Symantec presenta su reporte anual de amenazas de seguridad en Internet

Symantec presentó en **México** la vigésimo segunda edición de su **Informe sobre Amenazas de Seguridad en Internet** (**ISTR** por sus siglas en inglés) que reportas las incidencias del año **2016**, según el que los ataques de **subversión y sabotaje** se han incrementado y tomado relevancia con afectaciones en instalaciones de **operación crítica** resultantes en interrupciones del servicio eléctrico en Ucrania o las intromisiones de hackers en las elecciones presidenciales de Estados Unidos.

"El año pasado fue un año complejo en cuanto a **ataques**, sin embargo las herramientas que los **delincuentes** utilizan para infiltrarse en la organizaciones son del día a día como documentos de Microsoft Office o mensajes de correo electrónico", comparte Alejandro Zermeño, Estratega de **Seguridad** y Desarrollador de Negocios para Symantec en México.

Symantec construye su informe anual recopilando **datos** de la red de más de 175 millones de dispositivos que protege alrededor del mundo, que constituye la **base instalada** más grande a nivel global concentrando una porción de 14.4% del mercado de **software de seguridad para empresas** y 35.2% del de consumo; apareciendo como líder en 4 cuadrantes mágicos de la consultora **Gartner** que incluyen **Managed Security Services**, **Endpoint Protection**, **Enterprise Data Loss Protection** y **Secure Web Gateway**.

El reporte también establece que a nivel mundial 1 entre 131 mensajes de **correo electrónico** contiene **malware adjunto** o enlaces para su descarga (1 entre 506 en México); durante todo 2016 se observaron 401 millones de **instancias únicas de malware**, 89% de ellas nunca antes vistas, 20% de estas instancias ya son capaces de identificar **máquinas virtuales** de manera que evitan desempaquetar el **código malicioso** en el ambiente de **sandbox**, 4% utilizan **servicios en nube** y 3% se comunican de manera cifrada.

Arriba del 55% de los correos electrónicos recibidos por usuarios mexicanos corresponden a **mensajes de spam**, en tanto las iniciativas que buscan sorprender a los usuarios para el **otorgamiento de sus credenciales** (**phishing**) corresponden a 1 entre 5,877 correos.

Las grandes corporaciones concentran el mayor número de ataques de phishing dada la cantidad de **colaboradores** que concentran. Y contra lo que pudiera pensarse, los sectores de los **transportes y los servicios públicos**, la **manufactura**, y el **comercio mayorista** reciben más ataques de phishing que las empresas en el **sector financiero** en proporciones que pueden ser hasta 10 veces mayores.

Mientras que las **empresas pequeñas y medianas** son más susceptibles a recibir ataques de malware por correo electrónico que las empresas de mayor tamaño -aunque no la gran empresa-. En ese sentido, los ataques a organizaciones menores puede observarse como una puerta de entrada a empresas más grandes con las que hacen negocios y pudieran tener mejores **estrategias de seguridad.**

Otro tema toral del informe es el **ransomware**, que se reporta en 2016 tuvo 3 veces más familias que en 2015, los usuarios afectados en Estados Unidos están casi dos veces más dispuestos a pagar por el **rescate de su información** que en otras partes del mundo, asimismo el monto exigido se ha más que triplicado entre las últimas dos ediciones para alcanzar lo 1.077 dólares en promedio.

México continúa como el segundo país de **origen de ataques a nivel internacional e**n Latinoamérica detrás de Brasil, sin embargo su porcentaje de participación en los ataques que se realizan en el mundo creció entre 3 y 4 veces su tamaño entre 2015 y 2016.

Symantec asegura que todas la empresas ya utilizan **tecnologías en nube** dentro de sus sistemas, aunque el personal de TI no lo sepa debido a que los usuarios se acercan a aplicaciones disponibles en las tiendas o disponibles mediante otro tipo de **descargas sin autorización** para mejorar su productividad, al grado que calcula que son casi 1,000 las aplicaciones en nube que a las que los colaboradores de cada organización tienen acceso de manera cotidiana, muy distantes que 40 que los encargados tiene en el radar, de ahí que se considere el **cómputo en nube como el próximo campo de batalla en la guerra por la seguridad**.

Otra de las preocupaciones toma forma en los **dispositivos en entornos conectados**, pues de enero a diciembre del año pasado se duplicaron los ataques a los dispositivos para el **Internet de las Cosas**, al grado que un dispositivo sin protección podía recibir ataques en los primeros 2 minutos.

Finalmente, la compañía valora la importancia del **entrenamiento** de los colaboradores para las estrategia de seguridad de las compañías aduciendo que se debe levantar la **consciencia de que los riesgos son reales** y que la información de las personas y las organizaciones tienen un valor y hay gente dispuesta a pagar por ella.