



# OWASP - 14 Meses de observación del Phishing MX

Msc. Helios Mier Castillo  
GREX Tecnologías de Información  
Helios.mier en grex.mx  
(+52 444) 138 9342

**OWASP**  
Noviembre 2011

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**  
<http://www.owasp.org>

---

# Title

- Antecedentes
- Objetivo
- Metodología
- Resultados
- Casos de estudio
- Trabajo futuro
- Hechos recientes
- Conclusiones

# Antecedentes

- El Phishing está presente de una manera insistente en México.
- Desde los primeros días de la banca por internet.
- Se han introducido los Tokens de One Time Password, sin embargo, aún sigue ocurriendo incidentes.
- Conocer al enemigo ayuda a enfrentarlo, pero ¿cuál es el perfil, herramientas, tácticas y motivos?

# El Phishing

- El robar las credenciales de autenticación de alguien engañándolo para que las introduzca en un sitio que aparenta ser el que el usuario utiliza.
- Componente técnico
  - ▶ El procedimiento y herramientas a nivel tecnológico.
  - ▶ Tanto del lado de las víctimas y el atacante.
- Componente psicológico
  - ▶ La ingeniería social aplicada para engañar al usuario.
- Del lado técnico hay mecanismos de protección.

## Objetivo

- Crear un servicio de información que ayude al usuario a enseñarse a identificar las situaciones de phishing.
  - ▶ Generar un boletín periódico via e-mail.
  - ▶ Mostrarle cuales son las campañas de phishing vigentes.
  - ▶ Advertir de riesgos informáticos.
  - ▶ Hacer recomendaciones y mejora de hábitos.
  - ▶ Crear un repositorio de consulta de boletines.
- Obtener un punto de vista sobre la capacidad de los antivirus contra el factor técnico de phishing.

# Recolección de datos y muestras

- Se recolectaron correos de phishing a través de los siguientes vectores:
  - ▶ Correos recibidos directamente en buzones personales.
  - ▶ Correos enviados por conocidos que recibían algo sospechoso y querían colaborar en la investigación.
  - ▶ Correos extraídos de buzones de personas que fueron víctimas de phishing y pedían nuestra consulta.
  - ▶ Correos extraídos de PCs que llegaban a nuestro taller de mantenimiento y limpieza de malware.
  - ▶ Deliberadamente insertar cuentas en listas de spam.

# Email HoneyTokens

- Insertamos cuentas de correo escritas de froma clara en el HTML pero visualmente ocultas.
- Para que los web spiders usados para spam las capturen. Cerca de 30 cuentas expuestas.
- Creamos emails con nombres atractivos para el phishing: gerencia@ contabilidad@ pagos@ etc..



The image shows a screenshot of a webpage with a light blue circle highlighting a hidden email address in the HTML source code. The visible text on the page includes "COMPAC", "et", "is Web", "igo Abierto", "iento de", "Aplican n", "Adquiere", "Aviso: mantenimiento s", "COMPARTIR", and "AV".

```
<mailto:ventas@empresa.com>  
<font color=white size=1>  
ventas@empresa.com </font></mailto>
```

# Metodología

- Recolección de muestras de emails, archivos, imágenes y binarios sospechosos.
- Todos los emails se reenvían a un buzón único.
- Se verificaba el estado de links y sitios involucrados en el correo sospechoso:
  - ▶ Si estaban los sitios activos.
  - ▶ Si había interacción con el sitio suplantado.
  - ▶ Se ejecutaban los binarios en ambiente virtualizado.
- Se comparaba con los reportes de CERT-UNAM.
- Los binarios se revisaban en Virustotal.com

## Diseminación de información

- Al recibir un correo sospechoso se verificaban los enlaces.
- Si el correo descargaba binarios, se ejecutaban y se buscaban los cambios hechos al sistema.
  - ▶ En casi la totalidad de los casos solo ocurrieron cambios en el archivo HOSTS de windows.
- Si se encontraban sitios de phishing activos, enlaces a binarios publicados y con capacidad de interactuar con algún visitante, se reportaba a la Policía Cibernética de Jalisco.
- Correos que no se podían verificar se reportaban

# Boletín a subscriptores

- Publicación quincenal en web y a lista de correo.
- Enviar información simple, clara y ejemplos para que las personas reconocieran amenazas.

Se espera que conforme se acerca las temporadas de frío en el país, se incremente los fraudes relacionados a la epidemia de influenza H1N1 tanto dentro y fuera de internet.

## --- Alertas de Phishing ---

Para mantenerlos informados, en estos momentos circulan correos asociados con las técnicas de fraudes cibernéticos (phishing), de manera que les pedimos que no abran, no hagan click, ni reenvíen mensajes con la siguientes temáticas:

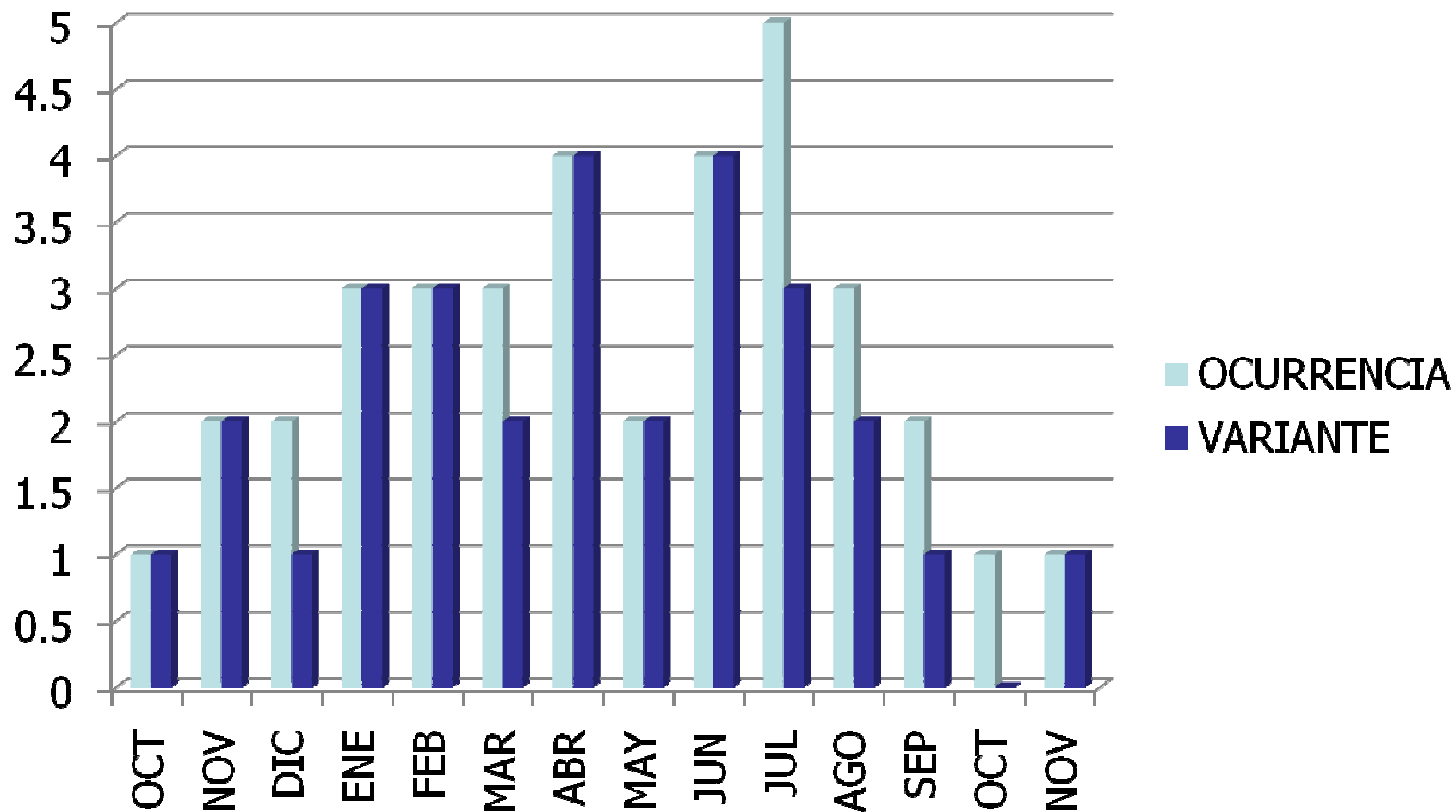
- \* Cualquier sitio de internet o correo electrónico que pretenda en relación con la epidemia de influenza:
  - venta de medicamentos, drogas o "curas milagrosas" contra la enfermedad.
  - venta o descarga de "guías infalibles" contra el virus.
  - Colectas, donativos o seguros para las víctimas.



## Estadísticas

- Gran cantidad de SPAM y gusanos. Muy demandante revisar correo por correo para determinar si era phishing o no.
- Se capturaron 36 correos de 29 variantes.
  - ▶ Algunas variantes se capturaron 2 veces.
- 24 variantes de phishing estaban dirigidas a potenciales víctimas en México.
- 5 variantes de phishing dirigidos a otros países.
- 3 variantes pertenecían a una campaña de phishing en curso. Sitios activos.
  - ▶ De las cuales 2 eran campañas en MX y 1 extranjera.

# Capturas de octubre 2008 a noviembre 2009



# Patrones observados



Muere el actor Roberto Gómez Bolaños a consecuencia de un paro respiratorio.

24-09-2008

México, D.F, 24 Septiembre. (LaCronica.com.mx - Notimex). El actor y productor mexicano Roberto Gómez Bolaños Cacho (n. 21 de febrero de 1929) falleció (sic), quien participó en diversas obras de teatro, filmografías, libros y películas, entre las cuales destaca El Chavo del Ocho, El Chapulín Colorado, El Chanfle y un gran sin número de producciones. Además de sus trabajos de ingeniero civil en la UNAM y Boxeador principiante, falleció este viernes a causa de un paro respiratorio.

[Ver Noticia](#)

En el siguiente vídeo se muestra también una entrevista con Carlos Villagrán y María

Aún le sobreviven su esposa



La cantante Rihanna se suicida tras escándalo con fotografías.

La cantante conocida en el ambiente de la música como Rihanna fue descubierta sin vida en su apartamento de New York. Las autoridades informan que el suceso probablemente se realizó tras el escándalo que se produjo tras el escándalo realizado por la filtración de unas fotos íntimas supuestamente tomadas por el cantante Chris Brown, donde la misma aparecía con poca ropa, mostrando posiciones sensuales al mismo tiempo que se tocaba sus partes más íntimas.

La cantante también conocida como la Madonna negra al parecer hizo uso de pastillas antidepresivas en exceso siendo éstas mismas las causantes de su fallecimiento. Espere más información

- Noticias sensacionalistas sobre algún personaje de la política o farándula.
  - ▶ Todos ellos invitando a ver un video al cual le faltaba un codec para poderlo abrir

Domingo en Michoacán .  
molicranía Vicente FOX - Santiago Creel - Eduardo Medina Mora.



CIUDAD DE MEXICO, Méx, 8 Jul. 2009 - En el video se ven a los señores funcionarios que en su momento recibían estos funcionarios por pertenecer a la Nomina del Cartel. Entre ellos el Ex Secretario de Gobierno Santiago Creel y el Ex Presidente de México Vicente Fox Quesada.

Y igual que los anteriores funcionarios también fueron señalados el actual Procurador General de la República Eduardo Medina Mora entre otros - [Escucha el Audio Original.](#)

14 de Octubre 2008

### El Narco Lanza Video con un Mensaje Dirigido al Presidente de la Republica.

En este video pueden apreciarse nombres de Altos Mandos de las Fuerzas Federales y Militares Vinculadas con el **Crimen Organizado**.



- Noticias sensacionalistas relativas a la violencia por el narcotráfico en México.
  - ▶ Usando la identidad gráfica de algún noticiero.
  - ▶ Se repetían en varias ocasiones con links renovados.

**TRANSMISIÓN EN VIVO**  
 www.PRESIDENCIA.gob.mx USTREAM



2135 Viewers / Broadcast

Canal ONCE TV, programa especial

[Descargar Video](#)

**Video Explicación y vacuna contra influenza.**  
 Tips para evitar la Influenza | Vacuna casera | Abril de 2009

Ante los constantes brotes del virus de la fiebre porcina, también conocido como influenza, el Gobierno Federal ha puesto en marcha nuevas medidas para abatirlo, ya que se ha declarado como epidemia total.

A continuación se muestra un video de los síntomas que puede presentar un paciente, desde cuando comienza hasta cuando muere.

Presidencia

Ante el inminente brote del virus de la fiebre porcina, también conocida como influenza, el Gobierno Federal ha puesto en marcha nuevas medidas para abatirlo, ya que se ha declarado como epidemia total a punto de convertirse en una pandemia mundial.

A través de este comunicado informamos a la población mexicana de los puntos críticos con más brotes de INFLUENZA además de los síntomas, prevención y los próximos puntos de vacunación para esta terrible enfermedad. La vacuna contra la influenza aún no es completada el 100% pero se estima que el día 6 de Mayo se habrá perfeccionado y será aplicada a la población mexicana sin costo alguno, por ello es necesario que registres tus datos para constatar las dosis necesarias que se aplicaran, ya que todo llevará un absoluto control, persona o familia no registrada ya sea por medio de Internet o en cualquier Centro De Salud Público, (CSA, IMSS) no será considerado y que para exento de esta vacuna, y solo se le aplicara si algún registrando faltara el día 6 de Mayo en el registro; por lo que le pedimos se registre para obtener su número y clave de control, con los cuales deberá acudir al lugar, fecha y hora indicados al momento de su registro, de este modo usted y/o familiares registrados serán vacunados y así evitaremos que este virus siga propagándose y causando más muertes.

Para obtener más detalles y conocer el modo que se utilizará para la aplicación de la vacuna haga [click aquí](#)

[Regístrate](#)

- Apelando a la buena voluntad o pánico del público sobre las emergencias en curso.
  - ▶ Este patrón se observa siempre en el malware.
  - ▶ Notablemente sobre la emergencia H1N1 y el huracán Wilma
  - ▶ También hubo correos de venta de medicinas falsas contra la gripe aviar.



- El envío de tarjetas de felicitación y animaciones referentes a las festividades del momento.
  - ▶ El sitio suplantado siempre era gusanito.com

## Software y Formas Fiscales

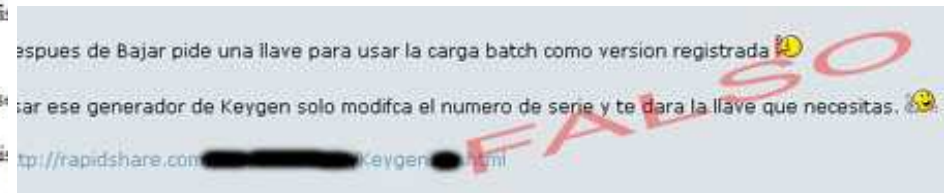
El SAT ha desarrollado diversas herramientas electrónicas para facilitar el cumplimiento de sus obligaciones, las cuales son gratuitas y pueden descargarse directamente desde este sitio.

También se enlistan las formas y formatos fiscales disponibles para consulta y, aquellos que indican que son electrónicos, pueden imprimirse considerando las indicaciones que ahí mismo se señalan. En esta sección encontrará las herramientas de cómputo que puede descargar e instalar en su equipo personal, permitiéndole cumplir con sus obligaciones fiscales de manera directa, rápida, sencilla, segura y cómoda.

Para obtener cualquiera de las herramientas de libre distribución, solo ponga el puntero sobre la opción deseada y se abrirá en una sola vez.

Ejemplo: Si usted necesita DEM Centros Cambiarios y de Transmisores de Dinero, solo de clic sobre el menú correspondiente.

- [Régimen de Micro, Pequeña y Mediana Empresa](#) Programa para ayudar micro, pequeña y mediana empresa en el cálculo de sus impuestos y el registro diario de sus operaciones.
- [Listado de conceptos del impuesto empresarial a tasa única, IETU](#) Para capturar y enviar la información y el Listado de conceptos que sirvió de base para calcular el IETU.
- [Listado de conceptos del impuesto empresarial a tasa única, IETU para empresas maquiladoras](#)



## ■ Relacionadas con novedades e información suplantando a la autoridad fiscal mexicana SAT.

- ▶ Nos pareció interesante que se enfocan hacia los usuarios que controlan los pagos en las empresas.
- ▶ Un mensaje hacia referencia a Cracks para programas de contabilidad.



- Para la obtención de créditos de telefonía celular.
  - ▶ Se observó en varias ocasiones, parece que realmente hay considerable número de víctimas que cae en este engaño.

## Antivirus

Con el antivirus gratuito de Ininitum, protege tu PC o Laptop de ataques de software dañino. Elimina eficientemente las posibilidades de contagio de virus y malware al estar conectado a Internet desde tu casa.

- ¡Olvídate de las infecciones!
- ¡Mantén a salvo tu seguridad!
- ¡Realiza tranquilamente operaciones bancarias y compras por Internet!

Servicio gratuito para clientes Ininitum.  
Precio normal \$49 al mes.

Instalar

[Registro para usuarios Telnet y Cuenta Maestra](#)

Departamento de Seguridad en Computo y el UNAM-CERT tiene como objetivo informar las amenazas de códigos maliciosos que se propaguen dentro



### ■ Invitación a actualizar o instalar falsas herramientas de seguridad.

- ▶ Se observó varias ocasiones uno relacionado al AV que ofrece Telmex.

A quien corresponda:

De mi mayor consideración ,

Estoy interesado en ser parte de un equipo que contribuya a un enriquecimiento interactivo entre vuestra em

Creo contar con los atributos necesarios para un buen desempeño y mi proyección a futuro.



in rric il mvitaa.doc

Hola,

Buen Día, quisiera saber si mi Abuelo era de : dicen que venía de allí, queremos estar para realizar un asunto legal que es de suma importancia exactamente, pero nos dicen que era de , pero algún municipio, su nombre era Felipe Gonzíe creamos que pudo haber sido registrado tambiín; sabemos, el nombre de la madre Guadalupe &iacute;e Gonzíe;les, naciíe, el 21 de Noviembre de : 1999, su esposa era &iacute;a del Carmen Segura C Norbertha, Miguel, &iacute;a del Rosaric, Federico Elida, Felipe y María del Carmen, todos de ap quisiera que me ayudaran para poder pedirles el acta

Saludos

## ■ Otros métodos

- ▶ Explotación de las vulnerabilidades descubiertas de Office en Junio 2009.
- ▶ Esto nos pareció muy avanzado con respecto a los otros correos y el patrón predominante.

## Técnicas de explotación

- Casi la totalidad de los mensajes buscaban descargar un binario ejecutable que modificaba el archivo HOSTS de windows.
- Un solo mensaje aplicaba enlaces ofuscados al sitio falso.
- Dos correos contenían un .DOCX con la vulnerabilidad MS09-junio de MS Office
- Un correo contenía una aplicación interactiva para capturar tarjetas de coordenadas de banco brasileño.

## El archivo de HOSTS

- En la campaña de phishing se colocaba un archivo ejecutable malicioso en algún sitio público (foros, bbs, etc.)
- Al ejecutar el archivo con permisos de administrador, se agregaban entradas estáticas suplantando los principales dominios de bancos mexicanos.
  - ▶ Particularmente BBVA y Banamex
- En varias ocasiones, los usuarios resultaban infectados, pero no sobre su banco habitual.

## Factores de riesgo

- Todos los sistemas infectados tenían como usuario principal una cuenta de administrador.
- PCs con sistemas operativos anticuados, particularmente sin navegadores modernos:
  - ▶ No cuentan con filtro anti paginas maliciosas.
  - ▶ No cuentan con restricción de ejecución de archivos descargados
- Malos hábitos de uso de internet y falta de mantenimiento preventivo de sistemas.
  - ▶ Un sistema afectado por phishing en HOSTS usualmente tenía otras infecciones.
  - ▶ El contar con software AV pirata tiene afectación.

# El factor Antivirus

Authentium	5.1.2.4	2009.07.13	-
Avast	4.8.1335.0	2009.07.13	-
AVG	8.5.0.307	2009.07.13	-
BitDefender	7.2	2009.07.13	-
CAT-QuickHeal	10.00	2009.07.10	-
ClimAV	0.94.1	2009.07.13	Trojan.Qhost-63
Comodo	1639	2009.07.13	UnclassifiedMalware
DrWeb	5.0.0.12182	2009.07.13	-
eSafe	7.0.17.0	2009.07.13	-
eTrust-Vet	31.6.6610	2009.07.13	-
F-Prot	4.4.4.56	2009.07.13	-
F-Secure	8.0.14470.0	2009.07.13	-
Fortinet	3.120.0.0	2009.07.13	Adware/ChangeHost
GData	19	2009.07.13	-
Ikarus	T3.1.1.64.0	2009.07.13	-
Jiangmin	11.0.706	2009.07.13	-
K7AntiVirus	7.10.791	2009.07.13	-
Kaspersky	7.0.0.125	2009.07.13	-
McAfee	5675	2009.07.13	QHosts-100!bat
McAfee+Artemis	5675	2009.07.13	QHosts-100!bat
McAfee-GU-Editron	6.8.5	2009.07.13	Heuristic.BehavesLike.Exploit.CodeExec.EPOD
Microsoft	1.4803	2009.07.13	-
NOD32	4240	2009.07.13	-
Norman	6.01.09	2009.07.13	-
nProtect	2009.1.8.0	2009.07.13	-
Panda	10.0.0.14	2009.07.12	Trj/CI.A
PCTools	4.4.2.0	2009.07.13	-
Prevx	9.0	2009.07.13	Medium Risk Malware
Rising	21.38.04.00	2009.07.13	-
Sophos	4.43.0	2009.07.13	-
Sunbelt	9.2.1858.2	2009.07.13	-
Symantec	1.4.4.12	2009.07.13	-
TheHacker	6.3.4.3.366	2009.07.12	-
TrendMicro	8.950.0.1094	2009.07.13	TROJ_QHOSTS.BB
YBA32	3.12.10.8	2009.07.12	-
ViRobot	2009.7.13.1833	2009.07.13	-



En las capturas de archivo binario malicioso que afectaba HOSTS, se analizaban en VIRUSTOTAL.COM para conocer la capacidad de Avs. Bastante bajo el porcentaje y con AV piratas aún más.

## Origen del phishing

- Por el modus operandi y el volumen de mensajes.
- Grupo nacional organizado
  - ▶ Sistemáticamente realizan la mayoría de las campañas enviando masivamente correos para distribuir archivos ejecutables que modifican el HOSTS de windows.
- Grupos nacionales varios
  - ▶ Diversas personas que no parecen tener relación entre sí puesto que se observan variadas técnicas y baja intensidad
- Grupos internacionales
  - ▶ Mensajes de phishing de habla hispana dirigido a organizaciones de otros países y que llegan a buzones MX
  - ▶ Usan técnicas mas avanzadas, como keylogger y rootkits.

## Caso de estudio: respuesta rápida a campaña

- 8 a.m. Al abrir los buzones de captura se registras dos correos idénticos de phishing recibidos con 40 mins de diferencia.
- Se revisan los enlaces, que descargan un archivo binario desde un foro en Ucrania.
- El archivo binario se ejecuta dentro de un windows xp sp3 virtualizado.
- El archivo de HOSTS es modificado añadiendo 7 direcciones IP estáticas a subdominios de BBVA.
  - ▶ Ningún otro cambio detectable en el sistema.

- Las direcciones IP apuntaban a un servidor en USA, donde se verificó que había un sitio suplantando a BBVA y que respondía a la interacción del visitante.
- El binario malicioso se reviso en VIRUSTOTAL con una respuesta positiva de solo 13 de 45 AV's
- Se envió un reporte de sitio de phishing activo a Policía Cibernética de SSP Jalisco.
- 18:30 hrs, se verifico que el sitio de phishing estaba fuera de línea.

## **Término del proyecto 14 meses después**

- Los buzones de correo recibían mucho SPAM, el proveedor de hosting no vió con buenos ojos los que pasaba y cancelo nuestra cuenta.
  - ▶ Se recupero el servicio pero ya no podiamos seguir, se eliminaron todos los buzones honeypot.
- El trabajo de revisar los correos se hizo muy demandante. Se consideró emitir un boletín semanal.
- Para mantener una mayor posibilidad de capturar correos, se tenía que expandir la red.
- Se necesitaba dedicar personal y recursos extra.
- Decidimos cerrar el ciclo, documentar e informar.



## Trabajo futuro

- Construir una plataforma dedicada a la recopilación de correos y colaboración de voluntarios. Independiente de un ISP/hosting.
- Distinguir la información entre campañas de phishing pasadas de las que se encuentran en curso.
- Recopilar más datos acerca del origen, fechas, objetivos y detalles técnicos de cada campaña de phishing.
- Integrar en el plan riesgos derivados de la evolución del phishing.
- Un counter-hack a los phishers es factible.

# Riesgos contemporáneos de Phishing MX

## ■ El hack a la empresa RSA

- ▶ En USA se retiraron todos los tokens OTP, en MX no se tiene información sobre un obligado cambio masivo.
- ▶ [http://www.schneier.com/blog/archives/2011/08/details\\_of\\_the.html](http://www.schneier.com/blog/archives/2011/08/details_of_the.html)

## ■ El Spear Phishing sigue latente

- ▶ La evolución natural del phishing para golpes más directos y efectivos. Es difícil detectar puesto que no se manifiesta de forma masiva.

## ■ Mayor auge e impulso por el crimen organizado

- ▶ Actualmente observamos un grupo mayormente organizado, no sabemos si detrás se encuentre el narco, pero no hay nada que les impida diversificarse

# El Botnet Phishing

- ▶ La empresa Trend Micro y otras casas de software de seguridad han dado seguimiento y destrucción en 4 ocasiones de una botnet formada exclusivamente por PCs zombies mexicanas. Origen: Guadalajara.
- ▶ Una botnet permite la modificación masiva en muy corto tiempo de miles de sistemas orientándolos hacia un sitio de phishing.
- ▶ [http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/discerning\\_relationships\\_\\_september\\_2010\\_.pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/discerning_relationships__september_2010_.pdf)



## Conclusiones

- No tenemos una forma de saber cuantas campañas de phishing existían en curso.
  - ▶ Teoría: el grupo de phishers principal crea una campaña nueva cada 2 semanas.
  - ▶ Esta el factor de que pueden ser desarticuladas.
- Los subscriptores de los boletines aceptaron que la información les ayuda a aprender a reconocer mejor cuando reciben un correo sospechoso.
- Sorprende la moderada capacidad de los antivirus para reconocer un ataque a HOSTS.
  - ▶ El mal hábito de usar AV piratas aumenta el riesgo.

- El objetivo predominante fue el archivo de HOSTS, de manera que cualquier mecanismo de protección que evite modificaciones de ese archivo dejaría inmunes contra el phishing visto.
- Es factible establecer una red de captura que permita identificar y desarticular campañas de phishing dentro de las primeras 24 hrs.
- Los filtros anti sitios maliciosos de los navegadores se pueden beneficiar de una alimentación más oportuna de la lista negra.

---

# ¿Preguntas? GRACIAS

Msc. Helios Mier Castillo

@hmier

Helios.mier en grex.mx

Blog: [www.seguridadyprivacidad.org](http://www.seguridadyprivacidad.org)

(+52 444) 138 9342