LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

IN BRIEF

# *The Stuxnet Worm: Just Another Computer Attack or a Game Changer?*

**Publication No. 2010-81-E**
**7 October 2010**

**Holly Porteous**

International Affairs, Trade and Finance Division
Parliamentary Information and Research Service

# *The Stuxnet Worm: Just Another Computer Attack or a Game Changer?*

## (In Brief)

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

*Ce document est également publié en français.*

Papers in the Library of Parliament's ***In Brief*** series provide succinct, objective and impartial overviews of current issues. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations.

Publication No. 2010-81-E
Ottawa, Canada, Library of Parliament (2010)

# CONTENTS

1 BACKGROUND ..... 1

2 HOW WAS THE ATTACKED LAUNCHED? ..... 1

3 WHO IS BEHIND THIS ATTACK? ..... 2

4 ISSUES AND IMPLICATIONS ..... 3

# THE STUXNET WORM: JUST ANOTHER COMPUTER ATTACK OR A GAME CHANGER?

## 1 BACKGROUND

In June 2010, reports surfaced that a new and highly sophisticated form of self-replicating malicious software (malware) known as the Stuxnet Worm[1] was infecting computers used to control critical industrial processes worldwide, hitting Iran particularly hard. It is believed to have been initiated through an infected USB memory stick.

Stuxnet is reported to be the first known malware to target and enable the hijacking of programmable logic controllers (PLCs).[2] PLCs are used to run a wide variety of industrial plants and factories as well as electric power plants and transmission systems worldwide.

Although systems have been infected in many countries, Stuxnet is thought to have been aimed at Iran because of the way it operates. Stuxnet seeks out Windows computers running two specific configurations of Siemens-manufactured PLC software, software which Iran uses to monitor and control processes at several key facilities, including its Bushehr nuclear power plant.[3]

However, if the intention was to cripple Iran's suspected nuclear weapons program, the country's centrifuge uranium enrichment facility at Natanz would have been a more valuable target than the light-water reactor at Bushehr. The Bushehr reactor is under tight international safeguards and produces spent fuel that is less useful for manufacturing nuclear weapons.

The Natanz facility is reported to have been subjected to previous sabotage operations.[4] One researcher who has been helping governments analyze Stuxnet suggests that an earlier version of the worm may already have been used against software controlling centrifuges at Natanz as early as July 2009.[5] Other analysts posit that the failure of this earlier Stuxnet variant to achieve its intended objective led its creators to code a new version of the worm that would spread beyond its original modest propagation limit, with the unintended consequence of broadening Stuxnet's impact well beyond Iran.[6]

## 2 HOW WAS THE ATTACKED LAUNCHED?

The reported launch of the Stuxnet attack through an infected USB memory stick echoes a method used in 2008 in the worst breach of United States Department of Defense systems to date[7] and may be why Iran has arrested an unspecified number of "nuclear spies" it accuses of cyber-attacks on its nuclear program.[8]

Delivering malware via a USB memory stick or other removable media enables an attacker to infect a computer or network that has no connection to the Internet.

Isolation from the Internet (also called “air-gapping”) is a security technique used to protect extremely sensitive systems like nuclear power plants against remote attacks.

In this instance, it appears that the use of one or more infected USB memory sticks did not achieve the attacker’s aim. The subsequent introduction of additional propagation capabilities, possibly compounded by a security lapse on the part of users on the targeted network, may have resulted in the unintentional amplification of Stuxnet beyond Iran. While the infected Iranian network may have been isolated from the Internet, it is possible that a laptop or perhaps one of the infected memory sticks used on this network was also used in a less secure network environment.

## 3 WHO IS BEHIND THIS ATTACK?

Given the absence of any reports of attempted blackmail and Stuxnet’s focus on hijacking industrial processes rather than on stealing funds or identities, most public commentators have dismissed the notion that a cyber-crime syndicate is behind the attack.[9]

Instead, the advanced capabilities of Israel and the United States in cyber-operations and concerns about Iran’s nuclear activities have led to widespread speculation in the media that one or both may have launched Stuxnet. Britain, Germany, France and even China – an important ally of Iran – have also been raised as possible culprits.[10] Others suggest that two other “cyber-powers” – India and Russia – should be considered as potential sources of the attack.

Private-sector experts who have analyzed Stuxnet believe the fingerprints of a state agency can be found in the malware’s enormous size, subtle functionality (for example, it masks changes made to the system it is attacking) and use of four “zero-day exploits.”[11] Zero-day exploits are computer codes that use previously unknown vulnerabilities in operating systems to gain unauthorized access or privilege. A great deal of time, money and leading-edge software engineering expertise is needed to create them. A zero-day exploit against closely guarded industrial software further reduces the likelihood of the Stuxnet attack being the work of amateur hackers.

On the other hand, given the demonstrated sophistication of cyber-crime syndicates and a lack of publicly available information on Stuxnet’s ultimate objectives, the possibility that this worm’s release was intended as a prelude to large-scale blackmail cannot be ruled out entirely.

However, if a nation-state was behind this attack, the processes underlying the preparation and execution of the attack are of interest. Was this an intelligence-led or a military-led undertaking? This question actually points to a legal distinction which is being established between the “exploitation” and the “attack” of a computer network, the first denoting a form of intelligence-gathering and the second a form of military operation.

Computer network *exploitation* aims to gain unauthorized access to a system, making it an important tool for intelligence agencies to surreptitiously collect information stored on foreign systems and networks. Computer network *attacks* seek

to alter data once authorized access has been gained, thereby causing some form of harm. Exploitation is the more challenging of these two undertakings, and intelligence agencies, particularly those focusing on signals intelligence collection, have developed a core expertise in this area.

In the case at hand, while a civilian signals intelligence agency may have developed Stuxnet, depending perhaps on the state involved, military personnel might have had overall responsibility for the operation.[12]

## 4 ISSUES AND IMPLICATIONS

Regardless of its origin and ultimate goal, the Stuxnet attack raises a number of issues and has several implications, including the following:

- Stuxnet demonstrates the potential for well-resourced cyber-attacks to damage or destroy critical infrastructures.
- Though Stuxnet shows hallmarks of nation-state involvement – meaning the attack was assisted, if not led, by a government intelligence agency – such involvement is unlikely to ever be publicly confirmed.
- Cyber-threats such as Stuxnet that target critical infrastructures, which are primarily private-sector operated, present challenges to wired democracies like Canada and its allies, challenges that are only magnified by the speed with which previously unknown threats can materialize.
    - First, wired and open societies are target-rich environments for cyber-theft, espionage or attack, against which they must protect themselves.
    - Second, because they know so much about how to exploit vulnerabilities in computer networks, intelligence agencies represent the best early warning and defensive capability of these societies. This, however, creates challenges in respect of privacy rights protection, information sharing, and liability. These challenges are only magnified by the need for near-automated response to suddenly emerging and dangerous threats such as Stuxnet.
- The United States, Britain and NATO have highlighted Stuxnet as further reason to develop international legal frameworks addressing this type of threat. In its recently released cyber-security strategy, Canada also emphasizes the need for international cooperation and legislation in this area.[13]

---

### NOTES

1. Worms are distinguished from viruses in that, once initiated, they are self-replicating.
2. The most detailed publicly available technical examination of Stuxnet to date has been performed by US-based Symantec Corporation. See Nicolas Falliere, "Exploring Stuxnet's Infection Process," *Symantec Security Connect*, 21 September 2010; Nicolas Falliere, Liam O'Murchu, and Eric Chien, "W32 Stuxnet Dossier," *Symantec Security Response*; Public Safety Canada, Canadian Computer Incident Response Centre, *Siemens SIMATIC "WinCC" or Siemens "Step 7" software vulnerabilities*, AV10-023,

27 July 2010; and Thomas Erdbrink and Ellen Nakishima, "Iran struggling to contain 'foreign-made' 'Stuxnet' computer virus," *Washington Post*, 27 September 2010.

3. According to the above-cited Symantec study, some 60% of systems infected by the worm were located in Iran. See William Maclean, "Cyber attack appears to target Iran-tech firms," *Reuters*, 24 September 2010. Though they admitted that tens of thousands of personal computers had been infected by Stuxnet, including personal computers owned by employees at Bushehr, Iranian officials publicly denied that the worm had caused delays or damage. See Erdbrink and Nakishima (2010).

4. For example, in his book on the A.Q. Khan proliferation network, David Albright discusses a US clandestine program to introduce faulty centrifuges into the network's smuggling operation to Iran. See David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*, New York, Free Press, 2010; Eli Lake, "Operation Sabotage," *The New Republic*, 14 July 2010.

5. To read further on the Bushehr versus Natanz debate, see Mark Clayton, "Stuxnet worm mystery: What's the cyber weapon after?," *Christian Science Monitor*, 24 September 2010.

6. Once Stuxnet infects a computer, it can communicate with other infected "peers" and be updated remotely. See Gregg Keizer, "Why did Stuxnet worm spread?," *Computer World*, 1 October 2010.

7. Ellen Nakishima, "Defense official discloses cyberattack," *Washington Post*, 24 August 2010.

8. "Iran arrests 'nuclear spies' accused of cyber attacks," *BBC News*, 2 October 2010.

9. For example, well-known US security commentator Bruce Schneier dismissed the notion of criminal origins, saying "Stuxnet doesn't act like a criminal worm. It doesn't spread indiscriminately. It doesn't steal credit card information or account login credentials. It doesn't herd infected computers into a botnet. It uses multiple zero-day vulnerabilities. A criminal group would be smarter to create different worm variants and use one in each. Stuxnet performs sabotage. It doesn't threaten sabotage, like a criminal organization intent on extortion might." See Bruce Schneier, "The Story Behind the Stuxnet Virus," *Forbes*, 6 October 2010.

10. David Sanger, "Iran Fights Malware Attacking Computers," *New York Times*, 25 September 2010.

11. Beyond the Symantec study, Microsoft (see Microsoft Malware Protection Center, *Malware Encyclopaedia*, "Stuxnet") and individuals with expertise in industrial control systems such as Hamburg-based Ralph Langner (see Langner Communications GmbH) are among those who have provided technical analysis of Stuxnet.

12. For more on the relationship between cybersecurity and signals intelligence, see Holly Porteous, *Cybersecurity and Intelligence: The US Approach*, Publication no. 2010-02-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 8 February 2010.

13. See Public Safety Canada, *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*, 3 October 2010.