Case Study - Stuxnet Worm

AUBURN UNIVERSITY

CPSC 4970 Applied Cyber Security

Stuxnet Worm Target

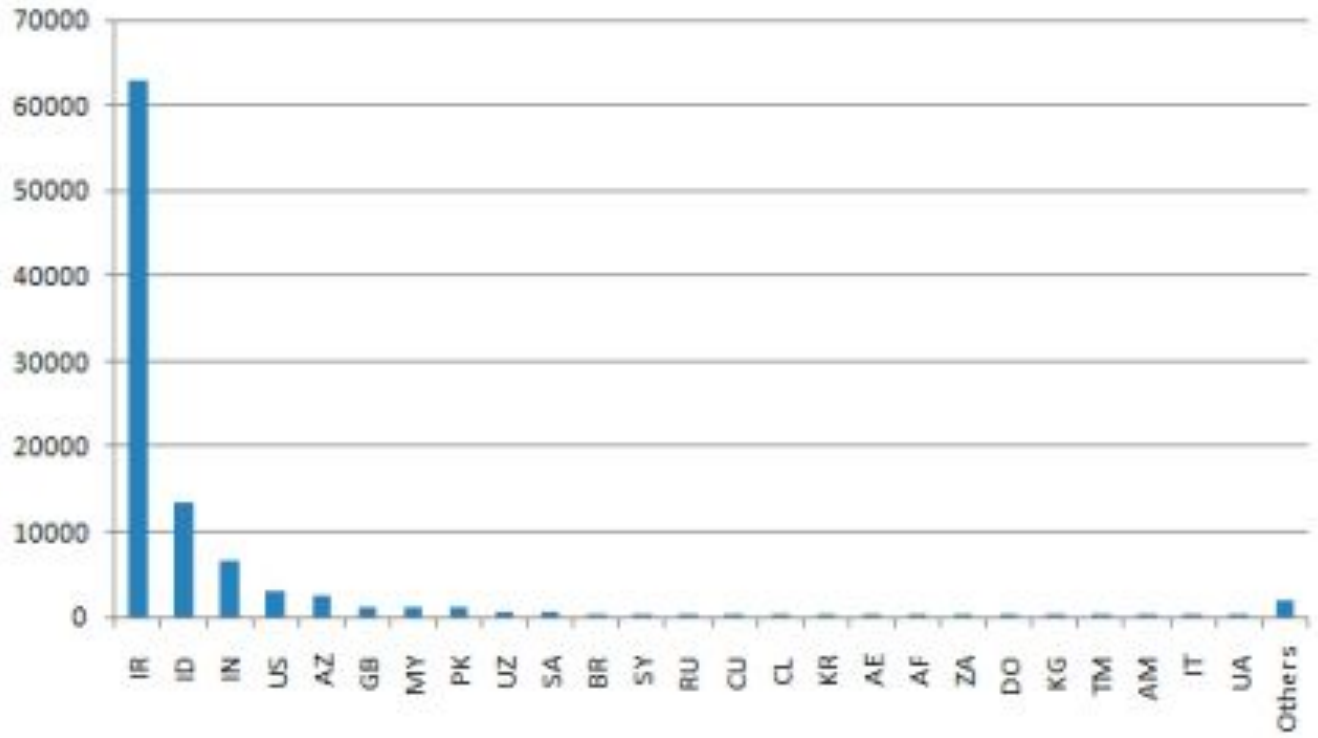
AUBURN

- The STUXNET worm is computer malware released in 2010
  - Designed to target Siemens industrial control systems
  - Designed to affect Siemens SCADA systems and PLC controllers centrifuges
  - Very specific targeting – only aimed at Siemens controllers for this type of equipment
  - It can spread to but does not damage other control systems
- Systems specifically used in Iran for uranium enrichment with the potential to make nuclear bombs
- Objective to damage or destroy controlled equipment
- Stuxnet was a malware type attack
  - Can infect a computer- based system and autonomously spread to other systems without user intervention
  - Unlike a virus, no need for a carrier or explicit user actions to spread the worm

Stuxnet Infection

AUBURN

- Sept 29, 2010 - Infected Hosts by country



Centrifuges

AUBURN

Stuxnet in Operation

AUBURN

- Takes over operation of the centrifuge from the SCADA controller
- Sends control signals to PLCs managing the equipment
- Causes the spin speed of the centrifuges to vary wildly, very quickly, causing extreme vibrations and consequent damage
  - Shaking occurs as they passes through naturally resonant frequencies
  - Youtube video demonstration
- Blocks signals and alarms to control centre from local PLCs

Stuxnet Attack

AUBURN

- Initially targets Windows systems used to configure the SCADA system
- Uses four different vulnerabilities to affect systems
  - Three of these were previously unknown - “Zero Day”
  - So if it encounters some systems where some vulnerabilities have been fixed, it still has the potential to infect them.
  - Spread can’t be stopped by fixing a single vulnerability
- Uses a vulnerability in the print system to spread from one machine to another
- Uses peer-to-peer transfer – there is no need for systems to be connected to the Internet
- Centrifuge control systems were not connected to the internet
  - Initial infection thought to be through infected USB drives taken into plant by unwitting system operators
  - USB sticks dropped on ground around buildings
    - Beware of freebies!
  - Exploited windows auto run feature on USB sticks or specific types of files.

Stuxnet Damage

AUBURN

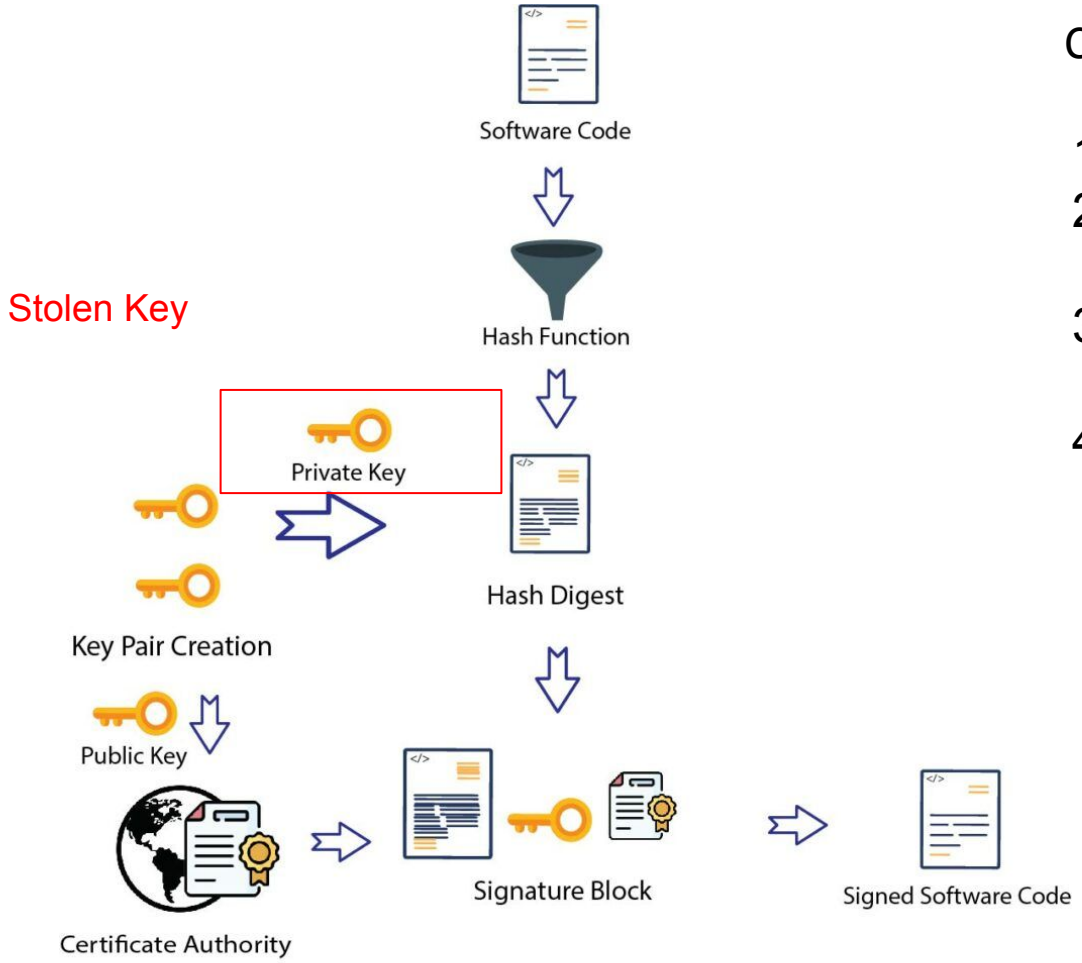
- It is thought that between 900 and 1000 centrifuges were destroyed by the actions of Stuxnet
- This is about 10% of the total so, if the intention was to destroy all centrifuges, then it was not successful
- Significant slowdown in nuclear enrichment programme because of
  - Damage to centrifuges as a result of spinning too fast for to long
  - Enrichment shutdown while the worms were cleared from equipment

How did Stuxnet get by Windows software protection?

AUBURN

- Used a legitimate digital certificate, which cryptographically vouched for the trustworthiness of the software's publisher
- Created using a compromised digital certificate from a Taiwanese semiconductor company
  - Someone stole the digital keys from the company
- Digitally signed software is often able to bypass User Account Control and other Windows measures designed to prevent malicious code from being installed.
- Digital certificates are a “Secret” that needs to be protected.
- Results was Windows did not detect malware software being installed.

Code Signing with Digital Certificates



Code Signing

1. Hash Software Code
2. Encrypt Digest with private key
3. Create digital certificate with public key
4. Signed Software can be verified by hashing software and comparing digital signature block

AUBURN UNIVERSITY