The #WannaCry Anatomy

Phase 1: External Attack
External Cyber-Kill Chain

- **External Reconnaissance**
  - Search for organizations with open port 445 endpoints and exploitable with EternalBlue.
- **Weaponization**
  - Creation of artifacts like the code to be injected in SMB process and KILL-SWITCH mechanism.
- **Delivery & Exploitation**
  - Exploit vulnerability with EternalBlue, a hacking tool stolen to NSA.
- **Installation**
  - It injects code into the SMB system process and becomes persistent by creating an entry in the Windows registry.
- **Command & Control**
  - Wait for domain controller orders to act. New variant without Kill-Switch.

Taking Control

- **External Reconnaissance**
  - Search for organizations with open port 445 endpoints and exploitable with EternalBlue.
- **Internal Exploitation**
  - Exploit vulnerability with EternalBlue. It injects code into the SMB system process and becomes persistent by creating an entry in the Windows registry.
- **Lateral Movement**
  - It copies itself to those vulnerable endpoints by exploiting a variant of the DoublePulsar payload. The process starts again on every infected computer. The capacity of propagation within the network is enormous.
- **Target Manipulation**
  - Proceeds to encrypt the files and directories of the system using an AES algorithm, which can only be decrypted if the private RSA key is available.
- **Taking Control**
  - Gets access to system files and deletes existing Shadow Copy folders to prevent the user from retrieving information.
  - Does not allow booting in system recovery mode. Hides the Recycle Bin.
  - It kills processes that have open databases to guarantee access to the encryption of such databases (mysql, sqlserver and Exchange).
  - Proceeds to encrypt the files and directories of the system using an AES algorithm, which can only be decrypted if the private RSA key is available.
  - When the file encryption finishes, it shows a dialog to the user requesting the ransom.