Cory Bryan

SE 4930

February 6, 2012

Stuxnet: Dissecting a Cyberwarfare Weapon

http://www.computer.org/csdl/mags/sp/2011/03/msp2011030049.html

This article, written by Ralph Langner, looks at the Stuxnet worm. Stuxnet appeared last year, and is considered to be the first cyberwarfare weapons ever. Stuxnet's goal was completely different from normal malware in that its goal was to physically destroy a target, while most security attacks are focused on stealing or manipulating information within computers.

Many people see Stuxnet as an attack on SCADA (supervisory control and data acquisition) systems, which allow for humans to monitor an industrial process, but Langner doesn't see this to be true. The SCADA system wasn't the target of the attack, but rather the industrial controllers attached to such a system were the target. Another thing Langner points out is that Stuxnet was completely stand-alone. It didn't require internet access, only contacted servers to report back on what it had compromised.

The writers of Stuxnet specifically wrote it with a specific target in mind: Iran's uranium enrichment plant. It spread mainly through USB flash drives and local networks, rather than using more conventional worm techniques. Stuxnet targeted only controllers made by Siemens, and performed a complex process to fingerprint the system using model numbers and configuration details to make sure it was on target. If the fingerprint matches, Stuxnet uploads code to the controller. Due to the lack of controller infections outside of Iran, Langner infers that this was its only target.

Stuxnet was designed to hide itself from the monitoring application and other code running on the controller. After being uploaded to the controller, it continued to allow legitimate code to be executed, and only took control occasionally. It targeted two controller models, Siemens 315 and 517. The 315 code was simple, and simply stopped legitimate code from running during a certain operational phase. The 417 code was much more complex, and acted as a man in the middle driver between the I/O and the legitimate code. The code saw good data from the I/O while Stuxnet sent invalid data.

Even with the updates provided by Microsoft for the vulnerability Stuxnet used to spread, the real vulnerability in the hardware controllers remains and won't be fixable without a new generation of controllers. Langner concludes that industrial controllers would need code signing to prevent such attacks from being carried out in the future. Another option is to check the controller for changes using a different code path, because the vender's DLL could be compromised.