La Anatomía de #WannaCry

Fase 1: Ataque Externo

External Cyber-Kill Chain

Reconocimiento Externo

Busca empresas con dispositivos que tengan el puerto 445 abierto, y que fuesen sensible al exploit EternalBlue.

Armamentismo y Paquetización

Creación artefactos como Código a inyectar en proceso SMB y KILL-SWITCH

Entrega y Explotación

Explota vulnerabilidad con Exploit Eternalblue, herramienta de hacking robada a la NSA

Instalación

Se inyecta en procesos del sistema SMB y se hace persistente.

Command & Control

Kill-Switck, espera órdenes para actualizar el dominio XXX. Una nueva variante sin Kill-Switch imparable.

Fase 2: Ataque Interno

Internal Cyber-Kill Chain

Reconocimiento Interno

Busca dispositivos de la red interna que tengan el puerto 445 abierto, y que fuesen sensible al exploit EternalBlue.

Explotación Interna

Explota la vulnerabilidad con el exploit EternalBlue y su variante PayLoad DoublePulsar y se inyecta en procesos del sistema SMB y se hace persistente.

Movimientos Laterales

Se propaga a aquellos dispositivos vulnerables y explota una variante del PayLoad DoublePulsar.
El proceso comienza nuevamente en cada equipo infectado. La capacidad de propagación de la red es enorme.

Manipulación del Objetivo

Toma de control

Accede a los ficheros del sistema y borra las carpetas de Shadow Copy para evitar que el usuario recupere la información.

No permite arrancar en modo recuperación del sistema.
Oculta la papelera de reciclaje.

Mata los procesos que tienen abiertas bases de datos para garantizar el acceso a la encriptación de esos datos.

Procede a encriptar los ficheros y directorios del sistema mediante un algoritmo AES, solo descifrable a través de la clave RSA privada.

Termina la encriptación y muestra un diálogo al usuario pidiendo el rescate.