Buenas prácticas en seguridad informática

Autor: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Martes 30 de Junio de 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Índice

Buenas prácticas para proteger el entorno de información

Introducción

Al igual que las amenazas informáticas en general, los códigos maliciosos han ido evolucionando a la par de las tecnologías de información y comunicación, aumentando considerablemente el nivel de complejidad y agresión. Es por ello que la visión y la filosofía de ESET contemplan la protección de manera proactiva, no sólo a través de sus soluciones de seguridad sino también a través de la educación.

Es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información, y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas. Pero para ello inevitablemente se deben conocer los peligros latentes, y cómo detenerlos a través de mecanismos de prevención **[1]**.

El presente documento expone medidas de seguridad tendientes a minimizar el volumen de "potenciales víctimas", brinda herramientas preventivas para cada una de las tecnologías y servicios más populares y más utilizados por los usuarios y aborda en cada punto los mecanismos de prevención que permiten detectar, de manera temprana y sin acciones complejas, las acciones maliciosas más comunes.

Mantener actualizado el sistema operativo y las aplicaciones

La historia del malware **[2]** nos brinda la respuesta de por qué es importante mantener actualizados los sistemas operativos (SO) y las aplicaciones **[3]** con sus correspondientes parches de seguridad, nombre que recibe el código que soluciona una debilidad en un SO o aplicación.

Códigos maliciosos como Slammer, Sasser o Zotob, que infectaban los sistemas a través de vulnerabilidades (debilidades en el código de los SO y aplicaciones) durante los años 2003, 2004 y 2005 respectivamente, y el reciente gusano Conficker, aparecido a finales de 2008 **[4]**, son pruebas de ello.

En cuanto a este aspecto de la seguridad, las medidas prácticas de prevención se enfocan en:

- No descargar actualizaciones desde sitios de dudosa reputación y hacerlo sólo desde sitios de confianza. Descargar las actualizaciones desde sitios no oficiales implica un potencial riesgo de infección.
- Descargar las actualizaciones a través de los mecanismos ofrecidos por el fabricante. En el caso de las actualizaciones de productos de Microsoft, la disponibilidad de los mismos es informada el segundo martes de cada mes, aunque puede haber excepciones en casos de vulnerabilidades críticas.
- Para las plataformas Microsoft se puede:
    - Acceder al sitio web de Windows Update[1] para obtener los últimos parches de seguridad
    - Configurar en el Centro de Seguridad de Windows la automatización, o no, de descarga de actualizaciones
    - Utilizar herramientas gratuitas como MBSA[2] (*Microsoft Baseline Security Analyzer*) para verificar la falta de actualizaciones en el sistema operativo, o PSI[3] (*Personal Software Inspector*) de la empresa Secunia para chequear las aplicaciones
    - Implementar (en entornos corporativos) los WSUS[4] (Windows Server Update Services) de Microsoft
- También en entornos corporativos, y sin importar la plataforma, se aconseja preparar políticas de gestión de actualizaciones claras, que permitan coordinar y administrar los parches de seguridad tanto de los sistemas operativos como de las aplicaciones. Lo ideal es que esta política de gestión forme parte de la PSI (Política de Seguridad de la Información)

[1] http://windowsupdate.microsoft.com

[2] http://technet.microsoft.com/es-es/security/cc184923.aspx

[3] http://secunia.com/vulnerability_scanning/personal

[4] http://technet.microsoft.com/en-us/wsus/default.aspx

Aseguramiento del sistema operativo

Otro de los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

- Deshabilitar las carpetas compartidas. Esto evita la propagación de gusanos que aprovechen ese vector como método de infección.
- Utilizar contraseñas fuertes **[5]**. El empleo de contraseñas fáciles de recordar es otra de las debilidades que los códigos maliciosos suelen aprovechar para propagarse por los recursos de información.
- Crear un perfil de usuario con privilegios restringidos **[6]**. Por defecto, el usuario que crean las plataformas Windows al momento de su implementación posee privilegios administrativos. Esto es un factor que aumenta la probabilidad de infección.
- Deshabilitar la ejecución automática de dispositivos USB **[7][8]**. Los dispositivos de almacenamiento removibles que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de gusanos.
- De ser posible, migrar hacia plataformas (sistemas operativos) modernas **[9]**. En la actualidad, los sistemas operativos antiguos (Microsoft Windows9x, NT) no cuentan con soporte técnico ni con actualizaciones de seguridad por parte de Microsoft, lo cual constituye un punto que permite la explotación de vulnerabilidades
- Configurar la visualización de archivos ocultos **[10]** ya que la mayoría de los códigos maliciosos se esconden en el sistema con este tipo de atributos.
- Configurar la visualización de las extensiones de archivos **[10]** para poder identificar las extensiones de los archivos descargados y no ser víctimas de técnicas como la doble extensión.

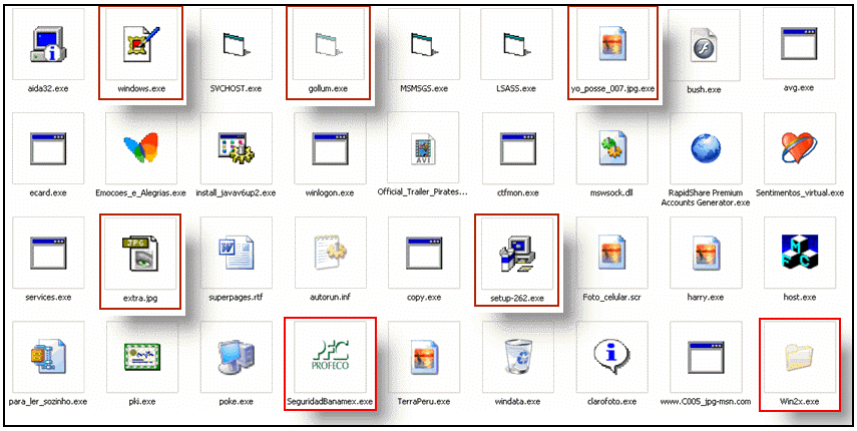

Imagen 1 – Incompatibilidad entre imagen del icono y extensión de archivo

Protección en el correo electrónico

El correo electrónico constituye uno de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de códigos maliciosos.

En consecuencia, a continuación se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante el uso del correo electrónico.

Spam

El spam **[11]** es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo de los usuarios.

Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos y por lo tanto se recomienda:

- No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto asegura que no se ejecutará un malware.
- Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, ya que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión del mismo.
- Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers [5]
- Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
- No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
- En lo posible, evitar el re-envío de mensajes en cadena (por lo general son hoax) **[12]**, ya que suelen ser utilizados para recolectar direcciones de correo activas.
- Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre Con Copia Oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.
- Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Esto previene que la dirección de correo personal sea foco del spam.

[5] Persona que disemina spam

- Utilizar claves seguras y cambiar la contraseña con periodicidad si se utiliza webmail. Esto favorece la seguridad de la cuenta, evitando que sea descubierta a través de un proceso sencillo.
- Configurar la pregunta secreta, además, de una forma que no sea adivinable para fortalecer aún más la seguridad de la cuenta.
- Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.
- También es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia. De esta manera se preserva la privacidad de la cuenta de correo y, por ende, la información que se intercambia a través de la misma.

Phishing

El phishing **[13]** es una modalidad delictiva encuadrada en la figura de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico.

Entre las buenas prácticas de seguridad que se recomiendan a los usuarios, para que éstos eviten ser víctimas del phishing, están las siguientes:

- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.
- Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles ya que suelen ser métodos de Ingeniería Social **[14]**
- No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden redireccionar hacia sitios web clonados o hacia la descarga de malware.
- Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La "***s***" final, significa que la página web es segura **[15]** y que toda la información depositada en la misma viajará de manera cifrada.
- Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado.
- Revisar que el certificado digital no haya caducado, ya que el mismo podría haber sido manipulado intencionalmente con fines maliciosos.
- Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.
- Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.
- Habituarse a examinar periódicamente la cuenta bancaria, a fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

- Denunciar casos de phishing (dentro de lo posible) en la entidad de confianza **[16]**, ya que además de cortar la actividad del sitio malicioso, se colabora con la seguridad general de la navegación en Internet.

Imagen 2 – Ejemplo de phishing

Para obtener más información sobre cómo evitar el phishing y otros medios de engaño, fraude y estafa puede consultar el curso gratuito **Seguridad en las transacciones comerciales en línea** disponible en la Plataforma Educativa de ESET Latinoamérica **[26]**.

Seguridad en la navegación

En los últimos años, Internet se ha transformado en una plataforma de ataque **[17]** donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download **[18]**. En consecuencia, es fundamental navegar con cautela y tener presente las recomendaciones más importantes. Entre ellas:

- Evitar el ingreso a sitios web con contenidos que, dependiendo el país, son ilegales, como aquellos que ofrecen cracks y programas warez; ya que constituyen canales propensos a la propagación de malware.
- Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. Es importante no hacer clic sobre el botón **ejecutar** ya que esto provoca que el archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad.
- Descargar programas de seguridad solamente desde el sitio oficial del mismo, para evitar la descarga de archivos que pudieran ser previamente manipulados con fines delictivos.
- Si es posible, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.
- No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.
- Configurar el navegador web para minimizar el riesgo de ataques a través del mismo **[19]**.
- Instalar, en lo posible, un programa antivirus con capacidades proactivas, como ESET NOD32, que permita detectar códigos maliciosos incluso desconocidos y explorar con el mismo cada archivo descargado.
- Disponer, además, de un Firewall personal que permita bloquear comunicaciones entrantes y salientes. ESET Smart Security, por ejemplo, incorpora un Firewall personal de manera integrada.
- Tratar de no acceder a servicios como Home-Banking desde lugares públicos (ciber, bibliotecas, cafés, hoteles, etc.).
- Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se haya ingresado datos.
- El bloqueo de determinados sitios considerados maliciosos, ya sea porque descargan malware o porque contienen material de dudosa reputación, es también otra de las mejores prácticas que ayudan a la prevención y refuerzan la seguridad del equipo.

Seguridad en redes sociales

En la actualidad, las redes sociales **[20]** son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo, se torna necesario tener en cuenta y aplicar las siguientes medidas preventivas:

- Intentar no publicar información sensible y confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.
- También es recomendable evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático.
- Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público.
- No responder las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas.
- Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware, además de otras acciones ofensivas desde el punto de vista ético y moral.
- No abrir contenidos con spam a través de este medio. De esta manera se evita formar parte del ciclo de vida del spam a través de este canal.
- Cambiar periódicamente la contraseña para evitar que la misma sea descubierta fácilmente.
- Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente provienen de quien dice ser.

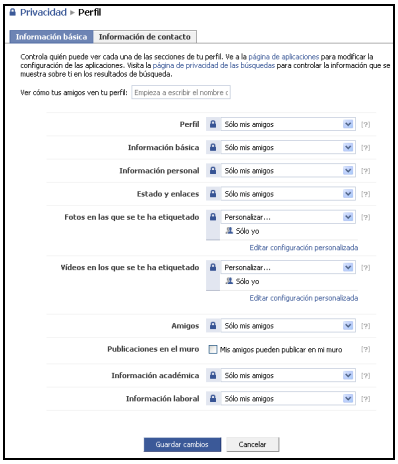

Imagen 3 – Configuración de privacidad en Facebook

Seguridad en redes P2P

Las redes Punto a Punto, más conocidas como P2P **[21]**, forman otro de los canales por donde se propagan diferentes amenazas informáticas y cuya relación con códigos maliciosos es muy activa. Esta situación obliga a tener en cuenta una serie de medidas preventivas tendientes a fortalecer la seguridad del sistema, entre las cuales se destacan:

- Explorar con una solución antivirus de alta efectividad en la detección de amenazas conocidas y desconocidas, como ESET NOD32, absolutamente todos los archivos que se descargan a través de esta red, sin importar su extensión.
- Evitar el almacenamiento de información confidencial y sensible en la misma computadora donde se comparten archivos por redes P2P, para evitar que la misma sea robada.
- Verificar que el programa cliente de intercambio de archivos no instale o descargue componentes extras, ya que en la mayoría de los casos son códigos maliciosos del tipo Adware/Spyware.
- Asegurarse de que los archivos a descargar no se encuentren sometidos a métodos de engaño como doble extensión, debido a que se trata de una técnica muy empleada por el malware.
- Controlar que exista coherencia entre el tamaño original del archivo descargado y el tamaño aproximado que debería tener, para descartar la posibilidad de que se esté en presencia de programas troyanos.
- Chequear que la carpeta de intercambio de archivos contenga sólo los archivos que se desea compartir.
- Revisar la configuración de seguridad del programa cliente. Esto ayuda a maximizar la seguridad durante el proceso de descarga de archivos.

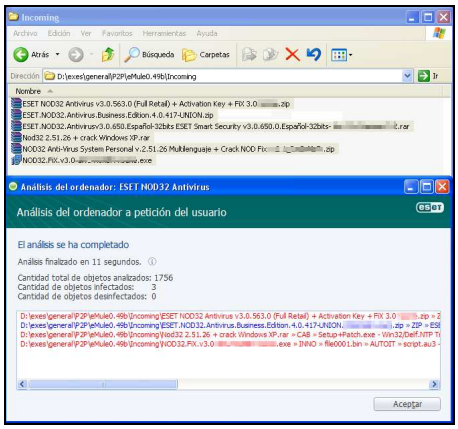

Imagen 4 – Descarga de malware a través de P2P

Seguridad en mensajería instantánea

Otro medio de comunicación popular, y que se emplea masivamente, son los clientes de mensajería instantánea **[22]**, que, en consecuencia, constituyen uno de los vehículos más explotados por diferentes amenazas, dentro de las cuales una de las más activas es el malware.

Por tal motivo poner en ejecución medidas tendientes a volver más seguro el cliente de mensajería instantánea se transforma en una tarea casi obligada. Para prevenir ser víctimas de acciones maliciosas llevadas a cabo a través de esta tecnología, se recomienda aplicar alguna de las medidas de seguridad que a continuación se describen:

- Evitar aceptar como contacto cuentas desconocidas sin verificar a quién pertenece, ya que en la mayoría de los casos se trata de intentos de engaños con fines maliciosos.
- No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma. Esto constituye una de las características principales de los códigos maliciosos que se propagan a través de este canal de comunicación.
- En caso de descargar archivos, explorarlos con una solución antivirus con capacidad proactiva como ESET NOD32 antes de ser ejecutados, para verificar que se encuentren libre de amenazas.
- Configurar en el cliente de mensajería la exploración automática de archivos en el momento de su recepción. La mayoría de estos clientes contemplan la posibilidad de configurarlos con un antivirus.
- Es recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar a páginas con contenido malicioso o hacia la descarga de malware.
- Cuando se reciben mensajes conteniendo un enlace no esperado, es recomendable preguntar si la otra persona realmente lo ha enviado; de esta manera se puede verificar la autenticidad del mismo.
- No escribir los datos de autenticación en páginas que prometen ofrecer información de contactos bloqueados y similares. Estos sitios suelen comprometer la privacidad de la información que se aloja en los correos, además de utilizar la cuenta con otros fines delictivos.
- Cambiar la contraseña de manera periódica. Ayuda a maximizar el nivel de seguridad.
- No compartir la contraseña con nadie. El carácter de ésta es privado, con lo cual lo recomendable es que sólo la conozca el usuario que la ha creado.
- Cuando se accede al mensajero desde lugares públicos, es recomendable deshabilitar la opción de inicio automático para que no quede la dirección (ni la contraseña) grabada. Esto evita que terceros inicien sesión de manera automática.
- No compartir información confidencial a través de este medio ya que la misma puede ser interceptada y robada con fines delictivos.

Seguridad en dispositivos removibles

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB **[23]** (memorias, cámaras digitales, filmadoras, teléfonos celulares, etc.), constituyen otro de los mayores focos de propagación/infección de códigos maliciosos. Por lo tanto, es necesario tener presente alguna de las siguientes medidas que ayudan a mantener el entorno de información con un nivel adecuado de seguridad, ya sea en entornos corporativos como en entornos hogareños:

- Establecer políticas que definan el uso correcto de dispositivos de almacenamiento removibles. Esto ayuda a tener claro las implicancias de seguridad que conlleva el uso de estos dispositivos.
- Brindar acceso limitado y controlado de los usuarios que utilizan estos dispositivos, para controlar la propagación de potenciales amenazas y el robo de información.
- De ser necesario, registrar el uso de los mismos y/o habilitar/deshabilitar puertos del tipo USB **[24]**. Esto permite un mayor control sobre el uso de dispositivos de este estilo.
- En casos extremos es recomendable bloquear, por medio de políticas de grupo, de dominio o corporativas, el uso de estos dispositivos.
- Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla. De esta forma, en caso de robo o extravío, la información no podrá ser vista por terceros.
- Ya sea en el hogar o en las organizaciones, se recomienda implementar una solución antivirus con capacidades proactivas como ESET NOD32 Antivirus y administrar cada nodo de la red de manera centralizada con ESET Remote Administrator.
- Es recomendable explorar con el antivirus cualquier dispositivo que se conecte a la computadora para controlar a tiempo una posible infección.
- Deshabilitar la ejecución automática de dispositivos en los sistemas operativos Microsoft Windows, ya que muchos códigos maliciosos aprovechan la funcionalidad de ejecución automática de dispositivos de las plataformas Microsoft para propagarse a través de un archivo Autorun.inf **[25]**.

Conclusión

Tanto los usuarios (sin importar el nivel de conocimiento) como las organizaciones, son cada vez más dependientes de Internet y de las tecnologías de información, lo que también los expone constantemente a diferentes amenazas, en las que se utilizan estas condiciones para cometer acciones delictivas con fines económicos.

En consecuencia es sumamente importante incorporar, como hábito cotidiano, las medidas de seguridad expuestas. Al bloquear las amenazas de forma temprana se reduce considerablemente la posibilidad de ser potenciales víctimas de las actividades delictivas, que se llevan a cabo atentando contra la seguridad de los entornos de información.

Estas medidas preventivas también deben ser acompañadas por herramientas de seguridad antimalware, como ESET NOD32 Antivirus o ESET Smart Security, que de manera proactiva frenan las acciones maliciosas a través de tecnologías de detección inteligente como la heurística.

Además se debe tener presente que también es necesario mantenerse informados en lo que respecta a los problemas de seguridad que suponen el uso de determinados medios de comunicación e interacción, entender cómo y por qué se gestan las diferentes maniobras delictivas y conocer cuáles son las herramientas que permiten hacer frente a una problemática que a nivel mundial no tiene en cuenta fronteras y afecta por igual a todos los usuarios.

Más información

[1] Herramientas para evitar ataques informáticos
http://www.eset-la.com/threat-center/2139-herramientas-evitar-ataques-informaticos
[2] Cronología de los virus informáticos: la historia del malware
http://www.eset-la.com/threat-center/1600-cronologia-virus-informaticos
[3] La importancia de las actualizaciones
http://www.eset-la.com/threat-center/1996-importancia-actualizaciones
[4] Noticias sobre el gusano Conficker
http://blogs.eset-la.com/laboratorio/index.php?s=conficker
[5] Seguridad en contraseñas
http://www.eset-la.com/threat-center/2037-seguridad-contrasenas
[6] Creando un entorno seguro en Windows XP
http://www.eset-la.com/threat-center/2038-proteccion-windows-xp
[7] Propagación de malware a través de dispositivos USB
http://www.eset-la.com/threat-center/1705-propagacion-malware-usb
[8] Bloqueo de puertos USB a través de ESET NOD32
http://blogs.eset-la.com/laboratorio/2009/04/16/bloqueo-puertos-usb-eset-nod32/
[9] Problemas de seguridad en sistemas operativos antiguos
http://www.eset-la.com/threat-center/2009-problemas-seguridad-sistemas-operativos-antiguos
[10] Disfrazando códigos maliciosos: Ingeniería Social aplicada al malware
http://www.eset-la.com/threat-center/1649-disfrazando-codigos-maliciosos
[11] SPAM: hoy, ahora y... ¿siempre?
http://www.eset-la.com/threat-center/1639-spam-hoy-ahora-y-siempre
[12] Hoax
http://blogs.eset-la.com/laboratorio/category/hoax/
[13] Entréguenos todo su dinero
http://www.eset-la.com/threat-center/1494-entreguenos-todo-dinero
[14] El arma infalible: la Ingeniería Social
http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social
[15] Protección contra intentos de robo de información
http://blogs.eset-la.com/laboratorio/2009/02/18/proteccion-contra-intentos-robo-informacion/
[16] Denunciar casos de phishing
http://blogs.eset-la.com/laboratorio/2008/04/01/denunciar-phishing/
[17] Tendencias 2009: Internet como plataforma de infección
http://www.eset-la.com/threat-center/2001-tendencias-eset-malware-2009

[18] Drive-by-Download: infección a través de sitios web
http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web
[19] Prevención en navegadores ante ataques ClickJacking
http://blogs.eset-la.com/laboratorio/2008/10/07/prevencion-navegadores-ataques-clickjacking/
[20] Utilizando redes sociales para propagar malware
http://www.eset-la.com/threat-center/2034-utilizando-redes-sociales-propagar-malware
[21] El malware en las redes P2P
http://www.eset-la.com/threat-center/1799-malware-redes-p2p
[22] Tu amigo falso, el malware mensajero
http://www.eset-la.com/threat-center/1607-amigo-falso-malware-mensaje
[23] Propagación de malware a través de dispositivos USB
http://www.eset-la.com/threat-center/1705-propagacion-malware-usb
[24] Prevenir la ejecución automática de malware a través de USB
http://blogs.eset-la.com/laboratorio/2008/08/06/prevenir-ejecucion-automatica-malware-usb/
[25] Sobre INF/Autorun
http://blogs.eset-la.com/laboratorio/2008/02/06/infautorun/
[26] Plataforma Educativa de ESET Latinoamérica
http://edu.eset-la.com/