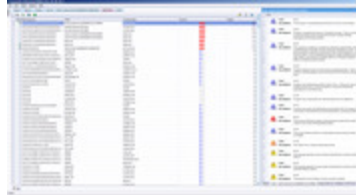


# Stuxnet code : Free Download, Borrow, and Streaming : Internet Archive

[archive.org/details/Stuxnet](http://archive.org/details/Stuxnet)



Due to a planned power outage on Friday, 1/14, between 8am-1pm PST, some services may be impacted.

The screenshot displays the Responder Professional Edition interface. The main window shows a list of digital DNA sequences with columns for Name, Process Name, Severity, and Weight. The list includes various system utilities and services like svchost.exe, lsass.exe, and explorer.exe. A detailed view of a specific trait is shown on the right, listing traits such as 89 22, 18 2A, 6E F6, A8 D5, 81 83, CA 05, DF 37, 82 46, 35 99, A7 95, 80 00, 80 02, and 80 08, each with a description of its behavior.

ddna\_panel.png

## Stuxnet code

### Usage

Public Domain Mark 1.0



## Language

English

Stuxnet is believed to be a jointly built American-Israeli cyber weapon and computer worm. These claims have never been confirmed by either nation state. According to anonymous US officials speaking to the Washington Post, the worm was developed during the administration of George W. Bush to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a rootkit component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet.

Stuxnet is typically introduced to the target environment via an infected USB flash drive. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the computer. If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

## Addeddate

2015-09-12 11:24:48

## Identifier

Stuxnet

## Identifier-ark

ark:/13960/t3hx5022b

## Scanner

Internet Archive HTML5 Uploader 1.6.3

---

## Reviews

There are no reviews yet. Be the first one to write a review.

**Add Review**

## SIMILAR ITEMS (based on metadata)

---

Terms of Service (last updated 12/31/2014)