Stuxnet

The most complex malware ever written (maybe)

$whoami

- Isaac Basque-Rice (@IBRice101)
- 3rd Year
- Linux Stan and IoT nerd
- Wiki Editor Extraordinaire
- Bass player n music lover
- Emote
- They/Them :)

Background

Iran, Iran so far away

- Iran was enriching uranium…
- Nuclear bombs perhaps?

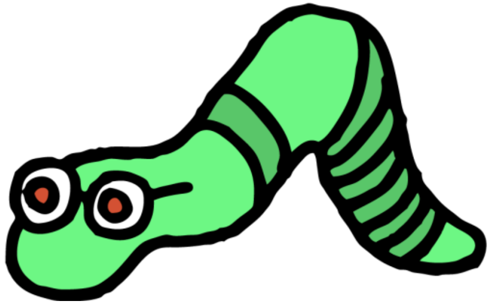
The US wasn’t very happy.

- Two main reasons:
  - Non-Proliferation Treaty
  - US-Israel Relations
- A non-lethal response was necessary

What is Stuxnet?

Pretty crazy stuff

- A computer worm, at its core
- Designed to target specific hardware
- Made use of 4 separate zero-days
- Would output fake data to hide itself

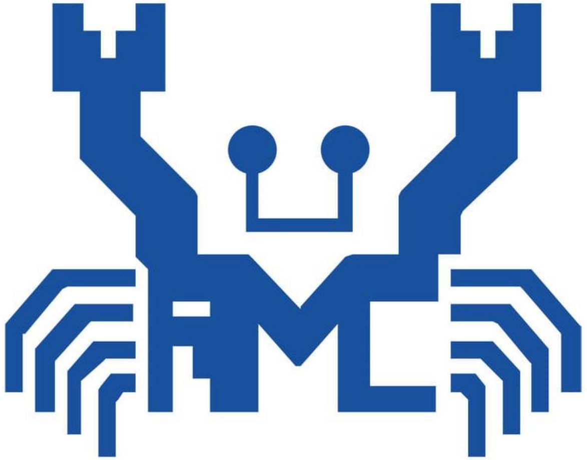


Operation Olympic Games

Also known as “Lets make Stuxnet lol”

Point of Entry

- Natanz was airgapped
- USBs plugged in by double agent
- Appeared genuine to the system



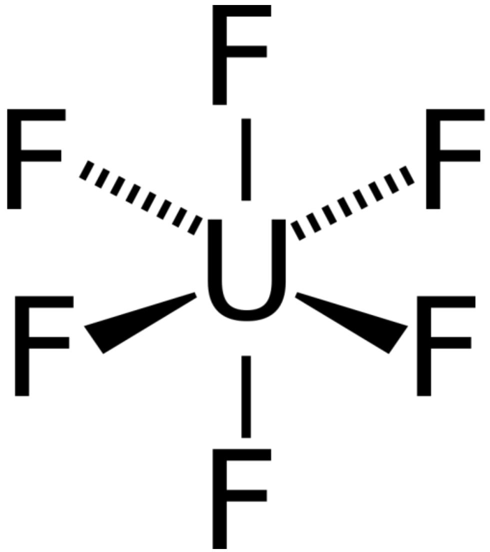
Once it’s in, now what?

- First, it tries to get itself to run…
- Then, it tries to PrivEsc…
- Then, it hides itself…
- Then finally, command and control.

HAHAHAHA HACKED!!!
You plugged this USB into the Iranian nuclear facility!!!! Love Timmy x

This is where the fun begins

- Then it just… goes to sleep
- Then things start getting a little strange
  - Unsafe RPM
  - Normal data replay
  - Gas pressure increase (time to rock)



Imagine for a second…

…You were a scientist at Natanz

- Everything looks normal?
- Centrifuges start breaking
- Uranium yield is plummeting
- What would you do?

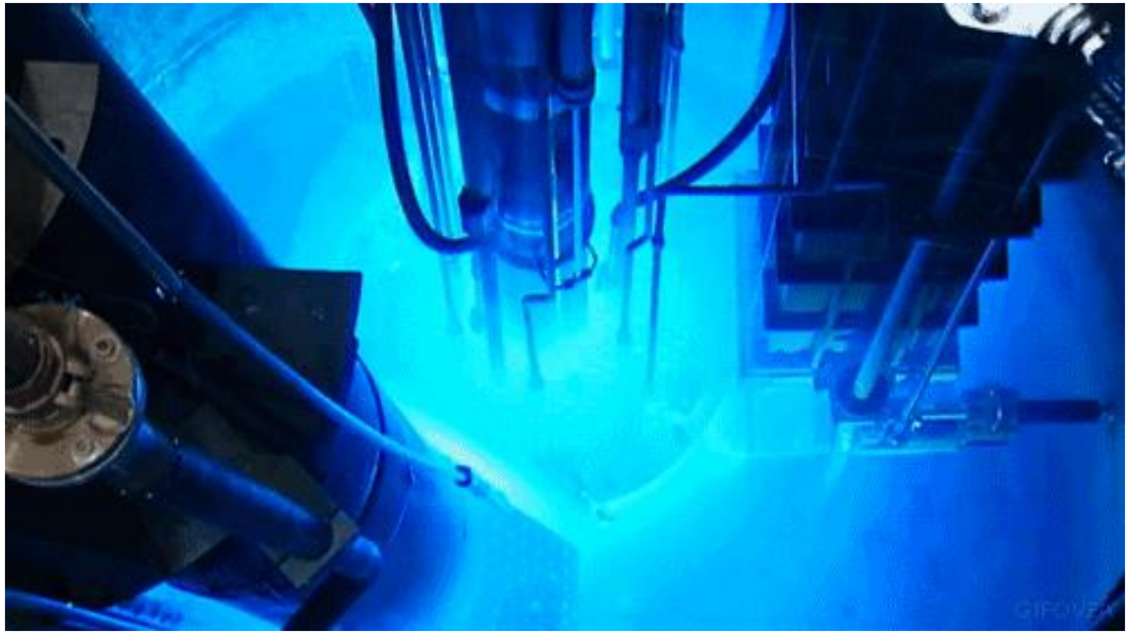
…You were an NSA spook (ALLEGEDLY) making the worm

The amount of work is insane

What happened next?

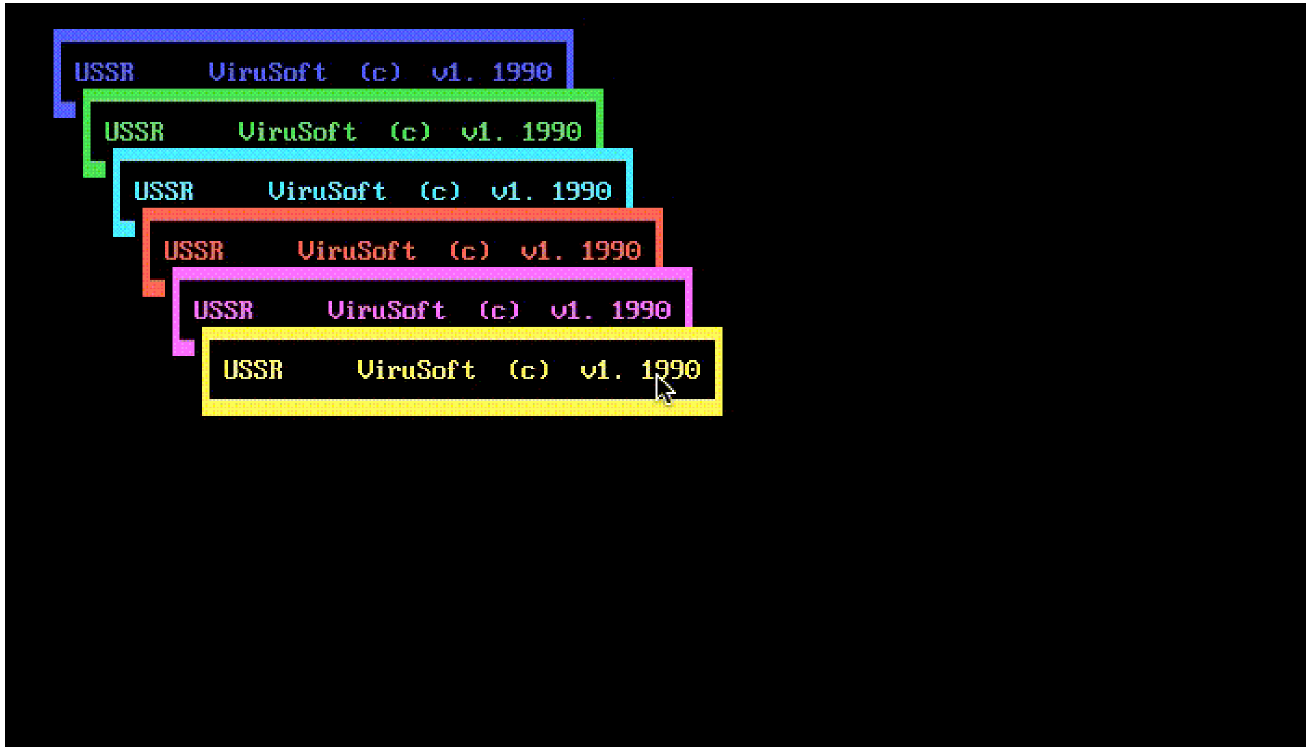
Politically

- Iran strengthened their cyber capabilities
- Iran Nuclear Deal



Technically

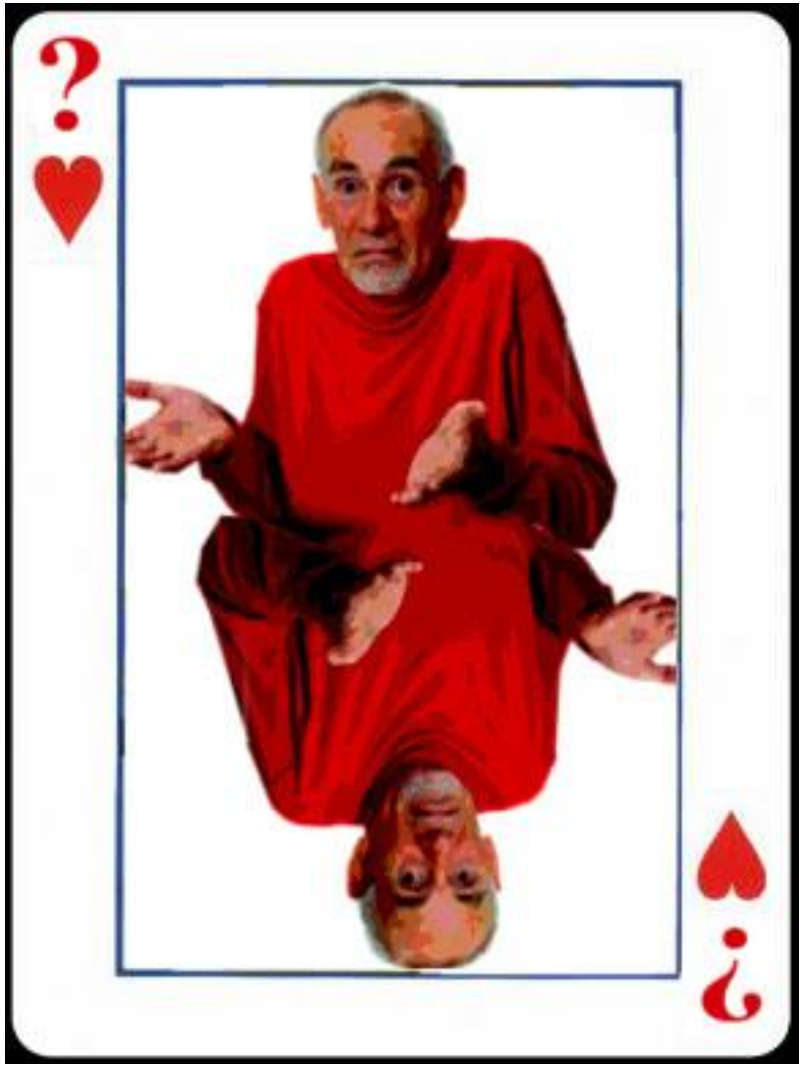
- Other Malware
  - Duqu
  - Flame
  - Havex
  - Industroyer
  - Triton



```
USSR     ViruSoft  (c)  v1. 1990
USSR     ViruSoft  (c)  v1. 1990
USSR     ViruSoft  (c)  v1. 1990
USSR     ViruSoft  (c)  v1. 1990
USSR     ViruSoft  (c)  v1. 1990
USSR     ViruSoft  (c)  v1. 1990
```

How’d it get out?

- Worker took their laptop home
- It was leaked (unknown who leaked it)
- IDF Retirement Party



Discovery and disclosure

- Reports of arbitrary BSODs
- Investigations continued for many days until they finally cracked it
- They published, and the rest is history
- Heavily recommend this article: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

Thank you for listening :)