Informe de Phishing 2012

13 de enero 2013

Por segundo año consecutivo **Segu-Info** y **Antiphishing.com.ar** analizan en profundidad denuncias de casos de correos fraudulentos y los compara con los datos anteriores para establecer el estado del arte en materia Phishing.

Este es el segundo informe con estadísticas de phishing de América Latina, con datos sobre la cantidad de casos, países y entidades afectadas además de las técnicas de propagación utilizadas.

Autor: Lic. Cristian Borghello CISSP-MVP
Versión: 1.0 (20130112)
Descarga: www.segu-info.com.ar

Versión	Fecha	Cambios
1.0	13/01/2013	Versión inicial

Introducción

En base a las denuncias recibidas por **Segu-Info** en los últimos seis años, el phishing es uno de los engaños y formas de manipulación de usuarios que más ha crecido en América Latina, y aun así, lamentablemente, no se puede decir que se configure como delito en alguno de los países de la región.

Realizar denuncias de Phishing:
www.antiphishing.com.ar/denuncia

En cada caso, se procede a realizar un seguimiento de la denuncia recibida para establecer la forma de operación del delincuente así como la información que el mismo desea obtener de la víctima. La información analizada es de vital importancia para establecer posibles nuevos vectores de ataques y también permite realizar estudios como el presente.

En vistas del incremento exponencial de los casos de Suplantación de Identidad Digital y Phishing, Segu-Info y La Red El Derecho Informático se han unido para generar la Primera **Cruzada por la Identidad Digital** contra el robo de identidad digital y el phishing.

http://cruzada.elderechoinformatico.com

Muestreo

Durante el año 2012, en **Segu-Info** se recibieron más de 800 denuncias de correos sospechosos. Es importante destacar que estos datos sólo reflejan la cantidad de denuncias realizadas por los usuarios y **no debe entenderse como el total de casos, que seguramente será superior**, o sobre que una entidad es más afectada que otra, si bien el muestreo es importante y posiblemente refleje la realidad.

A continuación, se realizó la siguiente clasificación sobre los correos recibidos:

1. Dañados o que no representan ningún riesgo
2. Correos reales que los usuarios confundieron con fraudulentos o peligrosos
3. Publicidad
4. Scam
5. Casos de phishing que sólo contenían el enlace al sitio falso
6. Casos de phishing con adjuntos o enlaces dañinos

En base a la clasificación anterior, se descartaron aquellos casos que no fueran representativos para el presente informe: scam, correos dañados o los que contienen publicidad, lo que permite considerar un total de **657 denuncias** (71% más que en 2011) de correos correspondientes a

phishing[1], que pretendían obtener información sensible del usuario y que podían o no contener archivos adjuntos.

Considerando que un mismo caso puede ser denunciado varias veces por diferentes usuarios, al agrupar las 657 denuncias, se obtiene un total de 314 casos únicos. Dependiendo la entidad y el grado de propagación del correo, se recibió desde una hasta un máximo de 12 denuncias.

De los 314 casos únicos, 263 corresponden a phishing tradicional (83%), donde el delincuente crea y simula sitios web de entidades financieras o bancarias de confianza para lograr que la víctima ingrese su información privada. Los 51 casos restantes corresponden a organizaciones públicas y privadas que ofrecen servicios varios: telefonía, *mailing*, diarios, aerolíneas, blogs, postales, redes sociales, etc.

Las entidades afectadas han sido las siguientes:

American Express	Banco Macro	COMAFI	Paypal
Auditoria Federal (Brasil)	Banco Patagonia	CorpBanca	Santander Rio
Banamex	Banco Popular	Davivienda	SICREDI
Banco AV Villas	Banco Sol	Groupon	Standard Bank
Banco Caja Social	Bancolombia	HSBC	US Bank
Banco CorpBanca	Banesco	ITAU	Veraz
Banco de Bogota	BBVA Bancomer	Mastercard	VISA
Banco de Chile	BBVA Francés	Mercado Libre - Mercado Pago	
Banco de Costa Rica	Bradesco	Pago Mis Cuentas	

Nota: no se informa los porcentajes de afectación a fin de no dañar la imagen de las entidades mencionadas y tampoco suministrar información que pueda orientar a los delincuentes a planear de mejor manera sus ataques.

[1] **Phishing:** técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. www.segu-info.com.ar/phishing

Con respecto a las 51 denuncias de correos que afectaban a otras empresas, se clasificaron de la siguiente manera:

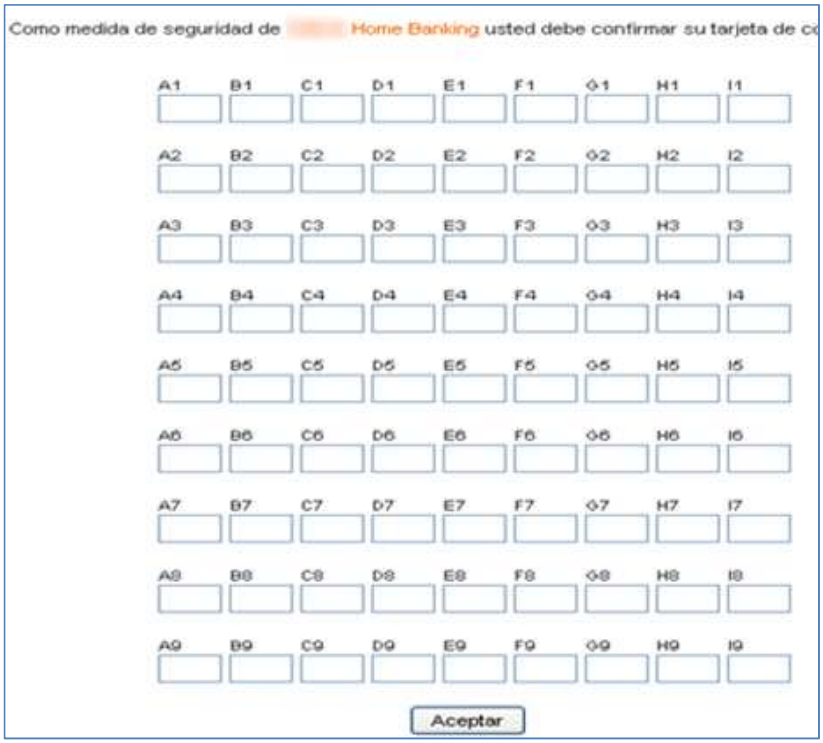
American Airlines	Fiscalía Federal de la Nación (Colombia)	Personal
CFE ? Comisión Federal de Electricidad (México)	LAN	TAM
Claro	Movistar	Twitter
Documentación falsa	Noticias falsas	UPS
Facebook		

Nota: Documentación falsa corresponde a multas, fotomultas, contratos laborales, envíos de productos y las noticias falsas corresponden a cualquier tipo de noticia que pudo ser de actualidad y altamente atractiva para una gran cantidad de lectores, lo cual facilita su propagación.

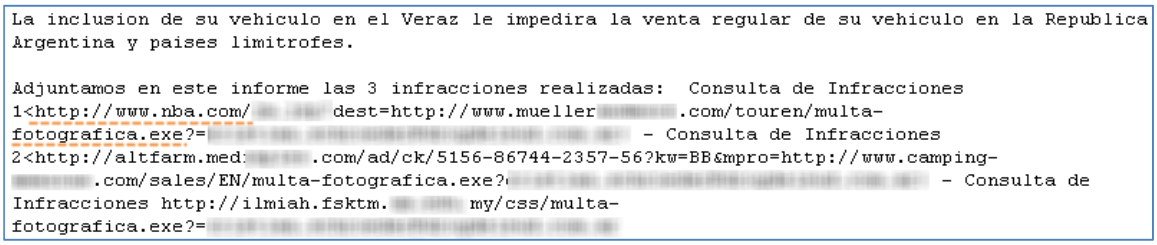
Análisis de casos

Luego de la clasificación inicial se realizó un análisis de cada correo recibido (314 casos) para determinar su forma de propagación y las técnicas utilizadas en los mismos:

1. 38,53% contienen URL a dominios y sitios muy confiables utilizados como redirectores.
2. 22,29% intentan robar *tokens* o tarjetas de coordenadas asociados por seguridad a las cuentas de los usuarios.

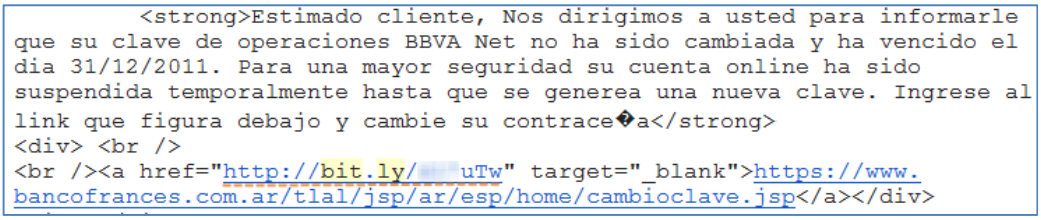


3. 56 casos (17,83%) contienen archivos adjuntos o enlaces a archivos dañinos (malware). De estos casos, 16 enlazan o descargan archivos EXE directamente y el resto utilizan la compresión (ZIP), lo cual indica la falta de educación del usuario quien primero debe descargar el archivo comprimido, descomprimirlo y luego ejecutar el EXE asociado.


La inclusion de su vehiculo en el Veraz le impedira la venta regular de su vehiculo en la Republica Argentina y paises limitrofes.

Adjuntamos en este informe las 3 infracciones realizadas: Consulta de Infracciones 1<http://www.nba.com/ dest=http://www.mueller .com/touren/multa-fotografica.exe?= - Consulta de Infracciones 2<http://altfarm.med .com/ad/ck/5156-86744-2357-56?kw=BB&mpro=http://www.camping- .com/sales/EN/multa-fotografica.exe? - Consulta de Infracciones http://ilmiah.fsktm. my/css/multa-fotografica.exe?=

4. 11,58% tienen enlaces acortados para lograr saltear los filtros *antispam* y confundir al usuario.


Estimado cliente, Nos dirigimos a usted para informarle que su clave de operaciones BBVA Net no ha sido cambiada y ha vencido el dia 31/12/2011. Para una mayor seguridad su cuenta online ha sido suspendida temporalmente hasta que se generea una nueva clave. Ingrese al link que figura debajo y cambie su contrace&#65533;a

https://www.bancofrances.com.ar/tlal/jsp/ar/esp/home/cambioclave.jsp

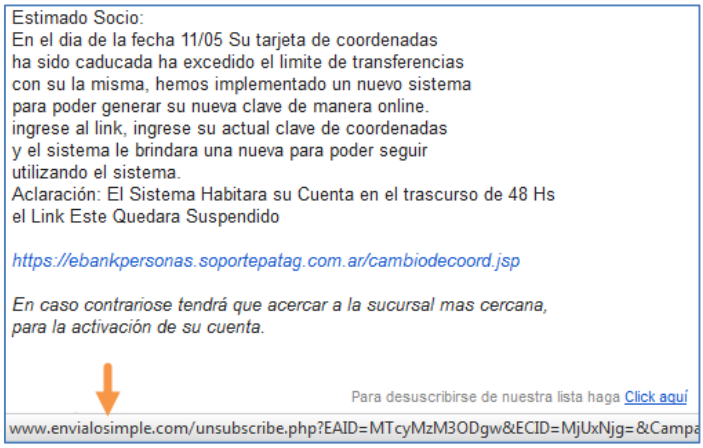
5. 11,46% ofrecen la descarga de supuesta documentación personal para el usuario (fotos, multas, testamentos, contratos, transferencias de dinero, etc.).


Estimado contribuyente:
Detectamos en nuestro Sistema Integrado de Multas de transito (ATM) infracciones cometidas por su vehiculo
Si usted no regulariza las infracciones correspondientes en los proximos 30 dias a partir de la fecha de emision de este comunicado, su vehiculo sera informado como deudor y usted pasara a formar parte del Veraz, conforme Ley n 19.216 de 1/12/2011
La inclusion de su vehiculo en el Veraz le impedira la venta regular de su vehiculo en la Republica Argentina
Infracciones al dia 14/02/2012
Girar a izquierda/derecha en lugar prohibido - No respetar Senda Peatonal/Paso Peaton - Exceso Velocidad hasta 20Km/h

El propietario del ve iculo queda notificado por este medio. Todas aquellas actas labradas con anterioridad a las fechas especificadas seguiran bajo la orbita de la Unidad dministrativa.

www.philipmorrisusa.com/ ?url=http://www. dox.be/para/photo/Informe_Deuda_PDF.exe

6. 6,36% utilizan enlaces creados a través de plataformas de e-mailing legales que ofrecen sus servicios de prueba gratuitos y estos son aprovechados por los delincuentes. Adicionalmente algunos de ellos también tienen vulnerabilidades en sus aplicaciones web y esto también permite el envío de correo masivo (*spamming*) y abuso del servicio por parte del delincuente.

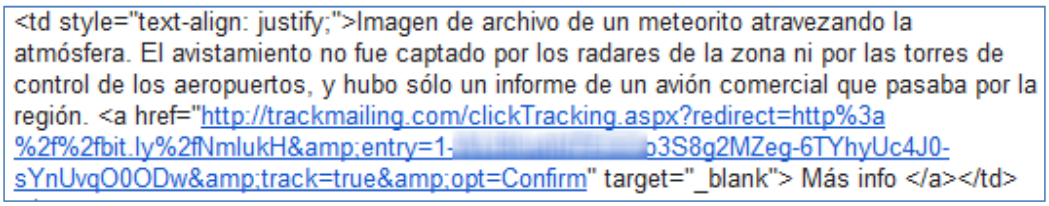

Estimado Socio:
En el dia de la fecha 11/05 Su tarjeta de coordenadas
ha sido caducada ha excedido el limite de transferencias
con su la misma, hemos implementado un nuevo sistema
para poder generar su nueva clave de manera online.
ingrese al link, ingrese su actual clave de coordenadas
y el sistema le brindara una nueva para poder seguir
utilizando el sistema.
Aclaración: El Sistema Habitara su Cuenta en el trascurso de 48 Hs
el Link Este Quedara Suspendido

https://ebankpersonas.soportepatag.com.ar/cambiodecoord.jsp

En caso contrariose tendrá que acercar a la sucursal mas cercana,
para la activación de su cuenta.

Para desuscribirse de nuestra lista haga Click aquí
www.envialosimple.com/unsubscribe.php?EAID=MTcyMzM3ODgw&ECID=MjUxNjg=&Campa

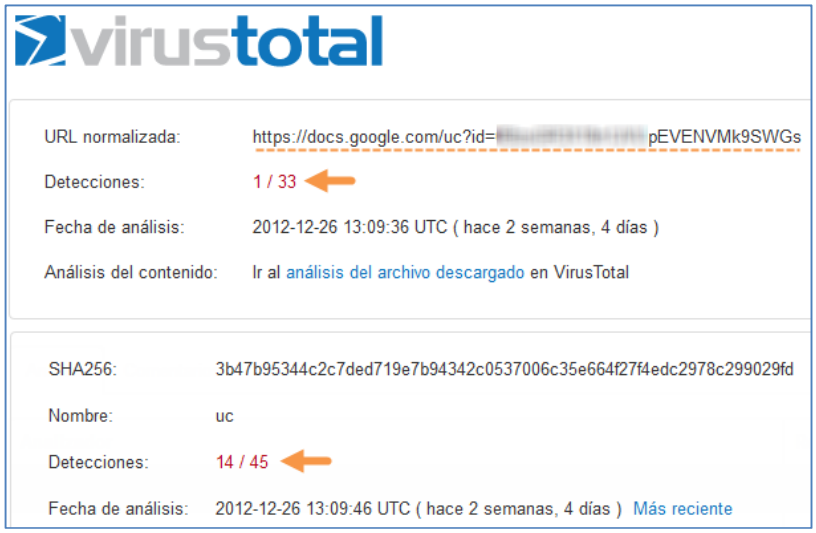
7. En el 5,74% de los casos se utiliza SMiShing, donde se envía un SMS al usuario tentándolo con una oferta "imperdible" y se le ofrece un enlace donde debe proporcionar su información personal.
8. En el 3,82% de los casos, se utiliza geo-localización (del lado del servidor o del lado del cliente) para lograr que solo los usuarios del país afectado ingresen al sitio o para rastrear a las posibles víctimas a través de su dirección IP. Por ejemplo la siguiente URL (de octubre de 2012), utiliza esta técnica para identificar al usuario:
   `http://www.mairie[XXX]avold.fr/admin/189.134.101.162/olb/Init.html`
9. 5 casos (1,59%) aprovechan noticias de interés local o internacional para engañar a los usuarios y lograr que hagan clic en un enlace o descarguen un archivo dañino.


<td style="text-align: justify;">Imagen de archivo de un meteorito atravezando la atmósfera. El avistamiento no fue captado por los radares de la zona ni por las torres de control de los aeropuertos, y hubo sólo un informe de un avión comercial que pasaba por la región. Más info </td>

Nota: los porcentajes no suman 100% debido a que varias técnicas pueden ser empleadas en el mismo correo.

Al evaluar el lugar donde se encontraban alojados los sitios falsos se deduce lo siguiente:

1. Sólo 5 casos (1,59%) utilizaron dominios raíz *(.com, .net, .org,* etc.) creados por el delincuente para la ocasión. La baja tasa indica el trabajo y riesgo mayor que el delincuente debería afrontar.
2. 6,68% estaban alojados en servidores gratuitos, lo cual indica una baja importante respecto al año anterior. En algunos de estos casos (2,54% del total) se utilizaron dominios de Cloud Computing para alojar los archivos dañinos como por ejemplo Dropbox o Google Docs.



3. 91,73% se encontraban en servidores ajenos vulnerados. Esto demuestra que para los delincuentes es mucho más fácil y redituable vulnerar un servidor ajeno, debido a que el tiempo de baja es mayor que si lo alojaran en un servidor gratuito.

En el último tiempo, la utilización de dominios confiables como redirectores, se ha transformado en un ataque clásico, ya que el usuario asocia un dominio con la confianza hacia el mismo pero, las vulnerabilidades en el servidor permiten que el delincuente lo utilice para engañar. Enlaces como el siguiente,

`www.nba.com/redireccion.jsp?url=www.sitio-dañino.com`

Podrían hacer pensar que se ingresará a NBA cuando en realidad el sitio de NBA redireccionará automáticamente al usuario al segundo dominio, sin que este lo note.

En el caso de servidores de terceros, inicialmente se toma el control del servidor aprovechando alguna vulnerabilidad que puede corresponder a sistemas operativos o servicios instalados por defecto, claves débiles, aplicaciones desarrolladas en forma insegura, etc. Luego, simplemente se sube el contenido del sitio falso a un directorio aleatorio del servidor.

Las URL en este caso pueden lucir de la siguiente manera:

`http://www.sitio-afectado.com.ar/descargas/img/nombre-banco/index.html`

`http://direccion-IP-servidor/nombre-banco/index.html`

Destaca también el crecimiento del uso de los SMS como herramienta de propagación. Esto se debe a la facilidad que tiene un delincuente para obtener un SIM y número telefónico por un bajo (nulo) costo y prácticamente sin correr riesgo. Este ataque se transforma en un arma ideal si también se considera la existencia de herramientas informáticas que permiten el envío de SMS masivos sin costo.

En estos casos, la tasa de víctimas crece exponencialmente porque el usuario tiende a pensar que solamente personas autorizadas y confiables podrían tener su número telefónico, por lo que si recibe un mensaje con supuestos premios, esto lo convierte en víctima potencial.

Conclusiones

La cantidad de técnicas utilizadas por los delincuentes para engañar a los usuarios está creciendo. Varían desde las más clásicas, donde se aloja un sitio o un archivo dañino en un servidor gratuito, hasta las más "modernas" donde se alojan los archivos en Cloud Computing y se rastrea al usuario para conocer su procedencia. Otras técnicas apuntan directamente a robar tarjetas de coordenadas y *tokens* de validación utilizados por algunas entidades para garantizar la seguridad del usuario al momento de realizar operaciones virtuales.

Sin dudas, desde hace tiempo, el phishing es un medio de vida para muchos grupos delictivos. Lamentablemente las entidades siguen prefiriendo cerrar los ojos antes de abrirlos a una realidad que los supera en muchos casos pero, en otros, simplemente es la conveniencia económica porque los montos robados son menores a los seguros que pagamos los clientes.

Cabe preguntarse ¿hasta cuándo seguirá la mentira, sin inversión y sin protección para los usuarios?