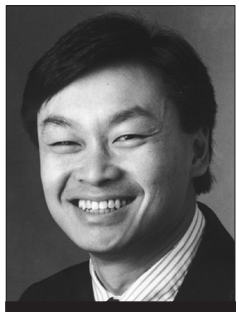
IEEE NETWORK®
THE MAGAZINE OF GLOBAL INTERNETWORKING

EDITOR'S NOTE

Stuxnet, the Real Start of Cyber Warfare?



Thomas M. Chen

In recent years, the press has been banging the drums about the prospects of cyber warfare between nations. It makes a good story. In the imagined scenario, national governments are gathering and training elite teams of computer hackers prepared to infiltrate or take down the computer network of an enemy nation. Every nation has the weapons — computers and software — to be a major threat without having to be a superpower. Any David can take on a Goliath, and in fact the most industrialized countries might be the most network-dependent and vulnerable.

The notable incident that attracted press attention was a three-week wave of distributed denial of service (DDoS) attacks on numerous Estonian web sites starting on April 27, 2007. At the time, Estonia and Russia were involved in a dispute over the removal of the Bronze Soldier of Tallinn, a Soviet war memorial in Estonia. Estonia relocated the statue on April 27, which prompted vigorous protests by ethnic Russians (1300 were arrested). Because the DDoS attacks started after the relocation of the statue, the conflict was perceived to be the reason for the attacks.

Suspicions about the perpetrator of the DDoS attacks immediately fell on Russia. The Estonian foreign minister and defense minister publicly accused Russia of coordinating the DDoS attacks, although they admitted that they had no proof. They brought the accusations to the attention of NATO, and the Estonian president even talked about it with U.S. President Bush in a June 25, 2007 meeting. According to Estonian government officials, the attacks had to be supported by a national government (presumably Russia) because of their large scale, sophistication, and coordination. However, some security experts in other countries downplayed these aspects in later analyses. The attacks were basically flooding attacks by botnets, and not particularly well coordinated, according to Prof. James Hendler (former chief scientist at DARPA). Mike Witt, deputy director of the U.S. CERT, commented that the scale of the attack was significant for Estonia, but not that significant from the U.S. perspective.

The DDoS attacks on Estonia may not have been a real "cyber war," but many governments are taking the possibility of nation-sponsored cyber attacks seriously. For instance, the United States established a Cyber Command (Cybercom) at Fort Meade, Maryland, in May 2010 to defend American military networks. The United Kingdom has set up a cybersecurity operations center at Government Communications Headquarters (GCHQ) based in Cheltenham.

Some security experts believe that an era of cyber warfare has now really begun. The latest development is the Stuxnet worm, first discovered by VirusBlokAda in Belarus in July 2010. The worm had already been in the wild for several months, although estimates vary. Microsoft reported that some evidence suggests the Stuxnet code dates back to January 2009. Stuxnet has raised the eyebrows of security researchers for three reasons: its choice of target, level of sophistication, and implications for future malware.

Choice of Target

Unlike most earlier worms, Stuxnet's choice of target is very specific. For historical context, consider some worm examples from 2003, sometimes called the worst year for worms, highlighted by Slammer, Blaster, and Sobig. These worms all attempted to spread to many targets as quickly as possible. Slammer spread quickly among Microsoft SQL servers. Blaster exploited a remote procedure call (RPC) vulnerability on Windows NT, Windows 2000, and Windows XP computers. Sobig flooded mail servers with copies of itself.

In contrast, the Stuxnet worm is highly selective not only about its targets but also in specific conditions on the targets. It reportedly attacks Windows computers using at least four zero-day exploits. However, it looks for a particular programmable logic controller (PLC) made by Siemens on the vulnerable computers. PLCs are an interface between a program and machines that perform physical work(e.g., to move robot arms or open elevator doors). That is, they enable computers to control some automated physical processes in common industrial control systems found in factories, refineries, and power plants. In this case, Stuxnet looks specifically for Siemens' WinCC/PCS 7 SCADA (supervisory control and data acquisition) software running on the PLC. Moreover, it waits and looks for a specific program condition before it will attempt to take over control by manipulating some of the settings.

Unlike earlier worms, Stuxnet appears to be aimed directly at controlling physical machinery. Earlier worms did have physical consequences (e.g., Slammer disrupted automatic teller machines and airline reservation systems), but they were really side effects of network congestion caused by fast worm spreading. Earlier worms were aimed at computer systems. Stuxnet is different in that it attempts to take control of critical physical infrastructure.

Stuxnet is estimated to have infected 50,000–100,000 computers, mainly in Iran, India, Indonesia, and Pakistan. Ralph Langner, a German security expert familiar with industrial systems security, has suggested that the primary target was the Bushehr nuclear plant in Iran based on his laboratory testing and dissection of the Stuxnet code. Iranian officials at the Bushehr nuclear plant have denied that Stuxnet has caused any damage to the main systems, although they appeared to admit that some staff PCs had been infected. A two-month delay in bringing the reactor online was blamed on a leak in a storage pool for the plant's fuel. Other experts have speculated that the primary target was the Natanz uranium enrichment facility in Iran. Coincidentally, the site appeared to mysteriously drop 15 percent in production in 2009, around when Stuxnet is believed to have been spreading.

Sophistication

Several aspects of Stuxnet discovered by security experts point to an extremely high level of sophistication for malware. The sophistication is found in Stuxnet's programming, and the insider information needed about PLCs and power plants. Ilias Chantzos, director of government relations at Symantec, has estimated the manpower required to develop Stuxnet to have been five to ten people working for six months with access to SCADA systems. All reports examining Stuxnet have agreed on the likelihood of a government's involvement in its development.

First, the Stuxnet code is unusually complex and large for malware — almost half a megabyte — and was written in multiple languages.

Second, its initial infection vector is a USB stick instead of the Internet. This suggests that the attackers were very familiar with the primary target and knew it was not reachable by the Internet. The USB stick keeps count and allows only three infections. The infection running on a target system attempts to spread for only 21 days. These suggest an intention to limit the spreading rate, perhaps to maintain stealth.

Third, it is digitally signed by two certificates (stolen from JMicron and Realtek) to appear legitimate, again for stealth.

Fourth, the code contains an unprecedented four zero-day Windows exploits. Zero-day exploits are highly valued by attackers, so four exploits represent an unusually high investment. However, Stuxnet does not seem to care about infecting all vulnerable systems. After being introduced into a network by USB, it seeks out and attacks only machines running WinCC and PCS 7 SCADA software through exploits and default Siemens passwords. One of the exploits is called MS08-067, also used earlier by the Conficker worm. Microsoft issued a patch for it in 2008, but the attackers seemed to know that SCADA systems are slow to be patched.

Fifth, Stuxnet demonstrates inside (not published) knowledge of Siemens WinCC/Step 7 software, reflected in its capability to detect specific conditions and make code modifications in a specific part of the Siemens program called Organizational Block 35. This part of the software monitors critical factory operations that need a response within 100 ms. This code injection seems to suggest that Stuxnet was designed for high impact damage.

Sixth, after successful infection, it installs a rootkit (to hide itself) and tries to connect to command and control servers in Malaysia and Denmark. It also mutates by downloading updates through peer-to-peer networking.

Implications for Future Malware

Ralph Langner has expressed his belief that Stuxnet is the first real "cyber weapon" because it is aimed at a physical and military target (the Bushehr nuclear plant, in his opinion). His main concern appears to be what Stuxnet implies for the future.

If Stuxnet really was developed for cyber warfare, it means that governments are now actively pursuing offensive "first strike" capabilities, not only network defense. Iran has suspected NATO and U.S. involvement behind Stuxnet, although both have denied responsibility. Some have also suspected Israel's Unit 8200. Israel has not publicly commented on Stuxnet, but Israel (as well as other national governments) acknowledges that cyber warfare is now part of their mission.

Langner is also concerned that the technology in Stuxnet will be copied by hackers, organized crime, and terrorists. The targets next time may not be power plants. PCLs are found widely in many automated industrial systems. Stuxnet has shown that a wide range of industrial systems are vulnerable. Stuxnet could be the first incident in a new era of attacks on critical infrastructures across many industries.

As always, I welcome your comments and feedback at tom_chen@yahoo.com.