Stuxnet - A new Cyberwar weapon

1. Abstract

With the advancement in modern technology, we can see a lot of changes in day to day life. The affect of such technologies can also be seen in the art of warfare where various countries (ethically or non ethically) is use softwares as weapon. It is beyond the imagination of common man that how a software can be powerful enough to destroy a nation. This essay is about one such lethal software virus called "Stuxnet" which posed as a challenging issue for the politics, defense and technology fields.

2. Technical Overview of Stuxnet

The existence of such deadly virus which is powerful enough to destroy a nuclear centrifuge was discovered in June 2010. It is basically a 500KB computer worm which infected many industrial plants in Iran including the Uranium enrichment plant. The virus was designed in a way such that it can spread rapidly from one computer through other with or without the Internet unlike the normal computer viruses. Stuxnet was crafted in such a way that it is quite impossible to predict and stop. StuxNet stealthily spreads between the computers running on windows even without Internet connection, through USB drives. Since it is much unsuspected that anyone could spread a worm in this way, it was unpredictable till the actual damages were reported.

The virus becomes functional in three different stages:
1. First : It targets the loopholes in windows (operating system) machines and networks and quickly replicates itself in a deeper(Penetrating deep into the system) and broader(targeting as many as such vulnerable systems) manner.

2. Second : Then it penetrated into the Siemens step7 software (which again is a windows based software), which is used to program industrial control systems.

3. Third: It compromises the logic controllers which give the creators of the virus the access to spy on industrial systems and also they get to control the whole system.

More technically speaking the careful evaluation of this weapon in the cyber-terrorism world, it exploits five different vulnerabilities [2] : LNK (MS10-046), Print Spooler (MS10-061), Server Service (MS08-067), Privilege escalation via Keyboard layout file, Privilege escalation via Task Scheduler.

3. Who are behind the scenes?

The authors of Stuxnet have not been identified officially [1]. But looking at the code size, complexity and the development efforts that has been put up build this lethal weapon, it is quite evident that it is impossible without the help of sponsorship of a nation-state. Though no one has officially come forward to claim the ownership responsibilities, many reliable sources strongly believe that it is a joint effort by United States of America and Israel.

3.1 Involvement of Israel:

Stuxnet sets a Registry key with a value "19790509" as an infection marker. The significance of this number was unknown until F-Secure Labs, Finland [3] which is one of the best malware security experts revealed the possibility that, it is a date - 9th of May, 1979. When the experts look back into history of all the countries in relation to Iran, it points to a date on which a Jewish-Iranian businessman called Habib Elghanian was executed in Iran. He was accused to be spying for Israel. There is a reference to "Myrtus" in the malware code, which might refer to myrtle plant or Hadassah in Hebrew. In reality the name Hadassah was the borth name of the former Jewish queen of Persia - Queen Esther. It's an artifact left inside the program when it was compiled. Basically this tells us where the author stored the source code in his system. The specific path in Stuxnet is: \myrtus\src\objfre_w2k_x86\i386\guava.pdb. such artifacts are seen in other malwares as well (for example, the Operation Aurora attack against Google was named Aurora after this path was found inside one of the binaries: Aurora_Src\AuroraVNC\Avc\Release\AVC.pdb). [4]

United States Cyber-Consequences Unit (US-CCU) suggested that Israel might prefer to mount a cyber-attack rather than a military strike on Iran's nuclear facilities. This makes sense because Israel is a very small country in terms of human resources and any other natural resources in comparison with Iran, but they are much ahead than any other country in terms of technical advancement. So it is obvious that they can fight with the enemy country using a cyber weapon which costs less monetary and resource loss. According to many media and government agencies, there are strong proofs about involvement of Israel in the injection of Stuxnet in Iranian territory. Meir Daga, the head of Mossads, the National Intelligence agency of Israel, extended his service in 2009 with a justification about the involvement in some important projects. Also it was predicted by the Israeli intelligence team that Iran will have a brutal nuclear weapon in 2014-2015, which is three years later than the earlier predictions.

3.2 Involvement of America:

It is believed that America started involving [5] in the Stuxnet project since the administration of President Bush and it accelerated in the time of barrack Obama. Some of the reliable wikileaks's sources disclose the interest of United states in Iran's nuclear power plants through covert sabotages. A published article in a well known national journal about cyberstike on centrifuges by John Bumgarner, who affiliates to US-CCU, suggests in that article about the cyber attack can be possible against nations which are operating Uranium Enrichment programs. He also claimed in this article that the centrifuges used to process fuel for nuclear weapons are a key target for cyber-war operations and that they can be made to destroy themselves via malware attacks.

In April 2011, the Iranian government stated that involvement of American and Israeli co-operation in the creation and spreading of Stuxnet malware against Iran as a cyber-war weapon. The whistle blower Edward Snowden while revealing many private illegal operations by USA - especially National Security Agency, confirmed the same. There are also possibilities of involvement of Jordan, France and China, which has not yet confirmed.

4. Who are affected?

As speculated earlier, Iran is the major target for some disputes of it with Israel, and America could be backing up Israel as Uncle Sam always wants to prove it's power everywhere. Apart from Iran, knowingly or unknowingly many computer systems in other nations have been affected and are tabulated as follows [6]:

Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%

In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a “cyber Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The next month, Chevron confirmed the speculation by becoming the first U.S. Corporation to admit that Stuxnet had spread across its machines. This might possibly deny the involvement of USA in this cyberwar. According to some sources Stuxnet is the reason for sink of Deepwater Horizon and cause the Mexican oil spill. But security experts like F-Secure, Kaspersky Lab deny such possibilities.

5. Overall Impact

With the combined effort of many security experts from the software research industry and government security agencies, it is believed that Stuxnet will not cause loss of lives or resources in Iran as it will be turned towards a dead target. But because of Stuxnet many political barriers have been arose between many nations. It revealed a strong bond between Israel and USA. Also it looks like third party nations like Russia(Through funding Kaspersky Lab) by backing up Iran, clearly shows it's hatredness towards US government. Finland (F-Secure) involvement proves that Finnish government indeed tries it is best to preserve harmony and peace between all the nations. Doubts about involvement of China could be an indication that China wants to play a big role in the world politics and military by establishing it's base in many countries. Jordan and Israel being traditional enemies has definitely disturbed the political harmony with Iran. In short, it somehow reveals who could be on who's side if in case world war -3 happens.

5. Conclusion

Stuxnet has created a revolution in the field of wars as one such weapon can be used to get access to nuclear centers of other nations, hence being a most dangerous and deadly advancement in war tactics. Many peace loving countries have awakened to prevent such developments in future by taking precautionary measures. Japanese government building defensive computer viruses was inspired by the Stuxnet case studies. White hacker's community of the computer world has extended its border to many less known political powers to establish a broader and deeper contribution from people from all over the world. In summary, one such weapon which is very new and unique in Warfield could pose as a serious challenge to the political, military and technological powers of the world.

References:

[1] Kushner, David. "The Real Story of Stuxnet" ieee.org. IEEE Spectrum. Retrieved 25 March 2014.
http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/
[2] "Stuxnet Questions and Answers - F-Secure Weblog" F-Secure (Finland). 1 October 2010.
http://www.f-secure.com/weblog/archives/00002040.html
[3] " The American-made Stuxnet virus has infected the International Space Station" November 12, 2013
[4] "Falkenrath Says Stuxnet Virus May Have Origin in Israel: Video. Bloomberg Television" 24 September 2010.
[5] Reals, Tucker (24 September 2010). "Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?" CBS News.
http://www.cbsnews.com/8301-501465_162-20017507-501465.html
[6] Wikipedia entry on “Stuxnet”
http://en.wikipedia.org/wiki/Stuxnet