



Open in app

Get started



Published in DataSeries



Bishr Tabbaa

Follow

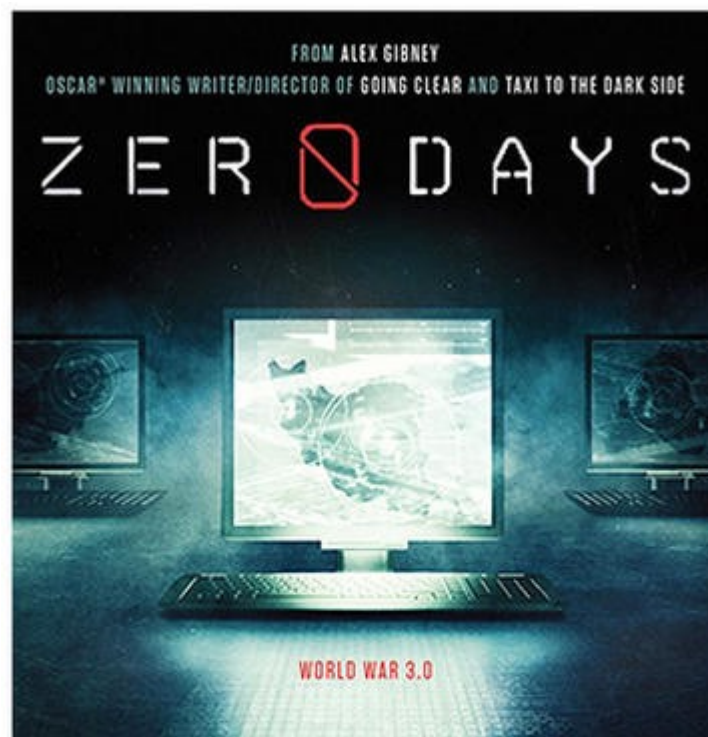
Jul 16, 2020 · 12 min read · [Listen](#)



Save



Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security



Continue to Medium



Sign up

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

principles and practices for solution delivery in the IT industry. In this blog and my forthcoming book, **Bugs: A Short History of Computer System Failure**, I will chronicle some important system failures in the past and discuss ideas for improving the future of system quality. As information technology becomes increasingly woven into society, the quality of computer hardware and software impacts our commerce, health, infrastructure, military, politics, science, security and transportation. The Big Idea is that we have no choice but to get better at delivering technology solutions because our lives depend on it.

On July 16, 2010, Microsoft, MITRE, and others published security advisories about the **Stuxnet** malware which targeted **Microsoft Windows** machines running **Siemens SIMATIC Step7** software for managing Programmable Logic Controllers (PLC) that automated, monitored, and operated physical assets including amusement parks, building alarms, chemical plants, energy pipelines, factory assembly lines, and nuclear power plants. Stuxnet infected more than *200,000* computers across the world including *14* industrial sites in Iran, damaged over *1,000* centrifuges in the Natanz facility that were essential to Iran's covert uranium enrichment program intended for developing nuclear weapons, and constituted an innovative inflection point in computer security that showed how serious the cyber threat was to physical infrastructure connected to the digital world. Stuxnet exploited several 0-day security vulnerabilities in Windows and Siemens software to propagate and control Windows hosts and the PLCs that were its ultimate target; technical analysis by several security experts including Symantec, Kaspersky Lab, Ralph Langner, and others suggested that the virus author was a nation state since only they would have the motive, opportunity, and means to execute such a sophisticated attack. This essay will explore the historical context of Stuxnet, the virus technology, as well as its implications for our modern society.

Continue to Medium

[Sign up](#)[Already have an account? Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

Satellite of Natanz facility in Iran (Source: Wired.com)

An abbreviated historical timeline of the relationship between Iran, US, and Israel as well as the Stuxnet virus follows:

- 1950s — US launches nuclear power program known as Atoms for Peace (AFP) under Dwight Eisenhower.
- 1953 — US CIA overthrows Iran's President Mohammed Mossadegh and brings Shah Reza Pahlavi to power.

Continue to Medium



[Sign up](#)

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

- 1979 — Islamic revolution overthrows Shah of Iran, and Ayatollah Khomeini replaces Shah as leader.
- 1995 — Iran signs agreement with Russia to complete power plant in Bushehr.
- 2002 — Dissident group reveals existence of uranium enrichment facility in Natanz.
- 2006 — US and Israel launch Operation Olympic Games to disrupt Iran's nuclear weapons program.
- June 2008 — Siemens cooperates with the US Idaho National Laboratory and Department of Energy to research computer security vulnerabilities in its PLC systems used to operate nuclear energy facilities. Siemens shares its source code with US authorities.
- 2008–2009 — Stuxnet is under development.
- December 2008 — Stuxnet domain (mypremierfutbol.com) is registered.
- June 22 2009 — Stuxnet v1 is deployed with moderate infections.
- March 2010 — Stuxnet v2 is deployed with USB 0-day exploit and spreads faster.
- June 17, 2010 — VirusBlokAda in Belarus discovers Stuxnet when it is contacted by an Iranian customer about Windows machines that were unintentionally and continuously being rebooted.
- June 24, 2010 — VirusBlokAda notified Realtek Semiconductor about theft of its digital certificate.
- Early July 2010 — VirusBlokAda contacted Microsoft about Stuxnet.

Continue to Medium

[Sign up](#)

Already have an account? [Sign in](#)

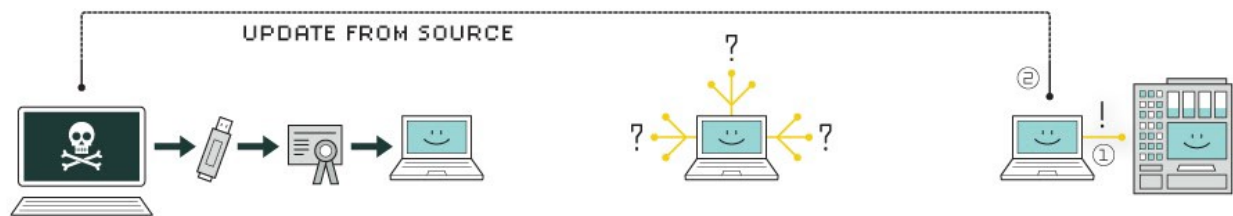
Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

- July 22, 2020 — Verisign revoked JMicro certificate.
- Nov 23, 2010 — Iran's Atomic Energy Organization Director Ali Salehi confirms that a computer virus attacked nuclear facilities in Iran.
- February 2011 — Microsoft publishes patches fixing all vulnerabilities exploited by Stuxnet.
- July 24, 2012 — Self-termination date for Stuxnet

How to Hack a Centrifuge

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the

5. control

In the beginning, Stuxnet spies on the

6. deceive and destroy

Meanwhile, it provides false feed-

Continue to Medium



[Sign up](#)

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

payload that penetrated Windows hosts, and then operated the Siemens PLCs. The worm component used several 0-day exploits to propagate the virus:

- **USB** — the virus copied itself as specially crafted .LNK files from connected USB devices onto the local computer. The .LNK files exploited a vulnerability for Microsoft Windows LNK File Execution Shortcuts (CVE-2010–2568) that automatically executed the virus when Windows Explorer or other visual Windows tools browsed the USB device contents on the machine. Note that disabling AutoRun and AutoPlay for USB devices would still leave systems vulnerable to this attack. Experts believe it was an infected USB stick either given to an Iranian facility operator through social engineering or used by a double  38 |  side the facility that originally defeated the “air gap” network defense since many of the industrial sites running Siemens software including Iran’s nuclear program were *not* directly connected to the Internet.
- **Local Network** — the virus could execute and exploit specific requests that would trigger remote code execution upon the localhost by calling the Microsoft Windows Print Spooler Server (CVE-2010–2779) or Microsoft Windows RPC Server (CVE-2008–4250). It could also copy itself to network folders shared on the local computer using local users found on the local computer, Windows domain, or through WMI Explorer impersonation.
- **Siemens** — the virus searched for Siemens SIMATIC Step7 projects (.s7p files) on the infected system, if found, then it would copy itself to the folders and modify the main index files. These project folders were often manually copied between Windows machines connected to the same Siemens PLCs operating at a specific facility.

Continue to Medium

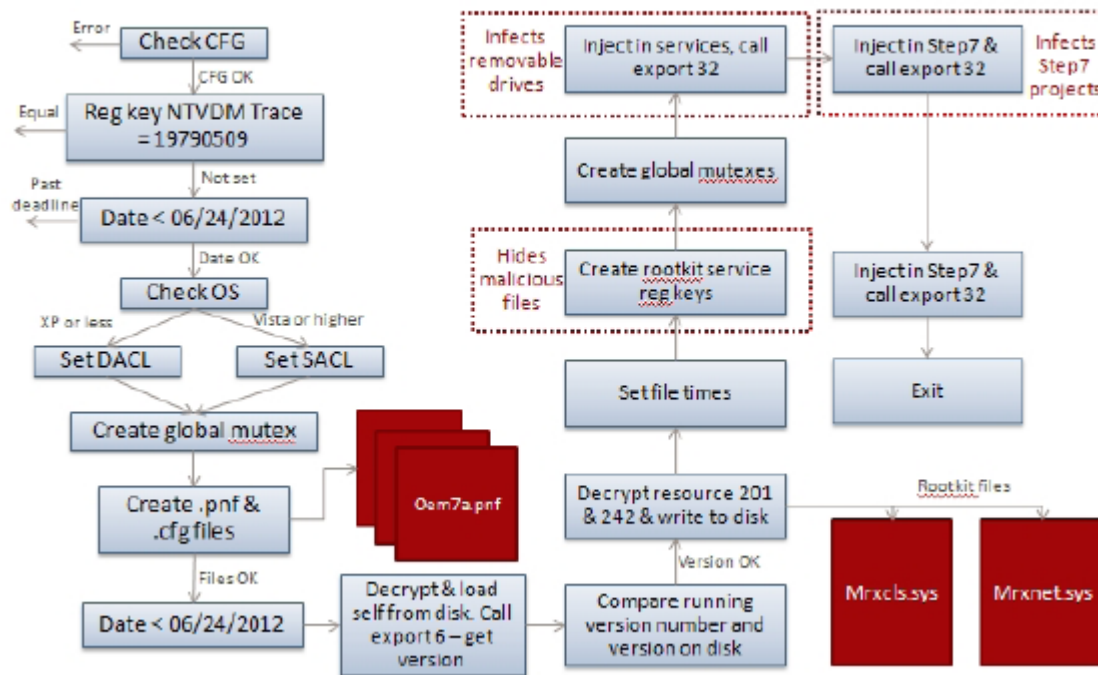
[Sign up](#)[Already have an account? Sign in](#)

Click “Sign Up” to agree to Medium’s [Terms of Service](#) and acknowledge that Medium’s [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

Figure 11

Infection routine flow



Stuxnet State Machine (Source: Symantec)

Once Stuxnet was inside a machine, it escalated its privilege from a local Administrator to SYSTEM using a 0-day exploit in the Windows Task Scheduler (CVE-2010-3888) or another in the Windows Win32 Keyboard Layout (CVE-2010-2743) and then installed a Windows rootkit as hardware driver-level modules (mrxnet.sys, mrxcls.sys) hidden behind a stolen digital certificate (initially from Realtek, then later JMicro) to pose as legitimate software and evade detection by traditional anti-virus software based on electronic signatures. After driver installation, the virus sets Windows registry entries (HKLM\System\CurrentControlSet\Services\MRXCLS and MRXNET) so that the two drivers are started as system services. Stuxnet then starts its own Remote Procedure Call (RPC) server and listens for incoming connections from other infected machine peers on the same local network. The RPC server has a fixed GUID that allows Stuxnet peers to

Continue to Medium

[Sign up](#)

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

Windows kernel's NTDLL.DLL, intercepting commands, and injecting code into already running trusted OS processes such as lsass.exe, svchosts.exe, and services.exe as well as security programs such as avp.exe (Kaspersky), mcshield.exe (McAfee), rtvscan.exe (Symantec), and others.

Once Stuxnet is installed as a service on the computer, it searches on the local computer for the Siemens SIMATIC Step7 software by looking in the Windows system folder for the file S7OTBXDX.DLL. Once found, it renames the file to S7OTBXSX.DLL and then replaces it with a modified version that has the same DLL exports as the original but with code modifications for more than a dozen critical functions related to access, read, write, and deletion of code blocks on the PLC. Stuxnet will execute additional instructions before calling the true functions contained in the original S7OTBXSX.DLL and by modifying data sent to or received from the PLC can also act as a Man-in-the-Middle attack. Note that if Siemens Step7 is not found, the Stuxnet does not perform further malicious actions on the computer host.

Stuxnet tries to contact a remote web server to test Internet connectivity using the following non-malicious URLs (windowsupdate.com or msn.com). If that works, then it connects to the following URLs to send and receive commands from a remote user (mypremierfutbol.com, todaysfutbol.com). It then generates the following URL and posts a message to the server: <http://www.mypremierfutbol.com/index.php?data={data}> where data is a XOR-encrypted hexadecimal value that contains the IP address, computer name, domain, OS version, and whether WinCC Step7 is installed or not. The server may reply to the infected machine by sending arbitrary code to be executed (likely updated version of the malware payload or some data exfiltration commands).

Finally, once all installation and setup operations are done, if the Siemens software was

Continue to Medium

[Sign up](#)

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

configuration data in the PLC, and it begins intercepting commands, altering their operation. Roughly every 30 days, Stuxnet then changes the output frequency of the converters for short periods of 15–50 minutes to either 1410 Hz or 2Hz respectively, then back to 1064 Hz (a normal frequency). Periodic modification of the output frequency sabotages the automation system, introducing mechanical stress to the centrifuges thereby increasing the likelihood for failure and reducing the quality of the processed uranium. Furthermore, Stuxnet replayed old, normal values to the visual SCADA components of the Simatic system so that operators would not suspect a problem much like criminals play an old videotape back to the guards during a typical bank heist movie plot.

Table 3

DLL Exports

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls Export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstalls Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection

Continue to Medium

[Sign up](#)[Already have an account? Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

Path\File	Size	Function
~wtr4132.tmp	513536	Dropper (all malware resources)
~wtr4141.tmp	25720	User-mode rootkit
%windir%\system32\drivers\mrxcbs.sys	26716	Kernel-mode loader
%windir%\system32\drivers\mrxcnet.sys	17400	Kernel-mode rootkit
%windir%\inf\mdmcpq3.pnf	variable	Configuration data
%windir%\inf\mdmceric3.inf	90	Configuration data
%windir%\inf\oem6c.pnf	323848	Log file (encrypted, log ops, infected files, etc)
%windir%\inf\oem7a.pnf	498176	Main payload (encrypted DLL)
%windir%\system32\s7otbxdx.dll	29800	Simatic Manager DLL replacement

Stuxnet Files (Source: Symantec)

The World is Not Enough

The Stuxnet code sophistication (multiple 0-day vulnerabilities, code obfuscation, code injection, modular design, remote command-and-control as well as peer-to-peer updating, all-in-1-payload), its fraudulent digital certificates, and the dogged patience of the cyberattack (taking place over months instead of minutes) all suggested that the Stuxnet author was a nation-state with comprehensive knowledge of cybersecurity and nuclear power plants. Several other coincidental facts also pointed to government actors or perhaps someone interested in framing one government for the actions of another. First, according to Symantec's analysis of the first 38,000 infected IP addresses, 22,000 were

Continue to Medium

[Sign up](#)

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

9, 1979 was the date the Iranian government executed Habib Elghanian by firing squad; Elghanian was Iranian of Jewish descent, and his death triggered the exodus of many Jews from Iran. The registry key value served as an inoculation marker on a machine that it had already been infected, and the virus would terminate its installation on that machine if it found the value in the registry. Third, buried in the main worm dropper was a compiled file reference to `b:\myrtus\src\objfre_w2k_x86\386\guava.pdb`. Although myrtus is a biological genus that contains the guava fruit, it also obliquely points to Queen Esther who saved the Jews from the Persians in the 4th century BC; Esther's Hebrew name was Hadassah which refers to the myrtle plant. The consensus estimate from experts at Symantec, Kaspersky Lab, and Langner was that Stuxnet was expensive to build. The virus software likely took 5–10 people six months to write using mostly C and C++ along with some SQL; setting up the laboratory for integrating the computers and the nuclear centrifuges to simulate and test would have taken additional time, money, and resources that most organizations do not possess. Finally, the attackers leveraged this digital weapon along with classical intelligence (e.g. on-site operatives or social engineering to influence said personnel) in a manner that again goes beyond what most cybercriminal organizations are capable of.

Stuxnet redefined what computer malware could do in terms of methods used and damage inflicted. It opened the digital door to further cyber warfare attacks on physical infrastructure. According to sources such as the Institute for Science and International Security and International Atomic Energy Agency, Stuxnet damaged about 1000 IR-1 centrifuges in the uranium fuel enrichment facility in Natanz, and it set back the Iranian nuclear program by one year. Malware authors also learn from each other. Since Stuxnet, there have been several descendants inspired by its engineering. Duqu in 2011 logged keystrokes and mined data from industrial facilities. Flame in 2012 also traveled via USB sticks and was a comprehensive spyware that logged keystrokes and recorded Skype

Continue to Medium

[Sign up](#)[Already have an account? Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

- Air gap defenses may not be enough.
- Removable storage media is a serious threat.
- Hard-coded default passwords are unacceptable.
- Digital certificates can be compromised and they are only as good as their verification process.

Solutions:

- Assess industrial systems that use **PLCs** for security vulnerabilities and investigate use of custom, site-specific passwords for PLC databases.
- Protect against **Insider** user threat (e.g. monitor employees and contractors in real-time using access and system logs, evaluate personnel through background checks).
- Deny any **Internet** connectivity in the Industrial Process Control network and limit PLC membership in TCP/IP networks through Network ACLs.
- Organizations need **defense-in-depth** and should use zone-based networks as described in the ANSI 99.02.01 and IEC-62443 standards. Between zones, there should be network firewalls that block the protocols that Stuxnet and viruses like it communicate with (e.g. HTTP, RPC, MSSQL). This would quarantine an infection to a small number of machines in a single zone.
- Block **external storage** devices (e.g. USB drives, contractor laptops, etc) to mind and enforce the “air gap”.
- Monitor systems and networks for **suspicious** behavior.

Continue to Medium

[Sign up](#)Already have an account? [Sign in](#)

Click “Sign Up” to agree to Medium’s [Terms of Service](#) and acknowledge that Medium’s [Privacy Policy](#) applies to you.

[Open in app](#)[Get started](#)

- Consider using **honeypots** consisting of dummy systems with fake HMI stations and PLCs to detect suspicious activity.
- Consider running **heterogeneous operating systems** such as Linux or QNX to control PLCs.

References

- <https://docs.broadcom.com/doc/stuxnet-missing-link-13-en>
- <https://ccdcoe.org/multimedia/stuxnet-facts-report-technical-and-strategic-analysis.html>
- <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>
- <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>
- <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>
- <https://www.schneier.com/blog/archives/2010/10/stuxnet.html>
- <https://archive.f-secure.com/weblog/archives/00002040.html>
- https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon

Continue to Medium

[Sign up](#)[Already have an account? Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.



Open in app

Get started



Continue to Medium



Sign up

Already have an account? [Sign in](#)

Click "Sign Up" to agree to Medium's [Terms of Service](#) and acknowledge that Medium's [Privacy Policy](#) applies to you.