Informe de Phishing 2013

22 de diciembre 2013

Por tercer 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 tercer 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 (20131222)
Descarga: www.segu-info.com.ar

Versión	Fecha	Cambios
1.0	22/12/2013	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 2013, en **Segu-Info** se recibieron más de **1000 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 **806 denuncias** correspondientes a phishing[1], que pretendían obtener información sensible del usuario y que podían o no contener archivos adjuntos.

[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

Esta cantidad representa un 23% más que en el año 2012 (657) y 110% más que en 2011 (384).

Considerando que un mismo caso puede ser denunciado varias veces por diferentes usuarios, al agrupar las 806 denuncias, se obtiene un total de 330 casos únicos. Dependiendo la entidad y el grado de propagación del correo, se recibió desde una hasta un máximo de 15 denuncias por caso.

De los 330 casos únicos, 287 corresponden a phishing tradicional (86%), 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 43 casos restantes corresponden a correos con archivos adjuntos y/o que contienen enlaces para descargar archivos dañinos (malware).

Las entidades afectadas han sido las siguientes:

American Express	Banco Davivienda	Banco Macro	Bradesco
Banamex	Banco de Costa Rica	Banco Mutualista Pichincha	Citi
Banco Agromercantil	Banco de Guayaquil	Banco Patagonia	Citibank
Banco Av Villas	Banco de la Nación	Banco Santander	Mastecard
Banco BaPro	Banco de Venezuela	Banco Santander Rio	Mercado Pago
Banco Caja Social	Banco do Brasil	Bancolombia	Pago Mis Cuentas
Banco COMAFI	Banco HSBC	BBVA Bancomer	Paypal
Banco Consorcio	Banco ICBC	BBVA Continental	Visa
Banco CrediChile	Banco Itau	BBVA Francés	

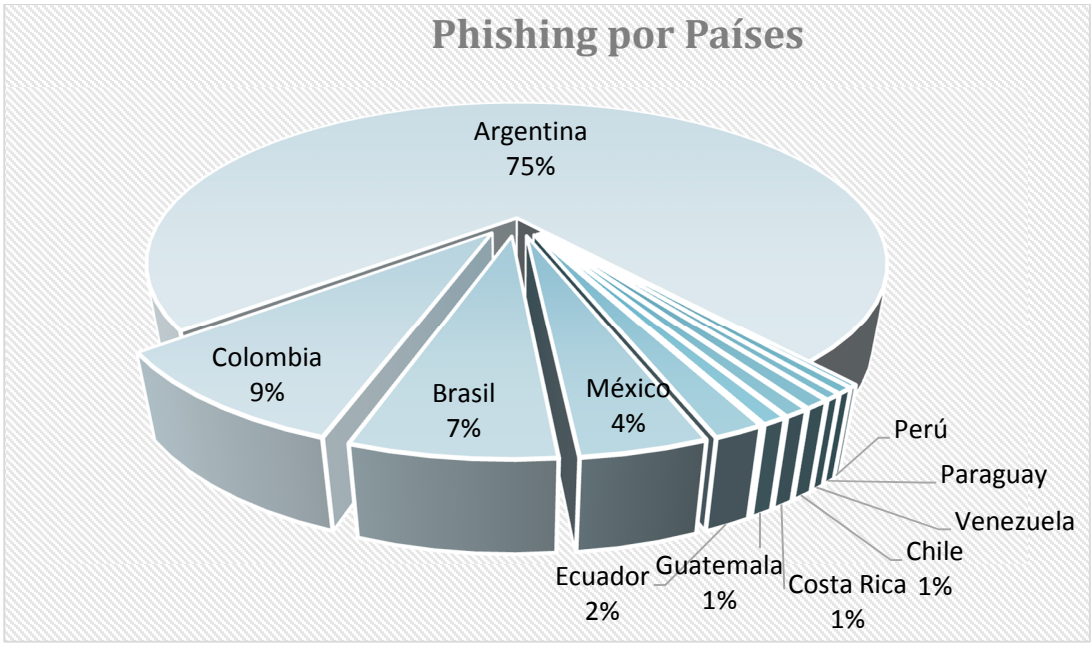
Nota: no se informa los porcentajes de afectación a fin de no dañar la imagen de las entidades mencionadas y tampoco suministrar información que pueda orientar a los delincuentes a planear de mejor manera sus ataques.

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

Claro	Google Docs
Documentación Falsa (*)	Hotmail/Outlook
Edatel	Movistar
Facebook	Personal
Fedex	Twitter

(*): Documentación falsa corresponde a multas, fotomultas, contratos laborales, envíos de productos y las noticias falsas que 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.

Con respecto a los países de América Latina afectados, el porcentaje de cada uno de ellos es el siguiente:



El porcentaje sobresaliente de Argentina corresponde a la gran cantidad de lectores que **Segu-Info** tiene en dicho país, motivo por el cual la confianza en el sitio hace que gran cantidad de denuncias provengan de allí.