WannaCrypt

Christofer Fabián Chávez Carazas
Universidad Nacional de San Agustín
Seguridad Computacional

22 de mayo de 2017

WannaCrypt (Wcry) es un ransomware cryptoworm con objetivo atacar sistemas Windows. Este virus fue partícipe de un ataque masivo a varias empresas y usuarios alrededor del mundo. [1] Este ransomware, como otros en su familia, encripta los datos alojados en la computadora a través del algoritmo AES, y pide un rescate en Bitcoins para su posterior desencriptación. El algoritmo AES necesita una key, que funciona tanto como para encriptar y desencriptar. Wcry no guarda dicha key en el ordenador local, sino lo almacena en la máquina desde la que se realiza el ataque. Otra de las dificultades que presenta este ransomware es que también afecta a las computadoras conectadas a la red. [2] Para poder infectar una computadora, Wcry utiliza el exploit EternalBlue desarrollado por la U.S National Segurity Agency (NSA).

El 12 de Mayo de 2017 se detectó los primeros ataques de Wcry. Se izo público rápidamente debido a las grandes empresas que se vieron afectadas, como Telefónica, Renault, FedEx, Nissan, Petro China entre otros. Además a afectado a gobiernos y universidades. Wcry ya ha infectado a más de 230,000 computadoras en 99 países [3] Debido a su creciente popularidad, varios investigadores se han puesto manos a la obra para poder encontrar formas de combatir Wcry. En las primeras versiones del ransomware se encontró un interruptor de apagado [4] que liberaba los datos sin ningún pago de por medio. Se cree que este interruptor se puso para hacer pruebas con el malware. Hoy en día se ha visto ataques con Wcry sin el interruptor de apagado. Se cree que puede haber una segunda holeada de ataques, ya que se han encontrado variantes del Wcry que dificultan la tarea de los investigadores para combatir el malware. [5]

Referencias

[1] Australian Broadcasting Corporation *Ransomware attack still looms in Australia as Government warns WannaCry threat not over*

[2] Javier Pastor *Wanna Decryptor: así funciona el ransomware que se ha usado en el ciberataque a Telefónica 12, Mayo, 2017*

[3] Eyerys *WannaCry Infecting More Than 230,000 Computers in 99 Countries*

[4] MalwareTech *How to Accidentally Stop a Global Cyber Attacks*

[5] Rosalía Rozalén *Se descubren nuevas variantes del ransomware WannaCrypt*