BOTNETS

Understanding and Mitigating Botnets

Name

Date

EXECUTIVE SUMMARY

BOTNET TECHNOLOGY AND ITS HISTORY

Bot code was originally created for purposes of maintaining and automatically administrating Internet Relay Chat (IRC) channels. With time, however, malicious developers figured out that it could be used to hack into other computers and use their networks to hack into others and obtain information for their own malicious uses.

A botnet is a collection of computers whose security has been breached by a third party using capable malware and which are then controlled by the third party (Puri, R., 2003). The word 'botnet' is a compounded word from 'robot' and 'network' which essentially connotes that the victim computers are then used by a third party to do his bidding, often without detection from the owner or owners of the botnet.

The particular concept of botnets first came to light at a time when there was a wave of technological advancement which was in the early 2000s. In a lawsuit by the company Earthlink against techno-innovator Khan C. Smith, the company alleged that the defendant had used malware to make computers in the company botnets and thus use them for the purpose of sending bulk spams to those he targeted (Credeur, 2002). Originally spamming was the main

purpose of this kind of technology but with time other uses (Security Intelligence, 2016) have arisen including:

- Commercial use of the technology by corrupting computers and selling the direct access to them to another person.
- Use of the botnets to obtain information.
- Use of the botnets to send malicious software to other computers which it is connected to.

These are, however, only a fraction of the functions to which botnets are put. Some criminal activity to which the technology is often put include:

- Industrial espionage.
- Extortion.
- Data theft.
- Propagation of illegal internet content.

Devices which are vulnerable to this breach include;

- Computers
- Smartphones
- Devices connected by IoT (Internet of things) network such as vehicles and home appliances which are electronic and share some form of connectivity.

PART A: UNDERSTANDING BOTNETS.

INTRODUCTION.

Terms and references.

Bot herder- the controller of the botnet.

Zombie computer- one or more of the computers which are being controlled by a third party.

Figure 1. ‘Five things you need to know about botnets’ adamlevin.com.

Is my computer vulnerable?

As earlier mentioned, botnets are illicit computer networks built for the benefit of a third party using malicious software.

There are several types of techniques used to build these networks:

1. The client-server model or use of IRC,
2. The peer-to-peer network (P2P),
3. Use of telnets.
4. Use of domains.

Use of IRC.

In the first model, the bot herder (the person controlling the botnet) communicates to the target computers using existing servers such as Internet Relay Chat networks (IRC servers) whereby when a computer accesses the infected IRC Server which is set up by the bot herder, it joins a channel which he controls. The bot herder then sends commands the computer through the server which it executes and sends back message of such execution (Schiller.C., et al., 2007). Through this process, the bot herder is able to control a number of computers which he can then use to create an even larger network although this increases to the risk of detection together with the fact that there is only one central point of command whose trail can be followed leading to exposure. The other defect of the model is the non-exclusivity of the access to the botnet network in that another person who is able to access the channel created by the original bot herder may obtain such control.

Peer-to-peer network.

In the second model known as the peer-to-peer network, what happens is that the bot herder uses preexisting malware in a particular computer. He then looks for computers with the same kind of malware by covertly probing IP addresses. When a computer with similar malware is detected, it is made compatible with the first computer by updating its software if need be and then sends in its list of known bots which is used to further enlarge the network. Cyber criminals often employ this second technique as all the computers in the network become both bots and command hence eliminating the risk of detection occasioned from having a centralized command (Wang, Ping et al., 2010).

Use of telnets.

The third model is a Command and Control protocol for botnets in which the network is created using one main command server which is to host the botnet. An external server is set up which runs a scanning script used to scan for and find the IP addresses of default login computers. The control computer then runs a malicious infection line via 'secure shell' connection connecting directly to the server prompting it to ping back to the control server. The bot herder then uses this connection to send attacks to other computers using the 'Dynamic Drive Overlay' software (DDoS) and enslave them. A known example of this method of creating botnets was in the case of the taking down websites belonging to the corporate websites of Xbox and the Playstation network by the 'Lizard Squad' group of hackers (Schiller.C., et al. 2007).

Use of domains.

One of the earliest constructions of Command and Control technology, the model encompasses use of pre-designed domains or webpage. What the bot herder then does is to design such a webpage and put in it a list of controlling commands. When a potential zombie computer access the webpage it is enslaved and the bot herder assumes control of it together with other computers.

The advantage of this technique is that it is fairly low maintenance with ready access at any point the herder may be while its disadvantage is that it can readily be taken down by government agencies on detection.

There are several other ways which cyber criminals use in the creation of botnets, some evolving by the day. Some of the other ways include:

- Use of open source instant message protocol and
- Use of Tor hidden services (Lucian.C., 2013).

In answer to the question therefore, whether or not one's computer is vulnerable to use as part of a botnet, one would be referred to an informative set of questions which are:

- Does the computer use other external servers?
- Is the computer connected to other computers?
- Does the computer send and receive information?

If the answer to one or more of these questions is yes, then the computer is at a potential risk of being hacked for purposes of forming a botnet and therefore appropriate action needs to be taken to avert such situation.

PART B: MITIGATING BOTNETS.

Figure 2. 'Corporate Fight Against Cybercrime is Working' NASA Federal Credit Union

How to detect botnets.

Botnet activities are detected using a number of systems and software, some of which are DNS block lists, Honey Pot systems and Darknets and Flow Based Analysis.

It is the argument of many a scholar that the war on botnet technology as a cybercrime cannot be fought solely by one organization or institution. A multi-sectored and multipronged is rather desirable. To this effect, there are several courses of actions that have been deemed likely to curb the menace.

1. Development of relevant policies and regulations.

The very first step in combating any crime is establishing a comprehensive legal framework. Laws to deal with botnet technology as a crime need to be established and must address several elements which are anti-spam laws, capacity building among stakeholders, International Corporation and outreach. Limitation of privacy rights in the interest of curbing the crime and lastly, a framework for enforcement of cybercrime and botnet mitigation.

In the first instance, there must be laws in place which specifically outlaw botnet as a cybercrime and lay out the penalties for its commission. In this, such matters as jurisdiction, the evidentiary burden and type of evidence required, must be addressed. An example of legislation which has effectively dealt with cybercrime is the Australian Spam Act of 2003 which, among other nuances, introduces the concept of an "Australian link" which is basically a rubberstamp for any online content which originates from Australia. This has thus made the content easily traceable making it easier to track and apprehend cyber criminals. There exists the ITU Toolkit for Model Cybercrime Legislation which serves to aid any jurisdiction which is looking to put in place effective laws on cybercrime.

Secondly, laws which promote capacity building among stakeholders will serve to consolidate efforts hence make them all the more effective. Such laws should lay training programs for all those involved in legislation, law enforcement and the judiciary. The trainings should be followed by regular seminars and campaigns alongside ensuring presence of investigators with the relevant tools for the purposes of bringing perpetrators to book. These laws must also address the issue of conflict between the right to privacy and investigation of cybercrime.

In the endeavor to produce a comprehensive legal framework, a legislator should address itself to international best practices with special attention to alleviation, detection and response to cybercrime.

Figure 3. Keypad key for ‘cyber security’. Retrieved from tech.ebu.ch.

2. Technical Response.

At an institutional level, computer users can protect themselves from botnet by a number of preventive measures. One such measure is filtering of inbound emails using IP block lists such as SURBL and such other methods as HELO filtering, Gray listing and Banner Delay. Internet service providers also install antivirus filtering which may aid by blocking the malware intended to create a botnet. While inbound filtering protects the concerned institution, several institutions have also undertaken to protect others by ensuring that there is no abusive traffic coming from their precincts using outbound filtering.

To go a mile further, institutions need to employ verification mechanisms. Internet service providers can verify any inbound content by employing such techniques as checking DKIM sender ID and SPF, path authentication and message authentication. In the first instance, the required ID information is readily available on information received and therefore one is able to tell if for example and email purporting to have been sent from a certain website is actually from said website. Using path authentication, an email receiver accesses information published by a domain's administrator which declares a list of valid servers that the domain sends the email from, from which the receiver is able to gauge the credibility of the information received.

Message authentication is done by checking message content with aim to establish whether the message sent is of the type the sender would normally send. If the message is valid then it will have some form of connections to the servers from which it emanates, however, if it is spam, then it will contrast with the servers it purports to be developed from.

The third and last step in the technical approach is consideration of the particular system's reputation. While an email may be verifiably from a source which can be authenticated, it is important for computer users to be aware of notorious spam sites and domains. This is with reason that there are sites that are clearly known for spamming and verifying and authenticating content sent from them will not serve to alleviate botnet if that is their intent.

Computer users can also self-protect against cyber crimes using system and network forensics toolkits.

3. The Social Approach.

As any other solution and as earlier mentioned, curbing cybercrimes requires a multi-sectored effort. The first of these efforts should be civic education on the nature of cyber crimes, the types that exist, detection of cyber crimes and finally, their mitigation or prevention all together. Target groups for this civic education must be those areas which are vulnerable to attacks either by the kind of data they process or by the multiplicity of computers and computer needs therein. For example, government agencies cannot be overlooked since they handle sensitive and usually top secret information. There have been incidents of attack on government institutions such as the notorious WikiLeaks whose effect on government reputation and functioning was catastrophic.

On the 21st of December 2018 for example, the site published what was allegedly procurement request by the United States embassies all around the world. In this, were spy gears which painted the United States in bad light and put its diplomatic relations in jeopardy. An even bigger scandal was the Hillary Clinton emails published all over the world on the 4th of March 2017 which almost destroyed the candidate's political prospects. The site has far reaching tentacles and has run exposes on several other governments such as Russia, the United Arab Emirates and also on multinational corporations such as Amazon, which, as expected, had devastating effects on those concerned.

There currently exist several civil societies' initiatives in the area of Information and Communication Technology such as the Global Programme on Cybercrime which runs under the United Nation's Office on Drugs and Crimes. What these initiatives require is capacity building and a helping hand from the government. This would further enhance their effectiveness.

In all these efforts, the operational agencies should make sure to deliver the message in such a way that it is understood by the common citizen. This will involve running audience-friendly advertisements, films and print media. Furthermore, the efforts would fail if the requisite software to deal with malware is not availed. In this regard, there should be provision of secure Customer Premises Equipment (CPE) which should include broadband routers and wireless access points that are secured and firewall enabled. Since the high cost of software leads users to buy pirated material, there should be a multi-sectoral to subsidize software or produce cheaper alternatives.

CONCLUSION.

It is undoubtedly clear that technology is the fastest growing industry worldwide. The industry has made the wide world a global village with convenient communication and information at one's fingertips and is as such, indispensable. With all the growth and advantage, however, there has also emerged the challenge of cybercrime which has occasioned loses in finance and morality.

Emergent in the field of cybercrime is the botnet technology which in essence turns other computers into robots using malware and uses them for the controller's ends such as defrauding and spamming. Ideal methods in the mitigation of this challenged should take the form of regulation, technical mechanisms and some social measures. Such efforts would include development of effective laws on cybercrime, provision of cybercrime-combating software and

corporation of all relevant stakeholders. All these are necessary for the purpose of ridding society of cybercrime.

References.

"Thingbots: The Future of Botnets in the Internet of Things". *Security Intelligence.*20 February 2016. Retrieved 9 January 2019.

Credeur, Mary. "Atlanta Business Chronicle, Staff Writer". Bizjournals.com. Retrieved 9 January 2019.

Lucian, C. (25 July 2013). "Cybercriminals are using the Tor network to control their botnets". Retrieved from https://www.pcworld.com/article/2045183/ cybercriminals-are-using-the-Tor-network-to control-their-botnets-researchers-say.html

Ramneek, Puri (2003-08-08). "Bots & Botnet: An Overview" SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/malicious/paper/1299.

Schiller, .C., et al. (01-01-2007). "Botnets" Burlington: Syngress. Pp. 29-75.

Wang, Ping et al. (2010). "Peer-to-peer botnets". Handbook of Information and Communication Security.