
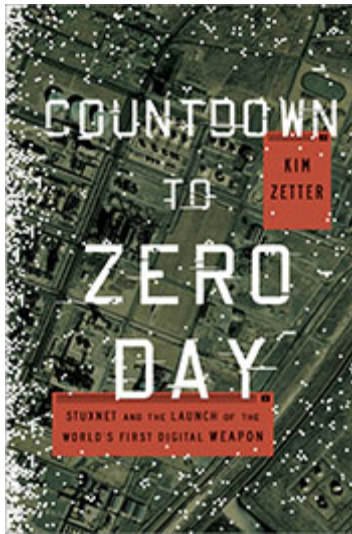


An Unprecedented Look at Stuxnet, the World's First Digital Weapon



This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.  AP Photo/Space Imaging/Inta SpaceTurk, HO



Excerpted from [Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon](#)

In January 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them.

Five months later a seemingly unrelated event occurred. A computer security firm in Belarus was called in to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. Again, the cause of the problem was a mystery. That is, until the researchers found a handful of malicious files on one of the systems and discovered the world's first digital weapon.

Stuxnet, as it came to be known, was unlike any other virus or worm that came before. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.

[Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon](#), written by WIRED senior staff writer Kim Zetter, tells the story behind Stuxnet's planning, execution and discovery. In this excerpt from the book, which will be released November 11, Stuxnet has already been at work silently sabotaging centrifuges at the Natanz plant for about a year. An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process. Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a “cascade”—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons. At the time of the attacks, each cascade at Natanz held 164 centrifuges. Uranium gas flows through the pipes into the centrifuges in a series of stages, becoming further “enriched” at each stage of the cascade as isotopes needed for a nuclear reaction are separated from other isotopes and become concentrated in the gas.

As the excerpt begins, it's June 2009—a year or so since Stuxnet was first released, but still a year before the covert operation will be discovered and exposed. As Iran prepares for its presidential elections, the attackers behind Stuxnet are also preparing their next assault on the

enrichment plant with a new version of the malware. They unleash it just as the enrichment plant is beginning to recover from the effects of the previous attack. Their weapon this time is designed to manipulate computer systems made by the German firm Siemens that control and monitor the speed of the centrifuges. Because the computers are air-gapped from the internet, however, they cannot be reached directly by the remote attackers. So the attackers have designed their weapon to spread via infected USB flash drives. To get Stuxnet to its target machines, the attackers first infect computers belonging to five outside companies that are believed to be connected in some way to the nuclear program. The aim is to make each “patient zero” an unwitting carrier who will help spread and transport the weapon on flash drives into the protected facility and the Siemens computers. Although the [five companies have been referenced in previous news reports](#), they’ve never been identified. Four of them are identified in this excerpt.

The Lead-Up to the 2009 Attack

The two weeks leading up to the release of the next attack were tumultuous ones in Iran. On June 12, 2009, the presidential elections between incumbent Mahmoud Ahmadinejad and challenger Mir-Hossein Mousavi didn’t turn out the way most expected. The race was supposed to be close, but when the results were announced—two hours after the polls closed—Ahmadinejad had won with 63 percent of the vote over Mousavi’s 34 percent. The electorate cried foul, and the next day crowds of angry protesters poured into the streets of Tehran to register their outrage and disbelief. According to media reports, it was the largest civil protest the country had seen since the 1979 revolution ousted the shah and it wasn’t long before it became violent. Protesters vandalized stores and set fire to trash bins, while police and Basijis, government-loyal militias in plainclothes, tried to disperse them with batons, electric prods, and bullets.

That Sunday, Ahmadinejad gave a defiant victory speech, declaring a new era for Iran and dismissing the protesters as nothing more than soccer hooligans soured by the loss of their team. The protests continued throughout the week, though, and on June 19, in an attempt to calm the crowds, the Ayatollah Ali Khamenei sanctioned the election results, insisting that the margin of victory—11 million votes—was too large to have been achieved through fraud. The crowds, however, were not assuaged.

The next day, a twenty-six-year-old woman named Neda Agha-Soltan got caught in a traffic jam caused by protesters and was shot in the chest by a sniper’s bullet after she and her music teacher stepped out of their car to observe.

Two days later on June 22, a Monday, the Guardian Council, which oversees elections in Iran, officially declared Ahmadinejad the winner, and after nearly two weeks of protests, Tehran became eerily quiet. Police had used tear gas and live ammunition to disperse the demonstrators, and most of them were now gone from the streets. That afternoon, at around 4:30 p.m. local time, as Iranians nursed their shock and grief over events of the previous days, a new version of Stuxnet was being compiled and unleashed.

Recovery From Previous Attack

While the streets of Tehran had been in turmoil, technicians at Natanz had been experiencing a period of relative calm. Around the first of the year, they had begun installing new centrifuges again, and by the end of February they had about 5,400 of them in place, close to the 6,000 that Ahmadinejad had promised the previous year. Not all of the centrifuges were enriching uranium yet, but at least there was forward movement again, and by June the number had jumped to 7,052, with 4,092 of these enriching gas. In addition to the eighteen cascades enriching gas in unit A24, there were now twelve cascades in A26 enriching gas. An additional seven cascades had even been installed in A28 and were under vacuum, being prepared to receive gas.



Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008. Office of the Presidency of the Islamic Republic of Iran

The performance of the centrifuges was improving too. Iran's daily production of low-enriched uranium was up 20 percent and would remain consistent throughout the summer of 2009. Despite the previous problems, Iran had crossed a technical milestone and had succeeded in producing 839 kilograms of low-enriched uranium—enough to achieve nuclear-weapons breakout capability. If it continued at this rate, Iran would have enough enriched uranium to make two nuclear weapons within a year. This estimate, however, was based on the capacity of the IR-1 centrifuges currently installed at Natanz. But Iran had already installed IR-2 centrifuges

in a small cascade in the pilot plant, and once testing on these was complete and technicians began installing them in the underground hall, the estimate would have to be revised. The more advanced IR-2 centrifuges were more efficient. It took 3,000 IR-1s to produce enough uranium for a nuclear weapon in one year, but it would take just 1,200 IR-2 centrifuges to do the same.

Cue Stuxnet 1.001, which showed up in late June.

The Next Assault

To get their weapon into the plant, the attackers launched an offensive against computers owned by four companies. All of the companies were involved in industrial control and processing of some sort, either manufacturing products and assembling components or installing industrial control systems. They were all likely chosen because they had some connection to Natanz as contractors and provided a gateway through which to pass Stuxnet to Natanz through infected employees.

To ensure greater success at getting the code where it needed to go, this version of Stuxnet had two more ways to spread than the previous one. Stuxnet 0.5 could spread only by infecting Step 7 project files—the files used to program Siemens PLCs. This version, however, could spread via USB flash drives using the Windows Autorun feature or through a victim's local network using the print-spooler zero-day exploit that Kaspersky Lab, the antivirus firm based in Russia, and Symantec later found in the code.

Based on the log files in Stuxnet, a company called Foolad Technic was the first victim. It was infected at 4:40 a.m. on June 23, a Tuesday. But then it was almost a week before the next company was hit.


The following Monday, about five thousand marchers walked silently through the streets of Tehran to the Qoba Mosque to honor victims killed during the recent election protests. Late that evening, around 11:20 p.m., Stuxnet struck machines belonging to its second victim—a company called Behpajoooh.

It was easy to see why Behpajoooh was a target. It was an engineering firm based in Esfahan—the site of Iran's new uranium conversion plant, built to turn milled uranium ore into gas for enriching at Natanz, and was also the location of Iran's Nuclear Technology Center, which was believed to be the base for Iran's nuclear weapons development program. Behpajoooh had also been named in US federal court documents in connection with Iran's illegal procurement activities.

Behpajoooh was in the business of installing and programming industrial control and automation systems, including Siemens systems. The company's website made no mention of Natanz, but it did mention that the company had installed Siemens S7-400 PLCs, as well as the Step 7 and WinCC software and Profibus communication modules at a steel plant in Esfahan. This was, of course, all of the same equipment Stuxnet targeted at Natanz.

At 5:00 a.m. on July 7, nine days after Behpajooch was hit, Stuxnet struck computers at Neda Industrial Group, as well as a company identified in the logs only as CGJ, believed to be Control Gostar Jahed. Both companies designed or installed industrial control systems.



Iranian President Mahmoud Ahmadinejad observes computer monitors at the Natanz uranium enrichment plant in central Iran, where Stuxnet was believed to have infected PCs and damaged centrifuges.  Office of the Presidency of the Islamic Republic of Iran

Neda designed and installed control systems, precision instrumentation, and electrical systems for the oil and gas industry in Iran, as well as for power plants and mining and process facilities. In 2000 and 2001 the company had installed Siemens S7 PLCs in several gas pipeline operations in Iran and had also installed Siemens S7 systems at the Esfahan Steel Complex. Like Behpajooch, Neda had been identified on a proliferation watch list for its alleged involvement in illicit procurement activity and was named in a US indictment for receiving smuggled microcontrollers and other components.

About two weeks after it struck Neda, a control engineer who worked for the company popped up on a Siemens user forum on July 22 complaining about a problem that workers at his company were having with their machines. The engineer, who posted a note under the user name Behrooz, indicated that all PCs at his company were having an identical problem with a Siemens Step 7 .DLL file that kept producing an error message. He suspected the problem was a virus that spread via flash drives.

When he used a DVD or CD to transfer files from an infected system to a clean one, everything was fine, he wrote. But when he used a flash drive to transfer files, the new PC started having the same problems the other machine had. A USB flash drive, of course, was Stuxnet's primary

method of spreading. Although Behrooz and his colleagues scanned for viruses, they found no malware on their machines. There was no sign in the discussion thread that they ever resolved the problem at the time.

It's not clear how long it took Stuxnet to reach its target after infecting machines at Neda and the other companies, but between June and August the number of centrifuges enriching uranium gas at Natanz began to drop. Whether this was the result solely of the new version of Stuxnet or the lingering effects of the previous version is unknown. But by August that year, only 4,592 centrifuges were enriching at the plant, a decrease of 328 centrifuges since June. By November, that number had dropped even further to 3,936, a difference of 984 in five months. What's more, although new machines were still being installed, none of them were being fed gas.

Clearly there were problems with the cascades, and technicians had no idea what they were. The changes mapped precisely, however, to what Stuxnet was designed to do.

Reprinted from [Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon](#) Copyright © 2014 by Kim Zetter. Published by Crown Publishers, an imprint of Random House LLC.