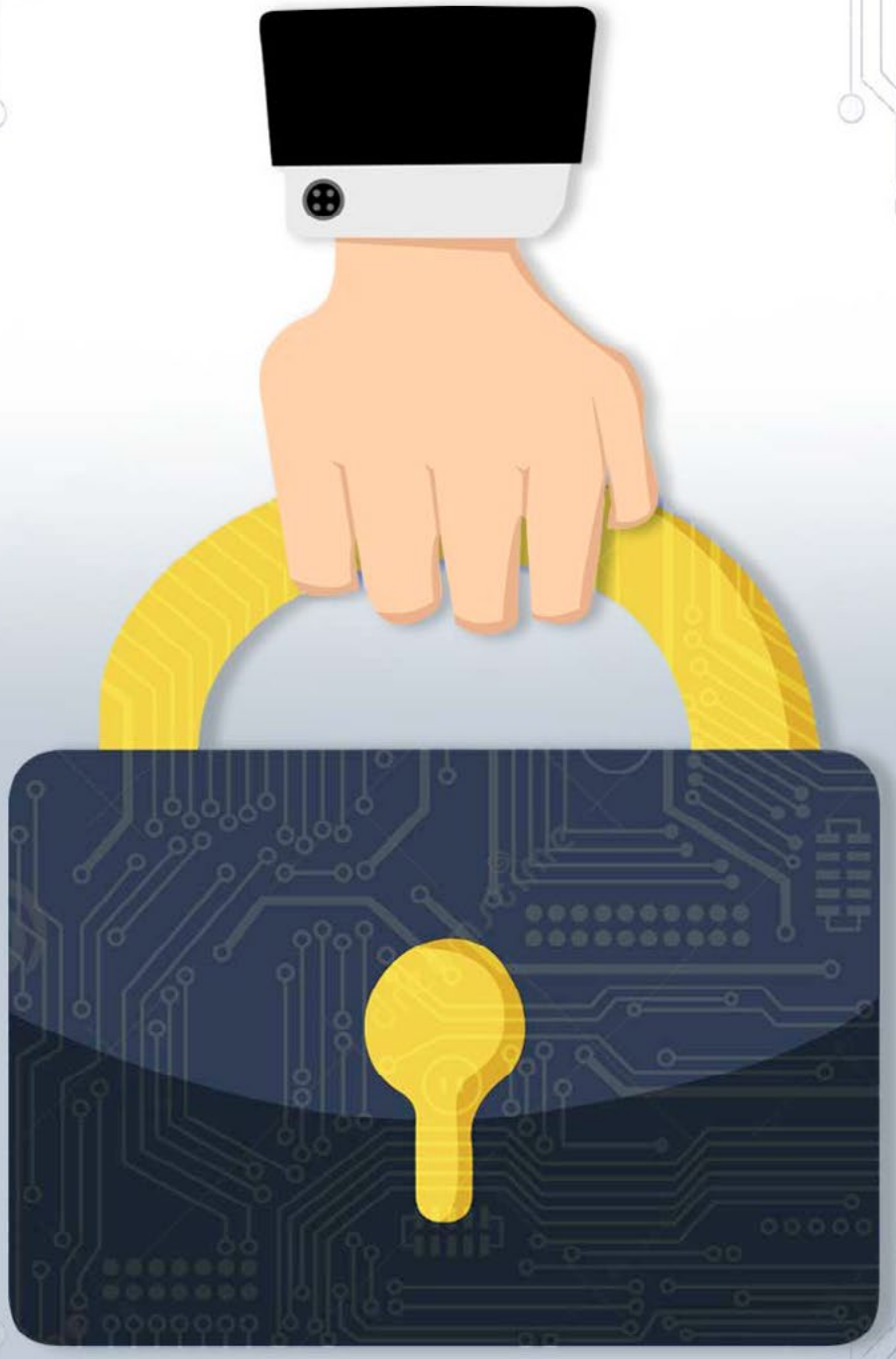
No. 27 / septiembre - octubre 2016

.Seguridad

Cultura de prevención para TI

27



Seguridad como estrategia de negocio

Contenido

.Seguridad
Cultura de prevención para TI

Universidad Nacional Autónoma de México. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Coordinación de Seguridad de la Información/UNAM-CERT. Revista .Seguridad Cultura de prevención para TI M.R., revista especializada en temas de seguridad del UNAM-CERT.

Editorial

Seguridad como estrategia de negocio

La gobernanza de TI

En el último año se ha detectado un aumento de amenazas dirigidas a organizaciones públicas y privadas. Los ciberdelincuentes buscan un eslabón débil, ya sea una persona o un punto vulnerable en los procesos de las organizaciones para obtener beneficios de distinta índole pidiendo rescate por información, haciéndose pasar por directivos para engañar a usuarios o realizar chantajes.

A pesar de la problemática, investigaciones realizadas por firmas de seguridad, dependencias gubernamentales y grupos universitarios indican que estos organismos no velan lo suficiente por su seguridad al no considerarla un área de importancia fundamental, inclusive descartándola como una inversión o estrategia de negocios.

La carencia o la mala elaboración de las políticas, así como la deficiente aplicación para el uso de herramientas TI, son sólo algunas de las preocupaciones reflejadas en los artículos que conforman esta edición.

Consideramos que la estructura de una organización debe estar comprometida en la generación, comprensión y ejecución de mecanismos y políticas internas claras para que se asegure la realización de buenas prácticas y así garantizar la seguridad.

Los autores en este número abordan la elaboración de políticas de seguridad y brindan recomendaciones para el uso de herramientas TI. También continuamos con temas presentados en el número anterior, como la implementación de un spampot y la configuración de un laboratorio virtual para analizar malware.

Esperamos que disfrutes este número de Revista .Seguridad.

Katia Rodríguez Rodríguez
Editora
Coordinación de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención para TI, revista bimestral, septiembre-octubre 2016 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

Consejos para desarrolladores web con enfoque a comercio electrónico

Jesús Mauricio Andrade Guzmán

Este artículo está orientado para negocios pequeños y medianos, así como equipos de desarrollo que buscan tener presencia web. La demanda de comercios en línea se está incrementando considerablemente. El manejo de transacciones monetarias en línea, sin considerar aspectos de seguridad informática, pone en riesgo la información de clientes y vendedores, por lo que es necesario contar con un plan de desarrollo integral que considere al menos las cuestiones básicas de seguridad.

A continuación se muestra un panorama general de los problemas de seguridad que se presentan durante el desarrollo de una solución de comercio electrónico y se discutirán consejos básicos a tomar en cuenta. No se pretende profundizar sobre varios temas relacionados, pero se ofrecerán algunas referencias de consulta. Algunos de ellos pueden no aplicarse al flujo de desarrollo de su empresa o equipo de trabajo por alguna razón, pero es importante que se consideren en lo general al menos. Del mismo modo, estas recomendaciones son suficientemente generales para aplicar en cualquier metodología de desarrollo, lenguaje de programación o enfoque que se adopte al desarrollar un sistema que pretenda ser tienda en línea.

Introducción

Actualmente no sólo hay más dispositivos conectados a Internet, también confiamos más en ellos y hacemos todo a través de la red.

El comercio en línea está creciendo de manera importante, tan sólo en México el comercio electrónico creció 34% en 2014 (AMIPCI, 2015). Debido a esta tendencia, una tienda de ropa, juguetes, alimentos o prácticamente lo que sea, si no está ya ofreciendo sus productos en línea, muy pronto buscará entrar al mundo del comercio electrónico.

Existen varias maneras de ofrecer productos y servicios por Internet, una empresa puede optar por:

A. Desarrollo libre. Este punto abarca tanto el diseño, desarrollo e implementación de una aplicación de comercio en línea, como el uso de herramientas de desarrollo prefabricadas para personalizar soluciones a través de un código (generalmente PHP, Java, JavaScript, CSS o HTML). Una empresa o un consultor externo puede desarrollar su propia plataforma utilizando herramientas como Magento, WooCommerce o PrestaShop e incluso desarrollar las funcionalidades completas con herramientas de programación como CodeIgniter, Zend, Bootstrap, entre otras.

B. Catálogo en línea. Es posible utilizar una plataforma para ofrecer productos como Amazon, MercadoLibre o eBay, las cuales ofrecen la gestión completa del proceso de venta, es decir, los métodos de pago, envío, seguimiento de usuarios, inventario, etcétera. Normalmente un usuario de estos servicios sólo debe crear una cuenta y proporcionar la información de sus productos para empezar a vender.

C. Software como Servicio. También pueden optar por soluciones SaaS (Software as a Service) como Shopify, Volusion, Square Space, entre otras. Estas ofrecen su plataforma a través de una cuota mensual, de esta manera una empresa puede personalizar y publicar una tienda en línea sin tener que contar con infraestructura propia.

El comercio en línea es actualmente un mercado en crecimiento (Informe sobre la economía de la información, 2015). Existen muchas alternativas y los actores involucrados buscan satisfacer a usuarios que cada vez están más conectados y acostumbrados a las nuevas tecnologías. Los retos a los que se enfrentan los mercados en desarrollo como México también son nichos de oportunidad para empresas internacionales y la competencia que deben enfrentar las empresas de desarrollo en nuestro país es cada vez mayor.

Muchas empresas de tecnología dedicadas al desarrollo de software ofrecen actualmente soluciones de comercio electrónico, y si no, lo harán pronto. Es muy importante que en el desarrollo de las soluciones se tomen en cuenta tanto la seguridad de las transacciones en línea que se realizan, así como la privacidad de los clientes a los que está dirigida esta tecnología.

Consejos

Estos “consejos” pueden ser leídos como simples comentarios de situaciones generales a los que se puede enfrentar un desarrollador web con un proyecto de tienda en línea.

Sobre el uso de HTTPS y la inyección de código

Utilizar HTTPS es un requisito indispensable para un comercio en línea pero no ofrece defensa para la mayoría de los ataques cibernéticos. El desarrollador debe estar consciente de las últimas tendencias en ataques y estrategias de defensa para sus sitios web.

No es suficiente activar el soporte para HTTPS en un sitio web, es necesario atender buenas prácticas de seguridad durante todo el ciclo de desarrollo del software, contemplar actualizaciones y pruebas de seguridad durante la vida del sistema.

En números anteriores de esta revista se ha discutido la utilización de un canal cifrado para transmitir tráfico web; también se han ofrecido consejos para evitar fraudes en línea. Actualmente resulta alentador saber que en la mayoría de los servicios en Internet ya se utiliza algún método de cifrado para la información que viaja por la red o al menos se ofrece la opción de usarlo. Sin embargo, basta con revisar las listas de 2010 o 2013 de OWASP de las principales amenazas que afectan a aplicaciones web, en las cuales la primera amenaza registrada desde hace varios años es la inyección de código.

La inyección de código ocurre cuando los datos de entrada a las aplicaciones no están debidamente validados, abriendo el paso a posibles ataques. Para "inyectar" código malicioso o consultas con intenciones maliciosas no es relevante si la aplicación web se transmite o no usando algún tipo de cifrado. Es importante distinguir esto, porque pensar que HTTPS protege de este modo a una aplicación puede resultar peligroso por la omisión de otras precauciones, como la validación y la detección de amenazas. Hablando de esto, también en números anteriores se ha discutido el tema de la detección y protección de aplicaciones utilizando un Firewall de Aplicación.

Por supuesto, estas medidas se aplican más a un enfoque de desarrollo de un sitio web propio, en el cual se tiene el control de las entradas y núcleo del sistema. Utilizar una plataforma como Magento o WooCommerce permite delegar esas funciones pero sólo si están actualizadas a la última versión, porque son precisamente esos problemas los que se corrigen en cada iteración.

Desarrollar con CMS o sin CMS

En estos días, el desarrollo web se ha orientado considerablemente a la utilización de gestores de contenido (CMS por sus siglas en inglés). El más popular para comercio electrónico es Magento, que ha sido la plataforma de desarrollo de comercio electrónico desde hace varios años. Los problemas de seguridad aplican también a este tipo de plataforma y es importante tener en cuenta las medidas preventivas que se pueden tomar. En números anteriores también se han discutido consejos de seguridad que se refieren a este tipo de tecnología.

Se puede argumentar que usar estas plataformas prefabricadas es "menos seguro" porque la aplicación web se expone a problemas conocidos por miles de personas y es posible explotarlos con mayor facilidad; lo cual es cierto, pero con reservas. Desarrollar una aplicación web sin usar gestores de contenido especializados en comercio implica que se deben tomar las precauciones mínimas para el manejo de entradas para evitar problemas de inyección y otras vulnerabilidades.

Es cierto que el mayor número de vulnerabilidades se encuentran en los gestores de contenido por su popularidad, pero hacerlo sin ellos tampoco es garantía de que sea más seguro. La complejidad de las transacciones monetarias, la gestión de cuentas de clientes del comercio en línea, inventarios y otros factores derivados de ser una tienda en línea, hacen que una aplicación derivada de un desarrollo propio sea difícil de diseñar, implementar y mantener. Por un lado, parecería que al tener un mayor control del desarrollo se pueden prevenir vulnerabilidades, pero en el caso particular de una tienda en línea, la complejidad y tamaño de este tipo de proyectos supera a una página web convencional. Además de esto, encontrar recursos humanos para el desarrollo propio no siempre es sencillo por las capacidades necesarias para llevarlo a cabo. Una aplicación personalizada puede fácilmente salirse de un presupuesto ajustado.

Por estas razones parece inevitable, al menos considerar, el uso de un gestor de contenidos para un proyecto de comercio en línea.

Mercado de complementos y plantillas

Si se decide usar un CMS debe tomarse en cuenta medidas de seguridad al utilizar plantillas (cf. *templates*) y complementos (cf. *plugins*). El uso de estos elementos en el desarrollo web a través de un CMS es común y en el caso de tiendas en línea, los complementos y plantillas normalmente tienen un costo; esto último es porque las plantillas y los complementos están orientados a generar un ingreso al ser para una tienda en línea.

El consejo de prevención que se da normalmente es tratar de mantener los complementos y plantillas siempre actualizados, al igual que el motor principal del CMS. Éste es un buen consejo y debe ser el primer paso, pero también es importante elegir complementos con una reputación bien establecida y con soporte del autor o de la comunidad.

Para el caso particular de tiendas en línea también es importante considerar el mercado de complementos y plantillas comerciales. Por la naturaleza de la distribución de estos elementos, la piratería no es rara en este tipo de desarrollo y puede ser una preocupación más para el desarrollador y el dueño del recurso.

No se hablará de los problemas legales o éticos de piratear complementos o plantillas[1] ya que este tema puede tener muchas implicaciones a tratarse en otro momento. El tema es delicado pero es necesario hablar claro al respecto: en México la piratería es un problema común y un desarrollador con presupuesto restringido o con poca experiencia puede verse tentado a descargar una copia ilegal de estos elementos para construir una tienda en línea.

Una posible solución a este problema es transferir la responsabilidad de la infraestructura de la tienda a un tercero, de esta manera las actualizaciones, complementos y varias cuestiones de desarrollo se transfieren a esas entidades. Algunas plataformas que se pueden utilizar para ofrecer productos son Amazon, eBay o Mercado Libre. Esta alternativa permite la venta de productos en línea, pero restringe el formato en el que se mostrará y la manera de procesar los pagos. La elección de estas tecnologías dependerá del objetivo del negocio y de los productos que se quieren poner en venta. Por otro lado, se puede requerir cierto tipo de personalización en la tienda en línea, es ahí donde entra la alternativa de Software como Servicio.

Desarrollo con Software como Servicio

Las soluciones que ofrecen compañías como Shopify, Volusion, Square Space y muchas más transfieren la administración y mantenimiento de la infraestructura tecnológica a una de estas empresas. Para contar con una tienda en línea, el usuario sólo debe subir sus productos y personalizar el funcionamiento de acuerdo con sus necesidades.

Esta alternativa es un poco más restringida que el desarrollo personalizado que se analizó antes, pero tiene la ventaja de poder personalizar más en comparación con los servicios de sitios como Mercado Libre o Amazon, que no lo permiten. El modelo de negocio de estos sitios generalmente incluye una cuota mensual y

posiblemente una cuota adicional por transacción (un porcentaje de cada venta). Por otro lado, servicios como estos no permiten acceder al sistema operativo o a las características internas de la arquitectura.

La forma de monetizar el servicio en estas empresas da la percepción de ser más costosas que las opciones anteriores, principalmente porque tecnologías como Magento o WordPress son de código abierto y de distribución libre. Sin embargo, debe considerarse cuidadosamente el precio real de desarrollar una tienda con software libre. El conocimiento necesario para desarrollar un sitio con herramientas de código abierto es considerable si se compara con servicios como Shopify.

La ventaja de usar Software como Servicio desde el punto de vista de seguridad es que las actualizaciones, parches y mantenimiento en general corren a cargo de estas empresas. Si se toma en cuenta que una tienda tiene el propósito de generar ingresos, puede ser visto como una inversión para poder ofrecer productos en línea de manera segura.

Conclusión

La decisión de ofrecer productos por Internet es un paso importante para una empresa en crecimiento y va de acuerdo con las tendencias del mercado global. Debe pensarse bien cuáles son los requerimientos y el objetivo de contar con una tienda en línea, para elegir el servicio que pondrá en marcha la tienda en línea.

La responsabilidad de las empresas de tecnología y equipos de desarrollo para cubrir esta necesidad es cuidar la información de sus clientes. Por ello es conveniente tomar en cuenta las recomendaciones mínimas para proteger la información durante todo el ciclo de desarrollo y mantenimiento de este tipo de sistemas.

Referencias

[1] Pero puede consultar fuentes como The Dangers of Pirate Plugins and Themes (2014) o How To Tell If Your WordPress Theme Is Legal (And Why You Should Care) (2014).

Aliysa. (2014, November 27). The Dangers of Pirate Plugins and Themes. Tsohost. Recuperado de https://www.tsohost.com/blog/the-dangers-of-pirate-plugins-and-themes

AMIPCI. (2015). Estudio de Comercio Electrónico. AMIPCI (Asociación Mexicana de Internet). Recuperado de https://www.amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

Coordinación de Seguridad de la Información/UNAM-CERT. (2014). Recomendaciones de seguridad para WordPress. Seguridad de la Información. Recuperado de http://www.seguridad.unam.mx/documento/?id=1927

Díaz, S. (2013, 5 de marzo). Firewall de Aplicación Web - Parte I. Revista. Seguridad Cultura de Prevención para TI, 16. Recuperado de http://revista.seguridad.unam.mx/numero-16/firewall-de-aplicaci%C3%B3n-web-parte-i

Espinosa, C. y Valdés, M. (2009, 9 de agosto). Tips para Evitar Fraudes en Línea. Revista .Seguridad Cultura de Prevención para TI, 02. Recuperado de http://revista.seguridad.unam.mx/numero-02/tips-para-evitar-fraudes-en-l%C3%ADnea

Hughes, M. (2014, May 20). How To Tell If Your Word Press Theme Is Legal (And Why You Should Care). MakeUseOf. Recuperado de http://www.makeuseof.com/tag/tell-wordpress-theme-legal-care/

OWASP. (2010). Top 10 2010. OWASP. Recuperado de https://www.owasp.org/index.php/Top_10_2010

———. (2013). Top 10 2013. OWASP. Recuperado de https://www.owasp.org/index.php/Top_10_2013

Ramírez, D. y Espinosa, C. (2011, 5 de marzo). El Cifrado Web (SSL/TLS). Revista .Seguridad Cultura de Prevención para TI, 10. Recuperado de http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

UNCTAD. (2015). Informe sobre la economía de la información. United Nations Conference on Trade and Development (UNCTAD). Recuperado de http://unctad.org/es/PublicationsLibrary/ier2015_es.pdf

Wikipedia. (2016). Sistema de gestión de contenidos. Wikipedia, la enciclopedia libre. Recuperado de https://es.wikipedia.org/w/index.php?title=Sistema_de_gesti%C3%B3n_de_contenidos&oldid=90567306

———. (2016). Software as a Service. Wikipedia, the Free Encyclopedia. Recuperado de https://en.wikipedia.org/w/index.php?title=Software_as_a_service&oldid=708416639

Si quieres saber más consulta:

- Tips para Evitar Fraudes en Línea
- Fraude Electrónico
- ¿Intermedios para Transferencias Monetarias?

Jesús Mauricio Andrade Guzmán

Maestro en Ciencias (Computación), egresado del Posgrado en Ciencia e Ingeniería de la Computación, de la Universidad Nacional Autónoma de México.

Colaboró con la Coordinación de Seguridad de la Información de 2003 a 2013. Especialista en defensa de aplicaciones web, administración de servicios y desarrollo de software.

Spampot para captura de correo electónico no deseado II

Miguel Raúl Bautista Soria

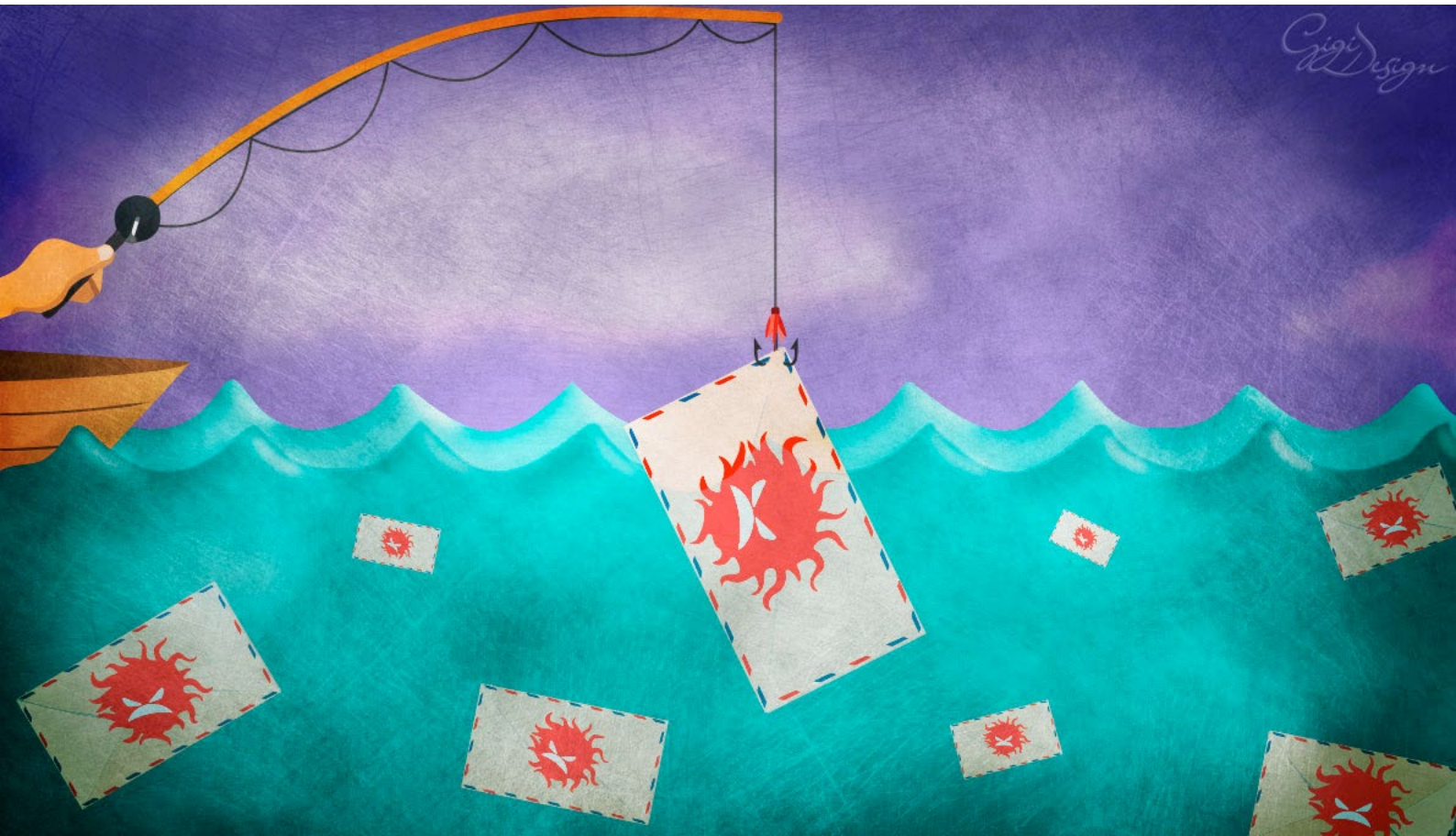
En el artículo anterior se abordaron los requerimientos funcionales de la herramienta spampot, un *honeypot* enfocado en capturar, analizar y ayudar a identificar el origen o destino de los correos electrónicos no deseados. En esta segunda parte se mostrarán las formas de ejecución de spampot.

Funcionamiento y estructura

La herramienta fue desarrollada para interactuar con equipos que envíen correo malicioso en Internet por medio de una arquitectura cliente-servidor, es decir, los clientes (remitentes de correo malicioso) se conectan al servidor (spampot) por medio de un socket, el cual se encuentra a la espera de nuevas conexiones en el puerto 25 (reservado para SMTP). Por cada conexión de un cliente, el servidor crea un hilo para atender dicha petición, la cual consistirá en el envío de un correo electrónico malicioso y el servidor simulará el envío del correo a su destino. Para este caso, los correos no son enviados pero sí analizados en busca de patrones que puedan dar un indicio sobre alguna actividad maliciosa, ya sea recurrente o que se detecte por primera vez en la red en donde se ejecute la herramienta.

Spampot está estructurada para analizar el correo electrónico recibido en cuatro fases:

La primera es la fase de red y recolección en la cual se llevan a cabo todas las funciones para preparar al servidor: verificar que se pueda poner el puerto 25 a la escucha en TCP; procesar todas las variables para los registros del servidor, tales como el directorio de trabajo,el directorio para guardar los correos electrónicos, la ubicación de la bitácora de ejecución del programa y algunos parámetros extra para el análisis de correos; obtener la



información de red de los clientes conectados, es decir, la dirección IP y el puerto origen, y los comandos para la interacción por medio de SMTP.

La segunda fase se ejecuta cuando la conexión con el cliente se ha cerrado y consiste en leer el archivo con la información del correo electrónico y buscar dentro de éste patrones de cadenas de caracteres que hagan referencia a campos específicos de un correo electrónico. Debido a que la información se recolecta en un archivo de texto plano, al emplear expresiones regulares con el lenguaje de programación Perl, la búsqueda de estos patrones en el archivo de texto se lleva a cabo de forma rápida y sencilla.

Dentro de los patrones al buscar se encuentran las siguientes categorías:

- Direcciones de correo electrónico origen y destino con el formato básico *usuario@dominio.com* y sus variantes
- Asunto del correo a través de la palabra ***Subject***
- Nombres de usuario obtenidos de las direcciones de correo electrónico
- Direcciones IP (versión 4) origen y destino y direcciones IP en los encabezados y cuerpo del correo
- Las URL que representan la dirección y ubicación correcta para acceder a un recurso en Internet
- Patrones predefinidos por el usuario, para encontrar información más específica

Una vez que se han encontrado estos patrones dentro del archivo de correo electrónico, todos y cada uno de ellos son almacenados en un tipo de dato de Perl llamado ***arreglo asociativo hash***, que es un conjunto de datos conformado por una llave y un valor. De esta manera es muy fácil almacenar información que se requiera cuantificar, expresar un número o agrupar datos dentro de otros (anidamiento).

En la Figura 1 se muestra un archivo de correo electrónico capturado por la herramienta el 7 de septiembre de 2014 y contiene la siguiente información (los caracteres '#' o 'X' ocultan información sensible que pudiera comprometer al sensor o a los usuarios de correo electrónico involucrados):

```
EHLO s15706526
MAIL FROM:<sales@amazonaws.com>
RCPT TO:<flXvXiX###@gmail.com>
DATA
MIME-Version: 1.0
From: sales@amazonaws.com
To: flXvXiX###@gmail.com
Date: 7 Sep 2014 12:21:00 +0200
Subject: ##.##.##.129,sales@amazonaws.com,sales
```

Figura 1. Muestra de correo electrónico capturado el 7/9/2014

De este archivo de correo electrónico se obtuvo la dirección IP que se conectó al sensor y desde donde se envió toda la información. La segunda fase obtuvo los valores mostrados en la figura 2:

```
Subject: ##.##.##.129,postmaster@amazonaws.com,postmaster
Usernames: flXvXiX###@gmail.com|2,postmaster@amazonaws.com|3
```

Figura 2. Registro generado por la segunda fase de ejecución

En la tercera fase de la herramienta se llevan a cabo dos acciones. La primera consiste en utilizar las URL encontradas para descargar posibles archivos maliciosos o relacionarlos con actividad maliciosa que intenta propagarse a través de correos electrónicos. La segunda es decodificar los archivos adjuntos del correo electrónico, los cuales viajan en una cadena de caracteres codificados en ***Base64***.

Al finalizar la tercera fase, todos los archivos descargados o decodificados son sometidos a una verificación de integridad utilizando un algoritmo digestivo llamado MD5. Gracias a este algoritmo, se podrán comparar las cadenas MD5 obtenidas de los archivos contra alguna base de datos de firmas de archivos maliciosos en Internet, como Virus Total[1].

La cuarta y última fase consiste en obtener toda la información de los *arreglos asociativos* que contienen los patrones buscados para procesarla y enviarla a una base de datos; ésta es el lugar lógico donde se guarda toda la información de las direcciones IP de los clientes y de los sensores, los patrones encontra-

dos, las URL y los MD5 de los archivos que se relacionan con el correo electrónico capturado. Una vez insertada en la base de datos toda la información recolectada, se cierra la conexión con la base de datos y el hilo termina, liberando la memoria y archivos utilizados para atender una nueva conexión.

Estructura de la base de datos

Los datos almacenados en la base de datos se guardan por medio de eventos, es decir, cada conexión al servidor (sin importar si es la misma dirección IP origen) se considera un evento. Cada evento puede contener uno o varios correos electrónicos recibidos, ya que de acuerdo al protocolo SMTP, se pueden enviar desde uno hasta varios correos por conexión a un servidor. Por cada evento se genera un identificador de evento (***id_event***), se obtiene la fecha y hora en que se registra la conexión, y se registra la dirección IP del cliente, la dirección IP del sensor (para identificar cada sensor en caso de contar con más de uno) y los puertos origen y destino. Toda esta información se almacena en una tabla llamada ***Events***, la cual tiene como llave primaria al campo *id_event*. Los patrones encontrados en cada evento se almacenan en seis tablas dentro de la base de datos:

- ***Binaries:*** con una llave primaria llamada *id_binary*, el campo *md5_list* y la llave foránea *id_event*.
- ***Domains:*** con una llave primaria llamada id_domain, los campos *id_domain, source_domain_list, destination_domain_list* y llave foránea *id_event*.
- ***IPs:*** con una llave primaria llamada *id_ip*, el campo *ip_list* y la llave foránea *id_event*.
- ***Subjects:*** con una llave primaria llamada *id_subject* y llave foránea *id_event*.
- ***URLs:*** con una llave primaria llamada *id_url* y llave foránea *id_event*.
- ***Usernames:*** con una llave primaria llamada *id_username* y llave foránea *id_event*.

Todas las tablas contienen una llave primaria y, a excepción de la tabla de eventos, una llave foránea. Esta llave foránea hace referencia a la llave primaria de la tabla de eventos para relacionar los patrones encontrados con un evento determinado.

El formato utilizado para almacenar la información dentro de la base de datos es:

patrón1|no. veces,patrón2|no. veces… patrónN|no.veces

Éste provee una gran rapidez para consultar la información almacenada utilizando expresiones regulares y técnicas de búsqueda por separadores de campos. Basta con realizar la consulta a la base de datos en la tabla deseada y seleccionar cualquier campo que termine con la palabra ***list***, a continuación se deben separar los campos primero por comas (,) y después por un ***pipe*** (|) para obtener la llave y el valor del arreglo *asociativo*.

Ejecución de la herramienta

Para ejecutar la herramienta, todos los módulos de CPAN deben estar correctamente instalados y la base de datos configurada apropiadamente. La configuración de la base de datos se debe hacer directamente en el servidor de base de datos y consiste en crear una base de datos denominada *spampot* y un usuario llamado *spampot*, el cual deberá tener todos los privilegios sobre la base de datos *spampot*. Todos los comandos de configuración de la base de datos se muestran en la Figura 3.

```
mysql> create database spampot;
Query OK, 1 row affected (0.00 sec)

mysql> create user 'spampot'@'127.0.0.1' identified by 'c0ntr4s3ñ@';
Query OK, 0 rows affected (0.01 sec)

mysql> grant all on spampot.* to 'spampot'@'127.0.0.1';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
```

Figura 3. Configuración del usuario de la base de datos

El puerto de red en el que la herramienta se ejecuta es el 25, correspondiente a STMP de acuerdo a la IANA. Todos los puertos menores al 1024 se llaman puertos reservados y, por lo tanto, requieren privilegios de administración para asignar una aplicación en éstos.

El comando de ejecución de la herramienta y los resultados de la misma al recibir y analizar un correo electrónico se encuentran en la Figura 4.

```
# perl spampot-ng.pl
Standard output debug mode on
Writing info to /home/spampot/spampot/log/spampot.log
Connected to
database:DBI:mysql:dbname=spampot;host=127.0.0.1;port=3306
Checking the total of tables on DB: 0
Created table Binaries
Created table Domains
Created table Events
Created table IPs
Created table Subjects
Created table Urls
Created table Usernames
################################################
UNAM-HONEYNET PROJECT
SSI/UNAM-CERT
honeynet@seguridad.unam.mx
------------------------------------------------
Spampot Tool v1.0
################################################
Binding on 0.0.0.0:25
HELO mail.server.com
MAIL FROM: <mail_user@mail.server.com>
RCP TO: <destination@mail.cloud-server.com>
RCPT TO: <destination@mail.cloud-server.com>
DATA
Subject: Winner Hi,I would like to inform you that you have been
selected as a winner in onr lotto please go to:
http://bit.ly/1xP9ZuUByc . QUIT
Connected to
database:DBI:mysql:dbname=spampot;host=127.0.0.1;port=3306
Matched URL: http://bit.ly/1xP9ZuU
Downloading File: 1xP9ZuU
Path: /home/spampot/spampot/output/binaries/192.168.0.200-
1416716750/1xP9ZuU
Created directory /home/spampot/spampot/output/binaries/192.168.0.200-
1416716750
Matched Subject: Winner
Matched Mail: mail_user@mail.server.com
Matched Email Domain: mail.server.com
Matched Mail: destination@mail.cloud-server.com
Matched Email Domain: mail.cloud-server.com
Matched Mail: destination@mail.cloud-server.com
Matched Email Domain: mail.cloud-server.com
0 file(s) decoded
Signed file: 1xP9ZuU - 955ccodffe0bccfb01d5d075fc9a08f4
Inserted Event with ID: 1
Inserted Urls for event [1]
Inserted Subjects for event [1]
Inserted Usernames for event [1]
Inserted Binaries for event [1]
```

Figura 4. Ejecución de la herramienta

En la ejecución mostrada en la sección anterior se observa una salida con la opción *Debug* habilitada con el valor 1, por lo que se identifican en pantalla varios mensajes que están clasificados en cinco códigos de color, los cuales corresponden a:

- **Comando de ejecución**
- **Mensajes de ejecución de la herramienta**
- **Mensajes relacionado con la base de datos**
- **Mensajes de correo electrónico recibido**
- **Mensajes de análisis del correo electrónico recibido**

En la Figura 5 se muestra la bitácora de la herramienta correspondiente a la ejecución anterior, la cual únicamente contiene los mensajes de la herramienta y las funciones como fueron llevadas a cabo en la ejecución.

El formato de la bitácora es el siguiente:

[Marca de tiempo]-[Tipo de mensaje]-[Seguimiento]-[Mensaje de la bitácora]

La marca de tiempo tiene el formato AAAA-MM-DDTHH:MM:SS.

El tipo de mensaje utiliza cuatro etiquetas sobre la ejecución:

- *FATAL_ERROR:* Error fatal y termina la ejecución inmediatamente.
- *ERROR*: Error genérico que requiere de una corrección por parte del usuario.
- *WARNING*: Advertencia sobre un posible fallo pero sin terminar la ejecución.
- *INFO*: Informe de la ejecución y las acciones realizadas.
- *DEBUG*: Muestra información más detallada y ayuda a detectar errores.

El seguimiento indica las funciones que han sido ejecutadas en el momento en que se escribe un mensaje en la bitácora; es un formato separado por el símbolo 'l'. Por último, el mensaje de la bitácora indica la acción que se está realizando.

```
[2014-11-22T22:25:14]-[INFO]-[main]-[Checking Spampot config...]
[2014-11-22T22:25:14]-[INFO]-[main]-[Writing info to /home/spampot/spampot/log/spampot.log]
[2014-11-22T22:25:14]-[INFO]-[CheckConfig|ConnectDatabase]-[Connected to database:mysql:spampot]
[2014-11-22T22:25:14]-[INFO]-[CheckConfig|CheckTables]-[Checking the total of tables on DB: 7]
[2014-11-22T22:25:14]-[INFO]-[main]-[Starting Spampot Tool v1.0]
[2014-11-22T22:25:14]-[INFO]-[main|StartServer]-[Started SMTP Server binded on 0.0.0.0:25]
[2014-11-22T22:26:02]-[INFO]-[StartServer|Collector]-[Saving data into file: 192.168.0.200-
1416716750]
[2014-11-22T22:26:55]-[ERROR]-[StartServer|Collector]-[Command not recognized [RCP TO:
        <destination@mail.cloud-server.com>]]
[2014-11-22T22:27:17]-[INFO]-[StartServer|Collector]-[Saving data into file: 192.168.0.200-
        1416716750]
[2014-11-22T22:28:57]-[INFO]-[StartServer|Collector]-[Closed file: 192.168.0.200-1416716750]
[2014-11-22T22:25:57]-[INFO]-[ParseMail|ConnectDatabase]-[Connected to database:mysql:spampot]
[2014-11-22T22.20.57]-[INFO]-[ParseMail|GetUrls]-[Getting URLs]
[2014-11-22T22:28:57]-[INFO]-[ParseMail|GetUrls]-[Looking blacklist patterns on URLs]
[2014-11-22T22:25:59]-[INFO]-[GetUrls|DownloadURL]-[Downloading URLs]
[2014-11-22T22.20.59]-[INFO]-[GetUrls|DownloadURL]-[Downloading file. 1xP9ZuU]
 [2014-11-22T22:28:59]-[INFO]-[GetUrls|DownloadURL]-[Created directory
        /home/spampot/spampot/output/binaries/192.168.0.200-1416716750]
[2014-11-22T22.20.59]-[INFO]-[ParseMail|GetSubjects]-[Getting Subjects]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|GetSubjects]-[Looking blacklist patterns on Subjects]
[2014-11-22T22:25:59]-[INFO]-[ParseMail|GetIPs]-[Getting IPs]
 [2014-11-22T22:25:59]-[INFO]-[ParseMail|GetDomains]-[Getting Source Domains]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|GetDomains]-[Getting Destination Domains]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|GetDomains]-[Getting Emails]
[2014-11-22T22:25:59]-[INFO]-[ParseMail|DecodeAttachments]-[Decoding Attachments]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|GetSignaturesList]-[Getting signatures of downloaded files]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|InsertEvent]-[Inserted event with ID: 1]
[2014-11-22T22:25:59]-[INFO]-[ParseMail|InsertEvent]-[Inserted Urls for event [1]]
[2014-11-22T22.20.59]-[INFO]-[ParseMail|InsertEvent]-[Inserted Subjects for event [1]]
[2014-11-22T22:28:59]-[INFO]-[ParseMail|InsertEvent]-[Inserted Usernames for event [1]]
[2014-11-22T22:25:59]-[INFO]-[ParseMail|InsertEvent]-[Inserted Binaries for event [1]]
```

Figura 5. Bitácora de ejecución

Resultados

Con el objeto de verificar el correcto funcionamiento de la herramienta, se llevó a cabo una fase de pruebas para descartar errores de ejecución, fallos en la recepción y envío de los comandos y la información, así como el análisis de la información que fue capturada.

Estas pruebas fueron realizadas utilizando servicios de verificación en línea, herramientas de uso abierto y la ejecución de la herramienta directamente en el entorno de investigación, mencionado en la primera parte de este artículo. Los servicios en línea utilizados para las pruebas de la herramienta son:

- MailRadar (http://www.mailradar.com/openrelay/): Es un servicio que realiza 20 pruebas a través del envío de varios correos electrónicos con diferentes remitentes y destinatarios analizando las respuestas del servidor de correo para determinar la configuración del servidor.
- MXToolBox (http://mxtoolbox.com/diagnostic.aspx): Servicio en línea que realiza una verificación del servidor SMTP y además corrobora que el nombre de dominio asociado al servidor corresponda con el mensaje de inicio e identificación del servicio de correo que se ejecuta.

Las herramientas de uso abierto utilizadas para probar la herramienta son:

- SWAKS (http://www.jetmore.org/john/code/swaks/): Denominada la navaja suiza para SMTP (*Swiss Army Knife for SMTP*) es una herramienta con varias opciones de ejecución para verificar el correcto funcionamiento de servidores de correo electrónico.
- relaycheck.pl (http://arpa.org/relaycheck.pl): Es un programa escrito en el lenguaje de programación Perl para realizar una verificación rápida de un servidor de correo electrónico mal configurado.

Dentro del entorno de investigación se recibe una gran cantidad de tráfico de Internet hacia las direcciones IP no asignadas de la red corporativa, por lo que todo ese tráfico originado por otras aplicaciones o usuarios en Internet se considera potencialmente malicioso. Bajo este esquema se reciben múltiples peticiones de diferentes aplicaciones por lo que, con este entorno, también se verifica la capacidad de respuesta de la herramienta ante grandes cantidades de tráfico.

Actualmente la herramienta se encuentra en la versión 1.0. El código fuente de la misma versión se encuentra disponible y gratuito para su uso y distribución en el sitio **GitHub**. En la siguiente URL se accede directamente a la herramienta: https://github.com/miguelraulb/spamhat. Dentro de la misma se encuentran las instrucciones y requisitos para ejecutar la herramienta, además se incluye un archivo instalador (*installer.sh*) para automatizar todo el proceso de instalación incluyendo las dependencias necesarias.

Conclusiones

Con el desarrollo y la implementación de esta herramienta se logró una gran visibilidad en la red para detectar nuevas amenazas y ataques debidos a la recepción masiva de correo electrónico no deseado en una red corporativa. Además, en conjunto con el análisis de patrones, se pudieron determinar las direcciones de correo electrónico, direcciones IP y nombres de dominio más utilizados dentro de estos ataques. Finalmente con el análisis del contenido de los archivos adjuntos y de las URL contenidos en el cuerpo del correo electrónico, se lograron detectar sitios con contenido malicioso, información fraudulenta o redirecciones a otros sitios maliciosos.

Debido a la forma en cómo se almacena la información dentro de la base de datos, se puede obtener un histórico de la actividad recolectada y clasificarla por día, mes y año. Gracias a estos históricos la información de los ataques recibidos es más fácil de revisar, entender y de comprender.

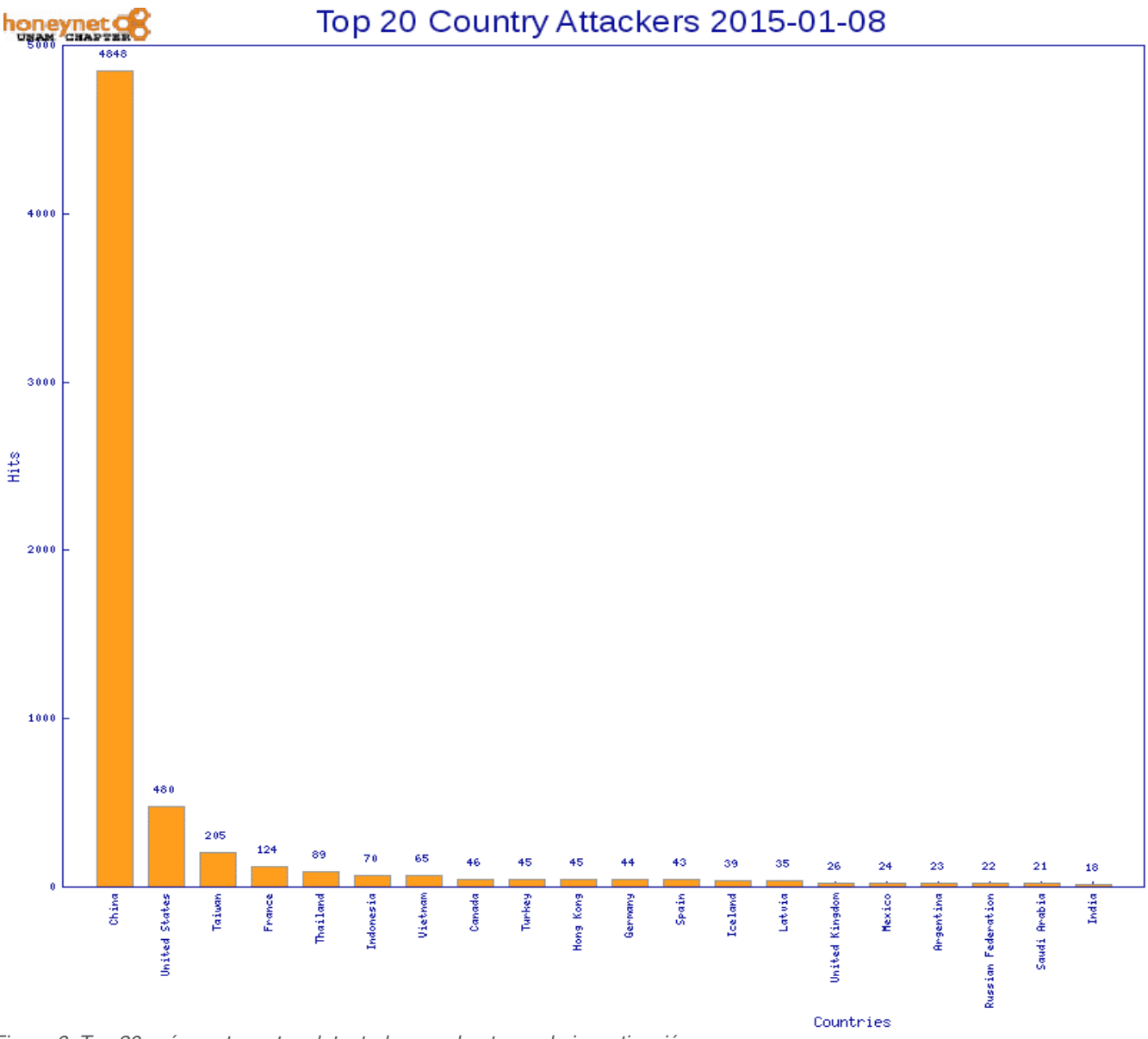


Figura 6. Top 20 países atacantes detectados en el entorno de investigación

Referencias

[1] Virus Total *es un sitio en Internet que permite analizar archivos, obtener el MD5 del archivo y compararlo con una lista de antivirus comerciales para así saber si el antivirus detecta la pieza maliciosa. También permite buscar directamente una cadena MD5 o una URL y realizar el mismo análisis que con un archivo malicioso.*

Si quieres saber más consulta:

- Spampot para la captura de correo electrónico no deseado
- Evita el correo basura: antispam
- Día de limpieza

Miguel Raúl Bautista Soria

Ingeniero en Computación por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM). Colaboró desde agosto de 2011 hasta septiembre de 2014 en la Coordinación de Seguridad de la Información /UNAM-CERT en el área de Detección de intrusos y tecnologías honeypot, en donde llevó a cabo actividades de desarrollo, instalación y pruebas de tecnologías honeypot para análisis y detección de actividad maliciosa. Cuenta con las certificaciones SFCP de Sourcefire y GCFW del SANS Institute. Actualmente labora en el TAC de Cisco México, en el equipo de seguridad informática y es miembro oficial de la organización de investigación The Honeynet Project.

¿Gobierno de la ciberseguridad?

Rosa Xóchitl Sarabia Bautista

Hoy en día, las amenazas cibernéticas se introducen en las organizaciones de diversas formas, ya sea por medio de los empleados, aplicaciones o sistemas utilizados en las operaciones del negocio. Lo que se mantiene constante es que existen riesgos en todas partes. Hemos llegado a una nueva era del cibercrimen en la cual se realizan ataques dirigidos a las empresas con la intención de ocasionar daño.

La seguridad requiere la participación activa de los altos directivos de las empresas. El término que describe el compromiso de la alta dirección es el gobierno corporativo, que es el conjunto de responsabilidades y prácticas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar una dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable.

Por lo tanto, la ciberseguridad debe ser parte integral del gobierno corporativo para lograr sus objetivos, no sólo para cubrir las necesidades actuales sino también las futuras. En general el gobierno de la ciberseguridad se puede englobar en el de seguridad de la información, dado que este último puede manejar información fuera del ciberespacio.

El objetivo de la seguridad de la información es desarrollar, implementar y administrar un programa de seguridad que alcance los siguientes cinco resultados básicos de un gobierno eficaz de seguridad:

1. Alineación estratégica: Alinear la seguridad de la información con la estrategia de negocio.
2. Administrar los riesgos: Ejecutar medidas

apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los activos de información.
3. Entrega de valor: Optimizar las inversiones en la seguridad.
4. Administración de recursos: Utilizar el conocimiento y la infraestructura de la seguridad de la información con eficiencia y eficacia.
5. Medición del desempeño: Monitorear y reportar métricas de seguridad de la información para garantizar que se alcancen los objetivos.

Para lograr un gobierno eficaz, la alta dirección debe establecer un marco que guíe el desarrollo y mantenimiento de un programa integral de seguridad como el que se muestra a continuación:

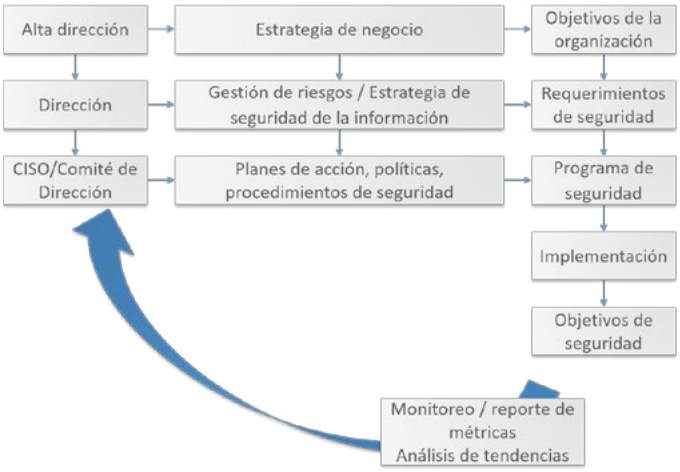


Figura 1 (IT Gobernance Institute, 2006)

La Figura 1 muestra las relaciones y los participantes involucrados en el desarrollo de una estrategia de seguridad alineada a los objetivos de negocio. La estrategia tiene como entradas la estrategia de negocio, el estado actual y deseado de seguridad, los requerimientos del negocio y procesos, los resultados de la evaluación de riesgos y requisitos regulatorios. La estrategia proporciona la base para el desarrollo de los planes de acción (iniciativas de seguridad) en cumplimiento de los objetivos de seguridad.

Debido a que las organizaciones tienen diversas necesidades y sus enfoques de gobierno pueden variar, se ha identificado un conjunto básico de principios y buenas prácticas para ayudar a guiar estos esfuerzos.

Principios:

- El riesgo de seguridad de la información es más que un problema de TI: es un componente clave en la gestión de riesgos de la organización, lo que requiere la supervisión de la dirección.
- El riesgo tiene implicaciones legales que los directivos deben entender.
- El riesgo debe ser un tema de discusión en la junta de dirección de forma periódica.
- Los directores deben implementar un marco efectivo de gestión de riesgos en la organización.
- La alta dirección y el consejo deben evaluar el riesgo de seguridad de la información al igual que otros riesgos a nivel organización para asegurar que los riesgos se acepten, eviten, mitiguen o transfieran.

Buenas prácticas:

- Realizar una evaluación anual de la seguridad de la información a cargo de la alta dirección.
- Llevar a cabo evaluaciones de riesgos periódicos como parte de un programa global de gestión de riesgos.
- Implementar políticas y procedimientos basados en las evaluaciones de riesgos.
- Establecer una estructura de gestión de seguridad para asignar individualmente roles y responsabilidades.
- Desarrollar iniciativas para brindar seguridad de la información a redes, instalaciones, sistemas e información en general.
- Tratar la seguridad de la información como parte integral durante el ciclo de vida de los sistemas de información.
- Proporcionar concientización, capacitación y educación en seguridad de la información para todo el personal.
- Conducir pruebas y evaluaciones periódicas para medir la efectividad de las políticas y procedimientos de seguridad de la información.
- Crear y ejecutar planes de acción para manejar cualquier deficiencia de seguridad

de la información.
- Desarrollar e implementar procedimientos de respuesta a incidentes.
- Establecer planes, procedimientos y pruebas para proporcionar continuidad de las operaciones.
- Utilizar las mejores prácticas como ISO 27001, NIST SP 800, CoBIT, entre otros.

Marco de ciberseguridad del NIST

Recientemente, el Instituto Nacional de Estándares y Tecnología (NIST) publicó un marco de ciberseguridad que permite a las organizaciones, independientemente de su tamaño, grado de riesgo o sofisticación de sus medidas de protección, aplicar las mejores prácticas para la gestión de riesgos que permita mejorar la seguridad y resiliencia de sus infraestructuras.

Son cinco las funciones básicas del marco que se definen a continuación:

1. Identificar: Desarrollar el conocimiento de la organización para gestionar riesgos de seguridad en sistemas, activos, datos y capacidades.

2. Proteger: Desarrollar e implementar las salvaguardas adecuadas para garantizar la prestación de servicios.

3. Detectar: Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de seguridad.

4. Responder: Desarrollar e implementar las actividades apropiadas para actuar ante un evento de seguridad detectado.

5. Recuperar: Desarrollar e implementar las actividades apropiadas para mantener planes de resiliencia y restaurar las capacidades o servicios que fueron perjudicados debido a un evento de seguridad.

Conclusiones

Para la mayoría de las organizaciones, el establecimiento de un gobierno de seguridad de la información eficaz es una tarea primordial para integrar los esfuerzos aislados de seguridad que puedan existir y lograr resultados significativos en la reducción de pérdidas.

La tendencia hoy en día es que conforme las organizaciones crecen, éstas se vuelven más dependientes de sus activos de información y al mismo tiempo están expuestas a amenazas cada vez más sofisticadas, por ejemplo, ransomware, ataques de denegación de servicio distribuido (DDoS), las amenazas persistentes avanzadas (APT), entre otras.

Es por ello que se requiere el apoyo de la alta dirección y la asignación de los recursos adecuados, así como la definición de una estrategia que guíe las iniciativas de seguridad.

Referencias

Binwal, P. (2015, 29 de junio). Creating a Cybersecurity Governance Framework: The Necessity of Time. Security Intelligence. Recuperado de https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010, September). Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology. The MITRE Corporation. Recuperado de: https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

IT Governance Institute. (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd edition). IL, Estados Unidos: IT Governance Institute.

National Institute of Standards and Technology. (2014, February 12). Framework for Improving Critical Infrastructure Cybersecurity. Recuperado de http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

R. Westby, J. (2015, October 2). Governance of Cybersecurity: 2015 Report. Washington, Estados Unidos: Georgia Tech Information Security Center. Recuperado de https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf

The Corporate Governance Task Force. (2004, April). Information Security Governance: A Call to Action. National Cyber Security Summit Task Force.

Threat Brief. (s.f.). Cyber Security and Corporate Governance: The five principles every corporate director should embody. Threat Brief. Recuperado de http://threatbrief.com/cyber-security-corporate-governance-five-principles-every-corporate-director-embody/

Si quieres saber más consulta:

- Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I
- Riesgo tecnológico y su impacto para las organizaciones parte I
- Buenas prácticas, estándares y normas

Rosa Xóchitl Sarabia Bautista

Maestra en Ingeniería en Computación por parte del Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) de la Universidad Nacional Autónoma de México (UNAM). CREA, CISA, CISM, CHFI, ISO 27001 Lead auditor.

Fue becaria de la tercera generación del Plan de becarios de seguridad en cómputo de la DGSCA, UNAM-CERT. Se ha desempeñado como Subdirectora de Estándares de Seguridad en la Policía Federal de México, E-crime lab manager en Banamex y Directora en Mnemo-CERT.

Seguridad en la nube para una IES

Israel Josué Novelo Zel

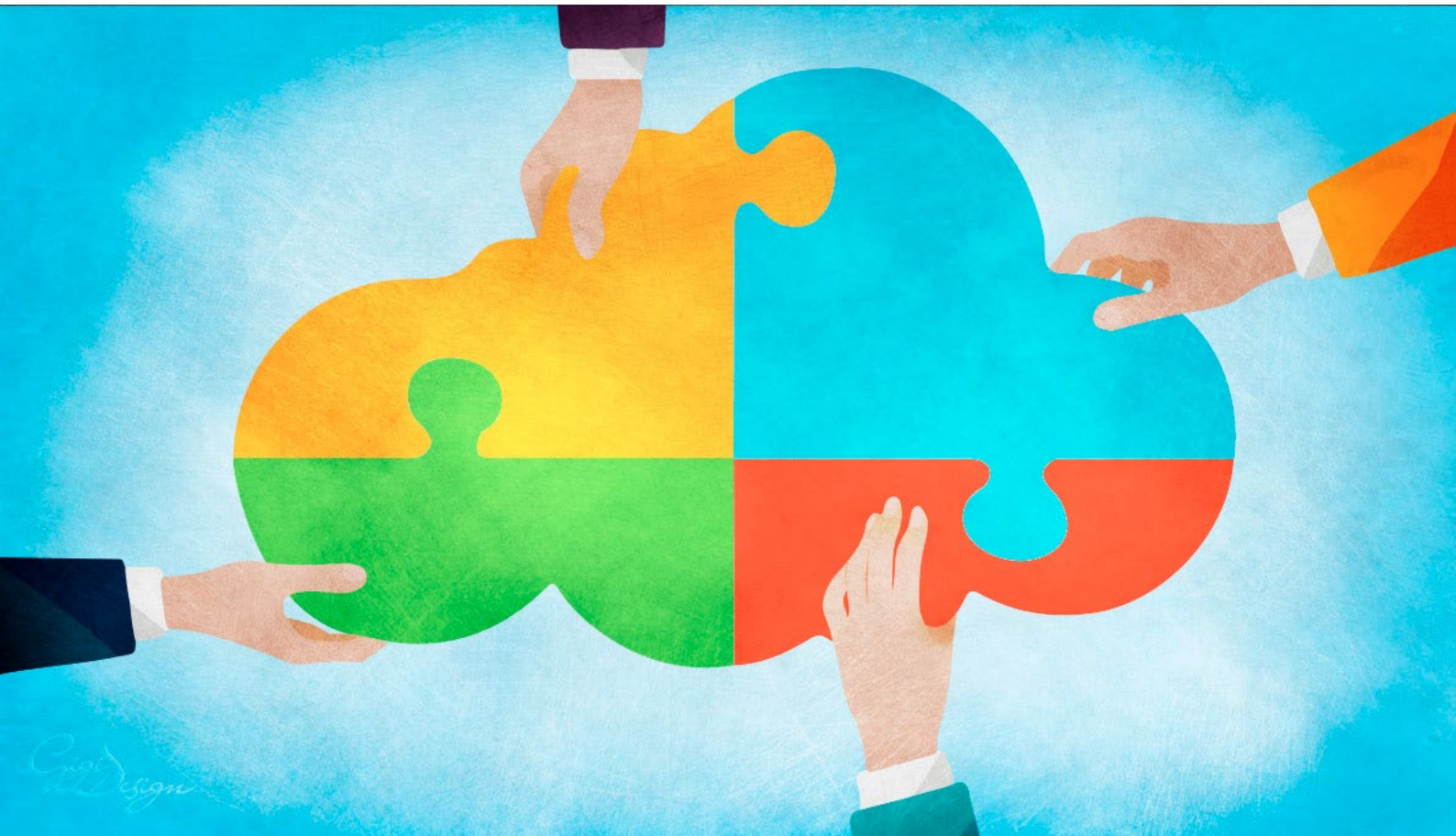
El uso del cómputo en la nube es un cambio significativo e importante en una Institución de Educación Superior en México (IES). Si bien es la respuesta ante las necesidades de mayores y rápidas implementaciones de Sistemas de Tecnologías de Información (STI), es claro que conlleva muchos retos de seguridad con el fin de tener éxito. El no atender las medidas claves de seguridad en un ambiente tan dinámico, cambiante y creciente como es la nube, seguramente arrastraría el proyecto de la nube al fracaso o ante situaciones de enfrentamientos legales de importancia.

No por esto se debe temer ante un cambio tecnológico como la nube, ya que es un reto que conllevará todos nuestros conocimientos y aptitudes sobre las tecnologías de información y seguridad, para alcanzar el éxito del proyecto.

El uso de las tecnologías de información en las Instituciones de Educación Superior en México (IES) han sostenido un crecimiento muy importante en los últimos años, debido a la necesidad de mejorar servicios relacionados a procesos administrativos, académicos, de investigación, así como optimizar el uso de recursos humanos y financieros.

Ante esta creciente demanda de servicios y necesidades, las IES están mirando a nuevos esquemas de cómputo que les permita continuar con la operación e incrementar sus servicios, atender eficientemente a los usuarios y bajar costos. En años anteriores se podría catalogar como ilógicas, sin embargo, hoy en día se han encontrado en la nube la respuesta a los retos y necesidades.

Si bien el cómputo en la nube puede ser una solución prometedora para las IES, la utiliza-



ción de esta implica un compromiso más alto de seguridad. Las siguientes preguntas son comunes al iniciar su uso: ¿Cómo es la seguridad en la nube?, ¿dónde queda la información de las IES?, ¿se cumplirán las leyes y normas del manejo de la información?, ¿qué información puede almacenarse fuera de las fronteras del país?, ¿debemos implementar una solución basada en la nube al 100%?, ¿debemos utilizar la nube híbrida (un porcentaje en la nube y otro en la red de la IES)?

Sin embargo, el cuestionamiento principal es cómo una IES puede sacar ventaja de un cambio de paradigma tan importante y que al mismo tiempo garantice la seguridad de la información de la institución. Esta pregunta debe contestarse con cuidado ya que cada IES tiene diferentes políticas y lineamientos que se deben cumplir, y de la misma forma tienen necesidades diferentes en cuanto a STI (algunas tipo *legacy*), que podría impactar directamente al éxito o fracaso de un proyecto, como es la nube.

Para la seguridad en la nube de una IES debemos tomar en cuenta los aspectos legales y tecnológicos. Los aspectos legales estarán determinados por la política y lineamientos de manejo de información de la IES, así como cualquier otra legislación a la cual deba obligarse.

En cuanto a los aspectos tecnológicos es determinante manejar una seguridad por capas en los STI que vayamos a manejar en la nube, es decir, que implique como mínimo, seguridad a nivel sistema operativo, de red, de aplicación y de transmisión de los datos. Sabemos que hoy en día la nube puede ofrecernos Infraestructura como Servicio (IaaS), Servidores Web como Servicio hasta Internet de las Cosas como Servicio, entre otras. Según la solución basada en la nube que necesitemos es la seguridad que debamos aplicar.

Todas las capas de seguridad son importantes y determinantes, sin embargo, las que estarán interactuando con los usuarios o clientes son de extremo cuidado. Podemos contar con una gran infraestructura de red, datos y servicios basados en la nube, pero a la par, debemos contar con aplicaciones lo suficientemente robustas para enfrentar inevitables ataques informáticos.

Recomendaciones para el uso seguro de la nube:

1. Implementar cifrado de datos. Esto puede realizar desde la base de datos, discos virtuales y necesariamente en las transmisiones de los mismos. Todo depende de los requerimientos del STI.
2. Establecer medidas de emergencia. Contar con respaldos automáticos que nos permitan recuperar la mayor cantidad de información, así como la restauración del STI, en el menor tiempo posible; en la nube esto es una realidad muy viable.
3. Contar con un proveedor de nube confiable. En caso de utilizar un servicio comercial, es determinante que el proveedor pueda contar con los más altos estándares de seguridad y privacidad de la información posible, además de poder cumplir con las políticas y lineamientos de la IES.
4. Emplear personal competente. Es importante contar con personal que tenga las suficientes competencias para poder realizar los trabajos en la nube y así poder explotar sus habilidades en el alcance de los objetivos.

Conclusiones

La nube no es una panacea, pero sí es una gran respuesta y puede representar la solución a múltiples escenarios de STI, sin embargo, si no se realiza bajo esquemas de seguridad adecuados es muy probable que se convierta en una pesadilla, y por ende se pierda información y/o reputación de la IES.

Es de suma importancia que el proveedor con que trabajemos cuente con estándares altos de seguridad y privacidad, ya que, al estar ocupando sus servicios, estaremos depositando la confianza de la IES en su infraestructura.

No se debe temer a la nube, pero sí debemos contar con todos los requisitos de gestión de las TIC y la seguridad de la información, es decir, encaminar las buenas prácticas y personal capacitado de la IES, para poder alcanzar el objetivo planteado, o como dirían en Los Tres Mosqueteros “todos para uno y uno para todos”.

Referencias

López, M.C.; Flores, K. (2010, octubre). Las TIC en la Educación Superior de México. Políticas y acciones. Repositorio Digital Universitario de Materiales Didácticos. Recuperado de http://repositalcuaed.unam.mx:8080/jspui/bitstream/123456789/1507/1/Las%20TIC%20en%20la%20educación%20superior%20de%20México.doc

Red de Seguridad en Cómputo (2005, noviembre). TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL SUR-ESTE DE MÉXICO. Consejo Regional Sur-Sureste de la ANUIES. Recuperado de http://www.anuies.mx/media/docs/89_2_1_1103091247Articulo_Tecnologias_de_la_Informacion.pdf

Si quieres saber más consulta:

- Cómputo en nube: ventajas y desventajas
- Tips de seguridad para el cómputo en nube
- Privacidad de la información en la nube

Israel Josué Novelo Zel

Maestro en Tecnologías de Información por la Universidad Virtual del Tecnológico de Monterrey. Cuenta con una especialización en Administración de Tecnologías por la Universidad Autónoma de Yucatán.

Es Responsable de Seguridad y Servicios de Tecnologías de Información, en la Coordinación Administrativa de Tecnologías de Información, Universidad Autónoma de Yucatán. Cuenta con 15 años de experiencia en seguridad en cómputo, gestión de tecnologías de información, servicios virtuales, gestión de la nube privada y pública.

Políticas de seguridad informática para las necesidades del usuario actual

Héctor Jesús Pérez Mancilla

Los equipos que alguna vez fueron máquinas superpotentes con millones de ciclos por minuto, ahora son sustituidos por pequeñas máquinas con 1/16 de su tamaño original, con la capacidad de ser portátiles e incluso de cuidar la salud del ser humano. Así también, Internet está marcando una tendencia hacia el cambio ubicuo que en la actualidad llamamos el Internet de las Cosas.

Por ello nos vemos en la necesidad de incrementar el nivel en la seguridad e implementar más opciones de cualquier política segura que conozcamos, ya que ahora no solamente se trata de salvaguardar la seguridad de la información, sino también la integridad del propio ser humano.

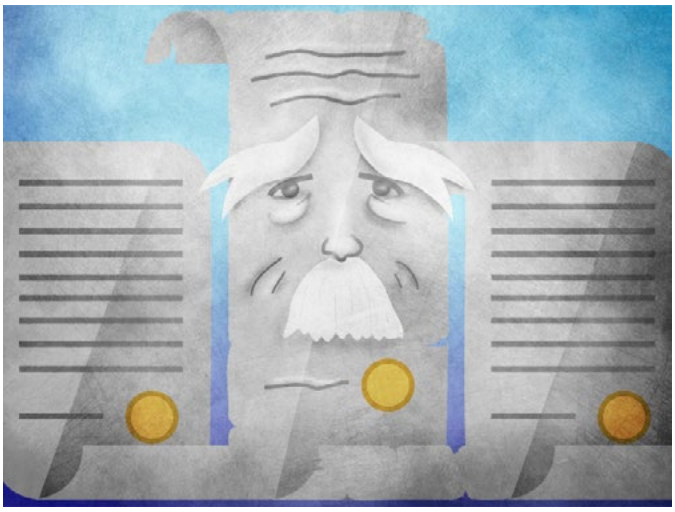
Es por eso que a las personas que se dedican a la seguridad informática de cualquier empresa u organización se les ha dado una nueva encomienda, una misión realzada en el ámbito de la seguridad informática que demanda un manejo de políticas más complejas, con mayor magnitud y con el fin de alcanzar el marco que nos garantice la seguridad de la información, siempre con un lenguaje asimilable para el usuario promedio y un entendimiento mínimo en la tendencia de la seguridad.

En este artículo se destacará la necesidad de tener buenas prácticas en las empresas sobre el manejo de la información y sus políticas de seguridad. En la mayoría de éstas el usuario promedio tiende a descuidar sus activos, ya sea personal o empresarial, con el fin de cumplir con su trabajo, lo cual provoca un incremento en los reportes de incidentes que se emiten en las organizaciones.

Se han encontrado empresas que carecen de políticas de seguridad informática o tienen algunas mal elaboradas o sin sentido, y otras que preservan políticas extremadamente ambiciosas y difíciles de cumplir. Un claro ejemplo es una entidad que basa la creación de sus políticas sin dimensionar el alcance de un modelo como ISO 27001 y sólo redacta el documento con el propósito de cumplir el estándar, sin antes saber los retos tecnológicos que conlleva.

Podemos encontrar una empresa que, con el fin de tener un modelo de políticas, únicamente las elabora basándose en reglamentos, sin dar prioridad a la función principal: la protección de la información. Esto no sólo lleva a tener un régimen de políticas pobre, sino que carecen de continua revisión y cambio con el fin de cumplir los requisitos, auditorías o procesos de evaluación empresarial.

También existen empresas que se proponen elaborar políticas extremadamente ambiciosas que no podrán cumplir ya que, por lo regular, no tienen los recursos necesarios en cuestiones económicas, tecnológicas o humanas. Normalmente el ciclo de vida de este documento provocará la desaparición y extinción de éste de forma total o, en el mejor de los casos, su adecuación favorable.



¿Cómo elaborar un documento de políticas de seguridad informática y de seguridad de la información?

Dada la importancia de un documento de esta magnitud en cualquier empresa y en especial en las empresas dedicadas a las TIC, al escribirlo deben contemplarse previamente los siguientes puntos:

1. Elaborar políticas claras. Cualquier usuario promedio podrá entenderlas, llevarlas a la práctica y cumplirlas en su totalidad.
2. Desarrollar políticas que la organización pueda realizar en función del usuario, ya que éste es quien logra que se lleven a cabo.
3. Establecer políticas que la alta dirección de la organización desee y pueda cumplir, no sólo elaborarlas para aprobar una auditoría o un proceso de evaluación.
4. Fijar políticas concretas. Deben mostrar tanto lo que se debe realizar como las limitantes de lo que se pretende proteger o no comprometer.
5. Toda política que se pretenda incluir en el documento se debe difundir; ningún usuario debe desconocerla.
6. El documento debe estar en un lugar de fácil acceso y consulta para que los usuarios de la compañía puedan leerla no como un complemento a sus labores sino como una obligación expresa en su contrato.
7. Se debe dar una clasificación de protección de la información al documento, de eso dependerá su capacidad de difusión hacia los usuarios.
8. Es indispensable que los proveedores de servicios ajenos a la organización conozcan el documento para que se apeguen a ellas y apoyen en su cumplimiento.
9. Las políticas deben tener una campaña de difusión: Puede ser distinta pero no ajena a la campaña de concientización en materia de seguridad de la información, ya que de ésta dependerá que el documento sea analizado por todos los usuarios de la empresa y no sea olvidado.

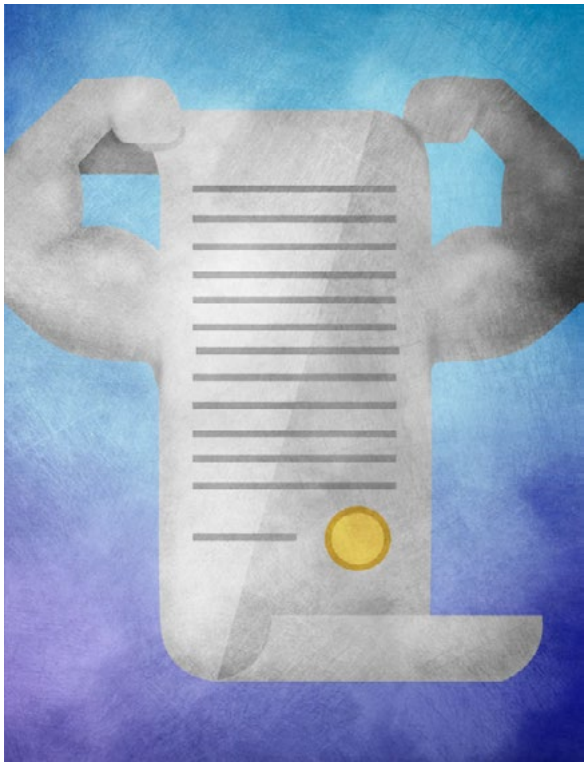
10. Se debe tener como mínimo una revisión del documento con una periodicidad menor a los 180 días. Lo más importante que debemos analizar y tener claro es que ninguna política es perfecta. Los usuarios tratarán de encontrar fallos en las mismas para burlarlas o no ser sancionados. Por eso, ninguna política es perpetua ni ha sido "escrita en piedra".

El marco de normatividad en el que nos basaremos para elaborar el documento deberá ser siempre aquel que nos acomode y sea acorde a nuestra organización (su giro, su capacidad tecnológica y su capacidad humana). No debemos ambicionar un marco normativo muy complejo si no lo vamos a cumplir, ya que de esto también depende que sea exitoso al ponerlo en marcha dentro de la empresa.

Respecto al marco de elaboración en que se basa, deberá ser siempre en total y completo apoyo de la dirección general o alta dirección de la organización y contemplar que la persona o área encargada de generar el mutuo acuerdo de documentación de seguridad sea totalmente ajena al área de tecnología. De esta manera evitaremos que exista un error muy común cometido en las organizaciones: atribuir funciones de juez y parte al área tecnológica.

Es preferible tener una persona o área de seguridad que no dependa de la tecnología y que esté siempre a la salvaguarda de la seguridad, verificando que se cumplan las políticas y que se gestionen correctamente los incidentes generados, con un seguimiento continuo de los mismos hasta su remediación.

No se puede dejar fuera nunca la ayuda de los consultores externos quienes, a través de su perfil de consultoría en seguridad informática, han obtenido la certeza de verificar un documento de políticas en el marco de su normatividad hacia la organización. Siempre es válido utilizar a una de estas personas que no intervenga directamente en la organización, únicamente en su verificación de documentación y procedimientos de seguridad informática.



¿Cómo saber cuándo nuestro documento de políticas está terminado?

Las características de nuestro documento al final de la redacción incluyen:

- Ser entendible.
- Ser fácil de asimilar.
- Que pueda ser cumplido por cualquier usuario de la organización.
- Ser factible para el área de tecnología.
- Estar disponible para cualquier miembro de la organización.
- Ser leído por los proveedores externos para que ayuden en su cumplimiento.
- Tener por completo el apoyo de la alta dirección de la organización.

Entonces podemos decir "misión cumplida" ya que así tendremos Políticas de Seguridad Informática y de Seguridad de la Información, y a partir de este momento comienza el cumplimiento del marco normativo en la organización del que serán partícipes los usuarios finales.

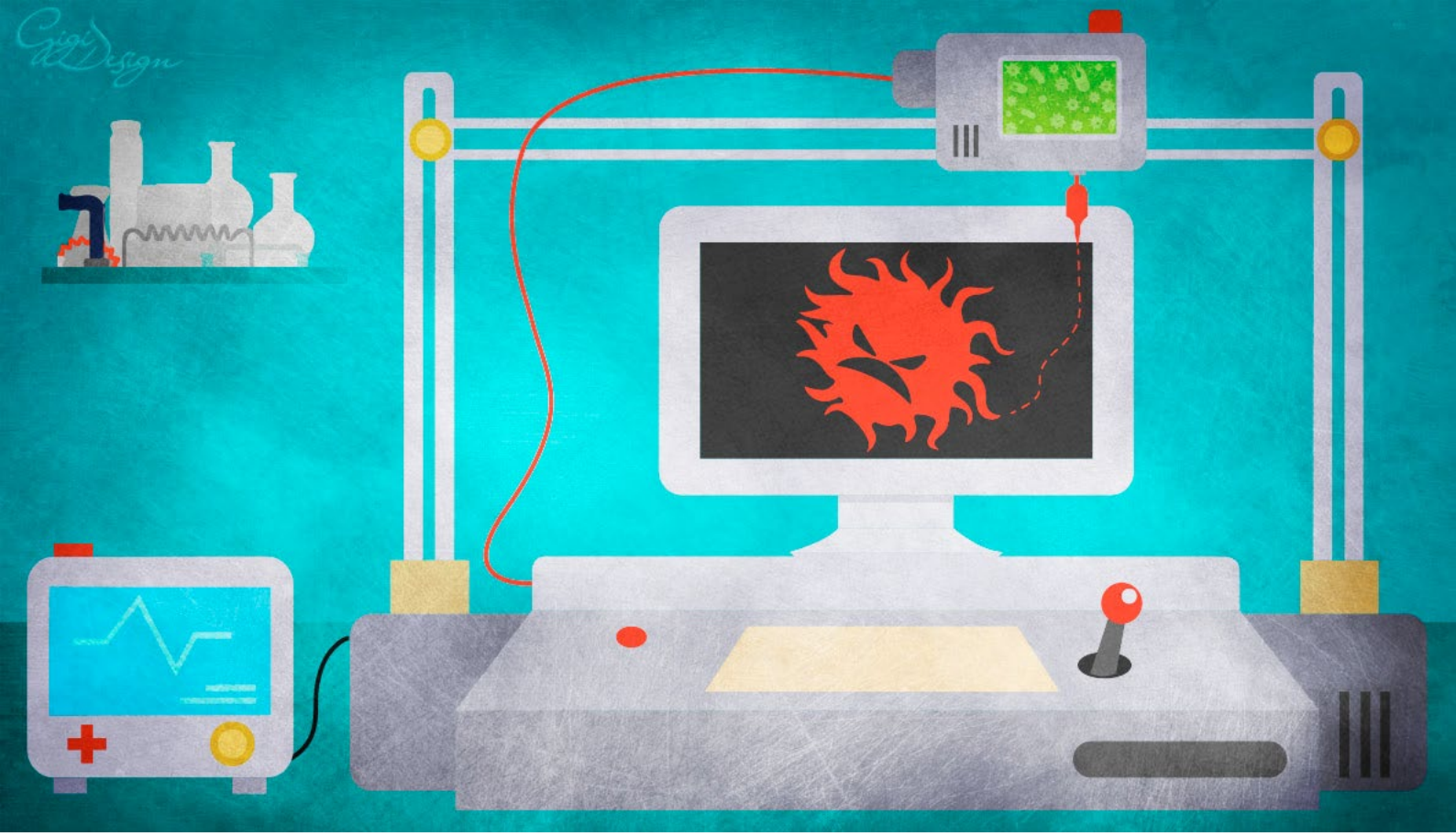
Si quieres saber más consulta:

- Gestión de seguridad de la información basado en MAAGTICSI
- Lo que no debes pasar por alto para gestionar la seguridad de la información
- Hablando correctamente de la seguridad de la información

Héctor Jesús Pérez Mancilla

Ingeniero en Computación por parte del Instituto Politécnico Nacional, egresado de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Posee las certificaciones Certified Ethical Hacker, Certified Hacking Forensics Investigator, Certified Network Security y Certified System Administrator por pate del EC-Council; y las Certified Information Systems Auditor y COBIT por parte de ISACA.

Ha dirigido diversas gerencias de sistemas en el sector privado y dedicado en los últimos 10 años de experiencia en preservar la seguridad de la información en diferentes áreas de seguridad desde formar parte de equipos de pruebas de penetración hasta dirigir actualmente equipos de cumplimiento de seguridad y auditoria de sistemas en su rol actual como Oficial de Seguridad de la Información de la empresa ATEB Servicios, S.A. de C.V.



Ghost: Honeypot para malware que se propaga a través de dispositivos USB - Parte II

Jonathan Banfi Vázquez

En el artículo anterior se describió una forma de instalar Ghost y algunas de sus características. En esta ocasión, se explicará cómo se configura en el laboratorio virtual para ver paso a paso la captura de una muestra de *malware*.

En esta sección se mostrará el funcionamiento del *honeypot* Ghost al infectar una de las máquinas de nuestro laboratorio con algunas muestras de *malware* que se propagan a través de dispositivos de almacenamiento extraíbles.

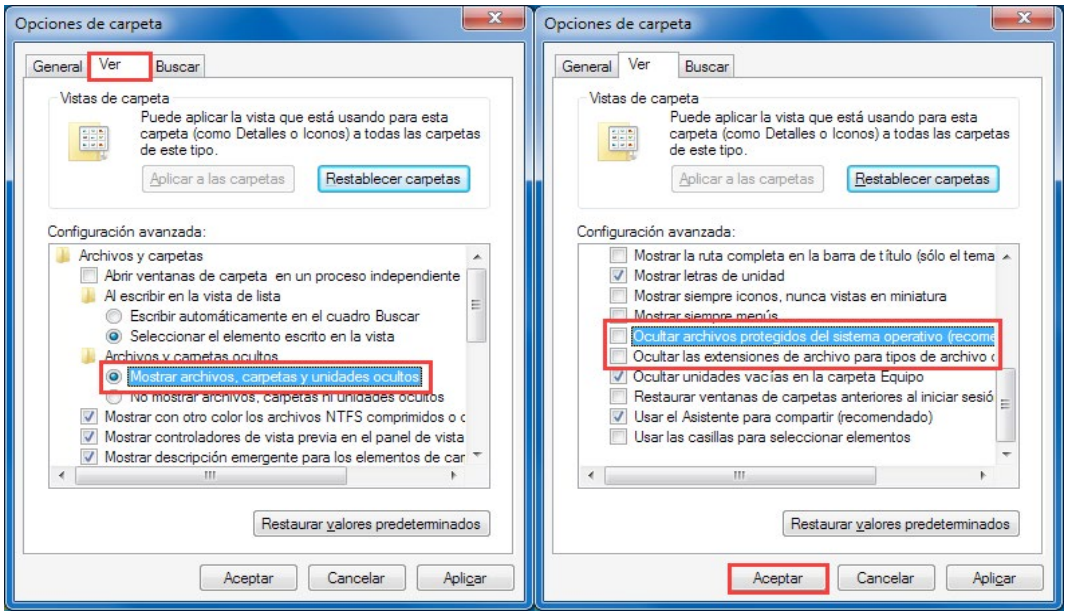
Configuración del laboratorio virtual

La siguiente configuración es sólo para ejecutar y visualizar correctamente los cambios realizados por las muestras que se analicen en nuestro laboratorio.

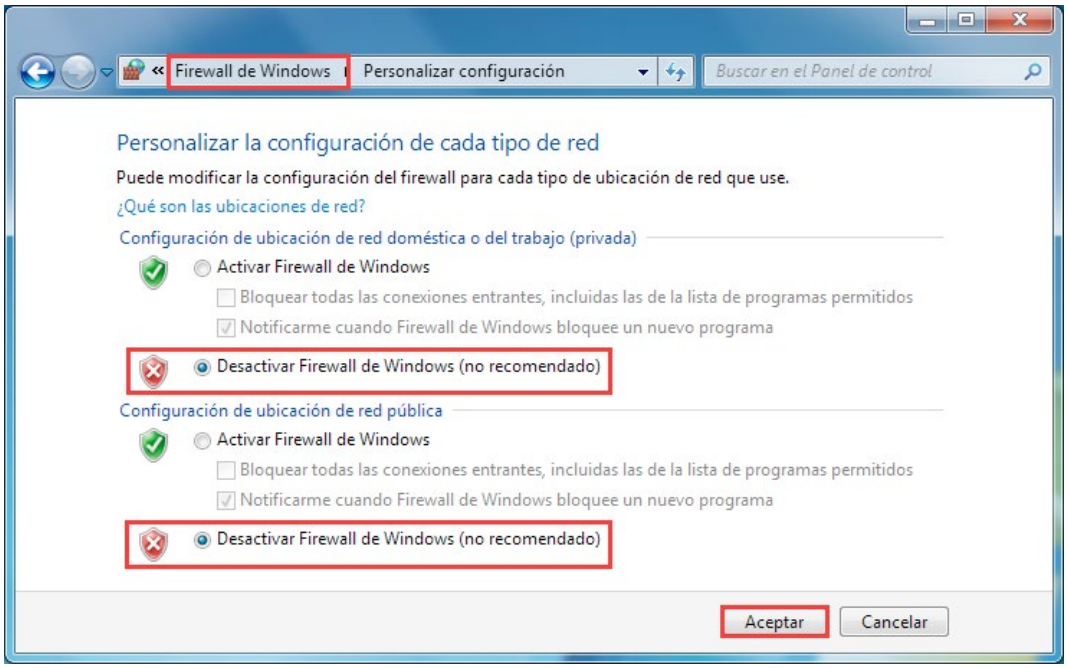
Se describe el procedimiento para Windows 7 y de igual manera se debe realizar en Windows XP.

Abrir el Explorador de Windows (Menú Inicio ‣ Equipo ‣ (tecla ALT) ‣ Herramientas ‣ Opciones de carpeta... ‣ pestaña Ver) para:

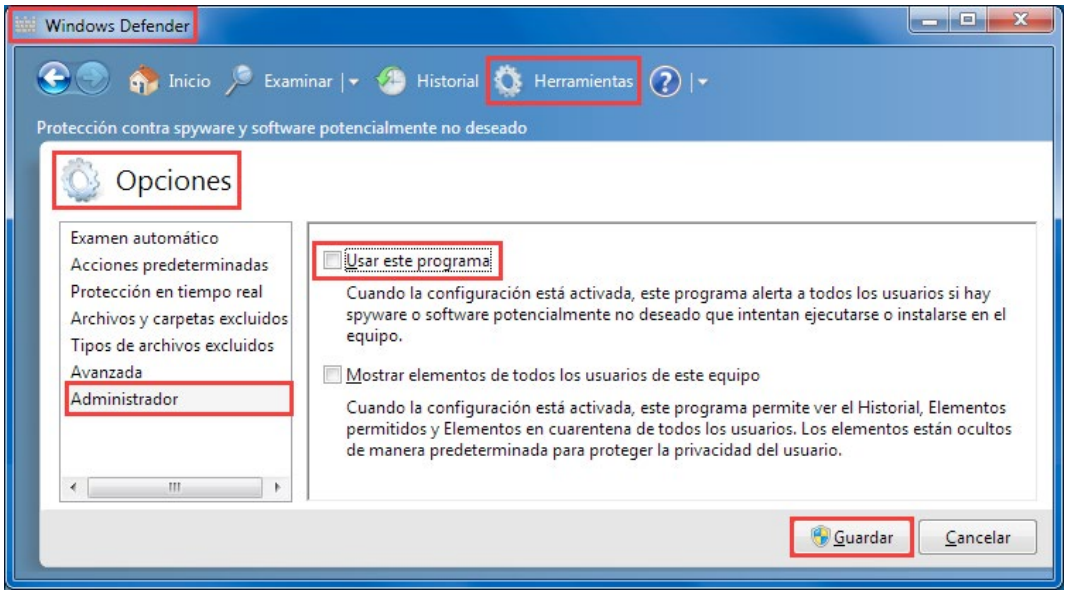
- Mostrar todos los archivos y carpetas ocultos
- No ocultar archivos protegidos del sistema operativo
- No ocultar las extensiones de archivos conocidos



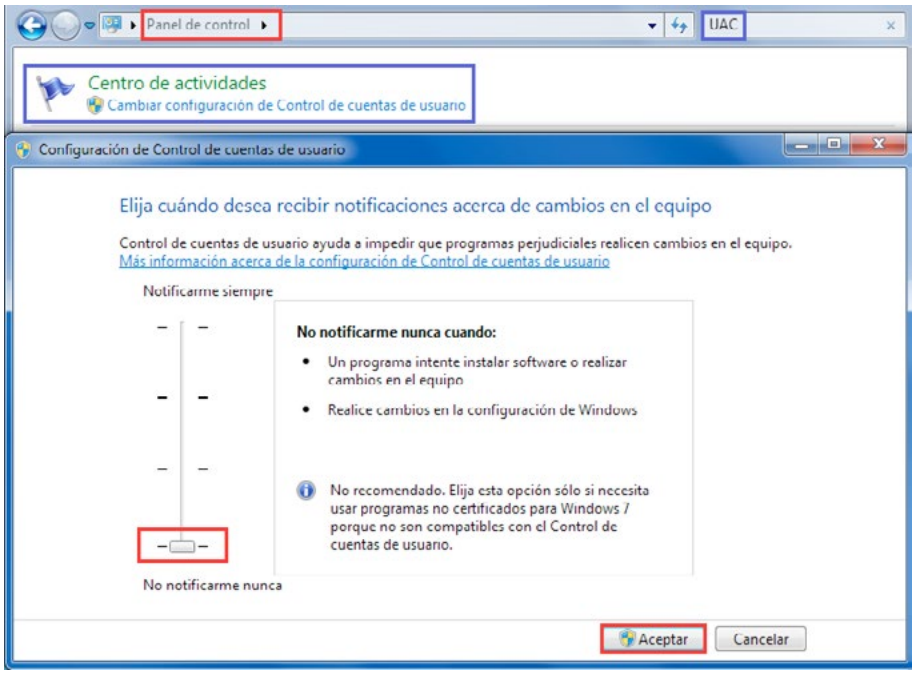
Desactivar el *firewall* de Windows desde el Panel de control:



Quitar la selección “Usar este programa” en Windows Defender para evitar que detecte las muestras que se manejen en el laboratorio:



En Windows 7 deshabilitar la característica del Control de Cuentas de Usuario (UAC) para permitirles mayor libertad al *malware* de interactuar con el sistema, así como a las herramientas de monitoreo que requieren permisos de administrador para funcionar correctamente, como en el caso de Ghost.

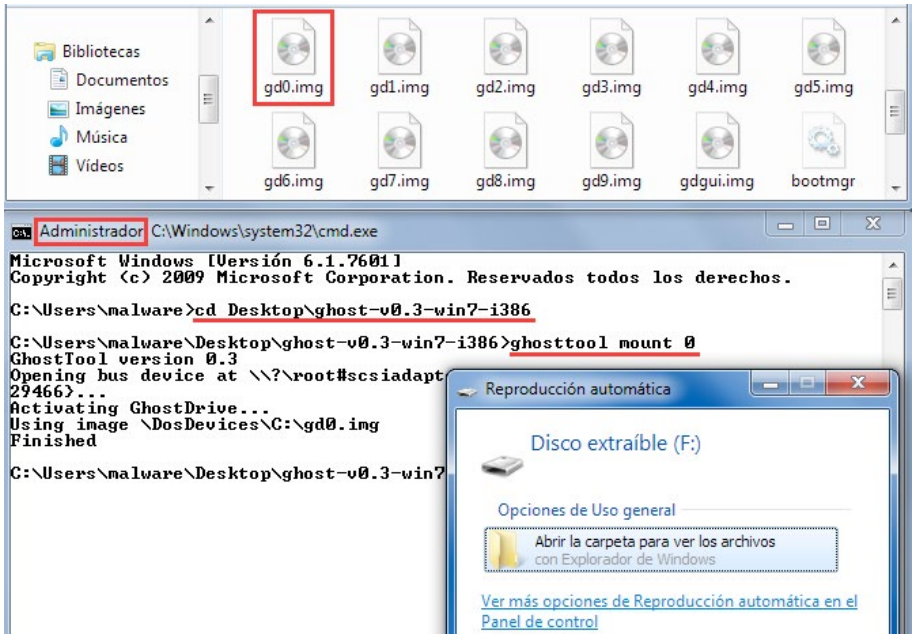


Creación de archivos y carpetas en el dispositivo USB

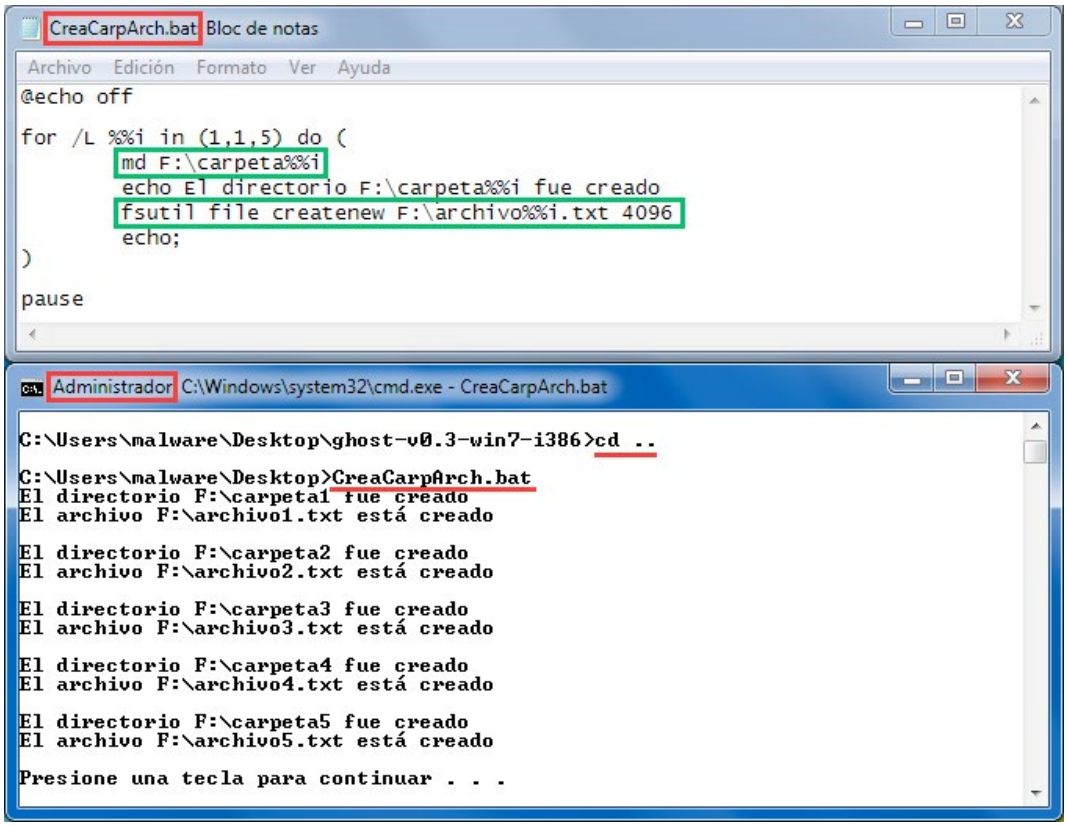
Antes de infectar la máquina Windows 7 crearemos algunos archivos y carpetas en el dispositivo de almacenamiento extraíble emulado para ver gráficamente su afectación una vez infectado el sistema.

Primero, ejecutar el programa cmd.exe (se iniciará con permisos de administrador por la configuración del UAC) y montar uno de los dispositivos USB, en nuestro caso será el dispositivo “0”:

- ghosttool mount 0

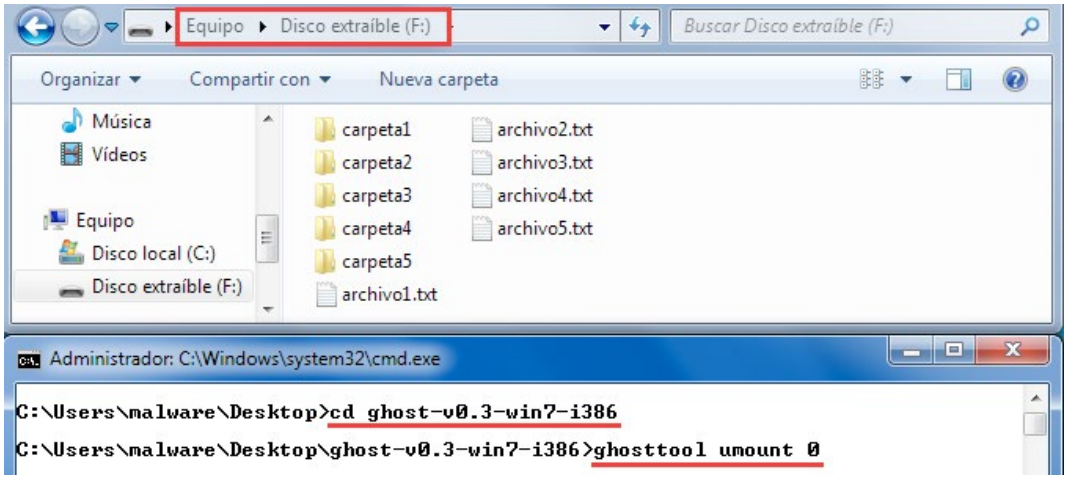


Posteriormente, para crear carpetas y archivos en el dispositivo se puede utilizar el siguiente *script* tomando en cuenta que la unidad montada tiene asignada la letra “F”.

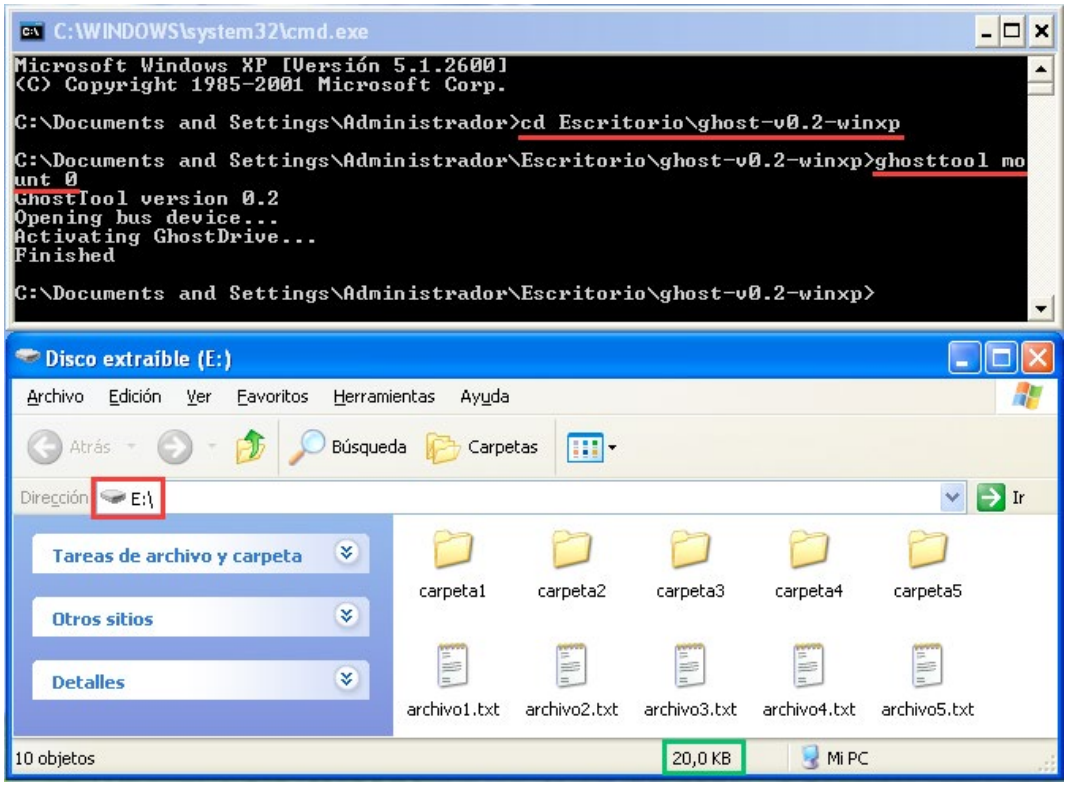


Finalmente, desmontar la unidad:

- ghosttool umount 0



Nota: La creación de carpetas y archivos en la imagen “gd0.img” (que montamos con el identificador 0) son cambios que quedan guardados, por lo que en una infección por malware se puede realizar una copia de dicha imagen y enviarse a otro equipo donde se pueda analizar la evidencia con mayor detalle.



Infección por software malicioso que se propaga a través de dispositivos extraíbles

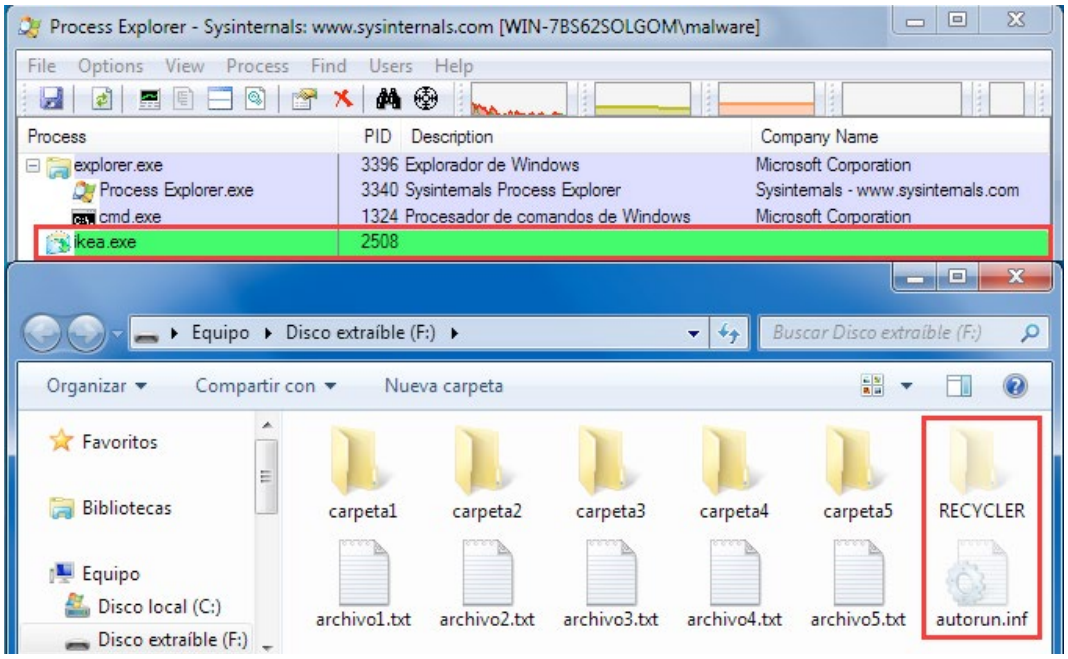
Los análisis que se mostrarán a continuación están enfocados únicamente a presentar la actividad realizada en el dispositivo extraíble emulado y no toda la actividad realizada en el equipo por fines demostrativos y extensión del artículo, pero pueden consultar los enlaces proporcionados para mayor información de la propagación, detección y la manera de cómo recuperar los archivos ocultos. El proceso de infección que se realizará por cada muestra es el siguiente:

- Iniciar la herramienta Process Explorer
- Ejecutar el software malicioso
- Montar el dispositivo USB con Ghost
- Observar los cambios realizados por la muestra

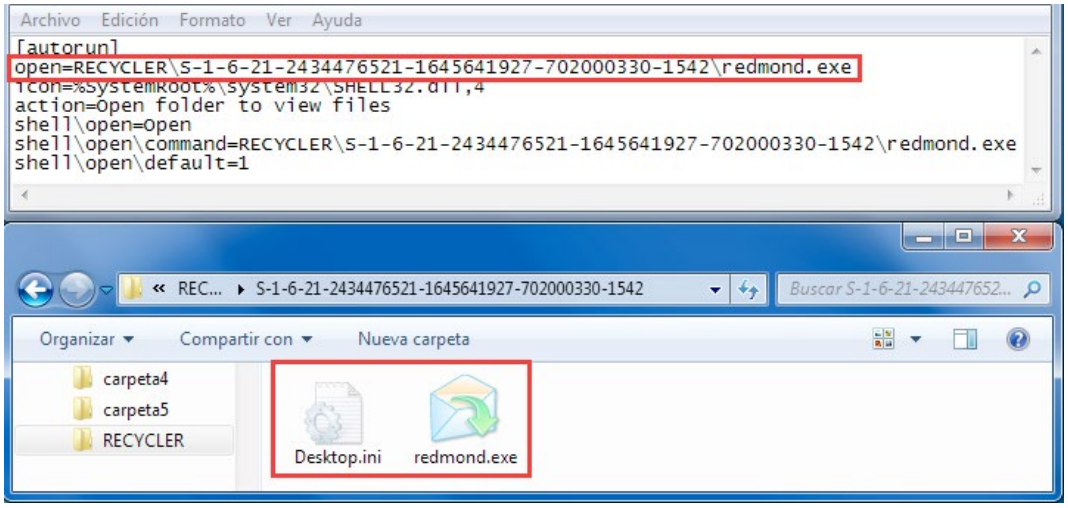
Caso 1: Creación o modificación del archivo Autorun.inf:

- **ikea.exe** (sha1: 3d1d5cf6dd898b81261495a3c7cfa01911af84d0)

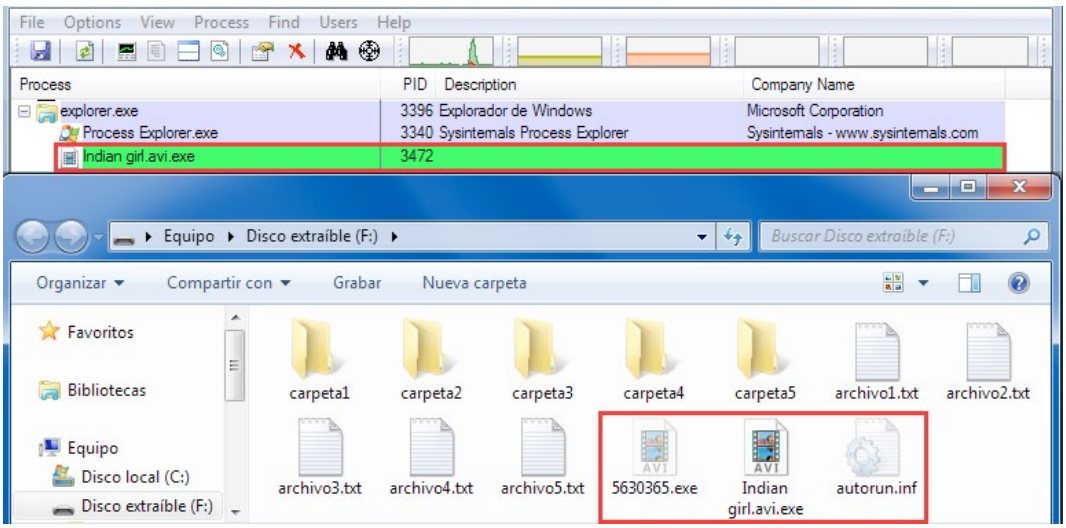
Una vez infectado el sistema se crea el archivo “autoruns.inf” y la carpeta “RECYCLER” en la raíz de la unidad emulada.



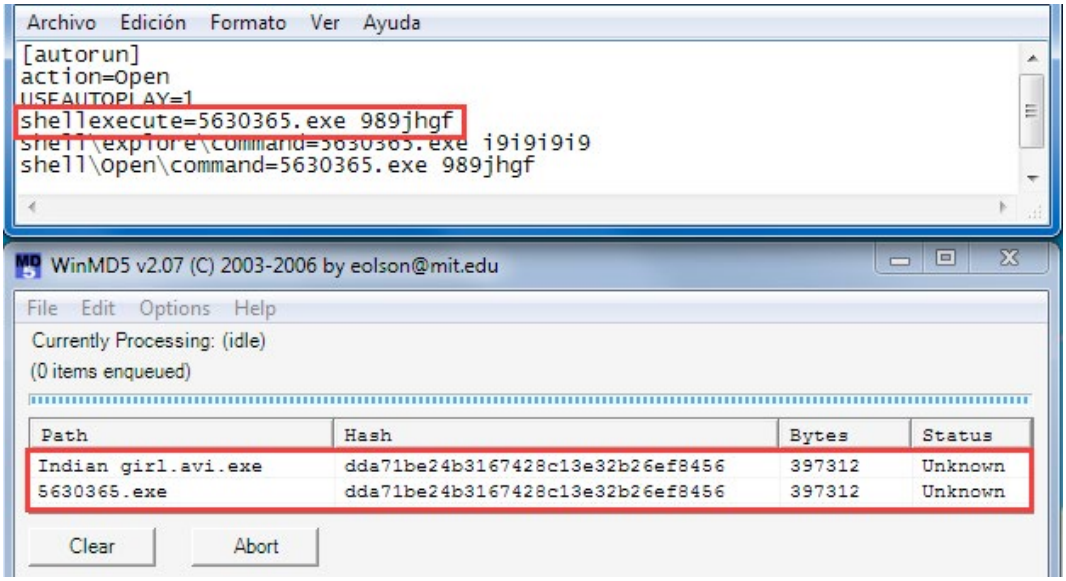
En el archivo autorun.inf la entrada "*open*" especifica la aplicación que AutoRun iniciará en la máquina (si es que tiene habilitada la función) cuando el usuario inserte el dispositivo extraíble. El archivo ejecutable se trata de una réplica de la muestra original.



- **Indian girl.avi.exe** (sha1: 2235d96e7c5b1044b19819e0b83a77b7f0707ee3)



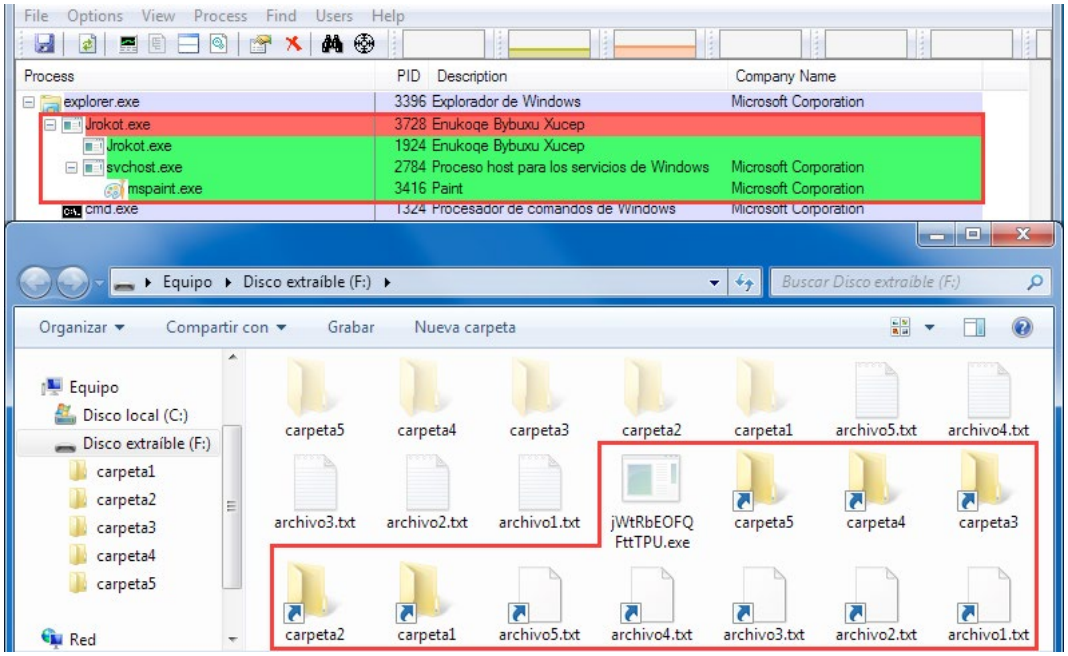
En el archivo autorun.inf la entrada "*shellexecute*" se utiliza en lugar de "*open*" cuando se requiere iniciar un archivo que no es ejecutable. Los archivos ejecutables son réplicas de la muestra original.



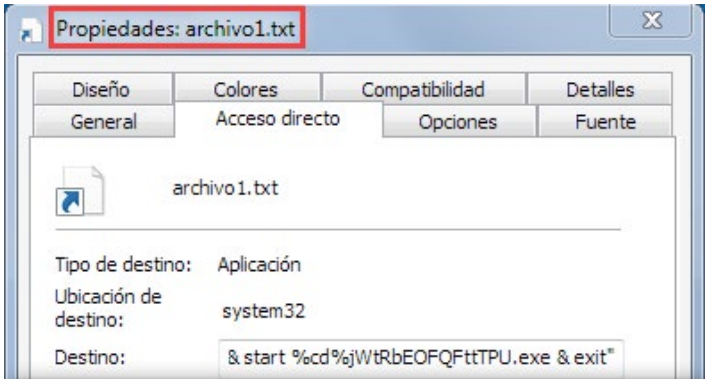
Caso 2: Creación de varios accesos directos:

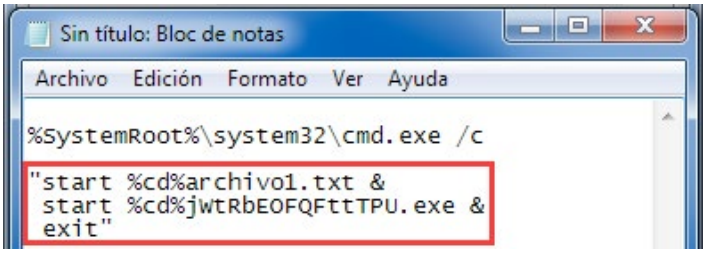
- **Jrokot.exe** (sha1: ead70669bdca4e25fa7be5d3ca3e482d266710cc)

Una vez infectado el sistema, se crean en la raíz de la unidad emulada accesos directos a las carpetas y archivos que el *malware* configuró como ocultos para forzar al usuario a darles doble clic.

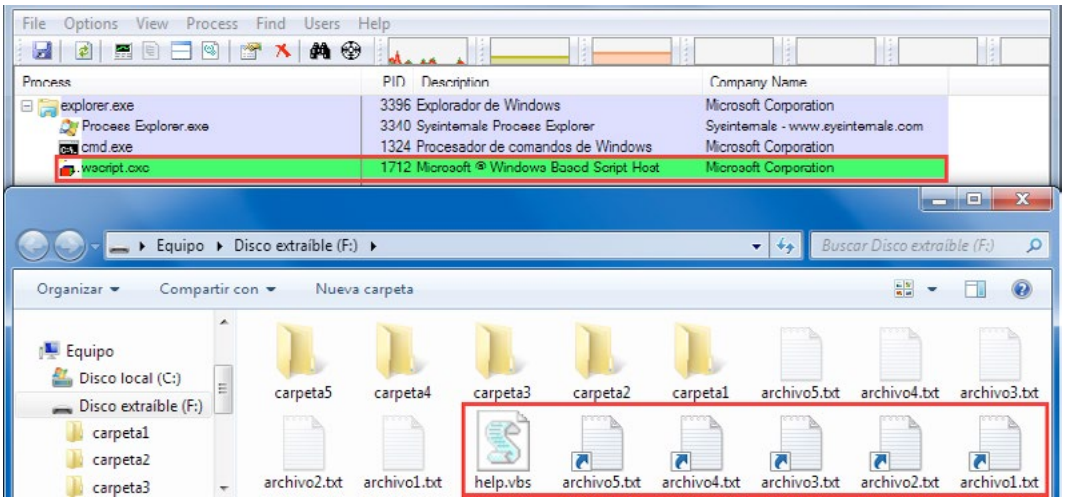


El acceso directo está diseñado para abrir el archivo al que apunta y además ejecutar el software malicioso en el dispositivo USB. El archivo ejecutable es una réplica de la muestra original.

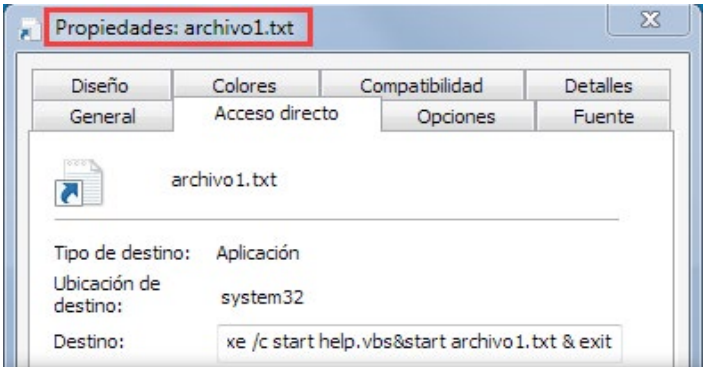


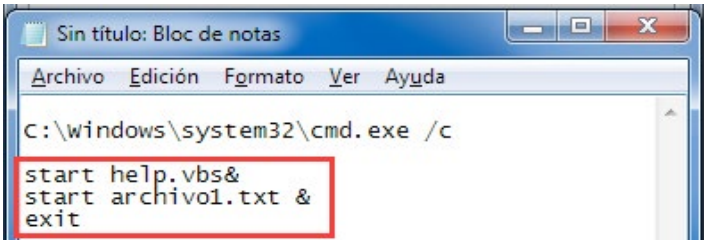


- **help.vbs** (sha1: 4586cf735e2ead5b6a57b2870076717014da16d4)



En este caso, el software malicioso únicamente cambia los atributos de los archivos y no de las carpetas. El código en *Visual Basic Script* se trata de una réplica de la muestra original.



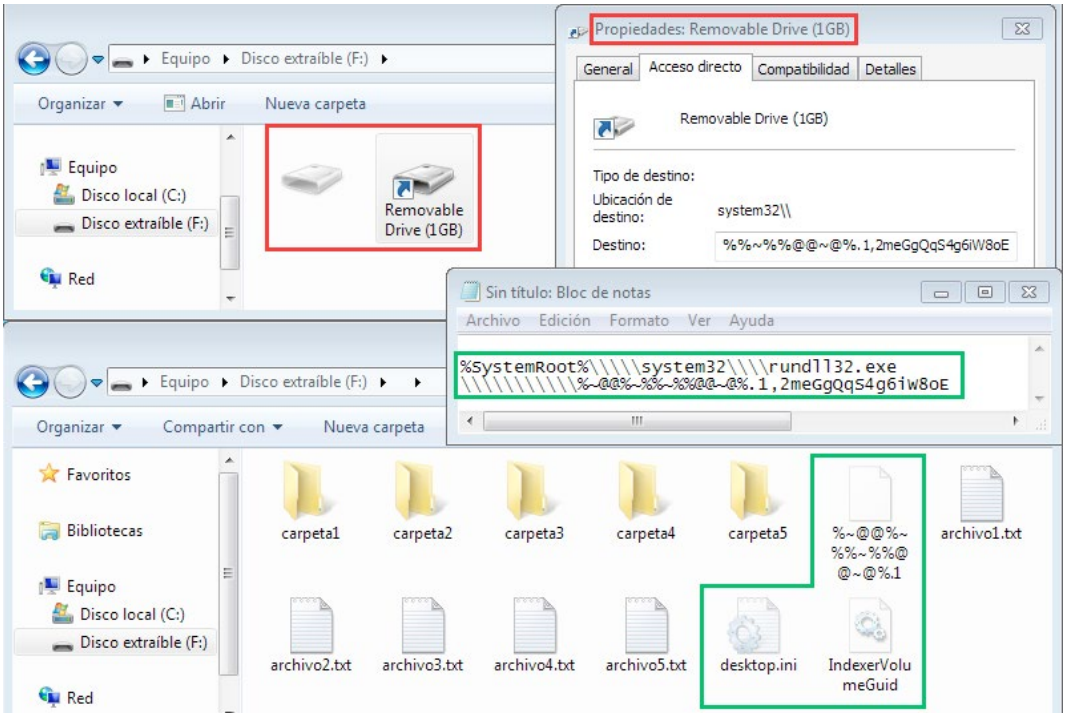


Caso 3: Creación de un sólo acceso directo

A continuación, se listan algunas piezas de *malware* identificadas recientemente que se propagan a través de dispositivos USB:

Nombre de la DLL maliciosa	Nombre de la función de inicio
lmCY2So2.m4Q.2Kg.oIm4Y2C.g2S2K.uKg2.we4I.e4Y2mm	tJnHlBf9d3X1Jnnn
cnu29AE.dhlw.x4CGNV.jqy29.BJTbl.w4B.biquUb.hYSW	t07FMUbiqx5CJHve
Zn126HIY.Wk2FXp.7Kcu7Q.6JaxAJX.k2Kcu.Nfk.RjwEW5L.2FYTOM	5CJKSZghpw3BIMQQ
~@%~@%~@%~@%~@~%.1	iOeK06mS8oUaqwc

En este caso se infectó el equipo del laboratorio con la muestra “~@%~@%~@%~@%~@~%.1” que tiene por firma sha1 “dd466d5b7ec61f28d07d2b29ef241d75c77aeda7” y la muestra generada en el dispositivo USB con nombre “%~@@%~%%~%%@@~@%.1” tiene por firma sha1 “dd64b7e3f965130aa3aacfa30d71da90f63d2f74”, por lo que se concluye que al infectar el dispositivo extraíble cambia su estructura interna (tamaño del archivo y nombre de la rutina que tiene programada) pero no su funcionamiento, dando origen a una nueva variante utilizando técnicas de polimorfismo.



Con la información mostrada en estos dos artículos pudimos darnos cuenta de lo importante que es la recolección de evidencia generada por el software malicioso que se propaga a través de dispositivos USB, ya que es posible identificar características sobre nuevos vectores de infección, propagación y métodos de evasión de antivirus para que las soluciones de seguridad tomen cartas en el asunto y puedan proteger a sus usuarios de las amenazas más recientes. Además, no debemos tomar a la ligera este tipo de propagación de malware, ya que continúa siendo muy utilizado para distribuir amenazas como Cryptolocker y USB Thief que pueden provocar un impacto significativo tanto en equipos de usuarios caseros como en grandes empresas.

Si quieres saber más consulta:

- Propagación de malware a través de dispositivos USB
- Script en Visual Basic ataca dispositivos USB, ¿cómo se propaga?
- Eliminar el virus de acceso directo USB

Jonathan Banfi Vázquez

Ingeniero en Computación por la Facultad de Ingeniería de la UNAM, con módulo de salida Redes y Seguridad.

Formó parte de la tercera generación del Programa de Certificación Cisco CCNA Exploration. Fue miembro de la sexta generación del Plan de Becas en Seguridad Informática de UNAM-CERT.

Cuenta con las certificaciones GIAC Reverse Engineering Malware (GREM) del SANS Institute y Certified Ethical Hacker (CEH) de EC-Council.

Actualmente labora en la Coordinación de Seguridad de Sistemas e Información de Telmex como Analista de Software Malicioso.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad *Cultura de prevención para* TI
No.27 / septiembre - octubre 2016