Balance sobre los pronósticos del 2012

Pronóstico para el 2012	¿Se cumplió?	¿Por qué?
los equipos móviles (smartphones y tabletas) serán uno de los principales objetivos de los cibercriminales	Sí, sobre todo en el caso de Android, utilizado tanto para smartphones como para tabletas.	¿Por qué Android es la plataforma móvil más atacada? Esto se debe a diferentes motivos: por un lado, Android permite que el usuario instale las aplicaciones que quiera, sin obligarle a pasar por la tienda oficial ni que tengan que venir firmadas las aplicaciones, como ocurre en iOS. Pero los ciberdelincuentes no se fijarían en esta plataforma si no tuviera un amplio número de usuarios. Google anunció en Junio que se había llegado a la cifra de 400 millones de dispositivos Android activados, y a principios de Septiembre ya había alcanzado los 500 millones, con un ritmo de activaciones de 1,3 millones al día.
Android seguirá siendo la predilecta para esparcir malware	Sí	Como hemos comentado en la pregunta anterior. A mayor número de usuarios, más atractivo para los ciberdelincuentes
la mayor adopción de Macs hará de su sistema operativo otro blanco de los hackers , sin que la cantidad de nuevos malware para este sistema alcance la de las amenazas existentes para PC.	Sí	Efectivamente , ha sido blanco de los hackers. El mito de que los Macs son invulnerables, se ha roto, de hecho, el mayor número de usuarios tanto de computadores como de Tabletas es una de las causas por las que los dispositivos de Apple hayan sido víctimas de más ataques que en años anteriores.
aumento en las amenazas para empresas por medio de ataques dirigidos	Sí	En el Informe de PandaLabs del tercer trimestre, tenemos algunos ejemplos- **Cibercrimen** Este trimestre hemos visto como numerosas empresas han sido hackeadas, llegando en algunos casos a robar datos de clientes. La empresa Dropbox sufrió una intrusión en la que fueron robados datos de clientes. De hecho, algunos de ellos dieron la voz de alarma cuando comenzaron a recibir spam en cuentas de correo que tenían como única función recibir comunicaciones de Dropbox. En Corea del Sur, KT Corp. fue víctima del robo de datos personales 8,7 millones de sus clientes de telefonía móvil. La policía anunciaba poco después el arresto de 2 programadores por su relación con el robo. La agencia de noticias Reuters ha sufrido dos hackeos en su plataforma de blogging. En el primero fueron publicadas informaciones falsas sobre el conflicto en Siria, lo que obligó a dejar offline durante unas horas la plataforma. Apenas 2 semanas después un incidente similar tuvo lugar y se publicó una falsa noticia anunciando la muerte del príncipe Saud al-Faisal, ministro de Asuntos Exteriores de Arabia Saudí. Blizzard, la famosa compañía de videojuegos detrás de obras como Warcraft, Starcraft o Diablo, informó en Agosto que había sufrido una intrusión en su red interna y aconsejaba a todos sus usuarios que cambiaran su contraseña de acceso a su servicio

		online Battle.net. Confirmó que habían sido robadas tanto direcciones de correo como las contraseñas (que se encontraban cifradas). En septiembre se supo que Adobe fue atacada, pero en este caso no para tratar de robar información de clientes sino para acceder a uno de sus servidores internos y firmar con un certificado digital de la empresa dos ejemplares de malware. El ataque sucedió en julio de este mismo año. Aparte de todos estos ataques, también se han producido buenas noticias en la lucha contra la ciberdelincuencia: Junaid Hussain, de Birmingham, Reino Unido y líder de TeaMp0isoN, se declaró culpable de hackear la cuenta de gmail del ex-primer ministro británico Tony Blair. Semanas más tarde se le condenó a 6 meses de prisión. Joshua Schichtel, de Phoenix, Estados Unidos, ha sido condenado a 30 meses de prisión por utilizar una red de bots de 72.000 ordenadores. En concreto se dedicaba a instalar diferente malware en estos ordenadores a cambio de dinero. En uno de los casos recibió 1.500$ por instalar un troyano en cada uno de los ordenadores de la red de bots. **Ciberguerra** En este trimestre hemos sido testigos de varios casos de ciberespionaje dirigido a periodistas que tratan de informar en diferentes países. Por ejemplo, en Marruecos una serie de periodistas locales premiados por Google por su trabajo durante la "Primavera Árabe" fueron infectados con un troyano para Mac. En China, corresponsales extranjeros en Pekín fueron víctimas de dos oleadas de ataque de malware a través de mensajes de correo semanas antes del congreso del Partido Comunista Chino. Este trimestre también hemos visto un par de casos de infecciones en empresas energéticas de Oriente Medio que aún no sabemos si podrían estar relacionados entre sí o ni siquiera si se trata de algún tipo de ciberataque, aunque en base a nuestra experiencia parece que todo apunta a ello. Saudi Aramco (Saudi Arabian Oil Co) fue víctima de una infección que llevó a la empresa a cortar completamente la conexión al exterior de todos sus sistemas informáticos de forma preventiva. Por otro lado RasGas, compañía qatarí de energía dedicada al gas natural licuado sufrió una infección. Ni en este caso ni en el de Saudi Aramco la producción de ambas compañías fue afectada.
Más malware como Stuxnet o Duqu	sí	Hemos podido ver el caso de Flame. En el blog de PandaLabs escribimos sobre el caso: Esta semana ha sido destapado un "nuevo" malware (echando un vistazo a la base de datos de nuestra Inteligencia Colectiva puedo confirmar que algunos de los ficheros de este ataque datan al menos de abril de 2011) que podría estar relacionado con un caso de ciberespionaje (es detactado como W32/Flamer.A.worm). Ha infectado ordenadores en países de oriente medio (Irán, Israel, Siria, etc.) y su objetivo es el robo de

información.

El CERT de Irán ha publicado información sobre este ataque **aquí** y nuestros colegas de Kaspersky lo han estado investigando durante un tiempo y han publicado un buen artículo con preguntas y respuestas sobre el caso **aquí**.

Normalmente los ataques dirigidos se llevan a cabo con troyanos, sin embargo en esta ocasión podemos ver que estamos hablando de un gusano. Los gusanos se autoreplican, por lo que en un momento dado el creador / propietario del gusano no puede controlar a quién está infectando o dónde, y cuando tienes unos objetivos específicos quieres permanecer por debajo de la señal del radar para evitar ser descubierto. ¿Cómo ha solucionado Flame este inconveniente? Aunque es un gusano, sus mecanismos de infección están desactivados. Parece que quien está detrás de este ataque puede activar esta característica cuando lo necesite, una estrategia inteligente cuando quieres pasar desapercibido.

¿Qué información puede robar Flame? ¿Busca los más escondidos secretos que ningún otro malwere es capaz de robar? La respuesta es no, aún no hemos visto una sola característica original, que no conozcamos de otras muestras de malware. Sin embargo puede robar información de múltiples formas al mismo tiempo, y tiene una serie de módulos que dan a Flame la capacidad de robar todo tipo de información de su objetivo, incluso puede encender el micrófono para grabar cualquier conversación que esté manteniéndose cerca del ordenador.

Me gustaría citar esta pregunta y respuesta del artículo de nuestros amigos de Kaspersky:

Is this a nation-state sponsored attack or is it being carried out by another group such as cyber criminals or hacktivisits?

Currently there are three known classes of players who develop malware and spyware: hacktivists, cybercriminals and nation states. Flame is not designed to steal money from bank accounts. It is also different from rather simple hack tools and malware used by the hacktivists. So by excluding cybercriminals and hacktivists, we come to conclusion that it most likely belongs to the third group. In addition, the geography of the targets (certain states are in the Middle East) and also the complexity of the threat leaves no doubt about it being a nation state that sponsored the research that went into it.

Lo primero que quiero decir es que efectivamente parece que se

		trata de un ataque que podría estar patrocinado o directamente ejecutado por algún gobierno. Sin embargo, la explicación dada para llegar a dicha conclusión es errónea: como no roba dinero de cuentas bancarias y no es una herramienta de hacking, debe ser un ataque lanzado por algún país. Seguro. Siguiendo ese razonamiento podríamos afirmar que **"I Love You" fue también un ataque realizado por algún país**. Flame está diseñado para robar información de muy diferentes formas, está controlado a través de diferentes servidores y ha sido desarrollado y utilizado de una forma muy diferente a lo que estamos acostumbrados a ver en casos de ciberdelincuencia. Puede propagarse pero únicamente cuando la gente que está detrás de Flame quiere, y sólo ha sido visto en un pequeño número de países en una región con multitud de intereses políticos y económicos.
el "hacktivismo " tomará más fuerza en Latinoamérica para emprender ataques con fines políticos e ideológicos.	Sí	Este año se han visto, el caso de una operación llamada #OpLatinFamily, con ejemplos en Argentina, afectando al Ministerio de Economía y al Banco Central. También Agro Turismo Misiones fue atacado y se alojó un juego para disparar misiles a la Presidenta Cristina Fernández. En Venezuela también, sitios como el Ministerio para Relaciones Interiores y Justicia, y Ministerio para los Pueblos Indígenas, para protestar contra la matanza de indígenas.
gran desarrollo en la tendencia opuesta: códigos maliciosos extremadamente sencillos que apelan simplemente a la ingeniería social para engañar al usuario	Sí	Esto es algo que no va a desaparecer. Por ejemplo con el mayor uso de redes sociales como Twitter o Facebook. Hace poco un link prometiendo mostrar un vídeo de Obama dando un puñetazo a un joven por insultarle: http://pandalabs.pandasecurity.com/es/obama-racismo-twitter-y-facebook-cocktail-explosivo-para-distribuir-malware/
el rogue en español comenzará a surgir en Latinoamérica. El scam o las falsas aplicaciones para el robo de información también serán notorias durante este año.	Sí	El caso más notorio es el llamado Virus de la Policía. Con información aquí: http://pandalabs.pandasecurity.com/es/el-auge-del-ransomware-virus-de-la-policia-reloaded/ Este ejemplar ha sido traducido a numerosos idiomas y se han visto casos en toda Latinoamérica. Recordemos que estamos en un mundo global y los usuarios están cada vez más interconectados.

2013

En cuanto a 2013, las perspectivas no son mucho mejores.

Troyanos:

Una vez más, los troyanos serán los grandes protagonistas tanto en el apartado de nuevo malware creado como en el porcentaje de infecciones causadas. La causa de este dato es que el robo de información es el motivo por el que se crean la mayoría de muestras de malware, y esto lo demuestra el resultado abrumador de los troyanos, siendo un 78,04% de todas las nuevas muestras de malware encontradas desde PandaLabs.

Dispositivos móviles
Cada vez hay un mayor número de dispositivos. Tabletas, Smartphones… La expansión de la movilidad y el mayor número de dispositivos personales en la oficina. El BYOD (Bring Your Own Device) puede provocar problemas si la información se permite manejar sin tener en cuenta medidas de protección necesarias y políticas de seguridad en las empresas.

Hacktivismo y ciberguerra
Los conflictos entre naciones, organizaciones y empresas es una tendencia ya en este año, que crecerá en los próximos años, así como los grupos que apoyan a diferentes movimientos.

Ransomware

Ya hemos visto que los falsos antivirus no están tan en boga, pero seguirán siendo un modo de infectar los PCs de usuarios, pero creemos que la solicitud de dinero para “desinfectar” los PCs seguirá teniendo su protagonismo en el año que viene.

Redes sociales
Al haber cada vez más usuarios de las redes, estamos completamente seguros que será una de las plataformas más utilizadas para los cibercriminales. Sobre todo, dado a que redes como Facebook harán posible los regalos en breve. Los usuarios incluirán sus datos personales y bancarios a través de esta plataforma y es muy probable que los robos sean más fáciles de realizar.