News

New evidence shows Stuxnet used since at least 2007

Researchers find older Stuxnet version with different centrifuge sabotage method

By Lucian Constantin
February 26, 2013 05:25 PM ET

IDG News Service - Researchers from security firm Symantec have found and analyzed a version of the Stuxnet cybersabotage malware that predates previously discovered versions by at least two years and used a different method of disrupting uranium enrichment processes at Iran's nuclear facility at Natanz.
Stuxnet was discovered in 2010 and was considered to be the most sophisticated malware ever seen until that time. It used multiple exploits to spread, most of them previously unknown, and was the first piece of malware to target industrial control systems. Based on time stamps found in the collected Stuxnet samples, security researchers believed that it was originally created in 2009 -- until now.

The version discovered by Symantec researchers -- dubbed Stuxnet 0.5 -- was actively used in 2007 and there is evidence to suggest that it might date back to 2005, when the domain names used for its command and control (C&C) servers were first registered.

Time stamps found in the Stuxnet 0.5 code are in the range of 2001, but these are unlikely to be accurate, said Vikram Thakur, principal security response manager at Symantec, on Tuesday.

The Symantec researchers believe that Stuxnet 0.5 is the missing link between Stuxnet 1.0 and the Flame or Flamer cyberespionage malware discovered in 2012, but which is believed to predate Stuxnet.

Technical evidence suggested that Flame and Stuxnet 1.0 were built on different development platforms, but security researchers established enough similarities between the two threats in order to conclude that Stuxnet's creators had access to the Flame code base.

Stuxnet 0.5 is evidence that not only did the Stuxnet developers collaborate with the Flame developers, but that the two threats actually shared a significant portion of their source code in the beginning.

Stuxnet 0.5 is partly based on the Flame platform, which is different from the Stuxnet 1.0 platform, called Tilded, the Symantec researchers said in a research paper released Tuesday at the RSA 2013 security conference in San Francisco. "The developers actually re-implemented Flamer-platform components using the Tilded platform in later versions."
Unlike Stuxnet 1.0, the 0.5 version only exploits a single vulnerability in the Siemens Step 7 engineering software to infect systems and spread from one machine to another via infected Step 7 projects copied on USB memory sticks. The Step 7 software is used to program PLCs (programmable logic controllers) -- special digital computers that control industrial machinery and processes.

In addition to the Step 7 vulnerability, Stuxnet 1.0 also exploited zero-day vulnerabilities in Windows in order to spread on local area networks.

Stuxnet 0.5 used a different sabotage strategy from the one used in Stuxnet 1.0. According to the Symantec researchers, this early version of Stuxnet injected attack code into Siemens 417 PLCs to manipulate the valves used to feed UF6 (uranium hexafluoride gas) into uranium enrichment centrifuges.

This attack would have "caused serious damage to the centrifuges and uranium enrichment system as a whole," the researchers said.

In addition, the rogue PLC code was designed to output fake readings in order to hide the attack and trick operators into believing that everything was running as planned. These were normal readings collected by the malware during a 30-day wait period following the time of infection and were being played back during the attack.

The malicious PLC code also prevented operators from intervening and altering the state of the valves while the attack was in progress.

In comparison, Stuxnet 1.0 was designed to infect a different model of PLC called 315 that was being used to control the speed of spinning uranium enrichment centrifuges. Incomplete sequences of the 417 PLC attack code had been found in Stuxnet 1.0, but their significance was unknown until now.

It's not clear why the Stuxnet creators decided to change the attack strategy from manipulating centrifuge valves to altering their spinning speeds. It's possible that the 417 PLC attack was not delivering the desired results, but it's also possible that the attacked entity replaced the 417 PLC model, forcing the Stuxnet creators to change their attack, Thakur said.

Stuxnet 0.5 was designed to perform extensive system fingerprinting in order to make sure that it only targets specific configurations of centrifuge cascades. Based on the values found in the code and open-source information from various sources it's very likely that the target was Iran's Natanz uranium enrichment plant, Thakur said.

The version of the malware was programmed to stop contacting the C&C servers after Jan. 11, 2009, and stop spreading several months later, on July 4, 2009. The oldest version of Stuxnet 1.0 found so far was compiled on June 22, 2009, but the Symantec researchers believe that there might have been other versions between 0.5 and 1.0 that have not been discovered yet.

Despite the fact that Stuxnet 0.5 was designed to stop spreading in 2009, Symantec was still able to identify a small number of dormant infections -- copies of the malware in infected Step 7 projects -- during the past year. Almost half of them were in Iran and 21 percent of them were in the U.S.
This version of the malware far surpasses the sophistication of any malicious program that existed in 2005, when the C&C domains were registered, or 2007, when a sample was uploaded to a public malware-scanning service, Thakur said. "The mere fact of it being able to do the kind of harm to hardware as it is designed to do is simply breathtaking."

"The people behind this were very, very forward looking; very focused in what their end goal was," Thakur said. "Nobody else was even close to doing what they did at that same point in time, as far as we know."

Expert Tips for 3 Key Requirements of BYOD Network - Nemertes Video

In this video, Henry Svendblad, Nemertes Principal Research Analyst, discusses three key requirements of your BYOD network - simplicity, scalability and security, and...

Evolve Your BYOD Network - HP Financial Services Video

Watch this quick 3-minute video to find out how to keep your BYOD strategy simple without capital budget requirements.

Is Your Enterprise Wireless Network Ready for BYOD - IDC Technology Spotlight Video

In this brief 7-minute video, IDC's Rohit Mehra, Vice President for Network Infrastructure, discusses the impact of enabling BYOD on Enterprise Wireless LANs...

All Cyberwarfare Webcasts

Cyberwarfare White Papers | All Cyberwarfare White Papers

- Surviving the Business Equivalent of the Zombie Apocalypse
- The Five Big Lies the C-Suite Hears About "Going Mobile"
- New Report: Mobile Shopping Satisfaction Survey
- Five Steps to Developing a Successful Mobile Strategy
- Mobilize: A unified IT approach to the mobile workspace
- The Cisco Unified Workspace
- Resolve Performance Issues Within Your Citrix Environment
- Forrester - Managing Performance of Critical Applications
- Integrated Data Protection for VMware Infrastructure
- HP Data Protector Software Data sheet
- When Disaster Tests Your Business, Cloud Can Save It
- New Report: mPayment Scenario Planning and Recommendations
- Is Your App Getting Used? Understanding UX and Your Audience
- The Total Economic Impact Of Desktop Virtualization
- Winning Strategies for Omnichannel Banking
- Creating the Right Mobile Strategy: What You Need to Know Before You Get Started
- Forrester - Turn Big Data Inward With IT Analytics
- The Cloud Threat
- Guide to virtual server protection: HP Data Protector software
- Cloud Backup and Recovery for Virtual Server Environments