ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Methodology of Malware Analysis, Tools and Technique for windows platform – RAT Analysis

Nayan Zalavadiya[1] Dr. Priyanka Sharma[2]

[1]M. Tech cyber Security, Department of Information Technology, Raksha Shakti University, Ahmedabad, India

[2]Professor, Department of Information Technology, Raksha Shakti University, Ahmedabad, India

ABSTRACT: Now a days internet threats are increasing day by day at the faster rate, which makes injection of malware inside the system a very easy process. Through malware, we can access the system in the way in which we want, can make desirable changes in the malicious manner, which will eventually make the security of the system a questionable concern. Therefore we will try to explore malware types, tools, techniques and will emphasize on analysis of particular malware which is remote access Trojan (RAT). RAT is very harmful malware because with the help of this malware we can access the remote system for malicious activity.

KEYWORDS: Malware analysis, Remote Access Trojan, malicious code, Trojan, virus, worm, spyware,Static Malware analysis, Dynamic Malware analysis, System Threats

I. INTRODUCTION

With the advancement of rural and urban life,Internet is becoming an essential part of the day to day life of people on the globe. With the help of internet one can avail many services just with the help of few clicks. The rate of netizens are increasing by leaps and bounds and hence the secure access to internet is becoming the major concern. The Internet has developed gradually from a basic network of communication to an interconnected set of information sources which helps in establishing a new platform for interactions, marketing and for selling of products and services. Online banking or advertisement of different services and products are the examples of the commercial services of the Internet. Same as in the physical world, there are various people on the Internet with evil-minded intents that attempts to enhance themselves by taking advantage of legitimate users whenever money is involved in the process. Malware is the software which has malicious intent can be used by attackers to accomplish their goals.

II. WHAT IS MALWARE

Malware stands for malicious software, which is programmed to damage or to gain access to a computer system without the knowledge of the owner of the system. Viruses, Worms, Trojan, Key loggers and Spyware are the examples of mostly used malware. In simple words we can define malware as a Software that “intentionally achieve the harmful goal of an attacker” and it is commonly mentioned as malicious software or malware. Terms, such as “worm”, “virus”, or “Trojan horse” are used for classification of malware that shows similar malicious behaviour.

A bot is a malicious code of malware which is remotely-controlled and infects the Internet-connected computer system. This bot enables an external entity, which is known as bot master, to remotely control and access the infected system. The set of machines that are controlled by the bot master is called a botnet. The attacker can take help from the bot master for spamming purpose in which the attacker might send spam emails containing links to a manipulated and infected web page. When the user will open this malicious link it might unknowingly install a spyware component which in return will collect personal information, such as credit card numbers, debit card numbers and online banking credentials. By using these stolen credentials one can misuse it by purchasing goods and services online. The cybercriminal will make money even at the cost of revealing personal information of the victim. With the increased use of the Internet and the number of attached hosts, it is now very much possible for a sophisticated attacker to infect thousands of hosts within a short span of time after releasing the malware into the victim computer [1].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

III. MALWARE CLASSIFICATION

The malwareclassification is cumbersome process. Malware can be classified in various classes and categories which generally are categorized according to their propagation processes and their reactions which is achieved on the infected system which depends on designing and development process of malicious program. The following diagram shows the various types of malware.

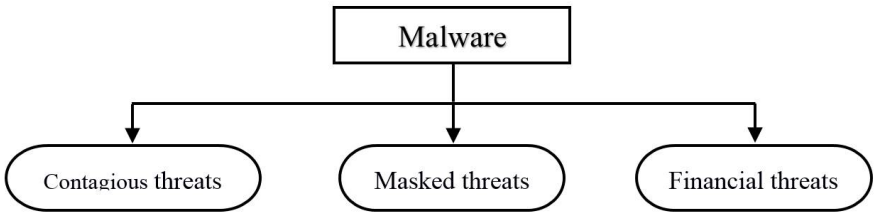


Fig. 1 Classification of Malware

I. Contagious Threats:

TABLE I CONTAGIOUS THREATS CLASSIFICATION AND DESCRIPTION

Malware	Characteristic	Mode of Functioning	Damage caused
Virus	A form of malware that takes unauthorized control of the infected computer and cause harm without the knowledge of the user	A Viruses program hidden within another harmless program such as executable file and its self-replicating capability into other program and spread the infection from one computer to another.	Performance degradation and Cause DOS (Denial of service)
Worm	Worms are standalone malicious software that can operate independently and don't hook itself to propagate	They exploit the security vulnerability by using computer or network resources and spread themselves via storage devices such as USB devices, communication media such as Email	Consume very large amount of memory of systems resources and Network performance issues

II. Masked Threats:

TABLE II MASKED THREATS CLASSIFICATION AND DESCRIPTION

Malware	Characteristic	Mode of Functioning	Damage caused
Trojan	Deadly piece of malware that hidden itself and behaves as a legitimate program to takes unauthorized control of the computer or system	Trojan does not self-Replicate instead Downloaded or copy through user interaction such as down loading a file from the internet or other device	Steal password or login details, Digital money theft, Modify/delete files, Monitor user activity
Backdoors	Bypasses the normal security controls and give the attacker to unauthorized access	Installed through program or any other malicious activity	Modify and delete system file and monitor system activity
Adware	Provides advertisers with information about the users browsing habits, thus allowing the advertiser to provide targeted add	Adware spread through website	Clickjacking, Phising or create malicioue activity using browser
Rootkits	Rootkits are the masking techniques for malware, basically designed to malicious intent of the program	Can be installed through a software exploit or by a trojan	Steal password or Install Keyloggers

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

III. Financial Threats:

TABLE III FINANCIAL THREATS CLASSIFICATION AND DESCRIPTION

Malware	Characteristic	Mode of Functioning	Damage caused
Ransomware	Ransomware is software designed to block access to a computer system until a sum of money is paid	Ransomware spread and delivered through social engineering and user interaction, opening a malicious email attachments clicking on a malicious link within an email or on a social networking site	Ransomware is malware for data kidnapping, Encrypts the victim's data and limits users from accessing their system
Spyware	Spyware track of user's activity without their knowledge and send back the sensitive information to attacker	Can be installed with other software such as freeware or dropped by Trojans	Sniffing network interface, Digital certificate, Encryption keys and other sensitive information.
Keylogger	Keylogger secretly record keystrokes	Can be installed by another malicious program or when a user visited a infected site	Capture sensitive information such as username, password, credit card number or online banking details

IV. MALWARE ANALYSIS

Malware analysis means a process of determining the functionality and purpose of the given malware sample which can be a virus, worm, or Trojan horse. For the effective detection technique of malicious codethe below described hierarchy should be considered [1].

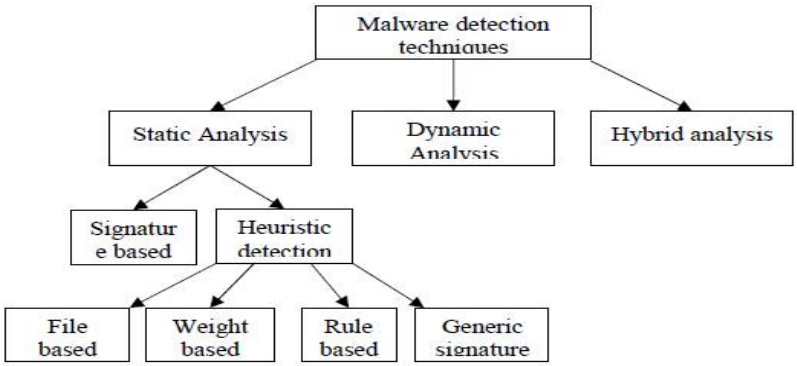


Fig. 2Classification of Malware Analysis and Detection techniques

I. Static analysis:

Static analysis can be described as analysing of the software before its execution. The static analysis is performed at the pre- execution time. On different representation of a program, static analysis can be performed. If the source code of the program is available, then with the help of static analysis tools the developer can find memory corruption flaws and can determine the correctness of models for a given system.

Various techniques are used for static malware analysis:

- File fingerprinting[1]
- Extraction of hard coded string[1]
- File format[1]
- Anti-Virus scanning[1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Packer detection[1]
- Disassembly[1]

A. Signature based detection technique:

Signature based detection technique is also known as pattern matching or string or mask or fingerprinting technique. A signature is a sequence of bits which is injected in the application program by malware writers, which uniquely identifies a particular type of malware. For detection of a malware in the code, the malware detector will search for a previously specified signature in the code.

B. Heuristic detection technique:

This technique is also known as proactive technique. There are many similarity between the signature based technique and heuristic detection technique, with a slightdifference that is instead of searching for a particular signature in the given code which is performed in signature based technique now in heuristic detection ,the malware detector will searchfor the commands or instructions that are not present in theapplication program. The main advantage of this technique is that with it becomes easy to detect new variants of malwarethat had not yet been discovered [2].

II. Dynamic analysis:

Dynamic malware analysis is also called as the analysis of infected file during its execution. During the dynamic analysis process, the infected files are analysed in simulated environment, something like a virtual machine. Dynamic analysis is not performed in real environment.

Mainly two basic approaches are followed for dynamic malware analysis:

- *Analysing the difference between defined points*: In this approach, thegiven malware sample is analysed for a certain period of time and afterwards the modifications are made to the system and again the malware isanalysed with respect to the initial system state. In this approach, the behaviour of malware is stated in the Comparison report [1].
- *Observing runtime-behaviour:* In this approach,malicious program which launches the malicious activities are monitored during runtime by using a specialized tool [1].

III. Hybrid analysis:

Hybrid analysis technique is the combination of both static analysis and dynamic analysis. It follows a very simple procedure in which it first checks for any malware signature available in the code, if the inspection process shows any malware signature present in the code thenit will monitor the behaviour of the code [2].

V. MALWARE ANALYSIS TOOLS

TABLE IV BRIEF OVERVIEW OF DYNAMIC ANALYSIS TOOLS

Dynamic Analysis Tools	Description
OllyDbg	OlldyDbg are the tools used to perform debugging/reverse engineering to malware
Regshot	Regshot is tools that are used to help analyze the registry
RegMon	Monitor operation on registry
FileMon	Monitor file operation
TCPView	Displays all TCP and UDP open connections and the process that opened and is using the port
TDIMon	Logs network connectivity, but does not log packet contents
Ethereal	Packet Scanner that capture packets and supports the viewing of cotents/payload
Comodo Instant Malware Analysis	Comodo Instant Malware Analysis is a malware sandbox created specifically for automatic malware analysis

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

TABLE V BRIEF OVERVIEW OF STATIC ANALYSIS TOOLS

Static Analysis Tools	Description
Process Monitor	Process Monitor is a program that monitors and displays all activities within the system in real-time
Process Explorer	Process Explorer is a program that monitors the processes that are currently in the system path of the computer
Dependency Walker	Dependency Walker is a program that performs the scanning modules on 32 bit or 64 bit programs
IDA Pro	The Interactive Disassembler (IDA) is a disassembler program.
BinText	BinText is a program which is capable of searching and display character strings from a binary file
Anubis	Anubis is a malware sandbox created specifically for automatic malware analysis
PEview	PEview is tools to display the structure and content of the Portable Executable
Md5deep	md5deep is a set of programs to compute MD5, SHA-1, SHA-256 on an arbitrary number of files
PeiD	Tools for detecting packed/obfuscated techniques
Exeinfo PE	Tools for detecting packed/obfuscated techniques
RDG Packer	Tools for detecting packed/obfuscated techniques
D4dot	Tools to remove obfuscated .Net Reactor technique
UFX	Executables into assembly instructions
Proc Dump	Dumps code from memory
Virustotal.com	VirusTotal.com is a free online scan service that analyses suspicious files using 40+ Anti-virus applications
ApateDNS	ApateDNS is a tool that is able to find out the IP address which is contacted by the malware
Wireshark	Wireshark is a program that can take the data contained in the packet network for analysis malware
Virtualbox / VMWare Workstation	It is virtual machine that is used as a place to run the malware

Sandboxes: For executing untrusted malicious programs in safe environment sandbox security mechanism is used. Use of sandbox helps in providing an environment in which "real" physical systems are safe. It comprises virtualized environments in such a way that ensures that if the malware is being tested it will function normally

TABLE VIMALWARE ANALYSIS SANDBOX TOOLS

Cuckoo	Anubis	IObit Cloud
Malwr	CWSandbox	Norman Sandbox
GFI Sandbox	ThreatExpert	Comodo MA
Joe Sandbox	BitBlaze	ViCheck

VI. MALWARE CATEGORIES

I. Encrypted Malware

The concept of encryption is used in this approach to prevent the designing of Antivirus Scanners which is based on signature.Encrypted malware has two important part that is –(1) Encrypted main body and(2) Decryptor. Different key is used every time when an encrypted malware is created and the key shouldbe different from its signature. The disadvantage of this approach is that the antivirus scannerscan easily detect malware as the same code pattern is present in the decryptor [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

II. *Oligomorphic Malware*

The advanced version of encrypted malware is oligomorphic malware. Thousands of new malwares are created every time when the malware authorschanges the decryptor. But still, with the help of its signature it can bedetected, as decryptor can replicate itself finite number of times [2].

III. *Polymorphic Malware*

The polymorphic malware has many similarity with oligomorphic malware, with a minute difference that is,infinite number of decryptor are generated by using different obfuscation techniques. Every time when the decryption is performed the basic function ofpolymorphic malware remains the same, only the code changes. Mutation Engine (ME) toolkit is used in order to change non-obfuscated code topolymorphic code. With each iteration, one part of the code remains the same, hence it can beeasily detected by Antivirus Scanner [2].

IV. *Metamorphic Malware*

New malware which is different from the previous malware is created at the time of each iteration and this malware is known as metamorphic malware. This type of malware can easily pass through AVS (Anti-Virus scanner) because AVSscanner is incapable in matching the signature of this malware. Metamorphic malware are not packedmalware, therefore, they never leave any traces in the memory that is uniquesignature related to the malware, as these signatures are not left in the memory no signature matching process can be accomplished[2].

VII. WHAT IS RAT

RAT is one type of Trojan which is widely known as Remote Access Trojan. RAT is a program which is used by intruders or attackers to control of the victim's computer and after gaining access to victim's computer attacker will perform various malicious activities. The below diagram describes the complete malware family which shows the various types of malware and classification of RAT malware:

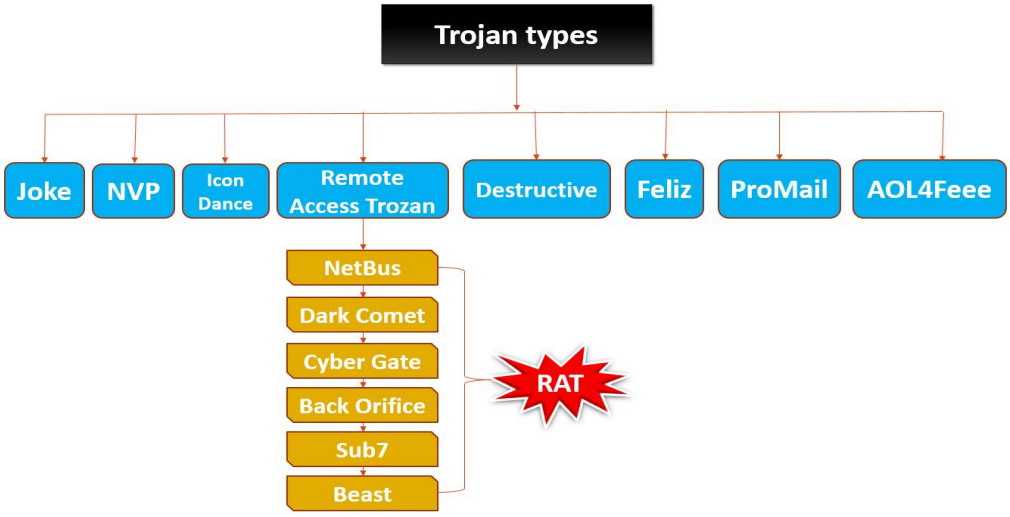


Fig. 3Classification of Different types of Trojan

Basically there are two types ofworking approach for Remote Access Trojan:

I. *Local Network (Within Network)*
- Net Bus

II. *Wide Network (Different Network)*
- Cyber Gate
- Dark Comet
- Back Orifice

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Sub7
- Beast

VIII. CONFIGURATION OF REMOTE ACCESS TROJAN

This will include Setting up a popular remote administration Trojan known as Dark comet and creating a basic RAT setup to grab slaves. This paper will summarize the making of a basic RAT server with Dark Comet5. RAT is remote administration Trojan, which is generally used by attackers to steal login credentials, user data, user keystrokes and much more. We are hereby discussing the setup of a well-known RAT Dark comet

1. PORT SELECTION:

Open DarkComet-RAT and Right click on Socket/Net tab and choose "Add port to listen" for description process. We are using port 1604, you can use any port you wish to use. Then hit listen. It will look like this

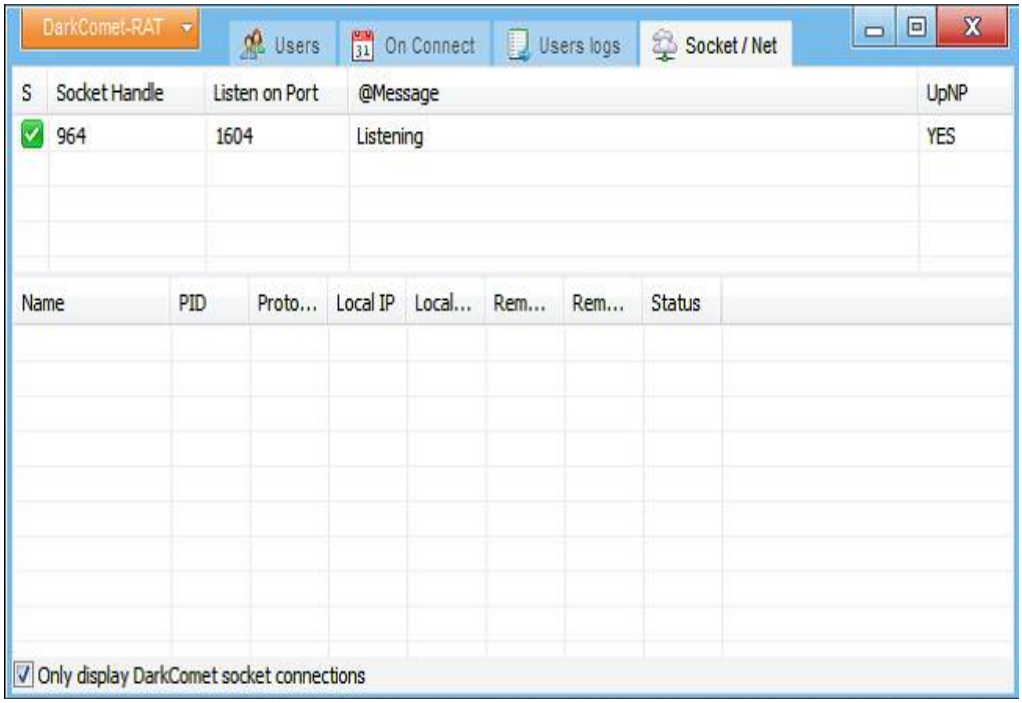


Fig. 4Port Selection

After selecting your desired port number you will need to do port forwarding (No-IP Provide free static IP service)

2. SETTING UP A NO-IP:

Static IP Account is Created Using NO-IP. To http://www.no-ip.com/ and hit create an account.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

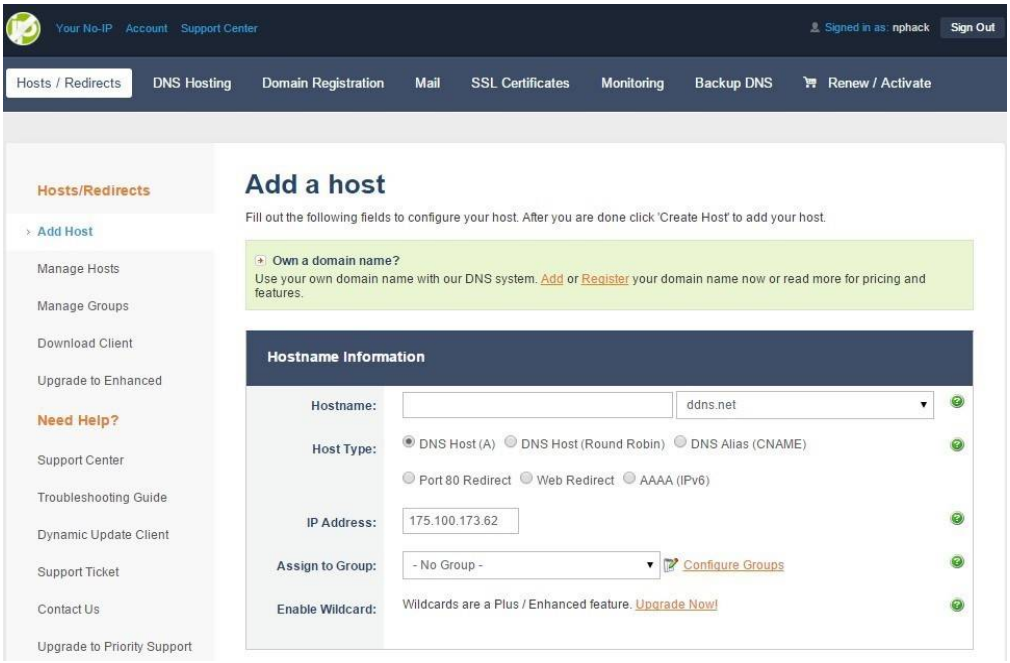


Fig. 5Configure Host using Add Host and fill Host Information

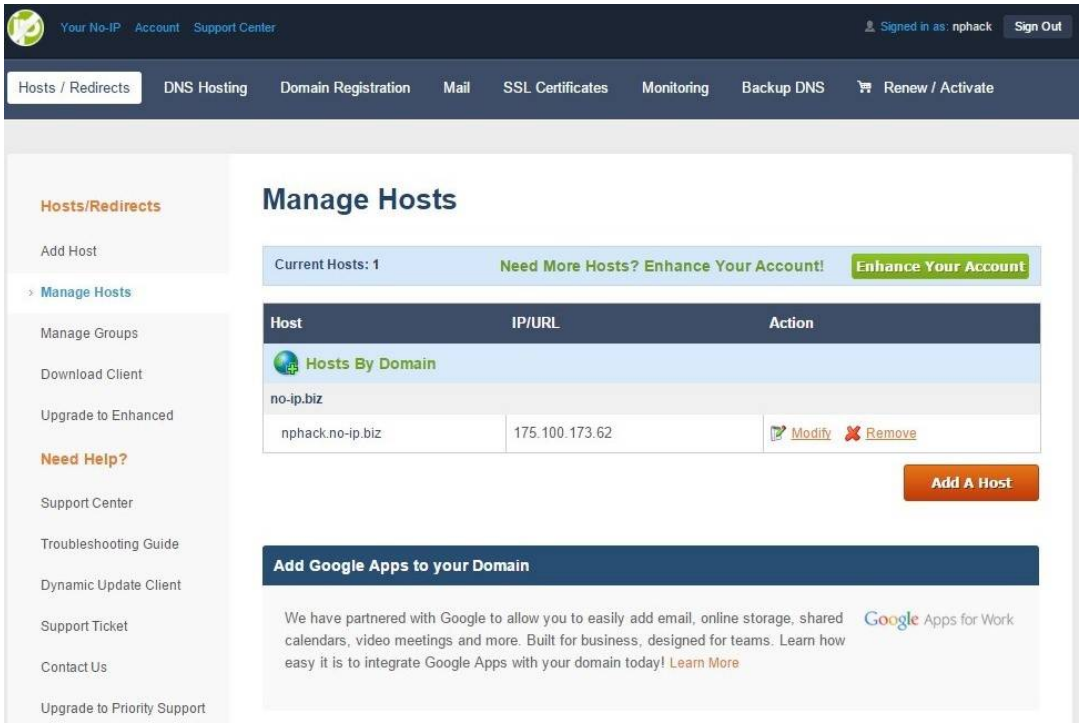


Fig. 6Manage Hosts or IP/URL Details

3. SETTING UP DUC:

A. Select your operating system and install it.
B. Open DUC it will ask you to log in.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

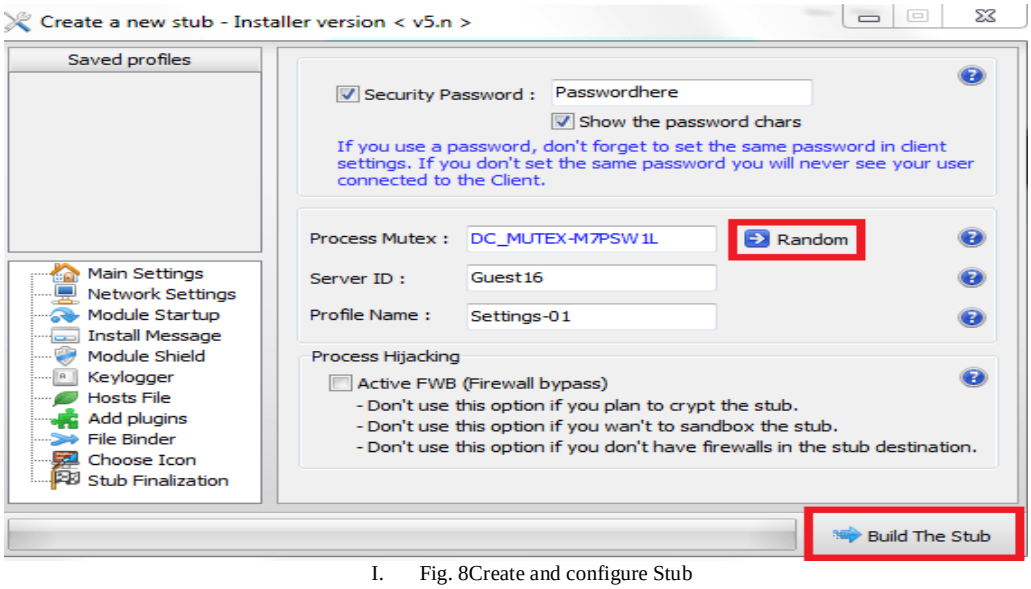
C. Hit select host then click in the check box next to the no-ip hostname you are using then hit save.
D. Now just hit refresh and you are done.

4. CREATING SERVER:

A. Open DarkComet 5
B. Click on the orange DarkComent-RAT and Click "Server module>> Full editor" (RATConfiguration)

Fig. 7Creating Server Module

C. In the Main Setting Click“generate few time” and leave everything else as it is. Shown in (Fig. 8)
D. Next clickNetwork settings in the "IP/DNS" type in your No-ip info and the same port you used to listen in. Then hit "Add this configuration"
E. Next click “Module Startup” and you can change various window startup options and file attributes.
F. Next click “Module shield” and you can disable system function stealth functions.
G. One by one you can modify setting like: keylogger, Host file, Add plugins, File Binder, Choose Icon.
H. Final Option is Stub Finalization then you have to click on Build the Stub and your file is created you can send or copy using usb to malicious activity.



I. Fig. 8Create and configure Stub

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

IX. IMPLEMENTATION REMOTE ACCESS TROJAN

1: Open DarkComet-RAT control panel (Perform this task in virtual environment. e.g. VMware workstation, virtualbox)

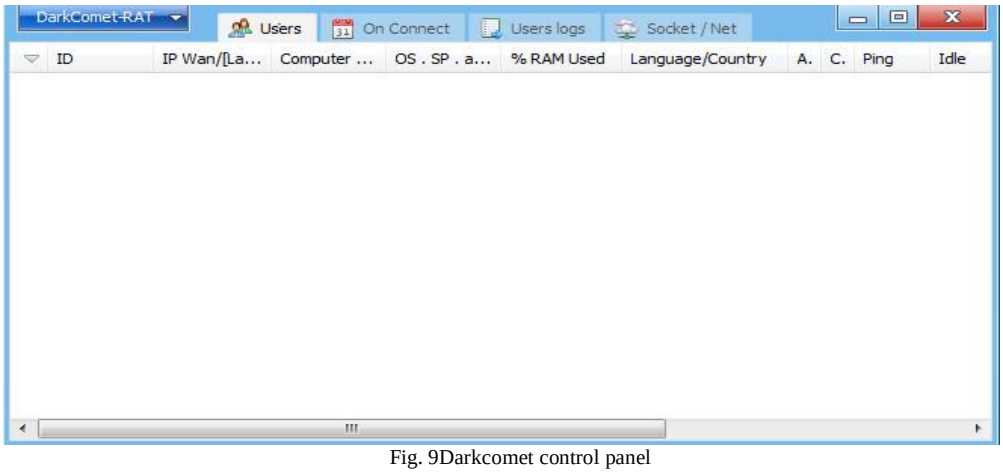


Fig. 9Darkcomet control panel

2: After Creating Infected File lock like this. (This malware is delete all doc files in windows system)

Fig. 10Remote Access Trojan Malware

3: Open "My Password" RATMalware or you canintegrate with other file like: Doc, PDF, exe, rar , etc.

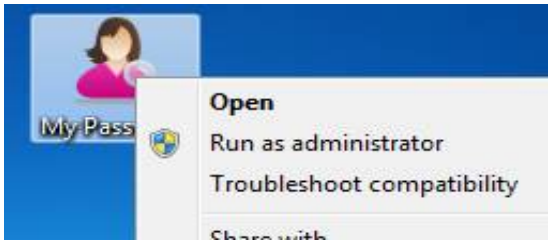


Fig. 11Open Malware File

4:After open malware file if it's successfully injected in system then message appear look like this. (You can modify error message to another message like: warning, success, info, prompt box, etc.)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Fig. 12Malware error message

After Remote access Trojan injected, open DarkComet control panel and look user's panel. It display Infected Host System. By using control panel you can monitor host system remotely.

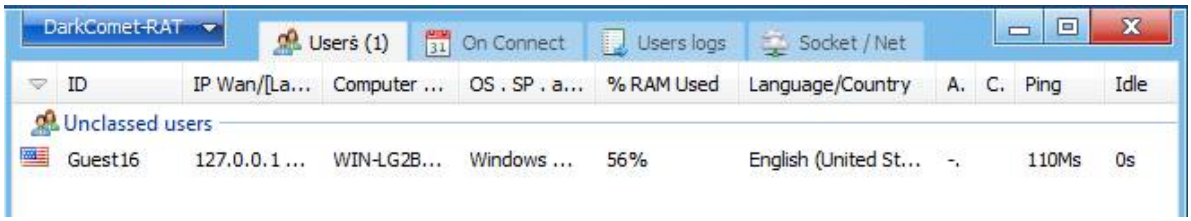


Fig. 13Control panel

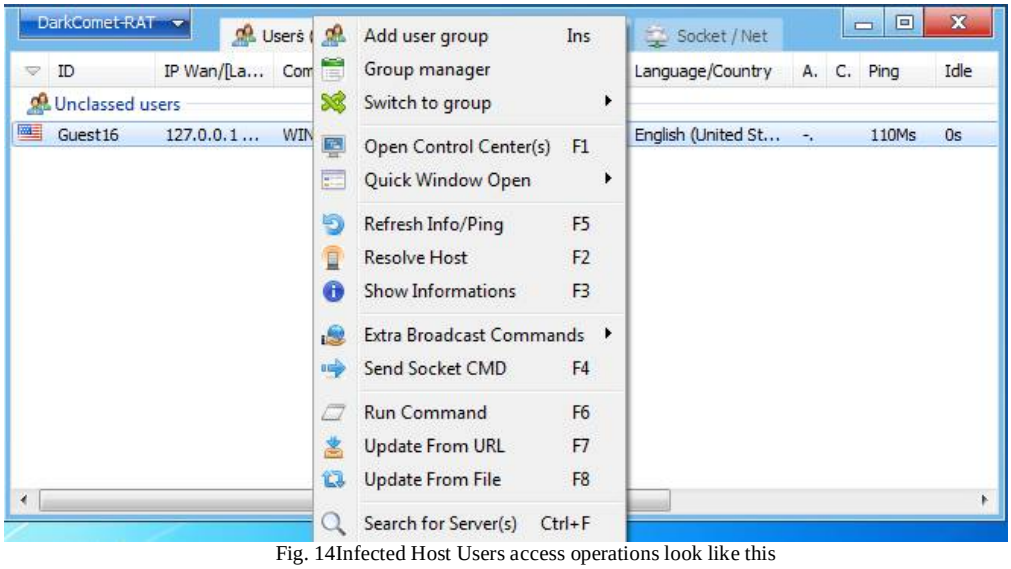


Fig. 14Infected Host Users access operations look like this

5: Click on "Open Control Center(s)" or Shortcut key-F1 to open control centre. Using control centre you can do many operation as shown in Fig.15

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

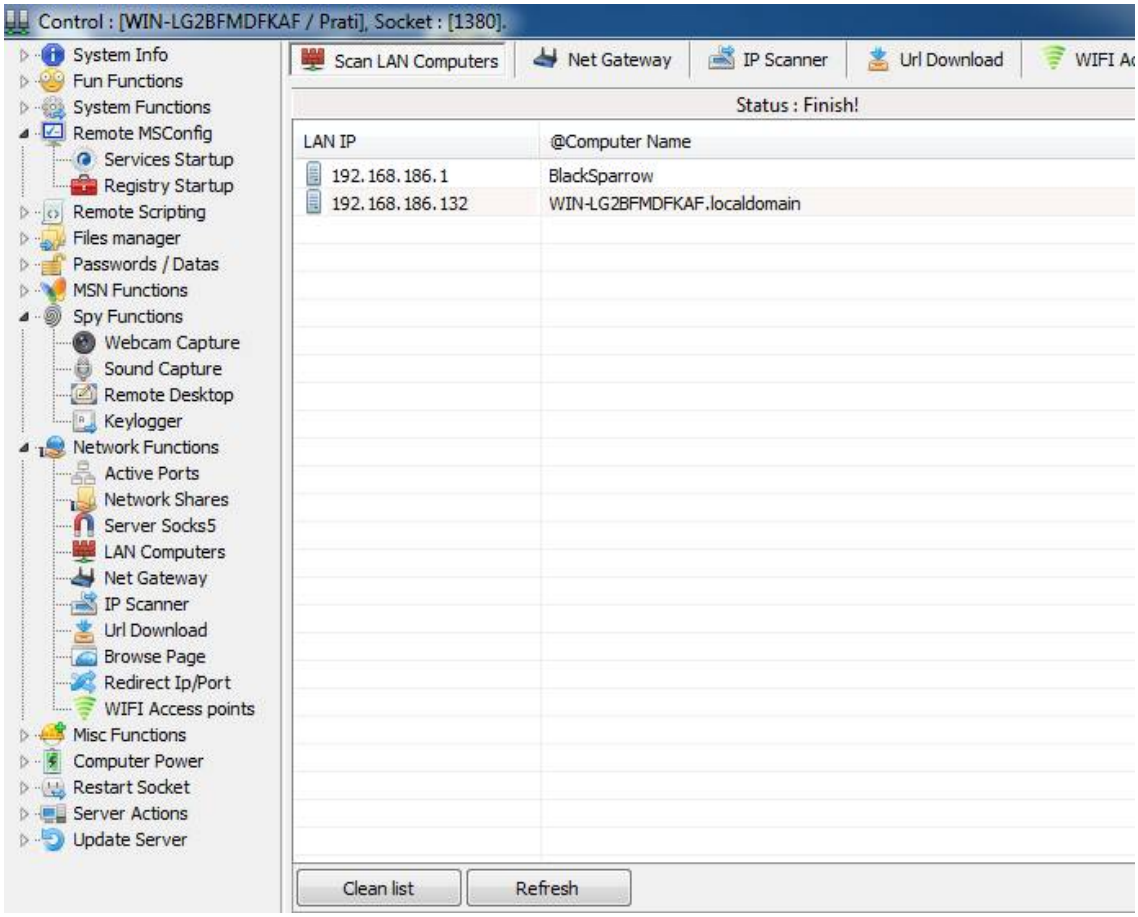


Fig. 15Control centre

X. YARA RULES

YARA is a popular tool which is used for inspection purpose, it will look after suspected files, directories and string matching which is defined in YARA rules. YARA tool provides a powerful language, which is compatible with Perl-based Regular Expressions [7].

```
rule rule_name : tag1 tag2 tag3
{
   meta:
      author      = "author's name and (if possible) link to profile"
      date        = "yyyy/mm/dd"
      description = "What does the rule do"
      reference/source = "Link to the blog, paper, ..."
      sample      = "file hashes"
  strings:
      XXXX
  condition:
      XXXX
}
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Rule Name is the identifier of the rule.They can contain any alphanumeric character and the underscore character, but the first character cannot be a digit. Rule identifiers are case sensitive and cannot exceed 128 characters [7].
- Strings: This section contains the strings/pattern/signature that we need to match against a file. It is optional [7].
- Conditions: Conditions sets evaluate Boolean expressions

XI. CONCLUSIONS

In this paper, we have learned about malware, malware analysis and detection techniques. We have also learned some limitations of static malware analysis. After analysing both static and malware analysis, we have reached to conclusion that Dynamic malware analysis is the best way to analyse malware samples. In this process of malware analysis we have gathered meaningful knowledge regarding some tools which are effective for the same. After studying malware and malware analysis techniques, we can say that sandbox environment is the best way to analyse dynamic malwares.

This paper elaborates effective and efficient methodology which can be applied to improve the performance of detection and removal of malwareswhich are collected and detected over an extended period of time. And the target of such a system is 97% malware detection and classification accuracy, which therefore significantly shows an improvement on current work.

REFERENCES

[1] Savan Gadhiya and Kaushal Bhavsar, "Techniques for Malware Analysis", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, pp. 972-975, April 2013.
[2] Dolly Uppal, Vishakha Mehra and Vinod Verma, "Basic survey on Malware Analysis, Tools and Techniques", International Journal on Computational Sciences & Applications, Vol. 4, No. 1, February 2014.
[3] Syarif Yusirwan S, Yudi Prayudi and Imam Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method", International Journal of Computer Applications, Vol. 117, No. 6, pp. 0975-8887, May 2015.
[4] M. Asha Jerlin and C. Jayakumar, "A Dynamic Malware Analysis for Windows Platform - A Survey", Indian Journal of Science and Technology, Vol 8, No. 26, October 2015.
[5] Rohitkumar Gautam, Sanjeev Kumar and Jhilik Bhattacharya, "CPU Mining Malware: Complete Analysis of Real World Virus", International Journal of Research in Advent Technology, Vol. 3, No. 9, E-ISSN: 2321-9637, September 2015.
[6] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim and W. Aigner "*A Survey of Visualization Systems for Malware Analysis*", Eurographics Conference on Visualization, 2015.
[7] http://resources.infosecinstitute.com/yara-simple-effective-way-dissecting-malware/
[8] Waqas Aman, "A Framework for Analysis and Comparison of Dynamic Malware Analysis Tools", International Journal of Network Security & Its Applications, Vol. 6, No. 5, September 2014.
[9] Gursimran Kaur and Bharti Nagpal, "*Malware Analysis & its Application to Digital Forensic*", International Journal on Computer Science and Engineering.
[10] Konrad Rieck, Philipp Trinius, Carsten Willems and Thorsten Holz, "Automatic Analysis of Malware Behavior using Machine Learning", Journal of Computer Security, 2011.
[11] Jozsef Hegedus, Yoan Miche, Alexander Ilin and Amaury Lendasse, "*Methodology for Behavioral-based Malware Analysis and Detection using Random Projections and K-Nearest Neighbors Classifiers*", Department of Information and Computer Science.
[12] Dr. Engin Kirda and Dr. Christopher Kruegel,"Large-Scale Dynamic Malware Analysis" December 2009.
[13] Murray Brand,"*Analysis Avoidance Techniques of Malicious Software*", November 2010.
[14] Xin Hu, "*Large-Scale Malware Analysis, Detection, and Signature Generation*", Computer Science and Engineering in the University of Michigan, 2011.
[15] Ronghua Tian,"*An Integrated Malware Detection and Classification System*" August 2011.
[16] "*Darkcomet – setting up the Remote Administration Tool*", OpenFire Security.
[17] Nwokedi Idika and Aditya P. Mathur, "*A Survey of Malware Detection Techniques*", Department of Computer Science, February 2007.
[18] https://github.com/Yara-Rules/rules/tree/master/malware
[19] https://github.com/Yara-Rules/rules/blob/master/malware/RAT_DarkComet.yar
[20] http://www.darkcomet-rat.com/
[21] http://www.noip.com/
[22] Kris Kendall, "*Practical Malware Analysis*"
[23] Dennis Distler, "*Malware Analysis: An Introduction*", SANS Institute InfoSec Reading Room, December 2007.

BIOGRAPHY

Nayan Zalavadiya received his bachelor's degree in Information Technology from Gandhinagar Institute of Technology in 2013. He is currently pursuing his M.Tech in Cyber Security at Raksha Shakti University, Ahmedabad, India.

Research Interest area: Malware analysis,Cyber Forensic Analysis, Vulnerability Assessment and Penetration Testing