Extensive summary report about symantec-w32.stuxnet dossier

Business, Company

ASSIGN BUSTER

In this article, Nicolas Falliere, Liam O Murchu, and Eric Chien detailed illustrate the attack scenario and the end purpose of Stuxnet. They speculate that “ the final goal of Stuxnet is to destroy a particular industrial control system in Iran which might be a power plant or a gas pipeline”. Via reprogramming programmable logic controllers (PLCs) to execute in a specific way, the hostile attack can be implemented. However, the attack scenario is pure surmised based on the architecture of Stuxnet. To calculate the rates and the positions of infected hosts, Symantec monitors the traffic flow of Stuxnet command and control(C&C) servers by installed a system. As a result, about 100, 000 computers are infected. “ The heart structure of Stuxnet contains a large . dll file which includes lots of various resources and exports that have all of the code to manipulate the worm and two encrypted configuration blocks”.

Stuxnet installation happened “ when the . dll file is loaded and called export 15 which is responsible for examining whether the version of Windows is compatible with the virus, the host is already infected, and any kind of antivirus systems are installed or not and assessing the privilege escalation”. After that, it chooses a unique inject process and calls export 16. Stuxnet takes advantage of the privilege of the current process to the system, a 0-day vulnerability in win32, to attack. Then, through export 16, Stuxnet use resource 242 Mrxcls. sys, “ a driver that signed with a compromised digital certificate and a driver registered as a boot start service, which would implement Stuxnet every time and acts as the main load-point”.

Next, Stuxnet collects information about the equipment connects the C&C server on port 80 by export 28 and sends some fundamental information, OS Version, Machine Name and Workgroup Name, about the infected host to the attacker. In order to avoid users from observing their own removable drive is compromised, Stuxnet can hide copies of its files. “ Also, it can propagate by copying itself over the network, removable drives, and step 7 project”. In network propagating routines, Stuxnet compromise the host by export 22 which establishes a “ Network Action” class that has five subclasses, including peer-to-peer communication, infecting WinCC computers, propagating through network shares, MS10-061 Print Spooler Zero-Day Vulnerability and MS08-067 Windows Server Service Vulnerability. In addition, the common way Stuxnet exploit in removable drive propagation is to copy itself to infected. Because most of the industrial control systems are programmed by a Windows system and not connected to the internet, they exchanged data via removable devices. As a result, Stuxnet is able to use two methods, using a vulnerability that allowed auto-execution when viewing the drive and using an autorun. inf file, to spread to and from removable drives. Moreover, Stuxnet utilizes the s7tgtopx. exe process that is used to manage a WinCC/Step7 project to propagate. “ Export 16, the main export, invokes export 2, which is responsible to link particular APIs that are used to open project files inside this process”. Via dropping resource 208 by export 17, Stuxnet can replace Simatic’s s7otbxdx. dll file which is used for handling PLC block exchange between the programming device and the PLC. Stuxnet targets the WinCC/Step7 project to get access to a PLC by installed a specific software. After the installation, Stuxnet can connect to the PLC and then reconfigure or reprogram it. That is, the PLC can be disconnected to the Windows computer and operate by itself. While PLC gets an infection, three main processes are included. Two of sequences, sequences A and B, are functionally equivalent. The third sequence is dubbed sequence C. In sequences A and B, after a PLC is found, it is checked by SDB blocks to determine whether it belongs to the type of 6ES7-315-2. When the infections start, " the DP_RECV block is copied to FC1869, and then replaced by a vicious block embedded in Stuxnet".

Stuxnet has another undermined strategy targeting S7-417 PLCs. However, the process is not complete and the PLC code, referred to as sequence C, is never purposefully copied onto a PLC or executed. The authors speculate that " the PLC code injection was active at a previous time, sequence C itself appears unfinished, contains unimplemented cases, unused code blocks, and test or debug code". This sequence is more complex than sequences A or B.

All in all, Stuxnet appears to be the most complex vicious worm in the history. " It is the first to exploit four 0-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator".