Ciberseguridad: se detectan más de 900 ataques a universidades en el último año - elEconomista.es - 21/02/2019

CIBERSEGURIDAD

Se detectan más de 900 ataques a universidades en el último año

Carmen García MADRID.

Cada vez es más complicado ocultar la información en la red. Las nuevas tecnologías están totalmente integradas no solo en el ámbito familiar, sino también en las aulas tanto de los colegios e institutos como de las universidades. A pesar de que se han constituido como herramientas positivas en el desarrollo de la sociedad, existen también aspectos negativos que hay que supervisar. Su uso cada vez más frecuente provoca que se incremente su defensa ante riesgos y amenazas al controlar todos los datos que se suben a la Red.

El aviso llegó hasta el mundo educativo y, en concreto, hasta la información que tienen las universidades en su poder. Desde Kaspersky, una empresa global de ciberseguridad fundada en 1997, se han lanzado varios mensajes a instituciones educativas, poniéndoles sobreaviso, al detectar numerosos ataques a, exactamente, 131 universidades de 16 países. Estos intentos de robar información sensible se realizaron en los últimos 12 meses, con casi 1.000 ataques de suplantación de identidad lanzados desde septiembre de 2017.

El número de universidades atacadas es preocupante. La educación se ha convertido en un objetivo muy apreciado entre los cibercriminales y las instituciones deben impedir que accedan a sus sistemas, por lo que tienen que ser proactivos a la hora de tomar las medidas de seguridad oportunas.

Usuarios y contraseñas

Alfonso Ramírez, director general de Kaspersky Lab, indica que a pesar de que a priori no parezca que los cibercriminales estén interesados en los datos personales de estudiantes, profesores y personal de las universidades, cada vez están poniendo más el foco en este ámbito: "La información que se puede conseguir es muy valiosa, puesto que sus bases de datos contienen información de muchos proyectos de investigación". En la mayoría de los casos crean una página web muy parecida a la auténtica del sistema de acceso digital a la universidad con el fin de hacerse con los detalles de usuarios y contraseñas.

Los 'hackers' crean una web parecida a la original para lograr suplantarla

A pesar de que las universidades están atentas a su seguridad IT, los atacantes encuentran formas de romper las defensas de los usuarios poco atentos. Es probable que las víctimas caigan en la trampa e introduzcan sus credenciales para enviar su información confidencial a los *phishers*.

Según Ramírez, para evitar volver a ser víctimas de estos ataques, las universidades deben implementar una solución de seguridad para *endpoints* fiable, que cuente con tecnologías anti suplantación de identidad. La idea es detectar y bloquear los ataques de *spam* y *phising*. Añade que "la concienciación y formación en materia de ciberseguridad es primordial para evitar cualquier intrusión". Es necesario establecer unas pautas en toda la organización para evitar ser víctima de la actividad cibercriminal.

Washington, el foco

Los analistas detectaron un total de 961 ataques contra 131 facultades, dirigidos principalmente a universidades de habla inglesa. De ellas, 83 instituciones se encuentran en los Estados Unidos y 21 en el Reino Unido. Los criminales estaban especialmente interesados en la Universidad de Washington, contra la que Kaspersky Lab detectó 111 ataques. Las estadísticas muestran también que instituciones educativas por toda Asia, Europa y África sufrieron los mismos movimientos. Entre julio y septiembre, las *botnets* DdoS atacaron objetivos en 82 países.

Una *botnet* es una red de equipos informáticos que han sido infectados con *software* malicioso, que permite su control remoto, obligándoles a enviar *spam*, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento de los propietarios del equipo.

China fue, de nuevo, el primer país en número de ataques recibidos. Estados Unidos se encuentra en segundo lugar y Australia, en el tercer puesto.

Educar en seguridad

Ante este fenómeno que está cada vez más generalizado, los alumnos deben tomar medidas de precaución que Alfonso resume en: "Revisar siempre la dirección del enlace y la dirección electrónica del remitente o no hacer nunca clic en el enlace, sino copiar la dirección y pegarla en la barra del navegador". Además, es importante no usar nunca la misma contraseña para varios sitios web o servicios y para crear contraseñas seguras lo mejor es utilizar una fuerte y robusta que contenga números, letras y símbolos. De esta forma, será más complicado para los cibercriminales intentar acceder a las cuentas que se tengan en Internet.

Alfonso resume a la perfección la realidad de estas prácticas: "Nadie está a salvo del cibercrimen". Es por ello que las organizaciones deben educar y concienciar a sus empleados para que no compartan datos confidenciales. La educación se ha convertido en un objetivo muy apreciado para el que Kaspersky Lab recomienda adoptar las siguientes medidas de seguridad para protegerse y evitar caer en las trampas de los *phishers*.

Para asegurarnos de que nadie acceda a la conexión, se debe utilizar una red segura, usando Wi-Fi seguro con cifrado y contraseñas fuertes, o aplicar soluciones VPN que cifren el tráfico. En esa misma línea, cuando se utilice el dispositivo para navegar en la red, será necesario usar siempre una solución de seguridad fuerte que nos ponga sobreaviso ante páginas web de *phising*.

Las instituciones educativas de China son las que reciben más amenazas

Sistemas Kaspersky

Kaspersky está altamente preparado para hacerle frente a todo tipo de peligros y para ello dispone de varios sistemas que contribuyen a mantener la seguridad en el ámbito educativo. A través de Kaspersky Password Manager se podrán crear contraseñas seguras a prueba de piratas sin tener que recordarlas. Para asegurar una conexión segura Kaspersky Secure Connection activará automáticamente el cifrado.

Es necesario insistir en el papel relevante que tienen las instituciones educativas a la hora de educar y concienciar a docentes y alumnos de que no compartan datos confidenciales como contraseñas y no hacer clic en enlaces que provengan de remitentes desconocidos. De esta forma se estará haciendo frente a uno de los gigantes que pretenden poner en peligro esta área.

En los últimos años, cada vez más centros educativos están llevando a cabo políticas de educación y sensibilización entre los menores sobre la importancia de este asunto. El profesorado es un elemento indispensable para educar a los más pequeños, no obstante, el rol de los padres es fudamental para concienciar sobre los riesgos y amenazas.

Ataque a la UVA

El pasado 14 de enero la Universidad de Valladolid fue víctima de un ataque informático que ha propiciado el robo de datos personales en la página web del Servicio de Relaciones Internacionales.

Tras conocer el ataque, los técnicos de la Universidad procedieron al bloqueo de la máquina afectada y al volcado de la copia de seguridad almacenada en otra máquina diferente.

La Universidad, al analizar los daños, procedió a la identificación de las personas afectadas y clasificación del riesgo al que habían sido expuestas, aunque evitó dar detalles concretos y el alcance de este ataque, para no afectar a las investigaciones.

La Secretaría General de la Universidad de Valladolid elaboró un informe sobre el incidente que se envió a la Agencia Española de Protección de Datos.

Desde el pasado mes de mayo, esta institución castellanoleonesa ha actualidado su esquema de seguridad y dispone de un Comité de Seguridad de la Información, además de contar con un responsable de privacidad y con un delegado de protección de datos.

ISTOCK