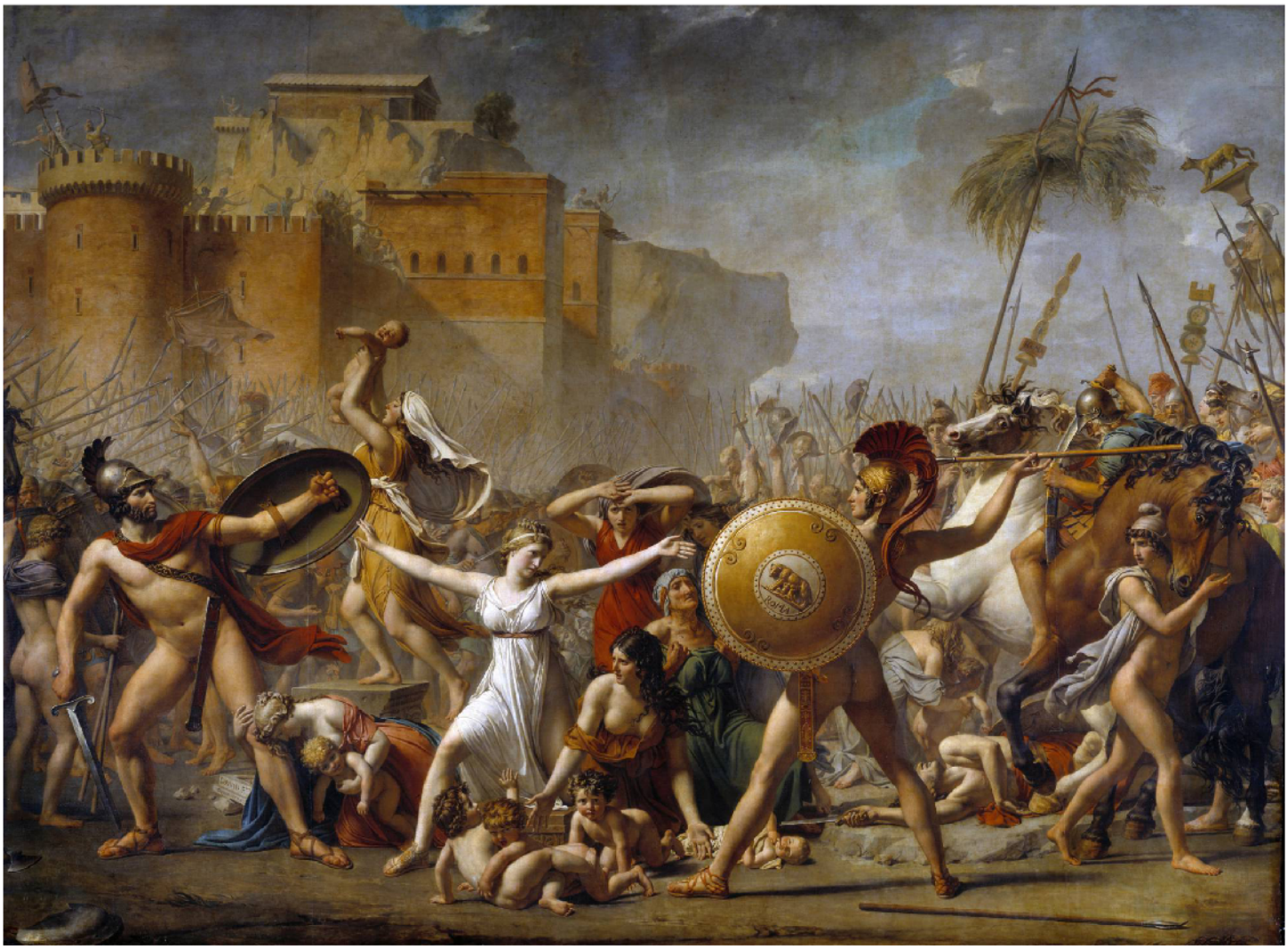

FIRMA INVITADA

La amenaza del secuestro digital

Por Sancho Lerena

El FBI inventarió el pasado 2018 unos 1.493 ataques de 'ransomware' a sujetos que se vieron obligados a pagar un total de 3.161.484 euros a los secuestradores

3 SEP 2019 - 08:21 CEST

Hace muy pocos meses surgió la noticia de que por primera vez un gobierno pagaba un rescate a un grupo cibercriminal. Se trataba del secuestro digital (*ransomware*) del gobierno local de Riviera Beach (ciudad de Florida de 35.000 habitantes). Este modo de ciberataque consiste en un acto criminal en el que un delincuente logra cifrar todos los datos de la víctima a través de un programa malicioso que bloquea el ordenador y pide un pago por desbloquearlos.

La mayor parte de estos casos se resuelven pagando un rescate

Los ataques de *ransomware* ya se han perpetrado con anterioridad en los sistemas de ciudades estadounidenses como Baltimore, Atlanta o Nueva Jersey. Casos que se integran en los más de 6.000 millones de ordenadores, tanto de particulares como de pequeñas y medianas empresas, que se han visto afectados en 2019 por este tipo de ofensivas. Detrás de ellas se encuentran grupos criminales que llevan años realizando y perfeccionando en todo el planeta. En 2017, Telefónica tuvo que vérselas con una extorsión de este tipo que afectó a gran parte de sus datos y a los ficheros de sus empleados; y, como ella, cientos de empresas en todo el mundo (Mondelez, DLA Piper, Maersk, Merck Sharp & Dohme, Saint Gobain...).

Aunque no se reconozca públicamente, la mayor parte de estos casos -por no decir todos- se resuelven pagando un rescate que siempre es muy cuantioso porque los

suma de 326.914 euros en bitcoins a los secuestradores. El grupo había dejado a la ciudad sin su sistema informático y pidió el rescate a través de este medio de pago para no ser rastreado.

Gastos adicionales

Además del rescate, el coste de la reconfiguración del sistema fue de 800.000 euros. Tras una contaminación de este tipo, los ordenadores perjudicados tienen que ser saneados, inspeccionados en busca de cualquier vulnerabilidad y volver a ser provistos de toda la información que contenían antes del bloqueo.

Lo normal es que las víctimas de extorsiones económicas no lo hagan público por el coste en reputación que ello conlleva. Es decir, los casos conocidos son solo la punta del iceberg, así que es lógico pensar que si cada vez se conocen más casos, es que el problema viene acrecentándose desde hace años.

El FBI inventarió el pasado 2018 unos 1.493 ataques de *ransomware* a sujetos que se vieron obligados a pagar un total de 3.161.484 euros a los secuestradores. Eso es una media de 2.107 euros por asalto. En España, según datos del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), en 2018 hubo 54 ataques contra infraestructuras críticas de la Administración (120.000 a las empresas). Y es que el *ransomware* se nutre de la falta de seguridad en varias áreas, como el control de ejecución de *software* malicioso, que se puede mitigar con un antivirus. Otro de los factores que facilita un expolio de este tipo es la falta de control en la plataforma de usuario, que se puede aplacar con una buena monitorización de la seguridad local y las políticas de usuario. Pero lo más importante y el motivo principal de que cientos de compañías hayan tenido que pagar rescates de miles de euros son las malas políticas de *backup*, que se pueden suplir con una monitorización específica de las copias de seguridad.

No se trata de tener un antivirus, una buena planificación de administración de equipos locales o una política de *backup*. Se trata de monitorizar que se estén empleando bien las herramientas, porque ¿de qué sirve tener un antivirus desactualizado o no instalado en todas y cada una de las máquinas de mi organización?, ¿de qué sirve tener una copia de seguridad desactualizada de hace seis meses? La monitorización precisamente ayuda a visualizar qué equipos son más vulnerables y a verificar que nuestros equipos de seguridad estén actualizados y preparados para cualquier amenaza.

Nadie puede parar un ataque de *ransomware* con el 100% de eficacia, pero es posible prevenirlo, interrumpir su curso y en el peor de los casos, contar con un plan de recuperación.

No se puede entender que hoy todavía se produzcan estos ataques maliciosos cuando se dispone de herramientas. El problema reside muchas veces en que no se tienen en cuenta estas herramientas básicas para controlar la tecnología.

Sancho Lerena es ingeniero de informática y fundador de Pandora FMS

Transformación digital · Tecnología digital · Seguridad internet · Internet · Empresas · Telecomunicaciones · Economía · Tecnología · Comunicaciones · Ciencia

Por

TOP

Ir a comentarios

Sancho Lerena

01

Internet: causante y víctima del calentamiento global

Las tecnologías digitales representan el 4% de la emisión de gases de efecto invernadero. A la vez, la Red también va a estar entre las principales perjudicadas por el cambio climático

02

Pornocapitalismo, Neuralink y los zombies

El pornocapitalismo actual ha declarado 'open for business' al Amazonas. Su siguiente objetivo de negocio puede ser nada menos que nuestro cerebro