What is an 0day (zero day) exploit?

- A bug that creates a hole that allows for a virus to write and run code within a computer or device. A rare security flaw that is unfixable.

How many 0days did Stuxnet have?

- 4.

What is SCADA?

- Technology that is controlling automation such as robots.

What is a PLC?

- Programmable logic controllers. Used to convert code to actions.

What was Stuxnet designed to do?

- Target Iranian centrifuges inside of Natanz Uranium Enrichment.

How exactly did Stuxnet work?

- Stuxnet attacked the centrifuges inside Natanz and instructed the PLC to increase or decrease the Hertz of the centrifuges. This increase or decrease would essentially destroy the equipment and in turn slow the production of enriched uranium.

How did Stuxnet hide itself?

- Stuxnet would record 30 days of normal activity and would then report that duplicate data while the virus was alternatively altering the speed at which the centrifuges were spinning.

How was Stuxnet unstoppable?

- Stuxnet hijacked the abort code that the operator had carried out and ignored it.

What does it mean when a network is ‘air-gapped’?

- The network is not connected to the World Wide Web or Internet.

How did Stuxnet jump the ‘air-gap’?

- Travelling on a USB stick and was plugged into a computer at Natanz.

What happened to the Natanz nuclear facility?

- Natanz was shut down by the Irani president and Israel was blamed for creating the virus.

Is the Stuxnet malicious code still a threat?

- Yes. Although we can recognize it after it has taken effect and take action to prevent it we are still at risk and as we continue to become more connected we are continually at risk from both Stuxnet and the viruses that other countries will now create.