Stuxnet explained: The first known cyberweapon

by Josh Fruhlinger Contributing writer

Analysis

Aug 31, 2022

CybercrimeMalwarePhysical Security

Thanks to Stuxnet, we now live in a world where code can destroy machinery and stop (or start) a war.

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. 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.

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 began 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. 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.

The classified program to develop the worm was given the code name "Operation Olympic Games"; 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.

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 Schouwenberg estimated that it

took a team of ten coders two to three years to create the worm in its final form.

Several other worms with infection capabilities similar to Stuxnet, including those dubbed Duqu and Flame, 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.

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.

How did Stuxnet work?

Stuxnet attacks all layers of its target infrastructure: Windows, the Siemens software running on windows that controls the PLCs, and the embedded software on the PLCs themselves. It is designed to be delivered via a removable drive like a USB stick—the Natanz facility where the uranium enrichment was taking place was known to be *air-gapped,* with its systems not connected to the internet—but also to spread quickly and indiscriminately from machine to machine on an internal network.

Stuxnet includes rootkit abilities at both user and kernel mode. To install the kernel-mode rootkit, it uses digitally signed device drivers that use private key certificates stolen from two well-known Taiwanese device manufacturers.

Once in control of the PLCs, Stuxnet varied the rotation speeds of the centrifuges while they were in operation in a way that damaged them and left them inoperable in short order.

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—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 Conficker 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.

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, 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.

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. 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. At the time, of course, nobody had any idea that computer malware was causing this.

How was Stuxnet discovered?

Stuxnet was discovered because, unexpectedly, it spread beyond the Natanz facility. As noted, Natanz was air-gapped, and it's not clear how Stuxnet got out. Many in the U.S. believed the spread was the result of code modifications made by the Israelis; then-Vice President Biden was said to be particularly upset about this. It's also possible that it escaped thanks to poor security practices on the part of the Iranians at Natanz—it could've been something as simple as someone taking a work laptop home and connecting it to the internet. Thanks to the malware's sophisticated and extremely aggressive nature, it then began to spread to other computers.

Stuxnet soon became known to the security community thanks to a call to tech support. An office in Iran (not part of the nuclear program) was experiencing mysterious reboots and blue screens of death, which were even affecting computers with fresh OS installs. The on-site security expert, unable to figure out the cause, contacted a friend of his, a Belarusian named Sergey Ulasen who was working for the antivirus vendor VirusBlokAda. Ulasen was at a wedding reception, but spent the evening on the phone with his Iranian friend trying to figure out the cause of the problem. Ulasen and his team managed to isolate the malware and realized how many zero-days it was exploiting and what they were up against. They began the process of sharing their discoveries with the wider security community.

Liam O'Murchu, who's the director of the Security Technology and Response group at Symantec and was on the team there that first unraveled Stuxnet, says that Stuxnet was "by far the most complex piece of code that we've looked at—in a completely different league from anything we'd ever seen before." And while you can find lots of websites that claim to have the Stuxnet code available to download, O'Murchu says you shouldn't believe them: he emphasized to *CSO* that the original source code for the worm, as written by coders working for U.S. and Israeli intelligence, hasn't been released or leaked and can't be extracted from the binaries that are loose in the wild.

(The code for one driver, a very small part of the overall package, has been reconstructed via reverse engineering, but that's not the same as having the original code.)

However, he explained that a lot about code could be understood from examining the binary in action and reverse-engineering it. For instance, he says, "it was pretty obvious from the first time we analyzed this app that it was looking for some Siemens equipment." Eventually, after three to six months of reverse engineering**, "**we were able to determine, I would say, 99 percent of everything that happens in the code," O'Murchu said.

And it was a thorough analysis of the code that eventually revealed the purpose of the malware. "We could see in the code that it was looking for eight or ten arrays of 168 frequency converters each," says O'Murchu. "You can read the International Atomic Energy Association's documentation online about how to inspect a uranium enrichment facility, and in that documentation they specify exactly what you would see in the uranium facility—how many frequency converters there will be, how many centrifuges there would be. They would be arranged in eight arrays and that there would be 168 centrifuges in each array. That's exactly what we were seeing in the code."

"It was very exciting that we'd made this breakthrough," he added. "But then we realized what we had got ourselves into—probably an international espionage operation—and that was quite scary." Symantec released this information in September of 2010; analysts who had gotten wind of the IAEA's observation of damaged Iranian centrifuges began to understand what was happening.

Is Stuxnet still out there?

Stuxnet hasn't vanished, but it is not a major cybersecurity threat today. In fact, while Stuxnet grabbed a lot of headlines due to its dramatic capabilities and cloak-and-dagger origins, it was never much of a threat to anybody other than the Natanz facility that was its original target. If your computer is infected with Stuxnet and you aren't connected to a centrifuge used for uranium enrichment, the worst case scenario is that you might see reboots and blue screens of death, like the Iranian office that brought the malware to the world's attention, but other than that little or no harm will come to you.

How to prevent Stuxnet

That said, you probably don't *want* your systems infected by powerful malware developed by U.S. and Israeli intelligence agencies. Fortunately, the zero-day vulnerabilities Stuxnet originally exploited have long been patched. As long as you're practicing the basics of good cyber hygiene, keeping your OS and security software up to date, you don't have much to worry about. Remember, Stuxnet affects PLCs, so you'll want to keep any operational technology as secure as possible as well.

Why is Stuxnet significant to cybersecurity?

If there's any threat coming from Stuxnet, it's one that emanates from its descendants. As we noted above, there are other malware families that seem to have functionality derived from Stuxnet; these may be from the same intelligence agency shop, or they might represent freelance hackers who have managed to reverse-engineer some of Stuxnet's power. Security researchers are still building off of Stuxnet to discover new attack techniques.

But beyond specific technologies, Stuxnet is significant because it represented the first widely recognized intrusion of computer code into the world of international conflict, an idea that previously had been in the realm of cyberpunk sci-fi. In the decade since, particularly in the Russia-Ukraine conflict, cyberattacks have become accepted as part of the arsenal of war.