FLAME Computer Virus

Business Info Systems and Analytics CA-01

Dr. Bryan Reagan

11/9/16

Marie Coors, Lauren Csubak, Anthony Deleva

The Flame computer virus could be considered one of the most destructive and powerful computer viruses in history. It has been connected to the Stuxnet virus, which had to ability to cause malfunctions in the nuclear equipment. The Flame virus was created by the United States and Israel in 2009 and 2010 in the hopes that they would be able to slow down Iran's ability to create nuclear weapons. This could also be considered a cyber-sabotage in trying to sabotage Iran. This bit of software would be able to hack into and monitor Iran's computers, and then send the information back to the United States. In addition to this virus, they also created another virus to get into Iran's software and cause malfunctions with the nuclear equipment. It was able to reach multiple places throughout the Middle East. It was originally created to slow down the creation of nuclear weapons in Iran, but it was also found to affect Palestinian territories, Sudan, Syria, Saudi Arabia, Lebanon, and Egypt.

The FLAME virus was first noticed by Iran when they detected the malware in their oil industry. The virus had disrupted their operations making things not work the way they were supposed to. When they investigated, they discovered the virus that had been put in place by the United States and Israel. The United States did not expect Iran to find this virus and they were thrown off by the discovery, as this virus was supposed to be undetectable. They expected the file to be huge enough and complex enough that it would be very hard to locate and hack into.

The virus was one of the most complex bits of malware ever created and it had the ability to hack into and replicate even the most highly secured networks, and then send its signals back to the creator of the virus. It is a mixture of a "Trojan" and a "worm." This means that it is harmless when it is first installed, like a Trojan, and can travel between computers or devices without a human doing anything with it, like a worm. This code had heability to activate microphones and cameras, take photos of the screen, send locations and images, makes notes of different computer patterns, collect passwords, and activate the Bluetooth system. The United States was able to control some functions of the computer through the wireless Bluetooth. In addition to being able to perform these functions, it also has the ability for the infected system to be controlled by the infector. The infector gains the ability to tweak the tools and add new functions to the programs.

Works Cited

Greenfield, R., Calamur, K., Garber, M., Sims, D., Bogart, L., Graham, D. A., . . . Thompson, M. (n.d.). A Complete Guide to Flame, the Malicious Computer Virus Ravaging Iran. Retrieved from http://www.thewire.com/technology/2012/05/complete-guide-flame-malicious-computer-virus-ravaging-iran/52949/

Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers. (n.d.). Retrieved from https://www.wired.com/2012/05/flame/

U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. (n.d.). Retrieved from https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html