A Comprehensive Study on Recent Botnet

Mersen Longkumer[1], Kapil Joshi[2]

Computer Science Department, Uttaranchal University, Dehradun, Uttarakhand

Abstract: ***Most of the email spams, DDos attacks and click frauds are caused by compromised machines which form botnets Botnets are also used for information thefts, either personal or cooperative. Mordern Botnets such as Mirai primarily targets online consumer devices such as remote cameras and home routers. Network formed by infected machines under the control of controller or Botmaster is called Botnet. It has been a serious threat to The Internet community since the advent of EggDrop during the year 1993 which is considered as the first recognized IRC bots. These types of networks were created to implement illegal activities, disturbing the normal activities of legitimate users. Though research on this topic is of great importance and has been going on for years, the researchers often face difficulty due to privacy issues for examination of packets and legal issues. This paper reviews and discusses the working of modern botnets (2010 onwards) like TDL4, Zues, Kelihos, Ramnit, Chameleon and Mirai and methods to detect and prevent them based on previously published studies. This paper also discusses the notable and insistent problems that researchers are facing.***

Keywords: Botnet, Network security, Bots, TDL4, Zues, Kelihos, Ramnit, Chameleon, Mirai

1. Introduction

Networks of Infected machines also called Botnets are one of the most critical Network security issue in the Internet in recent times. The bots or infected machines which are under the control of bot masters are used to carry out various malicious activities like DDos attacks, email spams ,banking information theft etc which causes harm or disturbs the normal operation of genuine users.

Botnets rely on C&C channels for communication with their Botmasters . The command which are passed on to the bots are through this channel .There are three types of channel Internet Relay Chat(IRC)-Based C&C channels, HTTP-based C&C channels and Peer-to-peer (P2P) based C&C channels[10] .Since botnets rely on these channels for their communication and co-ordination of attacks, this also becomes the weakest point of a botnet for example a centralized botnet for example an IRC botnet's or a HTTP botnet's functioning can be stopped by locating and shutting down its central server , and by capturing the bootstrap nodes in a peer-to-peer botnet,a peer-to-peer botnet will not be able to recruit new bots.[*13*].

Botnets have proven time and again to be one of the key factors of financial losses to Internet Service Providers (ISP), private companies, governments and even home users[11]. Botnets are also rented out by the cybercriminals (for example to spammers for promotion of their illicit goods [15]), several operations have been performed for it to be taken down[15][16] but sadly due to the involvement of many parties, the problem becomes so complex that it becomes hard to come up with a policy that prevents the cybercriminals from coming back into business[12].

Number of bots on the Internet is huge and these bots perform operation like steal sensitive information from compromised machines (Zues,Ramnit)[14][20],intercepting a system's network traffic in search of (for example passwords, banking information or any information that will add to the cybercriminal's financial gain)(TLD4),theft of bit coin(Kelihos),click frauds(Chameleon)[18][25],Locate and compromise IoT devices(for example webcams, routers etc)(Mirai)[21][24].Table 1 presents the creation year and the estimated number of bots for these botnets

2. Reference Work

There are several surveys and research on the botnets .In [17],C&C architecture are classified as centralized or decentralized and further breaks down botnet detection techniques into signature-based, anomaly-based, DNS-based, and mining-based. [19] explores the various components of the Zeus kit :-the builder (to create both encrypted configuration file and the bot executable), the configuration file(most essential component, if the bot is to be useful. Amongst other things it contains the address to which the stolen data is to be sent), the exe file(Built by the builder component) and the server (collection of php scripts that allows the botmaster to monitor the bots ,send command to the bots, retrieve information from the bots),it also talks about functionality and behavior of the Zeus binary .Eugene Rodionov et al.[22] investigated cybercrime group GangstaBucks and ways by which they distributed the TLD4 bootkit and also investigated the implementation details of the malware.Botnets tends to evolve overtime,[26] discusses and compares the evolution of Kelihos Botnet from its two predecessors(Waledac and Nuwar). Catrina Sharp [23] mentioned ways of protection and prevention from click frauds (Chameleon) which had stole over 6.2 million dollars per month from advertisers .With the rapid expansion of IOT, these devices are also prone to Bontnet evasion. Jialu Wei et al. [29] addresses how DDos attacks are co-ordinated through the security vulnerabilities of IOT devices and measures to be taken to enhance security of IOT devices

Table I: Creation year and the estimated number of recent botnets

Year created	*Name*	
2010(around)	TLD4	4,500,000
	Zeus	3,600,000(US only)
2010	Kelihos	300,000+
2011 or earlier	Ramnit	3,000,000
2012(around)	Chameleon	120,000
2016(august)	Mirai	380,000

3. The Zeus Botnet

Zeus also considered "King of Bots"[5][20]which has existed and evolved since 2007 is a malware package, the package usually contains a The Builder ,The Configuration File ,The Exe File ,The Server ,it is often available for sale or even traded [20][19]. The main Purpose of Zeus is financial gain for example stealing Banking information etc. The Bots generated runs silently on the background stealing sensitive information and sending it to its master (Botmaster). Since the Zeus toolkit is sold, there are many independent Botnet belonging to different Botmasters.

A) Installation

As mentioned in[20],Zeus botnet can be spread through popular methods such as drive by download and email spams . Spam Emails created using social engineering imitating a legitimate mail from a legitimate organisation. Once the bot is executed the injection process takes place. Firstly if the Zeus is running on an account with Administrative privillages, it will copy itself to system32\sdra64.exe,it sets previous path to o HKEY _ LOCAL _ MACHINE\Software\Microsoft\WindowsNT\winlogon\user init such that the winlogon.exe spawns the process at startup. It searches for winlogon.exe to increase its privillage, also injects its code plus a string table into this process and for the execution of this code a thread is created. At this point the execution of the main bot executable terminates as it completes its injection. The code which was injected in winlogon, it injects additional code into svchost.exe. It also creates a folder %System%\lowsec and places two files inside local.ds and user. ds, local.ds contains the latest dynamic configuration downloaded from its C&C server and the user.ds contains all the information stolen from the victims machine to be transferred to the server. The code injected into svchost.exe. is accountable for the network communication and third-party process injection required to hook Internet-related APIs for the injection or for stealing information to/from banking sites .Injected components communicate with the help of with mutexes and pipesnamed _AVIRA_x, where x is a number (eg: x=2109 in winlogon.exe, x=2108 in svchost.exe). If the zues bot is not running on an a account with administrative privillages the code injected into winlogon.exe will be injected into o explorer.exe instead. And the process of copying itself will be done into o %UserProfile%\ApplicationData\sdra64.exe, and will put the folder %UserProfile%\Application Data\lowsec instead of copying itself into the %System% folder. Finally, the bot will create a load point under the registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"userinit"="%UserProfile%\Application Data\sdra64.exe"

B) Detection and removal

It is advisable, to prevent users from clicking suspicious links in email or web and also always keeping updated antivirus. Symentecs has also claimed that Symentec Browser Protection can prevent attempt infection upto some certain level .Removal of the Zeus rootkit was confirmed by rebooting and performing subsequent scans of corroborating tools as well as observing the lack of certain behaviors like the hiding of the System32/lowsec lack of the backdoor TCP port associated with Winlogon.exe or Svchost.exe[1][4].

The evolved Zeus, Zeus v3 also known as Gameover Zeus or even P2P Zeus spread globally fig2 in the recent years. Later it was temporarily taken down by international inter-agency collaboration named Operation Tovar by temporarily cutting communication between Gameover ZeuS and its command and control servers in early June 2014.

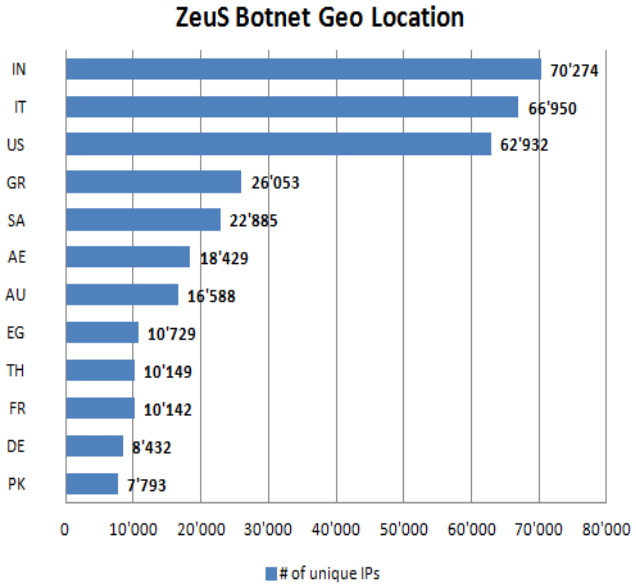


Figure 1: Zeus Botnet Geo Location

4. TLD4 and Kelihos Botnet

TLD4 botnet is generally used for Spam, denial os service attacks circulation of maleware, information theft and other online frauds. Typically TLD4 infects a machine by drive by download through questionable website (for example pitated media websites) .It spreads rapidly through Peer to Peer network and control instruction are passed from one peer to the other .After the installation of TDL4 it downloads more malware into to victim's computer. The software also makes sure that no other competitor's maleware is running by searching and removing it, if any present. It installs to the master boot record(MBR), so that it runs even before the host boots up not only that it also encripts its data to hide its communication from network analysis tools. Thus TLD4 is also reffered as The ‘indestructible’ botnet [27]. Kelihos like other botnet is used for spams and information theft. It seems that the initial spread is through mailicious link embedded in e-mails .Clicking on the link the Victim is directed to a page which recommends for a software update or download (for example flash player download) which leads to the download of the malware.

a) Installation

The installation of TLD4 is handled differently on x64 and x86 machines .The dropper when upacked if it is running in Wow64 process and determines which code to execute Kelihos malware executable file is a Microsoft Visual C++ 6.0 compiled binary with custom packed content stored in the executable's overlay section. It installs WinPcap, a legitimate and commonly used Windows packet capture library. Study on more recent updates of kelihos suggest that it uses the file name “winlogon.exe” for the malicious process executed under a user’s account. Which the Windows considers this process as a system process and protects it from being terminated even though it is run by “User”.

Table 2: Installation of TLD in x64 and x86 machines

TLD installation in x64	TLD installation in x86
The dropper writes all the hard disk by sending IOCTL_SCSI_PASS_THROUGH_DIRECT request to disk a class driver. It obtains disk’s parameters and creates the image of hidden file system in the memory buffer which is then written on the hard drive at certain offset. When the image is written the modification of the MBR of the disk takes place to get its malicious components loaded at boot time .The dropper then reboots the system by calling the ZwRaiseHardError routine ,passing as its fifth parameter OptionShutdownSystem which instructs the system to display Blue Screen of Death screen and then reboots the system.	To bypass Host Intrusion Prevention System the bootkit loads itself as print provider as trusted system process (spooler.exe) from where it loads a Kernel-mode Driver (drv32) which infects the system . Another Host Intrusion Prevention System is used by the loader that is it books Zwconnect port System routine exported from ntdll.dll. When the driver is loaded in the Kernel-mode address space it overwrites the MBR(Master Boot Record) of the disk by sending (SCSI Requesting Block) directly to the miniport device object, then it initializes the hidden file system.Createfile and Writefile API functions are used to write the bootkit’s module into hidden file system from the dropper

b) Detection and removal

Many antivirus company has come up with solutions for the detection and removal of TLD4 antivirus for example, the release of TDSSKiller by Kaspersky Labs for Windows users (all versions, 32 and 64-bit) which will detect and remove TDL4 rootkits or bootkits. This TDSSKiller also helps in detection of TDSS-rootkit family like TDL2 / TDL3, and unknown rootkits by analyzing Hidden or Blocked services, Hidden or Blocked files, Forged files Rootkit.Win32.Backboot.gen (generic / unknown MBR infection). Kelihos usually disables the antivirus or firewall installed on the computer .Experts suggest the use of anti-malware programs and cleaning windows registry is a way of removing Kelihos.

5. Ramnit and Chameleon

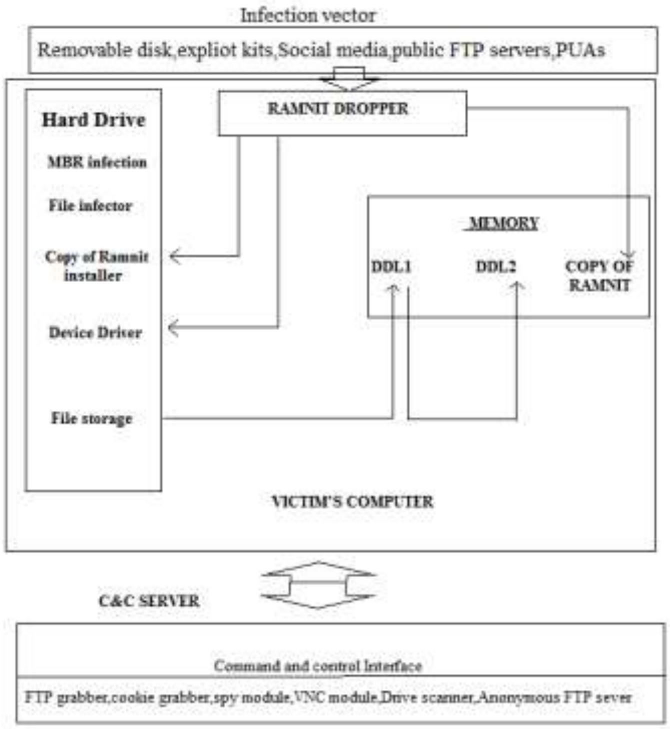
Chameleon is a Botnet that that commits Click fraud .Click fraud is a type of crime that abuses pay-per-click (PPC) advertising to make money through fake or fraudulent clicks on ads. PPC works by paying a certain amount of money when a link or an advertisment (ad) is clicked .Advertisers place ads on a website operators’ websites and has to pay a certain amont of fee when the ad is clicked. The advertising network which is the advertiser registers with the advertising network, places the ads on the publisher's website and each time thge ad is clicked the advitiser pay a certain amount to the network as well as the publisher places Click fraud is the process of clicking an ad with intension of of generating a charge without having any interest in the ad. The malicious actor can earn lots of money by generating fake clicks without the knowledge of the network[25] .Ramnit is used for stealing information such as online banking credentials ,passwords ,it generally spreads through the use of removable devices for example USB drives or Network shares.

a) Installation

Chameleon enters the systems through malicious email links or infected attachments or by programs that is installed unintentionally .Chameleon infects systems by attaching itself as extra payloads to other files. Once it has been injected o a system ,it modifies the Windows Registry for the malicious program to be started up during boot time .ots like Chameleon infect your system by attaching itself as extra payloads to other files. Chameleon then creates and starts a bot to do some task repetitively and automatically .It then spreads through the infected computer through network it use or by shared drives or even by spam mails send by the infected computer without its knowledge [8]. Ramnit enters the system generally by means of removable disk and network shares, through public FTP servers ,redirecting users to this exploit kit through ads on legitimate websites and by bundling the malware with potentially unwanted application(PUA) .Once the Ramnit has been injected and runned in a computer ,a copy of the installer is written into the computer's file system as well as the computer's memory ,so that whenever an antivirus software detects and removes it,it is constantly copied in the computer's file system and executed on the computer. In order to run with administrative rights the Microsoft Windows Kernel ‘Win32k.sys’ CVE-2014-4113 Local Privilege Escalation Vulnerability (CVE-2014-4113) may be used. The Ramnit installer contains three components. Firstly a device driver which is copied into the file system and loaded as a service called “Microsoft Windows Service”. After the installer makes a copy of itself into the file system and does modification to the registry so as to make the driver component load after the computer restarts .The 2nd and 3rd components are DLL files DLL_1 and DLL_2 and are put into the memory .DLL_1 stores the received modules from DLL_2 into storage containers and DLL_1 can load and run those modules whenever required basically DLL_1 acts as a bridge between DLL_2 and storage container or log file . DLL_2 acts as a backdoor and does work of establishing connection to C&C server using a custom domain generator algorithm .It receives and executes command on behalf of the attacker .After the connection with C&C server is done , the communication with the C&C server starts which has all the malware module ready to be used [7].Fig2 shows Ramnit’s infection vector, structure and module

b) Detection and removal

For Chemeleon, as for every botnet experts advice the keeping up with the Operating system and Antivirus update. For Ramnit detection and removal tools such as W32.Ramnit Removal Tool by Symantec can be used . This tool removes the malware by removing processes involved with Ranmit, repairs injected files, resets the registry key as it was before [28] .


Infection vector
Removable disk,expliot kits,Social media,public FTP servers,PUAs
Hard Drive
MBR infection
File infector
Copy of Ramnit installer
Device Driver
File storage
RAMNIT DROPPER
MEMORY
DDL1
DDL2
COPY OF RAMNIT
VICTIM'S COMPUTER
C&C SERVER
Command and control Interface
FTP grabber,cookie grabber,spy module,VNC module,Drive scanner,Anonymous FTP sever

[7] **Figure 2:** Ramnit's infection vector, structure, module

6. Mirai Botnet

With The Internet of thing (IOT) expanding rapidly the security of this thing become quite essential. The Mirai botnet aims for these type of devices that is IOT devices. The security problem arises as IOT is a new concept and likely that an IOT device is almost every time turned ON for example health monitoring system which can be easily detected by attackers constantly listening with port scans plus another concern is related to credential encryption and strength. IOT are usually IoT are usually kept with their default administrative usernames and passwords. Another reason may be because many IoT devices are rarely patched or taken care of[29]. Mirai botnets in recent years mostly infects cameras and routers and also printers .Investigation has uncovered 49,657 unique IPs which hosted Mirai-infected devices, which were mostly CCTV cameras[31].

a) Installation

Mirai's C&C (command and control) code is coded in Go, while its bots are coded in C. For recruiting bots , Mirai performs ip address scans the main reason of these scans is to locate unsecured IOT devices that can be accessed remotely by using easily guessable login credentials. According to experts most of the CCTVs login credentials have factory default usernames and passwords so as for routers that is admin/admin. Mirai also uses Brute force method (dictionary attacks) to guess passwords

b) Prevention

Prevention can be done by not using default/generic login credentials and disabling all remote WAN access to device .Shutting down unnecessary open ports or services . or can include technology to make ports invisible to random port sniffs[30] to prevent it. Use of account lockout policies to minimize the risk of brute force attacks and disabling Telnet and SSH on device if there is no requirement of remote management can reduce the infection as well[32]

7. Challenges

Although there are lots of research going on in this topic but there are lots of challenges that comes with it .Attackers have thousand of vulnerable ,unsecured host to be compromised but for the researchers can not access those host because administrative domain considers any information about their network to be a business secret and unlike botmasters ,researchers can obtain such information only through collaboration agreements. And also network traces which is the most detailed and most useful piece of information which may contain sensitive information are carefully controlled and never shared with outsiders or even with same organization [33].This makes the researchers to be in disadvantage when compared to the attacker, researchers generally end up using academic network to pursue their research .Academic network cannot imitates the reality of heterogeneous networks and thus proper study and understanding of the botnet become incomplete .Another challenge is estimation of how much a novel detection technique enhances overall botnet detection is difficult [33] A quantitative comparison of existing woks would become easier if there were a standard methodology or widely accepted benchmark for evaluating botnet but there is not. The growth of botnets will grow unless unless effective actions are taken to mitigate both technical and non-technical factors[11] (non-technical factors such as distributed environment, legal issues and low user awareness).Since botnets are distributed globally , thus agreement between countries are needed to prosecute cyber-crime in a consistent and coordinated way. Challenges of making aware of botnet is still there ,there are people who does not care to update antivirus or their operating system or even if there system tends to become slow as long as it runs and is able to surf the internet they use it, so user awareness is an important factor . And as for IOT devices , there are billions of it and we cant expect all the users to configure their device securely and it is also difficult for the vendor to make the device both simple, easly to use and secure at the same time ,[29] the choices between security, simplicity, and cost can be an tough one.

8. Conclusion

This paper discusses on the general overview of the recent botnets 2010 onwards. There will be more resilient and improved Botnets in future too. Botnet has been a serious network security threats and it will be in future too .With mobile platforms being used more and more for example smartphone and them being connected to The Internet almost all the time the Botnet threat becomes real scary. Ramnit botnet survived a takedown attempt in 2015 and has appeared again in 2016 , which suggest hackers or malicious person will always find its way to attack or compromise unsecured systems and the real question is how prepared are we?.Still many challenges lies ahead for researchers in this field like the difficulty of testing their proposals in a real scenario or using real data. It is very important to come up global policies to thoroughly combat the botnet threat

References

[1] Detection of Zeus Botnet in Computers Networks and Internet Dr.Laheeb M. Ibrahim Karam Hatim Thanoon Assistant Professor Assistant Lecturer/ PhD. Student Dept. of Software Engineering, College of Computer Sciences and Mathematical, University of Mosul

[2] FBI disrupts GameOver ZeuS and CryptoLocker Botnet abuse.ch The Swiss Security Blog https://www.abuse.ch/?p=7822

[3] TDL-4 (TDSS or Alureon) http://searchsecurity.techtarget.com/definition/TDL-4-TDSS-or-Alureon

[4] Arnold T. M. , ‖ A comparative analysis of rootkit detection techniques‖, 2011,thesis at the university of houston-clear lak

[5] Evolution of Zeus Botnet Shunichi Imano https://www.symantec.com/connect/blogs/evolution-zeus-botnet

[6] How to Detect and Remove TDL4 / TDL3 / TDSS / Alureon Rootkits http://practicalrambler.blogspot.in/2011/07/how-to-detect-tdl4-tdss-rootkits.html

[7] SECURITY RESPONSE W32.Ramnit analysis Symantec Security Response https://www.symantec.com/

[8] How to Remove Chameleon by Jay Geate http://www.solvusoft.com/en/malware/bots/chameleon/

[9] How to Get Rid of KELIHOS? by Jay Geater http://www.solvusoft.com/en/malware/worms/kelihos/

[10] Detection and Classification of Different Botnet C&C Channels by Gregory Fedynyshyn,Mooi Choo Chuah and Gang Tan

[11] Botnets: A surveySérgio by S.C. Silva , Rodrigo M.P. Silva , Raquel C.G. Pinto , Ronaldo M. Salles

[12] The Tricks of the Trade: What Makes Spam Campaigns Successful? by Jane Iedemska, Gianluca Stringhini, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna University of California, Santa Barbara {7 am, gianluca, kemm, chris, vigna}@cs.ucsb.edu

[13] Tsunami: A parasitic, indestructible botnet on Kad Ghulam Memon by Jun Li · Reza Rejaie

[14] SecurityResponse/W32.Ramnit https://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99

[15] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating LargeScale Spam Campaigns. In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2011.

[16] B. Krebs. Taking Stock of Rustock. http://krebsonsecurity.com/2011/01/taking-stock-of-rustock/, 2011

[17] M. Feily, A. Shahrestani, S. Ramadass, A survey of botnet and botnet detection, in: Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on, pp. 268–273.

[18] What You Need to Know About the Chameleon Botnet By Catrina Sharp http://blog.ezanga.com/blog/what-you-need-to-know-about-the-chameleon-botnet

[19] What is Zeus? By James Wyke, Threat Researcher, SophosLabs UK

[20] Zeus: King of the Bots by Nicolas Falliere and Eric Chien

[21] Webcam firm recalls hackable devices after mighty Mirai botnet attack by BY GRAHAM CLULEY https://www.welivesecurity.com/2016/10/24/webcam-firm-recalls-hackable-devices-mighty-mirai-botnet-attack/

[22] The Evolution of TDL: Conquering x64 Revision 1.1 Eugene Rodionov, Malware Researcher Aleksandr Matrosov, Senior Malware Researcher

[23] What You Need to Know About the Chameleon Botnet by Catrina Sharp

[24] What's a Mirai Botnet Doing With My Router? https://safeandsavvy.f-secure.com/2016/11/30/whats-a-mirai-botnet-doing-with-my-router/

[25] Chameleons, botnets and click fraud by Graham Cluley https://nakedsecurity.sophos.com/2013/03/20/chameleon-botnet-click-fraud/

[26] SAME BOTNET, SAME GUYS,NEW CODE Pierre-Marc Bureau ESET, spol. s r.o., Aupark Tower, 16th Floor, Einsteinova 24, 851 01 Bratislava, Slovak Republic Email bureau@eset.sk

[27] TDL4 – Top Bot By Igor Soumenkov, Sergey Golovanov on June 27, 2011 https://securelist.com/analysis/publications/36152/tdl4-top-bot/

[28] W32.Ramnit Removal Tool Symantec https://www.symantec.com/security_response/writeup.jsp?docid=2015-022415-4725-99

[29] DDoS on Internet of Things – a big alarm for the future by Jialu Wei , Ming Chow

[30] Paley, Walter. "Securing the Internet of Things | SafeLogic." SafeLogic. Safelogic, 02 Jan. 2015. Web. 14 Dec. 2016.

[31] Breaking Down Mirai: An IoT DDoS Botnet Analysis Ben Herzberg,Dima Bekerman,Igal Zeifman https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[32] Botnet cleaning and maleware analysis center cyber swachhta kendra http://www.cyberswachhtakendra.gov.in/alerts/mirai.html

[33] A. J. Aviv, A. Haeberlen, Challenges in experimenting with botnet detection systems, in: Proceedings of the 4th USENIX Workshop on Cyber Security Experimentation, and Test (CSET'11), 2011.