SONICWALL

# RESUMEN EJECUTIVO: LA ESTELA DE WANNACRY

## Anatomía de un ataque de ransomware

## Resumen

La falta de iniciativa a la hora de aplicar mejores prácticas de seguridad de red a menudo tiene consecuencias devastadoras. Un reciente ataque de ransomware que ocupó todos los titulares tuvo un gran impacto a nivel global. En este documento se examina cómo los criminales cibernéticos perpetraron este ataque, los retos continuos a los que todavía se enfrenta el personal de TI y las lecciones aprendidas para evitar ataques futuros.

### Una historia común

Fue una historia de lo más común. Recientemente, los cibercriminales accedieron a la red de una empresa mediante un e-mail de phishing que contenía ransomware WannaCry. El archivo adjunto que contenía el e-mail se abrió en un ordenador que no contaba con el correspondiente parche, dejando la red a merced de los hackers. Al preguntarle sobre el hecho de que su sistema no estuviera provisto del parche, el propietario de la empresa respondió que no creía que el parche fuera muy importante.

### Anatomía de un ataque

Si piensa lo fácilmente que la empresa podría haber evitado la brecha, simplemente le darán ganas de llorar, que es precisamente lo que significa el nombre del ataque "*WannaCry*." Este ataque de ransomware masivo en particular infectó más de 250.000 sistemas en más de 150 países, incluidas varias instituciones sanitarias de gran tamaño en el Reino Unido e incluso algunas empresas de telecomunicaciones importantes en España.

*WannaCry* es tan solo un ejemplo de una amenaza que combina propiedades de ransomware y de gusano, y que utiliza un exploit del protocolo para compartir archivos SMB. Se dice que inicialmente ciertas agencias gubernamentales crearon un kit de exploits (en este caso, EternalBlue), que supuestamente los cibercriminales robaron.

Aunque cada vez ocupan más titulares, los ataques de ransomware no son ninguna novedad. Los exploits están a la orden del día. La excusa "no lo sabía" no soluciona el problema.

En abril de 2017, Shadow Brokers filtró EternalBlue al público como parte de un volcado de mayor envergadura de exploits desarrollados por la Agencia de Seguridad Nacional de EEUU (NSA). A continuación, los criminales aprovecharon elementos de ese kit de exploits en una forma nueva y extremadamente agresiva de ramsomware que utiliza un ataque tipo gusano contra los equipos de red conectados, haciendo uso de varias funciones de lectura/escritura del sistema operativo de Windows. Este exploit en particular afecta a varias versiones de los sistemas operativos de Microsoft Windows, algunas de las cuales se encuentran en la fase de fin de vida. A pesar de que Microsoft publicó gran número de parches para hacer frente a esta vulnerabilidad, el ataque continúa siendo peligroso, ya que muchas organizaciones no han aplicado el parche.

La primera versión del paquete gusano/ransomware tenía un interruptor de apagado de emergencia que pudo utilizarse para desactivar la función de gusano, lo cual frenó su avance. Sin embargo, las más de 20 versiones posteriores no tienen este punto débil. En todo caso, es importante utilizar tecnología capaz de detener todas las versiones conocidas de ransomware, así como de detectar nuevos ataques de ransomware.

## Conclusión

Cada sesenta segundos se crean más de 114 nuevos virus y variantes. *WannaCry* no es ni mucho menos el primer exploit que utiliza esta forma de ataque, y desde luego tampoco será el último. Las organizaciones deben despertar ante la nueva realidad cibernética que amenaza la seguridad de las redes a nivel global.

**Obtenga más información**. Lea nuestro Resumen de la solución: 7 mejores prácticas para detener el ransomware.

## Acerca de SonicWall

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios globales en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Para más información, consulte nuestra página Web.
**www.sonicwall.com**

ExecBrief-InTheWakeOfWannaCry-US-VG-29362