Análisis de malware. WannaCry

Álvaro García Jaén

Darío Abad Tarifa

Índice

Introducción

Un ramsonware es un tipo de malware que secuestra la información de la víctima y amenaza con publicarla o bloquear su acceso de forma permanente mediante su cifrado a menos que su rescate sea pagado. Dicho pago se hace normalmente a través de criptodivisas como Bitcoin, lo que dificulta el rastreo de los delincuentes.

El ataque sucedido el 12 de mayo de 2017 que tuvo como protagonista al ramsonware WannaCry ha sido descrito como sin precendentes y afectó a más de 230.000 computadoras de más de 150 países, incluyendo compañías importantes como Telefónica en España, FedEx e incluso departamentos del servicio nacional de salud de Gran Bretaña.

Es común encontrar descripciones que definen este malware como un criptogusano, esto es debido al comportamiento que refleja y lo que, probablemente, propició el gran alcance del ataque a nivel mundial. Esta característica es algo poco común respecto a otros ramsonware, ya que lo normal es que los ataques de este tipo se lleven a cabo mediante troyanos que llegan a los equipos de las víctimas a través de campañas de phishing. Sin embargo WannaCry se expandía de forma automáticamente por los equipos de la red tras la infección de un equipo.

Dicha expansión se llevaba a cabo mediante el uso del exploit *EternalBlue*, que fue revelado por el grupo *The Shadow Brokers* el 14 de abril (1 mes antes del ataque). Dicho exploit se aprovecha de la vulnerabilidad *MS17-010* del protocolo *Server Message Block*. El detalle importante es que Microsoft liberó un parche para esta vulnerabilidad el 14 de marzo (2 meses antes del ataque), sin embargo, es probable que debido al poco margen de tiempo y la falta de concienciación dicha actualización no fuera aplicada en la mayoría de equipos. Una actualización que además no cubría versiones de Windows XP.

Aunque es un ataque de gran gravedad, las consecuencias podrían haber sido peores si no se hubiera descubierto el *kill-switch* que detuvo la propagación o si hubiera sido un ataque dirigido a infraestructuras críticas, como centrales nucleares o eléctricas.

En este documento se tratará el contexto que acompañaba al suceso, se documentará el funcionamiento del malware, se hablará del impacto que tuvo y la perspectiva actual que se tiene sobre los ataques ramsonware. Además se comentarán las diferentes teorías sobre la, poco clara, autoría del ataque y se realizará un análisis técnico de una muestra del malware mediante técnicas de ingeniería inversa.

Antecedentes

Funcionamiento

Impacto

Atribución del ataque

Análisis técnico de una muestra

Conclusión

Bibliografia