International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - ICSCAAIT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

An Imperceptible RAT using Python

Anshul Garg[1], Rachna Jain[2], Preeti Nagrath[2]
[1]Research Scholar, Bharati Vidyapeeth's College of Engineering, New Delhi, IPU, India
[2]Assistant Professor, Computer Science Department, Bharati Vidyapeeth's College of Engineering, New Delhi, IPU, India

Abstract: From the past few years, there has been an surge in malware in cyberspace like viruses, worms, ransomware etc. One of the most noted malware is Remote Access Trojans (RAT). RATs are mainly worn in spying on victim's system. It can also be used to outfit cybercrimes and terrorism by spying on suspect's computer. Using a RAT one can take control of any remote computer, typically consisting of a server covertly running and catching to specific TCP/UDP ports of a victim machine as well as the client acting as the alloy betwixt the server and the attacker. In this paper, we have explored the domain of malware analysis and threats from a different kind of malware. Our main cynosure is on the malware like Remote Access Trojans (RAT).

Keywords: Remote Access Trojan (RAT), Malware, Cybercrimes, Python, Security and Privacy.

I. INTRODUCTION

Either computer program that performs anything malicious and harmful without the user's sanction is termed as malware. There are legion types of malware in cyberspace like viruses, worms, spyware, adware, ransomware etc. One of them is RAT, which mainly bridles the victim's system from a remote computer.

A Remote Access Trojan (RAT) is a malware program that covers a back door for administrative control over the target computer. Once installed, RATs tick their unexpected or even unauthorized operations. Also, stay on victim systems for the lofty haul. A typical RAT consists of a server component running on a victim machine and a client program acting as the interface between the server and the attacker. The client establishes communications with its corresponding server as soon as the IP address and port of the latter become available through feedback channels such as E-mail, Instant Messaging, and Web access. While interacting with a RAT server, an attacker can record keystrokes, intercept passwords, manipulate file systems, and usurp resources of victim systems. By continually changing their name, location, size, and behavior, or employing information encryption and message tunneling for its communications, RATs may avoid the detection of security protection systems such as firewalls, anti-virus Systems, and intrusion detection/prevention systems (IDSs/IPSs). Once bound to programs, RATs in execution inherit a victim's privileges and raise havoc; Moreover, they launch attacks against other systems appearing themselves to be superusers. RATs provide the ideal mechanism for propagating malware including viruses, worms, back-doors, and spyware.

Remote administration refers to any method of controlling a computer from a remote location. In order to use or access web material from the system without being physically near it we use Remote Administration. Various types of RATs are distributed with legitimate .exe files for executing games and installing unwanted types of software. Intruders normally use a program called a binder to combine the legitimate executable files with RATs and toolkits. RAT is becoming increasingly common and is often used when it is difficult to be physically near a system in order to use this RAT, or in order to access web material that is not available in one's location and not present in other location.

Any computer with an Internet connection, TCP/IP or on a Local Area Network (LAN) can be remotely administered. RAT can be used for any of the activities and can span multiple categories of servers, such as database servers, middleware servers, etc. Endrosing employees to valve into the office. Local area network "LAN" from customer sites, hotels, internet cafe and airport check can notably surge business efficiency, prolific and job pride. Mobile empowerment based on mobile technologies allows the development and implementation of new business models and opportunities targeting micro enterprises and their customers in developing countries like South Africa. RATs have the potential to collect vast amounts of information against users of an infected machine. If Remote Access Trojan programs are endowed on a system, it should be deemed such that any personal information ingressed on the infected machine is compromised. Users should immediately refurbish all usernames and passwords from a tidy PC, and brief the appropriate administrator of the system's potential compromise[11]. Auditor credit reports and bank statements warily over the rear months to spot any suspicious hustle to financial accounts.

II. RELATED WORK

In this RAT we work on the python language which is an intercepted object-oriented high-level programming language with the dynamic semantic. Its high-level built in data structures, combined with dynamic typing dynamic binding, make it very attractive for rapid application development as well as for use as a scripting or glue language to connect existing components together [8].

Remote control software provides fast secure access to remote PC's on Windows platforms. Hackers and malware sometimes install these types of software on a

computer in order to take control of them remotely. As you are an IT support, you need to choose the software which leads your IT skills. After you determine how much you want to manage remotely, the next step is to select the tools and supporting components you need to accomplish your remote management tasks[1]. Our goal is detecting RAT activity in proxy server logs, even if the C&C server address is unknown and the distinctive communication pattern is unknown. We analyzed proxy server logs including RAT activity, and found that the RATs had characteristic features in the behavior. Then we proposed how to detect RAT activity in proxy server logs [2].

The python interpreter and extensive standard library are available in open source or binary form. Since there is no compilation step, the edit-test-debug cycle is incredibly fast. Debugging Python programs is easy: a bug or bad input will never cause a segmentation fault. Instead, when the interpreter discovers an error, it raises an exception [5].

When the program doesn't catch the exception, the interpreter prints a stack trace. A source level debugger allows inspection of local and global variables, evaluation of arbitrary expressions, setting breakpoints, stepping through the code a line at a time, and so on. The debugger is scripted in Python itself, testifying to Python's introspective power. On the other hand, often the quickest way to debug a program is to add a few print statements to the source: the fast edit-test-debug cycle makes this simple approach very effective[6].

III. PROPOSED WORK

The work on Remote Access Trojan (RAT) is divided into two parts:

1. Server: This opens a TCP/IP port on victim computer and listens for any incoming connections. On any incoming connection for it accept the connections and provides a network stream for data transfer. On its initial execution, it marks its entry in the windows registry so that it can run every time user logs on to his account. It also sends victim IP address to a particular email id. It then receives commands from the client , perform tasks and then returns the result to the client application.

2. Client: Client enables to connect to the victim using his IP and port address. Once the connection is established, it can perform following tasks:

- Can detect victim IP and send it to email ID, so that we can connect to them using that IP address. There is no need to get victim IP address physically gaining access to victim's computer.
- Can get victim computer information like their username, windows platform, active directory etc.
- Can capture and record the keystrokes of victim typed on his computer

We are using google mailing service "Gmail" as a cloud service for the purpose of data exchange between the machine without any problem. By using Gmail we are ensuring that no company or any institute will block the Gmail service which gives us two following advantages:

a. Gmail is allowed everywhere because it's a genuine service offered by the Google. So sending and receiving commands using emails is useful and become unnoticed by the firewall.

b. As we are using Gmail as could service so there is less chance of getting caught because the payload is not directly sent to the attacker.

IV. APPLICATIONS

a. To enable user to check system security and vulnerability.

b. To control terrorist activity by monitoring their activity.

c. To collect enough proofs to punish criminals. Evidence Tracking can be based on observing the physical locations as well as based on thorough examination of data or information.

V. ADVANTAGES

1. Unauthorized use of computers mainly stealing a username and password.
2. Theft of company documents and E-mail fraud.
3. Harassment and stalking in cyberspace.

VI. DISADVANTAGES

a. Inadequately protected computers can be easy targets for unauthorized users.

b. There are several technologies available to improve computer security but their effectiveness may be limited without user awareness and education.

c. Attempt to access information stored on a computer. Information may have a sale value (corporate espionage), may be valuable to the owner (ransom opportunity) or maybe for further illegal activity such as fraud.

VII. FUTURE WORK

The project can be further implemented to make it persistent and undetectable. It can include more feature like the key logger, webcam access, getting admin control. It lacks the inclusion of various tools like control, These tools must be taken into consideration for a full-fledged project. In RAT many of features like webcam control have not been taken into consideration so they can be looked open. In RAT some features are still lacking in some fields like advance disk handling, binders, cryptors.

VIII. CONCLUSION

An undetectable Remote Access Trojan (RAT) perfects the requirements of the computer security and in ethical hacking. It reduces the chances of cybercrime. It speeds up the processing work. It is very beneficial in collecting proofs against victims. It incorporates to charging needs of users. It is user-friendly in nature. It applies checks in modules is the data consist in nature and reliable.

IX. REFERENCES

[1] Ismail, A., Hajjar, M., & Hajjar, H. (2008). Remote Administration Tools: A Comparative Study. Journal of Theoretical & Applied Information Technology, 4(2).

[2] M. Mimura Y. Otsubo H. Tanaka "Evaluation of a Behavioral HTTP-Based RAT Detection Method in Proxy Server Logs" Proc. 2017 Symposium on Cryptography and Information Security 2017.

[3] Chen, Z., Wei, P., & Delis, A. (2008). Catching remote administration trojans (RATs). Software: Practice and Experience, 38(7), 667-703.

[4] Manjeri N. Kondalwar and Prof. C.J. Shelke, Remote Administrative Trojan/Tool (RAT), International Journal of Computer Science and Mobile Computing, 3(3), 482-487.

[5] Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in computing. Prentice Hall Professional Technical Reference.

[6] Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

[7] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

[8] Mimura, M., Otsubo, Y., Tanaka, H., & Tanaka, H. (2017, August). A Practical Experiment of the HTTP - Based RAT Detection Method in Proxy Server Logs. In Information Security (AsiaJCIS), 2017 12th Asia Joint Conference on (pp. 31-37). IEEE.

[9] Yassir, A., & Ismaeel, A. A. (2016). Current Computer Network Security Issues / Threats. International Journal of Computer Applications, 155(1).

[10] Mimura, M., Otsubo, Y., & Tanaka, H. (2016, August). Evaluation of a Brute Forcing Tool that Extracts the RAT from a Malicious Document File. In Information Security (AsiaJCIS), 2016 11th Asia Joint Conference on (pp. 147-154). IEEE.

[11] Jessica, May'17, "Remote Access Trojan (RAT) – How to Detect and Remove It?", Link: http://guides.uufix.com/remote-access-trojan-rat-how-to-detect-and-remove-it/