TECHNIUM

Technium Vol. 4, Issue 1 pp.68-75 (2022)
ISSN: 2668-778X
www.techniumscience.com

Quasar Remote Access Trojan feature extraction depending on Ethical Hacking

Mohanad R. Ibrahim[1]
Karam H. Thanoon[2]
[1] High Diploma student at Software Department, University Of Mosul, Mosul, Iraq

[2] Software Department, University Of Mosul, Mosul, Iraq

muhandsoftware4@gmail.com [1] karamhatim@uomosul.edu.iq [2]

Abstract. These days, computer Trojans had become in the top of the most dangerous types of malwares threats. There is a lot of remote access tools that have ability to manage and apply many features remotely. Quasar Trojan is one of the most uses for Remote Access Trojan (RAT). The researchers apply Quasar on real environment in lab (ethically and for education purposes) and this paper presents the capabilities of Trojans. This paper will present some of Quasar features by extract most important features also presents how to access remotely by using no-IP address (DUC) with other tools of applying access of internal network ethically.

Keywords. Ethical hacking, network security, trojan horse.

1. INTRODUCTION

Remote Access Trojan (RAT) is a malicious tool for attackers to do remote control and intercept information, which causes serious impacts and huge losses to the states, enterprises and individuals. Typically, the RAT consists of control side and controlled side. Attackers can use the method of spear phishing and social engineering attack to find the machines which can be infected, and then adopt the standard TCP/IP or UDP protocol to achieve real-time communication between the control and the controlled side. Not being same with the traditional security threats, the RAT is often used in data theft and privacy snooping with the performance of full feature, concealment and long persistence. Generally speaking, one of the hide methods is inject themselves into the other legal process, so it does not display on the task list. In addition, the operations of RATs are gradually similar with legal applications, which make the detection of RAT more difficult. The different RATs have widely difference on setting function and operating environment, but their network behavior has a certain similarity. Therefore, the network traffic feature can be extracted to train the detection model. We can take this traffic as an indicator, which reflected the integration of all information between the control side and the controlled side. Due to the current involvement of the digital world in our daily lives and the huge reliance on it, the protection of a given system can be less efficient as a result of poor or absence of the right security measures. As a result, malicious hackers can exploit these vulnerabilities and security gaps. In fact, most of the currently available websites, networks, and applications are poorly and hastily configured [1].

This lack of security is mainly caused by poor planning and/or poor coding configurations. This means that no consideration is taken about the consequences of any attack. Thus, making them prone to various types of malicious code injection attacks, along with networks, applications, web services, and infrastructure attacks. Therefore, this paper discusses how these attacks are conducted, along how they can affect one, many or all of the security goals in a given system. Furthermore, the lack of training and awareness among employees and IT staff is also problematic and seriously challenging. In fact, there is a remarkable and significant skill gap in the ethical hacking domain. Therefore, the need to continuously and constantly train employees, along with the need for more ethical hackers is a must.

Additionally, this paper also highlights the need for new security measures. This has led pen testing to become a new emerging trend, which is achieved by evaluating both levels of security and immunity against already known attacks and threats. This is done through vulnerability assessment, foot-printing, risk evaluation, and pen testing [1][7].

2. Related works:

Aldy et al in 2019: introduced study of what hackers use for remote access Trojans to damage the system and then steal victims' data. It provided an in-depth analysis of modern malware as malware can camouflage like an unexpected system. He explained how the use of basic analysis techniques depends largely on the behavior of the malware being analyzed, and he explored how to identify malware, especially Remote Access RAT Trojan**.** [11]

Jean et al in 2021: introduced A study of the main focus is to explain the technical and non-technical steps of penetration testing. He explained that the goal of penetration tests is to make existing systems and their corresponding data systems more secure, efficient, and resilient. Explain what a pen test is and how to simulate the attack in order to identify any exploitable vulnerability and the existence of a security hole. How to use any identified vulnerability to launch attacks on systems, devices, or personnel [12].

Nagham et al 2020: introduced Researchers have made an ethical breakthrough on a real laboratory environment (ethically and for educational purposes) using Lime Worm tools. It provides static analysis by applying several tools, which are used to obtain key information from the lime worm. This paper discovered that the application of static analysis to this type of worm is very effective and accurate. The basic information obtained is used to develop a program to detect and eradicate the Lime Worm [10].

Advaitha et al: 2019 introduced A study of different types of attacks such as malware, phishing, MitM Man in the Middle, DoS (Denial of Service), SQL insertion, etc. to get the point of view of hackers and to protect ourselves from being hacked, and the researcher concluded that it requires basic knowledge of networks and cyber security for an ethical hacker It also describes how hacking is carried out and what different tools and techniques are used. Hence, in his research, I provided a basic understanding in the context of ethical hacking to help one not be hacked by hackers [13].

3. Terminology:

Hackers (or bad guys) try to compromise computers, while Ethical hackers (or good guys) protect computers against illicit entry. Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases their status in hacker circles. Benefits are:

1. Penetration Tests are Designed to Identify Vulnerabilities Before They are Exploited.
2. Provides a Solid Understanding of What is Visible and Possibly Vulnerable
3. Preventative Measure – Can be Very Effective
4. Should Include a Remediation Phase– Correct Identified Vulnerabilities and Exposures [2].

4. Ethical Hacking

As security programs evolve to include an offensive component, the need for appropriate professionals to conduct these offensive engagements increased. These professionals are known as ethical hackers, or penetration testers. The term hacker was coined in the 1960's by programmers at MIT to describe someone who had the ability to understand and manipulate technology (Thomas, Burmeister, Low, 2018 p113). Since then, although hackers largely still manipulate technology, the role and type of hackers has evolved. Hackers have now been separated into categories that correspond with their intent; black, grey, and white hat. Hackers have also expanded outside of just manipulating technology to manipulating people, such as the phishing and broader scope of social engineering[3][6].

4-1 Black Hat Hackers

The most well-known type of hacker is the black hat hacker. Popularized by TV, movies, and often in the media, the black hat hacker has motives that are considered malicious. Also known as 'crackers'

(Graves, 2010, p3) they operate illegally, and they are driven usually by financial gain, personal gain or anarchist desires (Thomas, 2017). Using a variety of techniques such as social engineering, infecting machines with malware, or breaking into systems, they obtain confidential information such as credit card numbers, usernames, passwords, and personal information. This information can then either be used by the hacker or sold to others for conducting fraudulent activities. There is no 'typical' hacker and although it is often thought that a hacker is a teenager that sits in their parent's basement and wears a hoodie. While the teenage hacker no doubt still exists, many of which were referred to as 'script kiddies' and defined as 14 to 16-year old's and still at school (Barber, 2015, p15), malicious hackers are now often part of organized crime syndicates and account for over 60% of all external threat actors (Verizon, 2018).

4-2 Grey Hat Hackers

Often also acting illegally, but with motives that aren't purely malicious are grey hat hackers. Grey hats often start as black hats but transition their skills for good or perceived good (Thomas, Burmeister, Low, 2018). A grey hat may identify security vulnerabilities of an organizations systems without their express permission and then notify them of the vulnerability. Grey hats often want to highlight security issues and attempt to educate organizations to properly secure their systems (Graves, 2010, p4). State sponsored hackers are also considered grey hats. These hackers often act in the interest of national security for their country and hack a foreign country. Although this would normally be considered illegal, and is by the target, in the context of achieving national security it would likely be considered a grey area. Hacktivists are also categorized as grey hat hackers. Hacktivists may hack and deface a website to promote a cause or leak information they believe is in the public interest, rather than to just be malicious (Thomas, Burmeister, Low, 2018).

4-3 White Hat Hackers

The last category is the white hat hacker, also known as an ethical hacker or penetration tester. White hats, like black hats and grey hats use the same tools and techniques, but unlike the other categories they are given authorization to attack the engaging organization. White hats can also have transitioned from black or grey hat hackers; such as well-known hacker Kevin Mitnick who was once known as the most notorious black hat hacker in the world (Thomas, Burmeister, Low, 2018), be directly educated as a hacker through formal training, or move from other related professions such as Information Technology. White hat hackers are professionals used to test the security controls of an organization and ensure they are effective. An ethical hacker will identify vulnerabilities such as missing security updates, poor architecture, misconfigurations, and other weak spots within an organization. Depending on the engagement, the professional will usually attempt to exploit any vulnerabilities they discover with the purpose of gaining administrative access or 'owning' the network, or gaining access to information, especially confidential and sensitive information. Once the engagement has finished, the ethical hacker will then create a report of findings and which will usually include recommendations on what to remediate.

5. Ethical Hacking Phases

In today's increasingly risky information technology environment, every organization should prioritize addressing IT vulnerabilities and securing it from all forms of threats, including data breaches. There are six important phases as shown in figure (1) to conduct a pen test [4][5].

Figure (1) Ethical Hacking Phases

5.1 Information Gathering (Reconnaissance)

Reconnaissance, otherwise known as recon, is the first step of pen testing. The more valuable the information one has on a target, the more likely they are to discover weaknesses or vulnerabilities. To start a pen test, it is important to collect as much information as possible.

This can be done by looking for publicly available information about the system and the organization and determining the best way to use it. Information gathering is more than just a single step in the security testing process; it is a skill that every pen tester should master for a better experience.

Reconnaissance is considered to be the most important phase of ethical hacking. Information can be gathered through active reconnaissance and passive reconnaissance. Passive reconnaissance is performed by gathering publicly available information about the target without interacting with the target. Active reconnaissance, on the other hand, requires the ethical hacker to have some level of interaction with the target.

The information about an organization's network architecture, operating systems, applications, and users can be determined during reconnaissance.

Footprinting is a strategy for gathering as much information about a targeted network, system, or person as possible. It aids pen testers in gaining access to an organization's computer system in a variety of methods. Tools for footprinting include *Whois Lookup*, *NS lookup*, and *IP lookup*. There are different types or branches of footprinting:

- Open-source footprinting is the safest type of footprinting because it respects all legal limitations. Examples include finding someone's password, phone number, email address, home address, etc.
- Network-based footprinting is used to recover information such as user name, shared data among individuals, network services, and network topology.
- Domain Name Servers (DNS) interrogation gathers the needed information and then queries DNS using pre-existing tools. A DNS query is an information request sent from the user's computer to DNS servers.

5.2 Scanning and Enumeration

Scanning includes techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is an information-gathering retrieval mechanism used to generate an overview scenario of the target organization. For each type of scan, different tools are used. For example, a network scanning tool cannot be used for scanning the vulnerabilities of a web application. Among others, tools used for scanning and information gathering include *nmap, wireshark, OWASP ZAP,* and *nslookup*.

Vulnerability scanning is an automated process that checks your systems for known flaws and potential risks.

Enumeration is used to gather information such as usernames, group names, hostnames, IP tables and routing tables, and applications and banners.

Vulnerability scanning and enumeration are generally performed using automated tools which report the existence of vulnerabilities, without taking further action. Therefore, among automated tools, the pen tester should use the human element to analyze vulnerabilities and penetrate to a network or server.

5.3 Gaining Access

Having identified all possible vulnerabilities and entry points, pen testers use exploitation tactics to gain access to the targets. In this phase, pen testers actively attack the security weaknesses of the system, using numerous attack methods. The identified vulnerabilities are compared based on their CVSS (Common Vulnerability Scoring System) scores. The higher the CVSS score, the easier will be to exploit the vulnerability.

Techniques for gaining access are defined based on the pen testing scope. The main objective of this phase is to understand the level of damage that a hacker can cause. Once initial access is

established, pen testers will attempt to escalate their access privileges and pivot or access other parts of the network.

Through privilege escalation, pen testers are able to use captured existing credentials to gain access to other systems, thus avoiding detection. Methods for privilege escalation include credential harvesting and structured passwords.

5.4 Maintaining Access

Once the access to systems and networks is achieved, pen testers, similar to what black-hat hackers would do, try to maintain that access. In this phase, the system is already breached. The objective now is to remain in the system as long as possible. This phase allows pen testers to acquire adequate time to extract valuable information, pivot to other areas, or further exploit the environment. This also enables the identification of other hidden vulnerabilities in the system.

5.5 Cleaning Up

After achieving the objectives of the pen test, the pen tester should clean and destroy any artifacts created during the test. This is done to prevent potential hackers from using the actions or findings of the pen tester. Artifacts that should be removed by the pen tester include, but are not limited to, agents, scripts, backdoors, temporary files, and shell sessions. Cleaning up and destroying artifacts help the pen tester think like a hacker and define actions that potential hackers could take for removing their footprints.

5.6 Reporting

The findings of the pen test are analyzed and documented in a written report. Pen testers keep track of every action they take during all phases of the test. The main objective of this phase is to provide information on how entry points and security issues were discovered.

The report should include specific vulnerabilities that were exploited, the rating scale of the risk related to the identified vulnerabilities, and detailed explanations on the recommendations for mitigating each of them. It may also discuss possible modus operandi of cyber criminals and how to manage them. In addition, screen captures for exploited vulnerabilities are added in the report as evidence.

6. Trojan Attacks

A Trojan horse is type of malware software that had been designed to be injected in said another software to cover it, this software is used from the hackers and cyber criminals to gain access to the systems and other user's data, users usually get tracked by some of the hacker social engineering tricks to make you loads and run the software to get access to your system or your device and spay on you by having back door access can also do a different actions like Copying data, Delete data, Modifying data…etc (sky, 2019). [9]

7. Trojan classification

In Cyber-security professional classify Trojans due to the action that it will be when this Trojan executed on the system and as an example one these type of Trojan:

1- Trojan-Ransom: Trojan-Ransom or Ransomware it's type of Trojan that can encrypt your Data to make you un able to get access on them until you pay to the hacker and they only will ask you to pay with crypto-currencies to make you unable to track the transaction.
2- Trojan-DDoS: This is actually one of the Trojan powers wish is doing DDoS attacks without making the owner of the device know that, then the hacker makes the infected device or devices to attack a specific domain address by sending requests to make a huge load on the service and make it down and not working.
3- Exploit: this Trojan will be included for a code to take advantage from an application that the user already use them on their devices and this code will exploit a bug inside this software.

8. Quasar Trojan (RAT)

Quasar (our case study) is a remote access trojan is used by attackers to take remote control of infected machines. It is written using the .NET programming language and is available to a wide

public as an open-source project for Microsoft Windows operating systems, making it a popular RAT featured in many attacks, it's features include:[8][9]

- TCP network stream (IPv4 & IPv6 support)
- Fast network serialization (Protocol Buffers)
- Compressed & Encrypted communication
- UPnP Support
- Task Manager
- File Manager
- Startup Manager
- Remote Desktop
- Remote Shell
- Remote Execution
- System Information
- Registry Editor
- System Power Commands (Restart, Shutdown, Standby)
- Keylogger (Unicode Support)
- Reverse Proxy (SOCKS5)
- Password Recovery (Common Browsers and FTP Clients) ... and many more!

7.1 client building

To create a new trojan horse malware , the tab builder must be selected from server menu as shown in figure (2) . Then client building an IP setting for connection host control must be done in a perfect manner to ensure connection when the trojan work in victim computer. Finally setting port proxy communication for malware to be ready for work.

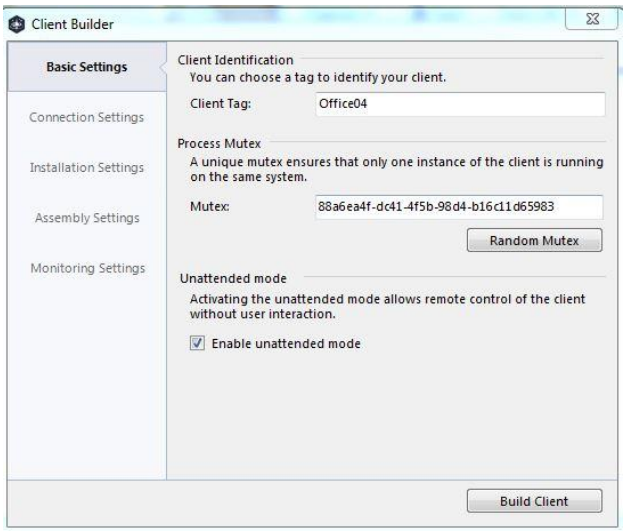

Figure (2): client builder window

7.2 Quasar features Testing

After malware was created in 7.1 , it will be transferred to victim computer ethically ,then it must be run ,and communicate with server and hacker , to ensure that 4 tests were done to prove that hacker computer can control victim computer.

A- Remote access to the client computer screen from the server

Technium Vol. 4, Issue 1 pp.68-75 (2022)
ISSN: 2668-778X
www.techniumscience.com

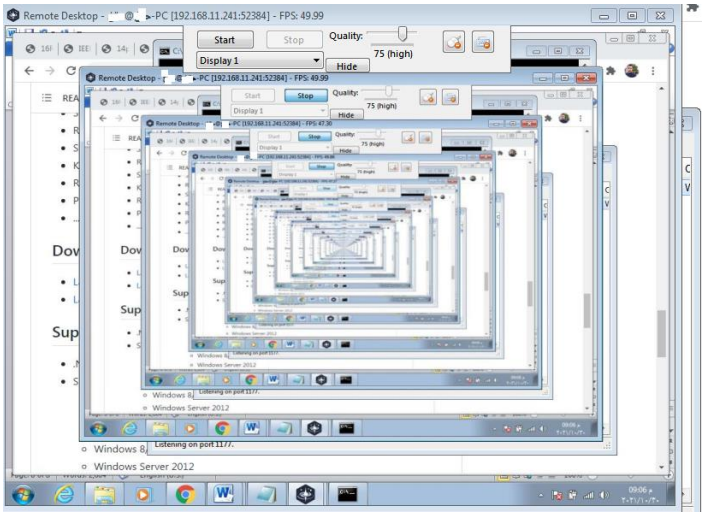

Figure (3): Remote access victim screen

B- Getting client system information remotely

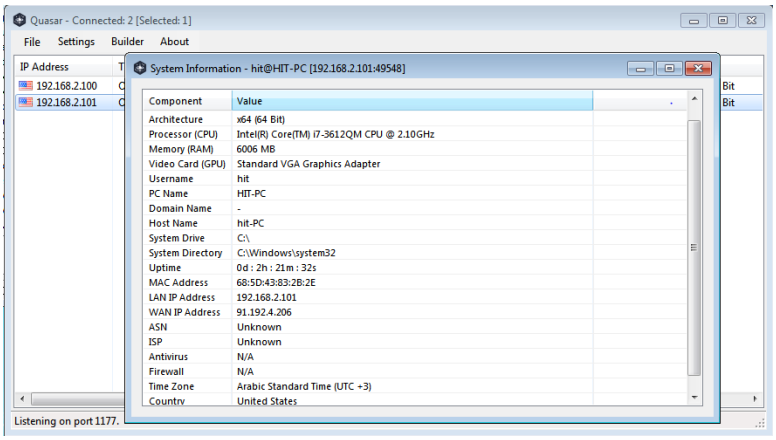

Figure (4) victim system information

C- applying client management to update or disconnect or reconnect or uninstall the client as we shown in figure (5).

D- Applying administration features of some action as shutdown or restart or standby of client system as we shown in figure (6).

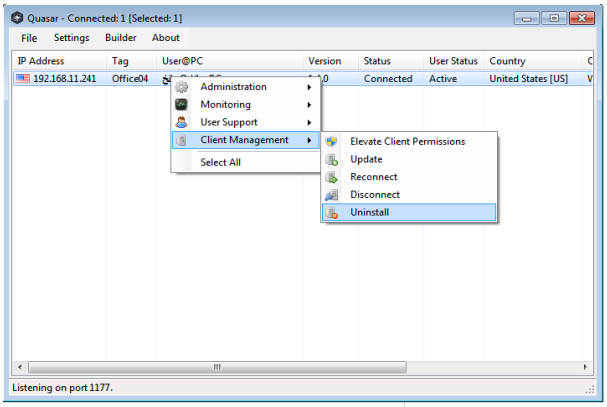

Figure (5) victim computer management

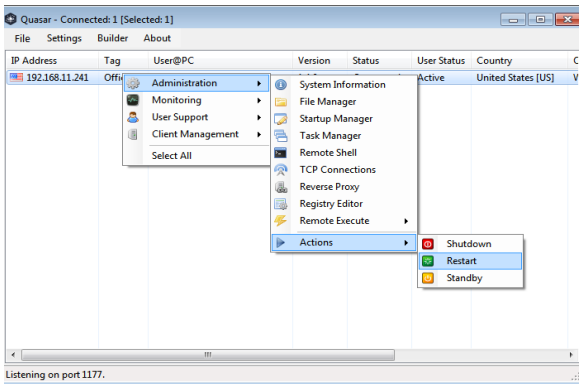

Figure (6) administration features

8- Quasar Detection

In this step for detection of Trojan quasar client the researchers have been applied C# programming language for detection of active process client. After detecting the active process it will provide some features such as abort or deny of access etc.

9- Conclusion

The researchers deal with real effects of the quasar Trojan by executing it in a real lab. This is due providing client to the victim device and start monitor it from the server device and apply the features that available inside quasar Trojan tools. The paper presents internal network witch work with static IP address and external network work with NO-IP address environment. Every type was used for specific purposes.

10- Future works

The researchers suggest to develop a special tool for discover Trojans witch can be activated dynamically when device booting and prevent access by blocking port of Trojans attackers at least for period of time.

11- Acknowledgment

Special thanks to University of Mosul and the computer Science Dept. for their Supporting us and provide computer laboratories.

12-Refrences

[1] Wei Jiang, et al ,(October-December 2019) ," A Highly Efficient Remote Access Trojan Detection Method", International Journal of Digital Crime and Forensics.

[2] Azhar Ushmani,(Nov-Dec 2018)," Ethical Hacking Cyber Security", Western Governor University Salt Lake City, Utah USA, International Journal of Information Technology (IJIT)

[3] Aldy A.Putra ,(April,2019)," Reverse Engineering for Analysis Malware Remote Access Trojan", Jurnal Edukasi dan Penelitian Informatika(JEPIN).

[4] Jean A. Yaacoub,et al,(March , 2021)," A SURVEY ON ETHICAL HACKING: ISSUES AND CHALLENGES", American University of Beirut,Electrical and Computer Engineering Department.

[5] Nagham A. Sultan, et al,(2020)," Ethical Hacking Implementation for Lime Worm Ransom ware Detection", Journal of Physics.

[6] Advaitha A., et al,(June,2019), "Ethical Hacking Tools And Techniques To Preserve Security",JETIR

[7] Bhavin A Patel, (January 2016) ,"Role of Ethical Hacking in System".

[8] Georg Thomas,et al,(October 2018), "Issues of Implied Trust in Ethical Hacking", ORBIT Journal https://github.com/quasar/Quasar

[9] N.p (Dec. 2018) ,"Certified Ethical Hacker - CEH Certification | EC-Council." EC-Council.

[10] Sai K.Manoj,et al, (May - Jun 2019)," Conceptual Oriented Analysis on the Modern Tools and Techniques to Enrich Security Vulnerabilities in Ethical Hacking", International Journal of Computer Science Trends and Technology (IJCST).

[11] Harika Reddy,et al,(June 2018)," Cyber Security and Ethical Hacking", International Journal for Research in Applied Science & Engineering Technology (IJRASET) ,

[12] https://github.com/quasar/Quasar

[13] https://any.run/malware-trends/quasar