International Journal of
Science and Engineering Investigations vol. 1, issue 2, March 2012

STUXNET, DUQU and Beyond

Mohammad Faisal[1], Mohammad Ibrahim[2]
[1,2] Dept. of Computer Sciences, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan
([1] mfaisal_1981@yahoo.com, [2]ibrahimislamian@yahoo.com)

Abstract- Stuxnet is a worm (self-replicating malware) objectively to reprogram industrial control systems while reprogramming programmable logic controllers (PLCs) for the purpose to deceive the changes from the operator of the device according to the wishes of the intruder.

Keywords- *STUXNET, DUQU, SCADA, o-day vulnerabilities.*

I. INTRODUCTION

Stuxnet is a large, complex piece of worm with diverse mechanism and functionalities. It can Self-replicate, update and Spreads itself in a LAN environment and then can be executed on remote systems as well. At all it exploits the privileges and control systems vulnerabilities through which it can successfully hides its modified binary values used as a base for its root kit. Stuxnet is a challenge where security software's are based on pre- assumption that the running programs are fulfilling all the legitimate conditionality and therefore it is a reliable process going on. Furthermore if the Stuxnet code contains any similar digital certificate for the installed software's that are published for the said organization/ company then Stuxnet can carry on as much as possible and as desired for the intruder. Due to the use of 0-day vulnerabilities it make possible to replicate the worm effectively and rapidly without any alert or notification generation in the target region/system until and unless the attack is generated and launched. Main causes of its success are Intelligence sharing ,0-Day vulnerabilities, Kernel Manipulation (through stolen Digital Signed Certificates),Weakness in SCDA (Supervisory Control And Data Acquisition) Systems, Lack of proper monitoring and check points, Lack of proper policies and standards.

Stuxnet consist of the four main file .They are .LNK file, ~WTR4141.tmp, ~WTR4132.tmp, Encoded payload .dll file with 13 functions and a variety of files (like .dll, .exe, .dat, .sys, .link, .tmp).The main encrypted payload is UPX packed .dll file which is a free, portable, extensible with high performance in many executable formats. It is present in one file of the removable devices [1].

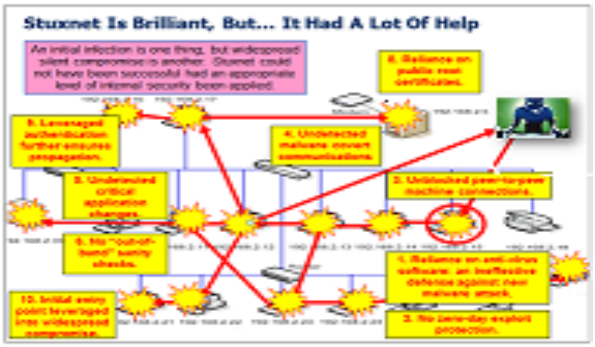

Figure 1 Stuxnet-worm-propagation-diagram-by-White Blocker Security

II. LITERATURE REVIEW

Stuxnet is operating in seven main phases. They are penetration, infection, propagation, detection avoidance, target identification, target modification, process impact. Considering the example of Step 7 Siemens software. First of all it locates and then infects the Step 7 programming station. Propagate through replacement of Step 7 DLL routines with its own. Identifying its target in the Siemens different models of PLCs i.e. (6ES7-417 and 6ES7-315-2) for specific configurations and strings. Modify the target by injecting the payload to PLC and change the process operation according to attacker wish and desire. [9]

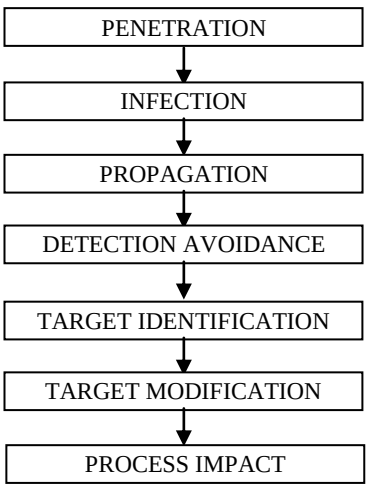

Fig 1. Phase/Control flowchart

Stuxnet targeting the SCADA (Supervisory Control and Data Acquisition) which contains control and monitoring data of critical infrastructure and PLCs information. Stuxnet reprogrammed these PLCs by performing man-in-the-middle attack between administrator and the PLCs. Interestingly Stuxnet also report to the administrator/operator the normal report [2].

Stuxnet was initially designed to exploits (Siemens S7-315 and S7-417) but later on Stuxnet also exploiting the hard-coded passwords of the Siemens Step 7 software which is categorized as CVE-2010-2770 vulnerability. Then Stuxnet can access the databases as a legitimate user even can block the system by changing the original password [3].

Stuxnet defeated many security assumptions like SCADA and digital certificates. Although it is a normal practice to keep the SCADA offline to make it secure. But while copying data to these systems through any mean evoke the capability of the worm to replicate and engulf the system through its notorious designs.

Secondly the use of digital certificates makes Stuxnet as legitimate users. Early versions of Stuxnet used certificates of Realtek Semiconductor systems while later versions using certificates from JMicron Technology Corporation [3].

Table 1 Source www.eset.com

Vulnerabilities	**Target**
CVE-2010-2568 (MS10-046)	Remote code execution
CVE-2010-2729 (MS10-061)	Print spooler services
CVE-2010-2743 (MS10-073)	Privileges elevation
CVE-2010-2772-Siemens	Default password
CVE-xxxx-xxxx (MS-xx-xxx)	Scheduler Task
CVE-2008-4250 (MS08-067)	Server Services

Stuxnet is operating in two modes they are user-mode and kernel-mode. In the user mode the Stuxnet injects its own code to the running processes and over its installation algorithms. Stuxnet is injecting its code by two different ways: (a) When a module is loaded into a current process, and (b) When the module is injected into a new process.

While Injecting code into a current process to avoid being detected by antivirus software the malware first allocates a memory buffer in the calling process for the module to be loaded then it hooks any of the given functions

ZwMapViewOfSection,

ZwCreateSection,

ZwOpenFile, ZwClose, ZwQueryAttributesFile, ZwQuerySection.

Then it calls desired exported function. At last it calls Free Library API function to free loaded library. To hook the functions specified above, the malware allocates a memory buffer for code that will dispatch calls to hooked functions, overwrite some data in header of the image with the code that transfers control to the new functions, and hook the original functions by overwriting its bodies.

While when injecting code into a new process the malware requires the module to be executed in a newly created process it uses different approach. To achieve this Stuxnet either creates a host process or replaces the image of the process.

Depending on the processes present in the system the mal ware chooses any of the host process lssas.exe (system process),avp.exe (Kaspersky), mcshield.exe (McAfee VirusScan),avguard.exe (AntiVir Personal Edition),bdagent.exe (BitDefender Switch Agent),UmxCfg.exe (eTrust Configuration Engine from Computer Associates International),fsdfwd.exe (F-Secure Anti-Virus suite),ccSvcHst.exe (Symantec Service Framework),ekrn.exe (ESET Antivirus Service Process),tmproxy.exe (PC-cillin antivirus software from TrendMicro).

The mal ware enumerates processes in the system and if it finds a process whose executable image has a name present in this list, and which meets certain criteria, then it is chosen to be a host for the module of the Stuxnet.

While in the kernel mode it can successfully hides its malicious .LNK files for its survival after reboot. The worm has some root kit functionality, as during infection of the system it drops and installs two kernel-mode drivers that allow it to hide files and inject code into process in the system using either MrxCls.sys or MrxNet.sys. as these modules are not packed or protected with any packer or protector [4].

Stuxnet used different methods for its propagation as Table 2.

Table 2 Source IBM Research group.

Procedure	**Propagation**
Autorun.inf	USB
.LNK	Explorer.exe
Sharing Networks	Replication
Print Spooler	copy In printer server
Network path	Via Folder conficker
Default password	WinCC SQL Server
Step 7 project files	Auto execution initially

III. STUXNET2 OR DUQU

Stuxnet2 or DUQU all the same emerged in the global scenario on October 18, 2011, which is primarily a remote

access TROJAN. In this version of Stuxnet the attacker now change its nature form WORM TO TROJAN or a remote access Trojan (RAT).

The threat is named Duqu [dyü-kyü] as it generates files through prefix "~DQ". W32.As it is a intimidation almost matching to Stuxnet, although with an entirely diverse rationale.

Three main files of DUQU are a driver, a main DLL, and an encrypted configuration file that contains the time the infections occurred. The injection process hides Duqu's activities and may allow certain behaviors to bypass some security products.

Almost there are twelve variants of DUQU. There is a little functional difference between variants. Mainly, the names of registry key and files used are different and unnecessary code has been removed. DUQU variants are jminet7.sys, cmi4432.sys, nfred965.sys, nfred965.sys, nfred965.sys, nred961.sys, adp55xx.sys, adpu321.sys, iaStor451.sys, allide1.sys, igdkmd16b.sys, igdkmd16b.sys.

Main characteristics of DUQU are that its executables share some code with the Stuxnet worm, there is no ICS specific attack code in the Duqu, the malware used a valid digital certificate, the malware is designed to self-delete after 36 days, DUQU is used as a key logger to store information that can be used for future attacks.

Duqu can be traced by any of the following indications like unexpected connections, Unknown drivers in %System%\Drivers\. •, "FILTER" has unknown hex data for any value• "Display Name", "Description", and "key name" all match•, drivers signed by unknown publishers that expire on August 2, 2012, Recent.pnf files in %Windir%\INF:• Have no ASCII strings inside• , Unexpected scheduled tasks or job files., An Event Log entry matching An Event ID of 0xC0002719/ 3221235481•, May have the following narrative:• DCOM was incapable to correspond with the system name by means of any of the configured protocols [6]

DUQU is using both HTTP and HTTPS for its communication with command and control server. DUQU using different proxies while launching attacks on the command and control servers. Configuring the servers to forward all the traffic on port 80 and port 443.at the end the attackers are capable to update its executables, ex-filtrate the internal information of the system to the remote server of the DUQU in the form of .jpg files to misguide the network communication.[6]

To avoid DUQU detection the threat creates a local file in the compromised system which can be used as a local command and control system for it. The threat connects to this file on a peer-to-peer connection receiving the commands and updates from this file. As the life time of the threat is 36 days by default but if not detected by the administrator's threat can extends its lifetime by downloading additional features from its main command and control server through this folder. However if the compromised system is shutdown the threat will remove itself automatically before its expiry [6].

According to the given similarities and differences (updates/changes given) between Stuxnet and DUQU we can observe that DUQU is the successor of the Stuxnet threat. Both composed of multiple modules, installing their own root kits to hide their activities, using drivers that are digitally signed (DUQU using C-Meia/Stuxnet using Realtik and JMicron), decrypting their secondary modules, decrypt their DLLS for its injection into the system process, their functionality is controlled over an encrypted configuration file, updating their self from command and control servers. But lifetime and key logger files are defined in DUQU only. [7]

IV. FRAMEWORK FOR SOLUTION

If the vital infrastructures are to be protected and sheltered, afterward the possessor and operatives required to identify that their control structure are currently in the intention of classy assaults and necessitate to regulate their security agendas consequently. In exacting, security plans required to be classified as defensive/proactive and offensive/reactive measures.

A. PROACTIVE Measures

- Implementing ISA-99 and IEC 62433 Security Standards. As no protective security posture is perfect, so dividing the network into segments to limit the consequences of compromise. Dividing the Control Network into Security Zones like:

1. SIS ZONE-Safety Integrated System.
2. PLC ZONE-Basic Control.
3. Supervisory or HMI ZONE-Human Machine Interface.
4. Process Information or Data Historian zone.
5. Information Technology Network zone.

- Jamming the traffic of the Protocols Used by Stuxnet particularly three protocols HTTP, RPC and in Siemens systems, MSSQL traffic should be managed.
- Blocking Outbound HTTP Traffic through which Stuxnet utilizes to connect reverse to its control hub via the Internet.
- Establish ICS-appropriate intrusion detection equipment to identify attacks and elevate an apprehension when equipment is compromised or at threat of compromise.
- Implement firewalls that are competent of profound packet scrutiny of key SCADA and ICS protocols.
- Creating a Hashed value for each instruction to be processed.
- Intermediate security policies/protocols/ports should be defined for host-to-host and zone-to-zone communication requirements.
- Install, activate and sustain at utmost valuable ICS-appropriate security expertise and practices.

- Implementation of strong patch management systems on device level can reduce attacks to the lowest level.
- By implementing security awareness programs in the organization such as to get better the traditions of industrial security amid management and technical groups.
- Consider the security of all possible infection pathways (removable media, file transfer, portable equipment, internal/external connections, wireless (Wi-Fi, Bluetooth) connections, serial and parallel interfaces) rather any one focus.
- Introduction of intrusion detection mechanisms (e.g., device specific honey pots)
- System hardening (e.g., hardware lockdown by disabling unnecessary I/O interfaces)
- Implementation of software restriction policies and updating ANTI virus regularly.
- All default username and passwords should be disabled.
- Through penetration testing, classify and accurate probable vulnerabilities by this means declining the probability of a triumphant attack.
- Replace the windows operating systems with LINUX operating systems.

B. REACTIVE Measures

- Review the system logs in all computer hosts and network appliances.
- Scheduled Revision of Setup test and validation systems and later on patch the system vulnerabilities as well.
- All non-essential communication should be suspended to contain the attack after the attack is launched.
- Incident response team should be maintained to re-establish the essential operations while recovering from the attack.
- Forensic procedures should be handled with care to maintain the integrity of the data within the infected system.

These developments to get better defense-in-depth situation for control systems are desirable immediately. Waiting for the next worm may be too late.

REFERENCES

[1] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier Version 1.4. Symantec Corporation" , February 2011, 7.

[2] Eric Byres, CTO Byres Security Inc, "The Future of Critical infrastructure Security. "

[3] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs Small Wars Journal ", April 2011, smallwarsjournal.com

[4] Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho, "Stuxnet Under the Microscope" Revision 1.31,Symantec Corporation www.eset.com

[5] Jon Larimer, "An inside look at Stuxnet, Senior Researcher," IBM X-Force, 2010

[6] Symantec security response, "W32.Duqu The precursor to the next Stuxnet Version 1.4 " (November 23, 2011)

[7] Peter Szor Sr. Director of Research, "Duqu– Threat Research and Analysis McAfee Labs, "October 2011

[8] Joe Weiss, CSFI member and CSFI STUXNET Project contributor "Cyber Security Forum Initiative (CSFI) Preliminary Stuxnet Report V1.0"

[9] Eric Byres et al, "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems, Tofino Security-Abterra Technologies", February 22, 2011