Emergence in Web-based Botnets Targeting Application Layer

Ritesh Talreja, Chandrashekhar Dashudu, Anish Raniwala
Computer Engineering Students
Vivekanand Education Society Institute of Technology
Mumbai, India

Mrs. Dimple Bohra,
Computer Engineering Mentor
Vivekanand Education Society Institute of Technology
Mumbai, India

***Abstract*— Botnets are ever increasing day by day for malicious purposes. Most recent trends indicate harnessing application layer vulnerabilities or targets that benefit the bot masters. This paper briefs about the Application layer based botnet attacks. Such attacks include: Botnet based Distributed Denial of Service (DDoS) attacks that are the most common and prevalent security attacks specially generating application layer traffic; another attack for financial gain is pharming, phishing along with fast flux making botnet harder to track down. Click Frauds are yet another example employed using botnets and proxies to gain financially. Another monetary gain attack which has recently emerged is mining of crypto-currencies such as Bitcoin, Litecoins etc.**

This papers describes in general about botnets, their infrastructure, their use in DDoS attacks, pharming, fast fluxing, Cryptocurrency mining. This papers also gives an insight into the methods that can be used to prevent these types of attacks.

General Terms
Information Security, Computer network

Keywords—Botnet, Digital Currencies, Identity Theft, DDoS Attacks, Pharming, Phishing, Web server, IRC, Fast flux attack, Click Fraud

I. INTRODUCTION

Botnet comes from the combination of robot and network. These bots are usually Internet-connected software bots that are under the control of a single server controlled by the bot master. The term originated from bots that were used for mundane purposes of maintaining Internet Relay Chat (IRC) channels, but eventually botnet led to malicious intents. Nowadays botnet is associated with malicious intents. Botnets in case of malicious intentions spread themselves through various vulnerabilities such as browser security flaws, removable disk transfers, spreading by worms, Trojans, email attachments, drive-by downloads etc. Once on a machine they infect them and cause user inconvenience, data loss and fulfilling any other malicious desires as commanded by the botnet operator or the bot master.

DDoS attacks are initiated in various types which include Internet Control Message Protocol (ICMP) Flood at network layer, SYN Flood, UDP Floods at the transport level and most recently used HTTP/S Floods at the application level.

Phishing is basically impersonating the look of a website in deceiving customers to give away their usernames, passwords and credit card numbers. Apart from proxy servers, anonymity can be increased using fast flux employed in bots code to hide their phishing/pharmed sites.

Digital currencies such as Bitcoin is a decentralized digital currency that can be obtained at outright or via mining them. Mining Bitcoins require intensive computer resources such as CPU/GPU power and RAM; power requiring to mine them can eventually outweigh profits that would be reaped out of Bitcoins earned. Hence malicious hackers thought of employing their Botnets computing resources for mining.

II. BOTNET INFRASTRUCTURE

Botnets are basically compromised internet connected hosts (software bots) which usually follow the commands given by a centralized bot-master controlled CNC/C&C (Command and Control) server. Malicious Bot code hides itself making it undetectable and allowing user to carry out its normal operation without them knowing bot is working in the background.

Botnet infrastructure usually comprises of 3 models: Agent-Handler, IRC-based, emerging Web-based models.

2.1 AGENT-HANDLER MODEL

The agent-handler model compromises agents, handlers and clients. Clients are the ones that actually perform the required operation as commanded by the CNC. All of these 3 are essentially compromised hosts forming the botnet. Agents are intermediaries between a handler and client. Agents eventually conduct the attack at appropriate time. The bot-master communicates with any of the online handlers to direct the attack. Handlers are usually installed on network servers or by replacing the firmware's of compromised routers. The terms "handler" and "agents" are sometimes replaced with "master" and "daemons" respectively. Compromising network servers/routers is difficult which leads us to next 2 models.

2.2 IRC MODEL

Internet Relay Chat (IRC) is a system that facilitates transfer of messages in the form of text. The chat process works on a client/server model of networking where IRC clients are computer programs that a user can install on their system. These clients are able to communicate with chat servers to transfer messages to other clients. It is mainly designed for group communication in discussion forums,

called channels, but also allows one-to-one communication too [1].

Hence bots installed connect to a central IRC server once they join the botnet. IRC-based botnets are a popular method for botnet and CNC communication. It's easier to track joining of a new bot in the botnet as the list of bots connected appears in the IRC group chat, easier to maintain track of online/offline bots and directing commands to individual bots.

2.3 WEB-BASED BOTNETS

Here bots are employed with usual ways of spreading worms, viruses, and emails etc. which communicate to a central Internet hosted website. These have gained more popularity than IRC-based botnets for the following reasons:

- Easier to develop and host websites
- Prevents IRC chat-hijacking
- Anonymity increased with online web hosting
- Conceal web server's presence amidst huge volumes of HTTP traffic with respect to network managers of compromised networks.
- The web server can be connected anonymously using high anonymity proxy servers.
- Increased anonymity using anonymizing networks such as TOR. The infamous drug dealing and elicit materials trading website Silk Road was untraceable as it could be reached only via a single network that is the TOR network. This essentially hosts an anonymous web server reachable only via its anonymizing network that makes it unreachable via standard browsers. Silk Road was shut down due to human error leaving behind his personal details ultimately tracking him down.
- Easier reporting
- Easier commanding
- Easy ease of use and acquisition.
- Encrypting traffic over port 443 (HTTPS)

III. DDOS ATTACK AND TOOLS

Denial of Service (DDoS) is a type of security attack that floods or continuously sends request packets to the victim server. The victim server thinks these requests are from legitimate users and hence replies to them. Eventually server gets overloaded of these malicious intent requests and can't serve the legitimate users hence denying legit users of services. DDoS still remains 1 of the hardest to prevent security attack till date.

DoS attack is launched by single host whereas DDoS attack is launched by multiple hosts under a single control command. Various script kiddies (skids) tools are also available for DDoSing such as:

- LOIC (Low Orbit Ion Canon) is a HTTP/TCP/UDP flooder that floods a single victim server. It gained popularity when it was used by a group of hacktivists "Anonymous" via Zeus Botnet network against various government websites such as Department of Justice (DOJ) and the Federal Bureau of investigation (FBI) [2].
- BlackEnergy employed by Russian hackers [3].

IV. DDOS ATTACK CLASSIFICATION AND COUNTERMEASURES

Various ways can be employed to flood the victim server with requests. 1st 3 include the traditional ways for carrying out DDoS [4]:

4.1 ICMP/PING FLOOD

Internet Control Message Protocol (ICMP) acts as a companion to Internet Protocol (IP) at the network layer reporting errors and used for troubleshooting. Pinging and getting replies from a host on the Internet defines its reachability from the sender. Ping Flood includes flooding continuously ping/ICMP/Echo packets to the victim server without waiting for replies (non-blocking/asynchronous calls). Ping Floods were common for many years as it occupied both outgoing and ingoing traffic at the server. Other ping related traffic includes Ping of Death and SMURF attack.

4.2 SYN FLOOD

SYN is a flag in the transport layer protocol: Transmission Control protocol (TCP) that is the first part of the 3-way TCP handshake used for establishing connections. HTTP and many other protocols such as FTP, VNC use TCP connections for reliable connection-oriented communication. 3-way handshakes include SYN packet being sent from client to server, server then allocates necessary buffers and maintains global data structure tables for the connection and sends back SYN+ACK packet and then the client in turn sends an ACK packet to the server completing the 3-way handshake. What SYN Flood exploits is that it sends only the SYN packet without sending back ACK packet or sending the SYN packet with a spoofed/false source IP address. In eventually makes the server maintain a huge number of half open connections thus overloading itself and coming down to a screeching halt.

4.3 UDP FLOOD

User Datagram Protocol (User datagram protocol) is another transport layer protocol that provides unreliable connection-less way of communication. Here the bots flood the victim server with source/spoofed source IP and random data.

4.4 HTTP/S FLOOD

Latest and most employed Flooding is by HTTP/S Flood to a Web server. HTTP resides at the application layer and hence differentiating between legit HTTP traffic and malicious traffic is difficult. Although one can argue that the attacking bot's IP can be blocked if they continuously flood with HTTP request packets to single URL; but botnets can employ the crawling method to imitate actual user traffic. Bots would attack the same domain/IP of the web server but eventually crawling over each URL it receives from the HTML code it received from the earlier HTTP web request.

4.5 Possible Countermeasures

Ping Floods can be prevented by not responding to pings at the network layer by configuration in the router. Ping of death was prevented by fixing the TCP/IP protocol stack code to avoid crashing due to re-assembling of big sized packets.

SYN Floods can be prevented using TCP SYN Cookies and postponing resource allocation after server receives ACK packet from client.

Another methods include application layer filtering using Firewalls and State full Firewalls. Firewalls with deep packet inspection prove useful for the above two.

V. DDoS Attack Classification and Countermeasures

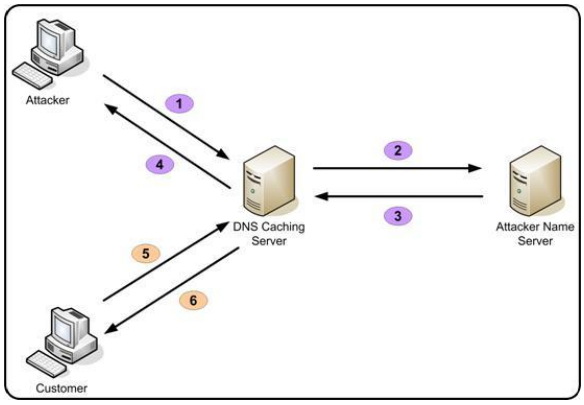

Figure 1: Typical Pharming Attack

Domain Name System (DNS) is a distributed network of servers having Resource Records (RR) that convert human readable domain names into machine understandable IP addresses.

Phishing is the process of impersonating a website by having the same look and feel of the victim site in order to deceive the users to submit their banking/personal details to the malicious site. Targets usually include Bank and Email sites.

Pharming is a portmanteau of Phishing and Farming. It helps triggering phishing along with other methods such as botnets, Spam Emails etc. Farming implies implanting seeds into DNS Servers to carry out phishing.

The basic procedure works as follows: Attacker attacks the DNS server and changes the IP address of victim's domain name to its fake/impersonated web servers IP address thus redirecting the original site to the attacker website.

1. Attacker attacks the DNS caching server usually the Internet Service Provider's (ISP) DNS server due to its less security with respect to root name servers or other big corporate public DNS servers like Google DNS or Open DNS.

2. Attacker's request to make an entry for the victim domain point to Attackers Web server IP address at ISP DNS

3. Attacker's name server sends back the attackers IP address for the victim domain that is cached at the ISP's DNS or the record can be deleted too.

4. Notification to attacker

5. Normal user requests for the victim domain in browser

6. User eventually gets the website hosted at attackers web server IP address.

Website has the same look and feel as the victim's website and users hand over their details.

5.1 Botnet employed pharming

Following methods are implemented by bots to carry out pharming at the infected/compromised machine:

- Bots or the compromised hosts can make the victim domain's point to their fake website located at their web server's IP address by putting "hosts" file entries in the system.
- Bots redirect all traffic to bot-master controlled proxy server which redirects victim website request to fake/phished sites for a particular victim domain.
- Bots poison the local DNS cache and redirect requests.
- FAST FLUX: It's a method employed by botnets to hide their phishing sites behind an ever-increasing compromised networks of hosts acting as proxies for victim domains request traffic.

5.2 Countermeasures against pharming

- DNSSEC protocol (DNS SECurity)
- Not trusting suspicious emails asking for banking/personal details.
- Browsing cautiously verifying SSL certificates

Some antiviruses do protect only against "hosts" file modifications.

VI. CLICK FRAUD

There is huge market of contextual Internet based ads marketing undertaken by Internet giants such as Google, Yahoo etc. Google get its more than 50% revenue from its AdSense/AdWords network.

Advertisers pay Google and use their network to display ads about the services/goods they offer. Contextual Advertising includes showing ads that are related to Google search keywords user type in. Google in turn publishes ads on its own webpages (search results, YouTube etc.) or on pages of a 3rd party publisher website.

Advertisers have to pay Google for displaying their ads using a CPC (Charge per Click) system. CPC system makes advertisers pay Google only for the number of clicks users click on their ads.

When 3rd party publisher websites host Google ads, each click's charge share is paid to the website owner too along with Google.

Botnets can be commanded to continuously click the ads (behind a huge round robin list usage of high anonymity proxy servers) to generate income for the website owner using robots (bots) without any intent in viewing the ads content, eventually imitating a legit user click.

Click Fraud has resulted in billions of dollars loss for advertising companies including Google and other Paid-To-Click companies which urged them to develop Click Fraud detection algorithms.

VII. CRYPTO-CURRENCY MINING USING BOTNET

Crypto currencies have emerged in the 2006-2010. Most famous being Bitcoins which are nothing but Open Source decentralized digital currencies that can be traded against goods/services just like traditional cash making it a medium of exchange [5].

Bitcoin solely operates Peer-2-Peer without any central authority as in case of traditional currencies such as Reserve Bank of India (RBI) in case of Rupee, US Government backed dollar etc. Introduced in 2009 by Japanese developer Satoshi Nakamoto, maximum of 12 million Bitcoins can be present in the market stored in Bitcoin online/offline electronic (password protected) wallets. Loss of password to wallet is essentially losing those Bitcoins forever, analogous to burning cash. Bitcoins possess low processing fees and can act as alternative to Payment processors like VISA, MasterCard or PayPal to buy goods over Internet. Bitcoins also help in avoiding Internet censorship and avoiding Governments to politically suppress Payment Processors to disallow transaction processing against any organization. An infamous example being PayPal, MasterCard, VISA stopping transactions and even going to the extent of freezing WikiLeaks accounts [6].

All Bitcoin are maintained in a global distributed leisure and these Bitcoins can be obtained by either buying them at outright, trading against goods/services or mining them just like gold. Bitcoins presently however are very volatile/fluctuating in nature with respect to traditional currency, but it's only a matter of time to get them stabilized as its market increases and people use it as store value.

Bitcoins are mined by performing complex mathematical calculations generating many Hashes/second required to acquire the Bitcoin. Bitcoin by its inherent nature of coding sets the difficulty level of mining higher and higher after every mined Bitcoin block release. Hence mining the starting range of Bitcoins was a matter of using spare old computers while mining Bitcoins later in the range is most difficult requiring many calculations and hence more computing power leading to more power consumption requiring more hardware cooling. Power bills effectively outweigh the profit acquired by Bitcoins mined.

Central Processing Unit (CPU) have been proven less efficient in power consumption and throughput (Mega Hash/second) with respect to Graphics Processing Units (GPUs). Also Linux OS are better alternatives as compared to Windows.

Mining Bitcoins requires intensive computing and increased power consumption, leading to emergence of Application Specific Integrated Chips/Circuits (ASICs) that are designed specifically to mine Bitcoins only and nothing else with as much as less power consumption.

7.1 BOTNETS IN CRYPTOCURRENCY MINING

Botnets can be employed, where central CNC server can command the bots to mine Bitcoins for the attacker using bots computing resources effectively costing pennies for the attacker in terms of mining Bitcoins [7]. Even Bitcoin mining pools can be used such as Slush's pool to distribute Bitcoins earned among a group of people (pool) according to amount of work done by each pool member.

VIII. CONCLUSION

Botnets are widespread and can be used for any purpose as wished by the Bot-master. Botnets are undoubtedly serious Internet security challenges. In this paper, we dealt with Botnets flooding victim servers mostly using HTTP traffic, corrupting DNS caches/servers carrying out pharming attacks along with increased anonymity by using anonymizing networks such as TOR and fast fluxing. Finally an emerging attack employed using botnet is cryptocurrency mining. Botnets are usually also obfuscated to avoid botnet busters to understand its operation.

Botnets are currently being detected by mining out patterns in infected network traffic for CNC communications; and then eventually blocking CNC traffic crippling bots as CNC URLs are usually hardcoded in bot software.

Botnets are now slowly gaining a more sophisticated nature of Peer-2-Peer (P2P) networking, where bots together control their own actions without the need of a central CNC, hence tracing the creator is even more difficult. These P2P bots forming their own network and carrying out tasks what they are designed for and that too autonomously which can be thought as malicious artificial intelligence development!

ACKNOWLEDGMENT

I, Ritesh Talreja being the prime author of this paper would like to thank my 3rd year Comp Engineering graduation colleagues: Anish Raniwala, Chandrashekhar Dashudu and many others. Also thanking my "Seminar" curriculum subject Mentor Mrs. Dimple Bohra of VESIT who guided me throughout in development of my own DDoS Botnet using C#.NET, PHP and Java.

REFERENCES

[1] IRC at Wikipedia: http://en.wikipedia.org/wiki/Internet_Relay_Chat

[2] InfoSec Institue, "LOIC (Low Orbit Ion Cannon) – DOS attacking tool".Availabe at: http://resources.infosecinstitute.com/loic-dos-attacking-tool/

[3] Jose Nazario, , ―BlackEnergy DDoS Bot Analysis,‖ Arbor Networks, 2007. Available at: http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf..

[4] Jelena Mirkovi´c, Gregory Prie,r Peter Reiher, "Attacking DDoS at the Source" at 10 th IEEE International Conference on Network Protocols (ICNP'02) 2002. (*references*)

[5] Reihan Salam, Jerry Brito "THE VICE PODCAST - PROFESSOR BITCOIN" at vice.com. Available at http://www.vice.com/read/the-vice-podcast-professor-bitcoin

[6] Ryan Fleming, "4chan-based group 'Anonymous' targets PayPal to support WikiLeaks", December 7, 2010. Available at http://www.digitaltrends.com/computing/4chan-based-group-anonymous-targets-paypal-to-support-wikileaks/#!F5irb

[7] David Gewirtz, "Want to make money mining bitcoins? Criminals have you beat" at ZDNet Government. Available at: http://www.zdnet.com/want-to-make-money-mining-bitcoins-criminals-have-you-beat-7000025361/