Fuente
Gestión

Fecha
23/May/2017

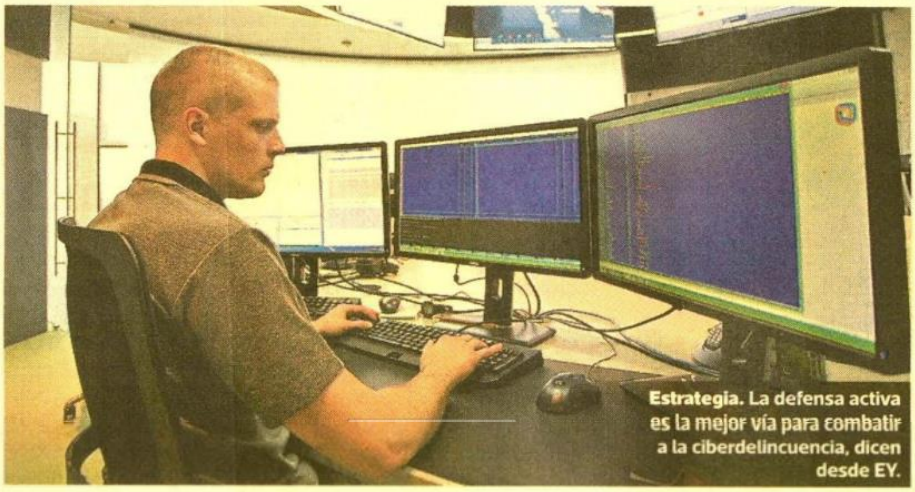
ANÁLISIS

WannaCry: el 'botón' que se pulsó en Perú y el nuevo capítulo que se estrena en cibercrimen

El virus supone un punto de inflexión para las siguientes amenazas. ¿Las firmas están del todo listas?

KAREN ROJAS ANDIA
krojas@diariogestion.com.pe

BLOOMBERG



Estrategia. La defensa activa es la mejor vía para combatir a la ciberdelincuencia, dicen desde EY.

"En el universo no hay cosas desconocidas sino temporalmente ocultas", decía el capitán James Tiberius Kirk en Start Trek. WannaCry, como ha sido bautizado el ataque global de dimensiones jamás vistas, así lo demuestra.

El virus, que se propaló desde el viernes 12, aprovechaba una vulnerabilidad de Windows a través de dos programas (o 'exploits'), Eternal Blue y Double Pulsar, que fueron robados por los cibercriminales a la agencia de inteligencia estadounidense (NSA).

El método llamó así la atención de los analistas porque WannaCry asumía la capacidad de expandirse en redes de ordenadores conectados entre sí, posicionándose como el software malicioso ideal para golpear empresas y oficinas gubernamentales.

El caso peruano

No obstante la fisura que sirvió para la campaña masiva de ransomware ya había sido aprovechada días antes por otro virus. El blanco, aseguran desde BBC, fue una institución financiera peruana.

"Nadie se detuvo a estudiar que los primeros 'abusos' de Eternal Blue se habían dado una semana antes y habían ocurrido en Perú", dijo Dmitry Bestuzhev, director del Equipo Global de Investigación y Análisis de Kaspersky Lab en América Latina.

De acuerdo al analista, si bien el ataque no utilizó el virus de la familia WannaCry, sí aprovechó una vulnerabilidad de Windows.

Según KPMG, es preciso actualizar todos los parches de seguridad, los sistemas antivirus, los perimetrales y análisis de red.

Y, aunque al inicio se pensó que era un ransomware común ("estas empresas reciben ataques de modo permanente", dice José Luis Najarro, director de Advisory de KPMG en Perú), después se advirtió que contenía las características que harían novedoso al ataque mundial.

Desde ESET Latinoamérica, Camilo Gutiérrez dice que lo ocurrido en Perú fue un "caso puntual (...) pues tenemos evidencia del uso del 'exploit' y la propagación de la misma familia de ransomware desde semanas antes".

A ello añade que, analizando los países donde hubo más detecciones de WannaCry, Perú se ubicaba hasta hace una semana séptimo en toda la región.

Punto de quiebre

Ahora bien, WannaCry tiene más víctimas que las declaradas (Europol dice que afectó 300,000 computadoras en 150 países).

Y es que, según El País, muchas de las firmas prefieren ocultar el bochorno que pasar por el escarnio de ser vulnerables por no ejecutar un simple parche de Windows.

Aunque, según dijo Dmitry Bestuzhev a **Gestión**, "la lucha por controlar la amenaza ya está dando frutos", la historia no acaba ahí.

Margen de mejora

Y si bien la conectividad nos conduce a un mayor desarrollo, también nos hace más vulnerables. Ningún sistema podría quedar librado de un siguiente ciberataque a escala.

WannaCry, en palabras de analistas de seguridad, es un nuevo paso en la evolución del cibercrimen, que pone sobre la mesa las capacidades ofensivas (y defensivas) de las naciones, los riesgos que supone un escalamiento de los ciberconflictos, entre otros.

De acuerdo a Elder Cama, socio de Consultoría de EY Perú, las empresas necesitan estar listas ante cárteles dedicados al terrorismo cibernético.

Pues, según una encuesta global de EY, el 86% de organizaciones señala que su función de seguridad cibernética no satisface plenamente sus necesidades. En el caso del Perú esa cifra se eleva a 90%.

La lección es clara: mantenerse por delante frente a escenarios inciertos, con el fin de actuar en consecuencia.

EN CORTO

Advertencia. Hacia marzo, el colectivo Shadow Brokers se jactaba de haberle robado a la NSA los programas Eternal Blue y Double Pulsar, que facilitaban ingresar a cualquier ordenador conectado y acceder a datos sensibles si tenían sistema Windows. Debido a ello, Microsoft lanzó un parche de seguridad, pero muchas empresas hicieron caso omiso.

LA CIFRA

4,000

millones de dólares habría sido el costo potencial del ataque.

Bastante por encima de los US$ 1,500 mlls. que dejaron las pérdidas por ataques en el 2016. Los criminales solo recaudaron US$ 104,000.

OTROSÍ DIGO

El alza de las firmas de ciberseguridad

Bolsas del mundo. Las compañías de ciberseguridad vieron al alza sus acciones mientras cientos de miles de computadoras aún padecen los estragos de WannaCry. Frente a la amenaza de otra oleada, Palo Alto Networks o FireEye subieron entre 3.39% y 5.4% en Wall Street.