10 tendencias en seguridad para 2011

En 2010 se produjeron detenciones importantes que golpearon al mundo del cibercrimen. Pero, lamentablemente, todavía son insuficientes. El mercado negro mueve miles de millones en beneficios, opera con total libertad amparándose en el anonimato de Internet y aprovecha los vacíos legales. La ingeniería social, el uso de las redes sociales como método de distribución y el malware cifrado y de rápida evolución, serán las principales tendencias para este año.
En tanto, el ciberactivismo en Internet y ciberguerra son tendencias que se mantienen en alza.

Reconocidos especialistas del sector IT presagian que 2011 traerá pocas innovaciones en lo que al ámbito del cibercrimen se refiere. Ciberactivismo y ciberguerra; más malware enfocado siempre a la consecución del beneficio económico, redes sociales, ingeniería social y códigos maliciosos con alta capacidad de cambio para evitar ser detectados son las principales claves para 2011, acompañado del aumento de amenazas para Mac, nuevos diseños para atacar sistemas 64 bits y nuevos ejemplares que se aprovecharán de vulnerabilidades zero-day.

A continuación, una breve descripción de cada uno de los ciberataques que podrán manifestarse e intensificarse a lo largo de este años.

1. Creación de malware

El año 2010 cerró con un aumento significativo del número de malware, del que ya se habla desde hace algunos años. En este ejercicio, han sido más de 20 millones lo que se han creado, cifra superior al que se creó en 2009. Así, las bases de datos tienen clasificados y almacenados más de 60 millones de amenazas. El ratio de crecimiento interanual, sin embargo, parece que está alcanzando su punto álgido: hace unos años, era de más del 100%. En 2010, ha sido del 50%. Se espera la misma tendencia para 2011.

2. Ciberguerra.

Stuxnet y la filtración de Wikileaks apuntando al Gobierno chino como responsable de los ciberataques a Google y a otros objetivos ha marcado un antes y un después en la historia de los conflictos. En las ciberguerras, al igual que sucede actualmente en las guerras del mundo real, no hay bandos con uniforme en el que se puede distinguir a los diferentes combatientes. Se habla de lucha de guerrillas, donde no se sabe quién es el que ataca, ni desde dónde lo hace, lo único que puede tratar de deducirse es el fin que persigue.

Con Stuxnet, quedó claro que se quería interferir en determinados procesos de centrales nucleares, específicamente en el centrifugado del Uranio. Ataques como éste, se incrementarán este año aunque muchos pasarán desapercibidos para el gran público, porque tardarán algún tiempo en conocerse.

3. Ciberprotestas.

Sin dudas fue la gran novedad de 2010. La ciberprotesta o ciberactivismo, nuevo movimiento inaugurado por el grupo Anonymous y su Operación Payback, atacando a organismos que pretenden acabar con la piratería en Internet primero, y apoyando a Julian Assange, autor de Wikileaks, después, se puso de moda. Incluso usuarios con pocos conocimientos técnicos pueden formar parte de estos ataques de Denegación de Servicio Distribuido (ataques DDoS) o campañas de spam.

Aún a pesar de que muchos países están intentado regular legislativamente este tipo de actuaciones, para poder ser considerada esta actividad un delito y, por lo tanto, perseguida y condenable, creemos que en 2011 proliferarán este tipo de cibermanifestaciones, tanto de este grupo como de otros que irán surgiendo. Internet tiene cada vez mayor importancia en la vida y es un medio de expresión que ofrece anonimato y libertad, por lo menos de momento, por lo que se verá cómo la sociedad civil se hace escuchar por estos métodos, y con éxito, por cierto.

4. Ingeniería social.

"El hombre es el único animal que tropieza dos veces con la misma piedra". Este dicho popular es cierto como la vida misma, y por eso uno de los mayores vectores de ataque seguirá siendo el uso de la denominada ingeniería social para lograr infectar a internautas confiados. Además, los ciberdelincuentes encontraron un caldo de cultivo ideal en las redes sociales, donde los usuarios son aún más confiados que cuando utilizan otro tipo de herramientas, como el correo electrónico.

Durante 2010 se vieron ataques cuyo cuartel general de distribución fueron las dos redes más utilizadas a nivel mundial: Facebook y Twitter. En 2011 no sólo se consolidarán como herramienta para los hackers, sino que seguirán creciendo en cuanto a ataques distribuidos.

Por otro lado, los ya conocidos ataques BlackHatSEO (indexación y posicionamiento de falsas webs en motores de búsqueda

Continúa en página 184

para engañar a los usuarios) serán también ampliamente utilizados, como siempre, aprovechando las noticias más relevantes del momento para llegar al mayor número posible de usuarios.

Y dada la proliferación, cada vez más notable, de contenido multimedia (fotos, videos, etc.), mucho malware seguirá siendo distribuido disfrazándose de plugins, reproductores y aplicaciones similares. No es que hayan desaparecido otros métodos, como el uso de las populares presentaciones de PowerPoint distribuyéndose a través de cadenas de amigos, pero la educación y concienciación en seguridad hace pensar que los usuarios ya han escarmentado con este tipo de aplicaciones.

Y como la crisis suele agudizar el ingenio, y lamentablemente cada vez son necesarios menos conocimientos para convertirse en un hacker y dedicarse al robo de dinero, veremos proliferar nuevas formas de intentar enganchar a los inocentes: a través de "links" falsos, con ofertas de trabajo irrechazables, con engaños cada vez más sofisticados, a través de ataques de phishing a las principales entidades ya no bancarias, sino de plataformas de pago, de tiendas online, etc.

5. Windows 7

Serán necesarios al menos dos años para comenzar a ver proliferar amenazas específicamente diseñadas para Windows 7. En 2010 se produjeron algunos movimientos en esta dirección, pero se cree que en 2011 se conocerán nuevos casos de malware que busca atacar a los cada vez más usuarios del nuevo sistema operativo.

6. Móviles.

Esta sigue siendo la eterna pregunta: ¿cuándo despegará el malware para móviles? Pues bien, parece que en 2011 podrían verse nuevos ataques pero no de forma masiva. La mayoría de los ataques actuales se dirigen a móviles con Symbian, sistema operativo que tiende a desaparecer. De los diferentes sistemas en auge, el número de amenazas para Android va a aumentar de forma considerable a lo largo del año, convirtiéndose en la plataforma preferida por los ciberdelincuentes.

7. Tablets

El dominio del iPad es total en este campo, pero en breve habrá competidores que ofrezcan alternativas interesantes. En cualquier caso, salvo alguna prueba de concepto o algún ataque anecdótico, no hay indicios de que en 2011 los tablets sean el principal objetivo de los ciberdelincuentes.

8. Mac

Malware para Mac hay y seguirá habiendo. Crecerá el número a medida que siga aumentando su cuota de mercado. Lo más preocupante es la cantidad de agujeros de seguridad que tiene Apple en su Sistema Operativo: más vale que rápidamente le pongan remedio, ya que los ciberdelincuentes son conscientes de ello y de la facilidad que conllevan estos agujeros de seguridad para distribuir malware.

9. HTML5

El que podría llegar a ser el sustituto de Flash, HTML5, es un candidato perfecto para todo tipo de delincuentes. El hecho de que pueda ser ejecutado por los navegadores sin necesidad de ningún plugin hace aún más apetitoso el poder encontrar un agujero que podría llegar a las computadoras de los usuarios independientemente del navegador utilizado. Con seguridad, veremos los primeros ataques en los próximos meses.

10. Amenazas cifradas y rápidamente cambiantes.

Este movimiento ya se vio en los dos últimos años y aumentará aún más. El malware está diseñado para el beneficio económico y para conseguirlo utiliza la ingeniería social para engañar a los usuarios. Por eso tiende a ser lo más silencioso posible, para que no se enteren las víctimas de que están infectados. Está cada vez más enfocado en las empresas , ya que la venta de datos cotiza en alza ■

Fuente: PandaLabs, laboratorio antimalware de Panda Security - http://www.pandalabs.com/es

PANDA SECURITY