

# 14 MESES DE OBSERVACIÓN DEL PHISHING EN MEXICO

MC. Helios Mier Castillo

GREX Tecnologías de Información San Luis Potosí

helios.mier [en] grex.com.mx

## Abstract

Por un tiempo de 14 meses se realizó una actividad de observación activamente estableciendo una red de captura de correos asociados a intentos de phishing que nos permite definir un perfil sobre la actividad criminal del phishing en México, las estrategias y técnicas, así como una noción acerca de los grupos que los originan.

Se han obtenido una cantidad de muestra de correos de diversas campañas de phishing que presenta un predominante modus operandi y técnicas de explotación frecuente, al mismo tiempo que se perfila una posibilidad de crear a gran escala un servicio de detección sobre ataques de phishing que permita integrar a diversas organizaciones y tecnologías para enfrentar con mayor eficacia los ataques de phishing.

## I Antecedentes

La técnica de fraudes por medio de Phishing es una amenaza de seguridad para las personas y las empresas que de forma global se está incrementando [1].

La clave del éxito de los ataques de phishing radica en primer medida en lo convincente del mensaje para engañar a la víctima, y en segunda medida por la efectividad y tipos de mecanismos de protección establecidos en los sistemas. [2]

Es posible establecer una adecuada configuración de seguridad de un sistema para enfrentar efectivamente el segundo factor de la amenaza [3], pero el primer factor depende de la educación del usuario de Internet con respecto a la seguridad en línea y en operaciones de banca electrónica, de manera que hay la necesidad de enseñarle al usuario a poder distinguir los intentos de phishing para que sea él mismo quien evite caer en ellos.

En base a experiencias profesionales previas para la detección de códigos maliciosos [4] y labores de alertamiento oportuno sobre riesgos de seguridad informática en Internet [5], se inicia como un proyecto secundario de nuestra empresa para complementar las fuentes de información confiable de nuestros clientes y sociedad en general, iniciando en una fase de prueba interna en Agosto de 2008 y emitiendo alertas públicas periódicas a partir del la segunda quincena de Octubre 2008 [6] concluyendo un primer

ciclo de observación en Noviembre de 2009.

## II Objetivo del servicio

Se busca lograr la educación del usuario de internet para lograr identificar las situaciones de phishing que pudieran presentarse por medio de la presentación de ejemplos de las temáticas y formas usadas en los ataques:

- Generar periódicamente un boletín que describa de forma general y simplificada las temáticas usadas en los mensajes de phishing contemporáneos, y proporcionar ejemplos visuales de algunos de ellos.
- Advertir de ser necesario sobre otros riesgos y amenazas de seguridad informática notables.
- Hacer recomendaciones y mejora de hábitos al usar Internet orientados a reforzar el conocimiento en diversos aspectos de seguridad y privacidad personal, familiar y organizacional en línea.
- Crear una lista de correo de acceso abierto para la distribución de las alertas
- Crear un repositorio de acceso público en internet para consultas de referencia y verificación de autenticidad de los comunicados.
- Obtener un punto de vista sobre la capacidad de los antivirus para detectar archivos binarios relacionados al phishing mexicano.

## III Recolección de datos y muestras

Se establecieron distintos vectores de recolección de reportes de phishing, mensajes en circulación y muestras de código malicioso:

- Correos sospechosos que se reciben directamente en los buzones personales de los integrantes de nuestra empresa.
- Deliberadamente en nuestros sitios web se publicaron direcciones de correo electrónico para alimentar intencionalmente los web spiders usados por spammers. Estas direcciones de correo algunas de ellas imperceptibles al a vista se incrustan ocultas dentro de paginas web personales y de voluntarios.
- Archivos y correos directamente extraídos de

las computadoras involucradas en un incidente cuando nos llaman a participar en la atención a un incidente y como opinión técnica en un proceso legal.

- Durante los servicios de mantenimiento técnico a los clientes de nuestra empresa, se tiene la oportunidad de recolectar muestras de códigos de computadoras que hayan sido atacadas en algún momento.
- Personas conocidas entre amigos y clientes que voluntariamente envían algún correo o archivo sospechoso que recibieron para que les demos una opinión profesional.
- Consulta de otras fuentes de información en línea como centros de estudios de seguridad y diarios de noticias.

Particularmente nos interesa observar actividad de phishing directamente dirigida a empresas e instituciones mexicanas, pero también documentar las dirigidas a afectar organismos de otras regiones.

#### IV Cotejar información

Al momento de recolectar un correo sospechoso o una muestra de código se realizaron los siguientes procedimientos para obtener más datos:

- Verificar el estado activo de links y sitios involucrados en el correo sospechoso para determinar si el ataque está en progreso o si ya fue desarticulado de alguna manera.
- Consultar reportes en Proyecto Malware de la UNAM para comparar capturas.[7]
- Verificar los binarios capturados en VIRUSTOTAL.COM para conocer el estado del reporte y capacidad de detección e interceptación de los programas antivirus en el momento de la recolección.
- Realizar pruebas de ejecución de los binarios sospechosos en ambiente controlado para determinar la carga dañina y comparar con otras técnicas de ataque.

#### V Diseminación de información

En caso de que un correo capturado o binario malicioso se encuentre relacionado con sitios en internet y enlaces activos del ataque en estado vigente, se notifica inmediatamente por correo electrónico a un buzón de reporte de la unidad de Policía Cibernética de la Secretaría de Seguridad Pública Jalisco, para que puedan realizar sus labores de desarticulación del ataque y desactivación de los sitios involucrados.

Se sabe que la unidad de policía cibernética posteriormente notifica al proyecto Malware y

unidades de combate al e-crime de instituciones bancarias. [8]

Correos sospechosos que no puedan ser verificados su autenticidad se reportan de igual manera a la unidad de Policía Cibernética de Jalisco para que sean cotejados.

#### VI Estadísticas

Se recopilaron un total de 36 ocurrencias de correos de 29 variantes de ataques.

Mes	Ocurrencias	Variantes
Octubre	1	1
Noviembre	2	2
Diciembre	2	1
Enero	3	3
Febrero	3	3
Marzo	3	2
Abril	4	4
Mayo	2	2
Junio	4	4
Julio	5	3
Agosto	3	2
Septiembre	2	1
Octubre	1	0*
Noviembre	1	1

Tabla 1 – Relación de capturas de correo por mes  
\* Se repitió una variante vista con anterioridad

Adicionalmente hubo una gran cantidad de correos catalogados como SPAM puesto que no estaban específicamente orientados a lograr un acceso a cuenta alguna que maneje algún tipo de valor monetario.

De estos totales, 24 variantes estaban orientados a afectar instituciones y usuarios mexicanos y 5 a atacar alguna organización en algún otro país.

De los correos capturados, en 3 casos se encontraron que el ataque se encontraba en progreso puesto que todos los enlaces para descarga de binarios maliciosos y sitios web suplantados aún estaban en línea y funcionando. 2 afectaban a instituciones mexicanas y 1 a una institución brasileña.

#### VII Patrones de conducta detectados

Se observan mensajes que reiterativamente buscan presentar a la potencial víctima el comunicado de una noticia sensacionalista procedente de alguna cadena de noticias de reconocimiento nacional suplantando

identidad gráfica y de formato tomando como tópicos alguna referencia a algún personaje de la farándula o política en situaciones de carácter escandaloso ya sea de tipo erótico, muerte o enfermedad o grabaciones inculpativas.

Dentro de este contexto, se observó que se repetía el patrón de conducta puesto que algunos de los tópicos usados en estos mensajes de phishing ya habían sido observados tiempo atrás al periodo que cubrimos. Sin embargo, nuevas variantes del mismo mensaje solo cambiando nombres de personajes famosos aparecieron en su mayoría todos ellos referentes a la cultura contemporánea y social mexicana.

También debido a la emergencia sanitaria internacional que se presentó debido al virus H1N1, este tema así como las alertas sobre desastres por fenómenos naturales fueron aprovechadas suplantando la identidad de agencias de gobierno, tal y como era esperado de acuerdo a patrones de conducta ya conocidos [9]

Se tiene también la captura de correos referentes al envío de tarjetas animadas de carácter general como cumpleaños, buenos deseos, pero también dependiendo de la época del año, mensajes de San Valentín, halloween y navidad entre otros.

A inicios del 2009 se presentaba en el país un cambio en las leyes tributarias de manera que algunos mensajes se disfrazaban como actualización de herramientas o manuales de ayuda para adaptarse a los nuevos regímenes fiscales, provenientes suplantando la identidad de la autoridad tributaria mexicana SAT o de alguna firma de asesores fiscales que no podía probarse si existía o no.

Se recopilaron escasos correos también dirigidos a atacar instituciones sudamericanas o españolas, que por el idioma, y nombre de las instituciones si se reconocía inmediatamente que no eran mexicanas.

Un tipo de correo que se presentaba con frecuencia fue el referente a la supuesta aparición de posibles métodos para obtener créditos gratuitos para líneas de telefonía celular.

También se observó la aparición constante de un mensaje donde invitaba al usuario a obtener versiones actualizadas y gratuitas de programas de seguridad y antivirus auspiciados por la compañía de Teléfonos de México a través de su línea de negocios de acceso a internet.

Hubo también mensajes relativos a ver supuestos videos sobre los últimos momentos de la muerte de Michael Jackson.

De los tópicos que los correos se observaron como parte de la ingeniería social aplicada figuran:

- Sobre escándalos de carácter erótico sobre alguna celebridad de la farándula o la política.
- Notas anunciando la muerte repentina de alguna celebridad.
- Falsas notificaciones sobre actualización de herramientas o manuales de ayuda de la Secretaría de Administración Tributaria mexicana relacionadas con los recientes cambios de la ley fiscal.
- Tarjetas de felicitación y cumpleaños.
- Oferta de herramientas o métodos para obtener de forma gratuita créditos para telefonía celular.
- Alertas de parte de varias autoridades mexicanas y manuales de sobrevivencia contra la emergencia sanitaria H1N1.
- Correos donde explican que se encuentran en una situación precaria y solicitan urgentemente trabajo enviando como archivo adjunto su curriculum vitae.
- Solicitudes de colectas y donativos para beneficiar a supuestas víctimas de desastres naturales.

#### VIII Tipos de phishing y técnicas de explotación

En cuanto a los tipos de correos formando parte de un ataque de phishing:

- Correos con enlaces directos a sitios fraudulentos usando un URL malformado.
- Correos con enlace a la descarga de un binario malicioso posando como una utilidad de software.
- Correos con enlace a la descarga de un binario malicioso posando como un codec multimedia para ver un video.
- Correos con enlace a la descarga de un binario troyanizado posando como una tarjeta de felicitación animada.
- Correos con enlace a la descarga de un binario malicioso contenido en un ZIP posando como una herramienta actualizada o ayudas para operaciones de carácter fiscal de la Secretaría de Administración Tributaria (SAT) mexicana. [10]

En único caso, se detectó un correo que usaba la técnica de phishing de ocultar un hipervínculo hacia un sitio suplantado con un URL engañoso.

En la mayoría de los casos se buscaba que la potencial víctima descargara un archivo ejecutable malicioso que modificaba el archivo de HOSTS de

windows[11].

En un par de correos se detectó el intento de explotación de las vulnerabilidades recién descubiertas de MS Office. [12]

En un caso orientado a atacar una institución financiera sudamericana, se descargaba toda una aplicación destinada a ser interactiva con la víctima presentando un falso procedimiento de actualización de mecanismos de seguridad, engañando al usuario para alimentar sin darse cuenta toda la información de su procedimiento de autenticación basada en tablas de códigos.

## **IX Factores de riesgos**

Un factor común que se presentaba en computadoras que ya habían sido afectadas por un archivo malicioso fue la presencia de sistemas operativos muy anticuados, sin actualizaciones de seguridad, de carácter pirateado, y adicionalmente con sistemas antivirus de carácter pirata.

Por las costumbres en México de usar software ilegal, observamos una muy diversa cantidad de software antivirus con cracks que no permitían que se actualizarán realmente las firmas de detección así como los motores de detección, los cuales no podían lidiar con la detección del simple ataque de modificación de archivos de HOSTS de windows.

Debido a la característica de la principal técnica de phishing al modificar el archivo de HOSTS, la totalidad de las computadoras de nuestros clientes que fueron sometidas a una revisión, se encontraban con la configuración de tener una cuenta de usuario con privilegios de administrador como cuenta principal del sistema.

Muchos de los sistemas afectados que revisamos, se encontraban con un navegador de internet desactualizado, de forma que en cierto grado los usuarios no contaban con la posible protección que los mecanismos anti phishing que tienen muchos navegadores modernos [13], pero sin embargo, la razón por la que no actualizaban o no cambiaban a otra marca su internet explorer versión 6 o 7 era porque la versión 8 más reciente u otros navegadores no eran 100% compatibles con la aplicación de banca en línea que usaban.

## **X Perfiles de grupos y modus operandi**

De acuerdo a las observaciones, podemos clasificar a los posibles emisores de los correos de phishing capturados en tres grupos:

### *A.- Grupo nacional organizado*

Se puede identificar claramente un grupo de phishers mexicanos que basan su modus operandi por medio del envío masivo reiterado de correos buscando la descarga de un archivo binario malicioso que modifique el archivo de HOSTS de windows para redirigir a las víctimas a los sitios suplantados.

También un comportamiento notablemente común fue el de ver el alojamiento de su archivo malicioso en sitios públicos diversos que tuvieran un error de configuración, como foros de discusión, o en los comentarios de blogs.

### *B.- Grupos nacionales variados*

En otro grupo podemos clasificar a diversos phishers que no parecen tener alguna relación entre sí puesto que usan diversas técnicas conocidas de phishing y su actividad es muy baja comparada con el grupo principal de atacantes.

### *C.- Grupo internacional*

En este grupo mencionamos a todos aquellos phishers que buscaban afectar instituciones de otros países y que por alguna razón sus correos llegan a usuarios en México.

Entre ellos podemos distinguir que se atreven a realizar ataques más osados contra otras técnicas de protección de cada institución regional.

También entre los correos generados por estos grupos fueron los únicos donde se observaron binarios maliciosos más avanzados como keyloggers y rootkits.

## **XI Caso de estudio de respuesta rápida**

En uno de los casos se recibió un mismo mensaje evidente de phishing en dos buzones de correo distintos con apenas 40 minutos de diferencia a temprana hora del día con la temática de descargar un programa para añadir créditos para telefonía celular.

Al hacer click en los vínculos se descargó un archivo malicioso que se encontraba hospedado en un sitio extranjero con el sistema phpBB de foros de discusión, al parecer el atacante logró obtener una cuenta de usuario en ese sitio que le permitía almacenar archivos a discreción en ese servidor, los cuales solo establecía el hipervínculo HTML en los mensajes de correo que enviaba.

Ambos correos provenían desde un servidor con dirección IP en Ucrania cuya etiqueta de remitente

había sido falsificada con el nombre la compañía de telefonía celular.

Se descargó el archivo binario y fue ejecutado dentro de un sistema windows virtualizado, el cual efectivamente modificó el archivo de HOSTS del sistema, donde se añadieron 7 registros de dominios de una misma institución bancaria BBVA Bancomer y por cada una de ellas se registraban varios subdominios de diversas paginas que conformaban su servicio de banca en línea.

Las direcciones IP insertadas en el archivo de HOSTS por cada institución bancaria afectada apuntaban a un hospedaje en Estados Unidos, a los cuales pudimos acceder y verificar que se encontraba una pagina suplantada de un banco que respondía de forma interactiva a las acciones del usuario y buscando que la víctima escribiera las claves de su cuenta y de su token de One Time Password.

Adicionalmente se envió el binario malicioso al servicio público de análisis de VirusTOTAL, arrojando que a pesar de la sencilla técnica de modificar el archivo de HOSTS de windows en una cuenta con privilegios de administrador, solo 13 de los 45 antivirus listados y actualizados al día pudieron reconocer el ataque o levantar alguna bandera de advertencia.

En ese mismo momento se notificó a la Policía Cibernética del estado de Jalisco que habíamos capturado los primeros mensajes de una nueva campaña de phishing puesto que todos los sitios que conformaban el ataque se encontraban en línea, recibimos un correo de confirmación que revisarían el reporte.

Ese mismo día aproximadamente a las 18:30 hrs., se revisó de nuevo la disponibilidad los sitios, tanto de donde se descargaba el archivo malicioso así como del sitio falsificado del banco, pero sin embargo, ignoramos si el cierre de esos sitios se debió a la intervención de la misma policía cibernética puesto que acostumbran no informar sobre el resultado de un reporte.

## **XII Caso de estudio de nuestro anuncio en sección amarilla**

Durante el periodo de 2009 nuestra empresa contrato el servicio de publicación en la Sección Amarilla correspondiente al estado de San Luis Potosí, para lo cual se creo un único buzón de correo que fue publicado de forma exclusiva en ese anuncio.

Esperabamos que tarde o temprano esa dirección de correo electrónico fuera recopilada por spammers locales e incluida inevitablemente en bases de datos

para mercadotecnia de SPAM por internet.

En dos ocasiones se recibieron en ese buzón exclusivo mensajes de phishing, lo cual es una prueba de que los delincuentes de phishing mexicanos estan alimentando sus bases de datos constantemente de las bases de datos de direcciones de correo que manejan los spammers de internet.

## **XIII Retroalimentación de subscriptores**

De nuestros clientes, colaboradores y amigos que formaron parte de este servicio, se recibieron diversos comentarios:

- Nuestros clientes que habían sido víctimas ya de un ataque de phishing comentaron que han aprendido a sospechar y evitar mensajes que concuerdan con los ejemplos de correos y temáticas similares.
- Clientes y colaboradores que nunca se han enfrentado a una situación de phishing, indicaron que podían reconocer mensajes evidentemente sospechosos, pero que algunos de los ejemplos mostrados si les parecían impresionantes y que si reconocían que habría una posibilidad de que cayeran en el engaño.
- Todo tipo de personas nos comentaron que aunque se apreciaba la información, si sentían que con el paso del tiempo y el envío de multiples mensajes, llegaba un momento en que ya los boletines no se revisaban en su totalidad.

## **XIV Conclusiones**

Con una red de captura modestamente conformada se lograron interceptar los mensajes de dos campañas de phishing dentro de las aparentes 24 horas de su inicio y reportar a la autoridad para su desarticulación inmediata, tenemos una buena pauta para teorizar que una red de captura activa de carácter nacional podría ofrecer muy buenos resultados para la rápida detección y desarticulación de un ataque de phishing perpetrado por delincuentes mexicanos dentro de las primeras 24 horas del inicio de la campaña de envío masivo de correos.

Cabe destacar que no se observó ninguna técnica de phishing dirigido a instituciones mexicanas que involucrará la instalación de un rootkit o una modificación más severa de algun componente del sistema operativo excepto el archivo de HOSTS de windows.

Podemos concluir que una de las principales técnicas que habrá para mitigar el riesgo ser víctima de un

ataque de phishing contra instituciones bancarias mexicanas serán aquellos mecanismos orientados a evitar la modificación de archivos de configuración del sistema operativo windows, siendo el más simple de todos el de tener cuentas sin privilegios de administrador.

Aunque de hecho se recolectaron muestras de archivos binarios con técnicas de intrusión mucho más avanzadas, todos ellos estaban asociados a un gusano o rootkit de mayor notoriedad y de características globales y ataques no dirigidos en su vector de ataque como botnets y spyware.

## XV Trabajos futuros

Se tuvo dificultades después de un tiempo para el mantenimiento de los buzones de correo donde se recopilaban los correos, puesto que también la técnica de recolección logro atraer una gran cantidad de mensajes de SPAM que saturaban las cuotas de disco.

El proveedor de hosting de nuestros buzones también se inconformó por la presencia de multiples mensajes en un solo lugar que activaban las alertas de los sistemas de detección de intrusos y de filtrados contra mensajes maliciosos, de forma que las cuentas de correo que usabamos en algunos momentos fueron suspendidas por el proveedor argumentando que violaban los terminos del servicio.

De manera que para poder continuar con el servicio de captura de correos y de envío de boletines, se requiere contar con infraestructura propia para evitar complicaciones con agentes terceros y tener el control completo de la entrada y salida de mensajes.

Se requiere también mejorar el mecanismo de entrega y formato de notificación, puesto que si bien se buscaba notificar de una manera directa y sencilla la información, con el paso del tiempo el suscriptor ya no apreciaba ni aprovechaba la información de la misma manera.

Consideramos de manera preocupante el ver la capacidad de los antivirus conocidos para detectar y detener un archivo malicioso creado de forma regionalizada que utilice una técnica de intrusión simple sobre el archivo de HOSTS, de forma que la comunicación formal constante con las casas desarrolladoras de productos antivirus y los servicios

de protección antiphishing de los navegadores de internet para asegurar que cuenten con capacidad de lograr este nivel de detección brindará en lo general a los usuarios de la banca en México un mejor nivel de protección.

## XVI Referencias

- [1] Estadísticas de reportes de incidentes, UNAM CERT <http://www.cert.org.mx/estadisticas.dsc>
- [2] How phishing works, Phishing Info , <http://www.phishinginfo.org/how.html>
- [3] Emig, Aaron, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005
- [4] Mier, Helios, Combatiendo códigos maliciosos desconocidos en una red institucional: un procedimiento basado en honeypots y honeytokens, Congreso de Seguridad en Computo, UNAM, 2004
- [5] Mier, Helios, Servicio de Alertas de Seguridad Informática , INTERCON X, Universidad Nacional del Callao, 2002
- [6] Boletines GREX de seguridad, <http://www.grex.com.mx>
- [7] Proyecto Malware UNAM-CERT, <http://www.malware.unam.m>
- [8] Policía Cibernética SSP Jalisco México, <http://www.jalisco.gob.mx>
- [9] OpenDNS PhishTank project, <http://www.phishtank.com/>
- [10] Servicio de Administración Tributaria México, Alerta de seguridad antiphishing, [http://www.sat.gob.mx/sitio\\_internet/plataforma/132\\_1\\_2466.html](http://www.sat.gob.mx/sitio_internet/plataforma/132_1_2466.html)
- [11] Olzak, Tom, DNS Cache Poisoning: Definition and prevention, 2006
- [12] Microsoft Security Bulletin Summary for June 2009, <http://www.microsoft.com/technet/security/bulletin/ms09-jun.mspx>
- [13] Internet Browser Anti-phishing Protection, <http://www.worldstart.com/tips/tips.php/3183>



### Mc. Helios Mier Castillo

Consultor en Seguridad de redes y sistemas de información con publicaciones y conferencias en foros nacionales e internacionales, así como catedrático en cursos de grado y postgrado. Ha desarrollado proyectos de seguridad informática en el sector público, privado y académico. Ha sido colaborador y asesor de grupos de combate a crimen cibernético, procesos electorales y atención a víctimas de delitos informáticos.