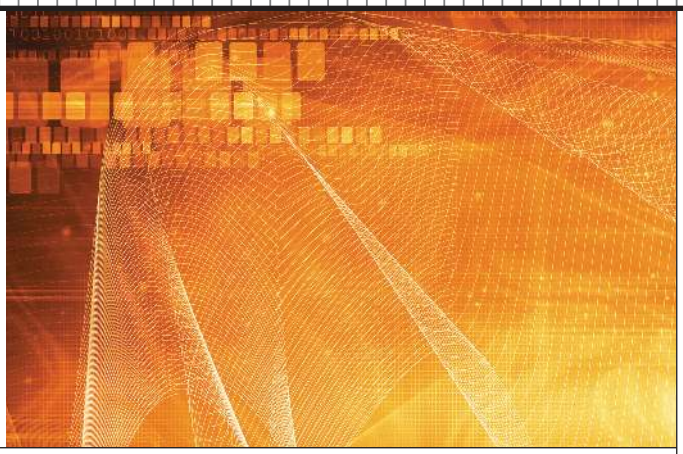
Lessons from Stuxnet

Thomas M. Chen, *Swansea University*
Saeed Abu-Nimeh, *Damballa Inc.*



Malware such as Stuxnet can affect critical physical infrastructures that are controlled by software, which implies that threats might extend to real lives.

Thousands of new malware appear in the wild daily. Most are evolutionary variants of existing families and don't have a widespread impact. However, occasionally a noteworthy new piece of malware will change the security landscape. For example, the 1988 Morris attack showed that an aggressive worm could bring down a substantial part of the Arpanet, and the 2003 SQL Slammer attack demonstrated that a simple user datagram protocol (UDP)-based worm could create devastating network congestion.

Stuxnet is teaching the security community new lessons. Since VirusBlokAda discovered the Windows worm in Belarus in July 2010, researchers have studied it intensely. They believe Stuxnet spread for several months before discovery and that it has already compromised its intended target.

As Table 1 shows, Stuxnet differs from past malware in several ways. First, most malware tries to infect as many computers as possible, whereas Stuxnet appears to target industrial control systems and delivers its payload under very specific conditions. Second, Stuxnet is larger and more complex than other malware. It contains exploits for four unpatched vulnerabilities—an unusually high number. The code is approximately 500 Kbytes and written in multiple languages. As a reference, the SQL Slammer worm was 376 bytes; the Code Red worm was approximately 4 Kbytes; the Nimda worm was 60 Kbytes; and variants of the Zeus banking Trojan ranged between 40 and 150 Kbytes. Virtually all malware is less than 1 Mbyte.

Based on Stuxnet's code, experts have speculated on its creators and intention. Its sophistication suggests that the creators had detailed knowledge of its target and access to immense resources, perhaps with government backing. Its choice of targets also suggests a political motive.

TARGET SELECTION

Unlike most malware, Stuxnet targets industrial control systems, which are used widely in factories, assembly lines, refineries, and power plants. It attacks Windows PCs that program specific Siemens programmable logic controllers—specialized computers that control automated physical processes, such as robot arms, in common industrial control systems. PLCs can have elaborate input/output arrangements for various applications in different physical environments. They often have sensors on the inputs (for example, for temperature), and the outputs typically operate equipment such as motors, switches, and relays.

Stuxnet targets vulnerable PCs running WinCC/Step 7 control software, which is normally used to program PLCs. When an infected PC connects to a Siemens Simatic PLC, Stuxnet installs a malicious .dll file, replacing the PLC's original .dll file. The malicious .dll file lets Stuxnet monitor and intercept all communication

Table 1. Stuxnet's novel characteristics.

Aspect	Stuxnet	Common malware
Targeting	Extremely selective	Indiscriminate
Type of target	Industrial control systems	Computers
Size	500 Kbytes	Less than 1 Mbyte
Probable initial infection vector	Removable flash drive	Internet and other networks
Exploits	Four zero-days	Possibly one zero-day

0018-9162/11/$26.00 © 2011 IEEE Published by the IEEE Computer Society

between the PC and PLC. Depending on specific PLC conditions, Stuxnet injects its own code onto the PLC in a manner undetectable by the PC operator.

Whereas most malware payloads have a clear purpose, such as spam or data theft, Stuxnet's intended goal is unknown. Security researchers believe that part of the injected code is intended to affect the frequency converter drives' speed. The code appears to alternate between slowing down and speeding up the normal frequency. Hypothetically, if the targeted PLC connects to a nuclear centrifuge, which is used for enriching uranium, the speed fluctuations could cause the centrifuge to fly apart. However, the real-world result is difficult to guess because PLCs can connect to a variety of equipment.

According to measurements of its traffic to command and control servers, Stuxnet has infected an estimated 50,000 to 100,000 computers, mainly in Iran (58 percent), Indonesia, India, and Azerbaijan (www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf). Iran also has a high percentage of infected hosts that are running Siemens Step 7 software—67 percent compared to other countries, where the infection rate is less than 13 percent.

Iran's high infection rate suggests a political motive. Based on his lab testing and dissection of the Stuxnet code, Ralph Langner—a German security expert familiar with industrial systems—has suggested that the primary target was Iran's Bushehr nuclear plant (www.langner.com/en). Iranian officials have denied that Stuxnet has caused any damage to the nuclear plant's main systems; however, they did admit that some staff PCs had been infected. Officials blamed a two-month delay in bringing the reactor online on a leak in the plant's fuel storage pool.

Other experts have speculated that the primary target was Iran's Natanz uranium enrichment facility. The site's production dropped 15 percent in 2009, around the time Stuxnet is believed to have begun spreading. In November 2010, Iran's president confirmed that several centrifuges were hit by malware, which lends support to the theory that Stuxnet targeted Iran's nuclear program.

INSIDER KNOWLEDGE

Stuxnet shows remarkably detailed knowledge of PLCs and industrial control systems. This type of information isn't published openly. For example, the creators knew that its target wouldn't be reachable through the Internet. Thus, the initial infection vector might have been a removable flash drive. Stuxnet is designed to infect and hide in removable drives, using a Windows rootkit to prevent a PC owner from discovering Stuxnet files. The flash drive allows only three infections, which attempt to spread for 21 days. This suggests an intent to limit the spreading rate, perhaps to maintain stealth.

Once installed on a local network, Stuxnet tries to find vulnerable PCs and propagates through network shares.

Once installed on a local network, Stuxnet tries to find vulnerable PCs and propagates through network shares. It copies itself to other Windows PCs through a print spooler vulnerability (MS10-061) and connects to other computers through the Server Message Block protocol and exploits a Windows Server Service remote procedure call (RPC) vulnerability (MS08-067). In addition, it seeks servers running Siemens WinCC database software, which has a hard-coded password that can't be changed or deleted. Stuxnet copies itself to the server by SQL injection.

Stuxnet also demonstrates detailed knowledge of Siemens WinCC/Step 7 software, reflected in its ability to detect specific conditions and modify code depending on the target PLC's CPU. Stuxnet's creators would have needed to know the target PLC's configuration, and probably required similar hardware to develop and test the malware code.

EFFORT LEVEL

Stuxnet's sophistication points to an unusually high effort level. Ilias Chantzos, director of government relations at Symantec, estimated the manpower required to develop Stuxnet to have been 5 to 10 people working for six months with access to Scada systems. All reports examining Stuxnet have agreed on the likelihood of at least one government's involvement in its development.

Besides detailed insider knowledge of the target, other aspects suggest that Stuxnet's creators expended considerable resources. The code contains an unprecedented four zero-day Windows exploits. Attackers value zero-day exploits, so four represents an unusually high investment. The Conficker worm likewise exploited the Windows Server Service RPC vulnerability, for which Microsoft issued a patch in 2008, but Stuxnet's creators seemed to know that patching Scada systems is time-consuming.

Stuxnet is digitally signed by two certificates to appear legitimate. Initially, it used a stolen certificate from Realtek Semiconductor, but VeriSign revoked the certificate on 16 July 2010. The next day, Stuxnet was found to be using a stolen certificate from JMicron Technology, which was subsequently revoked on 22 July. The two companies are situated near each other, suggesting physical theft at those locations.

Stuxnet goes to great lengths for additional stealth, but its techniques aren't novel. It attempts to bypass popular security software by injecting itself into a recognized process,

then installing a Windows rootkit to hide in an infected PC.

In addition, Stuxnet can update itself in two ways. An infected PC uses peer-to-peer communication to learn new updates. It also tries to connect to command-and-control servers (initially in Malaysia and Denmark) to report system data culled from the infected system and download arbitrary executables.

CONSEQUENCES AND IMPLICATIONS

Although important details about Stuxnet—its creators, motives, target, and whether it has accomplished its goal—remain speculative, it has certainly reignited concerns about the possibility of cyberwarfare. Some experts perceive Stuxnet as the first real cyberwarfare weapon.

Fears of cyberwar were raised earlier by distributed denial-of-service attacks on Estonia in mid-2007. However, a DDoS is a fairly simple brute-force attack. Stuxnet is far more sophisticated in its selectivity, stealth, self-protection, and self-updating. Similar malware might be suitable as a "first strike" weapon to compromise its target covertly before an overt offensive.

After Stuxnet's discovery, Iran accused NATO and the US of involvement in the attacks, but both have denied responsibility. Some have also suspected Israel's Unit 8200 security agency. Israel hasn't publicly commented on Stuxnet but acknowledges that cyberwarfare is now part of its mission. Israel is far from the only nation with cyberwarfare capabilities. The US established the Cyber Command (USCYBERCOM) at Fort Meade, Maryland, to defend American military networks. Other nations including the UK, China, and the Russian Federation are widely believed to be pursuing cyberwarfare capabilities as well.

Stuxnet has opened security researchers' eyes to the fact that malware isn't restricted to computers. Malware can affect critical physical infrastructures, which are mostly controlled by software. This implies that threats might extend to real lives.

Stuxnet has also shown that isolation from the Internet isn't an effective defense, and an extremely motivated attacker might have an unexpected combination of inside knowledge, advanced skills, and vast resources. Existing technologies would have difficulty defending against this caliber of attack. Indeed, Stuxnet might become the model for future generations of cyberoffense.

Thomas M. Chen *is a professor in the School of Engineering, Swansea University, UK. Contact him at t.m.chen@swansea.ac.uk.*

Saeed Abu-Nimeh *is a security researcher at Damballa Inc., San Diego. Contact him at sabunimeh@damballa.com.*

Editor: Jeffrey Voas, National Institute of Standards and Technology; jeffrey.m.voas@gmail.com