International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.2, No.1, January 2013, pp. 46~50
ISSN: 2252-8776

Botnet Prevention Strategies for Social Network users: Cases and Remedies

Nishikant C Dhande
School of Commerce and Management Sciences,
SRTM University, Nanded, India

Article Info

Article history:

Received Jul 17th, 2012
Revised Aug 20th, 2012
Accepted Nov 20th, 2012

Keyword:

Botnet
Computer Security
SNA
IDS.

ABSTRACT

A Botnet is a collection of computers infected with malicious code that use FTP, TFTP, and HTTP protocol based services for infecting the computers. They keep on spreading till a desired strength of Botnet is assembled. Since social networking users have inclination to grow the Social Networks, a poorly designed social networking website can have some loop holes which could invoke a Botnet to spread around the users connected to it. In this paper attempt is made to elaborate assimilation of social networks and to show how they can turn into Botnet. This study is based on the analysis of spam, Internet blogs, newsgroups & Cases for converging into conclusions.

Corresponding Author:

School of Commerce and Management Sciences, SRTM University, Nanded, India
Email : nishika.dhan@gmail.com

1. INTRODUCTION

A botnet is a collection of internet-connected computers whose security defenses have been breached and control ceded to an unknown party. Each such compromised device, known as an **"bot"**, is created when a computer is penetrated by software from a *malware* distribution. (as defined by en. Wikiped ia.org /wiki/Botnet).

Botnet Research Survey [1], Zhu et al. defined botnet as "*a collection of software or robots that run on host computers autonomously and automatically, being controlled remotely by an attacker or attackers*". They described four phases of botnet creation and maintenance: (1) Initial Infection, (2) Secondary Injection, (3) Malicious Activity, (4) Maintenance and Upgrade.

Initial infection is the exploit that an attacker makes to get the bot software running first time on the host computer. In secondary injection, the bot running on the infected host receives commands from the botmaster via the command-and-control network. It further autonomously carries out the malicious activities. The secondary injection specifies, the spread of itself to vulnerable peers, and occasionally reports in to the botmaster for maintenance and upgrades. All these phases show acceleration if they come across a network. With the advent of internet, as million of people browsing online have evidently formed their networks, which now days have become major cause for Botnet. The social networking (SN) websites are most popular among the Internet users. These websites carry some vital properties for botnet. These include huge number of users, communicating the same social interests, developing and in search of access to the same resources. Thus SN has become the platform for bots to spread across the network.

2. RESEARCH METHOD

2.1 Review of Botnet families:

Bots provide remote command and control access via a variety of protocols, including IRC, HTTP, instant messaging, and peer-to-peer (P2P) protocols. When several of these bots are under common control, it is commonly referred to as a botnet [2].

There are many families of bots viz. AgoBot, SDBot, SpyBot and GTBot. Every family has its own properties, versions and variants. The command and control system implemented in AgoBot is a derivative of IRC (Internet Relay Chat). The protocol used by compromised systems to establish connections to control channels is standard IRC. The command language implemented in SDBot is essentially a lightweight version of IRC. The command language implemented in SpyBot is quite simple and essentially represents a subset of the SDBot command language. This provides commands such as login <password>, info, spy, quit etc. GT Bot also uses IRC as its control infrastructure. GT Bot facilitates creation of versions with specific goal instead of developing a broad range of capabilities within a single line of the code base. A detailed note on these families is appeared in workshop discussions on "Inside Look at Botnets" [3]. Several studies were carried out and the corresponding reports [4], [5], [6], [7], [8], [9] mentioned the use of botnets in carrying out several types of attacks on almost all services available on the Internet. Botnet command and control (C&C) communications tend to be unencrypted, and since it's not uncommon for multiple bot infections to be located on the same network or system, attackers commonly instruct their bots to sniff network traffic looking for competing botnet communications [3]. This discussion gives the potential reason to look for the assimilation of social networks to show how they can turn into Botnet

2.2 Botnet Risks and Sources:

Botnets are used by botmasters for a wide variety of illegal activities. Botmasters are more numerous, sophisticated, harder to identify, have better tools and very large size of bot armies and thus can command the individual zombies to carry out various types of attacks that include, but not limited to, Distributed Denial of Services (DDoS), spamming, phishing, identity theft, click fraud, hosting of illegal material, disseminating malicious code, and a variety of other possible attacks [10].

Social networking is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision, the workplace, universities, and high schools, or regional .It is most popular type is online - the "Internet version" It is one of the advanced forms of communications , where internet websites are commonly used to spread the relationship. Social networking through websites, function like an online community of Internet users and the members share common interests like hobbies, religion, or politics. All these shared interests have a social capital as motivating force. Once we granted access to a social networking website we can begin to socialize. This socialization may include reading the profile pages of other members and possibly even contacting them. Nowadays the most popular ones are Facebook and Myspace, with 132 and 117 million users respectively in 2008 [11]. There are also some other networking websites such as Orkut (Google), Kibop, Flickr, hi5 etc. which often get identified as social networks.

A social network can be represented as a graph, where nodes are generally individuals or organizations, edges are relationships between two nodes, as in figure 1.

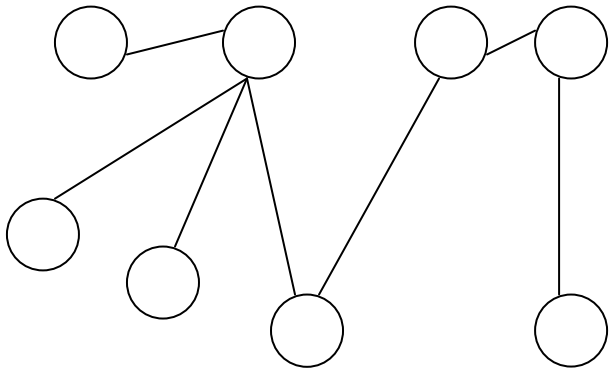

Figure1. Social network can be presented as graph

3. RESULTS AND ANALYSIS

3.1 Security holes in Social Networks: Obeservations

It is observed that the rapid adoption of the social networking websites by the internet users is raising the need to give attention on some important security holes. Following loop holes in the literature surveyed have been witnessed and presented in the form of observed case studies.

Observed Case 1:

Social networking websites like MySpace did not block HTML, CSS, and JavaScript in their forms [12]. This feature can be used to personalize user's pages by adding code to the form fields. Often such kinds of personalization are observed when the user changes the background and add multimedia to his pages. Unfortunately, no easy way is available to make these modifications and the individuals has to figure out about the CSS or HTML? and where to go in a form as well. Individuals choose a desirable layout and then they are instructed to copy and paste the code into the appropriate form. This code certainly includes links back to the helper page. A copy/paste culture emerged, as youth began trafficking in knowledge of how to pimp out their profiles and could invite a botmasters attention [12].

Observed Case 2:

Receiving an advertising or spam is another important factor that causes threat. The attacker can write or comment on people's profiles or may send a private mail, the attacker can distribute links advertising websites and products. If such an act is successfully carried out by attacker then contacts will quickly notice that the posts are stealthy advertising and will delete the attacker altogether. The same can be done by private Web messaging also, which all social sites allow but it is similarly ineffective for the same reasons stated above. These kinds of social networking spam usually run for very limited duration and come from pay-per-click or pay-per-action affiliate-based online marketing schemes [13]. If social website includes contact information such as email addresses or telephone numbers, these can provide a better target for spam, phishing, and voice phishing. The usefulness of such a database is measured on the quality of the data. Older email databases have been spammed over and over so the addresses might have been dumped or accounts are closed. The more risk prone email databases is the fresh and in use working emails such as the same as we usually find in social networking sites.

Observed Case 3:

The third possible risk is of phishing and/or malware installation. In this case attacker creates a phishing page identical to the social network login page. Then the status line may be change like "check this funny video" which links to the fake login page. This page forces to "log in" again, misleading the user to think that perhaps somehow their session had timed out. Thus the user re-logins, at this point of event, the attacker steals the victim's username and password. But the attack does not end here. After "logging in," the fake page displays a funny video that further makes the browser vulnerable by installation of a Trojan in the background.

Observed Case 4:

The social website like Twitter, has "cross-site scripting" attacks performed against it. In these cases, the attackers could change the Twitter status of any user accessing the attacker's account. In such a way attacker could make the user tweet bad links .This makes their Twitter group to be at the risk of being infected [14].

Observed Case 5:

XSS script can be used in code to communicate with the Face book page context Example so as to determine the identity of the profile viewer. However their current model barely makes any use of this functionality.

Observed Case 6:

Host scanning can also be one of the possible way of attack. Usually JavaScript is used by the attacker for some of the ports which are useful for internet browsing. The attacker randomly selects a host and a port, further requests an object through normal HTTP requests. Afterwards, based on the response time, which can be measured through JavaScript, the attacker can form botnet on the live port.

3.2 Face Book based social networks as Botnet:

Face book is one of the most popular social networking sites. It started as a project for students so as to keep track of schoolmates but has now grown up to serve more than 300 million people from around the world [15]. Face book consist of many applications and can be considered as XHTML snippets that inherit all properties of web applications. Applications are served externally but are viewed in the context of a Facebookhosted page with a Face book URL. Face book Markup Language (FBML) includes a "safe" subset of HTML and CSS as well as Face book-specific tag Face book uses two methods to identify and authenticate users: cookies, which contain session information, and hidden form IDs that are supposed to ensure that forms come from the user.

Using this cookie or knowledge of user's form ID, an attacker can imitate a victim. The session information of cookies is used by the attacker to construct XML-Http request and assume all same privileges as the user. The form would automatically submit when viewed by a logged-in user and have the authentication credentials of the unaware viewer. It is required that both hidden form IDs and cookies can be shielded from third-party applications.

FBML gives Face book the ability to abstract user information and maintain some uniformity of style between applications. Since the parsed third-party code is included directly in the page, any malicious code that could slip through their filters would have access to the hidden form IDs. Depending on the browser version, the code might also be able to fetch the user's Face book cookies. Many browsers (such as Firefox prior to the 2.0.0.5 release) ignore the *http-only* flag on cookies and would leave them accessible through the JavaScript document cookie variable. Face book therefore attempts to strip FBML of all references to JavaScript or external code. Similar technique is used by Adrienne Felt [16], he used code in the form as:

```
<fb:swf swfsrc="http://myserver/flash.swf"
imgsrc="http://myserver/image.jpg" imgstyle="-mozbinding:
url(\'http://myserver/xssmoz.xml#xss\');" />
```

After being parsed and added to the user's profile, the highlighted image style Attribute becomes:

```
<img src="http://facebook/cached-image.jpg" style="-mozbinding:
url('http://myserver/xssmoz.xml#xss');" />
```

This causes Firefox to retrieve and evaluate the contents of the external XML file. The Firefox XML file contains the attacker's JavaScript.

```
<? xml version="1.0"?>
<bindingsxmlns="http://www.mozilla.org/xbl">
<binding id="xss"> <implementation><constructor>
<![CDATA[ alert('XSS'); ]]>
</constructor></implementation></binding>
</bindings>
```

In this way the JavaScript in this file is now executing in the context of the authentic Face book page with the user's valid credentials.

3.3 Analysis & Discussion on Possible remedies

The only best remedy available is the careful browsing and downloading from known sources on the net. Usually user should not make any relations unless a rigid and confirm knowledge is obtained. After careful analysis and literature survey, some remedies can be suggested, as below:

1. To avoid being botted, user must have habit to filter all incoming traffic. The user can restrict traffic from sites which are responsible for Botnet using NIDS (Network Intrusion Detection System) or Firewall. Similarly, the social website designers should take care about their client side technologies used by the user like JavaScript, PHP *etc.*
2. While publishing a page Face book, servers requests any image URL and then serve these images, rewriting the "src" attribute of all "img" tags using a "*.facebook.com" domain. This will defend the privacy of Face book's users and not allows malicious applications to extract information from image requests made directly from the view of a user's browser. Thus, if the "src" attribute of an "iframe" is an image file (*like* .jpg, .png,), the Face book Platform can handle these frames in a way similar to "img" tags.
3. A social network operator should provide developers with a strict API, which will be capable of giving access to resources only related to the system.

The applications used by the social network should have constraints regarding their interactions with other hosts in Internet which is not part of the social network.

4. CONCLUSION

The social networks are very well-liked tools for botnet attacks. In recent days they have became the only way for Botnet to get installed, matured and then to get propagated further to carry out a number of attacks. There is little guarantee about the safety of the user computer while working with social network sites, as bot infection can take place in any form. Hence a suiable strategy is being shown as to how the integration of social networks can turn into Botnet. Many angles of the risks and the vulnerability situations have also been elaborated in the article. It is highly impossible to control such integration by devising a device or software tool. However some tips based on the observation and probable situations and cases are discussed for the benefit of the user to avoid being getting botted.

ACKNOWLEDGEMENTS

The work presented here is the outcome of sincere help and cooperation extended by the teachers and the students of the School of Commerce and Management Sciences and the School of Computational Sciences, Swami Ramanand Teerth Marathwada University Nanded. The details of the issue has been taken in to consideration based on the various survays made by different organizations on the internet and discussions made with the eminent persons in the professional and academic areas of knowledge.

REFERENCES

[1] Zhaosheng Zhu, Guohan Lu, Yan Chen, Z.J. Fu, P. Roberts, and Keesook Han. Botnet research survey, pp 967{972, 28 2008-Aug. 1 2008.
[2] Moheeb Abu Rajab Jay Zarfoss Fabian Monrose Andreas Terzis , A Multifaceted Approach to Understanding the Botnet Phenomenon, Conference proceedings *IMC'06,* October 25–27, 2006, Rio de Janeiro, Brazil.
[3] Barford, Paul; Yegneswaran, Vinod. *An Inside Look at Botnets* , Special Workshop on Malware Detection, Advances in Information Security, Springer Verlag, 2006 .
[4] Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds Kandula, S., Katabi, D., Jacob, M. & Berger, A. (2005).. Proceedings of 2nd Symposium on Networked Systems Design and Implementation, Boston, MA,http://nms.lcs.mit.edu/papers/killbots.pdf accessed May 17, 2008.
[5] McAfee. (2005). McAfee virtual criminology report. McAfee, Santa Clara CA.http://www.softmart. com /mcafee/docs/McAfee%20NA%20Virtual%20Criminology %20Report.pdf accessed May 17, 2008.
[6] AHTCC. (2006). International Internet Investigation nets arrest. Australian High Tech Crime Centre Media Release. http://www.ahtcc. Gov. au / news_ and_ information/ media_ releases/nat_060322i nternet arrest.pdf accessed May 17, 2008.
[7] Dunn, JE, Botnet chaos shut down hospital , (2005). Techworld, May 5, 2005. http://www.techworld.com/ security/news/index.cfm?NewsID=5951 accessed May 17, 2008.
[8] David, L., Phishing expedition at heart of AT&T hacking, (2006). San Francisco Chronicle. http://sfgate. com/ cgi-bin/article.cgi? f=/c/a /2006/09/01/BUGVBKSUIE1.DTL accessed May, 8, 2008
[9] FCAC (2006). FCAC Cautions Consumers About New Vishing Scam. Financial Consumer Agency of Canada. http://www.fcacacfc. gc. Ca / eng/media/news/default.asp?postingId=218 accessed June 8, 2008.
[10] McKewan , A. (2006). Botnes: Zombies get Smarter, Network Security, 6: pp18-20.
[11] http://www.informit.com/blogs/blog.aspx?uk=Security-Issues-of-Social-Network-Sites
[12] Danah boyd. (2007) "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press.
[13] David Sancho, Security Guide To Social Networks, A Trend Micro White Paper I August 2009.
[14] http://blogs.computerworld.com/twitter_stalkdaily_mikeyy_xss_worm
[15] FacebookStatistics,http:// www. facebook.com /press/ info. php?statistics.
[16] Defacing Facebook: A Security Case Study Adrienne Felt, University of Virginia felt@virginia.edu, www.cs.virginia.edu/felt/fbook

BIOGRAPHY OF AUTHOR

Dr. Nishikant C. Dhande, He got Diploma in Industrial Electronics, B.Sc. (Phy.Chem. Electronics) B.Tech (Electronics). M.Sc. (Computer Science), M.B.A. P.G.Diploma in Production Management, Ph.D. System Management. Assistant Professor, School of Commerce and Management Sciences, S.R.T.M.University, Nanded, Maharashtra India. Twenty-four years experience of Teaching, R & D, Industrial Consultancy. Review Member of IEEE SMC, Cybernetics, HBR Publications Courseware. Founder Member Computer Society of India, Aurangabad Chapter.