Ransomware

David Ricardo Cruz Juárez

Uno del malware utilizado con fines maliciosos fue "ransomware". El ransomware es un tipo de software malicioso que cifra los archivos o el sistema de un usuario y luego exige un rescate, generalmente en forma de criptomonedas, a cambio de proporcionar la clave de descifrado necesaria para recuperar los datos o el acceso al sistema.

Un ejemplo de este tipo de malware fue WannaCry.

En mayo de 2017, el ransomware WannaCry se propagó rápidamente a nivel mundial, este malware tenía como **mercado objetivo** el afectar a miles de organizaciones, incluyendo hospitales, empresas e instituciones gubernamentales, algunas de las entidades más notorias que fueron víctimas del ataque de WannaCry incluyen:

- Servicios de salud: La interrupción de los sistemas informáticos en entornos de atención médica puso en riesgo la atención a los pacientes y causó preocupación.
- Empresas: La pérdida de datos y la interrupción de operaciones tuvieron un impacto significativo en la productividad y las finanzas.
- Instituciones gubernamentales: Varios organismos y agencias gubernamentales que, al ser afectados por WannaCry, llevó a una respuesta urgente por parte de los gobiernos en buscar soluciones.
- Universidades y centros educativos: Afectó la infraestructura informática utilizada en la enseñanza y la administración.
- Organizaciones sin fines de lucro: esto demostró que WannaCry no discriminaba en función del tamaño o el tipo de entidad.
- Empresas de transporte y logística: Se reportaron casos en los que experimentaron interrupciones en sus operaciones debido al ataque, lo que afectó la gestión de la cadena de suministro.

Vulnerabilidad que explota WannaCry fue en el protocolo SMB (Server Message Block) de Windows, que había sido previamente filtrada por un grupo de hackers llamado "Shadow Brokers". Una vez infectado un sistema, WannaCry cifraba los archivos y mostraba un

mensaje de rescate en pantalla, exigiendo un pago en Bitcoin para desbloquear los datos. Este ataque causó interrupciones significativas y pérdidas financieras considerables.

¿Qué daños provoco WannaCry?

- Pérdida de datos: WannaCry cifró los archivos en las computadoras infectadas, lo que resultó en la pérdida de acceso a datos críticos para individuos y organizaciones.
- Interrupción de operaciones: Organizaciones, hospitales, empresas y servicios gubernamentales, experimentaron una interrupción significativa de sus operaciones, lo que provocaba que los sistemas afectados se volvieron inoperables, lo que tuvo un impacto en la prestación de servicios y la atención médica, entre otros.
- Pérdidas financieras: Las pérdidas considerables. Las organizaciones afectadas tuvieron que gastar dinero en recuperación de datos, mejoras de seguridad y, en algunos casos, el pago de rescates a los atacantes (aunque se desaconseja pagar rescates).
- Daño a la reputación: El ataque de WannaCry tuvo un impacto negativo en la reputación de muchas organizaciones afectadas, ya que mostró debilidades en sus medidas de seguridad cibernética.
- Conciencia de seguridad cibernética: Aunque tuvo un impacto negativo, el ataque de WannaCry también aumentó la conciencia sobre la importancia de la seguridad cibernética a nivel global. Llevó a empresas y organizaciones a tomar medidas más serias para proteger sus sistemas y datos.
- Desarrollo de parches y soluciones de seguridad: El ataque de WannaCry resaltó la necesidad de mantener sistemas operativos y software actualizados con los últimos parches de seguridad.

LINK CVE , Microsoft lanzó un parche de seguridad para la vulnerabilidad EternalBlue (CVE-2017-0144) CVE - CVE-2017-0144 (mitre.org)

EN resumen, el ataque de WannaCry fue uno de los más notorios de su tipo debido a su propagación rápida y generalizada y el daño causado por WannaCry fue significativo tanto en

términos de pérdida de datos como de interrupción de operaciones y costos financieros, además tuvo un impacto a largo plazo en la forma en que las organizaciones abordan la seguridad cibernética y la importancia de mantener sistemas actualizados y seguros.