Botnets – A tenacious Web Technology

Eva Aussems
Media Technology, Leiden
e.awesomes@gmail.com

Beryl Noë
Media Technology, Leiden
beryl.noe@gmail.com

Natalia Rios Rivera
Media Technology, Leiden
natalia.rios.rivera@gmail.com

ABSTRACT

Rather than talking about *a* web technology, we should perhaps use the term in plural, web technolog*ies*, when we are talking about botnets. They come with a great variety of structures, functionalities and purposes. Botnets have undergone a truly impressive development since they first were created, being mere automatic chat cleaners. In this report, we will attempt at giving the reader a conscise analysis of the technology, starting by a short history, an overview of the different types of botnets and insights into the operating principles. We will further discuss typical and suprising applications and give a step by step introductionally explanation of how one can set up a botnet. Finally, we will finish with concluding remarks on what we have all come to know about this technology.

1. PURPOSE, CONTEXT AND HISTORY

1.1. What is a botnet?

Etymologically, one could explain a botnet as being a *net*work of ro*bots*. It is a collection of (possibly compromised) computers that are connected to each other and are remotely controlled by a botmaster in order to perform certain tasks. Each of these computers can be called a bot or a zombie, a botnet may thus also be known as a zombie army. As botnets are mostly used for malicious intentions, the term botnet is thus usually employed in the context of malware. [1][2]

1.2. Purposes

1.2.1. Legal purposes

Even though botnets are usually thought of carrying on illegal tasks, some don't. There are some examples of IRC (Internet Relay Chat) bots that keep IRC channels clean from unwanted users. It is these botnets that were eventually exploited by hackers and used to the malware we now speak of more often.

1.2.2. Illegal purposes

Nowadays, botnets are used for all king of malicious purposes. Some of these are listed below:

-Spam

-Phishing

-Theft of confidential data

-Keystroke logging

-DDoS (Distributed Denial of Service) attacks

-Clickfraud. [3][4][5]

1.3. History

- Late 1980s: IRC botnets are created.
- 1991: Sub7, a Trojan, and Pretty park, a worm, first emerge in 1991 and are both seen as the malware that started the rise of the malicious botnets.
- 2000: Global Threat bot (Gtbot), a mIRC-based bot surfaces.
- 2002: SDBot and Agobot. SDBot was commercialized and its source code became thus broadly available providing an excellent base for the development of further botnets. Agobot introduced a new concept of attacks with several stages. The first would install a back door, the second disable the antivirus software, and the third would prevent the access to websites of security vendors.
- 2003: Spybot introduces new functionalities such as: keylogging, data mining, instant messaging spam and Rbot comes up with the DDoS functionality and brings out the SOCKS proxy. Rbot type botnets also make use for the first time of compression and encryption algorithms to evade detection from antiviruses.
- 2004: Polybot introduces polymorphism: changing appearance as often as possible to evade detection. Bagle and Bobax are the first spamming botnets.
- 2006: ZeuS begins with information stealing. This botnet has been commercialized at very high prices and has become the mostly used information stealing criminal tool.
- 2007: The FBI starts its operation “Bot Roast” to

disassemble bot herders.

- 2008: Many botnets were more or less successfully taken down. The take-down of botnet McColo in November lead to the immediate decrease of spam for almost 80%. However, three months later, the spamrate was back to its formal level.
- 2010: TDL-4, one of the most successfull botnets, infected over 4.5 million computers in the first 3 months of 2011 and it keeps growing. [6][7]

These were all but a few first steps, the number of botnets keeps increasing while governments, security companies and researchers keep trying to counter them.

Mid January, the Security Company Trend Micro unveiled a global botnet map that shows active C&C servers and bots across the world. On the 25th of June 2014 it shows 6.557 C&C servers and 5.985.409 botnet connections that have been active in the past 14 days. [8][9]

2. OPERATING PRINCIPLES

2.1. Architecture

Essentially, there are two types of botnet architecture: centralized or decentralized botnets.

2.1.1. Centralized botnets

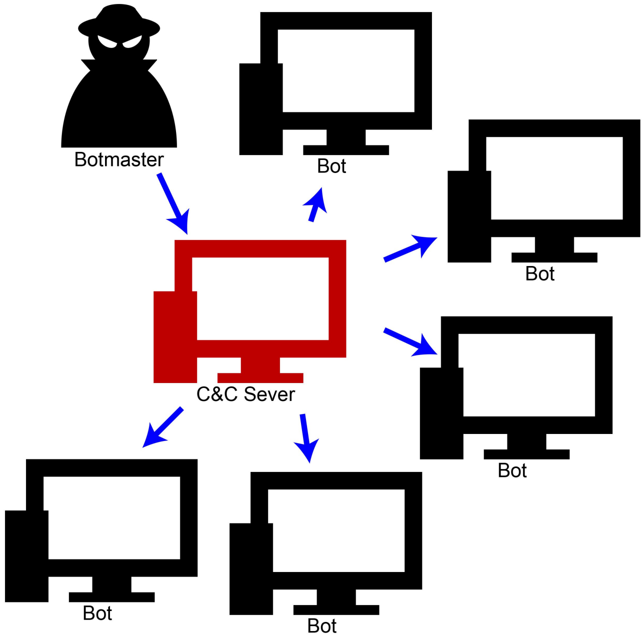


Figure 1. Centralized botnet topology

All bots are are connected to a single command and control center (C&C) that is managed by the botnet owner. They are far more common than decentralized botnets since this structure is the oldest and they are faster and easier to manage. However, they are also easier to destroy since the entire network is neutralized if the C&C server is put out of order. [3]

Two types of centralized exist: The most common one is based on the IRC protocol [10], the second, less prevailing, is a HTTP botnet [11]. The latter type is the newest structure development. It works by exchanging web requests using port 80 and sets up its communication with certain URLs using internet with HTTP messages, which contain unique identifiers for the bots. The server will reply to these HTTP messages with further investigation commands (e.g. GET). Interrogating command becomes the reason of downloading the infecting malicious commands. Contrary to the IRC botnet, the C&C of a HTTP botnet is web-based. And since it is a web server, it can continuously connect with the server. This feature lead to a regular traffic of the HTTP botnet. However, the bot packets are different from normal packets, which makes their detection procedure easy.

2.1.2. Decentralized botnets

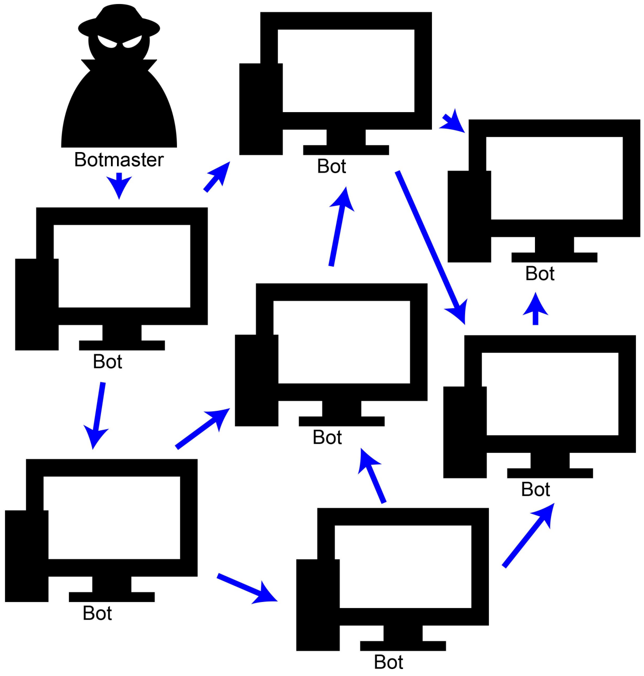


Figure 2. Decentralized botnet topology

All bots are are connected to several other bots in the network. The commands, rather than coming from a control center, are transferred from bot to bot. Each bot has a list of neighbours from which he receives and forwards commands. The creator of the botnet only needs access to one infected computer of the network to control the entire botnet.

Building and controlling such a network is much more difficult than for a centralized botnet, but dismantling such a decentralized network is in return much more difficult as well. [3]

The only known type of decentralized botnets are P2P (peer-to-peer) botnets. [12]

2.2. Operating principle of a typical (centralized) botnet

2.2.1. Step 1. The attacker infects a victim computer.

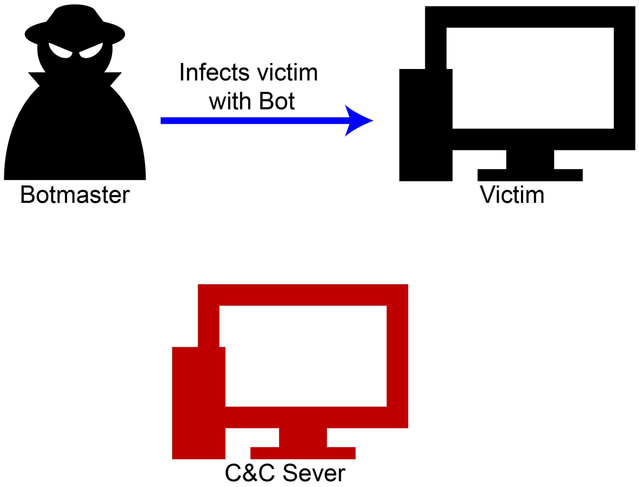


Figure 3. Step 1

For this, three main methods exist: drive-by downloads, email and active scanning.

In the case of drive-by downloads, the attacker can for example load his malicious code on a popular website with an exploitable vulnerability. The code typically redirects the user's browser to a site controlled by the attacker where the user's computer will download the bot code without the user even noticing.

In the case of an email infection, the attacker sends out massive amounts of spam with the bot code included it in in the form of a Word document, pdf or a link to a site as in the previous method. Once the code is downloaded, the computer has become a bot.

The scanning method however is seen as the most successful recruiting mechanism. Two types of scanning exist: (I) worm-like botnets that continuously scan certain ports following a specific target selection algorithm and (II) botnets with variable scanning behaviour.

A bot that has been infected by the first, worm-like, method will in his turn start scanning the IP space immediately in search for further victims. This ensures a fast growth of the population of infected computers, and can result in very large botnets.

The second type of botnets are the most common nowadays and they are much more difficult to track due to their intermittent and continuously changing behaviour. This flexibility is obtained by changing certain parameters: the target vulnerability, the scanning rate, the number of threads to use, the number of packets to send, and the duration of scanning. The thus created variability is what makes it harder for them to be tracked. [13]

Local networks can be scanned for unsecured computers or network services can be exploited to infiltrate computers. [2][14]

2.2.2. Step 2. The bot logs into the C&C server.

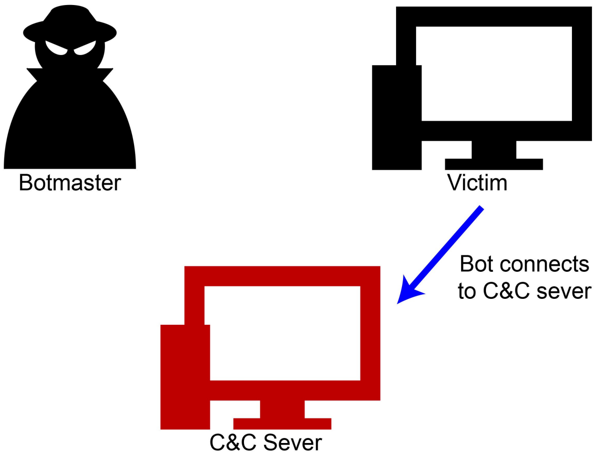


Figure 4. Step 2

2.2.3. Step 3. The attacker sends commands through the C&C server to the bot.

This is a very important aspect of the whole botnet since botmasters need to rapidly send out instructions but also do not want that communication to be detected.

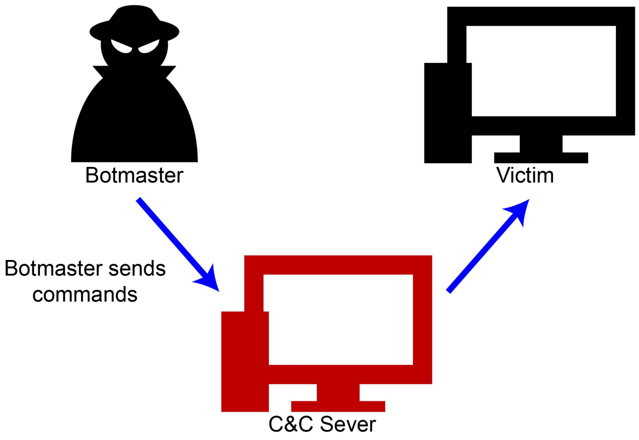


Figure 5. Step 3

We can discern three types of communication methods: centralized (I), decentralized (II) and unstructured (III). The characteristics of centralized and decentralized communication is intuitively very comparable to the botnet architecture bearing the same names.

Messages sent in a centralized system (I) are faster since the path the message travels is shorter, but are easier to expose since the activity is focussed around one point and this central point is precisely important and should preferably stay undetectable (in the botmaster's perspective, that is).

Messages sent in a decentralized system (II) are much harder to track but the delivery of these messages may fail and will typically be slower.

In the extreme scenario of an unstructured system (III), the communication is even more complex than in the previously mentioned method. In the decentralized system, the bots would have a list of neighbours to communicate with. Here, bots randomly scan the internet for other bots, and only if it finds one will pass on the message. Naturally, the chances of getting the message delivered to all bots is much lower and the whole process also takes much longer. However, it is much more secure against detection. [11]

The communication between bots among each other or with a C&C server is usually done using convert channels which can be HTTP, IRC and other protocols but also, and more recently, JPG images, Word files and LinkedIn statuses. The communication is usually encrypted for stealth and protection against the detection of the botnet. [15]

2.2.4. Step 4. Repeat.

Before long, the attacker will have a whole army of bots under his control. [16]

They are then used for different purposes, some of which are listed under the section 1.2.

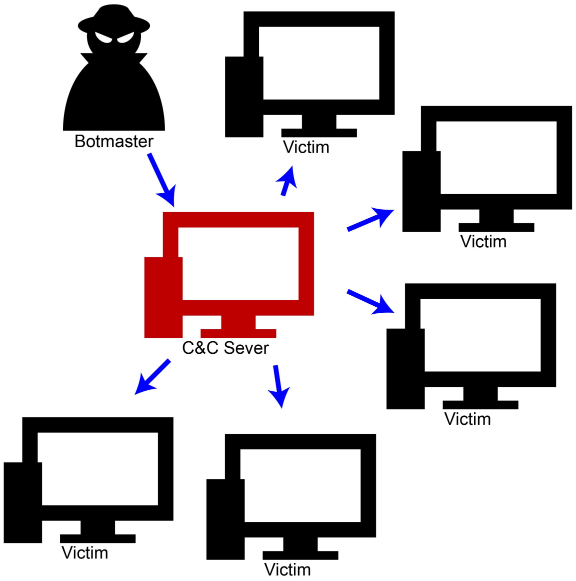


Figure 6. Step 4

3. STRENGTHS AND WEAKNESSES

Since there is such a big variety of botnets and their workings can be very different, one should not forget that beyond seeing strengths and weaknesses of the whole botnet concept, the advatanges and disadvantages of all different types should be considered too. Since a lot of more or less advantageous features have been discussed in the section 2. Operating principles, they will only be mentionned briefly here.

- The internet provides the botnets with one of its greatest strengths. The internet has no real central governing body. This means it is a wide-open environment that allows multiple forms of crime. This leads to a rapid growth in botnets since it is nowadays even common to see do-it-yourself botnet construction kits. These are extensively advertised and sold on the market.

  In fact the growth of botnets has been so rapid that around one quarter of all worldwide computers now may be participating in a botnet. [17]

- The above mentioned strength may at the same time be its greatest weakness. International political consensus imposing traffic inspection would make it possible to track and take down botnets. However, it does not exist yet and citizens may interpret it as an infringement of their rights. Besides this, a global disinfection may not be allowed unanimously by all countries since it would rise political questions. In other words, most countries would not agree on another country's forces remotely running software on their systems to detect botnet traffic. [18]

- Another major strength of botnets is that they not only represent a simple irritating computer infection for some people but they have become a very important weapon in cyberwarfare. In these wars, politically motivated hackers conduct sabotage and espionage on an international level and botnets play without doubt a part in these battles. [18]
- And finally, as mentioned previously, botnets' topology disclose that the IRC C&C centralized structure's weakness is a single-point-of-failure problem. Once it is detected, it will be relatively easy to dismantle. On the other hand, decentralized botnets like the P2P botnets are harder to disrupt as detection does not endanger the entire network of bots. [19]

4. TYPICAL APPLICATIONS

Botnets typically carry malicious software that infiltrate computers to obtain sensitive information (eg. codes to enter bank accounts). However botnets are not only used to extract sensitive information from the infected computers, they are also used to take over control of the entire machine and direct their behaviour.

It can for example, direct its bots to flood a certain targets with packets which creates an overload of requests and will cause a server or network crash. This particular application is called a DDoS (Distributed Denial of Service) attack. This attack may be done out of personal or political reasons, but the responsible botmaster may also use the attack to blackmail the owner of the server for money in return for 'releasing' the server of its overload.

However targets of attackers can vary from servers to somebody's personal phone. In other words, the range of people and instances that can be targeted is excessively wide, as can be the scale of the attack.

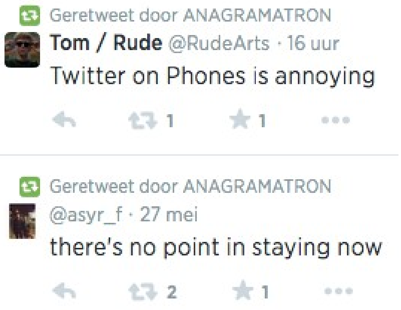
Another nowadays typical application of botnets, is when they are used to track the criminal botnets down. Honeybot is an example of one of those botnets that work in reverse: it uses vulnerable computers as ace when a criminal botnet bites and infects the computer. It traces back the network of infected computers. [20]

5. SURPRISING APPLICATIONS

Rather than being surprising by the way it is used, the first example highlights the surprising user of botnets. The NSA's department of TAO (Tailord Access Operation) revealed by Edward Snowden, made a botnet which infiltrated millions of computers to convey data from the Internet and phone network, monitoring millions of devices and illegally gathering private information from all over the world. With spam emails laced with malware the NSA admittedly were able to record audio, take snapshots with a webcam, download files from the hard drive with the help of fake facebook pages. In 2004, the NSA had only 100 to 150 infiltrated computers. In the meantime, this number has grown exponentially: ten years later millions more have been infected. [21]

Information theft is a known application of botnets, but the scale and the origin of the infection is truly astonishing.

The Carna Botnet is another example of a surprising application. It has been made by an anonymous hacker who called his work "The Internet Sensus 2012". He made a botnet that did not do any harm to the device it had infiltrated, but only registered that the device was there. Using this botnet, he mapped the usage of the internet and published an article online explaining that it was used for a good purpose. Discussions naturally follow, arguing whether one is allowed to use this information, since it has been gathered illegally. [22][23]



Geretweet door ANAGRAMATRON
Tom / Rude @RudeArts · 16 uur
Twitter on Phones is annoying

Geretweet door ANAGRAMATRON
@asyr_f · 27 mei
there's no point in staying now

Picture 1. Anagramatron tweets

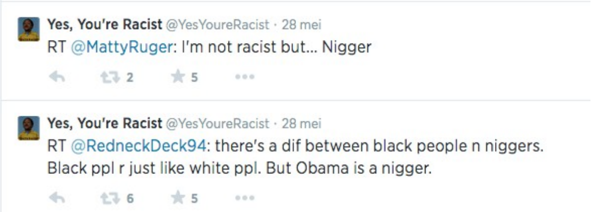
One of these surprising twitter bots is for example Anagramaton [24] created by Colin R. [25] The twitter bot pairs up tweets that are composed by the exact same letters. It gives combinations of the same characters which give a different meaning.

Twitter has quite some well-known bots that actively pursue more followers. Most twitter bots can be attributed to doubtful companies or individuals with low self esteem who would like to bump up the number of their followers. This is not really a surprising application, what is surprising however is that botnets are also used for poetic and/or creative twitter tweets.

There is also BDZNappa [26]; this twitterbot reacts to anybody that tweets nine thousand with the tweet: "WHAT?! NINE THOUSAND?!" The creator, Daniel Lo

Nigro, made his twitterbot to show how a simple “search and reply” twitter bot could work [27].

@Yesyoureracist [28] is a botnet created by Logan James Smiths. The Twitter bot grabs all the posts tagged with #notaracist and retweets the posts with @yesyoureracist in front of it. Most of the times, it displays people's comments that claim that they are not racist but actually prove the contrary.



Yes, You're Racist @YesYoureRacist · 28 mei
RT @MattyRuger: I'm not racist but... Nigger
2 5

Yes, You're Racist @YesYoureRacist · 28 mei
RT @RedneckDeck94: there's a dif between black people n niggers. Black ppl r just like white ppl. But Obama is a nigger.
6 5

Picture 2. YesYoureRacist tweets

Another surprising use of a botnet with Twitter as the medium is the usage of twitter as a command & control page [29]. In this situation, infected computers follow the twitter feed of the command and control through its RSS feed.

6. GETTING STARTED

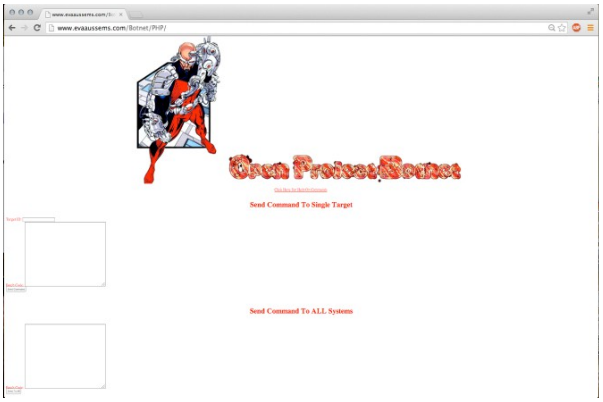
6.1. Setting up an IRC botnet

This section will provide brief instruction on how to create a custom IRC Botnet. The botnet is open source and can be downloaded from hackforums.net. There is no need for prior programming language knowledge to set up this botnet but basic programming skills are nonetheless recommended.

The Botnet can be easily setup from a windows operating system but it is recommended to install a virtual windows enviroment to keep any harmful side effects away from your operating system. To setup the botnet, PHP is embedded in a regular HTML document and the botnet runs on top of that.

Once you have your virtual windows environments, you will need to download the file that contains the open source botnet which is available in the web page kiwi6.com/file/ursvs1t5ef. The downloaded folder should contain two more folders: the PHP folder and the Botnet folder.

Then, create a basic HTML file and save the document into the Botnet folder, so everything is at the same place. Then open the delete.php file and copy the code into the html file. Do this with all the PHP files. To check if it works drag the HTML file into a web server which enables the visualization of the web page. Upload the contents of the PHP folder to a web hosting server with php installed. The web server must also allow php to create files and directories.


www.evaaussems.com/Botnet/PHP/
Send Command To Single Target
Send Command To ALL Systems

Picture 3. C&C webpage

Next, you have to upload the php files to the webserver account, open the Botnet folder then the autoplay folder and then open the last folder Docs (Botnet/Botnet/Autoplay/Docs). Then, when you are in the Docs file open the Host.txt with text editor and copy-paste the URL of the site where the php files are uploaded and save (eg. http://www.examplesite.com/).

Once the Host.txt file has been changed, zip the Botnet folder. For this you will need to open the zip2exe file so it is possible to zip the Botnet folder with the custom Host.txt into a single .exe file, which will be in the main folder. Make sure zip2exe zips the new Botnet folder and select to auto run the winsvc.exe file which is also in the main bot file. Finally, give the file a name in the output EXE and press create.

Now you have created an .exe file to implement on a computer. This computer will turn into a bot you can control from your C&C webpage once the connection between these two has been established. [30]

6.2. Setting up a Python Twitter Tool

Botnets come in many variations, as has been previously pointed out. In this section, we will explain how the Python Twitter Tool (PTT) [31] works. This application has been chosen since it has creative and surprising outcomes like for instance the already mentioned Anagramatron.

PTT can be seen as an application that gives users a framework to handle Twitter streams in the Python programing language [32]. It not only enables users to handle twitter streams but also gives users the chance to write their own programs using this application. PTT makes use of an IRC botnet to perform automated tasks.

The PTT application consists of:

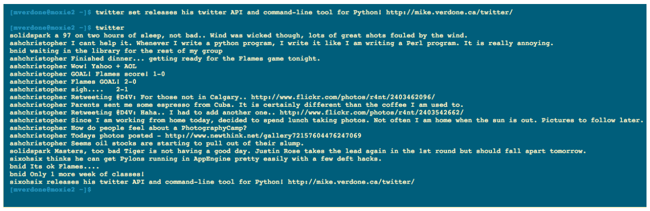
- a Twitter command line tool,
- an IRC bot,
- a Twitter log,
- a Twitter archive, and a Twitter follower.

Following steps need to be taken to set up such a Python Twitter Tool and its bot.

•

6.2.1. The Twitter command line tool

The Twitter command line tool enables users to view: tweets and recent replies. Futhermore, the user can tweet, chose to follow or unfollow friends and view public timelines. It also allows the user to chose between various output formats for tweet information. Thus, it basically has the same functions as Twitter, the only significant difference is the interface.



```
[mverdone@moxie2 ~]$ twitter set releases his twitter API and command-line tool for Python! http://mike.verdone.ca/twitter/

[mverdone@moxie2 ~]$ twitter
solidspark a 97 on two hours of sleep, not bad.. Wind was wicked though, lots of great shots fouled by the wind.
ashchristopher I cant help it. Whenever I write a python program, I write it like I am writing a Perl program. It is really annoying.
bnid waiting in the library for the rest of my group
ashchristopher Finished dinner... getting ready for the Flames game tonight.
ashchristopher Wow! Yahoo + AOL
ashchristopher GOAL! Flames score! 1-0
ashchristopher Flames GOAL! 2-0
ashchristopher sigh....   2-1
ashchristopher Retweeting @D4V: For those not in Calgary.. http://www.flickr.com/photos/r4nt/2403462096/
ashchristopher Parents sent me some espresso from Cuba. It is certainly different than the coffee I am used to.
ashchristopher Retweeting @D4V: Haha.. I had to add another one.. http://www.flickr.com/photos/r4nt/2403542662/
ashchristopher Since I am working from home today, decided to spend lunch taking photos. Not often I am home when the sun is out. Pictures to follow later.
ashchristopher How do people feel about a PhotographyCamp?
ashchristopher Todays photos posted - http://www.newthink.net/gallery72157604476247069
ashchristopher Seems oil stocks are starting to pull out of their slump.
solidspark Masters, too bad Tiger is not having a good day. Justin Rose takes the lead again in the 1st round but should fall apart tomorrow.
sixohsix thinks he can get Pylons running in AppEngine pretty easily with a few deft hacks.
bnid Its ok Flames....
bnid Only 1 more week of classes!
sixohsix releases his twitter API and command-line tool for Python! http://mike.verdone.ca/twitter/
[mverdone@moxie2 ~]$
```

Figure 7. Twitter command line tool

6.2.2. The IRC bot

The IRC bot should always stay connected to a twitter account, which has to be one accessible to the user. The IRC bot announces all tweets from friends it is following. It can be told to (un)follow friends through IRC message commands.

6.2.3. The Twitter log

The Twitter log is a command-line tool that collects all the tweets from a given user and stores it in a text format. It can be seen as a backup of all tweets.

6.2.4. The Twitter archive and the Twitter follower

The twitter archive and the Twitter follower will log all the tweets posted by any user connected to your account since they started posting. The Twitter follower will make a list of all the followers of a user (or all the users that the user follows).

To get the Python Twitter Tools running, one must first download the programming language Python 2.6 or newer [32]. Second, Python should have setup_tools installed, if that is not the case, they can be easily installed by following the steps given by the Python Enterprise Application Kit [33]. Finally, when the program has been installed it is possible to type –h twitter or twitterbot to learn more about the command-line tool.

To use the IRC bot, the Python IRC library needs to be downloaded [34] (it can be downloaded from the link provided by reference [35]). To install the IRC library in Python one must run “python setup.py install” (from the source distribution).

After these steps, PTT should be correctly installed. To create a new application, you can find more information on via the reference [36]. Otherwise, you can take somebody else’s code and see what surprising things can be done with it.

7. FINAL THOUGHTS

Working on this subject, we have come to realize how big of a threat botnets can be. And it's frightening how easily one can put his hands on such a powerful tool. As they are growing in number, they are also getting harder to dismantle. And we have probably only seen a fraction of what is “out there” now since hackers are getting more and more creative in their methods to infiltrate and control victim computers. So, while not all botnets are “bad”, we once more discovered the importance of a good and updated anti-virus security system. So let this be the final lesson of this research on botnets: Beware! Protect your computer well!

REFERENCES

[1] Botnet.
http://www.techopedia.com/definition/384/botnet

[2] What is a Botnet?
http://blog.kaspersky.com/botnet/.

[3] The botnet business.
http://www.securelist.com/en/analysis/204792003/The_botnet_business

[4] Bots and Botnets—A Growing Threat.
https://us.norton.com/botnet/promo

[5] Uses of botnets.
http://honeynet.org/node/52

[6] The History of the Botnet Part I.
http://www.businesscomputingworld.co.uk/the-history-of-the-botnet-part-i/

[7] The botnet threat.
http://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html

[8] Botnets wreak havoc.
http://www.itweb.co.za/index.php?option=com_content&view=article&id=134699:Botnets-wreak-havoc&catid=265

[9] Global Botnet Threat Activity map
http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/

[10] C. Kalt. Internet Relay Chat: Client Protocol. RFC 2812 (Informational), April 2000.

[11] Jing Liu,''Botnet: Classification, Attacks, Detection, Tracing and Preventive Measures", July 2009.

[12] Jaiswal, R., & Bajgude, S. (2013). Botnet Technology. In 3rd International Conference on Emerging Trends in Computer and Image

[13] Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006, October). A multifaceted approach to understanding the botnet phenomenon. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (pp. 41-52). ACM.

[14] Infection & Distribution Methods
https://sites.google.com/site/botnetmalware/impact-of-botnet-on-infrastructure-networks/infection-distribution-methods

[15] Botnet Command and Control via Covert Channels.
http://www.redteamsecure.com/labs/post/28/Botnet-Command-and-Control-via-Covert-Channels

[16] Botnets.
http://www.korelogic.com/Resources/Presentations/botnets_issa.pdf

[17] Daswani, N., & Stoppelman, M. (2007, April). The anatomy of Clickbot. A. InProceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets (pp. 11-11). USENIX Association.

[18] Leder, F., Werner, T., & Martini, P. (2009). Proactive botnet countermeasures–an offensive approach. The Virtual Battlefield: Perspectives on Cyber Warfare,3, 211-225.

[19] Banday, M.T., Qadri, J.A., Shah, N.A. 2009). "Study of Botnets and Their Threats to Internet Security," Sprouts: Working Papers on Information Systems, 9(24).

[20] Know your Enemy: Tracking Botnets.
http://www.honeynet.org/papers/bots

[21] How the NSA Plans to Infect 'Millions' of computers with Malware'.

[22] The Most Detailed, GIF-Based Map Of The Internet Was Made By Hacking 420,000 Computers.
http://www.huffingtonpost.com/2013/03/22/internet-map_n_2926934.html

[23] Mapping the Internet: A Hacker's Secret Internet Census.
http://www.spiegel.de/international/world/hacker-measures-the-internet-illegally-with-carna-botnet-a-890413.html

[24] Anagramatron
https://twitter.com/anagramatron

[25] colin r
https://twitter.com/cmyr

[26] Nappa
https://twitter.com/DBZNappa

[27] Twitter autoreply bot - DBZNappa
http://dan.cx/2011/06/twitter-autoreply-bot-dbznappa

[28] Yes, You're Racist
https://twitter.com/YesYoureRacist

[29] hackers Use Twitter to Control Botnet
http://www.wired.com/2009/08/botnet-tweets/

[30] [Release] Open Project Botnet + source
http://www.hackforums.net/showthread.php?tid=4091369/

[31] Python Twitter Tools
http://mike.verdone.ca/twitter/

[32] Python
https://www.python.org/

[33] Building and Distributing Packages with setuptools
http://peak.telecommunity.com/DevCenter/setuptools

[34] Internet Relay Chat (IRC) protocol client library
http://python-irclib.sourceforge.net/

[35] Internet Relay Chat (IRC) protocol client library
https://bitbucket.org/jaraco/irc

[36] Python Twitter API
https://github.com/sixohsix/twitter/tree/master.