A SURVEY ON MIRAI – THE MOST VULNERABLE TO THE IOT DEVICES

N.Krithika
PG Student
Sri Ramakrishna Engineeering College Coimbatore, India
krithika.natarajan93@gmail.com

Abstract—With rapidgrowthoftechnologysecuringthe informationisnecessary. Thisresearchisbeingcarriedout in context of threat named MIRAI. Presently an IOT deviceplays amajorpartin manyareas and therecomes a main problem.This paperbrieflydescribes how MIRAI works,basicsecuritypracticesandhowtoenhancethem byusingsomeofthemethodsto Avertttheseattackin future.

Keywords—BULLGUARDS IOTscanner,DDOS,MIRAI, Reimage.

I. INTRODUCTION

MIRAIisoneof themalwareorthreatthatturns the computer system running on Linux into remotely controlledbots.Itwasoriginatedin Japan. [9] TheworldcametoknowaboutMIRAIin Twitter,Netflix andAmazon.Themainfunction of MIRAIis tolaunchhttpfloods andvariousnetwork layerDDOSattacks.

Itmainlytargetson onlineconsumerdevices namely remotecamerasandhomerouters.This threatisusedinspreadingdistributeddenial of serviceattack.[10] Thedevicesthatareinfectedby MIRAIregularlyscanforthe IPaddressesranges ofinternetand Searchforthe uninfectedprivate networksandmakethemvulnerable.MIRAIfinds theweaknessofIOTdevicesusingtable,ofmore than60commonfactory defaultusernameand passwordsandlogintothem withMIRAImalware. Theinfecteddevicesneedtobe rebootedsoturnthe devicesoffforashortwhileandturniton once again.[9]NowChangetheloginpasswordorelse thedevice willbeinfectedagain withinminutes. NowMIRAIwillidentify opponentmalwareand remove them from memory and block administration ports.Therearehundredsof thousands of devices thatusesinternetof (IOT)defaultsettingsandmakethem vulnerable. Afterinfecting,thedevice will observeacommand andcontrolserver whichindicates targetofattack.

[2]Accordingtothe reportreleasedby Internetof Evilof thingsin2017morethan90 percent ofITpeoplessaythat connecteddeviceswillbethebiggestthreatin2017.Toun derstandthe risksfacedbyMIRAIsecurityteamcrossedvarious sectors suchas Retail,Hospitals,FinancialServices,Manufacturing,H ealth Care and Energy.Thousands ofWebcamsareattackedby MIRAIandthey does notknowthenecessarysolutiontorectifythem.

[4]Accordingtothe BlackHatAttendee surveyonJuly2015intheregionofNorthAmerica reportedthat 35percent ofsecurityprofessionals use theirtimeinlabelingthe vulnerabilities introducedby theirdevelopmentteam.33percent says that the vulnerabilities enter in the device wherewepurchaseonoff-shelf applications.30 percentofpeoplebelievesthatthemistakesareby internalandexternalby attackscausesthecompany to loss their regular requirement.[1] Many IT sectorsfacesthenewthreatinIOTdevicesnamed MIRAI.84percentof surveysaysthatMIRAI Malwaremadeheadlines globally.64percentof peopledonotknow how tochecktheirconnected devices,20percentofpeoplesay thattheirdevices smash with Ransomwareattacksand 16percent experiencedmaninthemiddleattacks.

[5]UnitedStatesandGermany conducteda survey tovariousresponders.Thissurvey tellsthat morenumbersattacks arehappenbecauseof carelessnessbytheemployeewithoutanyintention. 54percentofGermanagreedthatorganizationdoes nothave enoughsafety measurestoprotect.60 percent of US people reported that Senior Executives donottakenintoaccountaboutthedata securityasfirstpriority.

II. MIRAI MALWARE PACKAGE AND WORKINGPRINCIPLE

A. package

MIRAIarewrittenincandhas three componentsnamelyA callhomesystem,Setof attackroutines,NetworkScanner.

*a)*A call home system: It connects to commandandcontrol serverwhichisaninsecure IOTdevicefordownloadingthedetailsof whomto attack.

*b)*Asetofattackroutine:Itactlikeagenuine onebutits purposeis tostealthenetworkcapacity.

*c)*Anetworkscanner: It searchesacrossthe internetandlogintoknowthelistoftroubledIOT devicesfornewattacks.

B. workingmechanism

MIRAIattacksare tolaunchHTTPfloods andvariousnetworklayerattacks(OSI3,4). In networklayer,itiscapableoflaunchingGREIP andGREETHfloodsaswell as SYN,ACK, STDMP(simple textorientedmessage protocols), DNSFLOODSandUDPFLOODS.

To gain access MIRAI uses default passwordfor telnetandSSHaccount.Onceitsgain accessitinstallsmalwareon tothesystem.Now, MIRAIopen portsandbuildaconnection withbot masterstoanalysesifthereareanydeviceswhich are not infected by MIRAI. After finding the targeteddeviceswithnoinfectionitstartstoinject malwareintothem.Theworkingflowis depictedin fig1

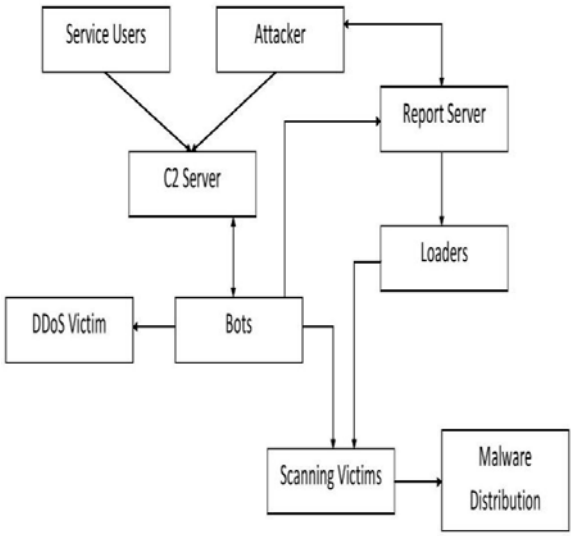

FIG1:WORKINGPRINCIPLEOFMIRAI

Servicesaresoldtothe customersforlaunching attacks via C2 API. Bots and C2server communicatefrequently stoknow IPaddress changedarenot.Hackers alwayshavealonglived connection withreportserver.If thereportserver found any victims it loaded into the loader. Damageddevicesareloggedonby theloaderto instructthem todownloadMIRAImalware.And thusvictim downloadedandinfectionsrunto becomebots.

III. HOW DOES MALWARE SPREAD AND WAYTOESCAPEFROMIT

IfwebuyIOTdevicesfirstlookforitsmanual andidentity themanufacturedcompany.After purchasingthedevicechangethedefaultpassword tostrongpasswordbasedontheuserneeds.

a)Modifythesecuritysettings(i.e.)turnoffthe telnetloginandemploySSH

b)Checkthe IOTdevicesforlatestupdates.

V. DETECTINGTHEMIRAI ACTIVITY

MIRAI lives in dynamic memory of a system that can be removed by rebooting. Even afterwe rebootthedevices therearealotofchances thattheinfectionwilloccuragain.

TodetectMIRAIactivityinnetworkcreate a dashboardinqualysassetview thatdisplays systems thatrunonthefollowingports

a)Forfindingdefaultusername/passwordin telnetuseQID38644

b) Monitor IP port 2323/TCP and port

23/TCPAttempttogainunauthorizedcontrolover IOT devices using network terminal (telnet protocol)

c)Lookforuncertaintrafficonport48101 infected devices this often attempt to spread infection by usingport48101forsendingresultsto threatactor.Blocktheportif theusercurrentlynot using.

TheMainmottoofMIRAIthreatistoscan for the IP addresses across the internet to find unsafedevicesandit'sprogrammedtoguesstheir loginauthorization.MIRAIscannerwillcheckthe gatewayfrom outsideofthenetwork toseeifthere areany remoteaccessportsthatarevulnerableto attackbyonlylooks intopublic IPaddress.

Ifthe scanner findsanydefenselessdevices it checksfor

a) Scan thenetworkagain toconfirm thatthe vulnerabilityhas beenresolved.

b)LogineachIOTdeviceson ournetworkand changethepasswordtobestrong.Impervais oneofthenewcompanieswhichofferafreescannerto detectIOTdevicesinfectedwithmalware.

V. WHATSHOULDWEDOTOPROTECTOUR INTERNETCONNECTEDDEVICES

Universalplugand play (upnp)isadefault application thatisalreadyinstalled on therouters. Upnpisamajorsecurityissuebecauseitiseasily allowsthetrustedlocalnetwork tobeforwarded withoutthesystem owner'sknowledge.Itdoesnot requireanyauthenticationfrom user.Itasksforthe routertoforwarda portoverupnp.Thusitisnot securedapplication.

To overcomemalwareenteringintoupnpapplication it is recommended that unless user needsanyapplicationthatrequiresaportforward. Upnp shouldbedisabledforsecurity.

VI. REMOVE MIRAI WITH SAFE MODE OF NETWORKING

[7]If wefindanyillegalactioninthedevice installasecurity applicationsuchasReimageor Malware Bytes antimalware that will help to removeMIRAI.Bull guardsIOTscannerchecksif any IOTdevicesarevulnerable.ToremoveMIRAI usingsafemodefirststepis torebootoursystem.

A. *[7] Systemrestores toremove MIRAI*

In windows 7, click the start button and pressshutdown waitforawhilethen restartthe system. When our pc is active start pressing f8 many timesuntil weseeadvancedboot options. From thatoptionsselectcommandpromptfrom the list.

In windows8pressthepowerbuttonin thelogin screen,pressandholdshiftandclickrestart.Now select troubleshootin thatadvanced optionsstart up settingsandpressrestart.When ourpcisactive selectenablesafemodewithnetworking.

B. [7] Restoresystemfiles andsettings

TypeCDrestoresin thecommandpromptthen presses enter and now type rstrui.exe and press enteragain.Waitingforthenewwindow showsup afterthatclicknextandselectourrestore pointand clicknextandpressyes tostartsystemrestore.

Afterrestoring,downloadandscan thecomputer with reimage andmakesurethatMIRAIremoved fully

VII. MITIGATINGFACTORSANDREACTIN FUTURE

Implementingindustry standardisthebest currentpracticesandby usingintelligentDDOS systemssuch asArborsp/TmsandAps.We can solve MIRAIattacksinfuture.Networkoperations shouldmakeuseof DDOSmitigationmechanism such assourcebasedremotely triggeredblack holes(s/RTBH),flowpec.

ToavoidMIRAIenteringinto the devices precautions areneededtheyare

a) LimitIOTdevices:Make the IOTdevices tobeofflimitednumber

b)Createstrongpolicy enforcement:By doing this we can prevent an attack on infrastructure.

c)DevelopalistofapprovedIOTdevices: Ensure all thedevicesmetwith aminimumlevel of security

d)Regularscan:Scan theDevicesregularly inordertoremoveMIRAIinfuture.

e)Utilizingnetwork segmentation:reduce organizationavailableattack

VIII.CONCLUSION

Thesecuritythreatsshouldbeanalyzedinorder toprotectthe IOTdevices.Varioussecurity mechanism and tools/techniques are needed. Hackers andmanyalgorithmsaretheretobreak passwords whichleadtogreatloss.Sowe need advancedsecuritymechanism tosecureour information.

References

[1]https://www.helpnetsecurity.com/2017/02/14/security-iot-threats/

[2]http://www.prnewswire.com/news-releases/connected-devices-expose-major-enterprise-cyber-risk-in-2017-300405995.html.

[3]https://www.tripwire.com/state-of-security/latest-security-news/black-hat-survey-enterprise-security-fails-to-address-the-biggest-threats/

[4]https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf

[5]http://www.securityweek.com/unintentional-mistakes-biggest-insider-threat-survey

[6]http://blogs.cisco.com/security/what-does-mirai-iot-botnets-mean-to-the-public-Sector

[7]http://www.2-spyware.com/remove-mirai-virus.html

[8]http://economictimes.indiatimes.com/industry/banking/finance/banking/axis-bank-yet-to-figure-out-extent-of-server-breach-damage-ifany/articleshow/54927032.cms
[9]https://en.wikipedia.org/wiki/Mirai_(malware)
[10]http://thehackernews.com/
[11]http://www.pcworld.com/article/3169413/security/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html
[12]http://thehackernews.com/2017/02/mirai-iot-botnet-windows.html
[13]https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack[14]http://www.itpro.co.uk/security/27292/new- scanner-allows-users-to-check-iot-devices-for-mirai-malware-infection
[15]https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind- recent-major-ddos-attacks
[16]https://nakedsecurity.sophos.com/2016/10/05/mirai-internet-of-things-malware-from-krebs-ddos-attack-goes-open-source/
[17]http://security.stackexchange.com/questions/144311/remove-mirai-virus-on-router
[18]https://www.helpnetsecurity.com/2016/10/31/extinguish-mirai-threat/
[19]https://www.pressreader.com/india/pcquest/20161201/28153511061358.