CSO ESPAÑA
COMPUTERWORLD FROM IDG

ENTREVISTAS | NOTICIAS | 19 MAY 2017

Claudia Ortiz-Tallo

Javier Candau: "Desde el CCN-CERT siempre recomendamos no efectuar el pago del rescate"

ComputerWorld ha tenido la oportunidad de entrevistar a Javier Candau, jefe de Ciberseguridad del Centro Criptológico Nacional, para poder profundizar sobre el ciberataque 'ransomware' del pasado viernes 12 de mayo.

¿Cómo se han vivido estos cuatro días en la organización?

Han sido días muy intensos, en los que todo nuestro equipo ha estado de guardia y en contacto directo con los principales equipos de respuesta a incidentes (**CERT/CSIRT**), nacionales e internacionales, así como con nuestros colaboradores habituales. Desde que a primeras horas del viernes 12 de mayo **nuestro Sistema de Alerta Temprana (SAT) comenzara a detectar los primeros incidentes relacionados con el *ransomware* WannaCry**, se redobló el trabajo para, en primer lugar, detectar y detener la propagación del código dañino en los sistemas del sector

público español y en las empresas de interés estratégico para el país. Ya esa misma mañana se ofrecían las primeras informaciones sobre las características del *malware*, **la explotación de la vulnerabilidad de Microsoft y las medidas de prevención y mitigación**. Mientras los teléfonos no dejaban de sonar al igual que la bandeja de entrada del correo no dejaba de recibir mensajes solicitando información, nuestro equipo se esforzó en buscar una vacuna que pudiera prevenir la infección. Finalmente, se consiguió el sábado por la mañana; una vacuna que viene actualizándose desde entonces). Todo ello intentando **informar a través de distintos canales** (boletines de alerta, comunicados en el portal web, redes sociales, etc.) de nuestros avances y pesquisas, sabedores del gran interés despertado tanto en España como en el resto del mundo.

¿Se puede cuantificar las pérdidas de las organizaciones españolas afectadas? ¿Qué empresas se han visto afectadas además de Telefónica? ¿Alguna infraestructura crítica?

Según nuestras primeras investigaciones, **las pérdidas de las organizaciones estarán más ligadas a la bajada de la productividad y al esfuerzo realizado por sus equipos de seguridad y sistemas que al pago del rescate**. Fueron numerosas las organizaciones que, o bien por estar infectadas o bien como medida de precaución, **cortaron cualquier conexión a la red de todos sus sistemas y decidieron solicitar a sus empleados que se fueran a casa**, precisamente para analizar los equipos y evitar la propagación por la red. Me consta que han sido numerosos los responsables de seguridad, tanto de la Administración como de empresas estratégicas, quienes han trabajado todo el fin de semana -el lunes además era fiesta en Madrid- para **analizar todos los equipos de su red y actualizar todos los que no lo estuviera**n. En este sentido, y aunque el parche apareció el 14 de marzo y hemos tenido casi dos meses para actualizar todos los sistemas, conviene reconocer que los parques informáticos del sector público son muy variados con numerosas tecnologías, y **su actualización no es tan sencillo como parece**.

En cuanto al posible pago del rescate, creemos que no ha sido muy elevado el porcentaje de usuarios que lo han hecho. Hay que tener en cuenta que, tanto en la Administración como en las grandes empresas, suele haber servidores de ficheros, en donde todos los usuarios tienen copia de respaldo. Costará mucho esfuerzo y trabajo reestablecerlos, pero **no es necesario pagar el rescate**. Otra cosa distinta será entre los usuarios finales.

Una de las medidas recomendadas es no pagar el rescate. ¿En qué casos puede haber excepciones y por qué?

Desde el CCN-CERT **siempre recomendamos no efectuar el pago del rescate**. En primer lugar porque no existen garantías de que los atacantes envíen la utilidad y/o contraseña de descifrado de los equipos. En segundo lugar porque se premia su campaña y se les motiva a seguir distribuyendo masivamente este tipo de código dañino. Se recomienda, además, conservar los ficheros que hubieran sido cifrados por la muestra de *ransomware* antes de desinfectar la máquina, ya que no es descartable que en un futuro apareciera una herramienta que permitiera descifrar los documentos que se hubieran visto afectados.

http://cso.computerworld.es/entrevistas/javier-candau-desde-el-ccncert-siempre-recomendamos-no-efectuar-el-pago-del-rescate