

[Download full-text PDF](#)[Download citation](#)[Copy link](#)[Technical Report](#) [PDF Available](#)

Stuxnet , A new Cyberwar weapon : Analysis from a technical point of view

May 2014

DOI:[10.13140/2.1.1419.5205](https://doi.org/10.13140/2.1.1419.5205)

Authors:



Siddharth Prakash Rao
Aalto University

[Citations \(4\)](#)[References \(2\)](#)

Abstract

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.

Discover the world's research

- 25+ million members
- 160+ million publication pages
- 2.3+ billion citations [Join for free](#)

[Public Full-text](#) (1)

Content uploaded by [Siddharth Prakash Rao](#) Author content
Content may be subject to copyright.

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.

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.

[Download full-text PDF](#)[Download citation](#)[Copy link](#)

Citations (4)

[References \(2\)](#)

... In January 2010, the Iranian nuclear programme was hit by the Stuxnet computer virus [25] a sophisticated cyber weapon which disabled about 96% of Iran's nuclear facility's capacity. According to the Lloyds "Business Blackout" report, the Stuxnet computer virus caused an estimated financial damage of between about US\$243 Billion in immediate and tangential economic loss, up to US\$1 Trillion [26]. ...

... Although it was sophisticated in nature, its scope was limited due to prompt isolation [27] in line with digital forensic ethics. It was widely speculated that Stuxnet was a targeted cyberwarfare against Iran as the country recorded 58.85% [25] of all infected systems globally. ...

A Review of Application Challenges of Digital Forensics

[Article](#) [Full-text available](#)

May 2020

 Kenneth Okereafor ·  Rania Djehaiche[View](#) [Show abstract](#)

... In January 2010, the Iranian nuclear programme was hit by the Stuxnet computer virus [25] a sophisticated cyber weapon which disabled about 96% of Iran's nuclear facility's capacity. According to the Lloyds "Business Blackout" report, the Stuxnet computer virus caused an estimated financial damage of between about US\$243 Billion in immediate and tangential economic loss, up to US\$1 Trillion [26]. ...

... Although it was sophisticated in nature, its scope was limited due to prompt isolation [27] in line with digital forensic ethics. It was widely speculated that Stuxnet was a targeted cyberwarfare against Iran as the country recorded 58.85% [25] of all infected systems globally. ...

A Review of Application Challenges of Digital Forensics

[Article](#)

May 2020

Kenneth Okereafor · Rania Djehaiche

[View](#) [Show abstract](#)

... Unfortunately these security methods have been found to not be enough to protect the devices as had been expected and hoped. Stuxnet was the first major attack on Smart Devices, it used the Supervisory Control and Data Acquisition (SCADA) platform to attack it's targets and is believed to have been responsible for the attack on Iran's nuclear program

[Download full-text PDF](#)[Download citation](#)[Copy link](#)

Assessment of the Impact of Cyberattacks on Power System Stability - Manipulation of Controllable Loads in Smart Homes

Thesis [Full-text available](#)

Jan 2021

 Robert Simpson

[View](#) [Show abstract](#)

... Organizations are encouraged to invest in preventive and detective control systems and other threat mitigation technologies that can anticipate, deter or halt cyberattacks proactively. The devastating impacts of Stuxnet [20] [21], WannaCry [22] [23] and NotPetya [24] [25] cyberattacks on organizations with inadequate protection are still fresh in memory. Preventive, detective and deterrent systems are very resourceful cybersecurity assets that save organizations from the following problems: ...

New Approaches to the Application of Digital Forensics in Cybersecurity: A Proposal

Article [Full-text available](#)

May 2020

 Kenneth Okereafor ·  Rania Djehaiche

[View](#) [Show abstract](#)

[Download full-text PDF](#)[Download citation](#)[Copy link](#)[Recommended publications](#) [Discover more](#)[Article](#) [Full-text available](#)

Arms Prices and Conflict Onset: Insights from Lebanon and Syria

September 2014 · European Journal on Criminal Policy and Research

 Nicolas Florquin

What drives the prices of arms and ammunition sold at illicit markets? Do the prices of illegal arms soar during episodes of marked insecurity, such as conflict onset? This article seeks to advance knowledge on the dynamics and determinants of weapons prices through the quantitative analysis of illicit arms market price data in Lebanon for the period February 2011 to September 2012. The article ... [\[Show full abstract\]](#)

[View full-text](#)

[Article](#)

The Diplomatic Presentation of the State in International Crises: Diplomatic Collaboration during th...

July 2019 · International Studies Quarterly

David E Banks

Theories of crisis (de-)escalation often focus on conflict, stress, and information problems. However, crisis (de-)escalation may sometimes hinge on how de-escalation is interpreted by domestic audiences. In this article, I combine Putnam's two-level games model of diplomacy with Erving Goffman's concepts of interaction order and face to create a mechanism I call "diplomatic presentation." I show ... [\[Show full abstract\]](#)

[Read more](#)

[Article](#)

The Iranian connection

August 2006

D.A. Fulghum · D. Barrie

The Iranian government has a cadre of hundreds of technical advisers in Lebanon that trained, and continue support, Hezbollah forces in the use of sophisticated anti-ship and anti-tank missiles and unmanned aircraft. The discovery of papers on the bodies of soldiers killed in Southern Lebanon on Aug.9 identified them as members of Iran's Revolutionary Guards. There is a possibility they could ... [\[Show full abstract\]](#)

[Read more](#)

[Article](#)

The economics of uranium enrichment in Iran

September 2016 · Physics Today

Michael Natelson

[Read more](#)

[Company](#)[Support](#)[Business solutions](#)[About us](#)[Help Center](#)[Advertising](#)

[Download full-text PDF](#)

[Download citation](#)

[Copy link](#)

