A Silent Attack, but Not a Subtle One

By JOHN MARKOFF
SAN FRANCISCO

AS in real warfare, even the most carefully aimed weapon in computer warfare leaves collateral damage.

The Stuxnet worm was no different.

The most striking aspect of the fast-spreading malicious computer program — which has turned up in industrial programs around the world and which Iran said had appeared in the computers of workers in its nuclear project — may not have been how sophisticated it was, but rather how sloppy its creators were in letting a specifically aimed attack scatter randomly around the globe.

The malware was so skillfully designed that computer security specialists who have examined it were almost certain it had been created by a government and is a prime example of clandestine digital warfare. While there have been suspicions of other government uses of computer worms and viruses, Stuxnet is the first to go after industrial systems. But unlike those other attacks, this bit of malware did not stay invisible.

If Stuxnet is the latest example of what a government organization can do, it contains some glaring shortcomings. The program was splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment. Computer security specialists are also puzzled by why it was created to spread so widely.

Global alarm over the deadly computer worm has come many months after the program was suspected of stealthily entering an Iranian nuclear enrichment plant, perhaps carried on a U.S.B. memory drive containing the malware.

Computer security specialists have speculated that once inside the factory and within the software that controls equipment, the worm reprogrammed centrifuges made by a specific
company, Siemens, to make them fail in a way that would be virtually undetectable. Whether the program achieved its goal is not known.

Much speculation about the target has focused on the Iran nuclear plant at Natanz. In mid-July the Wikileaks Web site reported that it had learned of a serious nuclear accident at the plant. But international nuclear inspectors say no evidence of one exists.

The timing is intriguing because a time stamp found in the Stuxnet program says it was created in January, suggesting that any digital attack took place long before it was identified and began to attract global attention.

The head of the Bushehr nuclear plant in Iran said Sunday that the worm had affected only the personal computers of staff members, Reuters reported. Western nations say they do not believe Bushehr is being used to develop nuclear weapons. Citing the state-run newspaper Iran Daily, Reuters reported that Iran’s telecommunications minister, Reza Taghipour, said the worm had not penetrated or caused “serious damage to government systems.”

Siemens has said that the worm was found in only 15 plants around the world using its equipment and that no factory’s operations were affected. But now the malware not only is detectable, but also is continuing to spread through computer systems around the world through the Internet.

It is also raising fear of dangerous proliferation. Stuxnet has laid bare significant vulnerabilities in industrial control systems. The program is being examined for clues not only by the world’s computer security companies, but also by intelligence agencies and countless hackers.

“Proliferation is a real problem, and no country is prepared to deal with it,” said Melissa Hathaway, a former United States national cybersecurity coordinator. The widespread availability of the attack techniques revealed by the software has set off alarms among industrial control specialists, she said: “All of these guys are scared to death. We have about 90 days to fix this before some hacker begins using it.”

The ability of Stuxnet to infiltrate these systems will “require a complete reassessment” of security systems and processes, starting with federal technology standards and nuclear regulations, said Joe Weiss, a specialist in the security of industrial control systems who is managing partner at Applied Control Solutions in Cupertino, Calif.

One big question is why its creators let the software spread widely, giving up many of its secrets in the process.
One possibility is that they simply did not care. Their government may have been so eager to stop the Iranian nuclear program that the urgency of the attack trumped the tradecraft techniques that traditionally do not leave fingerprints, digital or otherwise.

While much has been made in the news media of the sophistication of Stuxnet, it is likely that there have been many other attacks of similar or even greater sophistication by intelligence agencies from many countries in the past. What sets this one apart is that it became highly visible.

Security specialists contrast Stuxnet with an intrusion discovered in the Greek cellphone network in March 2005. It also displayed a level of skill that only the intelligence agency of some foreign power would have.

A two-year investigation by the Greek government found an extremely sophisticated Trojan horse program that had been hidden by someone who was able to modify and then insert 29 secret programs into each of four telephone switching computers.

The spy system came apart only when a software upgrade provided by the manufacturer led to some text messages, sent from the system of another cellphone operator, being undelivered. The level of skill needed to pull off the operation and the targets strongly indicated that the culprit was a government. An even more remarkable set of events surrounded the 2007 Israeli Air Force attack on what was suspected of being a Syrian nuclear reactor under construction.

Accounts of the event initially indicated that sophisticated jamming technology had been used to blind the radar so Israeli aircraft went unnoticed. Last December, however, a report in an American technical publication, IEEE Spectrum, cited a European industry source as raising the possibility that the Israelis had used a built-in kill switch to shut down the radar.

A former member of the United States intelligence community said that the attack had been the work of Israel’s equivalent of America’s National Security Agency, known as Unit 8200.

But if the attack was based on a worm or a virus, there was never a smoking gun like Stuxnet.

*Kevin O’Brien contributed reporting from Berlin.*
News Analysis - Stuxnet Worm Is Remarkable for Its Lack of Subtlety - NYTimes.com