Cumplimiento de tendencias pronosticadas para el 2012

Por Camilo Gutiérrez Amaya, especialista en Awareness & Research de ESET Latinoamérica

Pronóstico para el 2012	¿Se cumplió?	¿Por qué?
Los equipos móviles (smartphones y tabletas) serán uno de los principales objetivos de los cibercriminales	Si	Durante el año la cantidad de familias que se detectaron con los productos de ESET creció con respecto al año pasado. En 2012 la cantidad de detecciones únicas con respecto a 2011 crecieron 17 veces a nivel global. Durante el presente año las amenazas para *smartphones* han evolucionando con el objetivo de poder robar información de los usuarios directamente desde sus teléfonos. Para lograr este cometido han utilizado desde la inyección de código malicioso en juegos hasta la creación de falsos sistemas de seguridad que simulan ser aplicaciones bancarias. Además la consolidación de tendencias como BYOD (***bring your own device***), relacionada con que los empleados lleven sus teléfonos celulares a su lugar de trabajo, y utilicen libremente los recursos de la compañía, incluso recursos privilegiados, como por ejemplo email, servidores de archivos, acceso a base de datos, entre otros, convierten a estos dispositivos en blancos mucho más deseados por el tipo de información que manejan. ***Artículos relacionados*** Vulnerabilidades en Android puerta abierta para SMiShing Troyano SMS Boxer afecta nueve países latinoamericanos Código malicioso permite acceso remoto a tarjetas inteligentes Nueva variante de ZITMO afecta a usuarios móviles Dispositivos móviles atraen nuevas amenazas para las compañías Evolución de los troyanos bancarios para dispositivos móviles (Parte I) Evolución de los troyanos bancarios para dispositivos móviles (Parte II) Tendencias 2013: vertiginoso crecimiento de malware para móviles Dancing Penguins – Un caso de distribución de malware en Android

Android seguirá siendo la predilecta para esparcir malware	Si	Android se ha consolidado cómo el sistema operativo con mayor cantidad de móviles activados durante el 2012. La evolución de códigos maliciosos como ZITMO que convierte los dispositivos móviles en parte de una *botnet* o variantes que vulneran el control de doble autenticación de algunas entidades financieras e incluso algunas variantes de códigos maliciosos que instalan falsas actualizaciones del sistema operativo, son algunas amenazas que se vieron durante el 2012. Amenazas cómo Boxer, un troyano SMS que suscribe a la víctima a números de mensajería premium sin su consentimiento, tuvo gran influencia en la región. Una de las variantes analizada en el laboratorio de ESET Latinoamérica es capaz de afectar un total de 63 países, de los cuales 9 son de América Latina. ***Artículos relacionados*** Troyano SMS Boxer afecta nueve países latinoamericanos Falso Angry Birds propaga Boxer Nueva variante de ZITMO afecta a usuarios móviles Troyanos en Android: vulnerando sistemas de doble autenticación Android/NoComA: falsas actualizaciones e instalación de malware Primer malware que utiliza drive-by download en Android
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.	Si	Durante el año se detectaron amenazas para MAC, con las mismas características que para PC. Quizá el código malicioso de mayor propagación para equipos Mac es Flashback, un troyano detectado por la solución de ESET cómo OSX/Flashback. Durante este año Flashback superó los 750.000 usuarios de Mac infectados en todo el mundo y sólo en Latinoamérica alcanzó al menos unos 40.000 equipos víctimas. Además durante el año se desarrolló a modo de prueba de concepto, un rootkit capaz de funcionar bajo la edición de 64 bit del sistema operativo OS X de Apple. Los rootkit son herramientas diseñadas para obtener el control de programas, archivos, procesos, puertos, entre otros, de forma completamente oculta. A pesar que este este rootkit es sólo una prueba de concepto, es la muestra que este tipo de dispositivos son igualmente vulnerables al mismo tipo de amenazas que los PC. ***Artículos relacionados*** 40.000 equipos infectados con Flashback en Latinoamérica WordPress vector de propagación de Flashback ¿Cuál será el próximo Flashback?

		Malware 2011 para Mac y la educación de los usuarios Rubilyn: rootkit capaz de afectar computadoras Mac de 64 bit
Aumento en las amenazas para empresas por medio de ataques dirigidos	Si	Durante el 2012 se escuchó hablar de varias amenazas relacionadas con ataques dirigidos como: Stuxnet o Flamer. Pero particularmente, desde los laboratorios de ESET Latinoamérica se descubrió lo que fue catalogado como el primer caso de espionaje industrial en la región: se trata de Operación Medre, un ataque focalizado en Perú que robaba planos diseñados en AutoCAD. ***Artículos relacionados*** Operación Medre: estadísticas de un ataque dirigido a Perú Operación Medre: ¿espionaje industrial en Latinoamérica?
Más malware como Stuxnet o Duqu	Si	Luego de incidentes de alto impacto mediático como Stuxnet, Duqu o Flamer; desde el Laboratorio de ESET Latinoamérica hemos descubierto un ataque similar diseñado y perpetrado exclusivamente para un país de la región, Perú**.** A partir de las tasas de detección del gusano ACAD/Medre.A durante el 2012, que alcanzaron el 95% en este país, posicionándolo como un nuevo caso de malware diseñado para un ataque dirigido. ***Artículos relacionados*** Virus Bulletin 2012: Medre y el malware en AutoCAD Operación Medre: infografía y webinario público Sitio utiliza ACAD/Medre.A y falsa información para promocionar productos Análisis técnico de ACAD\Medre.A
El "hacktivismo " tomará más fuerza en Latinoamérica para emprender ataques con fines políticos e ideológicos.	Si	Las protestas de grupos hacktivistas se han desarrollado con mayor frecuencia a nivel mundial durante este año. En la región hemos sido testigos de ataques de denegación de servicio (DDoS) a entidades gubernamentales de Latinoamérica, generando en la mayoría de los casos la interrupción en la disponibilidad de los sitios. Además a nivel global, se informó varios casos de fuga de información asociados a grupos hacktivistas. ***Artículos relacionados*** Hacktivistas atacan varios sitios y acceden a 12 millones de UDID de iOS Operación Quirófano: Anonymous ataca al gobierno argentino Anonymous y su maratón hacktivista durante el fin de semana
Gran desarrollo en la tendencia opuesta: códigos maliciosos extremadamente sencillos que apelan simplemente a la ingeniería social	Si	Esta forma de llevar que un usuario se infecte con algún código malicioso es la forma clásica y la más utilizada por los ciberdelincuentes. Durante el 2012 fueron muchos los casos que utilizando noticias falsas o sucesos relevantes se emplearon como el medio para propagar códigos

para engañar al usuario		maliciosos, tal es el caso de Julian Assange y Wikileaks, tragedias relacionadas con tsunamis o terremotos, supuestos videos de Shakira, Alexis Sánchez, de presidentes latinoamericanos como también falsos sorteos y juegos de video. También las campañas de Phishing incluyendo características de geo localización para darle más credibilidad al engaño, fueron ampliamente utilizadas para engañar al usuario y robar principalmente su información financiera. La mayoría de los casos estaba relacionada con entidades financieras de toda Latinoamérica, pero también se identificaron casos asociados a compañías de celular, almacenes de cadena, aerolíneas, servicios en Internet, entre otros. ***Artículos relacionados*** Compañías de telefonía continúan utilizándose como tema para propagar malware Alerta: phishing utiliza geolocalización para asegurar mayor rédito Alerta: phishing de tarjetas de crédito en Argentina Troyanos bancarios en Latinoamérica: Brasil es el líder Dorkbot: Correo sobre falso video de Julian Assange Alerta: más de 31.000 usuarios de Twitter afectados por phishing Cibercriminales propagan phishing brasileño sobre conocida tarjeta de crédito Aerolíneas, promociones, autos deportivos y phishing de tarjetas de crédito Phishing bancario en México ahora con interacción telefónica
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.	Si	Durante el 2012 fueron identificadas varias estafas en español que utilizaban supuestas herencias, postales de amor falsas, situaciones personales delicadas, comentarios en redes sociales e incluso videos de situaciones comprometedoras en Facebook. También algunos casos de Phishing tenían asociado geo localización para mostrar información solamente a usuarios de determinados países y de esta forma maximizar las posibilidades de que alguien callera en el engaño. ***Artículos relacionados*** ¿Qué sucede si un usuario compra un rogue? ESET Rogue Applications Remover: herramienta para eliminar rogue persistentes Campaña de Dorkbot a través de postales de amor falsas Comentarios engañosos en YouTube Supuesto video de ex novia propaga engaño por Facebook Más sobre estafas por correo electrónico Crónica de una estafa real por e-mail Supuesta herencia utilizada para propagar scam personalizado