ONU: Los autores del ciberataque global serÃ¡n detenidos si cobran el rescate

Autor Administrator
Friday, 02 de June de 2017
Modificado el Friday, 02 de June de 2017

EFE

Los rescates del ciberataque global de hace dos semanas estÃ¡n localizados y ascienden a unos 100.000 euros. Y en caso de que los "hackers" quieran hacerse con el botÃ-n, serÃ¡n detenidos, explica el mayor experto de Naciones Unidas en cibercriminalidad, Neil Walsh.

"Vemos que todos los rescates pagados estÃ¡n localizados en cuatro direcciones de bitcoin (una moneda virtual) manejadas por los delincuentes que las crearon", declara a Efe Walsh, director del programa global contra la cibercriminalidad de la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD).

Los piratas informÃ¡ticos utilizaron un virus llamado WannaCry que, a partir del viernes 12 de mayo y en apenas 48 horas, bloqueÃ³ cientos de miles de ordenadores en mÃ¡s de 150 paÃ-ses y por cuya "liberaciÃ³n" exigÃ-an un rescate.

Europa y Asia fueron los continentes mÃ¡s afectados por el ataque, del que fueron vÃ-ctimas tambiÃ©n hospitales britÃ¡nicos, factorÃ-as francesas de coches, aeropuertos alemanes o el Ministerio del Interior ruso, entre otros.

"Si (los 'hackers') intentan cobrar el dinero, los detendremos, sabremos dÃ³nde estÃ¡n y quiÃ©nes son", agrega el experto, que durante mÃ¡s de 15 aÃ±os trabajÃ³ para el Gobierno britÃ¡nico en la lucha contra el crimen organizado internacional y el terrorismo.

Walsh recuerda que una de las especializaciones de su departamento en la ONU es el seguimiento de transacciones con "bitcoin", la criptomoneda virtual en la que exigieron el rescate los autores del ciberataque.

La ONUDD ha capacitado a investigadores y fiscales de decenas de paÃ-ses para rastrear este tipo de operaciones y reunir asÃ- pruebas de ciberdelitos.

"Podemos hacer un seguimiento de las transacciones con "bitcoins". Esto nos permite desafiar la narrativa de que si usas "bitcoins" no serÃ¡s detectado. Al final serÃ¡s descubierto", sostiene.

"Cualquier tipo de secuestro, fÃ-sico o virtual, sÃ³lo merece la pena si recibes un pago. Si no obtienes dinero no tiene sentido hacerlo", indica el experto, que considera fundamental atajar el potencial beneficio de estos ataque.

"Si preguntas a los delincuentes, lo que mÃ¡s les duele es el dinero", afirma.

Y agrega: "Es la mejor forma de golpear a una organizaciÃ³n criminal. Al final hay un objetivo econÃ³mico y si limitamos sus oportunidades de acceder al dinero, destruimos su modelo de negocio".

Sobre la naturaleza del ataque, lo considera poco sofisticado y profesional, de escaso Ã©xito monetario y, debido a la enorme repercusiÃ³n, contraproducente, ya que los ciberdelincuentes siempre tratan de quedar "fuera del radar de la atenciÃ³n pÃºblica".

Al parecer, los atacantes aprovecharon una vulnerabilidad informÃ¡tica que aparecÃ-a en archivos robados a la Agencia de Seguridad Nacional estadounidense (NSA) y que fueron difundidos en abril.

"Enviaron este 'ransomware' creyendo que iba a ser una forma fÃ¡cil de hacer dinero, pero atrajeron la atenciÃ³n de todo el mundo sobre ellos, lo que como modelo de negocio criminal es muy malo", resume.

Para Walsh, el virus WannaCry es un ejemplo excelente de un ataque de "nivel bÃ¡sico" y, debido a la atenciÃ³n que ha generado, puede tener un efecto positivo: hacer comprender a Gobiernos, compaÃ±Ã-as y usuarios la necesidad de estar preparados.

"La cibercriminalidad es prevenible si se conocen los riesgos y se tratan de minimizar", explica Walsh , quien pide a todos los Gobiernos que desarrollen planes para proteger infraestructuras crÃ-ticas.

Si ataques similares paralizasen redes elÃ©ctricas, el control aÃ©reo o pÃ¡ginas de reservas de hoteles, por ejemplo, una economÃ-a podrÃ-a resultar muy daÃ±ada, advierte el experto.

Y para desarrollar una investigaciÃ³n digital es indispensable una gran cooperaciÃ³n internacional, porque este tipo de delincuencia no conoce fronteras y cuentan con numerosos instrumentos para ocultar su identidad.

"El mayor desafÃ-o en un cibercrimen es identificar a quiÃ©n estÃ¡ detrÃ¡s y dÃ³nde se encuentra. Hay muchas formas de enmascarar la identidad, la localizaciÃ³n o la lengua que usas", dice.

El experto vaticina que los delitos virtuales van a seguir creciendo porque son relativamente fÃ¡ciles de cometer.

"Es un negocio que estÃ¡ creciendo porque ser cibercriminal ahora es muy fÃ¡cil. Hace diez aÃ±os necesitabas conocimientos informÃ¡ticos, pero ahora hay mercados en la 'web profunda' en la que pagas unos cientos de dÃ³lares y alguien te desarrolla un virus. No necesitas ningÃºn conocimiento informÃ¡tico", asegura.

"Es un modelo que llamamos ciberdelincuencia como servicio. Si quiero controlar una red o colapsar la web de un Gobierno no necesitas saber cÃ³mo se hace, basta con pagar a alguien", concluye.

http://www.2001.com.ve/tecnologia/160974/onu--los-autores-del-ciberataque-global-seran-detenidos-si-cobran-el-rescate.html