Chapter 30
Stuxnet–Tool for Zero-Day Attack

Anita Patil
https://orcid.org/0000-0002-2161-7128
Department of Information Technology, Ramrao Adik Institute of Technology, India

Swapnil Shinde
Department of Information Technology, Ramrao Adik Institute of Technology, India

Soumi Banerjee
Department of Information Technology, Ramrao Adik Institute of Technology, India

ABSTRACT

Stuxnet is a malicious code used to exploit multiple unpatched Windows vulnerabilities and infect end devices. It was very sophistically used by attackers to infect computers that are connected to specific models of Programmable Logic Controllers (PLCs) manufactured by Siemens. The stuxnet worm alters the PLCs' programming and raises a false alarm to machines, which leads to an accident. The worm uses zero-day vulnerabilities in the Windows operating system, and because of that, it remains undetected by the antivirus programs. The attacker attempts to breach the vulnerabilities in hardware systems and breaks the infrastructure, which leads to a watering hole attack. Thus, this chapter explores the different possibilities of the stuxnet-based cyber-attacks and their risk factors. The chapter represents an analysis that is performed on the different patterns of attacks, and its preventive measures are also proposed.

INTRODUCTION

Currently cyber warfare is a technology that generates harmful operations to victim nations which leads to increase cyber war situation. Many nations are trying to prevent and fight against cyber-attacks to save human lives, economy and geographical assets. Cyber operations are creating crucial condition for entire world because it directly effects on human lives. As per researcher Taddeo definition: Warfare based on certain uses of ICTs within a state-sponsored offensive or defensive military strategy aimed at

DOI: 10.4018/978-1-7998-5728-0.ch030

the immediate disruption or control of enemy resources and carried out in the information environment, with agents and targets ranging from physical to non-physical, and the level of violence of which may vary according to circumstances. Here we are focus on how one malware change the prospect of cyber security and cyber warfare. There is open security challenge to entire cyber world how could malicious things/objects change behavior to hide themselves from security measures and impacts more than expectations. Cyber Story began in 2010 when security company VirusBlokAda detected one malware that was Rootkit.Tmphider. Afterwards Symantec title as w32.Temphid and later changed the title as W32.Stuxnet. Stuxnet worm has three execution phases: i) It uses worm-script to sequentially load all payloads to perform successful attack ii) Link file automatically propagate worm script file and makes multiple copies and iii) Rootkit file hides all contents and supportive processes which is helpful to avoid the detection of stuxnet malware (Duqu, 2011).

Compare to other categories of malware objects, stuxnet did not affected computer and networks also it did not require any software requirements. Attacker identify target and only hit that target rather than releasing impact on network or computers. Attacker needs few layer of system to make an attack successful that are suspected windows operating systems, Siemens PC7, step7 and WinCC software and Siemens S7 PLCs.

Stuxnet is a malicious computer code that was first time detected in 2010. Basically, it is designed to infect the Supervisory Control and the Data Acquisition system (SCADA). The Siemens SCADA system is used to manage the working of many industrial equipment's. The Stuxnet as a cyber worm infects Programmable Logic Control system which allows the automation of electromechanical processes that are used to control machinery and industrial processes including centrifuges for spreading nuclear material. The Stuxnet is designed to exploit the Windows operating system vulnerabilities that are not auto patch. The study mainly focuses on which kind of vulnerability is susceptible to attempt cyber-attacks (Resource207, 2012).

Stuxnet worm basically explores a network via an infected USB device which goes through different steps: i. Malware or worm that executes the main signature or payload ii. An LNK file or service file (SVCHOST.exe) that automatically executes the propagated malware copies. iii. Genuine digital certificate by authenticated service provider that remains undetected by antivirus. iv. The rootkit used to hide all malicious codes and processes to bypass detection mechanisms (cv2, 2012).

In addition to this, Stuxnet also exploits a print spooler vulnerability in the Windows operating system to spread and infect all computers that use a shared printer. Other exploits attack vulnerabilities in a Windows keyboard file and Task Scheduler file through which the attacker gets control over the infected machine with administrative privileges. Stuxnet could exploit static password or default password that was hard coded by Siemens in its Step7 software. Stuxnet was able to obtain access using this password and also infect the database hosting server of Step7 which in turn infected the users and hosts connected with it. The attackers continuously try to intent on spreading infection of their payload or worm without getting detected by security applications. Stuxnet worm spreads via USB and infects the connected local area network (Hamdouni, 2017).

Unfortunately, Stuxnet was rapidly growing with the same or different format but the spreading speed is wider rather it continuously reported in different ways to get a major impact on operational programming and hardware too. From its origin to the victim it travels in a very silent situation but the impact of the attack is very dangerous. It was many time used to affect the economic zone, power plants, disaster equipment, etc. (ICS, 2017).