IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8542

OPTIMAL RESEARCH ON REMOTE ACCESS TROJAN (RAT)

Mrs. Prachi R Salve[1], Rajas Kulkarni[2], Pooja Bansod[2], Mohit Goyal[2]

Student, Computer Engineering, Dr D Y Patil School of Engineering Academy, Pune, India[1]

Assistant Professor, Computer Engineering, Dr D Y Patil School of Engineering Academy, Pune, India[2]

Abstract: One of the most powerful Trojans used by the attacker is the Remote Access Trojan. Remote Access Trojan (RAT) is one of the most terrible security measures that organizations face today. It is an outstanding example of how attackers can misuse remote access technology. Given that Trojan, it is a non-computer program that seeks to simplify the back door to access a computer program management. In this malware, there are two common methods of delivery. This is used for malicious purposes. This Trojan confirms the secret method of data collection by making it inaccessible. Now, these Trojans have the ability to perform various tasks that harm the victim. Trojan Access Trojans can also be viewed as authentic applications when downloaded, RAT also loads them. Enables the attacker to be able to control the target device. Remote access is often used for remote access to corporate network servers, workstations, while providing ease of use, and has also created security issues in auditing. In this paper, a representative-based safety research program is provided and can monitor the performance and maintenance, security of the system, the performance and maintenance of employees using the system through a web page, increasing the flexibility of deployment and ease of use.

Keywords: Remote administration, Network Security, Client-Server, payload Builder

I. Introduction

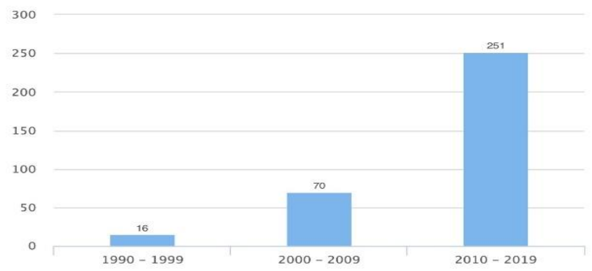
The organization or individual loses money, loss of reputation and business disruption as a result of data breach. As the threat of data breaches grows every year, the security of confidential information remains the same more important than ever. One of the main reasons for data violations is malicious malware attacks. Today, attackers have begun to use this tactic in the cyber world. Attackers can use their fraudulent tactics effectively and easily to gain profits or attacks to steal user information. This malicious software can easily infect user systems through various means such as custom-designed emails, unsafe web sites, cookies and fraudulent engineering attacks such as ads. The concept of espionage is not new in today's world. Throughout human history, espionage has been widely practiced by violent people, from the first world war until the present. Remote Access Trojan (RAT) can probably be considered a legacy tool. RAT is a computer-based program that uses the rear control department to manage a targeted computer. Therefore, RATs are used for increasing, confidential activities such as APTs. Using this dangerous approach, the attackers took their time to explore the victim's networks and assets, and then marched as quietly as possible to achieve their goals without being detected. Some APTs have been operating for years and RATs play a key role in empowering attackers to achieve their target while avoiding detection.

One of the most important steps to ensure computer security and security is to keep the app up to date with regular updates and updates, and measures such as not downloading and making unsolicited programs on unsafe websites also work to provide protection against spyware. This paper aims to start a discussion about RATs as a unique situation that requires further learning. We say that over the past decade there has been a change in the threat zone, where RATs have become a commodity.

II. LITERATURE SURVEY

From the data collected and shown in Figure 1, we can see that the growth of RATs increased slightly as compared to first two decades, but not until 2010 when their growth continued. The outstanding RATs we know these days have been developed over the past decade.

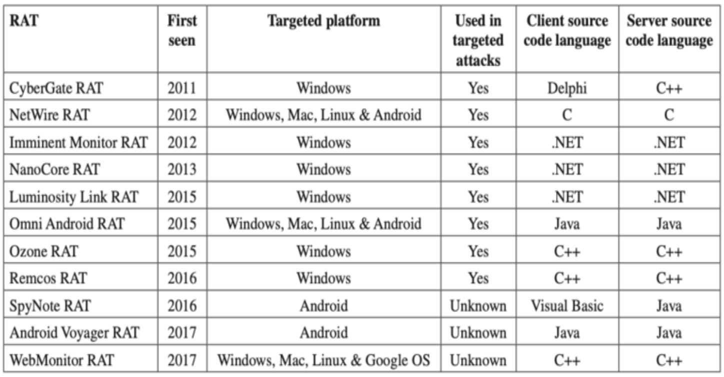
DOI: 10.17148/IARJSET.2021.8542



Take the Beast, RAT first spotted in 2002. It retained some of the original features of Trojans, but was able to do more complex things. It has used client / server build-up, such as Back Orifice, but has been among the first to put in touch with its victims. The client connects to the hacked computer number 6666, while the server opens the connection and returns to the client using port number 9999. When RAT finds other features, they are overjoyed. Soon, they began to be used as part of a more complex attack by cyber criminals and similarly sponsored attackers.

By the late 2000's, the RAT was available for download and use by anyone with an interest in hacking, writes researcher David Martin in his paper, Gh0st in Deshell: Decoding Undocumented Protocols"

Similarly, there are other types of malware, Rat's that are openly commercialized. These Rat's are summarised in the table given below. Some of them mentioned are: Web Monitor RAT, Omni Rat, Ozone RAT, Imminent Monitor RAT and much more.



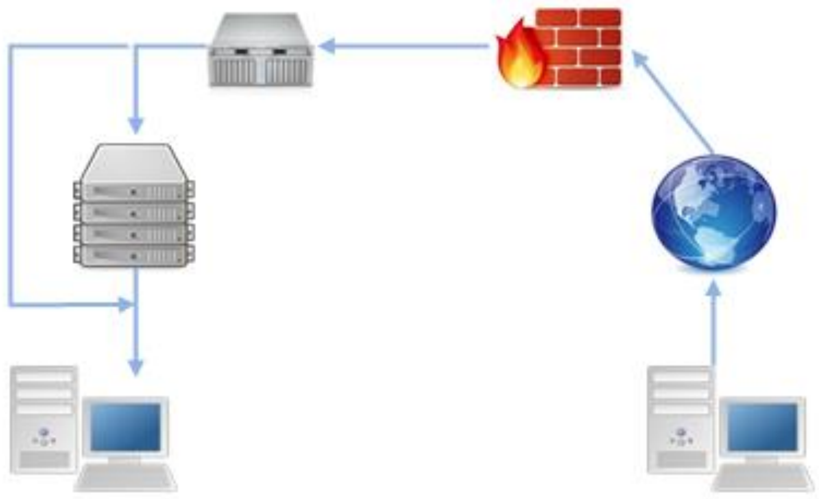
RAT	First seen	Targeted platform	Used in targeted attacks	Client source code language	Server source code language
CyberGate RAT	2011	Windows	Yes	Delphi	C++
NetWire RAT	2012	Windows, Mac, Linux & Android	Yes	C	C
Imminent Monitor RAT	2012	Windows	Yes	.NET	.NET
NanoCore RAT	2013	Windows	Yes	.NET	.NET
Luminosity Link RAT	2015	Windows	Yes	.NET	.NET
Omni Android RAT	2015	Windows, Mac, Linux & Android	Yes	Java	Java
Ozone RAT	2015	Windows	Yes	C++	C++
Remcos RAT	2016	Windows	Yes	C++	C++
SpyNote RAT	2016	Android	Unknown	Visual Basic	Java
Android Voyager RAT	2017	Android	Unknown	Java	Java
WebMonitor RAT	2017	Windows, Mac, Linux & Google OS	Unknown	C++	C++

It is a system communication protocol that has a problem with large design errors and fails to provide sufficient integrity, privacy, or authentication. Attackers can use this risk to remove unauthorized commands from client systems and apply unchanging code of administrative rights. Today One of the most and major confronting issue is Information security, In today's connected society travelling, telecommunication and every medium of working is attached to a real-time access to resource on corporate networks.

III.PROPOSED WORK

The project has a idea of how Remote administration can be done with a suitable line of code that will help them to monitor their process.

Basic Module program developed with python and showed with a User-friendly support using the UI which will enhance the user to access over a system, perform checks whether it may be Linux, Windows or IOS, all cross-platforms are here supported and the best thing it's open-source, no need to buy Tools charging you monthly. Start the server, deploy bots using your Local address and you got eyes over all your systems.



IV. MOTIVATION

Understanding the scale and nature of the criminal use of RAT malware is important in building effective barriers and minimizing the harm inflicted on its victims; however, rating The RAT ecosystem presents non-standardized challenges for other types of malware infections. Victims of RAT infection are hard to spot; as a rule, participants are generally not with major, noisy behaviours such as layoffs, spam, or fraud. Similarly, RAT backlinks are often targeted rather than widely distributed, creating their own command-and-control hard to find servers. And finally, to understand the motives of those working with RAT it is very difficult. While most malware has a specific purpose (e.g., ransomware), or issue commands to all botnet simultaneously (e.g., denial of service), RAT infections each, controlled by hand. In this article, I face these challenges while investigating the nature of the two most popular RATs, the range of goods, has so far not been studied in scale. Change well-established security strategies such as honey-potting, comprehensive online scanning and domain Sink holing, I created and used the tools for measuring and understanding the participants in this environment - invaders, their motives, the infrastructure they use, and their victims.

V. METHODOLOGY

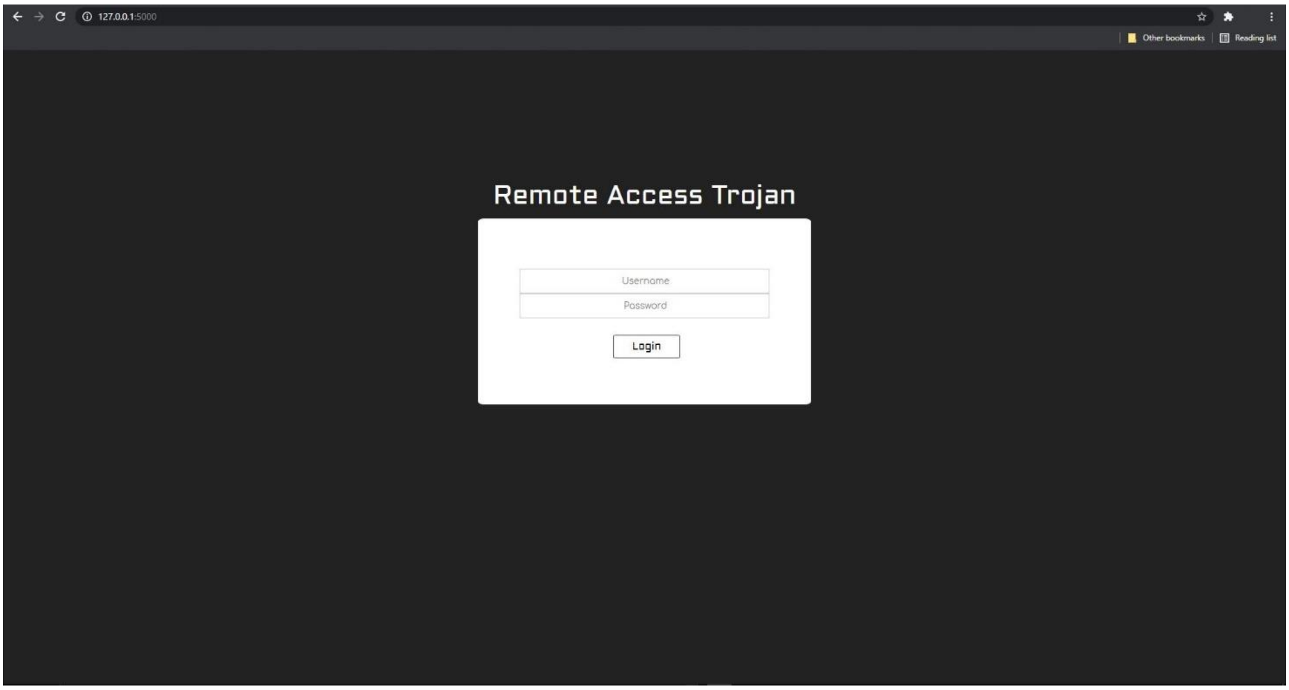
It uses a RSA-2048 with AES-256 to keep the communication safe between the infected client and the machine server. We have two types of connection possibility, one is using the Direct connection, In direct connection RAT is simply set-up where the client connection is to a single or multiple servers directly and the second one is the reversed connection using a backdoor, where the advantages is there would be no problem with routers about blocking incoming data as the connection would be started outgoing for a server. It will allow mass-updating of servers by broadcasting commands and can launch distributed denial of service (DDoS) attack.

RAT trojans can generally do the following things smoothly,

1. It can access the disk fragments and can also extract and delete the data from particular file location.
2. It is capable of dropping admin rights
3. Download, upload, delete, Rename. etc
4. Print Text, play sound
5. Start Keyloggers

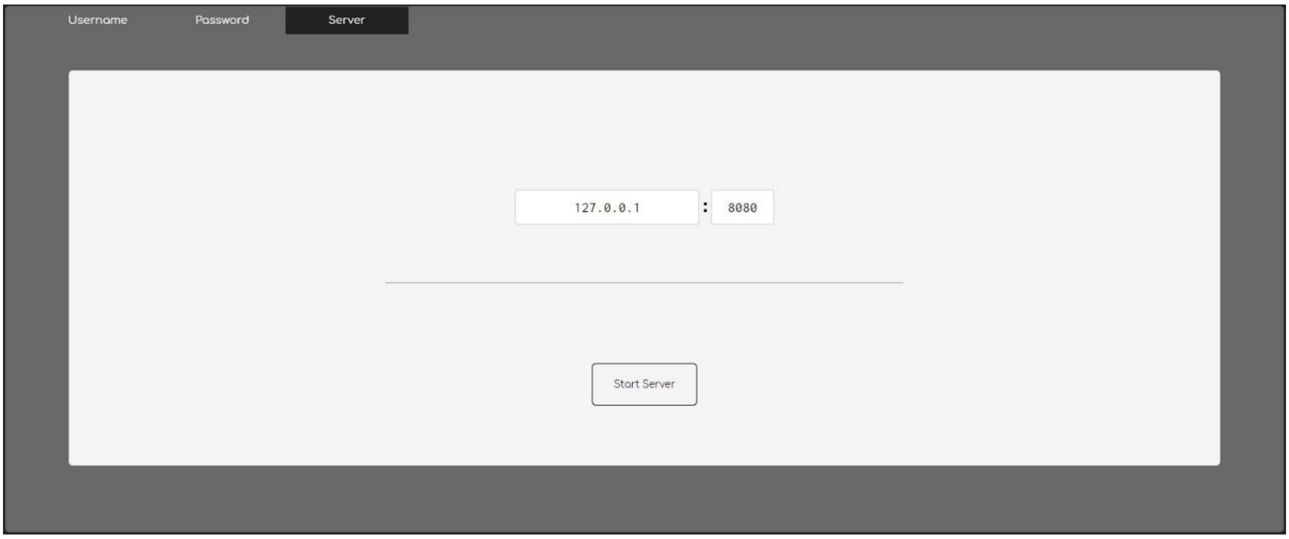
VI. RESULT

Step 1: Starting the server



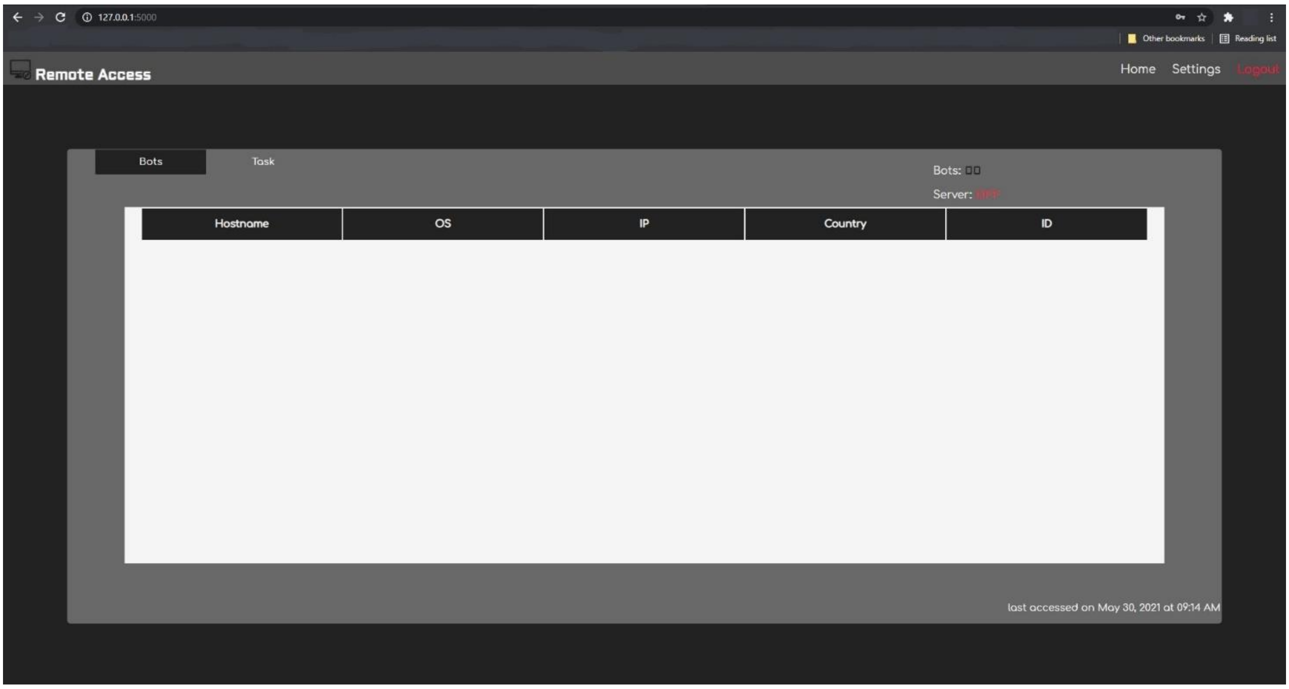
DOI: 10.17148/IARJSET.2021.8542

It all starts with starting with the server. Let Assume a organisation of 10 computers setup all connected to a single medium of connection. Count that medium as a server, consider all the connection goes through the local address 127.0.0.1, deploy the Payload inject the payload to all your 10 systems.



127.0.0.1 : 8080

Step 2: Main Screen



Bots: 00

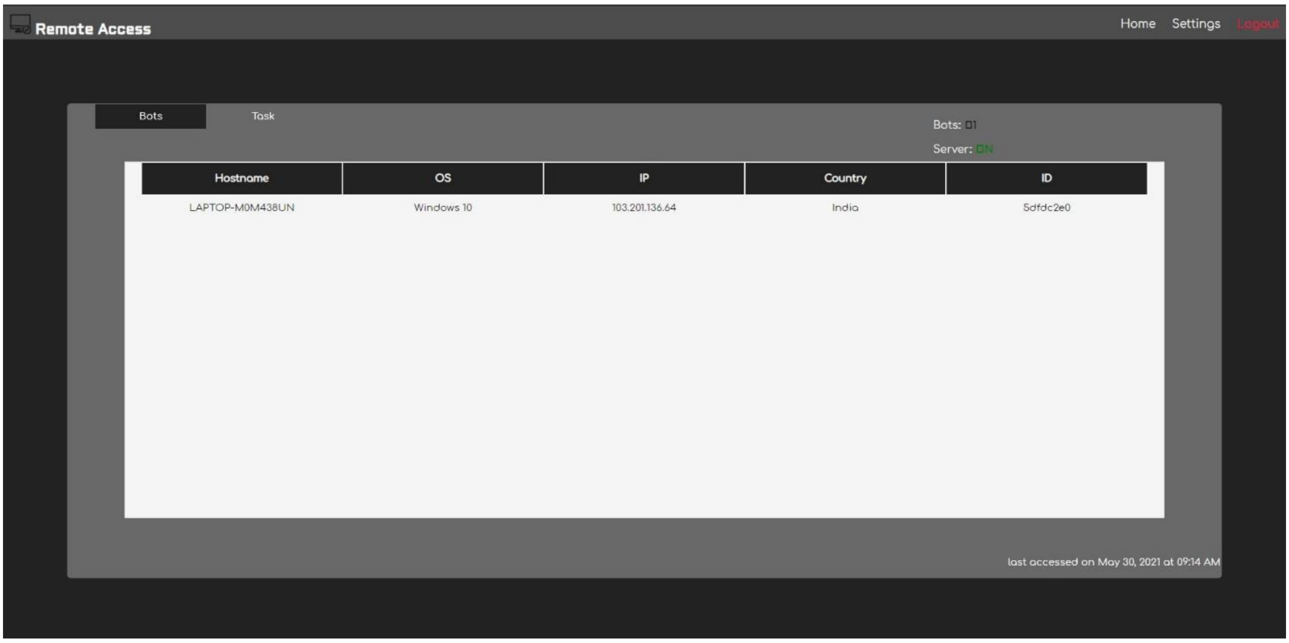
Server: OFF

Hostname	OS	IP	Country	ID

last accessed on May 30, 2021 at 09:14 AM

The main screen contains the information that a basic describes the user or server about the OS, Ip address, Hostname. Beside that is the Task function which gives the command output and can perform CMD runnable options. Once the payload is sent a single click will execute the payload that will make a forever connection to local address stored. Once this is done the client-server interaction is started address a Three-way handshake.

DOI: 10.17148/IARJSET.2021.8542



Bots: 01

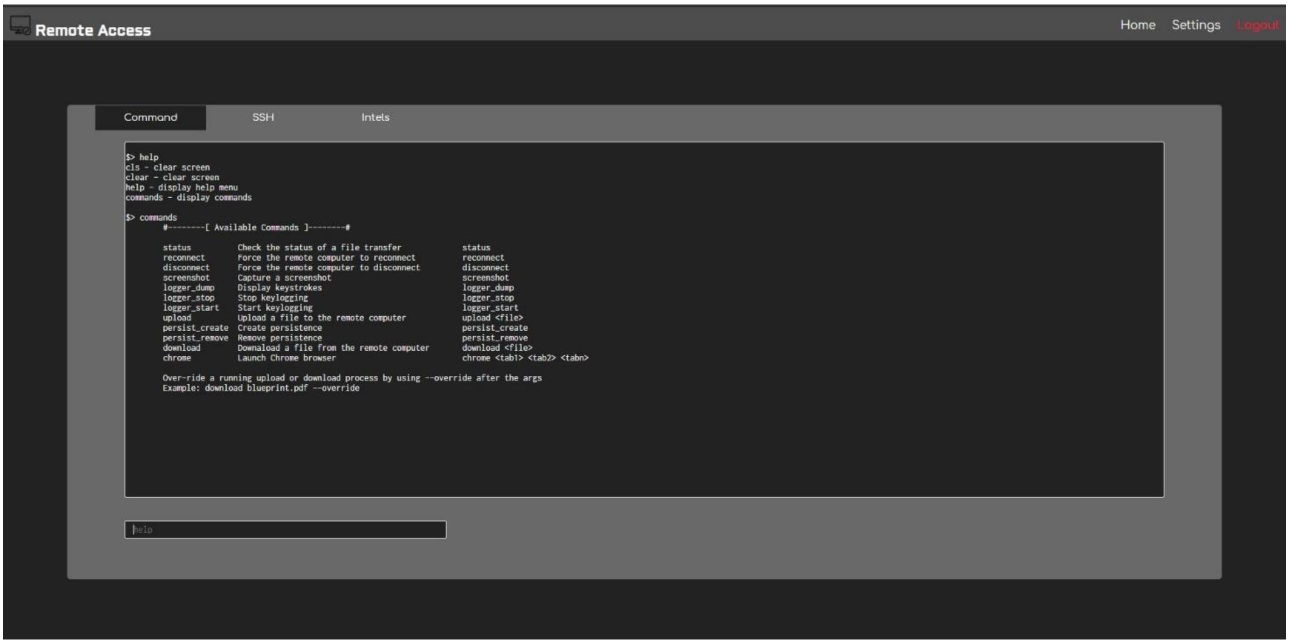
Server: ON

Hostname	OS	IP	Country	ID
LAPTOP-M0M438UN	Windows 10	103.201.136.64	India	5dfdc2e0

last accessed on May 30, 2021 at 09:14 AM

The above figure shows the after changes of the payload, once after the successful execution of the payload Hostname, OS, IP, Location and the particular ID it is serving is shown and after a single click on the hostname we can connect it with a remote access that is shown in the figure below.

Step 3: Remotely Connect



```
$> help
cls - clear screen
clear - clear screen
help - display help menu
commands - display commands

$> commands
        #--------[ Available Commands ]--------#

        status          Check the status of a file transfer             status
        reconnect       Force the remote computer to reconnect          reconnect
        disconnect      Force the remote computer to disconnect         disconnect
        screenshot      Capture a screenshot                            screenshot
        logger_dump     Display keystrokes                              logger_dump
        logger_stop     Stop keylogging                                 logger_stop
        logger_start    Start keylogging                                logger_start
        upload          Upload a file to the remote computer            upload <file>
        persist_create  Create persistence                              persist_create
        persist_remove  Remove persistence                              persist_remove
        download        Downaload a file from the remote computer       download <file>
        chrome          Launch Chrome browser                           chrome <tab1> <tab2> <tabn>

        Over-ride a running upload or download process by using --override after the args
        Example: download blueprint.pdf --override
```

```
help
```

After establishing a successful connection with the remote client, the Command and the SSH function can be performed. List of the functions that can be performed very basically are show like. Status, reconnect-disconnect, Keylogger start-stop, start application.

VII. CONCLUSION

The RATs (Remote Access Trojans) is capable of causing damage is dependent on the cleverness and brain of all attackers after them. Remote Access Trojans is not a good information, that is why it is very essentially important to protect your own devices against them.

Any antivirus software is not mean to replace your anti-malware products, but complements them, So you can always get benefits from the multiples layer of protection to always fight against virus and ransomwares. With all software products installed more security gaping are filled & hence you can always enhance online safety first.

The RATs (Remote Access Trojans has a greatness of collecting vast amount of data of users of an accessed machine. If RATs program is founded on any device, It should be always assume that if any personal data which has been accessed on the system have been not protected yet. User should immediately update all internal information with security codes from a clean device, and send notification to the user and administrator. Monitor outgoing traffics, reports, bank statements securely over the following weeks to detect any suspicious activity to accounts and devices. All the Advanced RATs (Remote Access Trojans) are especially used for System hardening. But here are some several measures which can be helpful on the size of the environment we are looking for protect. Including security awareness & antivirus software.

Colliding a host-based system with the networks based one of the most effective way to provide complete protection of your environmental. This combination is helpful to ensure that any strange or suspicious activity detection in configure changes and main access of your monitored system will be immediately detect and marked as a potential security threat. It also confirms strange activity in the data flow on your networks will be identified by the software.

VIII. References

[1]. Manjeri N. Kondalwar and C.J Shelke for “Remote Administrative Trojan/Tool(RAT)”,(2014)

[2]. Zhongqiang Chen, Peter Wei and Alex Delis for “Catching Remote Administration Trojans(RATS)”, (2002) Vol-3 Issue-5 2017 IJARIIE-ISSN(O)-2395-4396 6712 www.ijariie.com 1045

[3]. Jay Novak, Jonathan Stribley, Kenneth Meagher, and J.Alex Halderman “Absolute Pwnage: A Short Paper About The Security Risks of Remote Administration Tools”, (2011)

[4]. Rupal D.bhatt, D.B. Choksi, “A Comparative Evaluation of Remote Administration Tools”, (2013)

[5]. Anis Ismail, Mohammad Hajjar, Haissam Hajjar, “Remote Administration Tools: A Comparative Study”(2012)

[6]. Milajerdi, S.M.; Gjomemo, R.; Eshete, B.; Sekar, R.; Venkatakrishnan, V.N. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1137–1152, [CrossRef]

[7]. Valeros, V.; Garcia, S. Growth and Commoditization of Remote Access Trojans. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), Genoa, Italy, 7–11 September 2020; pp. 454–462, [CrossRef]

[8]. Rezaeirad, M.; Farinholt, B.; Dharmdasani, H.; Pearce, P.; Levchenko, K.; McCoy, D. Schrödinger’s RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem. In Proceedings of the 27th USENIX Conference on Security Symposium (SEC) SEC’18, Baltimore, MD, USA, 15–17 August 2018; pp. 1043–1060.

[9]. Wu, S.; Liu, S.; Lin, W.; Zhao, X.; Chen, S. Detecting remote access trojans through external control at area network borders. In Proceedings of the Symposium on Architectures for Networking and Communications Systems (ANCS), Beijing, China, 18–19 May 2017; pp. 131–141.

[10]. Moser, A.; Kruegel, C.; Kirda, E. Limits of Static Analysis for Malware Detection. In Proceedings of the Twenty-Third Annual Computer Security Applications Conference (ACSAC), Miami Beach, FL, USA, 10–14 December 2007.

[11]. Luo, Xin, and Qinyu Liao. Awareness Education As A Key to Prevention of Rugs, Information System Security, Volume 16, No 4, Pp. 195-202, 2007.

[12]. Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., & Tehranipoor, M. Hardware Trojans: Lessons learned after a decade of research. ACM Transactions in Design Automation for Electronic Systems (TODAES), Volume 22, No. 1, Pp. 6, 2016. [3] Kadir, Andi Fitriah Abdul, Natalia Stakhanova, and Ali A. Ghorbani. Understanding Malware Attacks in Android Finance: Taxonomy, Characterization, and Challenges. Cyber Security and Travel Journal, Volume 7, No. 3, Pp. 1-52, 2018.

[13]. Saracino, A., Sgandurra, D., Dini, G., and Martinelli, F: Active and effective malware detection and prevention of android. IEEE Transactions in Compompable and Secure Computing, Volume 15, No.1, Pp. 83-97, 2018.