A Survey on Botnet Attack

E.Padma
Research Scholar, Dept of CSE
mailtopadma@kanchiuniv.ac.in
SCSVMV (Deemed to be University), Enathur

Abstract: A *botnet* is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware. A network of robots used to commit cyber crime. Botnets are used to deploy malware, initiate attacks on websites, steal personal information, and defraud advertisers. The cyber criminals controlling them are called botmasters or bot herders. In the proposed work, the hackers are identified based on the entries of authentication. The authenticated users can predict their own authenticity to avoid attackers. Generally, password based attack, email address attack, man-in-the middle attack, compromised key attack has been given survey in the proposed paper. The attackers are identified based on how many times the proposed application has been compiled and run. The medium, low and high level hackers has been identified based on running the main application program.

Keywords: Botnet, Authentication, Attack, Security, Bot

I. Introduction

A **bot** is a computer that has been compromised through a malware infection and can be controlled remotely by a cybercriminal. The cybercriminal can then use the **bot** to launch more attacks, or to bring it into a collection of controlled computers, known as a **botnet**. The use of botnets to mine cryptocurrencies like Bitcoin is a growing business for cyber criminals. The authenticity for each user has been created with username and password. If the user enters into the system, the identification for the user will be verified followed by the password authentication. If unauthorized user tries to access the system he will be identified based on the attempts of trying the password by using brute force attack. The email address validation for the authorized user will be verified with the domain name service system. Only the user will be allowed to access the information with POP3 mail address checked with SMTP server for exchanging the information through the domain name server. Main-in-the middle attack will be checked based on the user entry with the registered system from the registered server. If the person tries to stole the information from the middle by hacking the information and modifying the same by resending to the receiver it can't be advisable. In such a way the threat has been identified and sent to the authorized server. With botnet, denial of service and malicious attacks has been identified. In the proposed work the attackers will be restricted to use the system. The client-server botnet structure is set up like a basic network with one main server controlling the transmission of information from each client. The botmaster uses special software to establish command and control (C&C) servers to relay instructions to each client device.

II. Proposed System

The proposed software based system has been designed using three way authentication. The Username and Password will be generated for the registered user in the system. As all the systems got connected through the network, only the registered user can have the access. One Time Password will be sent to the unregistered user if they want to access the information. It will check for the authenticity of the valid user. If the attacker wants to access the network, the password based attack will not be more effective. In Proposed system, the authentication can be dealt with registered machine in the network area. The machine once got registered, it will be identified for the uniqueness with its MAC Address. Each user will be given separate username and password. Dos attack is impossible as the network area is fully protected with three way authentication. If the user without registering in the network wants to access the information, he will use the secondary machine, To identify the unregistered user's entry he will be sent with an OTP as second way authentication. To access the encrypted information from the cloud the user will be sent with 12 digit random number to his mail id which will be an additional identity for the trusted user. The system got protected with full secure enhancement feature to avoid Dos Attack. In the proposed system, the information is in the cloud server with the encrypted format using Advance Encryption Standard Algorithm. Man in the middle attack causes no vulnerability to the proposed system, as the attacker want to communicate as a normal user also he will not be allowed to access the system. The proposed system has been protected with 12 digit random number for the valid user. The information from cloud server will get decrypt only for the authenticated user. In our proposed system, to access the encrypted information from cloud server 12 digit random number will be sent through email to the valid user. No compromised key attack will be possible for the hacker to steal the information. In the proposed system, high level security feature has been enhanced for the authorized user. The Application server attack will not attack the system because in the proposed system the decrypted information will no longer stayed in the server area. The information once retrieved will be erased automatically from the local storage area. The Cloud Server will maintain all the encrypted information with the protecting capability. So no attacker will attack the application.

III. IOT Security

IoT devices demand the following set of security requirements in order to be considered as Secure authentication, Secure bootstrapping and transmission of data, Security of IoT data, Secure access to data by authorized persons The following are various secure features of IOT: resiliency, data authentication, access control and client Privacy. Also, [6] proposes security requirements to protect IoT data transmission, which includes key management, appropriate secret key algorithms, secure routing protocols, intrusion detection technology, authentication and access control and security design. The authentication is required between two parties communicating with each other. For privileged access to services, the devices must be authenticated. The diversity of authentication mechanisms for IoT exists mainly due to the diverse heterogeneous underlying architectures and environments which support IoT devices. These environments pose a challenge for defining standard global protocol for authentication in IoT. Similarly, the authorization mechanisms ensure that the access to systems or information is provided to the authorized ones. A proper implementation of authorization and authentication results in a trustworthy environment which ensures a secure environment for communication. The attacks on IoT devices may hinder the provision of services through the conventional denial-of-service attacks. Various strategies including the sinkhole attacks, jamming adversaries or the replay attacks exploit IoT components at different layers to deteriorate the quality of service (QoS) being provided to IoT users.

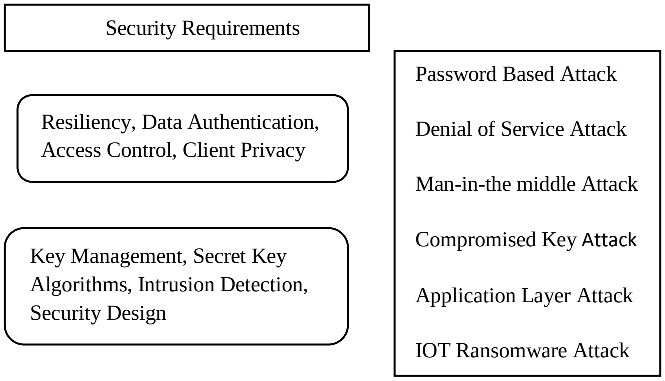

Fig 1: Representation of Security Requirements

IV. IoT Security challenges

IoT is data centric where all the devices/system connected operate based on the data that is available. When it comes to the data flow between devices, there is always a chance that the data can be accessed or read when getting transferred. From a testing standpoint, we need to check if the data is protected/encrypted when getting transferred from one device to the other. Wherever, there is an UI, we need to make sure there is a password protection on it. Evidently, the attack surface increasing the demand for more comprehensive IoT security, moreover, the lack of standardized approaches do not permit a comprehensive response to all IoT security and privacy requirements. Services such as context-awareness may risk personal privacy as critical user information may be disclosed by malicious parties

V. Literature Survey

[1] Massive botnets are used in distributed denial of service (DDoS) attacks, which are among the most intimidating types of attacks of which zombie botnet armies are capable. DDoS attacks are growing in number and severity. The increase in DDoS attacks is attributed to large scale botnets comprised of insecure IoT devices. A firewall is a tool that monitors traffic between an Internet connection and devices to detect unusual or suspicious behavior. Even if a device is infected, a firewall can keep a potential attacker from accessing all the other devices on the same network.

[2] Botnets aren’t typically created to compromise just one individual computer; they’re designed to infect millions of devices. Bot herders often deploy botnets onto computers through a trojan horse virus.

The strategy typically requires users to infect their own systems by opening email attachments, clicking on malicious pop up ads, or downloading dangerous software from a website. After infecting devices, botnets are then free to access and modify personal information, attack other computers, and commit other crimes. Botnets can infect almost any device connected directly or wirelessly to the internet. PCs, laptops, mobile devices, DVR's, smartwatches, security cameras, and smart kitchen appliances can all fall within the web of a botnet.

[3] Several powerful, record-setting distributed denial-of-service (DDoS) attacks were observed in late 2016, and they later traced to a new brand of malware known as Mirai. The DDoS traffic was produced by a variety of connected devices, such as wireless routers and CCTV cameras. Mirai malware is designed to scan the internet for insecure connected devices, while also avoiding IP addresses belonging to major corporations, like Hewlett-Packard and government agencies, such as the U.S. Department of Defense. Once it identifies an insecure device, the malware tries to log in with a series of common default passwords used by manufacturers. If those passwords don't work, then Mirai uses brute force attacks to guess the password. Once a device is compromised, it connects to C&C infrastructure and can divert varying amounts of traffic toward a DDoS target. Devices that have been infected are often still able to continue functioning normally, making it difficult to detect Mirai botnet activity from a specific device. For some internet of things (IoT) devices, such as digital video recorders, the factory password is hard coded in the device's firmware, and many devices cannot update their firmware over the internet. The Mirai source code was later released to the public, allowing anyone to use the malware to compose botnets leveraging poorly protected IoT devices.

[4] Today modern botnets are mainly comprised of infected IoT devices such as cameras, routers, DVRs, wearables and other embedded technologies. The evolution in the botnet landscape highlights the security risks from millions of Internet-connected devices configured with default credentials or manufactures who won't issue updates. Hackers can build enormous botnets consisting of a wide variety of devices. The process of capturing devices for a botnet is a fairly simple task that's mainly automated. Hackers typically compromise these devices via brute force login. They have also recently evolved to inject exploit via open ports to compromise devices. They leverage these exploits typically after a researcher discloses a vulnerability. IoT botnets continue to evolve and they are becoming more versatile. Mirai was simply a botnet comprised of infected IoT devices who left telnet open and utilized 61 default credentials found on popular devices. The IoT devices with a wide variety of payloads ranging from crypto mining and ransomware face denial of service and fraud.

[5] The reference link discussed about various attacks like Spambot A spammer will usually purchase a botnet from a bot herder in order to use the infected computers to send out the spam e-mails, concealing where the attacks are actually originating. Spyware is any malware that can be used to gain information from its target or targets, anything from passwords and credit card information to the physical data contained within files. Click fraud – This form of remote control can allow a bot herder to surreptitiously click links on Web sites and online advertising, bolstering numbers for advertisers and producing more money. Dial-up bots look to try to connect to dial-up modems and force them to dial phone numbers. Sometimes the effect is to tie up the line, eventually forcing the user to change numbers. Other times, the effect is to dial into premium phone number (1-900 numbers) in order to rack up charges on someone else's bill. It goes without saying that this type of attack is beginning to go by the wayside, as more and more people move away from dial-up modems to broadband connections.

VI. Discussion about various Attacks

A. Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to the network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.

- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

B. Denial-of-Service Attack

Unlike a password-based attack, the denial-of-service attack prevents normal use of the computer or network by valid users. After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

C. Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section. The man-in-the-middle concept is where an attacker or hacker is looking to interrupt and breach communications between two separate systems. It can be a dangerous attack because it is one where the attacker secretly intercepts and transmits messages between two parties when they are under the belief that they are communicating directly with each other. As the attacker has the original communication, they can trick the recipient into thinking they are still getting a legitimate message. Many cases have already been reported within this threat area, cases of hacked vehicles and hacked "smart refrigerators". These attacks can be extremely dangerous in the IoT, because of the nature of the "things" being hacked. For example, these devices can be anything from industrial tools, machinery, or vehicles to innocuous connected "things" such as smart TV's or garage door openers.

D. Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

E. Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

F. DDoS attacks

A denial of service (DoS) attack happens when a service that would usually work is unavailable. There can be many reasons for unavailability, but it usually refers to infrastructure that cannot cope due to capacity overload. In a Distributed Denial of Service (DDoS) attack, a large number of systems maliciously attack one target. This is often done through a botnet, where many devices are programmed (often unbeknownst to the owner) to request a service at the same time.In comparison to hacking attacks like phishing or brute-force attacks, DoS doesn't usually try to steal information or leads to security loss, but the loss of reputation for the affected company can still cost a lot of time and money. Often customers also decide to switch to a competitor, as they fear security issues or simply can't afford to have an unavailable service. Often a DoS attack lends itself to activists and blackmailers.

G. IoT ransomware attacks

Ransomware usually goes after computers and networks that house the mission-critical data necessary to maintain the day-to-day operations of a business. Such targeting ensures that once this data has been encrypted and rendered useless, the organization has adequate incentive to purchase the cryptocurrency (typically Bitcoin) being demanded by the hacker to release its data.

VII Result Analysis

The result of the proposed system has been audited using Acunetix Website Security Audit Report. Various classifications of results had been proved based on the possible attacks. The proposed application has been made run by using the web analyser tool and the following classification of results has been obtained.

A. Sample Result Page

Login page password-guessing attack

Classification
Base Score: 5.0
- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CVSS

Base Score: 5.3
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: Low

Application error message

Classification
Base Score: 5.0
- Access Vector: Network
- Access Complexity: Low
- Authentication: None
- Confidentiality Impact: Partial
- Integrity Impact: None
- Availability Impact: None

CVSS
Base Score: 7.5
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None
- Scope: Unchanged
- Confidentiality Impact: High
- Integrity Impact: None
- Availability Impact: None

Email address vulnerability

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Classification

Email address found
View HTTP headers
View HTML response
Launch the attack with HTTP Editor
Retest alert(s)
Mark this alert as a false positive
CWE CWE-200
CVSS Base Score: **5.0** -
AV:N/AC:L/Au:N/C:P/I:N/A:N
Access Vector: Network
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None

CVSS3 Base Score: **7.5** -
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality Impact: High
Integrity Impact: None

VIII. Conclusion

The research paper deals with attacks and the related features with the interconnected network as Botnet. The authenticated user only can have the access to the system with the trusted third party. The authentication can be dealt with registered machine in the network area. The system got protected with full secure enhancement feature to avoid Dos Attack. In the proposed system, the information is in the cloud server with the encrypted format using Advance Encryption Standard Algorithm. The information once retrieved will be erased automatically from the local storage area. The Cloud Server will maintain all the encrypted information with the protecting capability. So no attacker will attack the application.

IX. References

[1]https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/zombie-iot-botnets/
[2]https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/
[3]https://searchsecurity.techtarget.com/definition/botnet
[4] Daniel Smith, “IoT Botnets on the Rise” A Survery Paper on October 2, 2018
[5]https://www.nortonsecurityonline.com/security-center/bots.html
[6] K. Zhao and L. Ge, “A survey on the internet of things security,” in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 663–667, IEEE, 2013.
[7] Diego Mendez et.al., “Internet of Things: Survey on Security and Privacy” July 2017
[8] Minhaj Ahmad Khana et.al. “IoT Security: Review, Blockchain Solutions, and Open Challenges” Article in Future Generation Computer Systems · November 2017 DOI:10.1016/j.future.2017.11.022