the Availability Digest

www.availabilitydigest.com

Stuxnet – The World's First Cyberweapon

March 2011

Cyber warfare has so far been the premise of science fiction movies as well as the object of massive defense spending by many countries. However, it has just taken its first step into the real world. The Stuxnet worm, discovered last June by a security firm in Belarus retained by Iran, is designed to attack and sabotage control systems used in power grids, pipelines, nuclear plants, railroads, and other facilities controlled by computers.

The power and flexibility of Stuxnet is evidenced by the fact that it evidently is focused on Iran's nuclear efforts. However, the technology behind Stuxnet is now public knowledge; and this leaves any computer-controlled facility open to hostile attack.

Stuxnet has so far spread to 155 countries, mostly Iran. You may be infected. If you are, you probably don't even know it. Stuxnet activates only if you are a control computer configured in a very specific way. Otherwise, it will eventually delete itself from your computer.

What is Stuxnet?

Stuxnet is a very targeted piece of malware. It looks for industrial control systems. When one of the right type is found, it allows hackers to take control of the system and manipulate it remotely without the operator knowing.

Industrial systems are not controlled by the type of computers with which we are familiar. Rather, they are controlled by a separate, dedicated system known as a SCADA (Supervisory Control and Data Acquisition) system. These systems use firmware-based cards known as PLCs (Programmable Logic Controllers). PLCs are used to communicate with, monitor, and control remote devices such as motors, valves, and switches, either automatically or in response to operator commands. SCADA systems are typically not connected to the Internet, only to private networks. Though security is a very big topic in the SCADA industry, it is generally felt that these systems are very difficult to hack into since they are not on a public network.

Stuxnet avoids this inconvenience by propagating itself via USB thumb drives. If it finds that a computer is properly configured as a SCADA system with PLCs in which it is interested, it goes to work. If not, it looks on the private network to which the computer is attached, if any, to see what other computers it can infect.

Stuxnet is ingenious. It has two major components. One intercepts valid commands being sent to the PLCs and replaces them with potentially dangerous commands generated

© 2011 Sombers Associates, Inc., and W. H. Highleyman

automatically or by remote hackers. The other secretly records what normal operations at the facility look like and plays these back to the plant operators so that it appears to them that the plant is operating normally.

Stuxnet is specifically designed to spin centrifuges such as those used in Iran's nuclear facilities out of control, potentially destroying them. If your computer is not controlling those devices, the only impact of Stuxnet is that it will propagate itself to other computers on your internal network.

How Does Stuxnet Spread?

It would be difficult to attack PLCs directly since they are not connected to public networks. Furthermore, they are generally programmed in proprietary languages optimized for device control.

Stuxnet sidesteps this problem by instead targeting the Windows-based systems that are often used to oversee SCADA operations. It enters a Windows system via an infected USB thumb drive. Specifically, Stuxnet takes advantage of special files placed on thumb drives to automatically execute itself as soon as the file is read by the operating system. Simply browsing an infected thumb drive can load Stuxnet without any additional user interaction.

These malware files are digitally signed with the private keys of certificates stolen from two different companies, JMicron and Realtek. This makes the files easily installable and undetectable for a substantial period of time. The certificates have since been revoked by Verisign.

Once installed, Stuxnet goes to work. In addition to disrupting the operation of the SCADA system (if in fact that is the role of the computer), it also checks to see if the computer is on a private network. If so, it infects other computers on the network.

It also infects any other USB thumb drive that is inserted at a later time.

Stuxnet provides connections to remote command and control servers manned by the hackers. Two servers have been identified – one in Denmark and one in Malaysia – and have been taken down as part of an international effort to disable Stuxnet.

Stuxnet's spread seems to have originated in Iran. It may have begun by giving an Iranian plant operator an infected USB thumb drive or by simply leaving a few somewhere for inquisitive people to insert it into their computers.

What is known is that Stuxnet has now spread worldwide to about 100,000 computers. Over 60% of these computers are in Iran. Next comes Indonesia and India. Only about 6% are in the Western world, primarily in the U.S., the U.K., and Australia. Most of these infections are benign.

While Stuxnet is promiscuous, the attackers have taken great care to make sure that it is only their intended targets that suffer. If the appropriate control software is not found on the infected computer, Stuxnet will erase itself on June 24, 2012.

How Does Stuxnet Work?

The first thing that Stuxnet does is to search for industrial software made by German industrial giant Siemans, a major manufacturer of control systems and the providers of the Simatic WinnCC controllers used by Iran's centrifuges. If the software exists and is properly configured, it inserts itself into the WinnCC Step7 module, which is the module that is used to reprogram the firmware in the PLCs. It then reprograms the PLCs so as to include itself in the firmware programs.

Stuxnet intercepts legitimate commands being sent from the SCADA software to the PLCs. If certain conditions are met, it replaces these commands with potentially dangerous commands. It then returns a normal status reading, indicating to the plant operators that the controlled device is operating properly when in fact it is not.

Stuxnet is incredibly targeted. It requires specific variable-frequency motors to be attached to the targeted Siemans controller. Furthermore, it attacks motors from only two manufacturers, one located in Finland and one in Iran. It monitors the frequency of these motors and attacks only those spinning between 807 Hz and 1210 Hz. When certain conditions are met, it periodically modifies these frequencies to 1410 Hz, then to 2 Hz, then to 1064 Hz. This sequence can be very damaging to the motors. Stuxnet masks the changes in rotational speed so that the plant operators are unaware of out-of-control motors.

Stuxnet exploits four previously-unknown vulnerabilities in Windows to inject its code into the PLCs. The first vulnerability allows executable code on a USB thumb drive to spread to the Windows system.

The second vulnerability allows it to spread from machine to machine over a private network and to let it report back to the attackers on the Internet when it finds a computer that is running the Siemans SCADA software.

The next two vulnerabilities let Stuxnet escalate its privilege levels so that it can inject its code into the Siemans PLCs.

Russia has expressed intense concern for Stuxnet. In January, 2011, it called on NATO to launch an investigation of Stuxnet when the worm targeted a Russian-built Iranian power plant, saying the incident could have triggered a repeat of the Chornobyl disaster, the 1986 nuclear meltdown in the Ukraine. Russia reported that Stuxnet caused centrifuges producing enriched Uranium at the Bushehr plant to spin out of control. The operators thought that the centrifuges appeared to be working properly and took no action.

Siemans has released a detection and removal tool for Stuxnet. However, deleting Stuxnet from the Windows control system does not remove it from the PLCs. Therefore, a thorough audit of the PLCs is also necessary.

Who Did This?

Conspiracy theories abound. They focus mainly on a joint effort by the USA and Israel, though all is purely conjecture. There is not a single element of evidence that links anyone to Stuxnet.

Stuxnet is unusually large for malware – about a half megabyte – and it is written in several languages, including C and C++. It is so ingenious and requires the knowledge of so many technologies that most security specialists feel that the development and testing of Stuxnet was a massive, well-funded project, comprising perhaps ten to fifteen people over six months or more. In addition, knowledge of industrial control systems was needed along with access to such systems to do quality assurance testing, again indicating that this was a highly organized and well-funded project.

Stuxnet, named after initials found in its code, is the most sophisticated cyberweapon ever created. It is a cybermissile apparently designed to take over the controls of the centrifuge systems at Iran's uranium processing center in Natanz and its nuclear reactor in Bashehr.

Several observations have led to different speculations concerning Stuxnet's origin. In 2008, Siemans cooperated with the Department of Homeland Security to identify security vulnerabilities in Siemans' process control systems used by Iran's enrichment facilities. Siemans publicly announced these flaws later at a Chicago conference. It was these security holes that were exploited by Stuxnet. Was this deliberately planned by the U.S.?

Then there are the "DaVinci Code" theories of symbology. Stuxnet contains a file named "Myrtu." This may be an allusion to the Hebrew word for Esther. The Book of Esther, one of the books in the Hebrew bible, describes a plot by Persia against the Jews. The Jews attacked preemptively and foiled the plot. Or it could be for "My RTUs," referring to the Remote Terminal Units controlled by the PLCs.

Other clues are numeric. The number "19790509" appears in the Stuxnet code. It could be a reference to the day in 1979 when a prominent Jewish Iranian businessman was executed. Another date that appears is September 24, 2007. This is the date that the Iranian president, Mahmoud Ahmadinejad, spoke at Columbia University and questioned the validity of the holocaust.

Are these clues? Were they inserted by the hackers as their signature? Or were they inserted intentionally to implicate Israel? No one knows.

In any event, many security experts believe that Israel may have developed Stuxnet, with or without the help of the United States, as an alternative to a physical attack on Iran in the hope of avoiding the consequences of world opinion to an overt military attack.

What's To Come?

Now that it has been released on the Internet for other hackers to study, Stuxnet has opened a dangerous path for others to follow. It has shown that a targeted malware worm can take control of an industrial control system. The bar has been lowered for destructive attacks on many of the basic infrastructures upon which we depend.

Summary

An illuminating video prepared by Symantic that shows the effect of Stuxnet cam be viewed at http://www.symantec.com/tv/products/details.jsp?vid=673432595001.

Computer malware has until now primarily affected PCs or the servers to which they are connected. These keep businesses running. Malware may do all kinds of software damage to a system, but it does not threaten life, limb, or property.

Stuxnet is different. It is the first malware that can infect control systems and physically destroy or disable our infrastructure. Safety systems could be switched off at a nuclear power plant; fresh water could be contaminated with sewage, the valves in an oil pipeline could be opened, causing immense contamination; railroad switches could be thrown to cause collisions; electrical substations and even an entire power grid could be taken down.

Alan Bentley, senior international vice president at security firm Lumension, said that Stuxnet is "the most refined piece of malware ever discovered" and that the worm was significant because "mischief or financial reward wasn't its purpose. It was aimed right at the heart of a critical infrastructure."

Cyber security has taken on a new importance.

Acknowledgments

The Stuxnet Sting, *Microsoft Malware Protection Center*; July 16, 2010.

The Stuxnet Worm, *Symantic*; undated.

Stuxnet is the ‘work of a national government agency”, *The Guardian*; September 24, 2010.

Clues emerge about genesis of Stuxnet worm, *Christian Science Monitor*; October 1, 2010.

Stuxnet Worm Still Out of Control, Experts Say, *Fox News*; December 9, 2010.

Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times*; January 15, 2011.

Why the Stuxnet worm is like nothing seen before, *New Scientist*; January 18, 2011.

World’s First Cyberweapon, *Discover*; January/February 2011.

German analyst says Israel’s Mossad also involved, *The Vancouver Sun*; March 4, 2011.

Stuxnet, *Wikipedia*.

© 2011 Sombers Associates, Inc., and W. H. Highleyman