



RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/13450 y 184/13451

14/06/2017

38203 y 38204

AUTOR/A: DELGADO RAMOS, Juan Antonio (GCUP-ECP-EM)

RESPUESTA:

El viernes 12 de mayo a las 9:25 de la mañana se empezaron a producir una serie de infecciones en sistemas y redes informáticos de varias empresas españolas, así como de empresas en otros países, por un virus informático conocido como Wannacry, Malware (de malicious software) que era capaz de realizar un cifrado de los archivos de los ordenadores que infectaba, solicitando a continuación al afectado, mediante un mensaje en la pantalla del ordenador, un rescate de entre 300 y 600 dólares en BitCoins (una moneda virtual o criptomoneda) para poder descifrarlos y, por tanto, poder recuperarlos. Este tipo de virus se clasifican como “Ransomware”.

La primera empresa de la que se tuvo constancia que fue afectada contactó a las 11:15 de la mañana con el equipo técnico del CERT de Seguridad e Industria (CERTSI), operado conjuntamente por el Instituto Nacional de Ciberseguridad (INCIBE) del Ministerio de Energía, Turismo y Agenda Digital y el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), informando del problema e iniciando la colaboración para su contención, mitigación y recuperación.

A los efectos de incidencia internacional, España ha ocupado la posición 20 del ranking por países en número de infecciones acumuladas desde que se inició el ciberataque, cifrado en más de 180 países afectados y más de 360.000 infecciones. Según los datos del CERTSI en España se dispone a día de hoy de más de 2.500 evidencias acumuladas de conexiones de equipos a los dominios maliciosos. Por otro lado, por el momento el pago del rescate exigido por los ciberdelincuentes sería aproximadamente de entre 100.000 y 120.000 dólares en todo el mundo.

Las empresas españolas estratégicas afectadas hasta el momento han sido menos de una decena y pertenecen a diferentes sectores, entre ellos las Tecnologías de la Información y de la Comunicación (TIC), Energía, Sistema Financiero, y Sector Público, pero en ninguna de estas empresas se ha llegado a afectar a ningún sistema o red que dé soporte a servicios esenciales, a diferencia de otros países como Reino Unido, Rusia o Francia, en los cuales se ha producido impacto en el Sector Financiero, Transporte o Salud.



El Consejo de Seguridad Nacional convocó, inmediatamente después del incidente cibernético, una reunión extraordinaria en la cual los diferentes agentes que tomaron parte en el soporte, resolución y mitigación del ciberataque expusieron las diferentes acciones que llevaron a cabo durante la situación de crisis. En dicha reunión se debatieron los distintos puntos de mejora expuestos, entre los cuales se encuentra los procedimientos de coordinación, y la compartición de información relativa a los ciberataques. Para ello el CERTSI, operado por INCIBE y el CNPIC, en el ámbito del sector privado y especialmente las empresas y operadores estratégicos y críticos, cuentan con una herramienta para compartir información sobre ciberamenazas, denominada ICARO, en la cual y en tiempo real los posibles afectados pueden acceder a la información técnica más relevante para la mitigación del incidente, así como pautas para la recuperación de los sistemas y redes afectados. Asimismo, el Centro Criptológico Nacional, del Ministerio de la Presidencia y para la Administraciones Territoriales (CCN-CERT) en el ámbito de las Administraciones y Entidades Públicas, cuenta con una herramienta de compartición de información denominada REYES. Actualmente se está trabajando entre el CERTSI y el CCN-CERT para que ambas herramientas estén comunicadas y se pueda manejar en tiempo real por todos los Centros de Seguridad Públicos la información de ciberataques y ciberamenazas, y así hacer más efectivos los mecanismos y procedimientos de detección, prevención, respuesta, mitigación y recuperación.

Por otra parte, se indica a continuación el presupuesto del Instituto Nacional de Ciberseguridad (INCIBE), organismo es competente en materia de ciberseguridad a partir del ejercicio 2013:

| PRESUPUESTO INCIBE Año | Financiación PGE Aprobado (Miles de €) |
|----------------------------------|---|
| 2013 | 12.250 |
| 2014 | 12.250 |
| 2015 | 20.720 |
| 2016 | 20.720 |
| 2017 | 23.220 |

En cuanto al presupuesto del Instituto Nacional de Tecnologías de la Comunicación (INTECO) se señala que las cantidades consignadas fueron las siguientes:

| Año | Financiación PGE |
|-------------|-------------------------|
| 2006 | 2.000 |
| 2007 | 10.000 |
| 2008 | 11.280 |
| 2009 | 11.114 |
| 2010 | 7.147 |
| 2011 | 6.790 |
| 2012 | 7.000 |

Madrid, 14 de septiembre de 2017

