Expertos de EEUU y Gran Bretaña contienen ciberataque global

Por SARA BURNETT, ALLEN G. BREED y SYLVIA HUI
Associated Press, 14 de mayo de 2017

LONDRES (AP) — El ataque cibernético que paralizó redes en hospitales, bancos y agencias gubernamentales en diversas partes del mundo mediante la propagación de un programa informático malicioso, fue frustrado por un investigador joven británico y el registro de un dominio barato, con la asistencia de veintitantos ingenieros de seguridad en Estados Unidos.

El Centro de Seguridad Cibernética Nacional de Gran Bretaña y otras partes elogiaron al investigador de ciberseguridad de 22 años identificado en internet sólo como MalwareTech, que sin proponérselo, descubrió un “interruptor de emergencia” que contuvo el ataque sin precedentes.

Para entonces, el ataque de “ransomware”, en el que se pide rescate para desbloquear el acceso a archivos, había causado problemas a hospitales de Gran Bretaña y en los sistemas informáticos de diversos países, en un intento de los autores para extorsionar dinero a los usuarios de computadoras.

Sin embargo, las acciones del investigador quizá ahorraron a las compañías y gobiernos millones de dólares y frenaron el ritmo de propagación del problema antes de que un número mayor de computadoras fueran afectadas en Estados Unidos.

MalwareTech dijo en un blog publicado el sábado que él regresaba de almorzar con un amigo el día anterior y se enteró que diversas redes en el sistema de salud de

Gran Bretaña fueron afectadas por un ransomware, lo cual le indicaba de que “se trataba de algo grande”.

El joven comenzó a analizar una muestra del programa informático malicioso y advirtió que el código de éste incluía una dirección web escondida que carecía de registro. Dijo que inscribió “de inmediato” el dominio, lo que efectúa con regularidad en un intento por descubrir vías para rastrear o detener un programa informático malicioso.

Al otro lado del océano, Darien Huss, un ingeniero investigador de 28 años con la firma Proofpoint de seguridad cibernética, hacía su propio análisis. Huss, que vive en el oeste de Michigan, dijo que advirtió que los autores del programa informático malicioso dejaron una característica conocida como interruptor de emergencia.

Huss tomó una captura de pantalla de su descubrimiento y lo compartió en Twitter.

MalwareTech y Huss forman parte de una comunidad global relacionada con la seguridad cibernética cuyos miembros trabajan de manera independiente o para compañías del ramo. Estas personas vigilan constantemente los ataques y trabajan en conjunto para parar o impedir ataques cibernéticos, y a menudo comparten información vía Twitter.

Es frecuente que estas personas utilicen alias sea por asuntos de privacidad o para protegerse de agresiones de venganza.

Pronto Huss y MalwareTech compartían lo que habían descubierto: que registrar el nombre del dominio y redireccionar los ataques al servidor de MalwareTech había activado el interruptor de emergencia, lo que detuvo las infecciones de ransomware. Esta maniobra es conocida técnicamente como “sinkhole”.

___

Burnett informó desde Chicago y Breed desde Raleigh, Carolina del Norte. El periodista de The Associated press, Jim Heintz, en Moscú, contribuyó a este despacho.