# WannaCry

## Simple timeline - from EternalBlue to WannaCry

### 12/05 2017 — WANNACRY PROPAGATES

- 230 000+ machine infected
  Worm + Cryptolocker
- Propagates through SMB protocol (445/TCP) - not by email (confusion with JAFF)
- Uses MS17-10
- Ransom : 300 to 600 USD per machine
- 98% of the victims are running Windows7
- 13/05/17:MS releases a patch for XP & 2003

### 8/04 2017 — ETERNAL BLUE PUBLIC RELEASE

On 08/04/17 & 14/04/17 Shadow Brokers publish new documents and release the password to read the archive "eqgrp-auction-file.tar.xz.gpg",those files contains, among others, the exploit Eternal Blue

**The archive also contains other exploits (like EsteemAudit, targeting Terminal server) that could be worm-able!**

### 14/03 2017 — MS PUBLISHES MS17-010

Microsoft publishes a patch (MS17-010), this patch fixes the vulnerability used by EternalBue
No fix for XP & 2003 (end of support)

### 13/01 2017 — SHADOW BROKERS - MESSAGE FINALE

The Shadow Brokers group publish a new archive "equation_drug.tar.xz.gpg" , this archive is password protected and is supposed to contain new exploits

### 13/08 2016 — SHADOW BROKERS - AUCTION / POST

The Shadow Brokers is a hacker group that published several leaks containing hacking tools (supposedly) from the NSA, including several zero-day exploits.
They have posted on Github (and quickly removed) several files

- “eqgrp-auction-file.tar.xz.gpg” that contains a collection of exploits (password protected) - auction to get the password (price >500M USD)
- “eqgrp-free-file.tar.xz.gpg” that contains some samples of exploits and implants for a variety of networking equipment

### 2013 — ETERNAL BLUE CREATED

EternalBlue exploit has probably been coded back in 2013...

**SOURCES**
Wikipedia, Kaspersky lab, adamcaudill.com

**CREATED BY**
Hacknowledge ,Switzerland

Hacknowledge