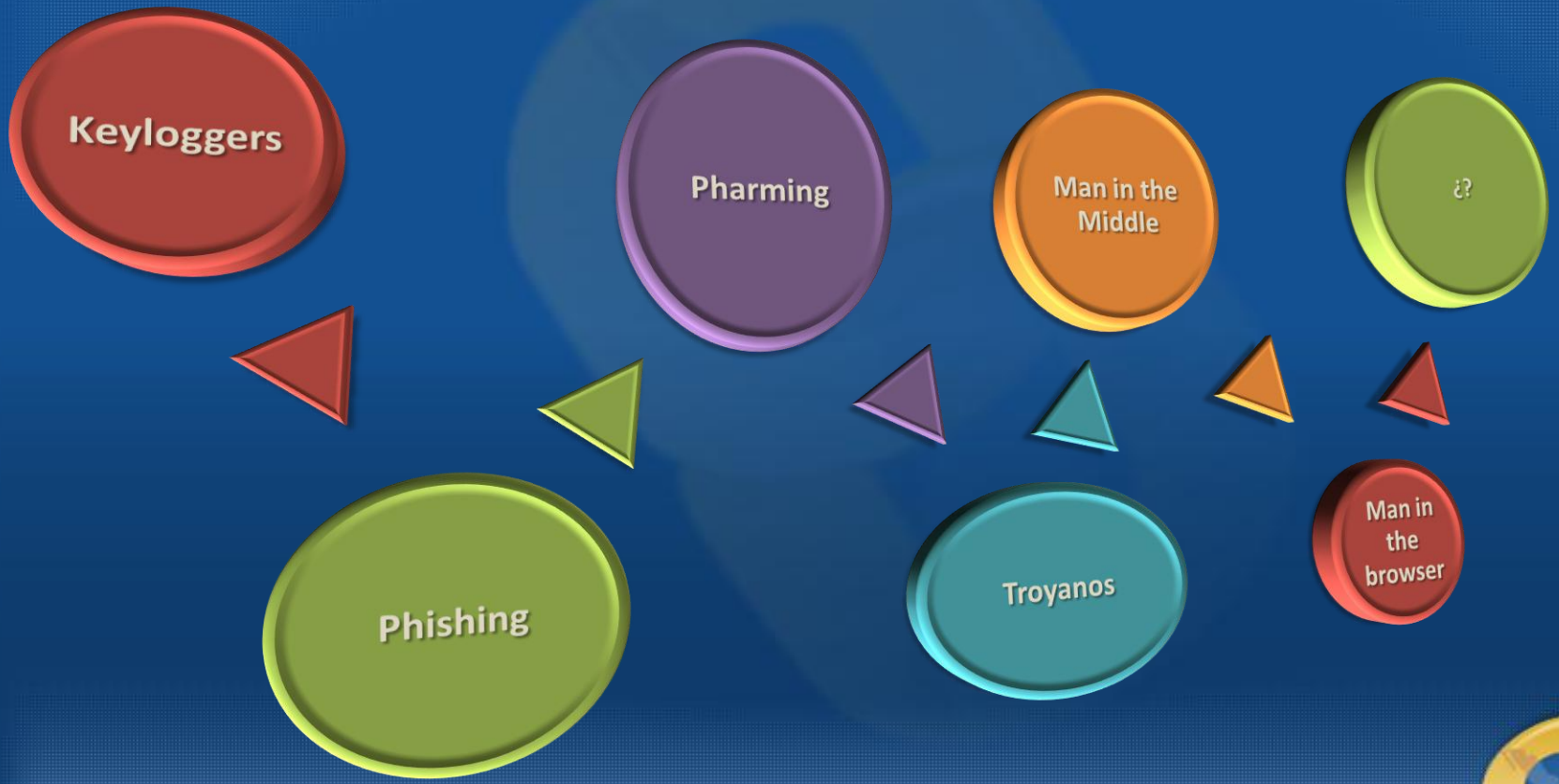
Características del Delincuente Infomático

Ingeniería Social

Técnica usada por la delincuencia para engañar a las personas, ofrecen beneficios económicos, premios, oportunidades únicas de negocio, necesidad de actualizar sus datos o amenazas, con la finalidad de conseguir información personal que le permita suplantar a la víctima y obtener beneficios económicos.

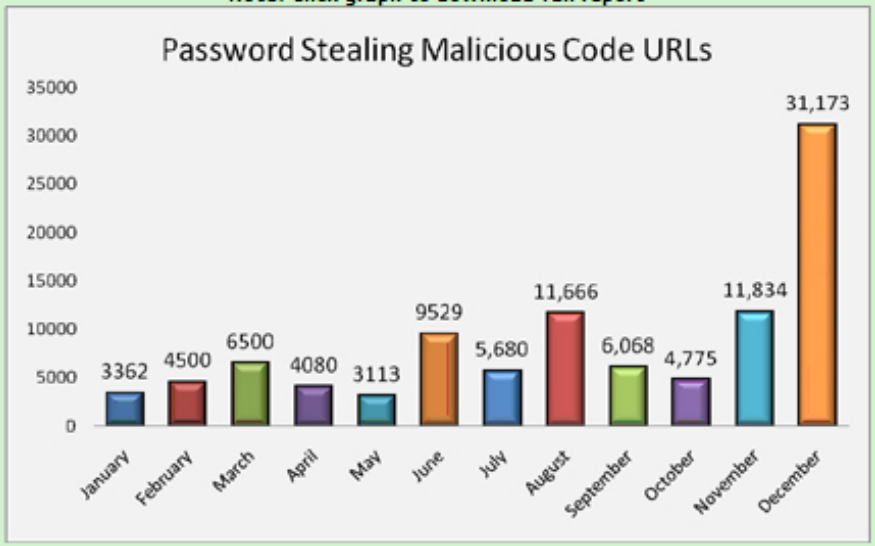


Evolución del Delito Informático



Actividad de Sitios que roban claves

Note: Click graph to download full report



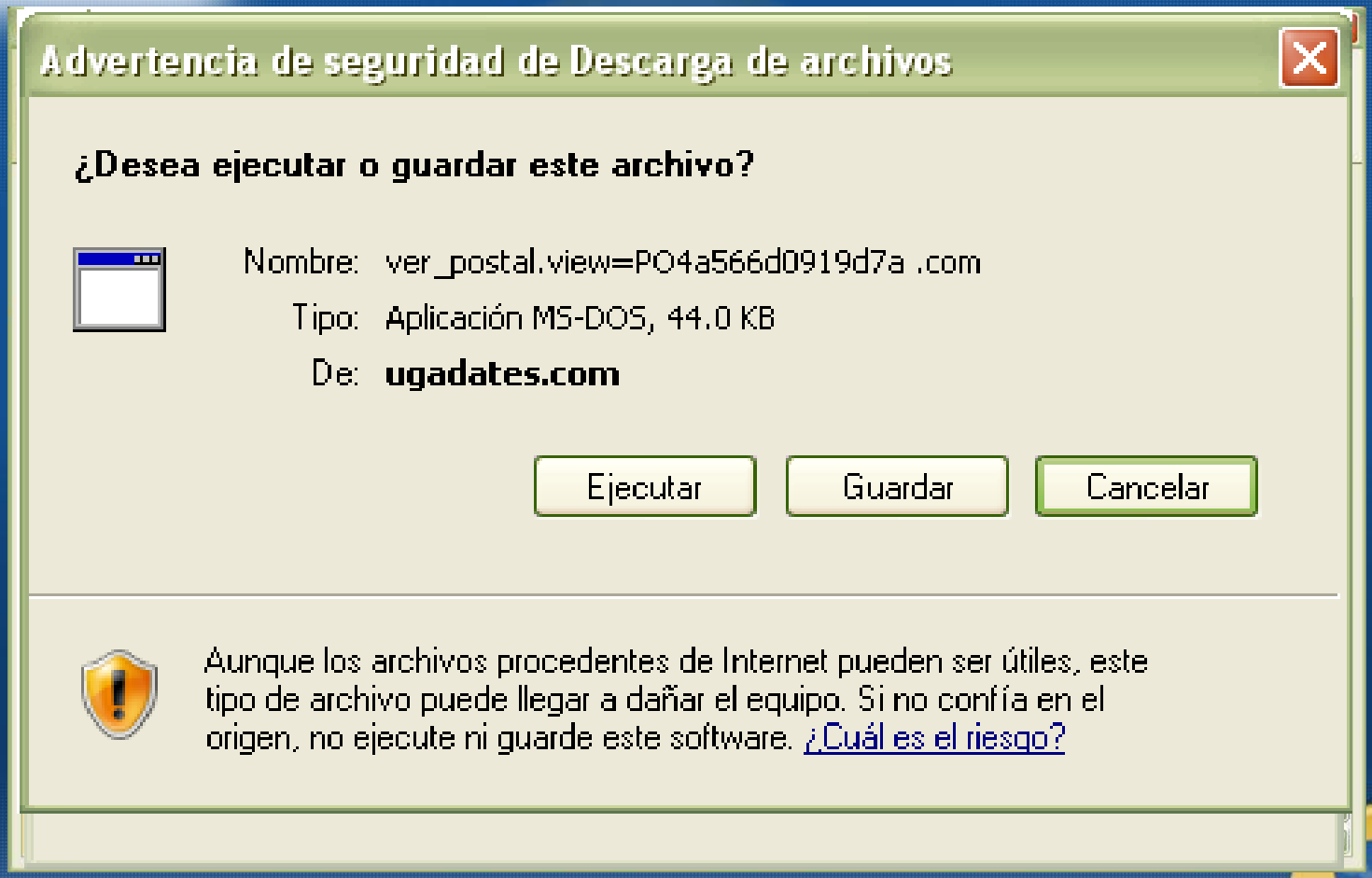
- The number of crimeware-spreading sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December, and 827% increase from January 2008.

- Unique phishing reports submitted to APWG recorded a yearly high of 34,758 in December.

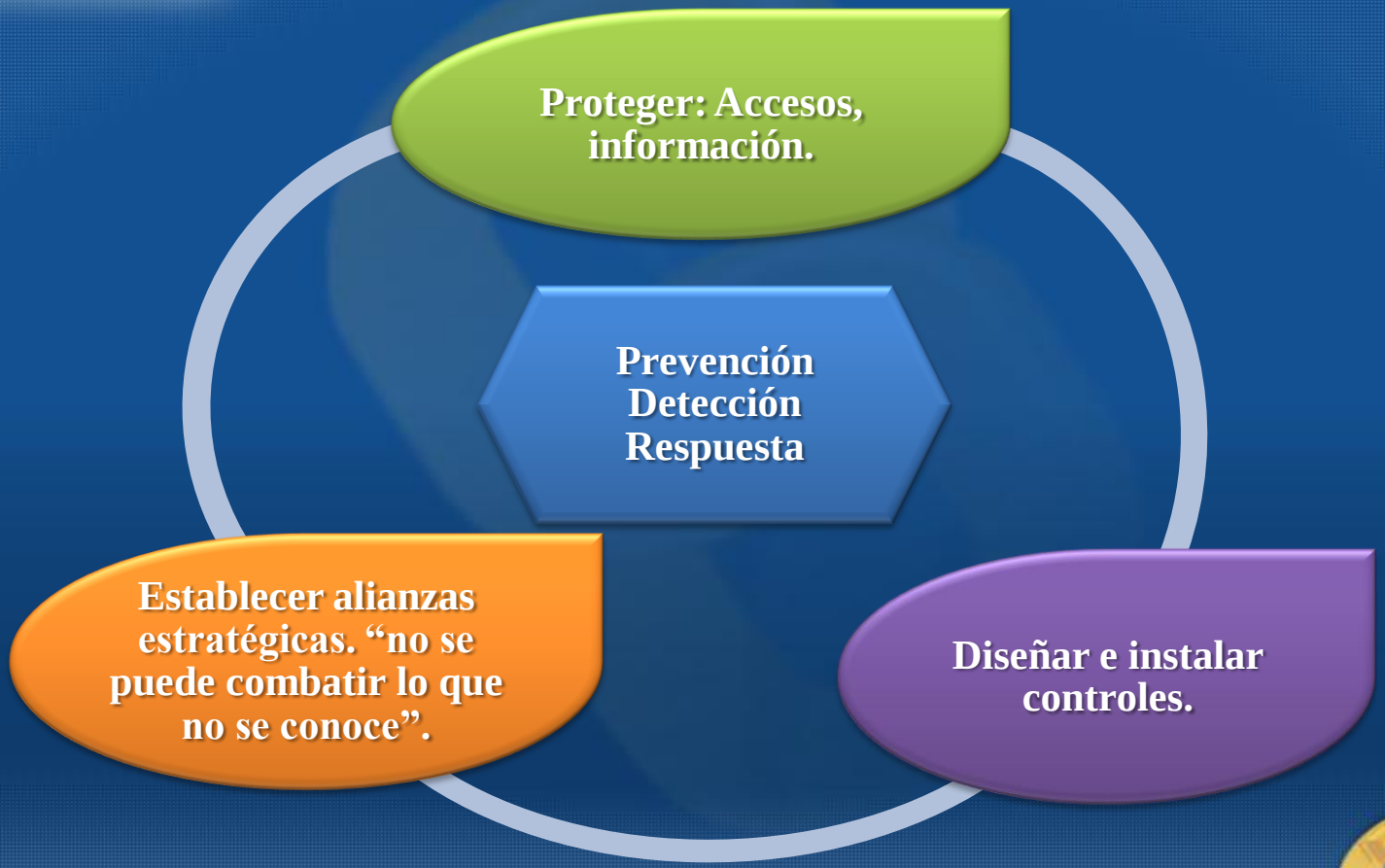
- The number of unigue keyloggers and crimeware-oriented malicious applications reached an all-time high in July reaching 1,519 in July.

- Rogue anti-malware began to rise in July, skyrocketing in December to 9,287.

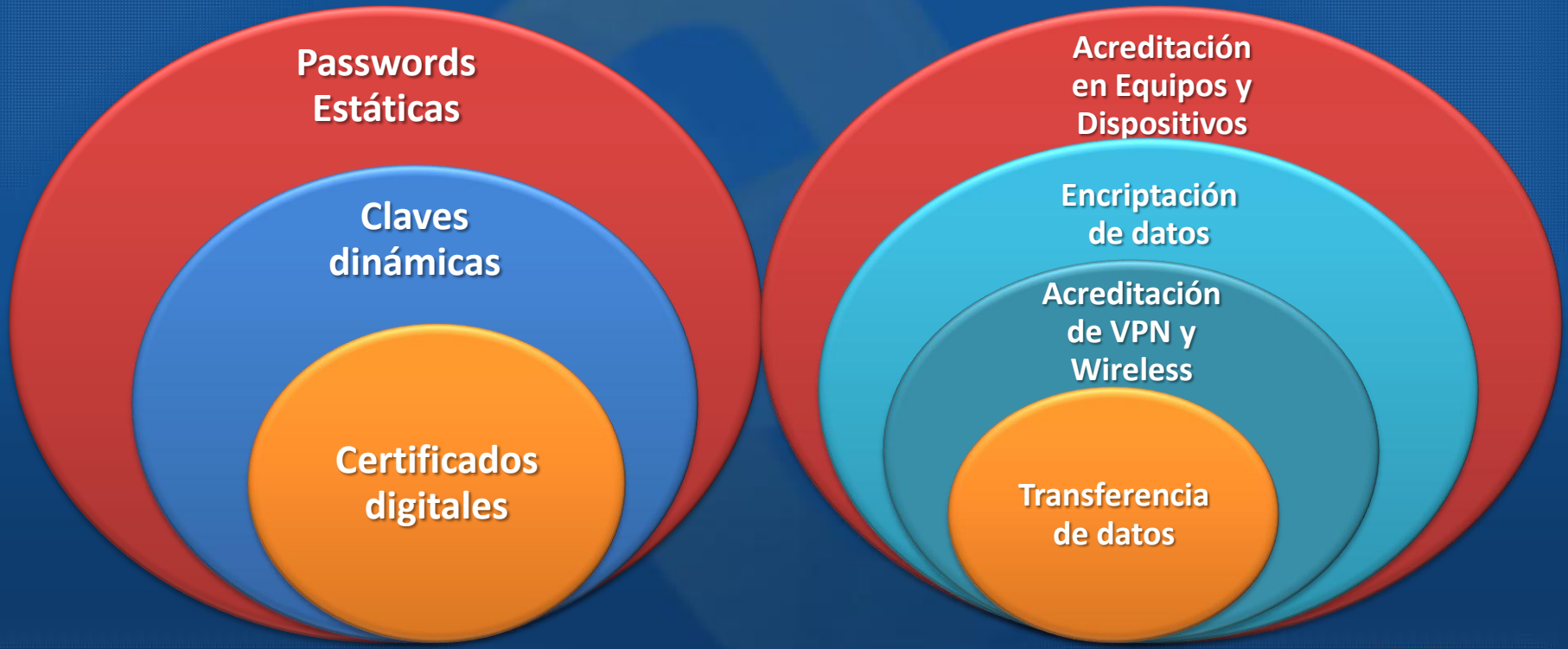
Esquema de ataque por virus Troyano



Consideraciones para el desarrollo de Productos Tecnológicos

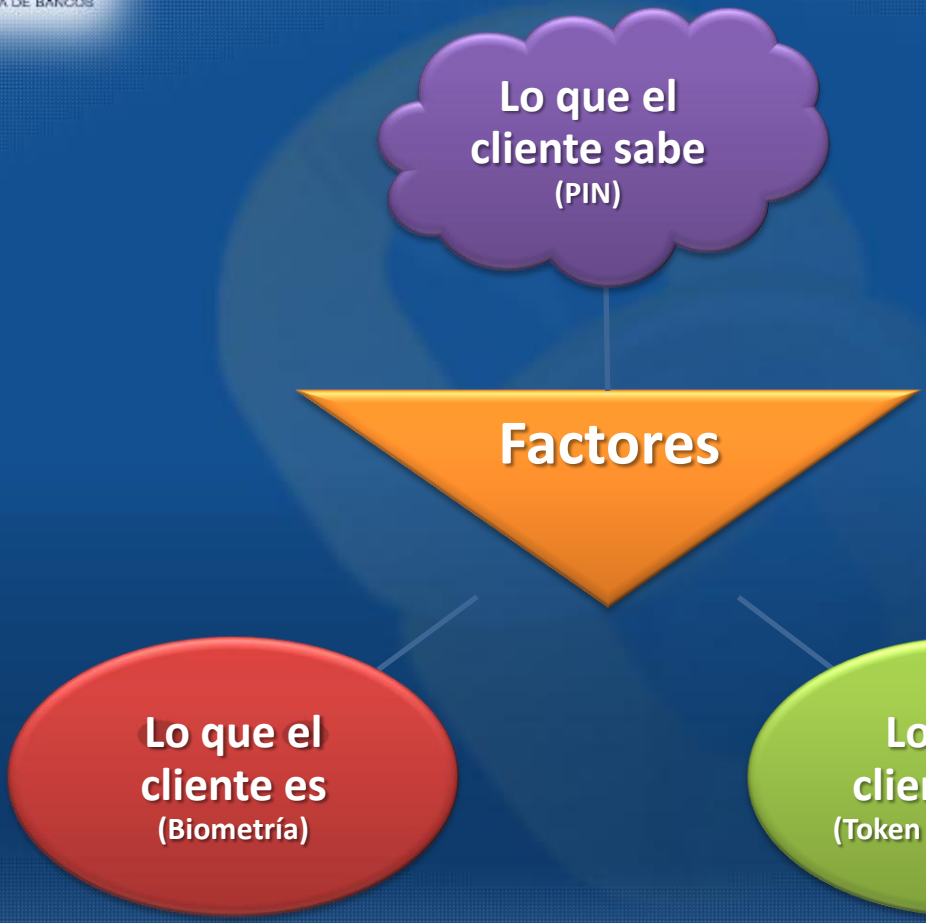


Autenticación y protección de datos

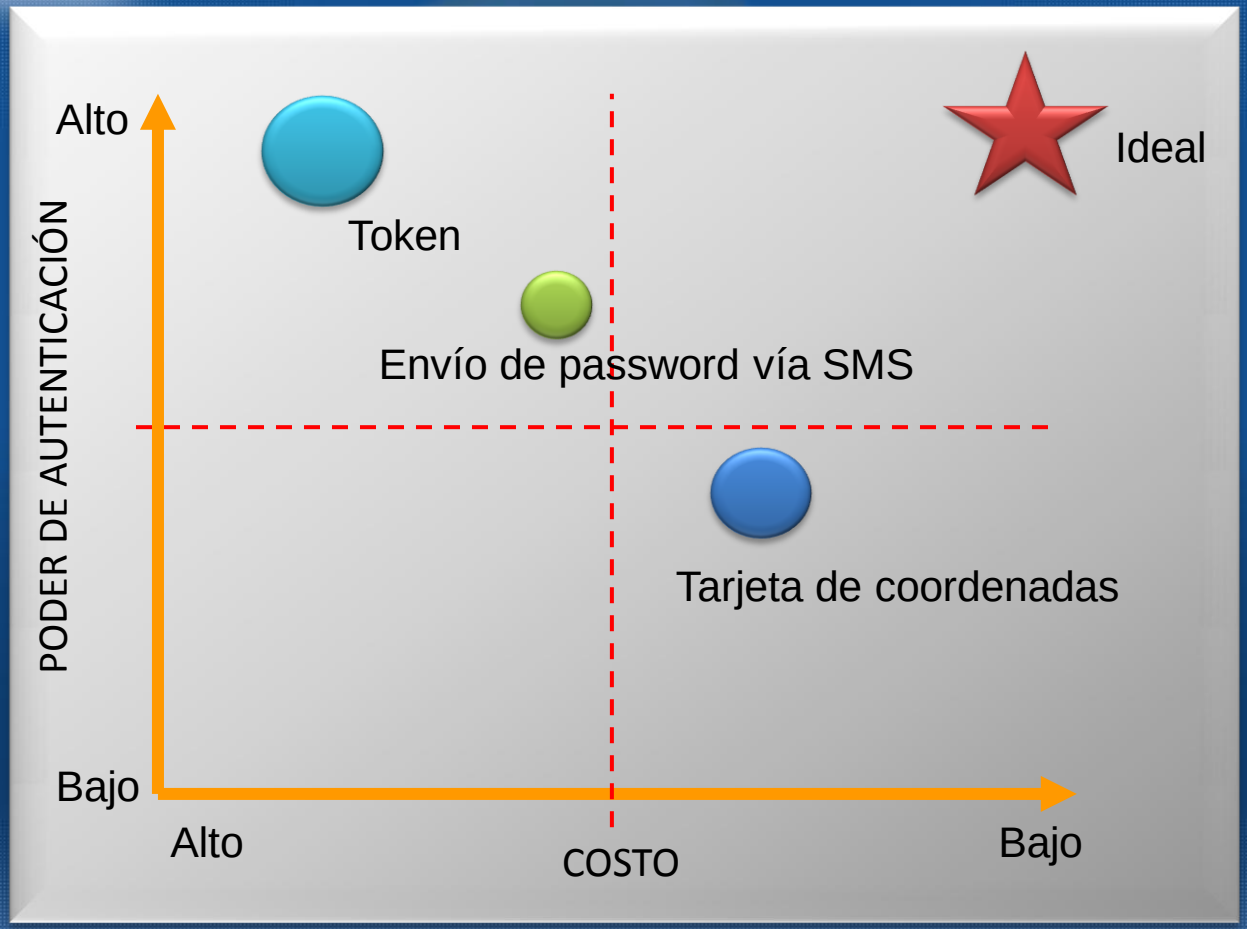


Gestión del Riesgo de la Información

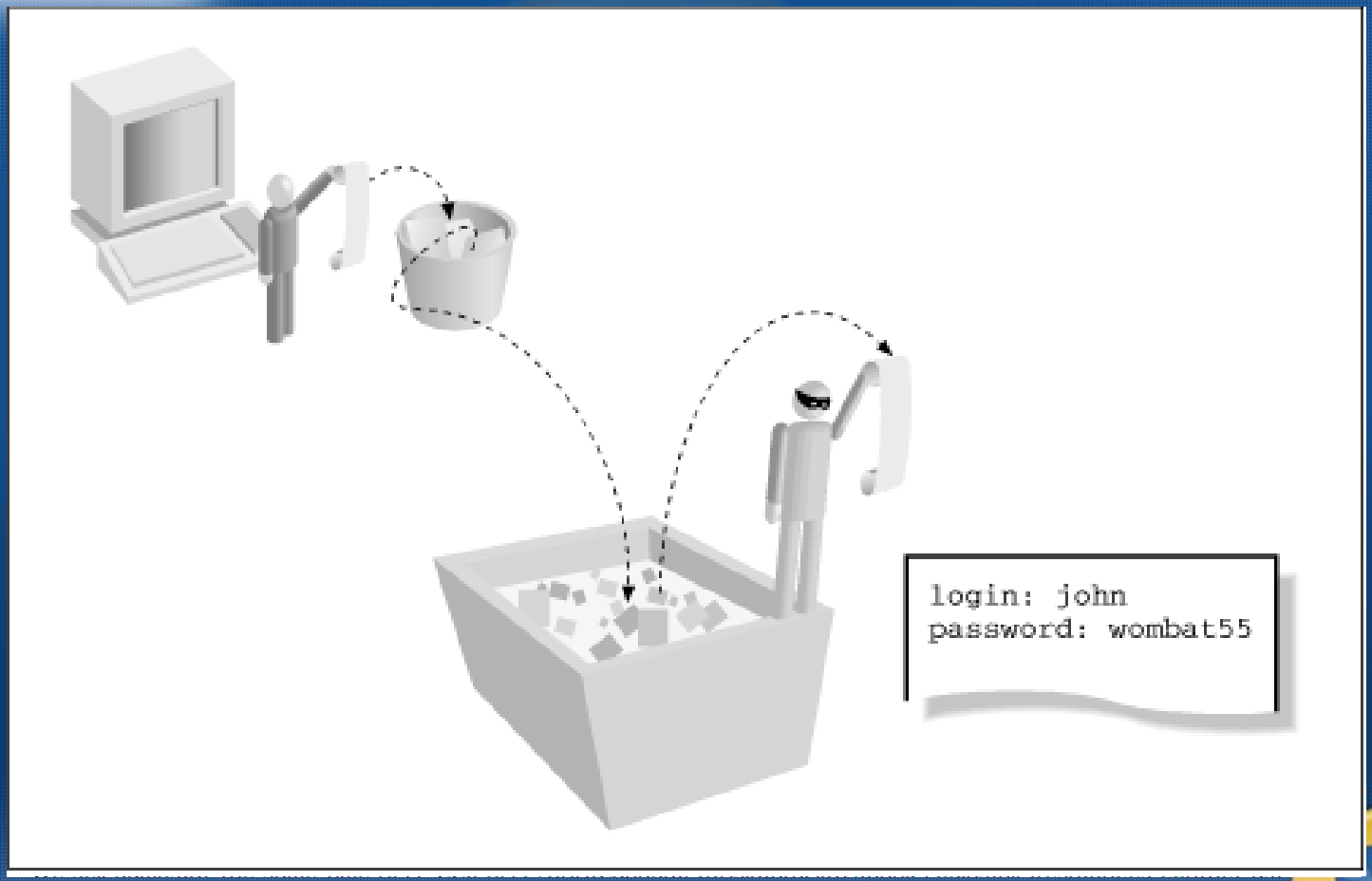
Autenticación Fuerte



Cuadro para la evaluación de métodos de autenticación

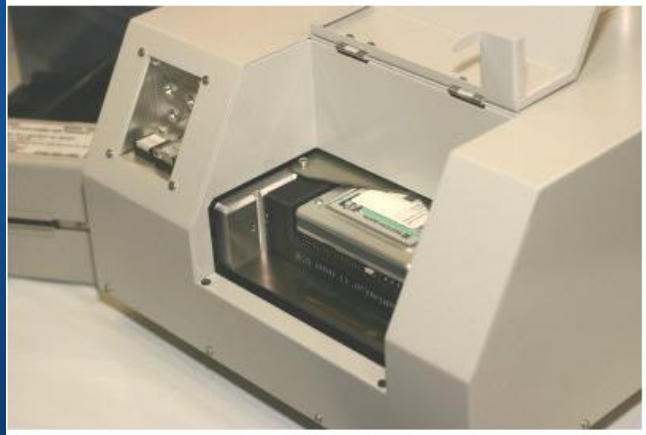


Venta de DUMP's



Destrucción de datos

SEM - Destruction Guaranteed



How do you make sure that your old hard-drives are erased? You can use SEM's EraSURE products to permanently erase the magnetic media. Simply insert your hard-drive into the unit, and a small conveyor belt slowly takes the drive under two extremely powerful rare-earth magnets. The process takes about 30 seconds.

The magnets are so strong that SEM officials say that the read/write heads are also rendered useless. And if you find yourself in the desert with no power outlet and desperately need to erase a hard drive, the EraSURE also comes in a hand-cranked version.

Compromiso de Información

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Sábado | 18.06.2005

Clarín.com

Inicio | Títulos | Secciones | Suplementos | Clasificados | Servicios

10:30 | DELITOS INFORMATICOS

Un hacker robó los datos de 40 millones de tarjetas de crédito en EE.UU.

Mastercard Internacional advirtió que un pirata informático violó la seguridad de una compañía subcontratista y accedió a la información de millones de clientes. El FBI investiga el caso.

Un hacker logró burlar los sistemas de seguridad informática de la compañía Mastercard Internacional y robó los datos de unos 40 millones de clientes de esa conocida tarjeta de crédito en los Estados Unidos.

LA INFO DE ESQUÍ ESTÁ EN

La compañía, una de las principales tarjetas de crédito del mundo, denunció el fraude ante el FBI. Según explicó, el 22 de mayo pasado un hacker **violó el sistema informático** de "CardSystems Solutions", una compañía subcontratista de Mastercard que procesa operaciones en nombre de bancos emisores de tarjetas de crédito y comerciantes, y robó los datos de sus clientes.

La compañía precisó que de las 40 millones de tarjetas robadas, unos 14 millones pertenecen a Mastercard, 22 millones a Visa International y el resto a distintas compañías. También aclaró que el pirata informático sólo **accedió a los números de las tarjetas de crédito** y no a datos como el número de seguridad social o fechas de nacimiento de los clientes, que podrían ser utilizados para realizar "robos de identidad" o solicitudes de crédito.

Sin embargo, MasterCard le solicitó a sus clientes que si notan **actividades sospechosas en sus tarjetas** lo denuncien a sus bancos. Y aclaró que en caso que se hayan registrado operaciones que no fueron hechas por sus clientes, la compañía tomará medidas para resolverlo

Una cadena de tiendas sufre el robo de datos de 46 millones de tarjetas de crédito

Un robo de los datos de 45,7 millones de tarjetas de crédito de los clientes de las cadenas de tiendas de ropa y artículos de decoración de la compañía estadounidense **TJX**, propietaria de TK Maxx, **ha afectado a millones de estadounidenses y británicos**.

30 Mar 2007 | AGENCIA EFE

Clientes de las ocho cadenas con las que opera TJX en Estados Unidos, Puerto Rico, Canadá, el Reino Unido, Irlanda -en estos dos últimos países opera 210 tiendas- han sido afectados por el robo de hasta un centenar de archivos con la información y perpetrado por 'piratas' informáticos.

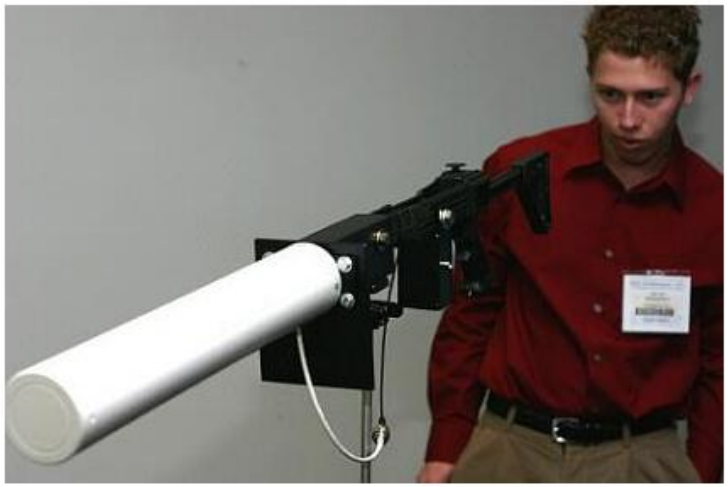
Éstos accedieron a los sistemas de varios puntos de Estados Unidos y Gran Bretaña durante un periodo de 17 meses y tomaron los datos de clientes de las tiendas de TJX entre diciembre del 2002 y noviembre del 2003, según informaron medios británicos.

La compañía, que comenzó a sospechar del robo hace tres meses e informó de él hace dos, aseguró en un comunicado no estar segura de la magnitud del robo ni del modo que afecta a sus clientes.

"Desconocemos el contenido de los archivos por los programas informáticos utilizados en la intrusión y por el sistema de eliminación de archivos que llevamos a cabo en el curso normal de nuestro negocio", dijo la portavoz de TJX Sherry Lang.

Aplicaciones móviles…

BlueSniper: Death From Above



On the first day of the RSA Expo, thousands of attendees jammed into the expo hall to look at the latest computer security wares. Little did they know that a trio of hackers had quietly set up their BlueSniper gun one floor above them. John Hering, James Burgess and Kevin Mahaffey scanned the attendees below, looking for vulnerable Bluetooth devices such as phones and headsets.

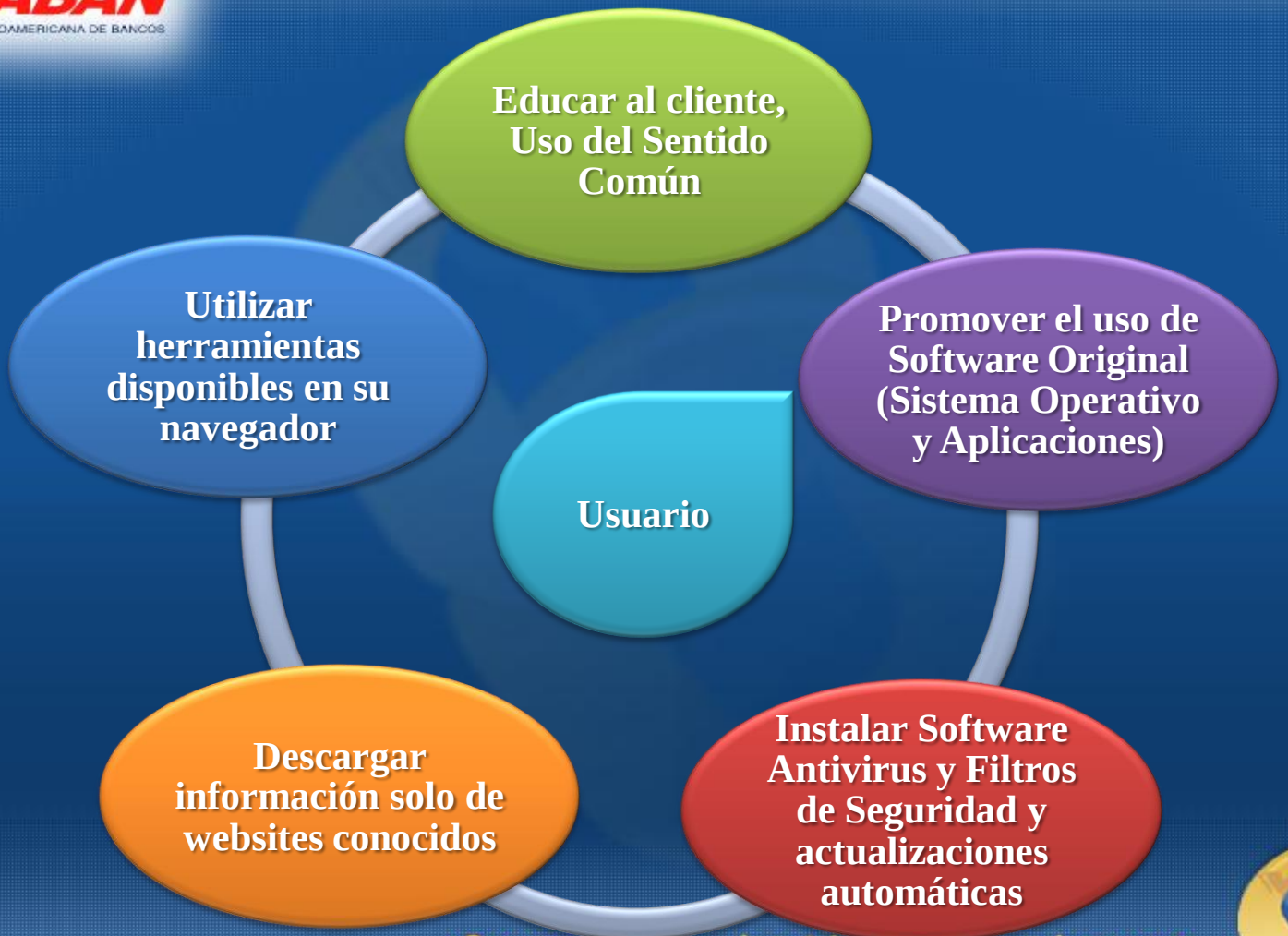
The gun is an upgraded version of the one they showed off at Defcon 12 in Las Vegas. A directional antenna amplifies the incoming Bluetooth signals, allowing the gun to tap Bluetooth devices from hundreds of meters away. The information is fed into a gum-stick-sized computer that is loaded into the gun like a magazine of ammunition.

The gun can scan for vulnerable devices and then list out available services. When a vulnerable device is found, an exploit can be attempted.

Importancia de compartir información como Estrategia para contrarrestar delitos

Congreso Latinoamericano
de Seguridad Bancaria - CELAES

Buenas prácticas

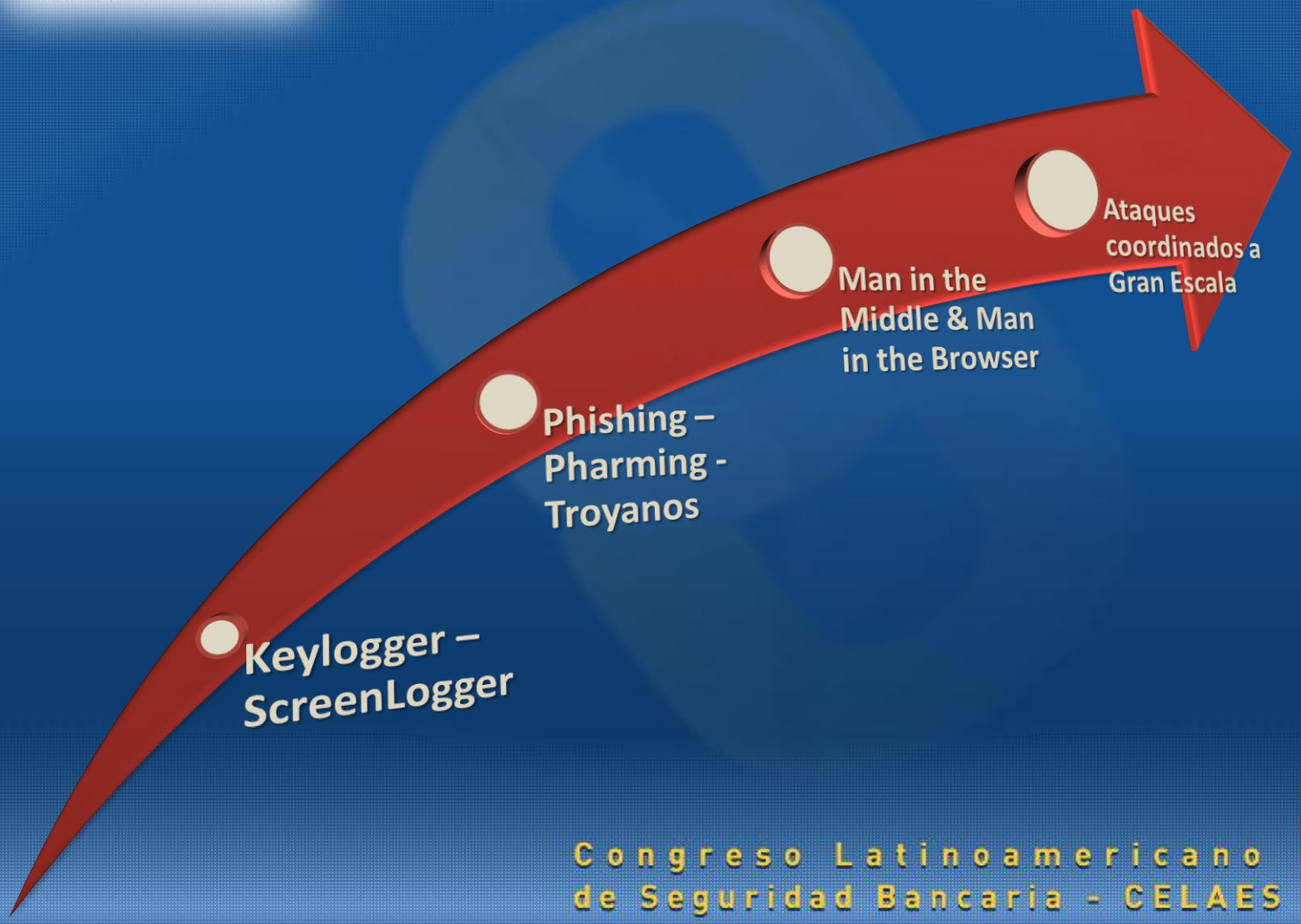


Buenas Prácticas - Usuarios

Sospeche de cualquier correo que requiera respuestas Urgentes	No use los enlaces de correos , mensajería instantánea o chat que oriente su navegación por Internet	Evite el llenado de formularios de mensajes de correo que solicitan información personal
Asegúrese de encontrarse en un sitio web seguro cuando proporcione su número de tarjeta u otra información sensible	Actualice la barra de herramientas de su navegador incorporando aplicaciones de detección de malware	Verifique regularmente el movimiento de sus cuentas, validando sus movimientos y comuníquese con su Entidad Financiera para comunicar consumos no reconocidos

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Tendencia mundial del Fraude



FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Que hay de nuevo en Seguridad de Información

y que podemos hacer para prevenir los riesgos en la industria bancaria

Ing. Giovanni Bautista Pichling Zolezzi
gpichling@asbanc.com.pe
www.giovannipichling.blogspot.com

Muchas gracias por la atención prestada

Congreso Latinoamericano
de Seguridad Bancaria - CELAES