¿Saldremos bien parados

del próximo Wannacry?

Dña. Claudia Gómez | Directora de Líneas Financieras en Aon Gil y Carvajal

Claudia Gómez
Directora de Líneas Financieras en Aon Gil y Carvajal

CIBERRIESGOS

Del 12 al 17 de mayo de este año se produjo uno de los mayores ataques cibernéticos a escala global. El virus Wannacry logró infectar, según las fuentes, entre 230.000/300.000 equipos en 179 países. De acuerdo con los datos oficiales de Incibe, España ocupó el 16º lugar de países más infectados. Esto coincide con nuestra experiencia en cuanto a los escasos incidentes declarados a pólizas de seguro. Pero la exactitud precisa de las cifras es poco relevante y nadie la conoce con exactitud.

Lo verdaderamente destacable es que durante esos días fuimos testigos de cómo empresas de todo tamaño, sector y condición resultaban infectadas, otras activaban rápidamente sus planes de crisis para prevenir la infección y otras fracasaba en gestionar la continuidad del negocio o el impacto mediático. Algunas de las empresas más afectadas están aún valorando los quebrantos.

Muchas pudieron recuperar la información soportando costes mínimos mientras que otras sin embargo tuvieron que pagar para poder recuperarla.

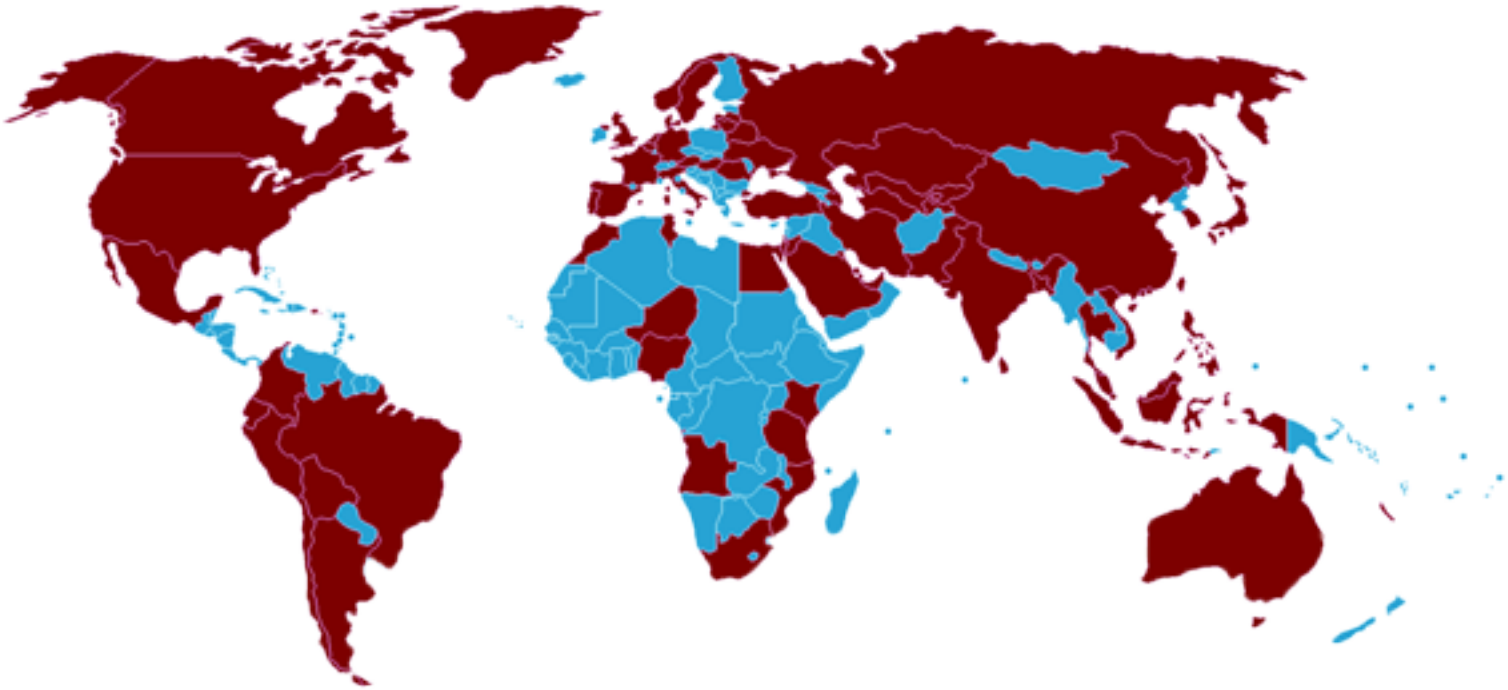
El origen del ataque apunta a los hackers del gobierno norcoreano, necesitado de fondos para financiarse a causa del bloqueo internacional, pero nuevamente esto tampoco es lo más relevante. Lo importante es que no estábamos preparados. El ransomware no es una nueva amenaza, más bien al contrario. Pero es tan rentable para los cibercriminales que siguen invirtiendo tiempo y dinero en detectar vulnerabilidades y generar nuevos softwares maliciosos y botnets.

Wannacry es sólo la punta del iceberg de una realidad que nadie pareciera querer ver. Antes y después de Wannacry, otros malware han seguido infectando equipos a diario en todo el mundo y en mayor número. No son mediáticos porque no han tenido la expansión virulenta de Wannacry ni ha habido grandes nombres de empresas para alimentar titulares de periódico, pero la realidad es que los secuestros de sistemas y datos sigue en aumento y que los usuarios seguimos clicando enlaces o abriendo ficheros que contienen software malicioso de forma negligente o porque somos excesivamente confiados.

Wannacry es sólo la punta del iceberg de una realidad que nadie pareciera querer ver.

Wannacry cuenta además con el dudoso "honor" de ser el primero de su especie en comportarse de forma tal virulenta. Como decíamos ha habido otros muchos gusanos posteriores, pero expertos en seguridad y autoridades coinciden en que las probabilidades de que repita un nuevo incidente global son muy elevadas, ya que los nuevos gusanos van a ser mucho más difíciles de detectar y más potentes a la hora de propagarse. Si a pesar de estos avisos y alertas nos vuelve a pillar desprevenidos es, como se dice coloquialmente, para hacérnoslo mirar en serio.

Países afectados por el Virus Wannacry de 12 al 17 de mayo de 2017



El ransomware goza de muy buena salud y vino para quedarse. El poder desarrollar un software malicioso que quiebre la seguridad de un banco, si lo consiguen (y muchas veces lo consiguen) es sumamente atractivo ya que la recompensa es mayor que la inversión realizada. Ahora además hay todo un universo nuevo al que infectar y monetizar rápidamente: OT, IoT, dispositivos móviles fuera del control corporativo, etc. Demasiado tentador como para ignorarlo.

No nos engañemos: si incluso gobiernos y grandes empresas que cuentan con más fondos les cuesta estar por delante en tecnología de seguridad para hacer frente a ataques y software maliciosos, cuánto más vulnerables serán todas las empresas que no cuenten con las mismas capacidades de defensa.

Por tanto, sigue siendo necesario que nos concienciemos en que hay que hacer una gestión de riesgos y que pasa por identificar nuestros activos tecnológicos críticos, en analizar las amenazas e impacto económico, en invertir en seguridad tecnológica y procesos (entre otros, implementar de forma adecuada las actualizaciones y parches), en seguir educando al personal y a la alta dirección de unas medidas de prevención básicas y en preparar planes de respuesta a incidentes adecuados para garantizar la continuidad del negocio y gestionar el potencial daño a la reputación, sin olvidar el respaldo de productos aseguradores que nos ayuden a mitigar la pérdida económica.

Con respecto al daño reputacional recordemos que cuando comience a aplicarse el nuevo reglamento de protección de datos o se transponga la Directiva NIS, las quiebras de datos y de seguridad se deberán hacer públicas. Sólo la autoridad de control decidirá en qué casos eximirá a las empresas de cumplir con dicha obligación. Pero dudamos que vayan a ser benévolas con aquellos que se han mostrado laxos en materia de ciberseguridad. Esperemos que los datos que revelan que muchas empresas no estarán preparadas para cumplir con el nuevo reglamento cuando entre en aplicación en Mayo 2018 hayan mejorado.