**Stuxnet – The Most Powerful Malware**

**Report by – Harsh Sharma**

**What is Stuxnet?**

It was coming into light in 2010 at security firm in Belarus when it malfunctioned the uranium enrichment centrifuges of a nuclear plant in Iran.

We can say it as a “worm,” “trojan” or “virus” due to its nature while activated but in this report, we are going to say this is a malware which consists of all the things mentioned above. Stuxnet is one of the most complex piece of code written in Assembly, whose origin is unknown to all even after all the happenings and cyber-attacks.

Some experts say it was made jointly by NSA and Mossad to prevent Iran from proceeding its nuclear program. Some believe that it was made by someone residing with German company “Siemens.”

Stuxnet was made specially for an ICS made by Siemens to control the functioning of nuclear power plant in Iran. It has ability to degrade or destroy the software which it operated. Industrial Control Systems are those which are used to control huge infrastructures like nuclear plants, dams, electricity grids etc. If this malware is successfully applied to a software, then it could result in manipulations and control to system which results in inoperability, unavailability, and long-term damage in the systems. It hideously identifies the control equipment and exploit it that controls a nation’s critical infrastructure. The main aim of Stuxnet was to make processes slower than normal and degrading the physical equipment’s at Natanz nuclear uranium enrichment centrifuges.

Stuxnet is a generic malware, it does not have to do with specific technology. Stuxnet can work on anything like power plants and dams. It just needs the right configuration to work on otherwise it will not work. Making it one of the malwares which can produce mass destruction only by tickling with Industrial Control Systems (ICS). Being a worm Stuxnet can spread through the networks and make them inoperable.

Trivia : The original name of Stuxnet was "The bug".

**How Stuxnet made problems in the Natanz Nuclear Plant**

As we all know a malware needs to get activated by a user input. As in the case of Stuxnet it was injected in the ICS operator software which was used by operators at the faculty. Stuxnet was not directly injected in the ICS as the ICS was not running on the windows. So, it was injected in the windows operator.

The malware attacks and disrupts a Microsoft Windows based Applications that is employed by a particular ICS produced by a German company “Siemens.”

Stuxnet has 2 parts:

* Malware Dropper
* Payload

Malware Dropper i.e., the malware injected in the windows pc as the malware was the windows file.

Payload i.e., the code which manipulated the controllers of the gray box on which centrifuges were connected.

As the Stuxnet needs to run on the right configuration, the code was written in such a way that it will only run on the right equipment with the right settings and parameters. The code consists of System function calls, timers, data structures.

Stuxnet malfunctioned the rotor of the centrifuges. As the malware was specially designed to sabotage the Natanz nuclear plant all the array data structures had the same values of IR-1 centrifuge cascade shapes had. There were Six IR-1 cascades. Stuxnet was hideous so it does not come to light when it was working behind as it was injected in the centrifuges with the help of sensors like pressure sensors, heat sensors of the centrifuges.

**Working of Stuxnet**

The worm can spread through the air-gapped networks by a removable device such as thumb drives and possibly through computers connected with internet.

Air gaps networks: Air gap networks are used to maintain security. It is a security measure on or more computers to make sure that a secure computer is separated from unsecured networks such as public internet or unsecured local network.

**Numbers affected by Stuxnet**

It ruined almost 1/5th of the nuclear plant centrifuges. Targeting ICS, the malware affected over 20,000 computers and 900 centrifuges.

**Who injected Stuxnet in the Nuclear Plant?**

An Iranian engineer recruited from Netherlands planted the Stuxnet virus at Iranian Nuclear Research Centre in 2007 sabotaging uranium enrichment centrifuges in what is widely regarded as the first major use of cyber weapons.

**Conclusion**

Stuxnet is one of the most powerful malwares ever made in the era of cyber security. No one knows its origin which makes it more anonymous and mysterious. Being written in Assembly language its speed of execution and spreading is fast. The malware is generic and can be used to attack Power grids, dams and other big infrastructures connected with ICS.

To get activated "the bug" at Nuclear plant requires:

* The location was Iran
* The PLC’s and equipment’s information were correct.
* Alter the PLC’s behaviour but show that everything is correct.