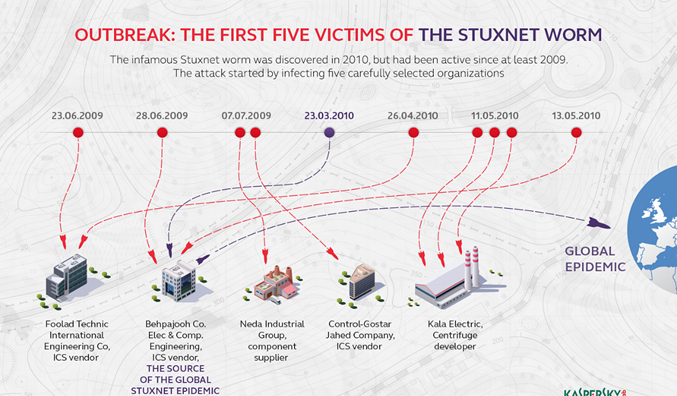
**STUXNET**

**What is Stuxnet**

Stuxnet is a powerful computer worm designed by U.S. and Israeli intelligence that to disable a key part of the Iranian nuclear program. Targeted at an air-gapped facility, it unexpectedly spread to outside computer systems, raising a number of questions about its design and purpose. Stuxnet exploited multiple previously unknown Windows [zero days](https://www.csoonline.com/article/3284084/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html). That description should probably make it clear that Stuxnet was a part of a high-level sabotage operation waged by nation-states against their adversaries.

**

**What did Stuxnet do**

Stuxnet was designed to destroy the centrifuges Iran was using to enrich uranium as part of its nuclear program. Most uranium that occurs in nature is the isotope U-238; however, the fissile material used in a nuclear power plant or weapon needs to be made from the slightly lighter U-235. A centrifuge is used to spin uranium fast enough to separate the different isotopes by weight via to centrifugal force. These centrifuges are extremely delicate, and it's not uncommon for them to become damaged in the course of normal operation.

When Stuxnet infects a computer, it checks to see if that computer is connected to specific models of programmable logic controllers (PLCs) manufactured by Siemens. PLCs are how computers interact with and control industrial machinery like uranium centrifuges. If no PLCs are detected, the worm does nothing; if they are, Stuxnet then alters the PLCs' programming, resulting in the centrifuges being spun irregularly, damaging or destroying them in the process. While this is happening, the PLCs tell the controller computer (incorrectly) that everything is working fine, making it difficult to detect or diagnose what's going wrong until it's too late.

## What language was Stuxnet written in

While security researchers don't have access to the Stuxnet codebase, they've been able to learn a lot by studying it, and have determined that it was [written in multiple languages](https://www.infoworld.com/article/2626009/is-stuxnet-the--best--malware-ever-.html), including C, C++, and probably several other object-oriented languages. This too is unusual for malware and is a sign of the level of sophistication involved in its creation.

## What vulnerability did Stuxnet exploit

In order to infect the Windows PCs in the Natanz facility, Stuxnet exploited [no fewer than four zero-day bugs](https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/) a Windows Shortcut flaw, a bug in the print spooler, and two escalation of privilege vulnerabilities along with a zero-day flaw in the Siemens PLCs and an old hole already used in the [Conifer](https://www.csoonline.com/article/2633232/conficker-malware-ups-the-ante.html) attack. The sheer number of vulnerabilities exploited is unusual, as typically zero-days are quickly patched in the wake of an attack and so a hacker won't want to reveal so many in a single attack.

## Who created Stuxnet

It's now widely accepted that Stuxnet was created by the intelligence agencies of the United States and Israel. Stuxnet was first identified by the infosec community in 2010, but development on it probably begin in 2005. The U.S. and Israeli governments intended Stuxnet as a tool to [derail, or at least delay, the Iranian program to develop nuclear weapons](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html). The Bush and Obama administrations believed that if Iran were on the verge of developing atomic weapons, Israel would launch airstrikes against Iranian nuclear facilities in a move that could have set off a regional war. Operation Olympic Games was seen as a nonviolent alternative. Although it wasn't clear that such a cyberattack on physical infrastructure was even possible, there was a dramatic meeting in the White House Situation Room late in the Bush presidency during which pieces of a destroyed test centrifuge were spread out on a conference table. It was at that point that the U.S. gave the go-head to unleash the [malware](https://www.csoonline.com/article/3295877/malware/what-is-malware-viruses-worms-trojans-and-beyond.html).

The classified program to develop the [worm](https://www.csoonline.com/article/3429569/what-is-a-computer-worm-how-this-self-spreading-malware-wreaks-havoc.html) was given the code name "Operation [Olympic Games](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.3283038083d7)"; it was begun under President George W. Bush and continued under President Obama. While neither government has ever officially acknowledged developing Stuxnet, a 2011 video created to celebrate the retirement of Israeli Defense Forces head Gabi Ashkenazi [listed Stuxnet as one of the successes under his watch](http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html).

While the individual engineers behind Stuxnet haven't been identified, we know that they were very skilled, and that there were a lot of them. Kaspersky Lab's Roel Schouw Enberg estimated that it [took a team of ten coders two to three years](http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/) to create the worm in its final form.

Several other worms with infection capabilities similar to Stuxnet, including those dubbed [Duque](https://www.csoonline.com/article/2130209/faq--what-s-the-big-deal-about-duqu-.html) and [Flame](https://www.csoonline.com/article/2131774/malware-cybercrime-researchers-identify-stuxnet-like-cyberespionage-malware-called-flame.html), have been identified in the wild, although their purposes are quite different from Stuxnet's. Their similarity to Stuxnet leads experts to believe that they are products of the same development shop, which is apparently still active.

## Was Stuxnet successful

The Stuxnet virus succeeded in its goal of disrupting the Iranian nuclear program; one analyst estimated that it [set the program back by at least two years](https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years). The first outsiders to notice the effects of the worm were inspectors from the International Atomic Energy Agency (IAEA), who were permitted access to the Natanz facility. Part of the IAEA's job was to inspect damaged centrifuges that were being removed from the facility to make sure they weren't being used to smuggle uranium out to some other plant that wasn't on the international community's radar. As noted above, it's typical for centrifuges to be damaged as part of the uranium enrichment process; at a facility on the scale of Natanz, you could expect about 800 centrifuges a year to be taken out of commission. But in 2010, the IAEA started noticing an unusually high number of damaged centrifuges, with one inspector estimating that [almost 2,000 were rendered inoperable](https://gizmodo.com/the-incredible-tale-of-stuxnet-a-weapon-for-the-digita-1656811897). At the time, of course, nobody had any idea that computer malware was causing this.