Stuxnet Computer Virus

Cyber-Security Group Activity

GBA 327- CA02 Bryan Reagan

Kayla Knightly, Sage Derrig,

Eoin McAvinchey, Kristiana Hinsch

Stuxnet is a computer worm that targets PLCS which is short for programmable logic controllers. The Stuxnet virus was discovered in June of 2010 by VirusBlokAda, which is a security company. Its name has changed multiple times however, “Stuxnet” name came from keywords within the software “.stu and “mrxnet.sys. The viruses intended target was the Natanz plant. However, it ended up accidentally spreading past its intended market because of a programming error within the update. Symatex researchers discovered that a version of Stuxnet was used to attack Iran’s nuclear program. Stuxnet allegedly was traded on the black market in November of 2010, according to an anonymous source reported by Sky News.

Stuxnet was a virus used to infiltrate the Iranian nuclear power plant. This attack took place in the mid mid-2000s to access and mess with nuclear program in order to damage equipment. Researchers of the Stuxnet virus, predict that the virus first attacked five component vendors that are crucial to the Iran’s nuclear data, even though the original story is that it was imported by an infected USB drive. The bug was issued to be able to view the electrical blue prints of the Natanz plant, which controls the centrifuges to the uranium.

Stuxnet is considered a worm virus. A worm virus is able to replicate itself and spread across a network. Stuxnet would enter a Windows system and replicate itself. Then it would infect Siemans Step7 software which operates and controls equipment. Lastly it would compromise the programmable logic controllers. This allows the author to spy on and control systems such as centrifuges. It spread to other systems by entering an external USB drive and that same USB would be inserted into another computer infecting it as well. (Kushner) Stuxnet is dangerous as it can spread and move silently without the victim knowing until it is too late.

Since the existence of Stuxnet has been known for several years now, the process of removing the worm virus is quite simple. One company known for their presence in cyber-security is Symantec, which offers data loss prevention products that protect computer information and technology infrastructure (About Symantec). In addition to desktops, their products protect mobile devices, servers, embedded systems, as well as the Cloud. The Symantec Power Eraser is one of the many tools that they provide, but it is the one specifically meant for removing the Stuxnet worm. It scans the computer and removes it upon user instruction.

Once Stuxnet has been removed, users must take several steps to prevent reoccurrence (2016). First, they should keep the computer protected using programs such as Firewall and Antivirus. The number of applications running on the computer as well as the number of devices connected to it should be limited. Blocking peer-to-peer usage is another wise prevention step since sharing files is an easy way to distribute malware. Keeping browser plugins patched is also recommended. From time to time, vendors like Microsoft release service packages and security updates that are meant to correct known defects in their operating systems.

References:

Kushner, D. (2013, February 26). The Real Story of Stuxnet. Retrieved November 11, 2016, from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxne

Symantec Corporation. (2016, November 13). About Symantec. Retrieved from https://www.symantec.com/about

Symantec Corporation. (2016, November 13. W32.Stuxnet Removal. Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=3