PROTECTION OF DATABASE IN MACHINE INDUSTRY AND DEFENSE OF CYBER ATTACK WITH ANTIVIRUS AND FIREWALL PROTECTION

UDC: 004.7:004.492
Original scientific paper https://doi.org/10.18485/aeletters.2019.4.2.4

Miroslav Spasic[1], Djordje Dihovicni[2]

[1] GLM RS Company, Pancevacka 36, Zrenjanin, Republic of Serbia
[2] Technical College, Bulevar Zorana Djindjica 152a, Belgrade, Republic of Serbia

Abstract:
The main objective of this paper is to show the technology to protect computer systems using firewall technology and through the configuration of firewall, construct defence and protection of the database of the mechanical system engaged in the auto industry which create pipe for exhaust systems on cars by using various techniques, tools, methods, and testing of the software of the firewall and anti-virus. For security reasons, it is necessary to create a script file for anti-virus system and firewall, and rules in order to handle with the database when it is updated.

ARTICLE HISTORY
Received: 12.05.2019.
Accepted: 10.06.2019.
Available: 30.06.2019.

KEYWORDS
Firewall, anti-virus, Phase logic system, database, mechanical system

1. INTRODUCTION

Computer viruses have appeared in 1981. The first computer virus was Elk Cloner. Elk Cloner virus was created by Rich Skrenta. The virus has infected the operating system Apple II computer and occasionally written message: "It will get on all your disks. It will infect your chips. Yes its Cloner. "In addition, this virus was able to copy on a floppy diskette.

Computer network ie. Internet network is used to connect, communicate, or sell. It can be concluded that computer crime can be divided into different levels of abuse. Thoughts on internet crime, crime in electronic commerce, crime in network communications. This paper describes the protection of computer systems using firewall technology and virus protection]. How firewall technology keeps intruders, viruses and thus protects data without using a firewall bring the computer system in a state of free attacks. Software firewall, packet filtering, proxy services, malware code, configuration. Firewall, virtual private network, tested programs, criteria firewall [1-3]. Regardless of what type of firewall is chosen, one thing is certain, if some customer connect to the Internet from a PC or laptop, it is necessary to have firewall protection [4].

Firewall is a protective safety system which is located between the local and public network i.e. Internet, and its role is to protect confidential information from unauthorized users by making the ban and block intrusion into the system.

Antivirus protection is now one of the most important system of protection measures in the software environment, when it is matter of protection of data on computers or larger systems in a company. Today, no computer should be without antivirus protection and Firewall protection. Antivirus protects the company computer from malicious software, malware and worm, while also could not function without antivirus firewall protection that protects access to malicious software and blocks it before accessing the information of system data.

Firewall Technology (eng. Firewall) are much changed over the years, since it first appeared on the market at the beginning of the 90s. The first firewalls were simple devices for packet filtering. Since then, they have become more advanced as far as the filtering capabilities, but also added some new features, for example such as state full firewall, Virtual Private Network - VPN), intrusion detection systems, authentication communications and virtual firewall. One of the incentives for the development of additional services in the

CONTACT: M. Spasic, e-mail: gimnasticar94@gmail.com
© 2019 Published by the Serbian Academic Center

protective walls, was a major expansion of services on the Internet that brought with them a large amount of network security problems [5-6].

2. FUZZY LOGIC AND APPLICATION IN MECHANICAL ENGINEERING

With the help of the method of neural network emerged Antivirus as a system for the protection of devices (computers, phones, tablets, large and small corporate companies which are used to exchange data and individual files). On neural networks is performed the requests that are easy to perform in the case of man, but are difficult for machine, wherein require a separate detached resource capacity, in the case of antivirus protection computer code required resources and virtual memory RAM of processor cores (CPU Threads). Fuzzy logic is used for commercial and logical application and can be applied in the management of machines and supplies of goods, and does not have to give accurate but rather acceptable and logical explanations, and helps when appeared not clear the state of engineering. Fuzzy logic works with the levels of possible inputs to reach a value of final output, Fig.1.

Common logical block that computer can understand, takes the precise input and produces a particular output as it is true (TRUE) or FALSE (FALSE), which is equivalent to the human answer YES (YES) or not (NO).

Lotfi Zadeh has found fuzzy logic and noticed that the difference between the computer and the adoption of human decisions, comprises the domain preferably between YES (YES) or not (NO) [7].

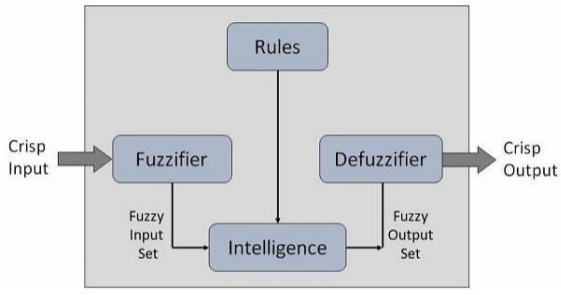

Fig.1. Fuzzy logic System

3. ANTIVIRUS, STRUCTURE AND APPLICATION

Computer viruses mostly consist of two parts:

- Self coded part-provides reproduction;
- Load - which can be harmless or dangerous.

Some Viruses consist only of self coded part, work and have no payload. The names can be used as the following characters: AZ, az, 0-9, _, $,%, -. & # 38;, #, where no distinction is made between small-capitalization [8-9].

Anna Kournikova or VBS / Onthelfy virus is virus of e-mail type, created by Jan de Wit by using Visual Basic programming language. Infection with the virus started in February 2001. The virus arrived in e-mail. Content of an e-mail was as follows: ,, HI! This Check! "On the attached Fig.2 is clearly seen as it looked the e-mail. Kornikova Virus is shown in the picture below and the way it looks when the virus attacks.

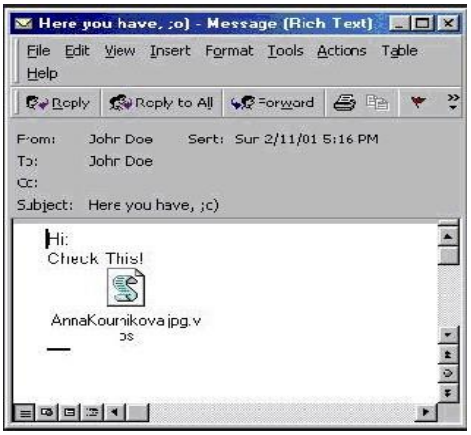

Fig.2. Kournikova Virus

The virus copies itself to the registry file, and enable continuous operation itself, as it is shown down below:

if month(now) =1 and day(now) =26 Then

WScriptShell.run "http://www.dynabyte.nl",3, false end if

The virus copies itself to the Windows directory:

Set WScriptShell = CreateObject("WScript.Shell")

WScriptShell.regwrite "HKCU\Software\OnTheFly", "Worm made with vbswg1.50b"

Checks whether Microsoft Outlook is installed in the client:

Set FileSystemObject = CreateObject("scripting.filesystemobject")

FileSystemObject.Copyfile WScriptfullname, FileSystemObject, GetSpeacialFolder(0) & "\AnnaKournikova.jpg.vbs"

If Microsoft Outlook is installed, and if it contains the e-mail address, it sends itself to all found addresses.

Anyway virus controls the current date, if the date is January 26 on in this case opens the following Web address, www.dynabzte.nl.

In order to defend the company, must be protected in order to prevent the virus from spreading further [10].

4. CREATION OF DATABASE ANTIVIRUS SCRIPT FILE

In this part of the paper it will be shown the way how it is created the script files, and antivirus protection.

In the first line of the script's header, it could be found information about the Engine version (ev), GUI version (gv), and the Log version (lv). This data might be used to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered. The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). The items should be marked for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

4.1 Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*), as it is shown down below:

*- \SystemRoot\System32\smss.exe *4725**

*- C:\Windows\system32\svchost.exe *FD08**
*+ C:\Windows\system32\module32.exe *CF8A**
a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

4.2 Loaded modules

This section lists currently used system modules.
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
In this example the module khbekhb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

4.3 TCP connections [11]

This section contains information about existing TCP connections.

- Active connection: 192.0.0.1:30606 -> 192.168.14.1:55320, owner: ekrn.exe
- Active connection: 192.0.0.1:50007 -> 192.168.14.1:50006,
- Active connection: 192.0.0.1:55320 -> 192.168.14.1:30606, owner: OUTLOOK.EXE
*- Listening on *, port 135 (epmap), owner: svchost.exe*
*+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System*
When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

4.4 UDP endpoints

This section contains information about existing UDP endpoints.

04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

4.5 DNS server entries

This section contains information about the current DNS server configuration.

+ 192.168.14.1:85
- 192.168.14.50:2

Marked DNS server entries will be removed when the script is executed.

4.6 Important registry entries

This section contains information about important registry entries.

** Category: Standard Autostart (3 items)*
HKLM\SOFTWARE\Microsoft\Windows\Current Version\Run
-HotKeysCmds=C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
HKCU\SOFTWARE\Microsoft\Windows\Current Version\Run - Google Update =

"C:\Users\antoniak\AppData\Local\Google\Updat\ GoogleUpdate.exe" /c
** Category: Internet Explorer (7 items) HKLM\Software\Microsoft\Internet Explorer\Main*
+ Default_Page_URL = http://thatcrack.com/

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

4.7 Services [12]

This section lists services registered within the system.

- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup: Automatic

- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup: Manual

The services marked and their dependent services will be stopped and uninstalled when the script is executed.

4.8 Drivers install

This section lists installed drivers.

- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot

- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual

When the script is executed, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

4.9 Critical files

This section contains information about files that are critical to proper function of the operating system.

** File: win.ini*

- [fonts]
- [extensions]
- [files]
- MAPI=1
** File: system.ini*
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
** File: hosts*
- 127.0.0.1 localhost
- ::1 localhost

The selected items will either be deleted or reset to their original values.

4.10 Scheduled tasks

This section contains information about scheduled tasks.
c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
c:\users\admin\appdata\local\google\update\googleupdate.exe
c:\users\admin\appdata\local\google\update\googleupdate.exe
c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
c:\users\admin\appdata\local\google\update\googleupdate.exe /c
c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent

5. CREATE DATABASE FIREWALL AND SCRIPT FILE

The process is pretty simple. Everything firewall-related in Server 2008/Vista / Server R2/ Windows 7, is managed through the HNetCfg.FwPolicy2 COM object, so. First it is defined some hash tables to convert codes to meaningful text, and a function to translate network profiles to names. So the same like on the home network [13].

```
$fw=New-object –comObject HNetCfg.FwPolicy2 ;

Convert-fwprofileType $fw.CurrentProfileTypes

returns "Private"

$FWprofileTypes= @{1GB="All";1="Domain";
2="Private" ; 4="Public"}
$FwAction    =@{1="Allow"; 0="Block"}
$FwProtocols  =@{1="ICMPv4";2="IGMP";6="TCP"
```

```
;17=”UDP”;41=”IPv6”;43=”IPv6Route”;
44=”IPv6Frag”;
47=”GRE”;
58=”ICMPv6”;59=”IPv6NoNxt”;60=”IPv6Opts”;112=
”VRRP”; 113=”PGM”;115=”L2TP”;

”ICMPv4”=1;”IGMP”=2;”TCP”=6;”UDP”=17;”IPv6”=
41;”IPv6Route”=43;”IPv6Frag”=44;”GRE”=47;

”ICMPv6”=48;”IPv6NoNxt”=59;”IPv6Opts”=60;”VR
RP”=112; ”PGM”=113;”L2TP”=115}
$FWDirection

=@{1=”Inbound”;
2=”outbound”; ”Inbound”=1;”outbound”=2}

Function Convert-FWProfileType
{Param ($ProfileCode)
$FWprofileTypes.keys | foreach –begin
{[String[]]$descriptions= @()} `


-process {if ($profileCode -bAND $_) {$descriptions
+= $FWProfileTypes[$_]} } `

–end {$descriptions}
}
```

The next step is to get the general configuration of the firewall; the Windows 7 machine is still on the defaults, and the result looks like this

```
Active Profiles(s) :Private
Network Type Firewall Enabled Block All Inbound
Default In Default Out
Domain          True          False Block     Allow
Private         True          False Block     Allow
Public          True          False Block     Allow
```

The Code is:

```
Function Get-FirewallConfig {
$fw=New-object –comObject HNetCfg.FwPolicy2
"Active Profiles(s) :"

+ (Convert-fwprofileType $fw.CurrentProfileTypes)
@(1,2,4) | select @{Name=“Network
Type”     ;expression={$fwProfileTypes[$_]}},
@{Name=“Firewall
Enabled” ;expression={$fw.FireWallEnabled($_)}},
@{Name=“Block All
Inbound”;expression={$fw.BlockAllInboundTraffic(
$_)}},
@{name=“Default
In”;expression={$FwAction[$fw.DefaultInboundAct
ion($_)]}},
@{Name=“Default Out”
;expression={$FwAction[$fw.DefaultOutboundActio
n($_)]}}|
        Format-Table -auto
}
```

Finally comes the code to get the firewall rules. One slight pain here is that the text is often returned as pointer to a resource in a DLL, so it takes a little trial and error to find grouping information.

The other thing to note is that a change to a rule takes effect immediately, so a group of rules can be enabled easily as [14-16]:

```
Get-FireWallRule -grouping "@FirewallAPI.dll,-
29752" | foreach-object {$_.enabled = $true}
```

```
Function Get-FireWallRule
{Param ($Name, $Direction, $Enabled, $Protocol,
$profile, $action, $grouping)
$Rules=(New-object–
comObjectHNetCfg.FwPolicy2).rules
If ($name)          {$rules= $rules | where-object
{$_.name    –like $name}}
If ($direction) {$rules= $rules | where-object
{$_.direction  –eq $direction}}
If ($Enabled)      {$rules= $rules | where-object
{$_.Enabled    –eq $Enabled}}
If ($protocol)     {$rules= $rules | where-object
{$_.protocol  -eq $protocol}}
If ($profile)      {$rules= $rules | where-object
{$_.Profiles -bAND $profile}}
If ($Action)       {$rules= $rules | where-object
{$_.Action    -eq $Action}}
If ($Grouping)     {$rules= $rules | where-object
{$_.Grouping -Like $Grouping}}
$rules}
```

Since this the rules aren’t the easiest thing to read it is usually piped the output into format.

```
Get-firewallRule -enabled $true

Sorted direction,applicationName,name

format-table -wrap -autosize -property Name,
@{Label=”Action”;
expression={$Fwaction[$_.action]}},
@{label="Direction";expression={ $fwdirection[$_.
direction]}},
@{Label=”Protocol”;
expression={$FwProtocols[$_.protocol]}} ,
localPorts,applicationname
```

If it is necessary to create a rule from scratch it is good habit to create a rule object with New-

object –comObject HNetCfg.Fwrule, then pass it to the add method of the Policy object's rules collection. In this way, it is created a database for the firewall.

6. CONCLUSIONS

First and foremost is that today in the modern world, more and more people use the Internet. To protect against malicious software such as viruses or malware, it is important to do three basic steps: the first step is to buy licensed antivirus software, install it on the computer and activate the license, the second step is to buy a firewall device and configure it in the company in order to access their data securely, at the end it is necessary to connect with antivirus software. Firewall protection wall is implemented through the server data.

In this way the workers in firm engaged in the auto industry which create pipe for exhaust systems on cars, and trucks can now safely use their data, database, backup and share files. In addition to all this taking into account the basic protection for companies in engineering industries, as necessary, in addition to purchasing hardware and software to enhance the program, the programmer must create additional script. In the first step script defined codes to identify the virus, then the line of code to prevent viruses at the end of the script. Apart scripts for antivirus, it is important to create a script for a Firewall device to protect firm so the hackers could not reach important data and they could not access the data. In this script it is defined the rules by which the whole system will work through a firewall. In this way our database for automobile industry is protected. Finally it is created a healthy and stable protection for the safe use of databases within the company and a very strong defence against malicious software and malicious threats.

REFERENCES

[1] D. Pleskonić, N. Maček, B. Djordjević, M. Crić, "Security of Computer Systems and Network" Book Preview, ComSIS 4 (1), 2007: 77-92.

[2] A. Horváth, 100% PC Protection. *Computer Panorama Ltd.*, Budapest, 2004.

[3] I. Kashefi, M. Kassiri, A. Shahidinejad, A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities. *Research and Applications*, 3 (2), 2013: 585-591.

[4] I. Palinkaš, A. Ašonja, E. Desnica, E. Pekez, Application of computer technologies (CAD/CAM systems) for quality improvement of education. *ANNALS of Faculty Engineering Hunedoara - International Journal of Engineering*, 14 (1), 2016: 179-184.

[5] J. Aycock, Computer Viruses and Malware. *Springer US*, Vol.22, 2006. https://doi.org/10.1007/0-387-34188-9

[6] J. Black, P. Rogaway, Ciphers with Arbitrary Finite Domains, RS Data Security Conference, Cryptographer's Track, Lecture Notes in Computer Science. *Springer*, Vol.2271, 2002.

[7] A.L. Mark, The little book of email viruses. *American Eagle Publications Inc.*, 1995.

[8] http://www.tutorialspoint.com/ (Downloaded 20.05.2019.)

[9] Dj. Dihovicni, M. Medenica, Fuzzy support model for long pipelines by using DB2 approach. *Applied Engineering Letters*, 2 (2), 2017: 76-83.

[10] P. Gregory, Computer Viruses for dummies. *Wiley Publishing Inc.,* 2004. pp.10-40.

[11] A. Gildas, J. Pascal, O. Philippe, Computer System Security. *CRC Press*, Paris, 2004.

[12] A. Ašonja, D. Mikić, E. Desnica, Adamović, Ž, Justifiability of Execution of Serbian Teleservice in Industry, IV International Conference Industrial Engineering And Environmental Protection 2014 (IIZS 2014), 15th October, 2014, Zrenjanin, Serbia, pp.379-382.

[13] R.S. Baghla, H. Monga, Method & Implementation of Data Flow. *Applied Engineering Letters,* 1, (4), 2016: 105-110.

[14] J. Kis, I. Szegedi, Vírushatározó, Cédrus Kiadó Kft., Budapest, 1992.

[15] M.D. Hester, Computers and Ethics in the Cuban Age. *By Pearson*, Belgrade, 2009.

[16] K. Kenan, Cryptography in the Database. *Symantec Press*, 2006.

This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License (CC BY-NC 4.0)