Publicación: **ADELANTOS JULIO GRANADA 2021** *Sección:* **Granada** *11/07/2021 20:51h Usuario: pquilez*
Página: **Ciencia abierta lunes 12 julio JOLNWS20210711_0790** *Edición:* **GRANADA**

GRANADA

CIENCIA ABIERTA

JOSÉ LUIS NAVARRO GALINDO

UNIVERSIDAD DE GRANADA

DEPARTAMENTO DE Didáctica DE LAS Ciencias Experimentales

● Relato de una ficción que puede convertirse en realidad en cualquier instante

Ciberataque al IES Zaidín-Vergeles

LOS servicios informáticos del IES Zaidín-Vergeles sufrieron un ataque la pasada madrugada del 11 al 12 de julio de 2021, según ha informado el propio instituto a través de su cuenta de Twitter.

"El IES Zaidín-Vergeles se ha visto afectado por un ataque informático. Los responsables técnicos del IES y los miembros del Departamento de Informática y Comunicaciones están trabajando de manera conjunta para determinar el origen y restablecer la normalidad lo antes posible", han comunicado.

La mañana del 12 de julio se detectó que la disponibilidad de la web se había visto afectada. Tras constatar que se trataba de un ciberataque, los técnicos han establecido los cortafuegos correspondientes, con el fin de evitar nuevas intrusiones y/o filtraciones de información. Precisamente, estos profesionales están evaluando los daños y el alcance del ataque.

Los servidores del IES almacenan datos confidenciales pertenecientes al alumnado, profesorado y otros miembros de la comunidad educativa; es importante determinar si se ha producido una filtración de información (Data Leak) o si, por el contrario, se han empleado técnicas 'ransomware' o 'secuestro de datos' para pedir posteriormente un rescate por los datos que se hayan perdido.

Una filtración de datos supondría que los ciber-delincuentes han sido capaces de recabar datos de carácter personal, tales como nombre, apellidos, DNI, email y dirección. Esta información es usada por los ciber-delincuentes para suplantar la identidad de las personas (phishing) con objeto de dar de alta algún tipo de suministro, como pueden ser: líneas telefónicas, electricidad, agua y gas. También es una práctica común de ellos el abrir nuevas cuentas bancarias con las que operar por Internet, por ejemplo, realizando compras online.

Aunque hasta el momento tampoco se ha recibido ninguna solicitud de rescate, la naturaleza de este tipo de incidentes de seguridad suele ser siempre la misma: el ciber-delincuente explota alguna vulnerabilidad para acceder a un ordenador del sistema que se ha convertido en su objetivo. Una vez dentro del equipo, lo infecta con un código malicioso que se propaga a través de la red interna y además encripta todos los archivos que va encontrando a su paso, para así hacer los equipos inutilizables. Por último, se exige un rescate económico, generalmente en criptomonedas (moneda virtual no rastreable), para que la víctima pague si quiere recobrar la normalidad.

Se está intentando determinar la identidad de los responsables del ciberataque a través de las direcciones IP desde donde se originó el ataque, es decir, el conjunto de números que identifica de manera única el dispositivo desde donde se conectaron a Internet. Esta labor es harto complicada, debido a que el ciber-delincuente común se suele ocultar detrás de la red Tor, una red descentralizada donde la información, en lugar de seguir siempre la misma ruta, va 'rebotando' por servidores en todo el mundo. Las ventajas que obtienen los ciber-delincuentes al usar la red Tor son el anonimato y privacidad en sus acciones, ya que no se puede rastrear el tráfico en ella.

Según apuntan los expertos, no existe un perfil claro del ciber-delincuente. La investigadora holandesa Marleen Weulen Kranenbarg ha determinado que, en su país, las motivaciones que llevan a cualquier persona a cometer un delito penal utilizando para ello las tecnologías de la información y comunicación (TIC) son: curiosidad, reto, ira, venganza, lascivia y lucro (en ese orden).

Los expertos coinciden en que la prevención es clave para que las empresas puedan sobrevivir a un ciberataque. Muchas no pueden asumir los costes asociados a resolver los problemas ocasionados por un incidente de seguridad, ni tampoco parar sus negocios si quieren salir adelante.

Cuántas veces hemos leído una noticia así que afecta a instituciones o empresas y que, desafortunadamente, cada vez leeremos más. En 2021, fueron atacadas e inutilizadas las webs de diferentes ministerios (entre ellos Justicia, Educación y Economía), del Instituto Nacional de Estadística (INE), del Servicio Público de Empleo Estatal (SEPE), del Tribunal de Cuentas, del Consejo de Seguridad Nuclear y de la Universidad de Granada entre los más destacados. El Ministerio de Trabajo y la Universidad de Córdoba recibieron un ataque de ransomware. En el ámbito empresarial, compañías como Phone House, Everis, Mapfre, Adeslas, Prosegur, Garmin y Electronic Arts también recibieron ataques con resultados catastróficos. Hace tan sólo unos días se detectaba una brecha de seguridad en el portal de certificados COVID de la Comunidad de Madrid donde quedaban expuestos los datos personales de miles de ciudadanos, incluidos los de Felipe VI, Pedro Sánchez o Aznar.

> En 2021 fueron atacadas e inutilizadas las webs de varios ministerios y distintas instituciones

Por último, cabe aclarar que lo relatado en el presente artículo es pura ficción, aunque perfectamente podría haber sucedido. En la próxima edición de 'Ciencia Abierta' os contaremos los hallazgos y vulnerabilidades que nuestro alumnado de Informática encontró en nuestra web durante la celebración del primer concurso de Ciberseguridad del IES Zaidín-Vergeles.

►**José Luis Navarro Galindo.** Doctor en Informática. Profesor de Sistemas y Aplicaciones Informáticas en el IES Zaidín-Vergeles.