Ejemplos de ataques informáticos

## Ataque a la Integridad

El 14 de enero de 2013 la Secretaría de la Defensa Nacional de México (Sedena) informó que hubo un hackeo de modificación de contenido que afectó la página principal de la secretaría.

La alteración al sitio de la Sedena fue dada a conocer a través de la cuenta de Mexican Hackers Team, un grupo de simpatizantes de Anonymous en México.

En el sitio web www.sedena.gob.mx los ciberactivistas colocaron un video donde se ven imágenes de los disturbios durante la toma de protesta de Enrique Peña Nieto y se escucha una voz en off que pronuncia el Manifiesto Zapatista.

## Ataque a la Confidencialidad

## Singapur ha sufrido la violación de datos "más grave", comprometiendo datos personales de 1,5 millones de pacientes de atención médica, incluido el de su primer ministro, Lee Hsien Loong.

## Los usuarios afectados son pacientes de SingHealth, que es el grupo de instituciones de atención médica más grande del país, que comprende 42 especialidades clínicas, cuatro hospitales públicos, cinco centros especializados, nueve policlínicos, así como tres hospitales comunitarios.

## Se han accedido y copiado detalles personales no médicos de 1.5 millones de pacientes que visitaron las clínicas especializadas y policlínicas de SingHealth entre el 1 de mayo de 2015 y el 4 de julio de 2018. Los datos robados incluyen el nombre de los pacientes, el número de identificación nacional, la dirección, el género, la raza y la fecha de nacimiento.

## Además, los datos médicos ambulatorios de unos 160,000 pacientes se vieron comprometidos, sin embargo, los registros no fueron modificados o eliminados, dijeron el Ministerio de Salud y el Ministerio de Comunicaciones e Información (MCI), en una declaración conjunta.

## Ataque a la Autenticidad

Corea del Norte ha sido noticia hace relativamente poco por su relación con diversos ataques informáticos realizados contra empresas estadounidenses, los cuales cuentan con una abanico de intenciones de lo más amplio, desde robar información hasta obtener un beneficio económico de manera directa.

Naturalmente, el país no se ve implicado de manera directa en estas acusaciones, sino que lo hace su grupo de informático de hackers, conocido como Lazarus.

El malware, que ha sido descubierto Kaspersky Lab y bautizado como AppleJeus, cuenta con diferentes peculiaridades, pero quizá la más notoria sea que se trata de la primera vez que se tiene consciencia de un software de este tipo dirigido por parte de Lazarus al sistema de la compañía de la manzana mordida. El modus operandi, detallan, consiste "en la penetración en la infraestructura del exchange cuando un empleado desprevenido de la empresa descarga una aplicación de terceros un sitio web de aspecto legítimo de una empresa que desarrolla software para el comercio de criptomonedas".

La aplicación, insisten, no tiene ningún aspecto sospechoso. Solo un detalle en el código es capaz de delatar el engaño, el cual se esconde en forma de actualizador. Este recolecta datos de la máquina en la que se ha instalado dicho software y lo envía a los ciberdelincuentes, decidiendo estos en base a la información obtenida si merece la pena atacar o no el equipo. En caso de considerarlo oportuno, un troyano reconocido como Fallchill –instalado mediante la herramienta mencionada– dota a los atacantes de la posibilidad de comprometer los datos del ordenador.

## Ataque a la Disponibilidad

ProtonMail es una de las plataformas de correo electrónico seguro y cifrado más conocidas, plataformas que nació en Suiza como una solución anti-NSA para que los usuarios pudieran mandar mensajes con la seguridad de que nadie más, salvo el receptor, puede acceder a ellos.

En 2015, esta plataforma de correo cifrado ya fue víctima de un grupo de piratas informáticos que dejaron sin servicio a la plataforma durante varios días. Igual que en su día no fueron capaces de protegerse adecuadamente de este tipo de ataques informáticos, ahora, que se vuelve a encontrar en la misma situación, los responsables de ProtonMail siguen sin ser capaces de poner solución.

La plataforma de correo seguro ProtonMail se encuentra bajo constantes ataques DDoS, ataques de denegación de servicio que están dejando sin acceso, de manera intermitente, a esta plataforma. Durante estos ataques, además, está haciendo problemas a la hora de enviar y recibir correos electrónicos. Radware y F5, las dos infraestructuras que utiliza ProtonMail, están trabajando en poder mitigar estos ataques, pero, de momento, los ataques son constantes y no son capaces de mitigarlos y garantizar el acceso a todos los usuarios.