CASE STUDY

CYBERSECURITY

2.1.1 - Threat Actors

Stuxnet

Article:

Confirmed: US and Israel created Stuxnet, lost control of it

JUN 1, 2012

Retrieved from: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Source: ARS Technica
Author: Nate Anderson

In 2011, the US government rolled out its "International Strategy for Cyberspace," which reminded us that "interconnected networks link nations more closely, so an attack on one nation's networks may have impact far beyond its borders." An in-depth report today from the New York Times confirms the truth of that statement as it finally lays bare the history and development of the Stuxnet virus—and how it accidentally escaped from the Iranian nuclear facility that was its target.

The article is adapted from journalist David Sanger's forthcoming book, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, and it confirms that both the US and Israeli governments developed and deployed Stuxnet. The goal of the worm was to break Iranian nuclear centrifuge equipment by issuing specific commands to the industrial control hardware responsible for their spin rate. By doing so, both governments hoped to set back the Iranian research program—and the US hoped to keep Israel from launching a pre-emptive military attack.

The code was only supposed to work within Iran's Natanz refining facility, which was air-gapped from outside networks and thus difficult to penetrate. But computers and memory cards could be carried between the public Internet and the private Natanz network, and a preliminary bit of "beacon" code was used to map out all the network connections within the plant and report them back to the NSA.

That program, first authorized by George W. Bush, worked well enough to provide a digital map of Natanz and its industrial control hardware. Soon, US national labs were testing different bits of the plan to sabotage Natanz (apparently without knowing what the work was for) using similar centrifuges that had come from Libya's Qadaffi regime. When the coders found the right sets of commands to literally shake the centrifuges apart, they knew that Stuxnet could work.

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

When ready, Stuxnet was introduced to Natanz, perhaps by a double agent.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others—both spies and unwitting accomplices—with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

When Barack Obama came to office, he continued the program—called "Olympic Games"—which unpredictably disabled bits of the Natanz plant even as it told controllers that everything was normal. But in 2010, Stuxnet escaped Natanz, probably on someone's laptop; once connected to the outside Internet, it did what it was designed not to do: spread in public. The blame game began about who had slipped up in the coding.

"We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

Once released more widely, the Stuxnet code was found and then disassembled by security researchers.

Please don't follow our example

As the International Strategy for Cyberspace notes, these sorts of electronic attacks are serious business. The US in fact reserves the right to use even military force to respond to similar attacks. "All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners," says the report. "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law."

Yet the US had just gone on the cyber-attack, and everyone knew it. Speculation has long swirled around government-backed hackers from nations like China and Russia, especially, who have been suspected of involvement in espionage, industrial trade secret theft, and much else. Would something like Stuxnet damage US credibility when it complained about such attacks? (China has long adopted the "you do it too!" defense on Internet issues, especially when it comes to censoring and filtering of Internet content.)

Obama was at least aware of the likely answer—yes—but pressed ahead, even accelerating the Olympic

Games program.

[Obama] repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons—even under the most careful and limited circumstances—could enable other countries, terrorists or hackers to justify their own attacks. "We discussed the irony, more than once," one of his aides said.

Stuxnet is old news by now. Even the newly discovered "Flame" malware was developed some time ago. While details about these two targeted attack packages are finally emerging, the next generation of attack tools has no doubt been developed and likely deployed.

Summary

Starting with the Bush Administration (and continued into the Obama Administration), the US Government started Operation Olympic Games, which aimed to stop the Israelis from bombing an Iranian nuclear facility. The operation ended up working alongside the Israeli government to plant a worm/virus inside the Natanz Iranian nuclear facility. The malware provided a map of the facility, which was valuable intel, but then the creators discovered that they could access the commands to the centrifuges. The program started making the centrifuges spin uncontrollably, destroying a key piece of the plant.

In 2011, the United States released the International Strategy for Cyberspace which warned nations that an attack on the US's networks could result in a military force response. However, while using Stuxnet, the US deployed a cyberattack against Iran. Obama even challenged the US's use of cyberweapons, stating that this could enable other countries, terrorists, or hackers to justify their own attacks.

Questions

- The article states "The US in fact reserves the right to use even military force to respond to similar attacks", should the US be carrying out cyberattacks like Stuxnet?
- What could Iran have done in response to the Stuxnet attack?
- If the US launches cyberattacks against other nations, do other countries, terrorists, or hackers reserve the right to launch cyberattacks against the US?
- Should there be an international agreement against unprovoked cyberattacks? What would repercussions of breaking the agreement look like?
- What are some reasons a Nation State would use malware to attack another nation? Why did the US and Israel use Stuxnet against Iran?
- At what point might a cyberattack bring about a physical ("kinetic") military response?

Further Study

- Washington Post article on Stuxnet: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html
- More detailed article about Stuxnet (Wired): https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
- Patch information about Stuxnet: https://www.zdnet.com/article/ms-ships-temporary-fix-it-for-windows-shortcut-zero-day-attacks/
- Response to the consequences of Stuxnet: https://www.zdnet.com/article/as-attacks-escalate-microsoft-ships-emergency-windows-patch/
- Article about Olympic Games, the larger group/attack that umbrellaed Stuxnet: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html