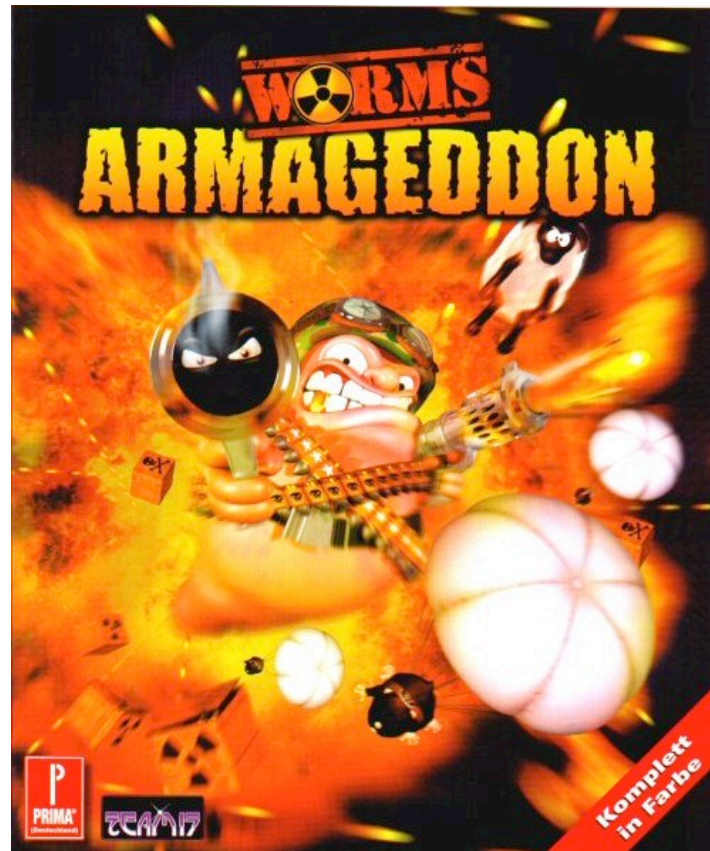


# The Threat of Worms!



Neil Kumar

# What is Stuxnet?

- Unusually complex
  - Over half a megabyte in size
  - Required highly specific knowledge to develop
  - Written in several programming languages

# What is Stuxnet?

- Highly resilient
  - Digitally signed with two (stolen) authentic certs
  - Can be updated through P2P communication
  - Utilized 4 zero-day vulnerabilities

# What is Stuxnet?

- Had a specific target(?)
  - **"Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?"**
  - Siemens?
  - Critical infrastructure *anywhere*?

# Not so subtle...

- Collateral damage as a *drawback* to its design.
- Compare to 2007 Israeli attack on Syrian plant
  - Pulled a kill switch at specific radar installations without anyone knowing

# How was it deployed?

- Physically, with USB sticks.
  - Speculation as to who could've started the spread
  - Went undetected for months potentially
  - The Russians?

# What does it mean?

- The initial purpose was thought to be stealing of industrial secrets
- But it turns out it was probably a bit more insidious than that...

“One-shot weapon?”

