The computer worm Stuxnet

Hans Kristian Flaatten - hanskrfl@stud.ntnu.no

April 29, 2012

1 Introduction

This document describes the computer worm Stuxnet in detail, how it spread and what it's objective was. The document also attempts to shed some light on who could have been behind the threat and why it was made.

2 Discussion

2.1 Overview

W32.Stuxnet (Stuxnet) is a computer worm targeting industrial control systems (ICS), systems which are usually found in gas pipelines and power plants. Stuxnet's ultimate goal was to modify the behavior of the ICS by altering code in the attached programmable logic controllers (PLCs) which are used to execute, control and monitor industrial processes.

2.2 Spread

Stuxnet was first discovered in July 2010 [3] og the attack vector for the Stuxnet threat was three different Microsoft Windows vulnerabilities, two of which were zero-day exploits:

1. Shortcut vulnerability via removable drives (CVE-2010-2568) [2]
2. Windows Printer Spooler vulnerability over LAN (CVE-2010-2729) [2]
3. Remote code execution vulnerability in SMB (CVE-2008-4250) [2]

By monitoring the command and control (C&C) servers Symantec, with help from SERT and some other organizations, were able to observe the infection rate counting approximately 100,000 infected hosts as of September 29, 2010. 58% of these machines were located in Iran and 67% of these had Siemens Software installed [4].

Because Stuxnet records the time and system information for each new infection within itself; researchers were able to backtrack to the original source of infection - five organizations within in Iran. There were a total of three attack waves where a new, and enhanced, version of Stuxnet was compiled and deployed: June 2009, March 2010 and April 2010.

Stuxnet would automatically delete itself from any removable drive after three infections to further avoid detection. Nor would it attempt to install itself past the fixed date of June 24, 2012.

2.3 Architecture

In the heart of Stuxnet resides a main .dll file which contains all of the functionality necessary to control the worm. This includes C&C communication, P2P updates, infection of Step 7 projects and infection of other devices.

Stuxnet was a fully equipped Windows rootkit. Using two stolen certificates from two reputable companies in Taiwan, as well as two zero-day privilege escalation exploits, Stuxnet was able to install itself without any user intervention. In order to avoid detection Stuxnet carefully evaluated the operating system and installed security tools before attempting an installation.

2.4 Goal

Stuxnet searched for Field PGs, computers running Simatic manager used to program Siemens PLCs. Stuxnet infected all Step 7 project files using yet another zero-day exploit and was able to inserted itself as a man-in-the middle, intercepting all communication between the Field PG and the PLC. This is the first ever discovered PLC rootkit. From here Stuxnet was able to insert it's own code onto the PLC as well as masking that the PLC had been infected.

Stuxnet only affected two specific types of Siemens PLCs, namely s7-300 and s7-400, with a very specific configuration and number of attached frequency convertors.

When Stuxnet is loaded onto the PLC for the first time it stays idle for almost an entire month (26,7 days [4]) and monitors the frequency for the attached motors. When it has enough data it calculates whether the target's frequency convertors are within a certain frequency range. If they are Stuxnet changes the frequency to above and bellow the normal operating frequency casing them to misbehave and eventually causing them to fail and sabotaging the ICS.

3 Conclusion

Stuxnet takes malicious software to a whole new level. A typical malware uses one, if any, zero-day exploits - stuxnet is the first ever to use four! It is also the very first to target industrial control systems. Symantec estimates that it took 5 to 10 core developers, excluding managers etc., for a minimum of 6 months to develop Stuxnet [4].

Sabotaging the ICS by damaging the PLCs was obviously a high valued target for the attackers due to the vast amount of recourses invested in the development of Stuxnet. Since the worm did not pose any danger to computers not used for managing PLCs, and the fact that Stuxnet only affected a very specific ICS with two types of PLCs, leaves us to believe that Stuxnet was a targeted attack. The attackers must also have obtained the design documents for their target prior to mounting the attack.

When analyzing the geographical dispersion of infected hosts as well as where the initial infection we can with good certainty conclude that the Stuxnet's target was some where in Iran. A industrial facility of some kind.

The attackers showed deep internal knowledge of ICSs and PLCs which is only possible if they had direct access to this equipment in order to experiment with it and test their code on while they developed Stuxnet.

When taking into account the cost and effort it takes acquiring an ICS, as well as the cost of creating a computer worm with this level complexity and quality, it is reasonable to believe that only a state would have the recourses enough to conduct this attack.

References

[1] Symantec Security Response Team, *W32.Stuxnet*, July 13, 2010, http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

[2] National Cyber-Alert System, *Vulnerability Summary for CVE-2010-2568*, July 22, 2010, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2568.

[3] Kaspersky Lab ZAO, *Rootkit.Win32.Stuxnet.a*, September 20, 2010, http://www.securelist.com/en/descriptions/15071647/Rootkit.Win32.Stuxnet.

[4] Symantec Security Response Team, *W32.Stuxnet Dossier*, February 11, 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.