Riesgos Cibernéticos

FUENTE: http://cnnespanol.cnn.com/2017/10/26/bad-rabbit-ataque-hackers-adobe-virus-ransomware-malware/

Bad Rabbit: el nuevo ciberataque que afecta a Rusia y se extiende a otros países

El gobierno de Estados Unidos emitió una advertencia sobre un nuevo ataque ransomware que se extendió en Rusia y Ucrania y ha afectado otros países del mundo.

Este ciberataque se hace pasar como una actualización de Adobe antes de bloquear las computadoras y exigirles dinero a los usuarios para recuperar sus archivos. Según los expertos en ciberseguridad, el ransomware fue dirigido contra empresas rusas de medios de comunicación y contra los sistemas ucranianos de transporte. También fue detectado en otros países, incluyendo a Estados Unidos, Alemania y Japón.

El Equipo de Respuesta ante Emergencias Informáticas de Estados Unidos señaló en la noche de este martes que "ha recibido múltiples informes de infecciones de ransomware" en muchos países del mundo.

Bautizado como Bad Rabbit, este virus es el más reciente caso de cibercriminales que utilizan el ransomware para tratar de extorsionar a víctimas en todo el mundo. Este año, dos grandes ataques internacionales, el NotPetya y el Wannacry, causaron una gran alteración que afectó a compañías, instituciones gubernamentales y hospitales.

Cuando Bad Rabbit infecta una computadora, se apodera de los archivos y exige un rescate para recuperarlos. Los expertos y las agencias estatales le aconsejan a las víctimas no pagar, pues según advierten no existe ninguna garantía de que puedan recobrar su información.

El virus atacó los grupos rusos de medios de comunicación Interfax and Fontank, así como a sistemas e instituciones de transporte en Ucrania, incluyendo el aeropuerto Odessa, el metro de Kiev y el Ministerio de Infraestructura del país, de acuerdo a lo que informó la compañía rusa de seguridad cibernética Group-IB. Interfax confirmó que sus servidores estaban fuera de línea debido a un ciberataque.

Riesgos Cibernéticos

FUENTE: http://cnnespanol.cnn.com/2017/10/26/bad-rabbit-ataque-hackers-adobe-virus-ransomware-malware/

Aunque la mayoría de víctimas estaban en Rusia, también se observaron ataques en Ucrania, Turquía y Alemania. La firma de ciberseguridad ESET también identificó casos de "Bad Rabbit" en Japón y Bulgaria. Avast, otra compañía, señala que el ransomware ha sido detectado en Estados Unidos, Corea del Sur y Polonia.

❖ ¿Relación con un ataque anterior?

El número de víctimas por Bad Rabbit parece ser significativamente menor que el del ataque NotPetya, que en junio pasado afectó a Ucrania y se extendió a otros países. De hecho, el daño que causó a algunas empresas importantes se estima en millones de dólares. Sin embargo, los expertos sostienen que hay vínculos claros entre los dos virus.

Según Vyacheslav Zakorzhevsky, jefe del equipo de investigación contra malware de la firma rusa de ciberseguridad Kaspersky Lab, reveló que el ataque Bad Rabbit atacó redes corporativas usando métodos similares a los de NotPetya.

Además, Costin Raiu, director del Equipo Global de Investigación y Análisis de Kaspersky Lab, explicó en un mensaje que Bad Rabbit fue lanzado a través de "una elaborada red de sitios web hackeados", con un enlace a NotPetya.

Group-IB también encontró semejanzas entre los códigos de los dos ransomwares.

❖ El virus usa un viejo truco

El ransomware Bad Rabbit accedió a las computadoras al hacerse pasar por un instalador de Adobe Flash, en los sitios web de noticias y medios que resultaron comprometidos. Este virus sirve como un recordatorio de que nunca se deben descargar aplicaciones o software desde publicidades emergentes o sitios web que no pertenecen a la compañía de software.

ESET indicó que una vez el ransomware infecta el dispositivo, escanea la red buscando carpetas compartidas con nombres comunes e intenta robar y explotar las credenciales de los usuarios para poder acceder a otras computadoras.