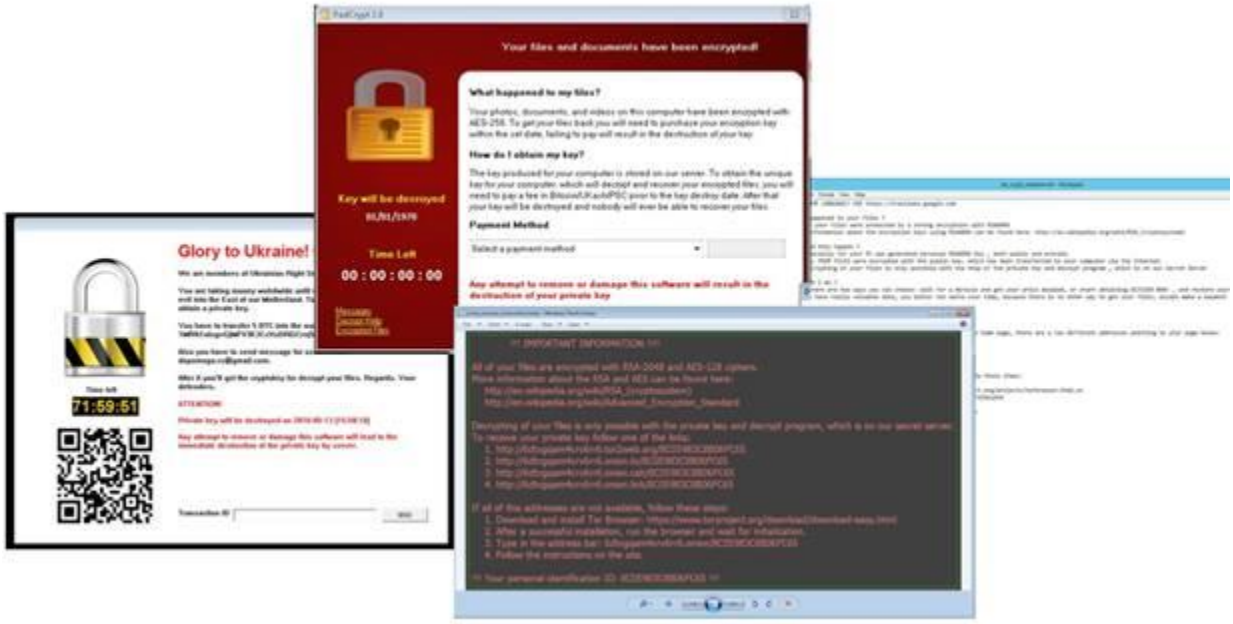
El viernes 12 de mayo se realizaron ataques cibernéticos mediante ***ransomware*** en diferentes partes del mundo. Por lo general, estos archivos maliciosos son enviados a través de correos electrónicos, redes sociales, entre otros. Recuerde que, si usted recibe un correo electrónico (usualmente en su *Junk Mail*) que no sea de una fuente de su confianza y tenga algún archivo adjunto o enlace, favor de borrarlo inmediatamente.

¿Qué es el *Ransomware*?



Ransomware es un tipo de virus informático (*malware*), que al infectar sistemas de computadoras o dispositivos móviles, restringe el acceso a archivos o documentos del usuario y en ocasiones al sistema en sí mismo. Es como si secuestrara los documentos, de ahí el termino *ransomware*, hasta tanto no se pague un "rescate" no se "libera" la data. Este tipo de malware ha sido observado en distintas variantes en los últimos años, pero en general funcionan de la misma forma, se intenta extorsionar a la víctima para obtener dinero, a cambio de la clave (*encryption key*) que le permitirá recuperar la data, de lo contrario, nunca podrá

recuperarla. El mensaje de pedido se da a través de una pantalla que aparece al tratar de acceder un archivo infectado o un sistema en particular y el precio del rescate oscila entre los $200 - $400 en moneda virtual (*bitcoins*), lo que evita el rastreo o ubicación del "secuestrador". En ocasiones se establece un periodo de tiempo para "pagar el rescate", de lo contrario será más costoso, esta técnica lleva a la víctima al desespero y muchas personas pagan el rescate, con el agravante que en la mayoría de las ocasiones no logran recuperar la información, puesto que han sido víctimas de réplicas del malware original, y los "secuestradores" realmente no poseen el *encryption key*.

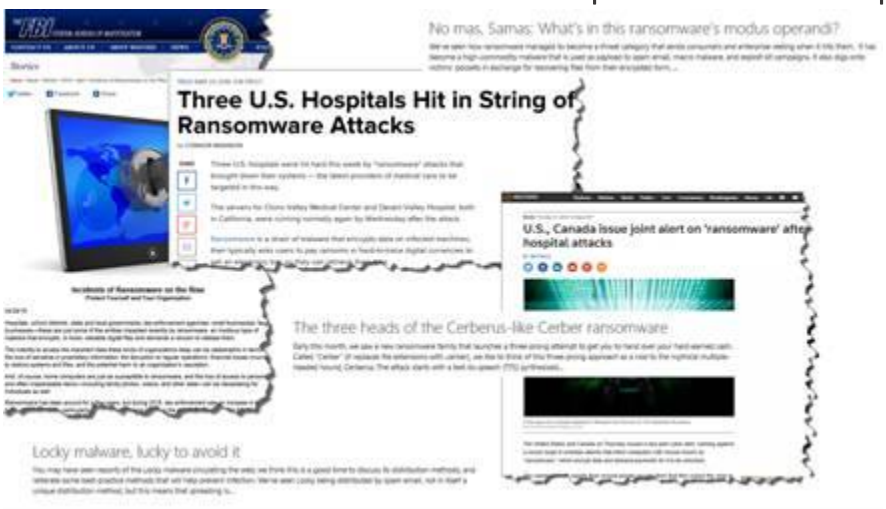
WannaCry

El nuevo virus *WannaCry*, que ha afectado hasta el momento más de 150 países, es un ataque de tipo *ransomware*. Fue descubierto en la tarde del viernes 13 de mayo al afectar el sistema de salud del Reino Unido y empresas españolas y francesas. Aunque el ataque original está parcialmente controlado, se espera que surjan más ataques con nuevas réplicas creadas a partir del virus original.

¿Cómo llega a la computadora de la casa o a una empresa?

Aunque se han registrado variantes de este tipo de malware que se propagan a través de redes sociales, especialmente Whatsapp o Facebook, el medio más común de infección es el correo electrónico. Cuando un usuario recibe, de otro usuario infectado, un correo electrónico con un documento adjunto (*attachment*) infectado, al abrirlo se infecta su computadora o dispositivo. No

solo se infecta con el llamado *ransomware*, también se infecta con otros tipo de malware cuya función es buscar información personal identificable (PII por sus siglas en inglés) o información bancaria para robarla. En ese mismo instante, el dispositivo de la víctima se convierte en *zombie* o *bot* que intentará propagar el virus a



cuantos contactos adquiera de las listas que obtenga. Inmediatamente el *ransomware* comenzará a cifrar ("encriptar") los archivos del usuario, comenzando por los menos usados, esto le dará tiempo de completar el proceso antes de que la víctima tome conciencia de lo que está sucediendo. Los dispositivos USB son también un vector importante de infección, pero es el correo electrónico, por su simplicidad de uso y alcance, el más común, especialmente en las empresas.

Impacto

Las infecciones con este tipo de *malware* son considerados como ataques cibernéticos por el gobierno de los E.E.U.U. Este tipo de ataque no solamente se da contra usuarios domésticos, es muy común en organizaciones privadas y públicas. Estas infecciones pueden tener consecuencias graves para una empresa, como la pérdida temporal o permanente de información confidencial o propietaria hasta la interrupción de las operaciones normales en

una empresa y por consiguiente pérdida de dinero y daño a la imagen corporativa. Se han registrado ataques a sistemas de proveedores de salud con consecuencias muy graves en la información de los pacientes.

Pagar el rescate no garantiza que los archivos se lograrán recuperar, lo único que garantiza es que los atacantes reciben dinero de la víctima, y en algunos casos, su información bancaria. Además, descifrar (*decrypt*) los archivos no significa que la infección de malware en sí se ha eliminado.

Solución

No hay una solución fácil a este tipo de infección, aunque se sabe de personas que han recuperado la información pagando el "rescate", la mayoría no logra recuperar nada. Lo más práctico para evitar pérdida de información en este tipo de casos es la prevención.

- Lo más importante: no abrir archivos o enlaces de correos electrónicos que no se hayan solicitado. Si estos provienen de una persona conocida, indagar antes con la persona que haya enviado el correo, las razones por las cuales lo ha hecho.
- Mantener un resguardo de la data, particularmente en un lugar seguro, los dispositivos USB (*USB Drives*) y los directorios compartidos (*Network Shares*) o directorios comunes, no son seguros, puesto que están sujetos a infección. Lo ideal es tener la data resguardad en un lugar que permita la recuperación de versiones anteriores de los archivos deseados. Esto se puede lograr usando sistemas como

SharePoint o *DropBox*. En el caso de computadoras personales, la opción *previous versions* (también conocida como *Volume Shadow Copies*) de Windows (v.v.7 – 10) puede ayudar, aunque no es del todo segura pues se han registrado versiones que también tratan de eliminar estos archivos.

- Mantener los anti-virus y el sistema operativo de las computadoras actualizados.
- Evitar navegar en portales de reputación dudosa o potencialmente peligrosos, como sitios de pornografía o de contenido compartido de manera ilícita, como los que se usan para bajar películas pirateadas.
- Infórmate sobre este y otros tipos de virusa informáticos y practica la "computación segura"

Información adicional

Para más información puede visitar https://www.us-cert.gov/ncas/alerts, El United States Computer Emergency Readiness (US-CERT) es una división del Gobierno de los E.E.U.U. adscrita a Homeland Security y cuya función es el desarrollo de medidas preventivas y reactivas ante ataques informáticos.

http://www.elnuevodia.com/tecnologia/tecnologia/nota/unaempresarusadenunciaciberataquea74paises-2320382/

https://diarioti.com/que-es-el-ransomware-y-como-evitarlo/104414

https://diarioti.com/centenar-de-paises-afectados-por-ransomware-habilitado-por-la-nsa/104410