Areview on Distributeddenialofserviceattack

Abstract

Today's world, technology has become an inevitable part of human life. In fact, during the Covid-19 pandemic, everything from the corporate world to educational institutions has shifted from offline to online. It leads to exponential increase in intrusions and attacks over the internet-based technologies. Distributed denial of service (DDOS) attack is one of the most dangerous attack that could cause devastating effects on the internet. These attacks are becoming more complex and expected to expand in number day after day, rendering detecting and combating these threats challenging. In network security this attack is very dangerous. The main aim of DDOS attack is to collapse the network or server with abnormal traffic to make server unavailable for the legitimate users. In this paper reviews various type of DDOS attacks, Symptoms of DDOS attack, role of botnet on DDOS attack and give some mitigation and prevention technique for DDOS attack

Keywords

DDOSattack, dangerous attack, abnormal traffic,Botnet

1. Introduction

Today volume of users are increasing in Internet world. Internet applications are alsoincreasingdaybyday.ComputernetworksaresubjecttoanunprecedentednumberandvarietyofattacklikethemajorityofwhichareDDOSattack.DDOSattacksareeverydayoccurrence in small company or huge multinational company. Online services, websites, everythingthat faces internet. It can be slowed or completely stopped by a DDOS attack. DDOS attackdistracted cyber security operations and other criminal activity. The first half of the year2021foundmassiveransomwareandransomDDOSattackthatinterruptedcriticalinfrastructure around the world and it also targeted schools, public sectors, travel organizationand many biggest fields in the world. Second half of the year recorded one of the mostpowerful botnets**Meris**and record breaking HTTP DDOS attacks and Network Layer attacksobservedoverthecloudflare[1]. Figure-1 neatly explain network traffic during ransome DDOS attack.

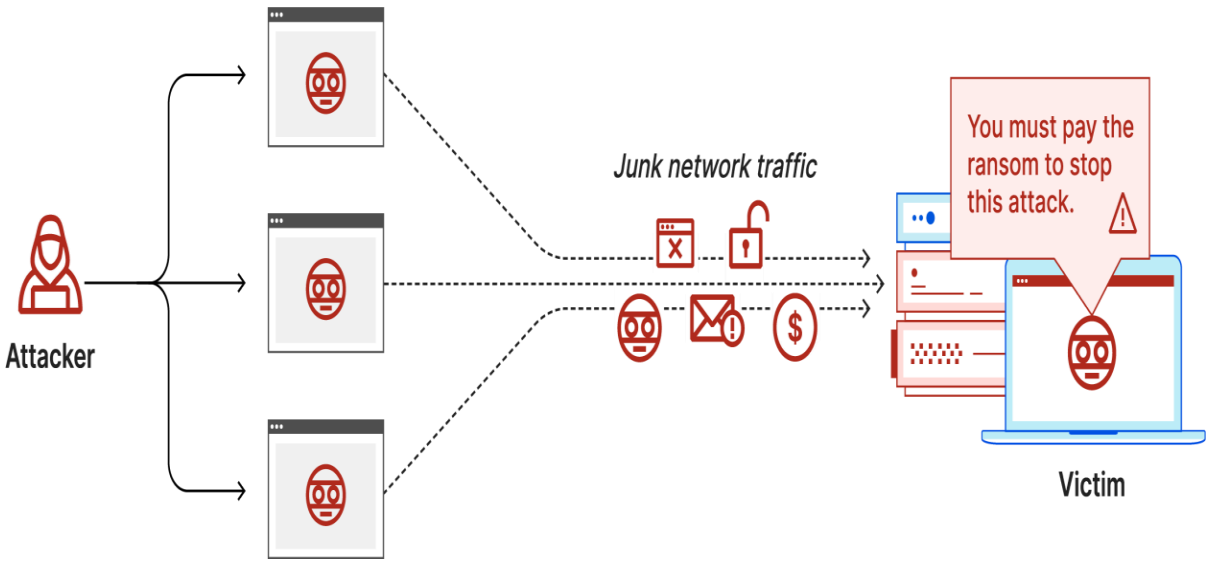

Figure1:RansomDDOSattack

In Q4 ransom DDOS attack increased by 29% YoY and 175% QoQ In this attackHackers are always finding new ideas to attacking servers that ideas are more effective andmostpowerful.

Recently some attacks are targeting the financial sector. An attacker encrypts data anddemands money such as Bitcoin for the return of data, or system access and so on. It is calledransom DDOS attack. This attack reached a rate of 2.5 million requests per second. Figure-2illustratethattheDDOSattackhas doublefrom2018to2023 and annual report of DDOS attack.

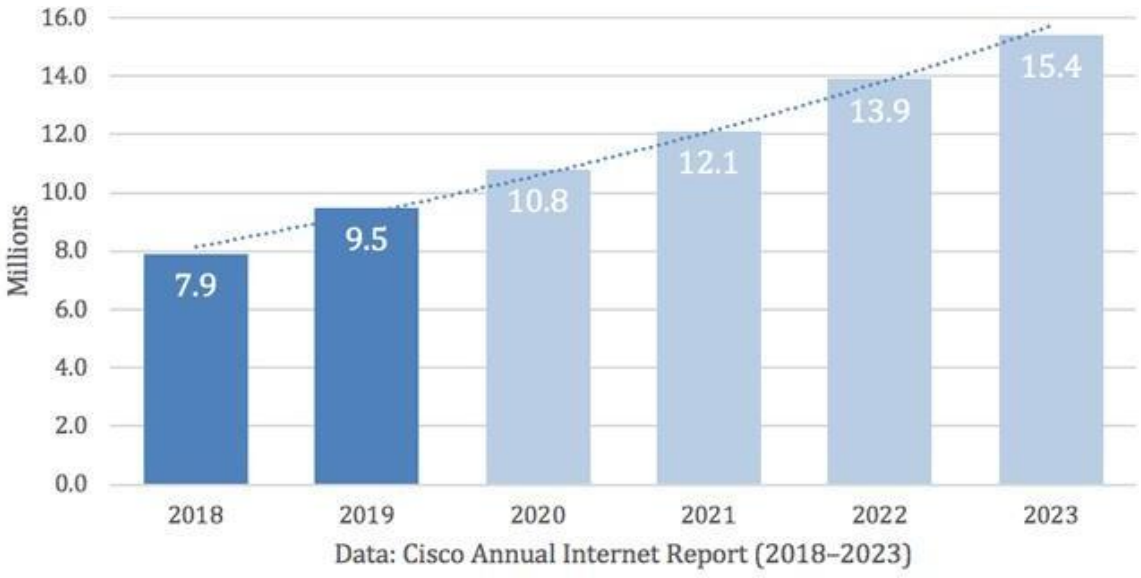

Figure2:DDOS attackAnnualreport

This paper organised as follows Introduction of DDOS attack present in Section 1.Section 2 Presents Literature survey.Explanation of botnet in DDOS attack in Section 3.Illustrate DDOS attack and its Types in Section 4. Some common methods for mitigation andpreventionare Section5.Finally,thispaperisconcludedisSection6.

2. LiteratureSurvey

ZsoltBederna. TamasSzadeczky [3] analyse what is the bot and botnet and role ofbotnet inDDOS attackand it said detailabouttheapplicationofbotnet andexplaindetailedinlifecycle of botnet. Here also author discuss important malware VPN filter and also detaildescriptionaboutheAPT28group.

In [4] explained detail about the DDOS attack and its types and also reviewed How toDDOS attack espionage cloud environment and how to mitigating and prevent the DDOSattack in cloud environment. In this paper author proposed solution for **multistage zonalclassification architecture** identifying, mitigating and prevent the slow rate HTTP DDOSattack.

PriyankaVermaet.al [5]in thisproposal focuson reducingVMlevel collateraldamages and to obtain the request awareness a novel cuckoo search based Identification ofrequest method. CS_IDR method helps request aware decision, which eventually reduces VMlevelcollateraldamages.

Aqeelsahi et.al [6]analysein this paperproposed new classification system fordetecting and preventing DDOS TCP flood attacks. Proposed CD_DDOS SYSTEM offers asolution classifying incoming packet and making decision based classification result. In thissystemhavingtwophasesdetectionphaseCS_DDOSidentifiespacketarenormalororiginatefro mtheattacker.Thennext preventionphaseinthisphasepacketclassifiedasmalicious,thatIPaddress willbeblacklisted.

Balasubramaniam.s et.al [12] in this proposal clearly explain DDOS attack explanation and its types and also it said identification of ddos attack and issues of ddos attack and ddos attack challenges.

PriyankaVerma,P. et.al [4] in this paper focus on reducing VM level collateral damages caused to the co hostedVms residing with the victim VM on the same host. In this paper also consist of request awareness based module and novel cuckoo search based identification of request.

3. Botnet

Botnets have one of the most common methods of malware deployment for the pastdecade. Hackers may use botnets to send spam messages, phishing or other trick for earningmoney.Theycanalsocollectedtheinformationfrominfectedmachine.

Bot which is a short form of robot.Attacker take a one computer in infected computersystem,makingitasDDOSmaster.Acomputerornetworkdeviceunderthecontrolofintrud erit is called as **Zombie.** It's another name is **bot.** The attack creates **Command and ControlServer(C&C). Telnet** botnets use simple command and control botnet. Collection of botscalled**Botnet.**Thepersoncontrolallbotiscalled**botmaster.**Botnet composed manynumberof bots. Botnets increasingly common tens or hundreds of thousands of its needs. There is noupperlimits ofbots[3].

Lifecycleofabotnet

Abotnetcanbemaintainedinfivephasesincluding:

- **Initial infection:** The botmaster scan target machine for known vulnerability andstartstoinfectusingdifferentexploitationmethods.
  Secondary injection: After successful infection the infected node executed script.That scriptiscalledshellcode.Shellcodefetchestheimage fromactualbotbinaryfrom specific location FTP, HTTP. The bot binary install itself. Once the botprogram is installed that machine is called Zombie machine that runs maliciouscode.
- **Connection:**Eachbotmachineconnectstothecommand andcontrolServer.

- **MaliciousCommandandControl:** AftertheconnectionphasethebotnetCommandControlphasearestarted.ThebotmasterusesaC&Cchannelstospread Commandtohisbotsarmy.Thebotprogramsarereceivedandexecutecommands sendbybotmaster.
- **Update and Maintenance:** Last phase is update and maintenance. In this phasebotsarecommandedtodownloadedandupdatebinary.Figure3clearlyexplaintheachitectureofbotnet.[3]

BotnetArchitecture

The botnet architecture is based on Client Server approach. It involves a C&C serverthatiscentralisedcontroloverthe bot.Botnetarchitecturehaveathreetypes,thatare

Centralised(orHierarchical): Thistypeofbotnetcontrolabotsinstaticnature.Herenature meanspredefinednumberofC&Cserverwithpredefinedreachability.Herebotsgetan information using push and pull technologGy. Pull technology means bot initiaterequesttoserver.Pushtechnologymeansserverstartupdate request toclient.

Decentralised (or Peer to Peer): Here no specific C&C servers. So such a botnetworking Peer to peer mode. In this method each bots register the number of bots availableinthissurroundingandcontinuouslyobserve anynew botsaredetected.

Hybrid botnet: Hybrid bot unify the advantages of centralised and decentralisedbotnets. The mixed architecture means C&C servers have a structure of decentralisednetworks and bots are connected to C&C server way of typical client server model. Thebotnetarchitecture and four types of botnet architectureexplaininFigure3.

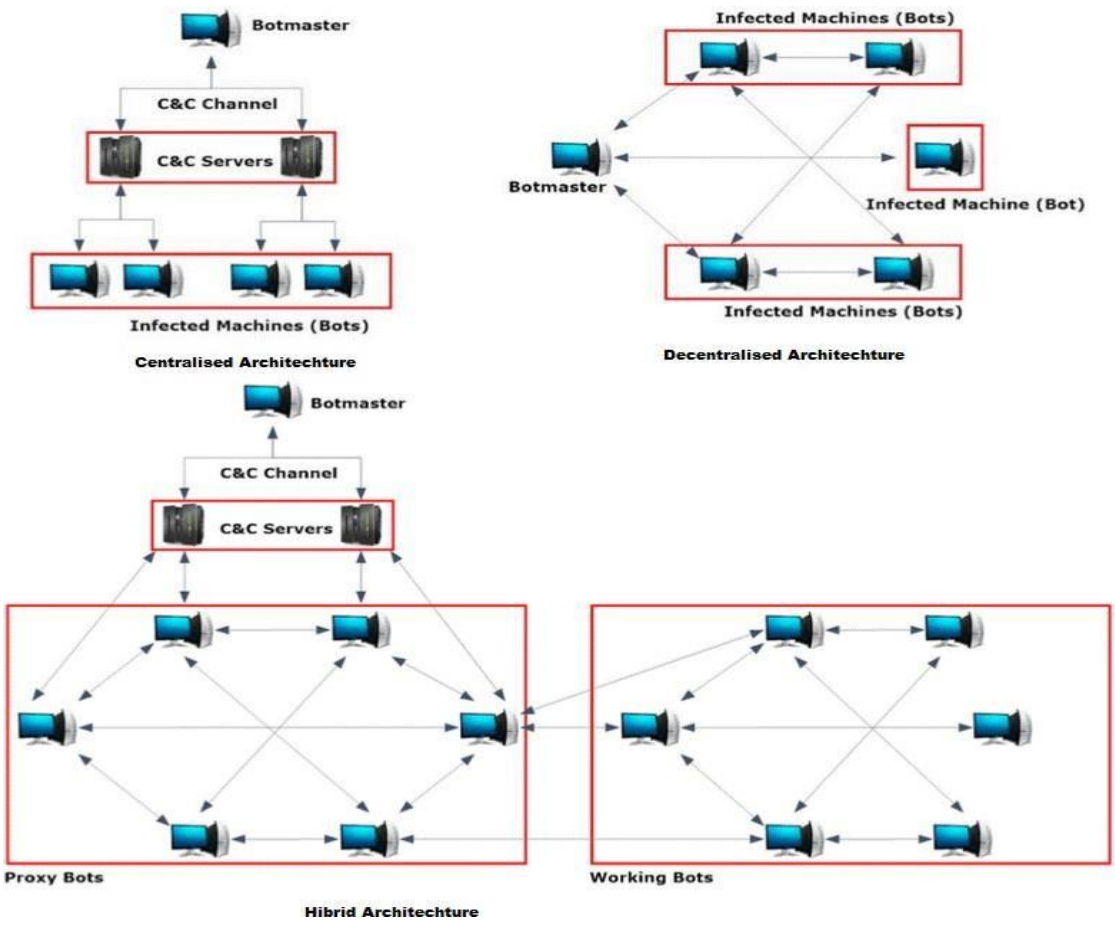

Figure3:Botnet Architecture

ApplicationofBotnet

Crimeware as a Service: It is used for identification of vulnerabilities and to createan exploit specifically for them. Main tools are available for this service that's are APT(AdvancedPersistenceThreads),rootkitsandrandsowareaswellasdropers,keyloggers,andhidingtools.

CybercrimeinfrastructureasaService: Itmakesinfrastructureelements(clientsandServeravailable).Clientsusedtovariousattacks.

Hacking as a Service: This service is a service **model** for whole attacking process.The"ServiceProvider"performsattacksasclientsanddemandtospecificserviceorprocessinformation.

4. DDOSattack

An attack originates from single source that is called DOS Attack. However commontoday **DDOS attack**s are originate from multiple source. Attacker creating a fake maliciousttraffic and send it to target Server website or other resource. Its main aim is force a targetedsystemto slow downorcrash.Difference of attacker traffic and normal trafficis clearly explaininFigure-4.

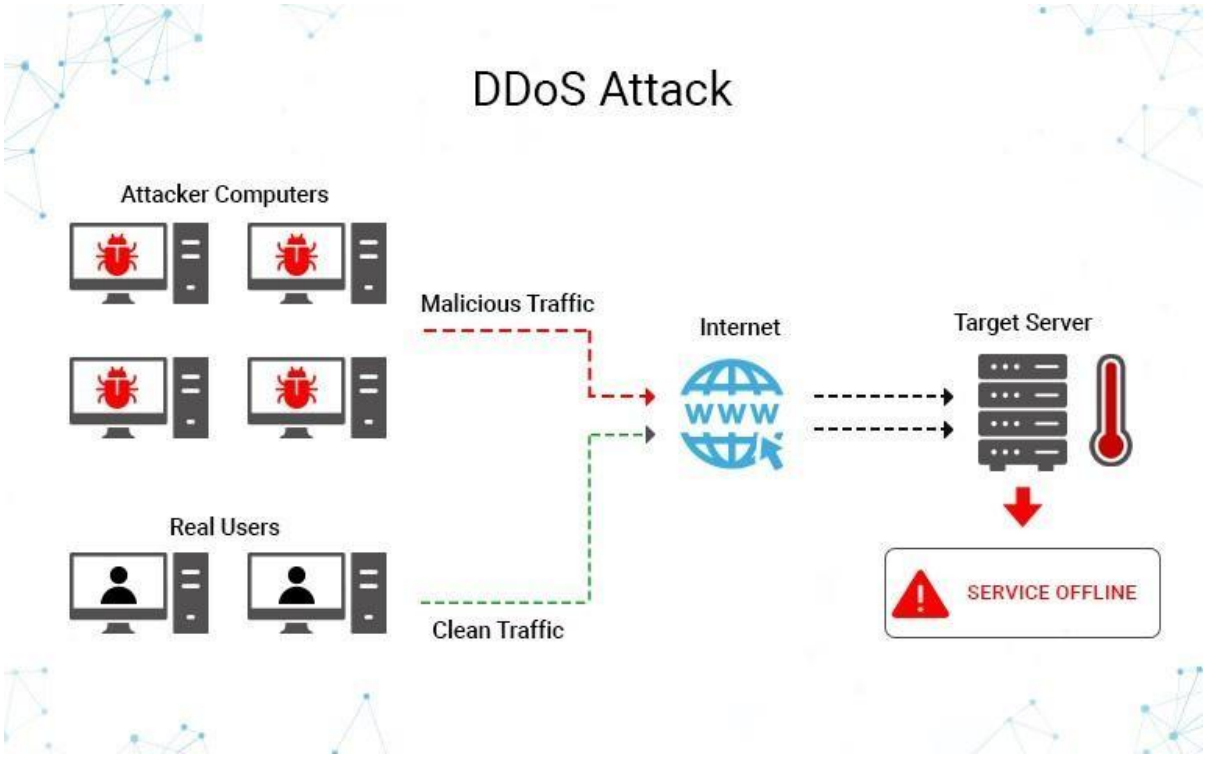

Figure4: DDOS attack

I. TypesofDDOSattacks

DDOS attacks come in a variety of flavours. Broadly speaking, they are classifiedbased on the type and quantity of traffic used for the attack and the exploited vulnerability ofthetarget.DDOSattackclassifiedintothreecategories:

- VolumebasedDDOS attack
- Protocolbasedattack
- ApplicationLayerbased attack

I. Volumebased DDOSattack

Volumetric DDOS attacks are sends high volume of traffic, request packets to target serverdevice this attack creating flood and slowdown or stopping their services. Different types ofvolumebasedattackseeinnext.

DifferentTypesofVolumetricattack

a. UDPflood

UDP flood is a type of DDOS attack it send large number of user datagram protocolpacketsto atargetedserver.It'smain aimoverwhelmingthedeviceabilityandrespond.

UDP is a networking protocol that is connectionless and session less protocol. UDPtrafficdoesnothaveathreewayhandshaking.Itrequirelessoverheadsoitisperfectlysuitablefor creating flood. UDP flood attacks take the form of DNS amplification attacks, also called**Alphabet soup attack. UDP** attack does not have a specified packet format. Attackers createlarge packets (sometime over 8KB), fill with textor numbers.In UDPflood attack thefollowingprocess occurs:

1. AnattackersendsUDP packetswithspoofedIPaddress.
2. Systemsidefollowingprocedurerepeatedforincomingpacket.
   a. CheckthereportspecifiedinUDPpacketforlisteningapplication;itisarandomlyselect edportsoitisgenerallynotincase.
   b. Send an ICMP destination unreachable packet to sender since IP address hasbeen spoofed these packets are usually received by some random bystander.Figure-5diffenciate legitimate traffic and attacker traffic inUDPfloodDDOSattack .

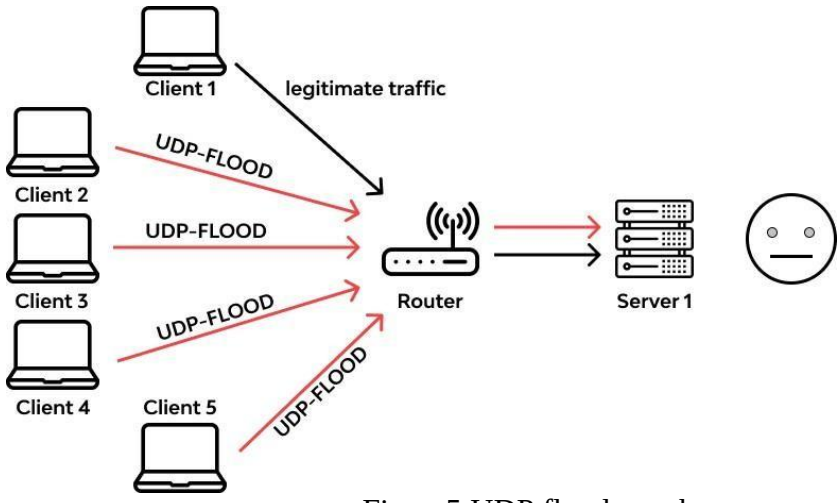

Figure5:UDP flood attack

b. ICMPflood

An ICMP flood DDOS attack is also called as ping flood attack. It sent large numberof ICMP echo request (pings) to target server using devices the victim machine start to replyusing ICMPechoreplypacket.Nowtargetedmachinetakestwicethebandwidthwasonceforreceivingthep acketsanotheroneisrespondreplies.Sovictimmachinegetfloodednetwork

traffic. SoCPUwantslarge numberofCPUcyclesmanybegoingtoshutdown.

SignsofICMPflood DDOSattack

In ICMP flood attack attacker know IP address of the target Machine. Attacks can beseparatedintothreecategoriesthatare givenbelow:

I. **Target local disclosed**: In this type of DDOS attack ping flood target specificmachine on the local network. In this attack attacker must know the IP address ofthe destinationbeforehead.

II. **Router disclosed:** In this type of DDOS attack targets the routers. This mainobjectiveisinterruptingthecommunicationbetweenthecomputernetworks.Inthis typeofattackattackermustknowbeforethetargetedIPaddress.

III. **Blind ping:** This type of attack involves using external command to reveal the IPaddress of the target computer or router before launching the attack. Figure-6 explains ICMP echo request and ICMP echo response in ICMP flood ddos attack.

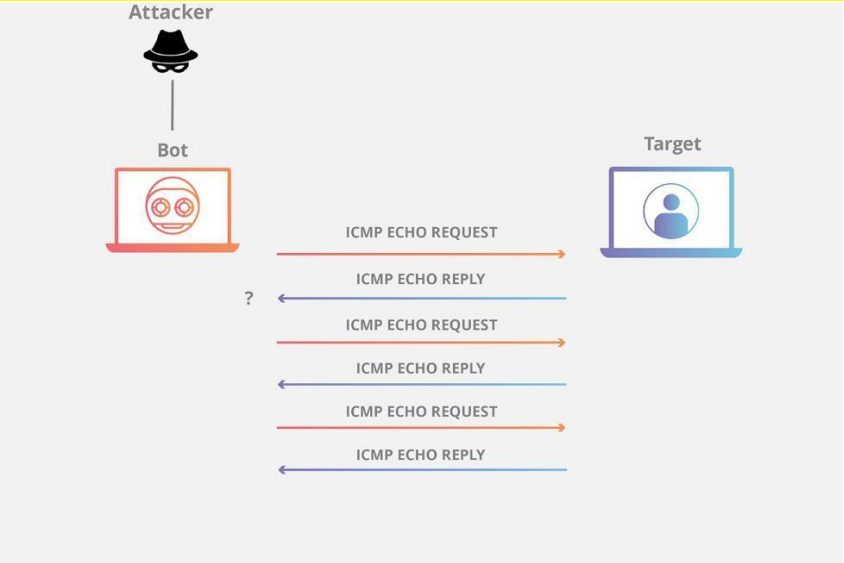

Figure6: ICMP flood

c. Spoofedpacket

Spoofingisthatactofcamouflageacommunicationfromaunknownsourcebeingfroma trusted source. Spoofing can apply phone calls and websites and emails and can be moretechnicalthatareDNSserverspoofing,ARPspoofing,IPaddressSpoofing

DNSserverspoofing: ModifiesDNSserverandredirectadomainnametodifferentIPaddress. Itisalsousedfor spreadviruses. Figure-7explain different between real website and DNS server spoofing fake website.

ARPspoofing: ItwillbelinkaperpetratorsMACaddresstolegitimateIPaddressthroughspoofedARP message.Itwillbemainlyusedformaninthemiddleanddenialofserviceattack.

IPaddressspoofing: Disguisesanattacker'soriginalIP address.

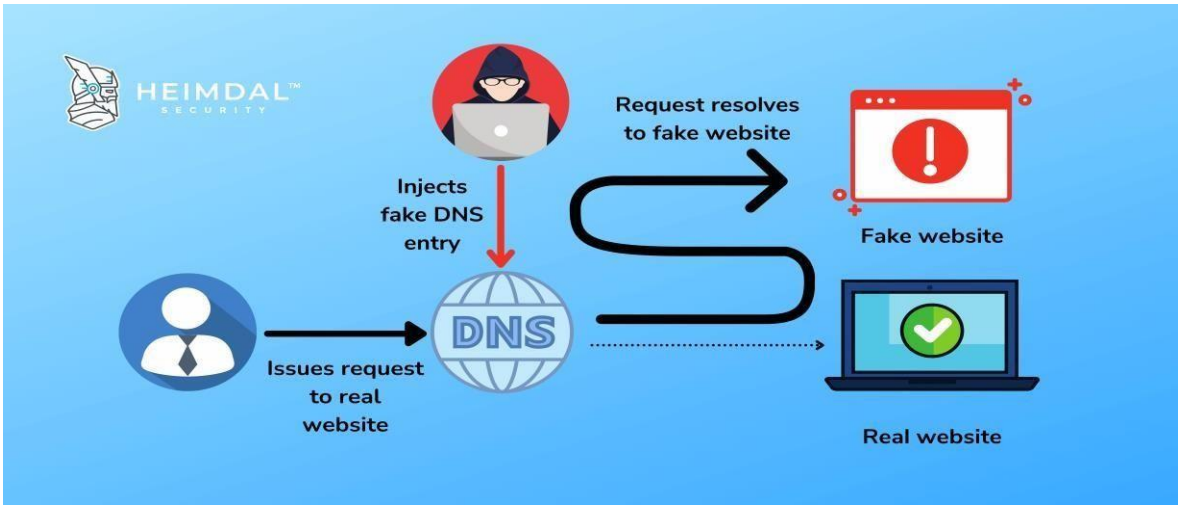

Figure7:DNSSpoofing

d. ReflectionamplificationDDOSattack

Reflectorisaserver.ItwasreachablefromInternet.Itwillofferservicetoclient(DNS,NTP, SNMP, gaming) attackers launch a DDOS flooding attack it sends a legitimate requesttoserverthenetworktrafficcontainspoofedsourceIPAddressofvictim.

IP spoofing performed two reasons. First it hides identity of attacker sound queryresponse send from reflector to victim. Significantly larger than original query request. ForexampleDDOSamplificationattackcontainsmanyIPaddress.Itmakesresponseasymmetricalt erms ofconsumedbandwidth.

With the botnet command and control server instruct thousands and thousands of botsto send request number of reflect in parallel. It will increase attack traffic and to increasingvolumeofattack.Figure-8 explaintheReflection attack and reflector(intermediaries) of AmplificationAttack.

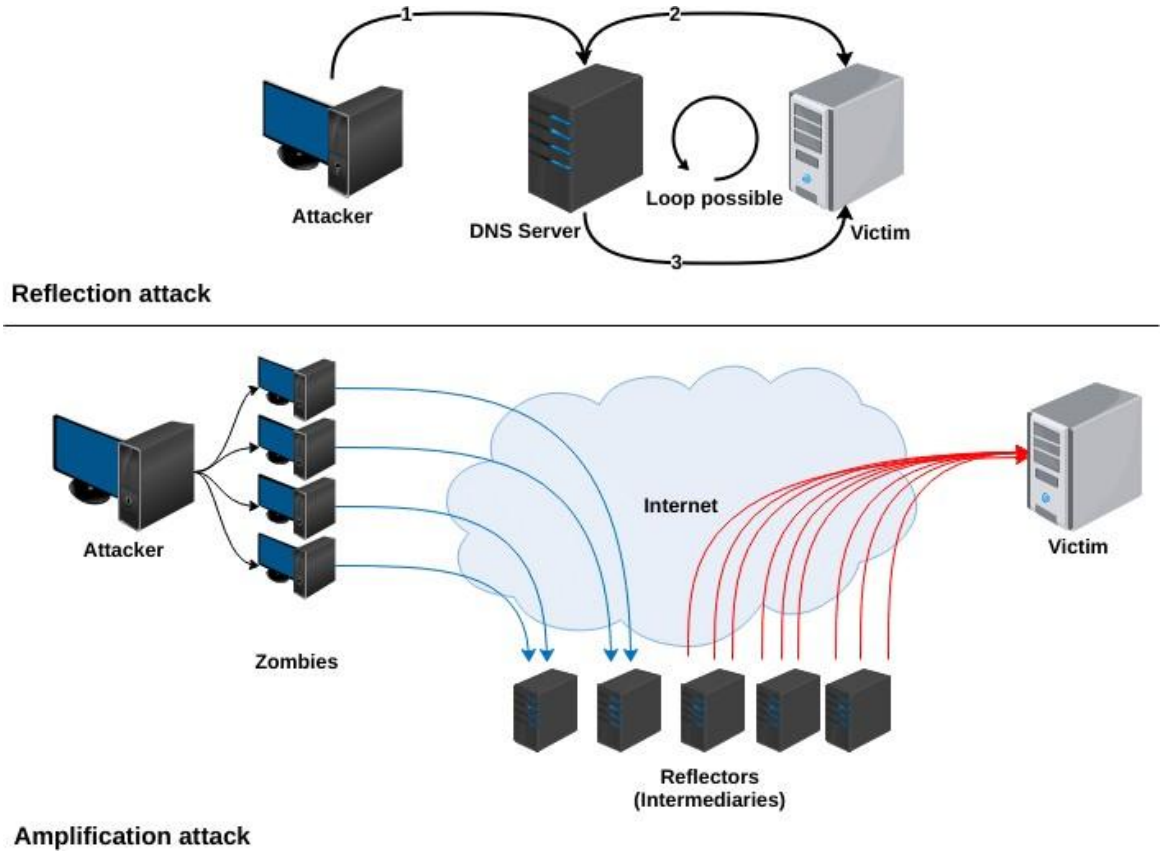

Figure8:ReflectionandAmplificationAttack

e. IP/ICMPfragmentation

IP fragmentation IP datagrams are fragmented into small packets, then that will betransmitted throw the network and finally it will be re assembled into original datagram innormalcommunication.

This process have a size limits for each network can handle. That limit is described asmaximum transmission unit (MTU).When a packet is too large that will be sliced into smallpackets and transmitted successfully. One which contain all information about ports, length,etc.Thisis theinitialfragmentation.

AttackersendsIP/ICMPbasedfragmentationattackstypicallysubmittedfakefragmented. It takes more memory resource. So server become completely overwhelmed andultimately.Figure-9differentiate normal fragment packets and fake fragment packets.

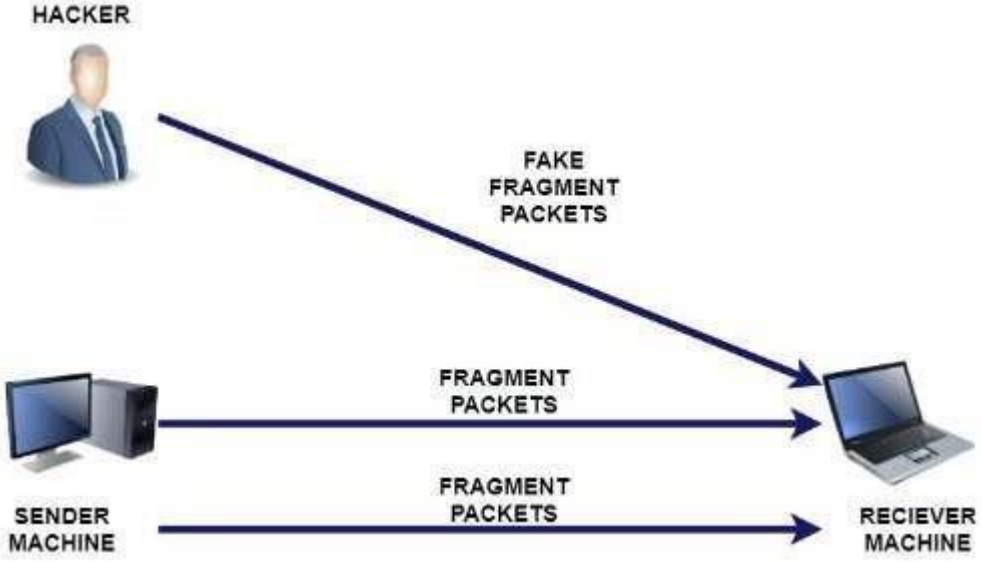

Figure9:ICMP fragmentation

II. Protocolbasedattack

Protocol attack also known as state execution attacks. It cause a service disruption byoverconsumingserverresourcesandnetworkequipmentlikefirewallsandloadbalance.Itwillbe utilize weakness load balancers layer3 and layer 4 protocol stack torender targetinaccessible.Ithasmanytypeofattacksthatarebriefedinthefollowingsections.

a. SYNfloodattack

SYN flood attack also called as TCP flood attack it's another one name is half openattack. This type of attack sending large number of SYN packets to the targeted server fromspoofedIPaddress.Theserverrespondingtoeachoneofconnectionrequest andleavesaopenportforreceivingtheresponse.

The server waits for final acknowledgement packet but it will not arrives. Instead theattacker sending new SYN packet. Because of this reason the server temporarily maintainnetwork port connection for certain time. All the ports are used the server does not functionnormally.Thenetworkingwhenaserverconnectionisopenbutanothersideisnot.Itiscalledh alf open connection. In this type of DDO`S attack targeted server is continuously leaving foropen connection and waiting for each connection time out before port become again availablethis typeofattackconsideras halfopenattack.Thisprocessillustrates inFigure-10. ThisSYNfloodattackcanattacktwodifferentwaysthatare

Direct attack: This type of SYN flood attack the IP address is not spoofed it is knownasdirectattack.Thetypeofattackattackerdoesnotmask theirIPaddressforalltime.

Spoofed attack: In this attack is created using botnet. It is spoofed IP address fromwhichitsends.Forexamples**MiraiandMeris botnet.**

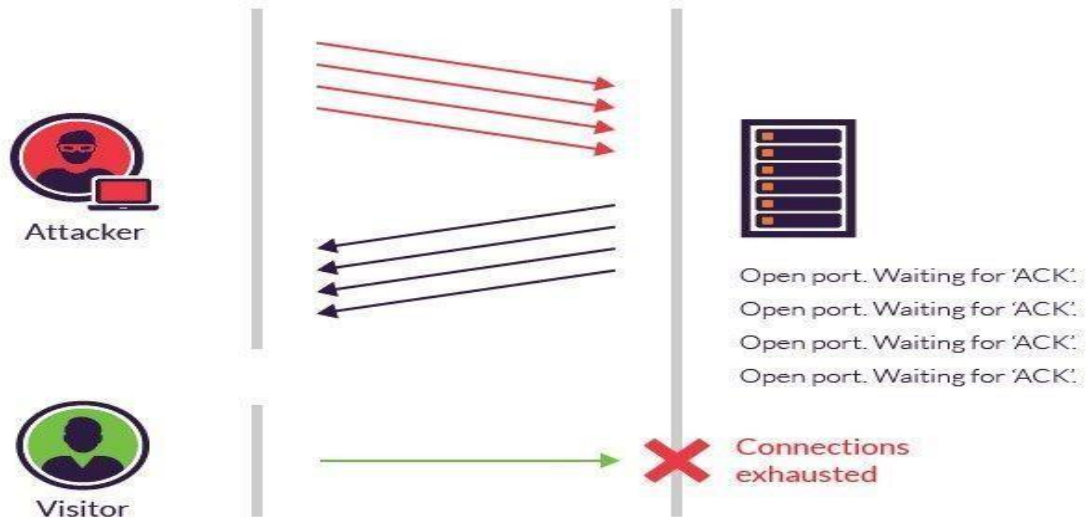

Figure10: SYNfloodattack

b. Pingofdeath

Attackersendsmalformedoroversizedpacketsusingsimplepingcommand.Thistypeofattackattackerattemptstocrashorfreezethetargetedcomputerorserver.

PingofdeathissenddeliberatelyIPpacketslarger than65,536bytestotargetedserver.The ping of death attack also called teardrop attack this ping of death attack objectified ICMPandTCPanditisunderminingofallICMPattack.

It can also doing against different protocols like UDP. That is from 0 to 65,500 bytesof data in ICMP echo request packet. If we try to send data size above 64,500 that time pingcommandwillshowanerrormessage.

IPV4 header is 16 bit field. The maximum possible value of 16 bit binary number is65,535 sending an ICMP echo request packet larger than 65,535 bytes size in IPV4 datagrampingcommand memoryoverflowcanhappen.Alsopossibletotargetmachinefreezeorcraze.Pingofdeath working mechanism explaindetailedinFigure-11.

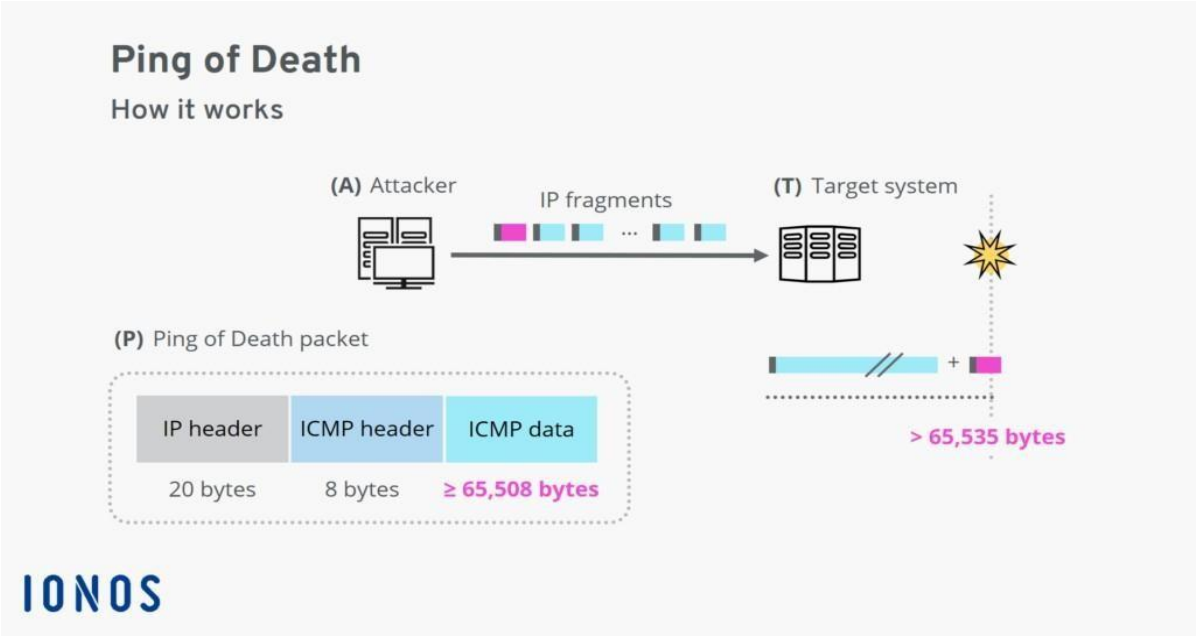

Figure11:Pingofdeathattack

c. SmurfDDOSattack

SmurfattackaresimilaraspingfloodattackasbotharecarriedbysendingICMPechorequestpacketsSmurfmalwareisusedtofakemalware,usingspoofedsourceIPwhichistargetserveraddress.

InSmurfattacksendingspoofedpacket thatattachedtoafalse IPaddressthatiscalledas**spoofing**thatpacketscontainasICMP pingmessage,whichcommandnetworknodesendsreply.ThisprocessknownasICMPechocreates**infiniteloop.**Thatoverwhelmsnetworkwithconstantrequests.Figure-12 explain attackers Smurf attack working principles.

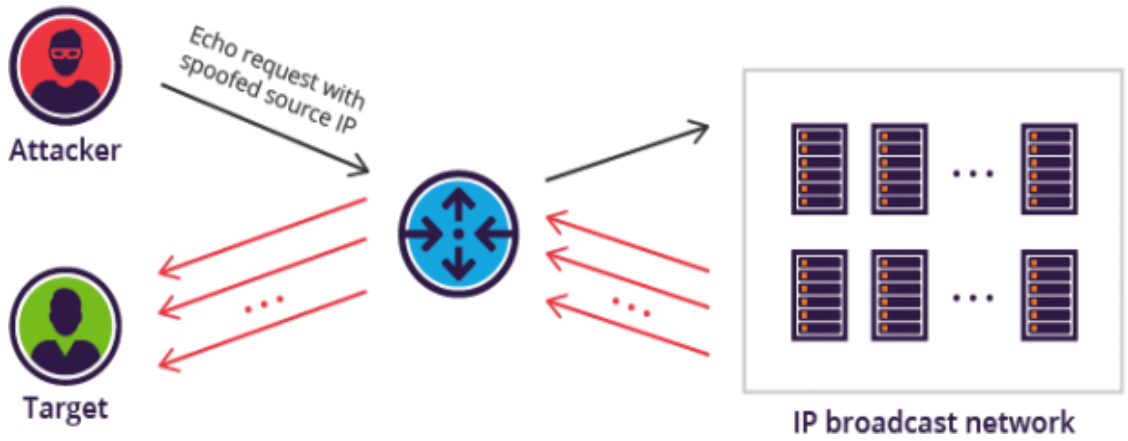

Figure12:Smurfattack

III. Applicationlayerattack

Application layerattacks calledlayer7 attack. Manufacturingindustry wasmostaffected in Q421. It increasing 64% QoQ in the number of attacks. Business Services andgambling industries are second and third most affected industries. For the fourth time in thisyearChinachartswithheightspercentageofattacksarecomingfromApplicationLayerattack.In the middle 2021 a new bot is recorded that name is called **Meris**bot net. Meris botnetattackinga serverfor**17.5Millionrequestper second**[1]**.**

Initiallythisresearchwas estimatedonly30000to56000botsbuttheestimatedactualyto much higher 2, 20,000 bots are founded. In five year ago Mirai bot net was detected. It wasinfectedhundredsofthousandsofIOTdevicesbutMeriswasmostpowerfulthanMirai.LaterMiraicodewasLeaked andfoundanotherversionofMiraithatnameis**Mobot**[1]**.**

a. Slowloris

Slowloris open multiple connections to the target web server and open as long aspossible.ItdoessendingpartialHTTPrequestmoreofwhichcompleted.Theserveropenmoreand more connections open. Slowloris send subsequent HTTP headers for each request butnevercompletestherequestthetargetedservermaximumconcurrentconnectionisfilledtothelegitimateconnectionattemptaredenied.TheFigure-13 Explain Slowlorisattack and difference between normal http request_response connection and attack time request response connection.

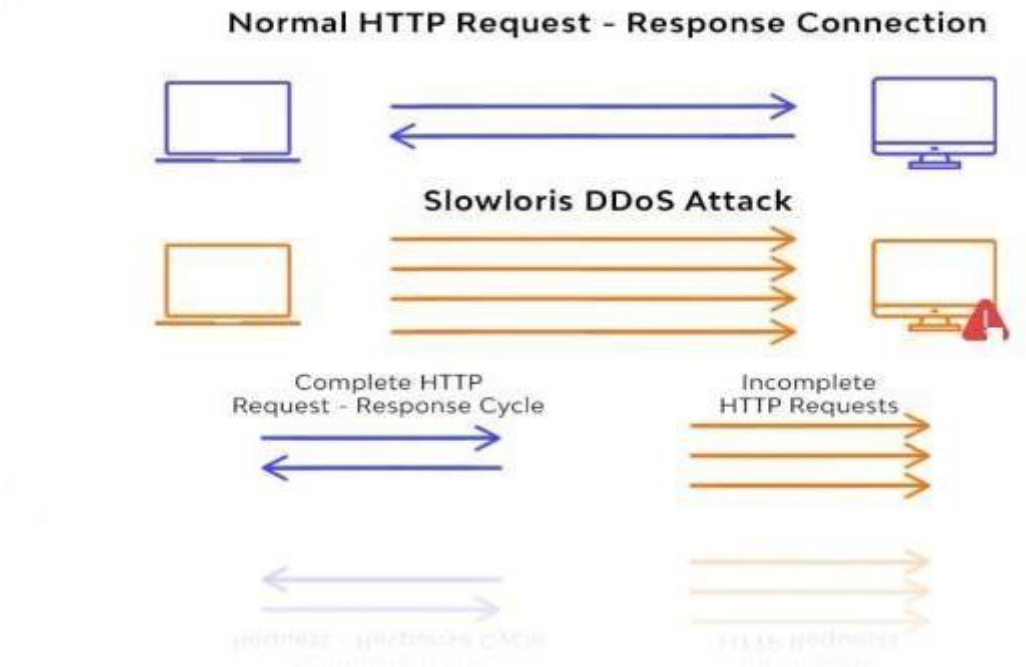

Figure13:Slowlorisattack

b. Zero dayattack

When a user visits in a website can exploits security vulnerability in the web browserto infect system. Cyber criminals use social engineering for infect system. For example theymay send phishing email with an attachment on clicking mail that time malicious code wasexecuted and download malware in thatand then infect it. The Figure-14 gives an idea ofzerodayattack.

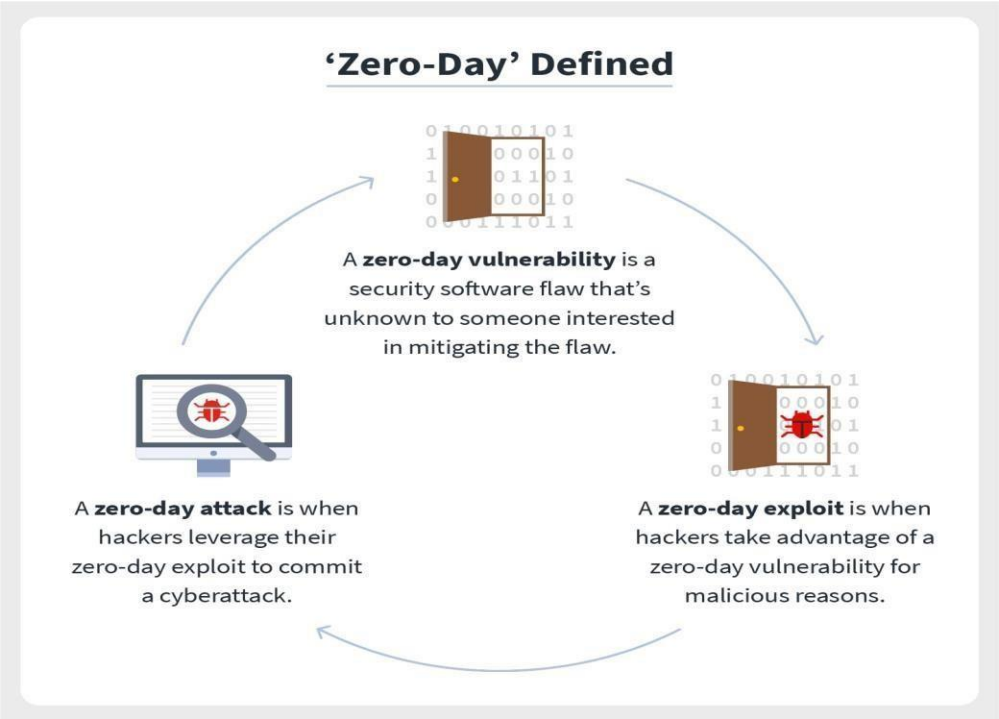

Figure 14:Zerodayattack

5. Best methodsforpreventDDOSattack

- Ensure high levelsofNetworkSecurity
- HaveServerRedundancy
- Lookupforthewarning signs
- ContinuousMonitoringofnetworktraffic
- LimitNetworkBroadcasting
- LeveragethecloudtopreventDDOSAttacks.
- DonotOverlooktheDDOSthread

6. EffectivetipsforDDOSprotection,Mitigation,and Defence

- MitigateDDOSattackswithMultilayered,MultimoduleDefence
- EarlydetectionandTrafficMonitoringareCritical
- BuildaResilientInfrastructure
- GetRealTimeIntelligence andAct onThem
- Knowthe attacksymptoms
- GoodCyberHygieneisIndispensable
- CreateaDDOS ResponsePlan
- WatchoutforSecondaryAttack

7. Conclusion

RussiaandUkraineaggression waron going.In this timegeopolitical tensionsincreased when the Ukraine defence ministry, the armed forces of Ukraine, some state backedbanks MiroHost (a hosting provider) were hit by DDOS attacks. This attack will be lasted byone hour or two. According to Threatpost report no data was stolen or damaged but websiteswere disabling and banking applications could not be used in few hours. On mid-January 70Ukrainiangovernmentwerehacked.[1]

Detection, prevention and mitigation of DDOS attack is most important for NationalSecurity.Theinternetisanimportantcomponentofcommunicationinfrastructure.Inthesa memanner internet has become most user friendly over the last decade and more individual,businesses, and government agencies make use of it, hacking and disrupting network traffic.Attacking tools have become more sophisticated. And also very easiest to use.But one of themost important issues that will impact how defence against DDOS attacks. In this surveyclearly explained what is DDOS attack? And type of DDOS attack and also give detailedexplanationofmitigationandprevention techniques ofDDOSattack. Software Defined Network, Cloud computing, Internet of things Devices, Wireless SensorNetworks, and Mobile Ad hoc Network these environments are largely affected for DDOSattack.Manytechniquesusedforpreventingandmitigatingtheseattacksthat'sareBlackholef ilteringmethods,Intrusiondetectionmethod,using some algorithms.In future work prevent DDOS attack using above some techniques.

8. References

1. Cloudflare statistic reporthttps://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
2. Bederna.Z,Szadeczky.T.CyberespionagethroughBotnets.SecurJ33,43–62(2020).https://doi.org/10.1057/s41284-019-00194-6.
3. A.Dhandapal and P. Nithyanandham. The slow HTTP DDOS ATTACKS: Detection,mitigationandpreventionintheCloudEnvironmentScalablecomputing:Practice andexperienceVolume20,Number4,pp.669-785.
4. PriyankaVerma,P.,Tapaswi,S.&Godfrey, W.W.Arequest-awaremoduleusingCS-IDRtoreduceVMlevelcollateraldamagescausedbyDDoSattacksincloudenvironments.ClusterComput24,1917–1933(2021).doc:https://doi.org/10.1007/s10586-021-03234-2
5. K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, SYN Flood Attack DetectionbasedonBayesEstimator(SFADBE)ForMANET.(2019)InternationalConferenceonComputerandInformationSciences(ICCIS),2019,pp.1-4,doi:10.1109/ICCISci.2019.8716416.
6. A.Sahi,D. Lai,Y. LiandM.Diykh. AnEfficient DDoSTCPFloodAttackDetectionand Prevention System in a Cloud Environment, in IEEE Access, vol. 5, pp. 6036-6048,2017,doi:10.1109/ACCESS.2017.2688460.
7. SubhiR.M.Zeebaree,KarwanJacksi,RizgarR.Zebari.ImpactanalysisofSYNfloodDDOS attack on HAProxy and NLB cluster based web server,Indonesian Journal ofElectrical EngineeringandComputerScienceVol.19,No.1,July2020,pp,510-517ISSN:2502-4752 doi:10.11591/ijeecs.v19.il.pp510-517
8. Shivansh Kumar Ruhul Amin. Mitigating Distributed denial of service attack: Blockchain and software defined networking based approach, network model with futureresearchchallenges WileyPublication.doi:10.1002/spy2.163
9. TasnuvaMahjabin, Yang Xiao, Guang Sun “A survey of distributed denial of serviceattack,preventionandmitigatingtechniques”International Journal of DistributedSensorNetwork. http://doi.org/10.1177/1550147717741463
10. BadrAlshery and William Allen “Proactive Approach for the Prevention of DDOSattacksinCloudComputingEnvironments. SpringerInternationalpublishingAG2017R.Lee(ed.),AppliedComputingandInformationalTechnology,doi:10.1007/978-3-319-51472-7_9
11. MitkoBogdanoski,TomislavSuminoski, AleksandarRisteski. Analysis of the SYNFloodDosAttack.InternationalJournalofComputerNetworkandInformationSecurity(IJCNIS)5(8),1-11,2013,doi:http://doi.org/10.5815/ijcnis.2013.08.01
12. Balasubramaniam, S., Vijesh Joe, C., Sivakumar, T. A., Prasanth, A., Satheesh Kumar, K., Kavitha, V., & Dhanaraj, R. K. (2023). Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing. International Journal of Intelligent Systems, 2023.
13. Balasubramaniam, S., & Kavitha, V. (2015). Hybrid Security Architecture for Personal Health Record Transactions in Cloud Computing. Advances in Information Sciences and Service Sciences, 7(1), 121.
14. Balasubramaniam, S., & Kavitha, V. (2014). A survey on data encryption tecniques in cloud computing. Asian Journal of Information Technology, 13(9), 494-505.