

... and it turned vicious

## **WannaCry** and **NotPetya** (2017)

- Use the *EternalBlue* vulnerability found in the NSA hacking toolkit leak
- Researcher has found a "kill switch"
- Paralyzed hospitals in UK and trains in Germany
- Caused \$10B+ damage, largest cyber-incident to date

## **LockBit 3.0** (2024)

- Advanced RaaS (Ransomware as a Service)

# Late 10's - the emergence of IoT malware and Cryptominers

## **Mirai** (2016)

- Infects IoT devices
- Most powerful DDoS attacks to date

## **Coinhive** (2018)

- Javascript embedded in website (either legitimately or not) and popular malware as well

## **Crypto Drainers** (2023)

- Target custodial and non-custodial crypto wallets
- Uses Telegram and Discord bots for C2