iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: III Month of publication: March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3039

Hacking and Cyber Security

Dinesh Kumar P[1]

[1] *Mca, Ganadipathy Tulsi's Jain Engineering College, Vellor-632102*

Abstract: ***Hacking is one of the important issues while using internet. In this paper we are going to demonstrate on how the hackers are hacking the data of our systems. This method is composed of two parts: first, hacking stories by hacking / hacker levels, Second, to prevent users from hackers. The major problems in the IT are hacking only. No one as figured how to do stop this problem. Main purpose of this paper is to promote the security in the entire situation. We also analysed Hacking and Cyber Security techniques to solve those problems and recover the issue which we will focus. Some of the precautions and remedies are demonstrating in this scenario and we would not repeat the problem same in the future.***

Keywords: Password Attack, DDOS Attack, DDOS Botnet, DOS vs DDOS, Malware

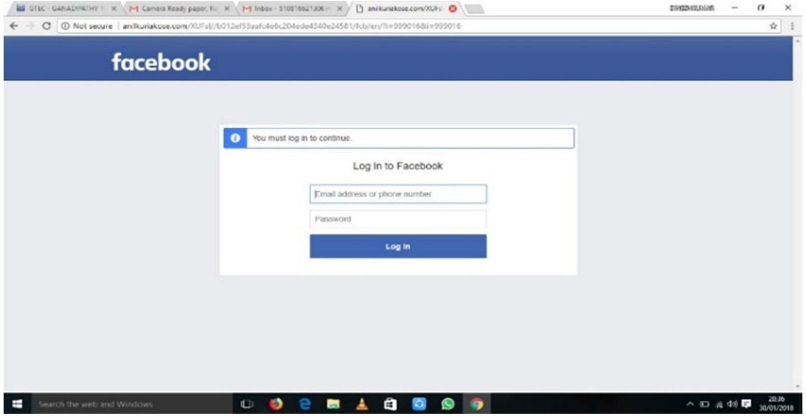
I. PASSWORD ATTACK

A. Brute Force Attack

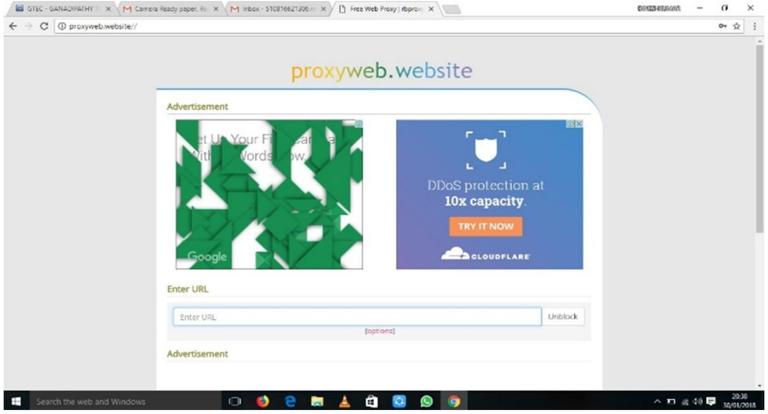
A hacker uses a computer program or script to try to log in with possible password combinations, usually starting with the easiest-to-guess passwords. (So just think: if a hacker has a company list, he or she can easily guess usernames. If even one of the users has a "Password123", he will quickly be able to get in)

B. Victom Proxy Attack

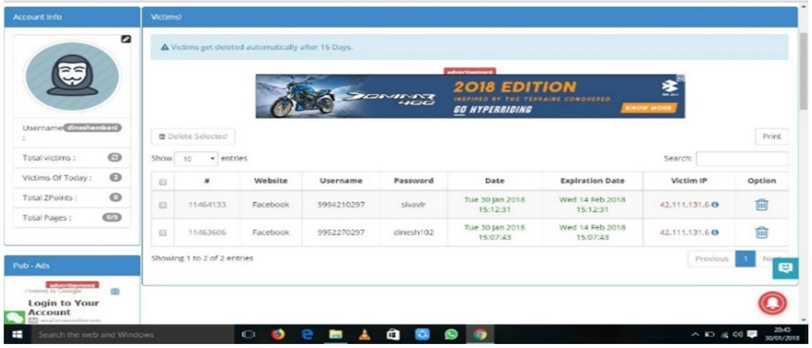
It is a Web password cracking tool that can work through a proxy. Victum uses send the victom link through email or social media. After we can use the link to login your password and user name is hacked easily.


facebook
You must log in to continue.
Log In to Facebook
Email address or phone number
Password
Log In
Search the web and Windows

Sample Victom Page



Proxy Error



Account Info

Username : dineshambani

Total victims :	2
Victims Of Today :	2
Total ZPoints :	0
Total Pages :	0/5

Victims!

Victims get deleted automatically after 15 Days.

Show 10 entries

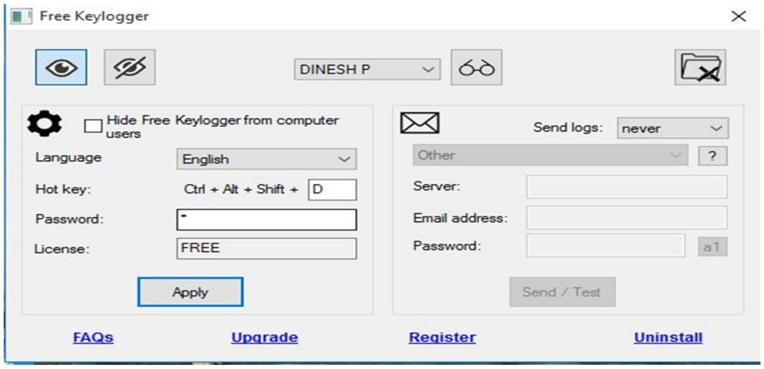
	#	Website	Username	Password	Date	Expiration Date	Victim IP	Option
□	11464133	Facebook	9994210297	sivavlr	Tue 30 Jan 2018 15:12:31	Wed 14 Feb 2018 15:12:31	42.111.131.6	
□	11463606	Facebook	9952270297	dinesh102	Tue 30 Jan 2018 15:07:43	Wed 14 Feb 2018 15:07:43	42.111.131.6	

Showing 1 to 2 of 2 entries

Victom Admin Page

C. Key Logger Attack

A hacker uses a program to track all of a user’s keystrokes. So at the end of the day, everything the user has typed—including their login IDs and passwords—have been recorded. A key logger attack is different than a brute force or dictionary attack in many ways. Not the least of which, the key logging program used is malware (or a full-blown virus) that must first make it onto the user’s device (often the user is tricked into downloading it by clicking on a link in an email). Key logger attacks are also different because stronger passwords don’t provide much protection against them, which is one reason that multi-factor authentication (MFA) is becoming a must-have for all businesses and organizations



Free Keylogger

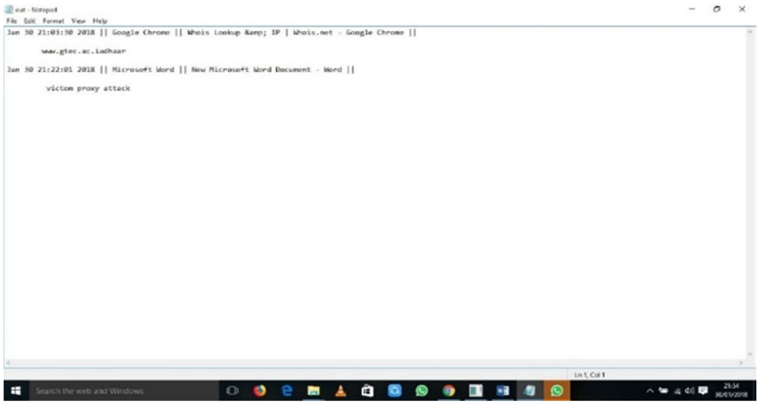
DINESH P

□ Hide Free Keylogger from computer users

Language	English
Hot key:	Ctrl + Alt + Shift + D
Password:	*
License:	FREE

Send logs:	never
	Other
Server:	
Email address:	
Password:	

Keylogger Tool



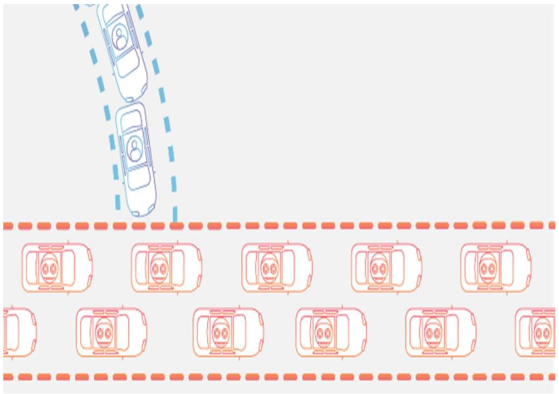
out - Notepad

```
Jan 30 21:03:30 2018 || Google Chrome || Whois Lookup &amp; IP | Whois.net - Google Chrome ||

        www.gtec.ac.iadhaar

Jan 30 21:22:01 2018 || Microsoft Word || New Microsoft Word Document - Word ||

         victom proxy attack
```

Victom Stored

D. Ddos attack.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.

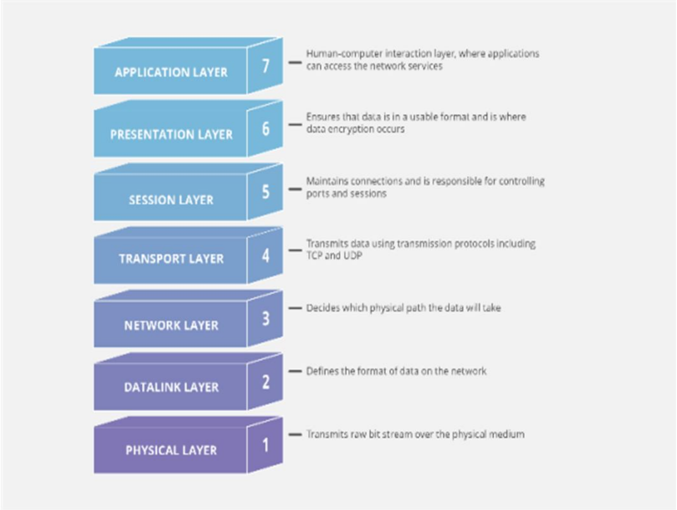


Computers and other machines (such as IoT devices) are infected with malware, turning each one into a bot (or zombie). The attacker then has remote control over the group of bots, which is called a botnet.

Once a botnet has been established, the attacker is able to direct the machines by sending updated instructions to each bot via a method of remote control. When the IP address of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

What are common types of DDoS attacks?

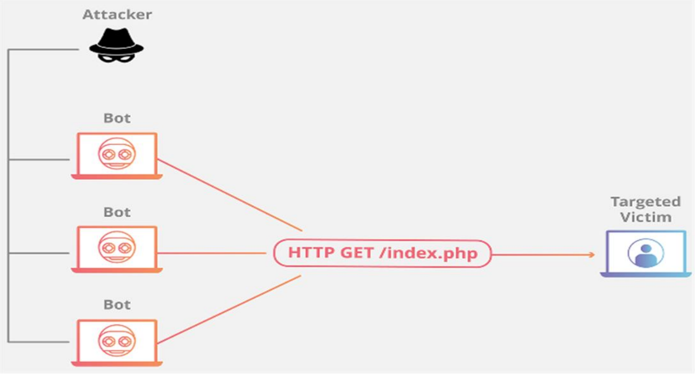
Different DDoS attack vectors target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made. A network connection on the Internet is composed of many different components or “layers”. Like building a house from the ground up, each step in the model has a different purpose. The OSI model, shown below, is a conceptual framework used to describe network connectivity in 7 distinct layers.


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may make use one or multiple different attack vectors, or cycle attack vectors potentially based on counter measures taken by the target.

E. The Goal of the Attack

Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the resources of the target. The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is cheap to execute on the client side, and can be expensive for the target server to respond to as the server often must load multiple files and run database queries in order to create a web page. Layer 7 attacks are difficult to defend as the traffic can be difficult to flag as malicious.



Application Layer Attack Example

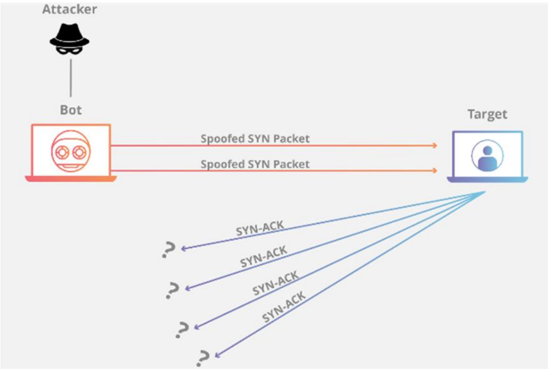
F. HTTP Flood

This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service.

This type of attack ranges from simple to complex. Simpler implementations may access one URL with the same range of attacking IP addresses, referrers and user agents. Complex versions may use a large number of attacking IP addresses, and target random urls using random referrers and user agents. Protocol Attacks

G. The Goal of the Attack:

Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by consuming all the available state table capacity of web application servers or intermediate resources like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.



Protocol Attack Example

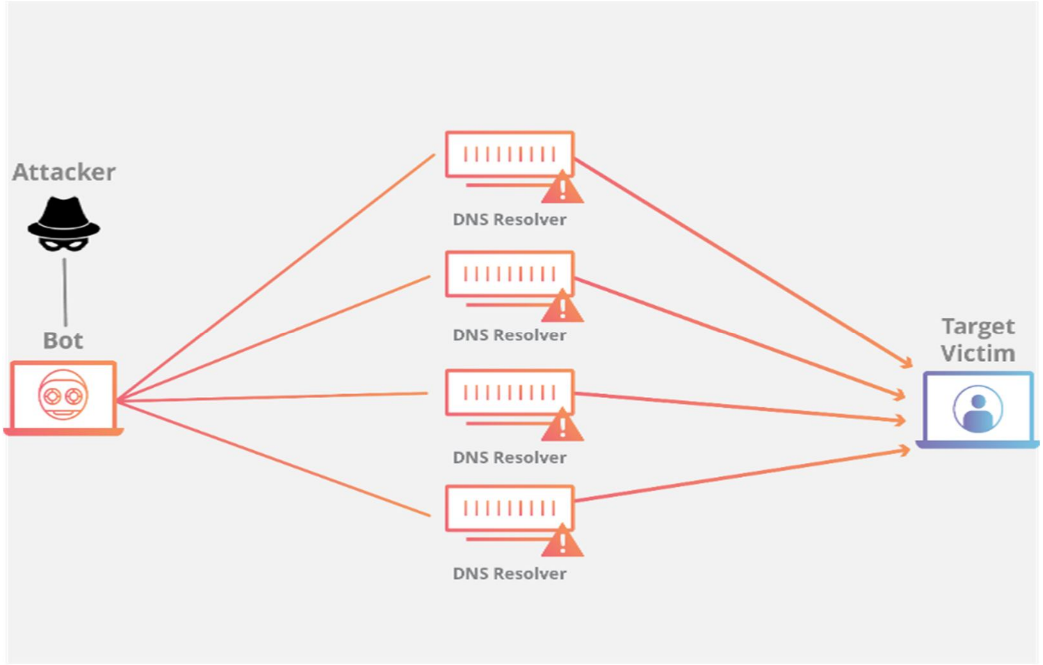
H. SYN Flood

A SYN Flood is analogous to a worker in a supply room receiving requests from the front of the store. The worker receives a request, goes and gets the package, and waits for confirmation before bringing the package out front. The worker then gets many more package requests without confirmation until they can't carry any more packages, become overwhelmed, and requests start going unanswered.

This attack exploits the TCP handshake by sending a target a large number of TCP "Initial Connection Request" SYN packets with spoofed source IP addresses. The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target's resources in the process.

I. The Goal of the Attack

This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.



Amplification Example

J. DNS Amplification

A DNS Amplification is like if someone were to call a restaurant and say “I’ll have one of everything, please call me back and tell me my whole order,” where the callback phone number they give is the target’s number. With very little effort, a long response is generated.

By making a request to an open DNS server with a spoofed IP address (the real IP address of the target), the target IP address then receives a response from the server. The attacker structures the request such that the DNS server responds to the target with a large amount of data. As a result, the target receives an amplification of the attacker’s initial query.

K. What is the process for mitigating a DDoS attack?

The key concern in mitigating a DDoS attack is differentiating between attack and normal traffic. For example, if a product release has a company’s website swamped with eager customers, cutting off all traffic is a mistake. If that company suddenly has a surge in traffic from known bad actors, efforts to alleviate an attack are probably necessary. The difficulty lies it telling apart the real customer and the attack traffic.

In the modern Internet, DDoS traffic comes in many forms. The traffic can vary in design from un-spoofed single source attacks to complex and adaptive multi-vector attacks. A multi-vector DDoS attack uses multiple attack pathways in order to overwhelm a target in different ways, potentially distracting mitigation efforts on any one trajectory. An attack that targets multiple layers of the protocol stack at the same time, such as a DNS amplification (targeting layers 3/4) coupled with a HTTP flood (targeting layer 7) is an example of multi-vector DDoS.

Mitigating a multi-vector DDoS attack requires a variety of strategies in order to counter different trajectories. Generally speaking, the more complex the attack, the more likely the traffic will be difficult to separate from normal traffic - the goal of the attacker is to blend in as much as possible, making mitigation as inefficient as possible. Mitigation attempts that involve dropping or limiting traffic indiscriminately may throw good traffic out with the bad, and the attack may also modify and adapt to circumvent countermeasures. In order to overcome a complex attempt at disruption, a layered solution will give the greatest benefit.

Black Hole Routing

One solution available to virtually all network admins is to create a blackhole route and funnel traffic into that route. In its simplest form, when blackhole filtering is implemented without specific restriction criteria, both legitimate and malicious network traffic is routed to a null route or blackhole and dropped from the network. If an Internet property is experiencing a DDoS attack, the property’s Internet service provider (ISP) may send all the site’s traffic into a blackhole as a defense.

L. Rate Limiting

Limiting the number of requests a server will accept over a certain time window is also a way of mitigating denial-of-service attacks. While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be insufficient to handle a complex DDoS attack effectively. Nevertheless, rate limiting is a useful component in an effective DDoS mitigation strategy. Learn about Cloud flare’s rate limiting.

Web Application Firewall

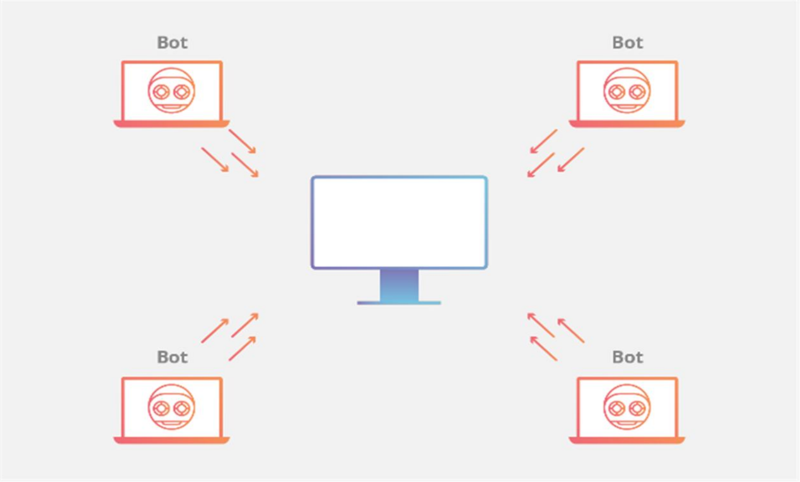
A Web Application Firewall (WAF) is a tool that can assist in mitigating a layer 7 DDoS attack. By putting a WAF between the Internet and a origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic. By filtering requests based on a series of rules used to identify DDoS tools, layer 7 attacks can be impeded. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack. Learn about Cloud flare’s WAF.

This mitigation approach uses an Anycast network to scatter the attack traffic across a network of distributed servers to the point where the traffic is absorbed by the network. Like channeling a rushing river down separate smaller channels, this approach spreads the impact of the distributed attack traffic to the point where it becomes manageable, diffusing any disruptive capability.

The reliability of an Anycast network to mitigate a DDoS attack is dependent on the size of the attack and the size and efficiency of the network. An important part of the DDoS mitigation implemented by Cloudflare is the use of an Anycast distributed network. Cloudflare has a 15 Tbps network, which is an order of magnitude greater than the largest DDoS attack recorded.

If you are currently under attack, there are steps you can take to get out from under the pressure. If you are on Cloudflare already, you can follow these steps to mitigate your attack. The DDoS protection that we implement at Cloudflare is multifaceted in order to mitigate the many possible attack vectors. Learn more about Cloudflare's DDoS protection and how it works.

M. Ddos botnet.



A botnet refers to a group of computers which have been infected by malware and have come under the control of a malicious actor. The term botnet is a portmanteau from the words robot and network and each infected device is called a bot. Botnets can be designed to accomplish illegal or malicious tasks including sending spam, stealing data, ransomware, fraudulently clicking on ads or distributed denial-of-service (DDoS) attacks.

While some malware, such as ransomware, will have a direct impact on the owner of the device, DDoS botnet malware can have different levels of visibility; some malware is designed to take total control of a device, while other malware runs silently as a background process while waiting silently for instructions from the attacker or “bot herder.”

Self-propagating botnets recruit additional bots through a variety of different channels. Pathways for infection include the exploitation of website vulnerabilities, Trojan horse malware, and cracking weak authentication to gain remote access. Once access has been obtained, all of these methods for infection result in the installation of malware on the target device, allowing remote control by the operator of the botnet. Once a device is infected, it may attempt to self propagate the botnet malware by recruiting other hardware devices in the surrounding network.

While it's infeasible to pinpoint the exact numbers of bots in a particular botnet, estimations for total number of bots in a sophisticated botnet have ranged in size from a few thousand to greater than a million.

N. Why are botnets created?

Reasons for using a botnet ranges from activism to state-sponsored disruption, with many attacks being carried out simply for profit. Hiring botnet services online is relatively inexpensive, especially in relationship to the amount of damage they can cause. The barrier to creating a botnet is also low enough to make it a lucrative business for some software developers, especially in geographic locations where regulation and law enforcement are limited. This combination has lead to a proliferation of online services offering attack-for-hire.

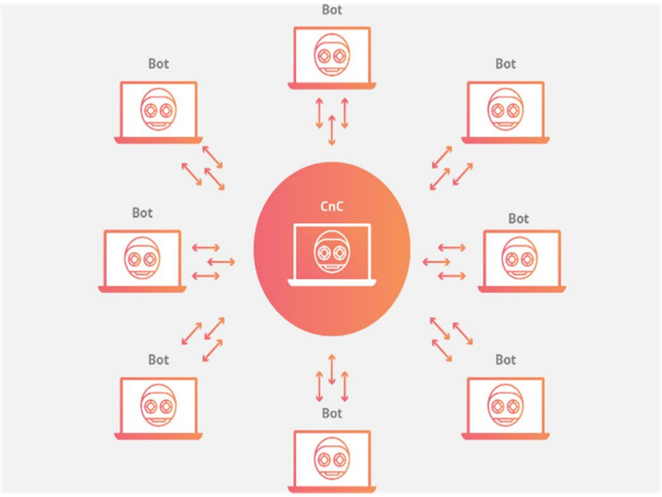
O. How is a botnet controlled?

A core characteristic of a botnet is the ability to receive updated instructions from the bot herder. The ability to communicate with each bot in the network allows the attacker to alternate attack vectors, change the targeted IP address, terminate an attack, and other customized actions. Botnet designs vary, but the control structures can be broken down into two general categories.

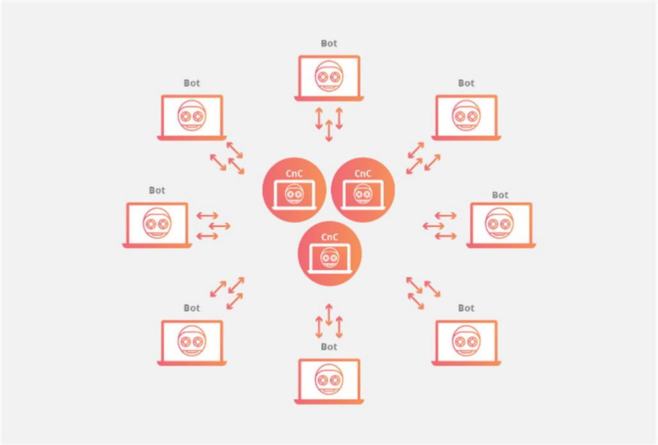
P. The client/server botnet model

The client/server model mimics mimics the traditional remote workstation workflow where each individual machine connects to a centralized server (or a small number of centralized servers) in order to access information. In this model each bot will connect to a command-and-control center (CnC) resource like a web domain or an IRC channel in order to receive instructions. By using these centralized repositories to serve up new commands for the botnet, an attacker simply needs to modify the source material that each botnet consumes from a command center in order to update instructions to the infected machines. The centralized server in control of the botnet may be a device owned and operated by the attacker, or it may be an infected device.

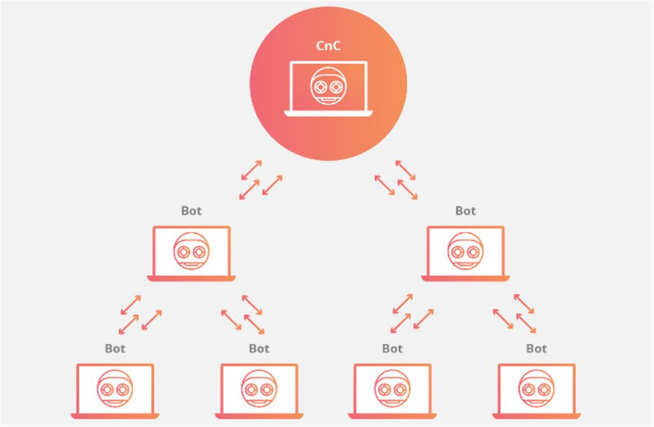
A number of popular centralized botnet topologies have been observed, including:



Star Network Topology



Multi Server Network Topology



Hierarchical Network Topology

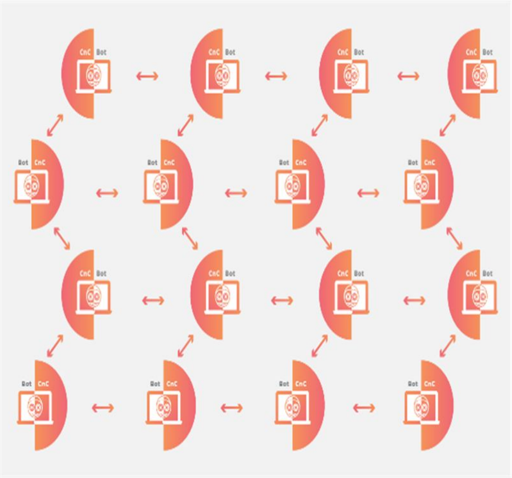
In any of these client/server models, each bot will connect to a command center resource like a web domain or an IRC channel in order to receive instructions. By using these centralized repositories to serve up new commands for the botnet, an attacker simply needs to modify the source material that each botnet consumes from a command center in order to update instructions to the infected machines.

Hand-in-hand with the simplicity of updating instructions to the botnet from a limited number of centralized sources is the vulnerability of those machines; in order to remove a botnet with a centralized server, only the server needs to be disrupted. As a result of this vulnerability, the creators of botnet malware have evolved and moved towards a new model that is less susceptible to disruption via a single or a few points of failure.

Q. The peer-to-peer botnet model

To circumvent the vulnerabilities of the client/server model, botnets have more recently been designed using components of decentralized peer-to-peer filesharing. Embedding the control structure inside the botnet eliminates the single point-of-failure present in a botnet with a centralized server, making mitigation efforts more difficult. P2P bots can be both clients and command centers, working hand-in-hand with their neighboring nodes to propagate data.

Peer to peer botnets maintain a list of trusted computers with which they can give and receive communications and update their malware. By limiting the number of other machines the bot connects to, each bot is only exposed to adjacent devices, making it harder to track and more difficult to mitigate. Lacking a centralized command server makes a peer-to-peer botnet more vulnerable to control by someone other than the botnet’s creator. To protect against loss of control, decentralized botnets are typically encrypted so that access is limited.



Peer-to-Peer botnet model

How do IoT devices become a botnet?

No one does their Internet banking through the wireless CCTV camera they put in the backyard to watch the bird feeder, but that doesn't mean the device is incapable of making the necessary network requests. The power of IoT devices coupled with weak or poorly configured security creates an opening for botnet malware to recruit new bots into the collective. An uptick in IoT devices has resulted in a new landscape for DDoS attacks, as many devices are poorly configured and vulnerable.

If an IoT device's vulnerability is hardcoded into firmware, updates are more difficult. To mitigate risk, IoT devices with outdated firmware should be updated as default credentials commonly remain unchanged from the initial installation of the device. Many discount manufacturers of hardware are not incentivized to make their devices more secure, making the vulnerability posed from botnet malware to IoT devices remain an unsolved security risk.

R. How is an existing botnet disabled?

Disable a botnet's control centers:

Botnets designed using a command-and-control schema can be more easily disabled once the control centers can be identified. Cutting off the head at the points of failure can take the whole botnet offline. As a result, system administrators and law enforcement officials focus on closing down the control centers of these botnets. This process is more difficult if the command center operates in a country where law enforcement is less capable or willing to intervene.

S. Eliminate Infection on Individual Devices

For individual computers, strategies to regain control over the machine include running antivirus software, reinstalling software from a safe backup, or starting over from a clean machine after reformatting the system. For IoT devices, strategies may include flashing the firmware, running a factory reset or otherwise formatting the device. If these option are infeasible, other strategies may be available from the device's manufacturer or a system administrator.

T. How can you protect Devices from Becoming Part of A Botnet?

Create secure passwords: For many vulnerable devices, reducing exposure to botnet vulnerability can be as simple as changing the administrative credentials to something other than the default username and password. Creating a secure password makes brute force cracking difficult, creating a very secure password makes brute force cracking virtually impossible. For example, a device infected with the Mirai malware will scan IP addresses looking for responding devices. Once a device responds to a ping request, the bot will attempt to login to that found device with a preset list of default credentials. If the default password has been changed and a secure password has been implemented, the bot will give up and move on, looking for more vulnerable devices.

U. Allow only Trusted Execution of Third-Party Code

If you adopt the mobile phone model of software execution, only whitelisted applications may run, granting more control to kill software deemed as malicious, botnets included. Only an exploitation of the supervisor software (i.e. kernel) may result in exploitation of the device. This hinges on having a secure kernel in the first place, which most IoT devices do not have, and is more applicable to machines that are running third party software.

Periodic system wipe/restores:

Restoring to a known good state after a set time will remove any gunk a system has collected, botnet software included. This strategy, when used as a preventative measure, ensures even silently running malware gets thrown out with trash.

Implement good ingress and egress filtering practices Other more advanced strategies include filtering practices at network routers and firewalls. A principle of secure network design is layering: you have the least restriction around publicly accessible resources, while continually beefing up security for things you deem sensitive. Additionally, anything that crosses these boundaries has to be scrutinized: network traffic, usb drives, etc. Quality filtering practices increase the likelihood that DDoS malware and their methods of propagation and communication will be caught before entering or leaving the network.

If you are currently under attack, there are steps you can take to get out from under the pressure. If you are on Cloudflare already, you can follow these steps to mitigate your attack. The DDoS protection that we implement at Cloudflare is multifaceted in order to mitigate the many possible attack vectors. Learn more about Cloudflare's DDoS Protection.

Denial-of-service (DoS) attacks are the precursor to DDoS attacks. Historically, DoS attacks were a primary method for disrupting computer systems on a network. DoS attacks originate from a single machine and can be very simple; a basic flood attack can be accomplished by sending more ICMP (ping) requests to a targeted server then it is able to process and respond to efficiently. Just about anyone with a networked machine is able to launch this type of attack by using built-in terminal commands. More complex DoS attacks may involve using packet fragmentation, such as the now largely defunct_Ping of Death attack.

V. DoS vs DDoS

Attacks involving multiple computers or other devices all targeting the same victim are considered DDoS attacks due to their distributed design. Of the two, DDoS attacks are more prevalent and damaging in the modern Internet. Due to the relative simplicity of purchasing or creating a group of malicious machines capable of sending a massive amount of Internet traffic to a target, bad actors are able to use networks of devices such as botnets to flood a target with requests. By utilizing a large network of machines infected with malware, a malicious actor is able to leverage the attack traffic of a large number of computer systems. With the rise of poorly secured Internet of Things (IoT) devices, more electronic hardware is able to be commandeered for nefarious puposes. Not all distributed attacks involve botnets; some attack tools leverage volunteers who work together by sharing their available computer resources to take part in a common goal. The hacker group Anonymous has used DoS and DDoS tools, coupled with willing parties, for this very purpose.

W. How are DoS/DDoS attack tools categorized?

A number of different attack tools or “stressors” are available for free on the Internet. At their core, some of these tools have legitimate purposes, as security researchers and network engineers may at times perform stress tests against their own networks. Some attack tools are specialized and only focus on a particular area of the protocol stack, while others will be designed to allow for multiple attack vectors. Attack tools can be broadly characterized into several groups:

Low and slow attack tools As the name implies, these types of attack tools both use a low volume of data and operate very slowly. Designed to send small amounts of data across multiple connections in order to keep ports on a targeted server open as long as possible, these tools continue to utilize server resources until a targeted server is unable to maintain additional connections. Uniquely, low and slow attacks may at times be effective even when not using a distributed system such as a botnet and are commonly used by a single machine.

Application layer (L7) attack tools These tools target layer 7 of the OSI model, where Internet-based requests such as HTTP occur. Using a type of HTTP flood attack to overwhelm a target with HTTP GET and POST requests, a malicious actor can launch attack traffic that is difficult to distinguish from normal requests made by actual visitors.

Protocol and transport layer (L3/L4) attack tools Going further down the protocol stack, these tools utilize protocols like UDP to send large volumes of traffic to a targeted server, such as during a UDP flood. While often ineffective individually, these attacks are typically found in the form of DDoS attacks where the benefit of additional attacking machines increases the effect.

What are commonly used DoS/DDoS attack tools?

X. A few commonly Used Tools Include

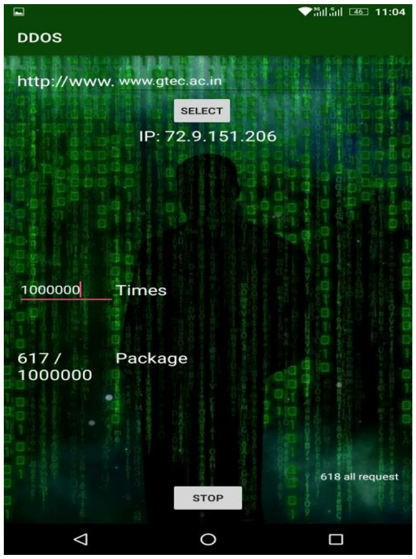
Low Orbit Ion Cannon (LOIC) The LOIC is an open-source stress testing application. It allows for both TCP and UDP protocol layer attacks to be carried out using a user-friendly WYSIWYG interface. Due to the popularity of the original tool, derivatives have been created that allow attacks to be launched using a web browser.

High Orbit Ion Cannon (HOIC)

This attack tool was created to replace the LOIC by expanding its capabilities and adding customizations. By utilizing the HTTP protocol, the HOIC is able to launch targeted attacks that are difficult to mitigate. The software is designed to have a minimum of 50 people working together in a coordinated attack effort.

Y. Slowloris

Apart from being a slow-moving primate, Slowloris is an application designed to instigate a low and slow attack on a targeted server. The elegance of Slowloris is the limited amount of resources it needs to consume in order to create a damaging effect.



http://www. www.gtec.ac.in

IP: 72.9.151.206

1000000 Times

617 / 1000000 Package

618 all request

LLOC Tool

Z. R.U.D.Y (R-U-Dead-Yet)

This is another low and slow attack tool designed to allow the user to easily launch attacks using a simple point-and-click interface. By opening multiple HTTP POST requests and then keeping those connections open as long as possible, the attack aims to slowly overwhelm the targeted server.

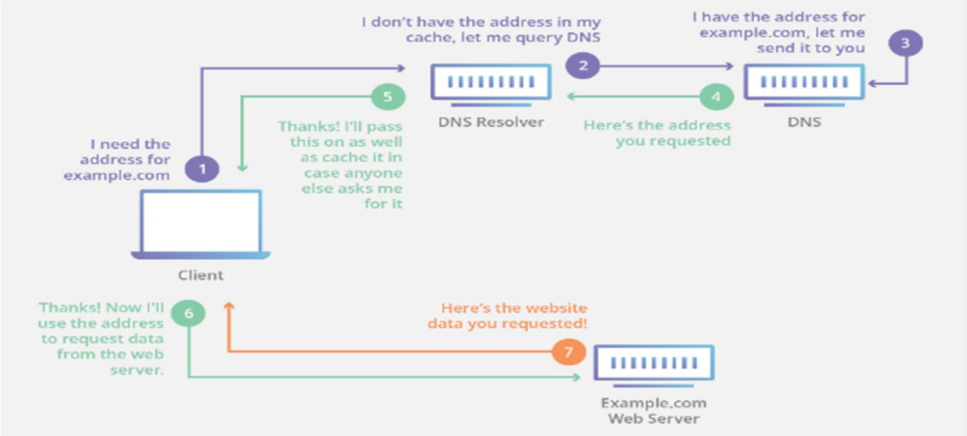
AA. DOMAIN NAME SYSTEM

DNS is often referred to as the phonebook of the internet, when a user types a web address into their browser, DNS is what connects that user with the web site they are seeking. DNS stands for Domain Name System, and the DNS maintains a directory of every website on the internet.

A computer can only find a website using it's IP address, which is a long, punctuated string of numbers, such as 192.168.1.1 in the older IPv4 format, or 2400:cb00:2048:1::c629:d7a2 in the new IPv6 . These addresses can be hard for humans to remember, and on top of that, the IP addresses for some websites are dynamic and can change periodically. DNS makes it easier for people to access websites by letting them use human-friendly web addresses, also known as URLs.

For example, a current IPv6 IP address for Cloudflare.com is 2400:cb00:2048:1::c629:d7a2. Instead of memorizing that address, a user can type 'www.cloudflare.com' into their browser. When that happens, the browser sends out a request to DNS, and DNS returns a response telling the browser the IP address of that website, and the browser then sends a request to that IP address which responds with the website's data.

BB. How does a DNS request work?



I don't have the address in my cache, let me query DNS
I have the address for example.com, let me send it to you
3
2
5
4
DNS Resolver
DNS
Thanks! I'll pass this on as well as cache it in case anyone else asks me for it
Here's the address you requested
I need the address for example.com
1
Client
Thanks! Now I'll use the address to request data from the web server.
6
Here's the website data you requested!
7
Example.com Web Server

CC. Malwares

Malware, a portmanteau from the words malicious and software, is a general term which can refer to viruses, worms, Trojans, ransomware, spyware, adware, and other types of harmful software. A key distinction of malware is that it needs to be intentionally malicious; any software that unintentionally causes harm is not considered to be malware.

The general goal of malware is to disrupt the normal operations of a device. This disruption can range in purpose from displaying ads on a device without consent to gaining root access of a computer. Malware may attempt to obfuscate itself from the user in order to collect information quietly or it may lock the system and hold data for ransom. In DDoS attacks, malware such as Mirai affects vulnerable devices, turning them into bots under the control of the attacker. Once modified, these devices can then be used to carry out DDoS attacks as part of a botnet.

The creation of malware arose as the result of experiments and pranks by computer programmers, but discovery of the commercial potential it creates has turned malware development into a lucrative black market industry. Today, many attackers offer to create malware and/or launch malware attacks in return for compensation.

What are some common types of malware?

Spyware - As the name implies, spyware is used to spy on a user’s behavior. Spyware can be used monitor a user’s web browsing activity, display unwanted ads to the user, and modify affiliate marketing streams. Some spyware uses what’s called a keylogger to record the user’s keystrokes, giving the attacker access to sensitive information including usernames and passwords.

Viruses - A virus is a malicious program that can be embedded in an operating system or a piece of software; the victim needs to run the operating system or open the infected file to be affected.

Worms - Unlike viruses, worms self-replicate and transmit themselves over a network, so the user doesn’t have to run any software to become a victim, just being connected to the infected network is enough.

Trojan Horses - These are pieces of malware that come hidden inside other useful software to entice the user to install them. Pirated copies of popular software are often infected with trojan horses.

Rootkits - These software packages are designed to modify an operating system so that unwanted installations are hidden from the user. A famous example is the 2005 Sony rootkit scandal, when Sony sold 22 million music CDs that came infected with a rootkit that would secretly install software intended to disrupt CD-copying on the purchaser’s computer. This rootkit opened up the door for other attackers to target infected computers with additional malware.

Ransomware - This software can encrypt files or even an entire operating system on a computer or network and keep them encrypted until a ransom is paid to the attacker. The emergence of bitcoin and other cryptocurrency has created a surge in the popularity of ransomware attacks, as attackers can anonymously accept currency and minimize the risk of getting caught.

DD. What are the risk factors for malware infection?

Security bugs - Software such as operating systems, web browsers, and browser plugins can contain vulnerabilities for attackers to exploit.

User Error - Users opening software from unknown software or booting their computers from untrusted hardware can create a serious risk.

OS Sharing - The use of a single operating system by every computer on a network also increases malware infection risk; if all the machines are on the same OS, then it is possible for one worm to infect them all.

No one can be completely impervious to malware attacks; new attacks are constantly being developed to challenge even the most secure systems. But there are plenty of ways to minimize vulnerability to malware attacks, these include:

Anti-virus and anti-malware software - Running regular scans on a computer or network is crucial to detecting threats before they can spread.

Website security scans - People who have websites should be aware that malware can target a website’s software to view private files, hijack the site, and potentially even harm that site’s visitors with forced malware downloads. Running regular security scans on a website can help to catch these threats.

Web Application Firewall (WAF) - Another good resource for webmasters is a WAF, which can block malware at the edge of a network and prevent it from reaching a site’s origin server.

Air gap isolation - Considered to be a last resort, air gap isolation means cutting a computer or network off from all outside networks and Internet communication by disabling any hardware that would make communications possible. Even this isn’t a fool proof defense and has been compromised by tactics such as the ‘dropped drive’ attack, where usb drives are dropped in a company’s parking lot in hopes that a curious employee will find one and plug it into a computer on the network, infecting the isolated network with malware.

II. CONCLUSION

This paper addressed hacking from several perspectives hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. On the other hand hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole

REFERENCE BOOKS

[1] Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002
[2] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002
[3] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011

REFERENCE LINKS

[1] European Union cyberterrorism policy announcement: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/689&format=HTML&aged=0&language=EN&guiLanguage=en
[2] New York Times story on China's cyberwarfare preparation: www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?ex=1184817600&en=18f2e485db106 6ce&ei=5070
[3] Mi2g story on China's cyberwarfare preparation: www.intentblog.com/archives/2007/05/cyber_warfare_b.html
[4] US Defense Department report o wer-final.pdf#n Chinese military capabilities: www.defenselink.mil/pubs/pdfs/070523-China-Military-Po

REFERENCES

[1] Dineshkumar.P Master of Computer Application
9952270297,9994210297
dineshtvmalai297@yahoo.in