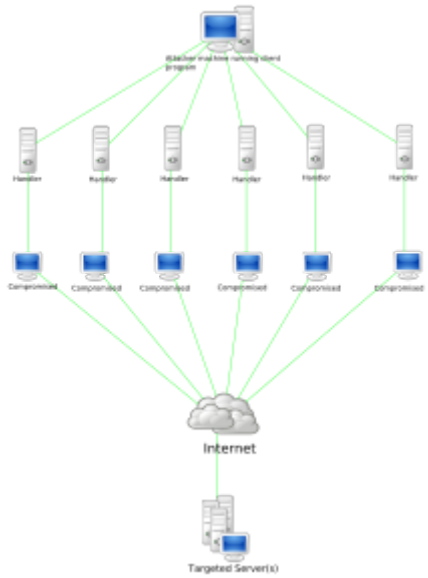
WIKIPEDIA

Botnet

A **botnet** is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data,[1] send spam, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software.[2] The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.



Stacheldraht botnet diagram showing a DDoS attack. (Note this is also an example of a type of client-server model of a botnet.)

Contents

Overview

A botnet is a logical collection of internet-connected devices such as computers, smartphones or IoT devices whose security has been breached and control ceded to a third party. Each such compromised device, known as a "bot", is created when a device is penetrated by software from a *malware* (malicious software) distribution. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP).[3]

Botnets are increasingly rented out by cyber criminals as commodities for a variety of purposes.[4]

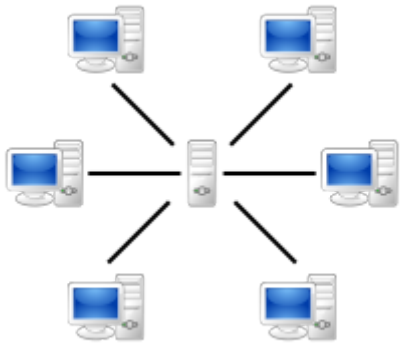
Architecture

Botnet architecture has evolved over time in an effort to evade detection and disruption. Traditionally, bot programs are constructed as clients which communicate via existing servers. This allows the **bot herder** (the person controlling the botnet) to perform all control from a remote location, which obfuscates their traffic.[5] Many recent botnets now rely on existing peer-to-peer networks to communicate. These P2P bot programs perform the same actions as the client-server model, but they do not require a central server to communicate.

Client-server model

The first botnets on the internet used a client-server model to accomplish their tasks. Typically, these botnets operate through Internet Relay Chat networks, domains, or websites. Infected clients access a predetermined location and await incoming commands from the server. The bot herder sends commands to the server, which relays them to the clients. Clients execute the commands and report their results back to the bot herder.

In the case of IRC botnets, infected clients connect to an infected IRC server and join a channel pre-designated for C&C by the bot herder. The bot herder sends commands to the channel via the IRC server. Each client retrieves the commands and executes them. Clients send messages back to the IRC channel with the results of their actions.[5]



A network based on the client-server model, where individual clients request services and resources from centralized servers

Peer-to-peer

In response to efforts to detect and decapitate IRC botnets, bot herders have begun deploying malware on peer-to-peer networks. These bots may use digital signatures so that only someone with access to the private key can control the botnet.[6] See e.g. Gameover ZeuS and ZeroAccess botnet.

Newer botnets fully operate over P2P networks. Rather than communicate with a centralized server, P2P bots perform as both a command distribution server and a client which receives commands.[7] This avoids having any single point of failure, which is an issue for centralized botnets.

In order to find other infected machines, the bot discreetly probes random IP addresses until it contacts another infected machine. The contacted bot replies with information such as its software version and list of known bots. If one of the bots' version is lower than the other, they will initiate a file transfer to update.[6] This way, each bot grows its list of infected machines and updates itself by periodically communicating to all known bots.

A peer-to-peer (P2P) network in which interconnected nodes ("peers") share resources among each other without the use of a centralized administrative system

Core components of a botnet

A botnet's originator (known as a "bot herder" or "bot master") controls the botnet remotely. This is known as the command-and-control (C&C). The program for the operation which must communicate via a covert channel to the client on the victim's machine (zombie computer).

Control protocols

IRC is a historically favored means of C&C because of its communication protocol. A bot herder creates an IRC channel for infected clients to join. Messages sent to the channel are broadcast to all channel members. The bot herder may set the channel's topic to command the botnet. E.g. the message `:herder!herder@example.com TOPIC #channel DDoS www.victim.com` from the bot herder alerts all infected clients belonging to #channel to begin a DDoS attack on the website www.victim.com. An example response `:bot1!bot1@compromised.net PRIVMSG #channel I am DDoSing www.victim.com` by a bot client alerts the bot herder that it has begun the attack.[6]

Some botnets implement custom versions of well-known protocols. The implementation differences can be used for detection of botnets. For example, Mega-D features a slightly modified SMTP implementation for testing spam capability. Bringing down the Mega-D's SMTP server disables the entire pool of bots that rely upon the same SMTP server.[8]

Zombie computer

In computer science, a zombie computer is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack. Many computer users are unaware that their computer is infected with bots.[9]

The process of stealing computing resources as a result of a system being joined to a "botnet" is sometimes referred to as "scrumping".[10]

Command and control

Botnet Command and control (C&C) protocols have been implemented in a number of ways, from traditional IRC approaches to more sophisticated versions.

Telnet

Telnet botnets use a simple C&C botnet Protocol in which bots connect to the main command server to host the botnet. Bots are added to the botnet by using a scanning script, the scanning script is run on an external server and scans IP ranges for telnet and SSH server default logins. Once a login is found it is added to an infection list and infected with a malicious infection line via SSH on from the scanner server. When the SSH command is run it infects the server and commands the server to ping to the control server and becomes its slave from the malicious code infecting it. Once servers are infected to the server the bot controller can launch DDoS attacks of high volume using the C&C panel on the host server. These types of botnets were used to take down large websites like Xbox and PlayStation network by a known hacking group called Lizard Squad.

IRC

IRC networks use simple, low bandwidth communication methods, making them widely used to host botnets. They tend to be relatively simple in construction and have been used with moderate success for coordinating DDoS attacks and spam campaigns while being able to continually switch channels to avoid being taken down. However, in some cases, merely blocking of certain keywords has proven effective in stopping IRC-based botnets. The RFC 1459 (IRC) standard is popular with botnets. The first known popular botnet controller script, "MaXiTE Bot" was using IRC XDCC protocol for private control commands.

One problem with using IRC is that each bot client must know the IRC server, port, and channel to be of any use to the botnet. Anti-malware organizations can detect and shut down these servers and channels, effectively halting the botnet attack. If this happens, clients are still infected, but they typically lie dormant since they have no way of receiving instructions.[6] To mitigate this problem, a botnet can consist of several servers or channels. If one of the servers or channels becomes disabled, the botnet simply switches to another. It is still possible to detect and disrupt additional botnet servers or channels by sniffing IRC traffic. A botnet adversary can even potentially gain knowledge of the control scheme and imitate the bot herder by issuing commands correctly.[11]

P2P

Since most botnets using IRC networks and domains can be taken down with time, hackers have moved to P2P botnets with C&C as a way to make it harder to be taken down.

Some have also used encryption as a way to secure or lock down the botnet from others, most of the time when they use encryption it is public-key cryptography and has presented challenges in both implementing it and breaking it.

Domains

Many large botnets tend to use domains rather than IRC in their construction (see Rustock botnet and Srizbi botnet). They are usually hosted with bulletproof hosting services. This is one of the earliest types of C&C. A zombie computer accesses a specially-designed webpage or domain(s) which serves the list of controlling commands. The advantages of using web pages or domains as C&C is that a large botnet can be effectively controlled and maintained with very simple code that can be readily updated.

Disadvantages of using this method are that it uses a considerable amount of bandwidth at large scale, and domains can be quickly seized by government agencies without much trouble or effort. If the domains controlling the botnets are not seized, they are also easy targets to compromise with denial-of-service attacks.

Fast-flux DNS can be used as a way to make it difficult to track down the control servers, which may change from day to day. Control servers may also hop from DNS domain to DNS domain, with domain generation algorithms being used to create new DNS names for controller servers.

Some botnets use free DNS hosting services such as DynDns.org, No-IP.com, and Afraid.org to point a subdomain towards an IRC server that harbors the bots. While these free DNS services do not themselves host attacks, they provide reference points (often hard-coded into the botnet executable). Removing such services can cripple an entire botnet.

Others

Calling back to large social media sites[12] such as GitHub,[13] Twitter,[14][15] Reddit,[16] Instagram,[17] the XMPP open source instant message protocol[18] and Tor hidden services[19] are popular ways of avoiding egress filtering to communicate with a C&C server.[20]

Construction

Traditional

This example illustrates how a botnet is created and used for malicious gain.

1. A hacker purchases or builds a Trojan and/or exploit kit and uses it to start infecting users' computers, whose payload is a malicious application—the *bot*.

2. The *bot* instructs the infected PC to connect to a particular command-and-control (C&C) server. (This allows the botmaster to keep logs of how many bots are active and online.)
3. The botmaster may then use the bots to gather keystrokes or use form grabbing to steal online credentials and may rent out the botnet as DDoS and/or spam as a service or sell the credentials online for a profit.
4. Depending on the quality and capability of the bots, the value is increased or decreased.

Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.[21]

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. After the software is downloaded, it will call home (send a reconnection packet) to the host computer. When the re-connection is made, depending on how it is written, a Trojan may then delete itself or may remain present to update and maintain the modules.

Others

In some cases, a botnet may be temporarily created by volunteer hacktivists, such as with implementations of the Low Orbit Ion Cannon as used by 4chan members during Project Chanology in 2010.[22]

China's Great Cannon of China allows the modification of legitimate web browsing traffic at internet backbones into China to create a large ephemeral botnet to attack large targets such as GitHub in 2015.[23]

Common features

- Most botnets currently feature distributed denial-of-service attacks in which multiple systems submit as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests. An example is an attack on a victim's server. The victim's server is bombarded with requests by the bots, attempting to connect to the server, therefore, overloading it.
- Spyware is software which sends information to its creators about a user's activities – typically passwords, credit card numbers and other information that can be sold on the black market. Compromised machines that are located within a corporate network can be worth more to the bot herder, as they can often gain access to confidential corporate information. Several targeted attacks on large corporations aimed to steal sensitive information, such as the Aurora botnet.[24]
- E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying, or malicious.
- Click fraud occurs when the user's computer visits websites without the user's awareness to create false web traffic for personal or commercial gain.[25]
- Bitcoin mining was used in some of the more recent botnets have which include bitcoin mining as a feature in order to generate profits for the operator of the botnet.[26][27]
- Self-spreading functionality, to seek for pre-configured command-and-control(CNC) pushed instruction contains targeted devices or network, to aim for more infection, is also spotted in several botnets. Some of the botnets are utilizing this function to automate their infections.

Market

The botnet controller community features a constant and continuous struggle over who has the most bots, the highest overall bandwidth, and the most "high-quality" infected machines, like university, corporate, and even government machines.[28]

While botnets are often named after the malware that created them, multiple botnets typically use the same malware but are operated by different entities.[29]

Countermeasures

The geographic dispersal of botnets means that each recruit must be individually identified/corralled/repaired and limits the benefits of filtering.

Computer security experts have succeeded in destroying or subverting malware command and control networks, by, among other means, seizing servers or getting them cut off from the Internet, denying access to domains that were due to be used by malware to contact its C&C infrastructure, and, in some cases, breaking into the C&C network itself.[30][31][32] In response to this, C&C operators have resorted to using techniques such as overlaying their C&C networks on other existing benign infrastructure such as IRC or Tor, using peer-to-peer networking systems that are not dependent on any fixed servers, and using public key encryption to defeat attempts to break into or spoof the network.

Norton AntiBot was aimed at consumers, but most target enterprises and/or ISPs. Host-based techniques use heuristics to identify bot behavior that has bypassed conventional anti-virus software. Network-based approaches tend to use the techniques described above; shutting down C&C servers, null-routing DNS entries, or completely shutting down IRC servers. BotHunter is software, developed with support from the U.S. Army Research Office, that detects botnet activity within a network by analyzing network traffic and comparing it to patterns characteristic of malicious processes.

Researchers at Sandia National Laboratories are analyzing botnets' behavior by simultaneously running one million Linux kernels—a similar scale to a botnet—as virtual machines on a 4,480-node high-performance computer cluster to emulate a very large network, allowing them to watch how botnets work and experiment with ways to stop them.[33]

One thing that's becoming more apparent is the fact that detecting automated bot attacks is becoming more difficult each day as newer and more sophisticated generations of bots are getting launched by attackers. For example, an automated attack can deploy a large bot army and apply brute-force methods with highly accurate username and password lists to hack into accounts. The idea is to overwhelm sites with tens of thousands of requests from different IPs all over the world, but with each bot only submitting a single request every 10 minutes or so, which can result in more than 5 million attempts per day.[34] In these cases, many tools try to leverage volumetric detection, but automated bot attacks now have ways of circumventing triggers of volumetric detection.

One of the techniques for detecting these bot attacks is what's known as "signature-based systems" in which the software will attempt to detect patterns in the request packet. But attacks are constantly evolving, so this may not be a viable option when patterns can't be discerned from thousands of requests. There's also the behavioral approach to thwarting bots, which ultimately is trying distinguish bots from humans. By identifying non-human behavior and recognizing known bot behavior, this process can be applied at the user, browser, and network levels.

The most capable method of using software to combat against a virus has been to utilize Honeypot software in order to convince the malware that a system is vulnerable. The malicious files are then analyzed using forensic software.

On July 15, 2014, the Subcommittee on Crime and Terrorism of the Committee on the Judiciary, United States Senate, held a hearing on the threats posed by botnets and the public and private efforts to disrupt and dismantle them.[35]

Historical list of botnets

The first botnet was first acknowledged and exposed by Earthlink during a lawsuit with notorious spammer Khan C. Smith[36] in 2001 for the purpose of bulk spam accounting for nearly 25% of all spam at the time.[37]

Around 2006, to thwart detection, some botnets were scaling back in size.[38]

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity (bn/day)	Aliases
2003		MaXiTE	500-1000 servers	0	MaXiTE XDCC Bot, MaXiTE IRC TCL Script, MaxServ
2004 (Early)		Bagle	230,000[39]	5.7	Beagle, Mitglieder, Lodeight
		Marina Botnet	6,215,000[39]	92	Damon Briant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken
		Torpig	180,000[40]		Sinowal, Anserin
		Storm	160,000[41]	3	Nuwar, Peacomm, Zhelatin
2006 (around)	2011 (March)	Rustock	150,000[42]	30	RKRustok, Costrat
		Donbot	125,000[43]	0.8	Buzus, Bachsoy
2007 (around)		Cutwail	1,500,000[44]	74	Pandex, Mutant (related to: Wigon, Pushdo)
2007		Akbot	1,300,000[45]		
2007 (March)	2008 (November)	Srizbi	450,000[46]	60	Cbeplay, Exchanger
		Lethic	260,000[39]	2	none
		Xarvester	10,000[39]	0.15	Rlsloup, Pixoliz
2008 (around)		Sality	1,000,000[47]		Sector, Kuku
2008 (around)	2009-Dec	Mariposa	12,000,000[48]		
2008 (November)		Conficker	10,500,000+[49]	10	DownUp, DownAndUp, DownAdUp, Kido
2008 (November)	2010 (March)	Waledac	80,000[50]	1.5	Waled, Waledpak
		Maazben	50,000[39]	0.5	None
		Onewordsub	40,000[51]	1.8	
		Gheg	30,000[39]	0.24	Tofsee, Mondera
		Nucrypt	20,000[51]	5	Loosky, Locksky
		Wopla	20,000[51]	0.6	Pokier, Slogger, Cryptic
2008 (around)		Asprox	15,000[52]		Danmec, Hydraflux
		Spamthru	12,000[51]	0.35	Spam-DComServ, Covesmer, Xmiler
2008 (around)		Gumblar			
2009 (May)	November 2010 (not complete)	BredoLab	30,000,000[53]	3.6	Oficla
2009 (Around)	2012-07-19	Grum	560,000[54]	39.9	Tedroo
		Mega-D	509,000[55]	10	Ozdok

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity (bn/day)	Aliases
		Kraken	495,000[56]	9	Kracken
2009 (August)		Festi	250,000[57]	2.25	Spamnost
2010 (March)		Vulcanbot			
2010 (January)		LowSec	11,000+[39]	0.5	LowSecurity, FreeMoney, Ring0.Tools
2010 (around)		TDL4	4,500,000[58]		TDSS, Alureon
		Zeus	3,600,000 (US only)[59]		Zbot, PRG, Wsnpoem, Gorhax, Kneber
2010	(Several: 2011, 2012)	Kelihos	300,000+	4	Hlux
2011 or earlier	2015-02	Ramnit	3,000,000[60]		
2013 (early)	2013	Zer0n3t	200+ server computers	4	Fib3rl0g1c, Zer0n3t, Zer0Log1x
2012 (Around)		Chameleon	120,000[61]		None
2016 (August)		Mirai	380,000		None

- Researchers at the University of California, Santa Barbara took control of a botnet that was six times smaller than expected. In some countries, it is common that users change their IP address a few times in one day. Estimating the size of the botnet by the number of IP addresses is often used by researchers, possibly leading to inaccurate assessments.[62]

See also

- Computer worm
- Spambot
- Timeline of computer viruses and worms
- Advanced Persistent Threat

References

1. "Thingbots: The Future of Botnets in the Internet of Things" (https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/). *Security Intelligence*. 20 February 2016. Retrieved 28 July 2017.
2. "botnet" (https://www.techopedia.com/definition/384/botnet). Retrieved 9 June 2016.
3. Ramneek, Puri (2003-08-08). "Bots &; Botnet: An Overview" (http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299) (PDF). SANS Institute. Retrieved 12 November 2013.
4. Danchev, Dancho (11 October 2013). "Novice cyberciminals offer commercial access to five mini botnets" (http://www.webroot.com/blog/2013/10/11/novice-cyberciminals-offer-commercial-access-5-mini-botnets/). Retrieved 28 June 2015.
5. Schiller, Craig A.; Binkley, Jim; Harley, David; Evron, Gadi; Bradley, Tony; Willems, Carsten; Cross, Michael (2007-01-01). *Botnets* (http://www.sciencedirect.com/science/article/pii/B9781597491358500044). Burlington: Syngress. pp. 29–75. ISBN 9781597491358.

6. Heron, Simon (2007-04-01). "Botnet command and control techniques" (http://www.sciencedirect.com/science/article/pii/S1353485807700454). *Network Security*. **2007** (4): 13–16. doi:10.1016/S1353-4858(07)70045-4 (https://doi.org/10.1016%2FS1353-4858%2807%2970045-4).
7. Wang, Ping et al. (2010). "Peer-to-peer botnets". In Stamp, Mark & Stavroulakis, Peter. *Handbook of Information and Communication Security* (https://books.google.com/books?id=I-9P1EkTkigC&pg=PA335). Springer. ISBN 9783642041174.
8. C.Y. Cho, D. Babic, R. Shin, and D. Song. Inference and Analysis of Formal Models of Botnet Command and Control Protocols (http://www.domagoj-babic.com/index.php/Pubs/CCS10botnets), 2010 ACM Conference on Computer and Communications Security.
9. Teresa Dixon Murray. "Banks can't prevent cyber attacks like those hitting PNC, Key, U.S. Bank this week" (http://www.cleveland.com/business/index.ssf/2012/09/banks_cant_prevent_cyber_attac.html). Cleveland.com. Retrieved 2 September 2014.
10. Arntz, Pieter (30 March 2016). "The Facts about Botnets" (https://blog.malwarebytes.com/cybercrime/2015/02/the-facts-about-botnets/). Retrieved 27 May 2017.
11. Schiller, Craig A.; Binkley, Jim; Harley, David; Evron, Gadi; Bradley, Tony; Willems, Carsten; Cross, Michael (2007-01-01). *Botnets* (http://www.sciencedirect.com/science/article/pii/B9781597491358500056). Burlington: Syngress. pp. 77–95. ISBN 978-159749135-8.
12. Zeltser, Lenny. "When Bots Use Social Media for Command and Control" (https://zeltser.com/bots-command-and-control-via-social-media/).
13. Osborne, Charlie. "Hammertoss: Russian hackers target the cloud, Twitter, GitHub in malware spread" (http://www.zdnet.com/article/hammertoss-russian-hackers-target-the-cloud-twitter-github-in-malware-spread/). *ZDNet*. Retrieved 7 October 2017.
14. Singel, Ryan (13 August 2009). "Hackers Use Twitter to Control Botnet" (https://www.wired.com/2009/08/botnet-tweets/). Retrieved 27 May 2017.
15. "First Twitter-controlled Android botnet discovered" (https://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/). 24 August 2016. Retrieved 27 May 2017.
16. Gallagher, Sean (3 October 2014). "Reddit-powered botnet infected thousands of Macs worldwide" (https://arstechnica.com/security/2014/10/reddit-powered-botnet-infected-thousands-of-macs-worldwide/). Retrieved 27 May 2017.
17. Cimpanu, Catalin (6 June 2017). "Russian State Hackers Use Britney Spears Instagram Posts to Control Malware" (https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-britney-spears-instagram-posts-to-control-malware/). Retrieved 8 June 2017.
18. Dorais-Joncas, Alexis (30 January 2013). "Walking through Win32/Jabberbot.A instant messaging C&C" (https://www.welivesecurity.com/2013/01/30/walking-through-win32jabberbot-a-instant-messaging-cc/). Retrieved 27 May 2017.
19. Constantin, Lucian (25 July 2013). "Cybercriminals are using the Tor network to control their botnets" (http://www.pcworld.com/article/2045183/cybercriminals-increasingly-use-the-tor-network-to-control-their-botnets-researchers-say.html). Retrieved 27 May 2017.
20. "Cisco ASA Botnet Traffic Filter Guide" (https://www.cisco.com/c/en/us/td/docs/security/asa/special/botnet/guide/asa-botnet.html). Retrieved 27 May 2017.
21. Attack of the Bots (http://archive.wired.com/wired/archive/14.11/botnet.html) at *Wired*
22. Norton, Quinn (2012-01-01). "Anonymous 101 Part Deux: Morals Triumph Over Lulz" (https://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux/3/). Wired.com. Retrieved 2013-11-22.
23. Peterson, Andrea (April 10, 2015). "China deploys new weapon for online censorship in form of 'Great Cannon'" (https://www.washingtonpost.com/blogs/the-switch/wp/2015/04/10/china-escalates-censorship-efforts-with-debut-of-offensive-cyber-weapon-researchers-say/). The Washington Post. Retrieved April 10, 2015.
24. "Operation Aurora — The Command Structure" (https://web.archive.org/web/20100611140112/http://www.damballa.com/research/aurora/). Damballa.com. Archived from the original (http://www.damballa.com/research/aurora/) on 11 June 2010. Retrieved 30 July 2010.
25. Edwards, Jim (27 November 2013). "This Is What It Looks Like When A Click-Fraud Botnet Secretly Controls Your Web Browser" (http://uk.businessinsider.com/this-is-what-it-looks-like-when-a-click-fraud-botnet-secretly-controls-your-web-browser-2013-11). Retrieved 27 May 2017.

26. Nichols, Shaun (24 June 2014). "Got a botnet? Thinking of using it to mine Bitcoin? Don't bother" (https://www.theregister.co.uk/2014/06/24/bad_news_malware_infections_are_mining_bitcoin_good_news_theyre_not_making_any_money/). Retrieved 27 May 2017.
27. "Bitcoin Mining" (https://www.bitcoinmining.com/). BitcoinMining.com. Archived (https://www.bitcoinmining.com) from the original on 30 April 2016. Retrieved 30 April 2016.
28. "Trojan horse, and Virus FAQ" (http://www.dslreports.com/faq/trojans/1.0_Trojan_horses). DSLReports. Retrieved 7 April 2011.
29. Many-to-Many Botnet Relationships (https://www.damballa.com/downloads/d_pubs/WP%20Many-to-Many%20Botnet%20Relationships%20%282009-05-21%29.pdf), *Damballa*, 8 June 2009.
30. "Detecting and Dismantling Botnet Command and Control Infrastructure using Behavioral Profilers and Bot Informants" (http://wwweb.eecs.umich.edu/fjgroup/botnets/).
31. "DISCLOSURE: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis" (https://www.cs.ucsb.edu/~chris/research/doc/acsac12_disclosure.pdf) (PDF). *Annual Computer Security Applications Conference*. ACM. Dec 2012.
32. *BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic*. Proceedings of the 15th Annual Network and Distributed System Security Symposium. 2008. CiteSeerX 10.1.1.110.8092 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.8092).
33. "Researchers Boot Million Linux Kernels to Help Botnet Research" (http://www.eweek.com/c/a/Security/Researchers-Boot-Million-Linux-Kernels-to-Help-Botnet-Research-550216/?kc=EWKNLLIN08182009STR2). IT Security & Network Security News. 2009-08-12. Retrieved 23 April 2011.
34. "Brute-Force Botnet Attacks Now Elude Volumetric Detection" (https://www.darkreading.com/endpoint/brute-force-botnet-attacks-now-elude-volumetric-detection/a/d-id/1327742). DARKReading from Information Week. 2016-12-19. Retrieved 14 November 2017.
35. United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Crime and Terrorism (2018). *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing before the Subcommittee on Crime and Terrorism of the Committee on the Judiciary, United States Senate, One Hundred Thirteenth Congress, Second Session, July 15, 2014* (https://purl.fdlp.gov/GPO/gpo110983). Washington, DC: U.S. Government Publishing Office. Retrieved 18 November 2018.
36. Credeur, Mary. "Atlanta Business Chronicle, Staff Writer" (http://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html?page=all). bizjournals.com. Retrieved 22 July 2002.
37. Mary Jane Credeur (22 July 2002). "EarthLink wins $25 million lawsuit against junk e-mailer" (https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html). Retrieved 10 December 2018.
38. "Hackers Strengthen Malicious Botnets by Shrinking Them" (http://www.computer.org/csdl/mags/co/2006/04/r4017.pdf) (PDF). *Computer; News Briefs*. IEEE Computer Society. April 2006. doi:10.1109/MC.2006.136 (https://doi.org/10.1109%2FMC.2006.136). Retrieved 12 November 2013. "The size of bot networks peaked in mid-2004, with many using more than 100,000 infected machines, according to Mark Sunner, chief technology officer at MessageLabs.The average botnet size is now about 20,000 computers, he said."
39. "Symantec.cloud | Email Security, Web Security, Endpoint Protection, Archiving, Continuity, Instant Messaging Security" (http://www.messagelabs.com/mlireport/MLI_2010_04_Apr_FINAL_EN.pdf) (PDF). Messagelabs.com. Retrieved 2014-01-30.
40. Chuck Miller (2009-05-05). "Researchers hijack control of Torpig botnet" (http://www.scmagazine.com/researchers-hijack-control-of-torpig-botnet/article/136207/). SC Magazine US. Retrieved 10 November 2011.
41. "Storm Worm network shrinks to about one-tenth of its former size" (https://web.archive.org/web/20071224115139/http://tech.blorge.com/Structure:%20/2007/10/21/2483/). Tech.Blorge.Com. 21 October 2007. Archived from the original (http://tech.blorge.com/Structure:%20/2007/10/21/2483/) on 24 December 2007. Retrieved 30 July 2010.
42. Chuck Miller (2008-07-25). "The Rustock botnet spams again" (http://www.scmagazine.com/the-rustock-botnet-spams-again/article/112940/). SC Magazine US. Retrieved 30 July 2010.
43. Stewart, Joe. "Spam Botnets to Watch in 2009" (https://www.secureworks.com/research/botnets2009). *Secureworks.com*. SecureWorks. Retrieved 9 March 2016.
44. "Pushdo Botnet — New DDOS attacks on major web sites — Harry Waldron — IT Security" (https://web.archive.org/web/20100816044216/http://msmvps.com/blogs/harrywaldron/archive/2010/02/02/pushdo-botnet-new-ddos-attacks-on-major-web-sites.aspx). Msmvps.com. 2 February 2010. Archived from the original (http://msmvps.com/blogs/harrywaldron/archive/2010/02/02/pushdo-botnet-new-ddos-attacks-on-major-web-sites.aspx) on 16 August 2010. Retrieved 30 July 2010.

45. "New Zealand teenager accused of controlling botnet of 1.3 million computers" (http://www.h-online.com/security/news/item/New-Zealand-teenager-accused-of-controlling-botnet-of-1-3-million-computers-734068.html). The H security. 2007-11-30. Retrieved 12 November 2011.
46. "Technology | Spam on rise after brief reprieve" (http://news.bbc.co.uk/2/hi/technology/7749835.stm). BBC News. 2008-11-26. Retrieved 24 April 2010.
47. "Sality: Story of a Peer-to-Peer Viral Network" (http://www.symantec.com/connect/sites/default/files/sality_peer_to_peer_viral_network.pdf) (PDF). Symantec. 2011-08-03. Retrieved 12 January 2012.
48. "How FBI, police busted massive botnet" (https://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/). theregister.co.uk. Retrieved 3 March 2010.
49. "Calculating the Size of the Downadup Outbreak — F-Secure Weblog : News from the Lab" (http://www.f-secure.com/weblog/archives/00001584.html). F-secure.com. 2009-01-16. Retrieved 24 April 2010.
50. "Waledac botnet 'decimated' by MS takedown" (https://www.theregister.co.uk/2010/03/16/waledac_takedown_success/). The Register. 2010-03-16. Retrieved 23 April 2011.
51. Gregg Keizer (2008-04-09). "Top botnets control 1M hijacked computers" (http://www.computerworld.com/s/article/9076278/Top_botnets_control_1M_hijacked_computers). Computerworld. Retrieved 23 April 2011.
52. "Botnet sics zombie soldiers on gimpy websites" (https://www.theregister.co.uk/2008/05/14/asprox_attacks_websites/). The Register. 2008-05-14. Retrieved 23 April 2011.
53. "Infosecurity (UK) - BredoLab downed botnet linked with Spamit.com" (https://web.archive.org/web/20110511115226/http://www2.canada.com/topics/technology/story.html?id=3333655). .canada.com. Archived from the original (http://www2.canada.com/topics/technology/story.html?id=3333655) on 11 May 2011. Retrieved 10 November 2011.
54. "Research: Small DIY botnets prevalent in enterprise networks" (http://www.zdnet.com/blog/security/research-small-diy-botnets-prevalent-in-enterprise-networks/4485). ZDNet. Retrieved 30 July 2010.
55. Warner, Gary (2010-12-02). "Oleg Nikolaenko, Mega-D Botmaster to Stand Trial" (http://garwarner.blogspot.com/2010/12/oleg-nikolaenko-mega-d-botmaster-to.html). CyberCrime & Doing Time. Retrieved 6 December 2010.
56. "New Massive Botnet Twice the Size of Storm — Security/Perimeter" (http://www.darkreading.com/attacks-breaches/new-massive-botnet-twice-the-size-of-storm/d/d-id/1129410?). DarkReading. Retrieved 30 July 2010.
57. Kirk, Jeremy (Aug 16, 2012). "Spamhaus Declares Grum Botnet Dead, but Festi Surges" (http://www.pcworld.com/article/260984/spamhaus_declares_grum_botnet_dead_but_festi_surges.html). *PC World*.
58. "Cómo detectar y borrar el rootkit TDL4 (TDSS/Alureon)" (http://infoaleph.wordpress.com/2011/07/03/como-detectar-y-borrar-el-rootkit-tdl4-tdssalureon/). kasperskytienda.es. 2011-07-03. Retrieved 11 July 2011.
59. "America's 10 most wanted botnets" (http://www.networkworld.com/article/2260410/network-security/america-s-10-most-wanted-botnets.html). Networkworld.com. 2009-07-22. Retrieved 10 November 2011.
60. "EU police operation takes down malicious computer network" (http://phys.org/news/2015-02-eu-police-malicious-network.html).
61. "Discovered: Botnet Costing Display Advertisers over Six Million Dollars per Month" (http://www.spider.io/blog/2013/03/chameleon-botnet/). Spider.io. 2013-03-19. Retrieved 21 March 2013.
62. Espiner, Tom (2011-03-08). "Botnet size may be exaggerated, says Enisa | Security Threats | ZDNet UK" (http://www.zdnet.com/botnet-size-may-be-exaggerated-says-enisa-3040092062/). Zdnet.com. Retrieved 10 November 2011.

External links

- The Honeynet Project & Research Alliance (http://www.honeynet.org/papers/bots/) – "Know your Enemy: Tracking Botnets"
- The Shadowserver Foundation (http://www.shadowserver.org/) – an all-volunteer security watchdog group that gathers, tracks, and reports on malware, botnet activity, and electronic fraud
- EWeek.com – "Is the Botnet Battle Already Lost?" (http://www.eweek.com/c/a/Security/Is-the-Botnet-Battle-Already-Lost/)
- Botnet Bust – "SpyEye Malware Mastermind Pleads Guilty" (https://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty), FBI
