Un año de phishing en números

7 de enero
2012

Durante 5 años **Segu-Info** ha recibido miles de denuncias de casos de correos fraudulentos. En este documento se analizan los correos del último año así como las tendencias delictivas y estadísticas que se desprenden de los mismos.

Este es el primer informe con estadísticas de phishing de América Latina, con datos sobre la cantidad de casos, países y entidades afectadas, las técnicas de propagación utilizadas y el dinero recaudado por los delincuentes.

Autor: Lic. Cristian Borghello CISSP-MVP
Versión: 1.2 (201201010)
Descarga: www.segu-info.com.ar

Versión	Fecha	Cambios
1.2	10/01/2012	Nota y aclaraciones sobre tipo de entidades
1.1	09/01/2012	Correcciones menores. Agregado proyecto de ley antiphishing en Argentina
1.0	07/01/2012	Versión inicial

Introducción

En base a las denuncias recibidas por **Segu-Info** en los últimos cinco 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 configura como delito en alguno de los países de la región.

Realizar denuncias de Phishing: www.segu-info.com.ar/denuncia

Para que el Phishing sea considerado delito, también se deberían tipificar otras actividades relacionadas como el robo de identidad y otras acciones que son preparatorias para la comisión del robo económico posterior.

Proyecto de Ley Antiphishing en Argentina: http://j.mp/x5Lq0D [PDF]

En cada caso, y en base a estas denuncias recibidas, se procede a realizar un seguimiento 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.

Muestreo

Durante el año 2011, en **Segu-Info** se recibieron más de 500 denuncias de correos sospechosos, los cuales fueron clasificados como:

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

El **scam** es un intento de engaño o fraude en el cual el delincuente busca convencer a la víctima diciéndole que obtendrá grandes ganancias o premios económicos (loterías, herencias, donaciones, etc.)

En el presente se consideran **384 denuncias** de correos correspondientes a scam y phishing, que pretendían obtener información sensible del usuario y que podían o no contener archivos adjuntos.

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

De dicha cantidad, se crearon dos grupos de 250 y 134 respectivamente. El primer grupo corresponde al phishing tradicional, en donde el delincuente crea y simula sitios web de entidades financieras o bancarias de confianza para lograr que la víctima ingrese su información privada. El segundo corresponde a organizaciones públicas y privadas que ofrecen servicios varios como puede ser telefonía, *mailing*, diarios, blogs, postales, redes sociales, etc.

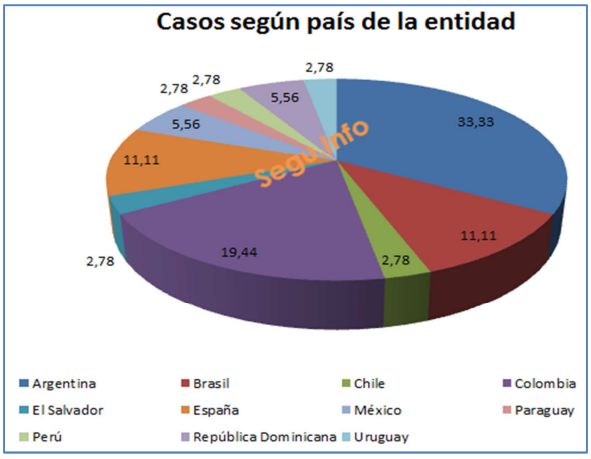

Imagen 1 – Porcentaje de casos por país

Del primer grupo de 250 correos, las entidades afectadas corresponden a los países que se ven en esta imagen.

Es importante destacar que estos porcentajes sólo reflejan la cantidad de denuncias realizadas por los usuarios de esos países y **no debe entenderse que un país recibe menos o más correos fraudulentos que otro**, si bien puede ser posible.

El **SMiShing** es una variante del phishing en el que se emplean mensajes de texto dirigidos a usuarios de telefonía móvil

Las entidades afectadas han sido las siguientes:

AFIP	Colmena BCSC	Itaú	BBVA Francés
American Express	Colpatria Multibanca	Promerica	Galicia
BanColombia	COMAFI	Banco Regional	MasterCard
Banregio	Davivienda	Santander Chile	Mercado Pago
Banreservas	Banco Nación Argentina	Santander Real	Pago mis cuentas
BHD	BROU	Santander Río	Visa
Bradesco	Banco de Sabadell	BBVA Bancomer	Provincia
Caja Madrid	Banco Do Brasil	BBVA Colombia	Banamex
Tarjeta Naranja	AV Villas	BBVA España	

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.
AFIP (Administración Federal de Ingresos Públicos) es el ente de recaudación y fiscalización de rentas de Argentina pero se incluye en este grupo porque los correos recibidos hacen alusión a montos y deudas.

Con respecto a las 134 denuncias de correos que afectaban a otras empresas, se clasificaron de la siguiente manera:

Paypal	Hotmail - Live – MSN	TAM
Claro	LAN	Telefónica Argentina
Disney	Movistar	UPS
Skype	Youtube	Twitter
Facebook	Fedex	Gusanito
Google	Telecom Personal	

Nota: ídem anterior.
Paypal es una entidad financiera pero se incluye en este grupo por no corresponder a América Latina.

Análisis de casos

Luego de la clasificación inicial se realizó un análisis de cada correo recibido para determinar su forma de propagación y las técnicas utilizadas en los mismos. Del primer grupo resulta:

- 27,60% contenían URL a dominios muy confiables utilizados como redirectores
- 14,8% contenían archivos adjuntos o enlaces a archivos dañinos (malware)
- 1,6% (4 de 250) fueron propagados por SMS a través del teléfono móvil (ataque conocido como SMiShing), además del correo electrónico

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:

- 2,40% correspondían a dominios raíz (.com, .net, .org, etc.) creados por el delincuente para la ocasión
- 17,20% estaban alojados en servidores gratuitos
- 80,40% se encontraban en servidores vulnerados, utilizados por los delincuentes como plataforma de ataque

Nota: los porcentajes suman 100%.

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.segu-info.com.ar`

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.

Nota: en este caso se ha modificado la URL real para no facilitar ataques.

La diferencia entre la utilización de servidores gratuitos o de terceros vulnerados no aloja ninguna sorpresa ya que los delincuentes buscan maximizar sus ganancias con el mínimo esfuerzo posible. En el primer caso se elige alguno de los centenares de sitios que ofrecen *hosting* gratuito, se crea una cuenta y se aloja el sitio falso, copia exacta del real. La URL luce de la siguiente manera:

`http://www.sitio-gratuito.com/nombre-entidad/`

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 o cualquier otro error. 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`

En raras ocasiones, por el riesgo que representa, puede ocurrir que el servidor pertenezca al delincuente y se utilice un servicio de DNS gratuito para redireccionar al usuario al dominio falso. En ese caso la URL será parecida a la siguiente:

`http://servicio-DNS-gratuito/nombre-banco/`

Esta técnica también es utilizada por los creadores de malware y administradores de botnet para enviar o recibir información a un dominio/IP controlado por el delincuente.

Una **botnet** es una red de equipos infectados por un malware y controlados en forma remota por un delincuente

Sí sólo se consideran los 6 casos en los que se registraron dominios raíz, se está hablando de ataques planeados con mayor cantidad de tiempo y en el cual seguramente se dispuso de la oportunidad de realizar *cybersquating* a la organización víctima, como por ejemplo registrar el dominio www.mercad0.com en donde se remplazó la letra “o” por el número “0”.

Destaca también el crecimiento del uso de los SMS como herramienta de propagación.

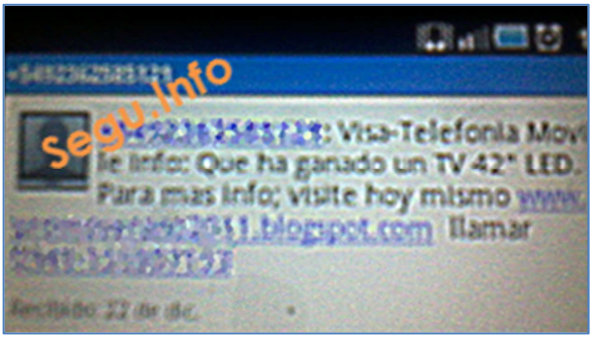

Imagen 2 - Mensaje de SMS fraudulento

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.

A mitad de año, un caso llamativo y que tuvo una tasa de éxito mayor que los casos tradicionales correspondió a sitios web de e-mail marketing que fueron vulnerados y utilizados por los delincuentes para crear y enviar el correo falso, de forma tal que para cualquier ojo (experto o no), el correo era totalmente real. Por supuesto, el enlace al sitio falso siempre era una forma efectiva de corroborar el engaño.

Por otro lado, del análisis del segundo grupo de correos, que corresponde a empresas resulta que:

- 54,47% contenían archivos adjuntos o enlaces a archivos dañinos
- 21,64% utilizaron las redes sociales y su reputación como imagen, para lograr que el usuario haga clic en el enlace ofrecido
- 19,40% correspondían a trabajos, premios, loterías, herencias o mensajes que prometían grandes ganancias económicas a los lectores
- 14,92% ofrecían la descarga de supuesta documentación personal para el usuario (multas, testamentos, contratos, transferencias de dinero, etc.)
- 11,19% aprovecharon noticias de interés local o internacional para engañar a los usuarios
- En 3,73% (5 de 134) de los casos se utilizó SMiShing
- 2,23% de los enlaces ofrecidos no tenían que ver con el correo que se recibía. Por ejemplo en el correo se menciona una red social pero en enlace lleva a publicidad o anuncios de productos farmacéuticos (técnica ampliamente utilizada por *spammers*)

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

El crecimiento de archivos dañinos en este grupo con respecto al primero, indica una clara intención por parte del delincuente: obtener información sensible a través de cualquier método y no solo a través del ingreso del usuario a un sitio web falso. La tasa de correos que contienen archivos adjuntos representa un porcentaje importante porque los delincuentes intentan infectar al usuario con troyanos bancarios, los cuales enviaran información de cualquier entidad a la que ingrese la víctima. Es decir que con un correo y una infección se logran varios objetivos, como lo demuestra el análisis de varios troyanos de este tipo, realizados por **Segu-Info** durante el año [1].

Si se analizan el grupo total (384 correos), resultan lo siguientes números:

- El 89,58% de los correos estaban en idioma español; 9,90% en portugués y orientado a entidades de Brasil y; el resto 0,52% (2 casos) en inglés.
- 77,86% contenían imágenes
- 31,25% contenían enlaces acortados a través de alguna herramienta *online*
- El 4,94% no contenía enlaces en el cuerpo del mensaje
- Sólo 4,68% de los casos no mencionaba a una empresa, organización o entidad conocida
- Sólo 1,04% (4 correos del total) no contenía errores de ortografía o gramaticales (¡un logro importante!)
- Ningún sitio utilizaba HTTPS, por la complejidad relacionada al proceso

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

El contenido de imágenes en los correos para lograr un engaño efectivo es un anzuelo clásico pero, que un tercio de los correos utilicen conocidos acortadores de URL, tendencia que creció en forma alarmante en la segunda mitad del año, indica que las organizaciones responsables de estas herramientas deben realizar un mayor esfuerzo para controlar su uso, como lo hemos expresado desde **Segu-Info** en varias ocasiones durante los últimos años [2].

Imagen 3 - Utilización de imágenes y acortadores

Por supuesto, los delincuentes siempre podrán crear sus propios acortadores pero, el bloqueo de dominios sospechosos es más sencillo que el bloqueo de uno conocido como *t.co*, *bit.ly* o *goo.gl*, ampliamente utilizados por los usuarios, quienes ya confían sin reservas en ellos.

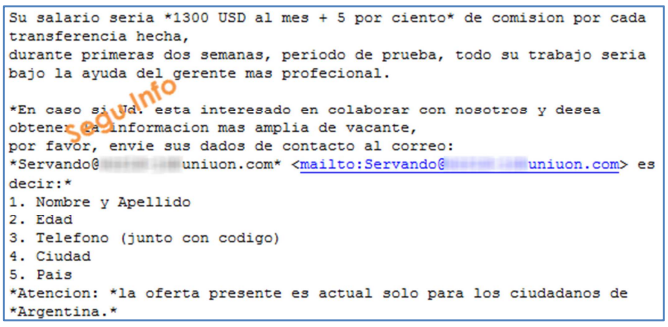

Imagen 4 - Scam

En aquellos mensajes que no contienen enlaces, ni adjuntos, ni imágenes (los que podrían llamarse *scam* puro) el método para robar la información es mucho más sencillo: simplemente se solicita al usuario que responda el correo con la información solicitada.

Ganancias económicas del delincuente

Para el delincuente, todo lo analizado tiene un solo objetivo: obtener el mayor rédito económico a través de la información recolectada de las víctimas. Este objetivo puede cumplirse básicamente de las siguientes maneras:

- Venta de la información a otros delincuentes en el mercado negro. En este caso la información cotiza de acuerdo al grado de plenitud y exactitud (no es lo mismo una base de datos con el nombre de usuario y contraseña que aquella que además contiene el número de tarjeta de crédito y su PIN). Sólo para tener una idea, los datos de una tarjeta de crédito clásica pueden ser vendidos a un promedio de U$S 10 y aumentar de acuerdo al tipo de tarjeta (*gold*, *platinum, black*, etc.)
- Extracción de dinero de las cuentas obtenidas y movimiento del mismo a través de la utilización de mulas. Los montos extraídos (del rango de U$S 30 a 300) generalmente no son demasiado altos y se evita el vaciado de la cuenta, de forma de minimizar la probabilidad de que la víctima se percate y efectúe la denuncia.

- Realización de compras con la información obtenida y a través de canales virtuales que no soliciten la presencia del titular o de su documentación. En este tipo de fraude es común la compra de crédito para líneas de teléfono móvil.
- Robo de identidad para lograr que una persona adquiera beneficios y productos que la víctima deberá abonar o, para cometer delitos de mayor monto en nombre de otro.

Se llama **mula** a la persona que facilita su cuenta bancaria para realizar movimientos de dinero obtenido de transacciones fraudulentas. Este tipo de acción, calificado como "lavado de dinero", generalmente se realiza a través de la captación de víctimas con ofertas de trabajos sencillos y demasiado bien remunerados *("trabaje 2 hs desde su casa y gane $5800")*.

A continuación se analizan algunos de los casos de phishing en los que fue posible conocer la cantidad de clics que los usuarios realizaban sobre el correo fraudulento así como la cantidad de ellos que ingresó su información personal y financiera: la posible ganancia del delincuente [3].

En el primer caso analizado, la cantidad de visitas al sitio fraudulento fue de 1.604 clics en 16 horas, lo que equivale a casi **2 ingresos por minuto**.

En el siguiente caso, la cantidad de visitas al sitio falso fue de 1.968 pero muchas personas habían repetido el ingreso para verificar el sitio o convencidas de que el mismo era real. Si se eliminan esos ingresos repetidos quedan **1.047 usuarios únicos (IP únicas)** y si se realiza un filtrado de los usuarios que ingresaron su información personal y sus datos bancarios reales, se obtienen **132 víctimas**. Es decir que el **12,6% de los usuarios que ingresaron al sitio falso, además le brindaron sus datos personales al delincuente**.

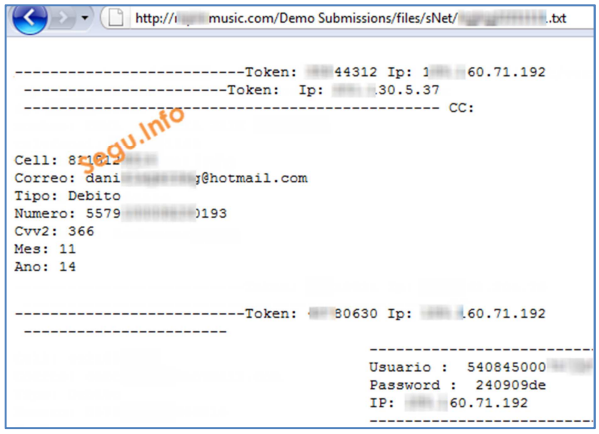

Imagen 6 - Datos robados a la víctima

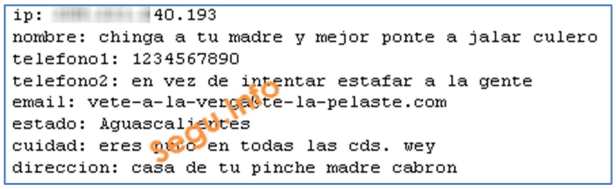

Imagen 5 – Mensaje "alegórico" al *phisher*

En el último caso un delincuente había creado tres sitios falsos de la misma entidad financiera en 10 días y había logrado **1.325 clics** entre de usuarios engañados. Si el 12% de los usuarios ingresó sus datos, el delincuente logró al menos 159 cuentas válidas. Suponiendo, en forma optimista, que el *phisher* sólo robó U$S 30 de cada cuenta obtenida, **estaría logrando al menos U$S 4.770 en 10 días "de trabajo"**, un número para nada despreciable considerando que es una actividad que se puede realizar en los tiempos libres y con un esfuerzo casi nulo.

Conclusiones

Las actividades informáticas delictivas están en pleno auge en América Latina y representan un área en crecimiento, con técnicas que van de las más simples y clásicas a otras que están siendo probadas y mejoradas constantemente, en aquellos casos que representan vectores de ataque con mayor porcentaje de éxito.

Algunos de los correos analizados durante el año se han cobrado una mayor cantidad de víctimas que otras, debido a lo específico de las técnicas de ingeniería social utilizadas y al sentido de oportunidad del delincuente y de su experiencia en el campo.

Estas actividades son altamente redituables para los delincuentes y con las tasas de crecimiento de usuarios conectados a Internet y al sistema financiero *online*, tienen cada vez mayor cantidad de potenciales víctimas.

Debe entenderse que todas las empresas y organizaciones de la región, independientemente del país al que pertenecen, son potenciales víctimas de este tipo de fraudes y es necesario emprender acciones legales, judiciales y técnicas en forma urgente para detener el crecimiento de esta actividad.

Es necesaria la implementación de mayor cantidad de controles proactivos por parte de las organizaciones y entidades afectadas así como la realización de campañas de concientización orientadas a que los clientes entiendan que son responsables de las actividades que realizan con sus cuentas en sus computadoras.

Referencias

[1] Troyanos bancarios
http://blog.segu-info.com.ar/2011/12/correo-falso-de-banco-galicia-trae.html
http://blog.segu-info.com.ar/2011/12/vuelven-las-fotomultas-con-malware-con.html
http://blog.segu-info.com.ar/2011/12/malware-en-postales-falsas-de-gusanito.html

[2] Uso de acortadores como engaño
http://blog.segu-info.com.ar/2010/07/nueva-tecnica-de-phishing-abusa-de.html
http://blog.segu-info.com.ar/2011/02/cantidad-de-descargas-de-malware-desde.html
http://blog.segu-info.com.ar/2011/02/500-infectados-en-2-horas-utilizando.html
http://blog.segu-info.com.ar/2010/04/la-inseguridad-de-los-acortadores-de.html
http://blog.segu-info.com.ar/2009/07/abuso-de-acortadores-de-url.html
http://blog.segu-info.com.ar/2011/12/correos-propagan-malware-en-dropbox-con.html

[3] ¿Cuánto gana un phisher?
http://blog.segu-info.com.ar/2011/02/cantidad-de-ingresos-un-sitio-de.html
http://blog.segu-info.com.ar/2011/02/los-numeros-del-phishing-ii.html
http://blog.segu-info.com.ar/2011/03/los-numeros-del-phishing-iii-400.html
http://blog.segu-info.com.ar/2011/11/cuanto-gana-un-phisher-numeros-del.html
http://blog.segu-info.com.ar/2011/11/cantidad-de-visitas-en-casos-de.html