.Seguridad
Cultura de prevención para TI
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

LA VIDA DESPUÉS DE WANNACRY

Francisco Carlos Martínez Godínez

numero-30

"Como en la mayoría de incidentes de seguridad, este no es un problema tecnológico, es un problema de procesos y de gente" (Litan, 2017).

Es cada vez más común ver a organizaciones invertir en dispositivos y herramientas de seguridad, adquirir soluciones para mantener a la empresa segura, y diseñar campañas informativas y de concientización. Lo que ocurrió en mayo de 2017 significó una sacudida mayor para los programas de

seguridad de la información en compañías de todos los tamaños alrededor del mundo, y reveló una verdad irrefutable: las organizaciones no están preparadas.

Se trató de un incidente de seguridad como no se había visto antes, al menos en cuanto a impacto y alcance, y deja varias preguntas en el aire que deberán ser respondidas en varios niveles dentro de las organizaciones. ¿Cómo una vulnerabilidad conocida pudo ser aprovechada a estos niveles? ¿Pudo hacerse algo más? ¿Dónde se está fallando? Y lo más importante, ¿qué lecciones se aprendieron?

EL MUNDO SECUESTRADO

WannaCry es un *ransomware* que explota la vulnerabilidad de SMB (MS17-010), la cual es considerada crítica por Microsoft, y afecta a todas las versiones de los sistemas operativos Windows. Este tipo de malware no es nuevo, de hecho el secuestro de equipos se ha vuelto cada vez más frecuente. Sin embargo, la aparición de WannaCry representa un evento importante en el mundo de la seguridad a nivel global, pues lo que se presenció con este *malware* no tiene precedentes principalmente por tres factores.

Primero, el alcance. Cinco continentes, más de 179 países y más de 300,000 equipos infectados (Tovar, González, y García, 2017); 16 hospitales en Reino Unido, Renault, FedEx, el operador español de telefonía móvil Telefónica, la estación de trenes alemana en Frankfurt, el ministerio interior y el banco Sberbank rusos, son solo algunas de las instituciones que fueron golpeadas por este malware (Times Media, 2017). El ataque, cuyos primeros indicios fueron detectados en España y Reino Unido, se propagó en minutos alrededor del mundo.

Segundo, la arquitectura del ataque. Wannacry está formado por dos componentes clave: un gusano y un ransomware. El gusano utiliza un exploit que aprovecha una vulnerabilidad en SMB y se propaga sin la necesidad de la interacción de usuarios (Williams, 2017).

Tercero, la utilización de una herramienta creada originalmente por una institución gubernamental. Resulta interesante el hecho de que WannaCry utiliza para propagarse SMBv1 Eternalblue, un exploit que, se asume, fue robado a la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en inglés), y el cual se hizo público apenas un mes antes de la propagación del ransomware (Williams, 2017). Eternalblue implanta una pieza específica de *shellcode* llamada Doublepulsar, la cual tiene la particularidad de ejecutarse en el espacio de kernel. Eternalblue forma parte del grupo de herramientas de hacking desarrollado por la NSA y que fue filtrado por el grupo de hackers Shadow Brokers (Ullrich, 2017). Existen fuentes que apuntan a la existencia de este grupo con los servicios de inteligencia rusos, lo que resulta interesante y paradójico, siendo que instituciones rusas fueron de las primeras afectadas tras este ataque (Price, 2016).

UNA VERDAD INCÓMODA

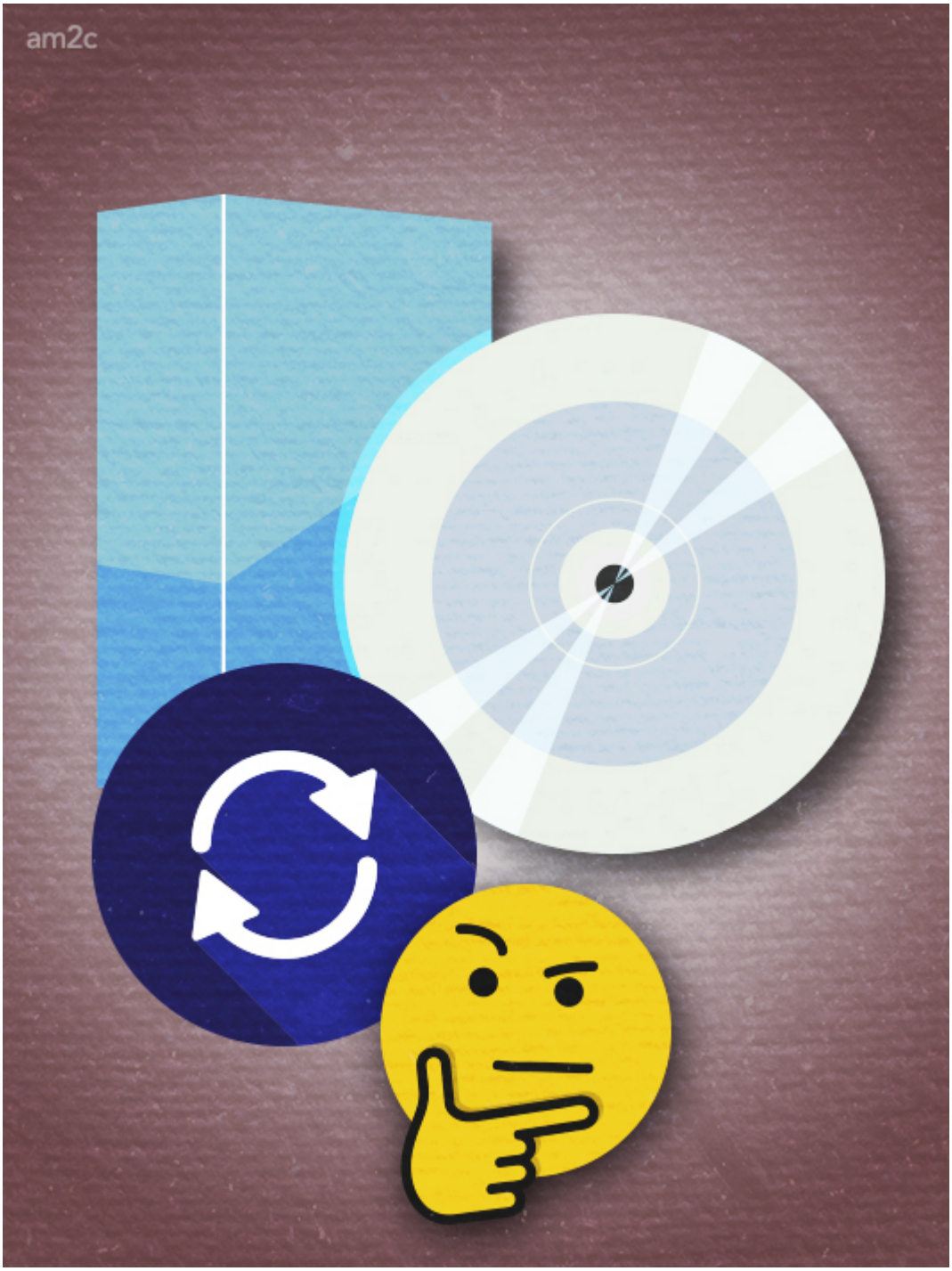
Existe una preocupación detrás de ataques como WannaCry, y es el hecho de que se ha dejado en

evidencia una profunda desconexión entre el trabajo realizado por los equipos de TI, encargados de la operación, y los de seguridad, encargados de prevenir ataques contra la organización, así como la falta de procesos adecuados en ambas partes. De acuerdo con Avivah Litan, analista de Gartner, más del 90% de los ataques utilizan vulnerabilidades comunes y que pueden ser prevenidos manteniendo los sistemas actualizados, lo que indica que los procesos, como el de la instalación de actualizaciones, están fallando (Litan, 2017).

En el caso de WannaCry, las áreas de seguridad de las compañías debieron tener una visibilidad mínima de los sistemas vulnerables y por lo menos sugerir alguna acción acorde con el nivel de la amenaza. Sin embargo, es indudable que los encargados de la gestión de actualizaciones y la instalación de las mismas son las áreas operativas. Falta de seriedad o conocimiento respecto a la amenaza o falta de mecanismos y recursos para mitigarla son algunos de los posibles factores que desembocaron en el resultado ya conocido. La forma de enfrentar un incidente de seguridad debe estar soportada por procesos sólidos, y es ahí donde se están encontrando carencias. Se sigue invirtiendo todo tipo de recursos en cubrir necesidades tecnológicas olvidando que el eslabón más débil de la cadena sigue siendo las personas. Sin un plan de acción adecuado dominado por todos los involucrados, inevitablemente se volverán a cometer los mismos errores.

¿EXISTE UN PLAN B?

Si la falta de actualizaciones fue lo que abrió la puerta a WannaCry, ¿por qué no simplemente actualizarlo todo? ¿Por qué no deshacerse de una vez por todas de sistemas con Windows XP y/o mantener actualizados sistemas operativos y aplicaciones en cuanto nuevas actualizaciones son liberadas? Suena bien, pero el mundo real es mucho más complejo que eso. Muchas veces sistemas y aplicaciones no pueden ser actualizados sino hasta después de meses debido a la propia demanda de la operación, y existe infraestructura crítica que no puede ser ni actualizada ni migrada a nuevas versiones simplemente porque la interrupción del servicio que brinda es impensable, y tendría un impacto mayor en la salud, las finanzas o la seguridad de una organización o incluso de una nación entera.



Si la remediación no puede ocurrir por medio de actualizaciones, entonces, ¿no hay nada por hacer? Anton Chuvakin, analista de Gartner, señala que “si las organizaciones no pueden corregir el problema y no pueden aceptar el riesgo, ¿por qué no mitigan más? Generalmente porque el mitigar requiere controles y los controles cuestan dinero y/o tiempo” (Chuvakin, 2017). Así que, ¿cómo mitigar? ¿Cómo mantener seguros sistemas obsoletos y que no pueden ser actualizados? Ese es el reto. En ese sentido, el establecimiento de controles compensatorios, como el deshabilitar servicios, limitar el acceso a la red, endurecer configuraciones o implementar controles a nivel de red, de host o de

aplicación, pueden ayudar a reducir el riesgo inherente a sistemas que no pueden ser actualizados (Chuvakin, 2013).

CONCLUSIONES

Meses han pasado desde la aparición de WannaCry y aún parece poco tiempo para saber qué lecciones se aprendieron. Un mes después de este ataque, apareció un nuevo ransomware conocido como NotPetya, una variante del malware Petya, el cual aprovechaba la misma vulnerabilidad que WannaCry para su propagación, sin embargo, el impacto y los tiempos de respuesta ante este incidente fueron mucho menores. A primera vista, este hecho no representa una mejora significativa en la forma en que se afrontan incidentes de seguridad, ya que las compañías estaban preparadas para un ataque con esas características específicas. Sin embargo, este hecho parece demostrar que una vez que se cuentan con planes y procesos adecuados, el impacto y los riesgos pueden ser disminuidos. Los niveles de sofisticación y alcance de los ataques está creciendo día con día, y este crecimiento no va a detenerse. El siguiente gran ataque está gestándose en estos momentos en algún lugar del mundo y las organizaciones deberán estar preparadas, si es que algo se ha aprendido.

REFERENCIAS

- Chuvakin, A. (2017). WannaCry or Useful Reminders of the Realities of Vulnerability Management. *Gartner*. Recuperado el 14 de agosto de 2017, de http://blogs.gartner.com/anton-chuvakin/2017/05/18/wannacry-or-useful-reminders-of-the-realities-of-vulnerability-management/
- Chuvakin, A. (2013). Cannot Patch? Compensate, Mitigate, Terminate! *Gartner*. Recuperado el 14 de agosto de 2017, de http://blogs.gartner.com/anton-chuvakin/2013/10/28/cannot-patch-compensate-mitigate-terminate/
- Litan, A. (28 de junio de 2017). Wannacry and Petya point to dangerous disconnects between IT operations and security. *Gartner*. Recuperado el 14 de agosto de 2017, de http://blogs.gartner.com/avivah-litan/2017/06/28/wannacry-and-petya-ransomware-point-to-dangerous-disconnects-between-it-operations-and-security/
- Price, R. (16 de agosto de 2016). EDWARD SNOWDEN: Russia might have leaked alleged NSA cyberweapons as a 'warning'. *Business Insider Deutschland*. Recuperado el 14 de agosto de 2017, de http://www.businessinsider.de/edward-snowden-shadow-brokers-russia-leaked-nsa-equation-group-files-warning-dnc-hacking-2016-8
- Times Media (6 de mayo de 2017). *Infographic: The impact of WannaCry in numbers.* Recuperado el 14 de agosto de 2017, de https://www.businesslive.co.za/fm/fm-fox/numbers/2017-05-26-infographic-the-impact-of-wannacry-in-numbers/
- Tovar, S., González, R. y García D. (Junio 2017). Wannacry: Ataque mundial y consideraciones sobre ciberseguridad. *Revista .Seguridad Cultura de Prevención para TI* . Recuperado el 14 de agosto de 2017, de https://revista.seguridad.unam.mx/numero29/wannacry
- Ullrich, J. (15 de mayo de 2017). WannaCry/WannaCrypt Ransomware Summary. *SANS Internet Storm Center*

. Recuperado el 14 de agosto de 2017, de https://isc.sans.edu/forums/diary/WannaCryWannaCrypt+Ransomware+Summary/22420
- Williams, J. (12 de mayo de 2017). Special Webcast: WannaCry Ransomeware Threat - What we know so far. *SANS*. Recuperado el 14 de agosto de 2017, de https://www.sans.org/webcasts/special-webcast-wannacry-ransomeware-threat-105160?msc=wannacry

SI QUIERES SABER MÁS, CONSULTA:

- Wannacry: ataque mundial y consideraciones sobre ciberseguridad
- Concienciar para prevenir
- Ransomware, ¿quién secuestra nuestra información?
