

Stuxnet Threat Analysis in SCADA (Supervisory Control And Data Acquisition) and PLC (Programmable Logic Controller) Systems


Zulfikar Sembiring¹

¹Program Studi Teknik Informatika, Universitas Medan Area, Indonesia

ABSTRACT

This journal is devoted to the analysis of the Stuxnet malware known as (Win32 / Stuxnet) which has suddenly caught the attention of virus researchers in the last three years. In this journal, an overview of attacks targeted at the SCADA (Supervisory Control And Data Acquisition) system and PLC (Programmable Logic Controller) will be explained as the main targets of Stuxnet. Besides that, it will also explain the history of the development / variant of Stuxnet and the prevention that can be done against the Stuxnet threat.

Keyword: malware, Stuxnet, viruses, SCADA, PLC

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Corresponding Author:

Zulfikar Sembiring,
Program Studi Teknik Informatika
Universitas Medan Area
Jl. Kolam No 1 Medan Estate, 20223, Indonesia.
Email : zulfikarsembiring@staff.uma.ac.id

Article history:

Received Aug 20, 2020
Revised Aug 30, 2020
Accepted Sep 03, 2020

1. INTRODUCTION

Recently, the world's first virus for industrial control systems - seismic networks (Stuxnet) has attracted widespread attention. Because this virus uses the Siemens control system (SIMATIC WinCC / Step7) to infect gaps in data acquisition and control systems (SCADA), to understand the impact of this new virus, the Stuxnet Virus version 0.5, is expected to operate from 2007 to 2009 (Matrosoft et al., 2010).

The main purpose of this virus is to access Simatic WinCC SCADA, which is used as an industrial control system and is tasked with supervising and controlling industrial, infrastructure, or facility-based processes. Similar systems are used extensively in refineries, power plants, large communications systems, airports, shipping and even military installations globally. The target of the attack and the areas infected by this virus (mainly Iran) (Albright, Brannan, & Walrond, 2011).

Iran started its nuclear program in the 1950s. Iran has been slow to revolutionize the program. A few years later, the new leadership continued, in 2002, the revolution started and Iran declared that it would build 2 nuclear facilities. Iran increased Uranium processing in 2003 and stopped temporarily in 2006 because the IAEA did not approve it. However, in early 2007 Iran continued to cultivate Uranium until now (Falliere, Murchu, & Chien, 2011).

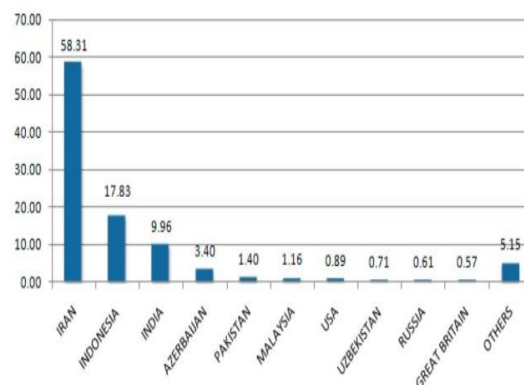


Figure 1. Distribution of Infection by Geographical

Israel first completed 3 years of its nuclear program before Iran finished building its nuclear. Israel has confirmed that Iran will stop enriching uranium, using a viral attack to paralyze Iran's nuclear power before the Stuxnet virus struck in 2012. The US government says the attack was not created by the United States. Stuxnet Virus attack is more effective than a military attack.

Stuxnet is a computer virus that was discovered in July 2010. This malware targets Siemens software and devices running on the Microsoft Windows operating system. This isn't the first time a cracker has targeted industrial systems. However, it is the first malware found stalking and disrupting industrial systems, and the first to include a programmable logic controller (PLC) rootkit.

The virus initially spreads blindly, but loads a highly specialized malware load designed to target only the Siemens Supervisory Control And Data Acquisition (SCADA) system set up to control and monitor specific industrial processes. Stuxnet infected PLCs by changing the Step-7 software application used to reprogram the device.

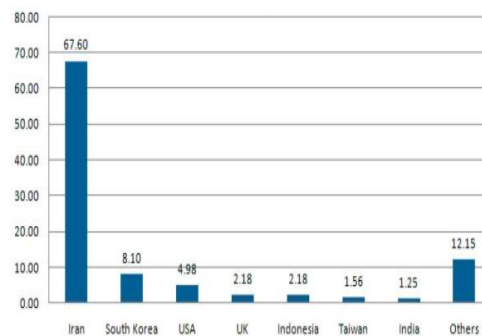


Figure 2. Percentage of Stuxnet hosts infected with Siemens Software

A different variant of Stuxnet has targeted five Iranian organizations, possibly the widely suspected target of uranium enrichment infrastructure in Iran. Symantec noted in August 2010 that 60% of infected computers worldwide are in Iran. Siemens said on November 29 that it had caused no damage to customers, unless Iran's nuclear program, which uses Siemens embargoed equipment obtained in secret, had suffered damage due to Stuxnet. Russian computer security firm Kaspersky Lab concluded that the sophisticated attack could be carried out "with state support" and it has been suggested that Israel and the United States may have been involved (Kursner, 2013).

Symantec logs events that occur as a result of W32.Stuxnet. namely: On November 20, 2008, Trojan.Zlob was discovered using the file extension LNK which was later identified as Stuxnet. Then in April 2009 the security magazine Hakin9 released a detailed, remote executing code that became a virus on the service coil inside the printer. Later identified as MS10-061. June 2009, Stuxnet appeared and was shown as harmless as MS10-046. Has no sign of a moving virus file. January 25, 2010, a sign of the movement of the Stuxnet virus with a certificate belonging to the semiconductor company Realteck. March 2010, the first variation of the Stuxnet virus exploits MS10-046. June 17, 2010 VirusdBlokada reported W32.stuxnet (name RookitTmphider). The report stated that the virus used something vulnerable to attack in the process of its .LNK shortcut file inside the propagate / reproduce command (later identified as MS10-46). July 13, 2010, Symantec said it was detecting W32.Tempid (previously detected as a Trojan). July 16, 2010, reported a security issue for susceptible viruses within the Windows Shell which allows executing remote code (2286198). It's protection that is easily exposed in the process of .LNK shortcut files. Semiconductor company Relteck withdrew the certificate. Tempid (previously detected as a Trojan). July 16, 2010, reported a security issue for susceptible viruses within the Windows Shell which allows executing remote code (2286198). It's protection that is easily exposed in the process of .LNK shortcut files. Semiconductor company Relteck withdrew the certificate. Tempid (previously detected as a Trojan). July 16, 2010, reported a security issue for susceptible viruses within the Windows Shell which allows executing remote code (2286198). It's protection that is easily exposed in the process of .LNK shortcut files. Semiconductor company Relteck withdrew the certificate.

July 17, 2010, Eset identified a new movement of stuxnet, a token with a certificate from technology company JMicron. 19 July 2010, Siemens reported that they had reported Malware infecting the Siemens WinCC SCADA system. The system detects it as W32.Stuxnet. July 19, 2010, Symantex records Stuxnet commands and their working controls. July 22, 2010, the Jmicron Tecnology company,

Stuxnet Threat Analysis in SCADA (Supervisory Control And Data Acquisition) and PLC (Programmable Logic Controller) Systems (Sembiring)

revised the certificate. August 2, 2010, Microsoft took issue with MS10-46, which created a shortcut to the vulnerable Windows shell. August 6, 2010, Symantec reported that Stuxnet was able to enter and decode an industrial Control system using a PLC. September 14, 2010, reported that MS10-061 stuck to the vulnerable printer coil identified by Symantec in August. Microsoft reported 2 other pervasive features identified by Symantec in August. September 30, 2010, Symantec presented in the Virus Bulletin and released a comprehensive review of Stuxnet analysis.

2. LITERATURE REVIEW

Stuxnet is malicious software, or malware, that commonly attacks industrial control systems created by the German company Siemens. Experts say the virus can be used for spying or sabotage. Siemens said the malware spreads via infected USB thumb drive memory devices, exploiting a vulnerability in Microsoft Corp.'s Windows operating system. Malware software attack program through Supervisory Control and Data Acquisition System, or SCADA. The system is used to monitor automatic power generation - from its food and chemical facilities to power plants (Gollmann, 2010).

Analysts say the attackers will deploy Stuxnet via thumb drives because many SCADA systems are not connected to the Internet, but have USB ports. Once a virus infects a system, it quickly establishes communication with the attacker's server computer so that it can be used to steal corporate data or control SCADA systems, said Randy Abrams, a researcher with ESET, a private security company who has studied Stuxnet (Karnouskos, 2013).

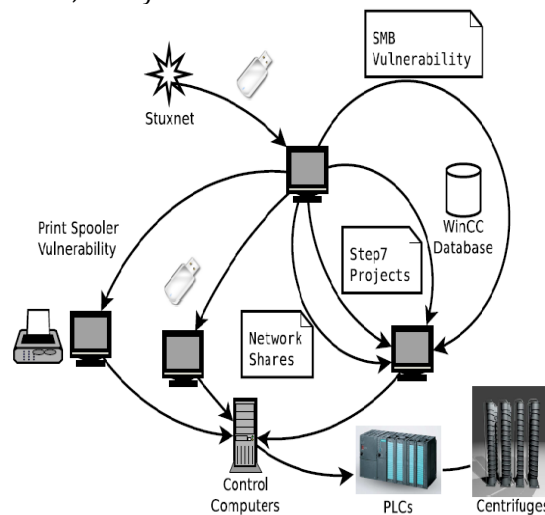


Figure 3. Stuxnet Deployment

A. On Data and Applications (Siemens Simatic WinCC SCADA and PCS7 DCS)

Most computer automation systems Iran and other countries are manufactured under the Siemens SCADA brand (supervisory control and data acquisition) these systems are the main target. If all infected IPs are cleaned, the threat remains, the virus has not disappeared. (Symantec)

The main purpose of this worm is to access somatic WinCC SCADA, which is used as an industrial control system and is tasked with supervising and controlling industry, infrastructure, or facility-based processes. This worm can infiltrate the computer control system made by Siemens machines which are used to control dams, power plants, mines, and other industrial facilities.

B. On the Operating System

Stuxnet reportedly only attacks SCADA (mostly oil and gas companies), especially on computer users in Iran, but its development has also attacked computers that don't use SCADA, including Windows Vista and 7.

- Windows Server Service / RPC (MS08-067), with the same technique as the worm conficker, using a Windows system that is not updated, the worm will easily infect computers.
- Windows shell icon handler / LNK (MS10-046), Stuxnet is a worm that exploits this vulnerability. By making use of shortcut files. Worm infects computers easily.

- Windows print spooler / spoolsv (MS10-061). According to the observations, vaccincom computers have problems with the print server or printer share. And apparently, the Stuxnet worm also exploits the print spooler in action
- Windows win32K layout module (MS10-073), one of the new loopholes of the window that stuxnet has successfully passed by exploiting the w32k.sys file and injecting it, the Stuxnet worm can have administrator rights and easily infect computers.
- Windows task scheduler. This gap is used to penetrate new systems from Windows Vista and Windows 7, namely UAC (user account control). By creating a task schedule file so that it can easily infect computers.

C. On Computer Networks

Stuxnet doesn't just rely on the help of users to spread it. For this, stuxnet also uses two other security flaws which can be exploited remotely in the local network. The first relates to the Microsoft printer spooler, while the second targets a vulnerability in the server service (MS08-067).

Pint Spoiler: This security vulnerability was originally published in Hackin9 Magazine during 2009. When the printer is shared on the system, users can "print" (read and write) files in the "System %%" directory. The exploitation of this security vulnerability occurs in two stages. the first consists of depositing the files "winsta.exe" and "sYsnullevent.mof" in the "Windows \ System32" and "Windows \ System32 \ WBEM \ mof" directories respectively. The second stage in exploiting this vulnerability consists of executing the "sysnullevent.mof" script. This file, in MOF ("manage object format"), is used to force Windows to run the code contained in the "winsta.exe" file. The execution of this script is automatic. This is because the MOF files in the "Windows \ System32 \ WBEM \ mof" directory are automatically compiled by "mofcomp.exe" to record the WMI context that triggers script execution. This security vulnerability was fixed by Microsoft which added a series of checks before allowing documents to be printed.

Server Service: Finally, Stuxnet exploits the security vulnerabilities of MS08-067 in the Server service. This vulnerability, which at that time was extensively exploited by Conficker1 Downadup, was here to be used to store files in shared directories of type C \$ or Admin \$. Execution of this file has been mutually planned, using the \ task scheduler. it appears that the shell code used by the malware to perform these two actions is relatively advanced, in contrast to that used by Conficker. This security vulnerability was fixed by Microsoft when it published bulletin MS08-067.

The exploitation of these security vulnerabilities allows the malware to distribute itself both on the local network and, more widely, on all systems to which users can connect removable storage media. Once installed on a Windows system, malware has several functions that allow it to work as part of a network. Among other things, the malware installs an RPC server which allows it to communicate various items of information with other infected systems on the LAN.

D. On the PLC (PROGRAMMABLE LOGIC CONTROL)

Stuxnet was the first malware found lurking and disrupting industrial systems and the first to include a Programmable Logic Controller (PLC) rootkit. Stuxnet infected PLCs by changing the step-7 software application used to reprogram the device. PLCs are commonly referred to as mini computers that store the operational code of industrial devices. The code itself was programmed by a Windows-based computer, stuxnet poisoned the computer-based programming, to then enter the "wrong" code according to the attacker's desire (Lubis et al, 2019).

Code-The code entered by Stuxnet itself attempts to disrupt the speed of the centrifuge from the nuclear reactor enrichment process. Stuxnet instructs the machine to spin faster or slower than normal, thereby destroying the enrichment output. After finding the right target then replace the s7otbxdx.dll library which is used to communicate between the PLC and the Step7 software. Inject malicious code into PLC, Execute periodic attacks on centrifuge by changing rotor speed Sabot centrifuge. (Lubis et al., 2019)(Prayudani et al., 2019)

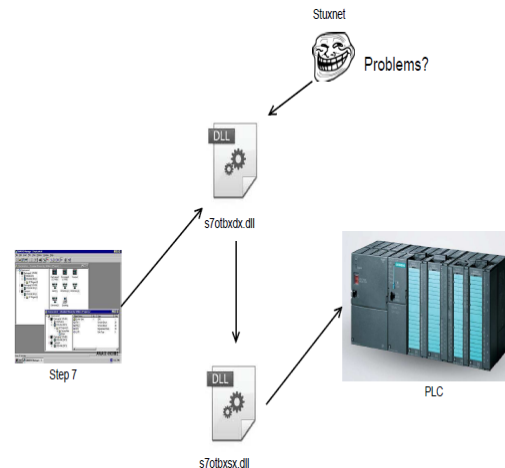


Figure 4. The Stuxnet image wraps a library used to communicate with PLCs

3. RESULTS AND DISCUSSION

Prevention that can be done on the Windows operating system is by using several antiviruses, as follows:

A. On Kaspersky Antivirus

Kaspersky antivirus can detect Stuxnet into several variants including viruses (worms) and trojans (rootkits). Following are precautions for trojan variant (Rootkit.Win32.Stuxnet.a) [7]. This is a rootkit designed to run malicious code in the user's system and run on the NT kernel driver. This rootkit is 26,616 bytes in size. This rootkit copies itself as the file % System% \ drivers \ mrxcls.sys.

The Rootkit creates the following registry keys which are used when the operating system is rebooted:

Table 1. Key Table Regstri on Kaspersky Antivirus
Kunci Registri Yang Diiptkan Rootkit Pada Sistem Operasi Reboot

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls]	"ImagePath"="\\??\%System%\Drivers\mrxcls.sys"
"Description"="MRXCLS"	"Start"=dword:00000001
"DisplayName"="MRXCLS"	"Type"=dword:00000001
"ErrorControl"=dword:00000000	
"Group"="Network"	
Rootkit ini juga menciptakan file lain yaitu :	%WinDir%\inf\oem6C.PNF
%System%\drivers\mrxnet.sys dikenal sebagai	%WinDir%\inf\oem7A.PNF
Rootkit.Win32.Stuxnet.b dengan ukuran 17400 bytes. Serta	%System%\drivers\mrxcls.sys
menciptakan kunci registry yang digunakan pada saat reboot :	%System%\drivers\mrxnet.sys
	%WinDir%\inf\mdmcpq3.PNF
	%WinDir%\inf\mdmmeric3.PNF
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet]	<path to winccproject>\<project_name>\GraCS\cc_tag.sav
"Description"="MRXCLS"	<path to wincc project>\<project_name>\GraCS\db_log.sav
"DisplayName"="MRXNET"	
"ErrorControl"=dword:00000000	
"Group"="Network"	
"ImagePath"="\\??\%System%\Drivers\mrxnet.sys"	Serta menciptakan beberapa kunci registry yang diaktifkan pada saat komputer reboot.
"Start"=dword:00000001	
"Type"=dword:00000001	
dan juga menciptakan beberapa file yaitu :	[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS]
%windir%\inf\mdmcpq3.pnf - 4633 bytes.	"NextInstance" = "1"
%windir%\inf\mdmmeric3.pnf - 90 bytes.	[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000]
%windir%\inf\oem6c.pnf - 323848 bytes.	"Class" = "LegacyDriver"
%windir%\inf\oem7a.pnf - 498176 bytes.	"ClassGUID" = "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
Rootkit ini juga menyebar via removeable media (USB) dengan beberapa file berikut ini :	"ConfigFlags" = "0"
"Copy of Shortcut to.lnk"	"DeviceDesc" = "MRXCLS"
"Copy of Copy of Shortcut to.lnk"	"Legacy" = "1"
"Copy of Copy of Copy of Shortcut to.lnk"	
"Copy of Copy of Copy of Copy of Shortcut to.lnk"	
~wtr4132.tmp	

~wtr4141.tmp

Untuk penjegahannya jika komputer yang tidak menggunakan antivirus yang up to date maka disarankan untuk menghapus file dengan langkah berikut ini :

- 1) Hapus file rootkit yang asli (lokasi akan tergantung pada bagaimana program awalnya menembus mesin korban).
- 2) Hapus kunci registry
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls]
- 3) Hapus file
%System%\drivers\mrxnet.sys
%System%\drivers\mrxcls.sys
%windir%\inf\mdmcpq3.pnf
%windir%\inf\mdmeric3.pnf
%windir%\inf\oem6c.pnf
%windir%\inf\oem7a.pnf
- 4) Reboot komputer
- 5) Menonaktifkan tampilan ikon di file manajer untuk menghindari infeksi berulang.
- 6) Hapus beberapa file berikut ini pada removeable media jika ada :
"Copy of Shortcut to.lnk"
"Copy of Copy of Shortcut to.lnk"
"Copy of Copy of Copy of Shortcut to.lnk"
"Copy of Copy of Copy of Copy of Shortcut to.lnk"
~wtr4132.tmp
~wtr4141.tmp

Selanjutnya pencegahan untuk varian virus (Worm.Win32.Stuxnet.e) sebagai berikut : Program jahat ini dirancang untuk menyerang komputer yang menjalankan visualisasi proses sistem Siemens WinCC. Ketika program ini diaktifkan maka akan menciptakan file

```
"DisplayName" = "MRXCLS"
"ErrorControl" = "0"
"Group" = "Network"
"ImagePath" =
"\??\C:\WINDOWS\system32\Drivers\mrxcls.sys"
"Start" = "1"
"Type" = "1"
[HKLM\SYSTEM\CurrentControlSet\Services\MRxCls\Enum
]
"0" = "Root\LEGACY_MRXCLS\0000"
"Count" = "1"
"NextInstance" = "1"
[HKLM\SYSTEM\CurrentControlSet\Services\MRxNet]
"Description" = "MRXNET"
"DisplayName" = "MRXNET"
"ErrorControl" = "0"
"Group" = "Network"
"ImagePath" =
"\??\C:\WINDOWS\system32\Drivers\mrxnet.sys"
"Start" = "1"
"Type" = "1"
[HKLM\SYSTEM\CurrentControlSet\Services\MRxNet\Enum]
"0" = "Root\LEGACY_MRXNET\0000"
"Count" = "1"
"NextInstance" = "1"
```

```
"Service" = "MRxCls"
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000\Control]
"*NewlyCreated*" = "0"
"ActiveService" = "MRxCls"
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET]
"NextInstance" = "1"
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000]
"Class" = "LegacyDriver"
"ClassGUID" = "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
"ConfigFlags" = "0"
"DeviceDesc" = "MRXNET"
"Legacy" = REG_DWORD, 1
"Service" = "MRxNet"
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000\Control]
"*NewlyCreated*" = "0"
"ActiveService" = "MRxNet"
[HKLM\SYSTEM\CurrentControlSet\Services\MRxCls]
"Data" = " ...m}.....$z...#.....Q*..j..O..i|.;...u...3H
...../...!..uh.....{...rG.....2...86kl..o...J...K...AK...$...7.
B..j.....<1.....{d.H.L..Tbt..1...~.i.B...o..F.h..b.....3l...VT..z
{w.....^.<c.>`.....7..W...kA.m.9q.....}...pF.$...`r....4RK}
_..5...>x.....Z.OZV...../...+?IA...qgi..iw.....}&Z\F...
(..K.:<.....!O.n.....S...1.8{7.....L.3...h1- .Pd
{9.....l*...%C..
('s.E.S.....(..Z.....%...LHFY@.0...v.....j.."
"Description" = REG_SZ, "MRXCLS"
```

- 3) Hapus beberapa file berikut :
%System%\winsta.exe
%System%\wbem\mof\good\sysnullevnt.mof
%WinDir%\inf\oem6C.PNF
%WinDir%\inf\oem7A.PNF
%System%\drivers\mrxcls.sys
%System%\drivers\mrxnet.sys
<path to wincc project>\<project_name>\GraCS\cc_alg.sav
<path to wincc project>\<project_name>\GraCS\cc_tlg7.sav
%WinDir%\inf\mdmcpq3.P<F
%WinDir%\inf\mdmeric3.PNF
<path to wincc project>\<project_name>\GraCS\cc_tag.sav
<path to wincc project>\<project_name>\GraCS\db_log.sav
- 4) Reboot komputer
- 5) Menonaktifkan tampilan ikon di file manajer untuk menghindari infeksi berulang.
- 6) Hapus beberapa file berikut ini pada removeable media jika ada :
"Copy of Shortcut to.lnk"

Untuk penjegahannya jika komputer yang tidak menggunakan antivirus yang up to date maka disarankan untuk menghapus file dengan langkah berikut ini :

1) Hapus file rootkit yang asli (lokasi akan tergantung pada bagaimana program awalnya menembus mesin korban).

2) Hapus beberapa kunci registry berikut ini :

```
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS]
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000]
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000\Control]
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET]
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000]
[HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000\Control]
[HKLM\SYSTEM\CurrentControlSet\Services\MRxCls]
[HKLM\SYSTEM\CurrentControlSet\Services\MRxCls\Enum]
[HKLM\SYSTEM\CurrentControlSet\Services\MRxNet]
[HKLM\SYSTEM\CurrentControlSet\Services\MRxNet\Enum]
```

"Copy of Copy of Shortcut to.lnk"

"Copy of Copy of Copy of Shortcut to.lnk"

"Copy of Copy of Copy of Copy of Shortcut to.lnk"

~wtr4132.tmp

~wtr4141.tmp

B. On McAfee antivirus

This antivirus can detect Stuxnet into several variants of Stuxnet! Lnk and stuxnet [8]. For treatment please use the following instructions for all supported versions of Windows to remove the threat and other potential risks:

1. Disable System Restore.
2. Update to DAT file for detection and deletion.
3. Run a complete Scan

Modify the system Registry and / or INI files for system startup setup, if that doesn't work then use the recommended engine and the DAT (or higher) combination.

Table 2. Microsoft Recovery Console Settings table and for cleaning MBR

<i>On windows XP</i>	<i>On Windows Vista and 7</i>
<ul style="list-style-type: none"> • Insert the Windows XP CD into the CD-ROM drive and restart the computer. • When the "Welcome to Setup" screen appears, press R to start the Recovery Console. • Choose compromised Windows installation and provide administrator password • 'Fixmbr' command issue to restore the Master Boot Record • Follow the instructions on the screen • Reset and remove the CD from the CD-ROM drive. 	<ul style="list-style-type: none"> • Insert the Windows CD into the CD-ROM drive and restart the computer. • Click "Repair Your Computer" • When the System Restore Options dialog appears, choose Command Prompt. • Issues 'bootrec / fixmbr' command to restore the Master Boot Record • Follow the instructions on the screen • Reset and remove the CD from the CD-ROM drive.

C. On Symantec antivirus

Symantec Antivirus can detect Stuxnet into several variants including worm (W32.Stuxnet) and virus (W32.Stuxnet! Ink) [9]. Prevention can only be done by updating the antivirus database.

D. On ESET antivirus

ESET Antivirus can detect Stuxnet into W32 / Stuxnet variants [10]. Prevention can only be done by updating the antivirus database.


4. CONCLUSION

Stuxnet is malware that attacks the Siemens control system (SIMATIC WinCC / Step7) to infect gaps in data acquisition and control systems (SCADA). The main purpose of this virus is to access Simatic WinCC SCADA, which is used as an industrial control system and is tasked with supervising and controlling industrial, infrastructure, or facility-based processes. From the gap in the SCADA system, the threats that can occur in data and applications (Siemens Simatic WinCC SCADA and PCS7 DCS), Windows operating systems, computer networks, spoolers, server services, on PLC devices (PROGRAMMABLE LOGIC CONTROL). As for prevention that can be done at this time only use a few

REFERENCES

- Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet malware and Natanz: Update of ISIS December 22, 2010 report. *Institute for Science and International Security*, 15, 739883-3.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6), 29.
- Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5), 544-554.
- Karnouskos, S. (2011, November). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*(pp. 4490-4494). IEEE.
- Kushner, D. (2013). The real story of stuxnet. *ieee Spectrum*, 3(50), 48-53.
- Lubis, A. R., Lubis, M., & Listriani, D. (2019, August). Big Data Forecasting Applied Nearest Neighbor Method. In *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)* (pp. 116-120). IEEE.
- Lubis, A. R., Prayudani, S., & Lubis, M. (2019, November). Analysis of the Markov Chain Approach to Detect Blood Sugar Level. In *Journal of Physics: Conference Series* (Vol. 1361, No. 1, p. 012052). IOP Publishing.
- Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). Stuxnet under the microscope. *ESET LLC (September 2010)*.
- Prayudani, S., Hizriadi, A., Lase, Y. Y., & Fatmi, Y. (2019, November). Analysis Accuracy Of Forecasting Measurement Technique On Random K-Nearest Neighbor (RKNN) Using MAPE And MSE. In *Journal of Physics: Conference Series*(Vol. 1361, No. 1, p. 012089). IOP Publishing.
- <http://www.xmco.fr/actusecu.html>
- <http://tekno.kompas.com/read/2011/01/17/10224487/awas.stuxnet.juga.ancam.windows>.
- <http://securelist.com>

BIOGRAPHIES OF AUTHORS

	<p>Name: Zulfikar Sembiring Address: jalan Melur Komp. Pemda Tanjung Morawa No telp: 081221214686 e-mail: zulfikarsembiring@staff.uma.ac.id</p>