

OWASP - 14 Meses de observación del Phishing MX

Msc. Helios Mier Castillo
GREX Tecnologías de Información
Helios.mier@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>

Agenda

- 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..



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 acercan las temporadas de frío en el país, se incrementen 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.

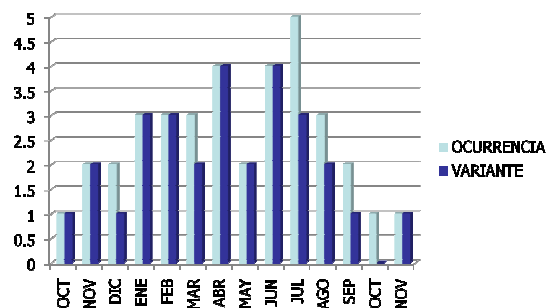


No es necesario esperar cuando el virus nuevo H1N1 de la gripe entró en su puerta. La medicina contra la influenza salvó a la posibilidad a su

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.

México, D.F., 24 de septiembre. (LACONEX.COM.MX) - Falleció el actor y presentador mexicano Roberto Gómez Bolaños (Chespirito) a los 79 años de edad. Participó en programas de televisión, películas, series y películas. Colaboró en el teatro. El Chavo del Chavo, El Chapulín Colorado, El Chavo y un gran número de producciones. Además de su trabajo de presentador civil en la ciudad y Roberto arquitecto, músico, actor, volvió a Casa de un paro respiratorio.

En el siguiente video se muestra también una entrevista con el actor, Villalón y Macías.

[Ver noticia](#)



La cantante Rihanna se suicida tras escándalo con fotografías.

La cantante conocida en el ambiente de la música como Rihanna fue encontrada sin vida en su apartamento de Miami.


Las autoridades indican que el presunto probable asesino es el actor que se involucró en un escándalo por la publicación de fotos íntimas de la cantante con el actor Chris Brown, desde la cual se espera con poca esperanza, se restablezca al mismo tiempo que se resuelva su parentesco materno.

La cantante también conocida como la Malakana empezó a parecer hace unos días patillas y andrajos en su rostro cuando estos minutos se comunicó a su familia materno. Esperen 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

OWASP 13

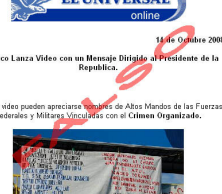


El Marco Lanza Video con un Mensaje Dirigido al Presidente de la Republica.

En este video pueden apreciarse algunos de Albas Mandos de las Fuerzas Federales y Militares Vinculadas con el Crimen Organizado.

CIUDAD DE MÉXICO, México, 24 de 2008. Fue el primer video en internet que se difundió en los últimos días recibiendo estos funcionarios por primera vez a la honra del Canal. Entre ellos al Ex. Secretario de Gobierno Santiago Creel y al Ex. Presidente de México Vicente Fox Quesada.


■ Igual que los anteriores Noticias también fueron satelizados el actual Procurador General de la República Eduardo Medina Mora entre otros. [Enlace al video. Falso.](#)



■ 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.

OWASP 14




Video Explicación y vacuna contra influenza.

Ante los constantes brotes del virus de la gripe por el cual el gobierno Federal ha tomado nuevas medidas para combatir el virus que se a declarado como epidemia.

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

[Descargar Video](#)



Ante el constante brote del virus de la gripe aviar, también conocido como influenza, el Gobierno Federal y quienes se encarga de la salud pública para combatir, se han a la medida como medida para combatir el virus.

A través de este comunicado informamos a la población Mexicana de las pautas correctas que seguir para evitar la infección por este virus.

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

■ 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.

OWASP 15



FALSO



¡Felicitaciones!

Haga clic aquí

■ El envío de tarjetas de felicitación y animaciones referentes a las festividades del momento.

- ▶ El sitio suplantado siempre era gusanito.com

OWASP 16

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 podíamos 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.

- 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

(+52 444) 138 9342