Tecnológico Nacional de México

Instituto Tecnológico de Tijuana

Semestre:

Cuarto

Carrera:

Ingeniería Informática

Nombre de la materia:

Taller de legislacion informatica.- 4IF4A

Clave de la materia:

4IF4A

Actividad:

Profesor:

SANCHEZ VIZCARRA DANIELA ADRIANA

Alumno(s):

Arriaga Castillo Ismael Arafath - 20212745

León Quintero Saúl Andrés - 20212114

Cardenas Lopez Erick Alexis - 19211137

Fecha de entrega:

31/05/2022

¿Qué es el ransomware WannaCry?

WannaCry es un ejemplo de ransomware de cifrado, un tipo de software malicioso que los cibercriminales utilizan a fin de extorsionar a un usuario para que pague.

El ransomware ataca cifrando archivos valiosos para que no puedas acceder a ellos, o bien bloqueando tu acceso al ordenador para que no puedas utilizarlo.

Al igual que otros tipos de ransomware de cifrado, WannaCry secuestra tus datos con la promesa de devolverlos si pagas un rescate.

Este se aprovechaba de un fallo de seguridad conocido como "EternalBlue" en una versión del protocolo Server Message Block (SMB) de Windows para propagarse en forma de “gusano” en redes específicas.

WannaCry tiene como objetivo los ordenadores que utilizan Microsoft Windows como sistema operativo. Cifra los datos y exige el pago de un rescate en la criptomoneda bitcoin por su devolución.

¿Cuál fue el ataque ransomware WannaCry?

El ataque de ransomware WannaCry fue una epidemia global que tuvo lugar en mayo de 2017.

Este ataque de ransomware se propagó a través de ordenadores con Microsoft Windows. Los archivos del usuario se mantuvieron retenidos y se solicitó un rescate en bitcoins para su devolución.

Si no fuera por el uso continuado de sistemas informáticos obsoletos y por la formación deficiente en torno a la necesidad de actualizar el software, el daño causado por este ataque podría haberse evitado.

¿Cómo prevenir ataques de malware WannaCry?

Normalmente se piden los mismos requisitos para cualquier ataque de malware. A continuación se darán las prevenciones para este malware en específico:

- No descargar archivos desconocidos o de dudosa procedencia.
- Tener un antivirus activo.
- No abrir correos de orígenes desconocidos.
- Revisar conexiones u opciones en la configuración del wifi o router.
- Revisar actualizaciones con relación a los antivirus.
- (opcional/preferente) Realizar un respaldo o copia de seguridad de todo el ordenador y/o archivos importantes.