Survey on Botnets and Their Impact

Neharika Singh [1], Pooja Redekar [2], Madhumita Chatterjee [3]
[1, 2, 3] PCE,New Panvel, Computer Engineering, Mumbai University,
Email: neharikasingh23@gmail.com, redekar.pooja@gmail.com, mchatterjeee@mes.ac.in

Abstract— presently a day's different types of malware are developing as the most perilous risk to the security. As of late Botnets has turned into the most loved apparatus of aggressors to perform numerous unlawful exercises, for example, dispatch appropriated foreswearing of administration assault, phishing and click misrepresentation to separate individual data from the casualty. This paper exhibits the review of existing botnets and their design, assaults, discovery methods, portable and social botnet.

Keywords—Botnet, Botnet Attacks, Detection Techniques, Mobile Bots, Social Bots.

INTRODUCTION

Botnets are the biggest threat to internet security. Botnets consist of the networked collection of compromised machines called robots, or 'bots'. Bots are called "Zombies", and Botnets are also called "Zombies armies". Bots are controlled by nodes called 'Botmaster'. Bots are infected with malicious code that performs work on behalf of the botmaster. Typically, bots contact the botmaster for infections, software updates and to deliver status and exfiltrated data [1].

A. Botnet Attack

Botnet attack can done in many way but out of them this two attack damage the most.

- **DDoS**

It assaults a system that makes lost administration clients, commonly the loss of system availability and administrations, by expending the transfer speed of casualty's system or high data transfer capacity or over-burdening the computational assets of the casualty's framework.

- **Phishing**

Attacker gathers personal information by deception, misdirection and hidden installation of the malicious program which is called a "phisher". The phisher will need a list of email address a place to store stolen information. Phisher then uses the email list of send fraud message

B. DEFENSE, PREVENTION AND MITIGATION TECHNIQUES

This segment gives moderation, avoidance and resistance methods to decrease the impact of a movement which is destructive to others:

a) Mitigation Techniques: -

Actualizing channels on interior switches, firewalls, and other systems administration gear is suitable to disengage tainted sections. Physically detaching tainted PCs from the system. Considering a choice of quick obstructing all outbound movement to outer systems. Observing all system activity to address conceivable multifaceted assaults. Reinstall OS of a tainted framework.

b) *Defense Techniques: -*
Layer various systems for the most ideal barrier. Utilize the arrangement that relates danger data amongst email and web doors and in addition sellers and utilize aggregate knowledge to share data on assaults.

c) *Prevention Techniques: -*
Abstain from tapping on astounding Links. Never consenting to download documents with no required work. Try not to give individual data to anybody. Abstain from posting URL's or post short URL's with the goal that your status doesn't naturally conjure minor urls. Teach and spreading attention to an online client about a current leaving assault. Stay up with the latest. Snap just substantial connections and checks legitimate web joins. Be somewhat selective about your companions.

BOTNET ARCHITECURE

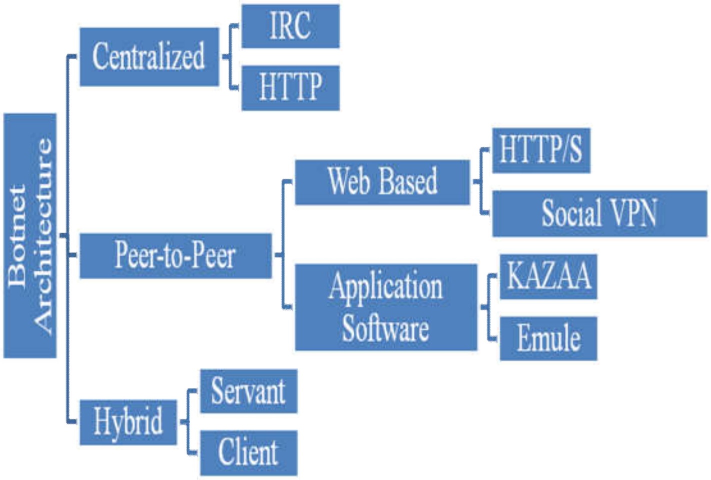

Figure 1: Botnet Architecture

A. Centralized Architecture
The Centralized C&C approach looks like the customary customer/server engineering. The IRC convention is a case of brought together C&C engineering wherein bots build up a solid correspondence channel between one or different association focuses.

B. Decentralized /Peer-to-Peer C&C Architecture
In a decentralized engineering, present day Botnets take more noteworthy adaptability to get a bigger number of bots and to accomplish the greatest advantage/benefit.

C. Hybrid C and C Architecture
The hybrid model inherits the properties of both decentralized and Centralized /P2P architectures.
The hybrid model is classified into two categories: -

- Servant Bot
- Client Bot

The worker bot goes about as a customer and a server all the while, which is designed with routable IP address, interestingly, the customer bot does not tune in to approaching associations as arranged with non-routable IP address.

Worker bots send IP deliver data to the associate rundown and remain in listening mode to distinguish the port for approaching association. So also, hireling bots have extra obligation to apply symmetric keys for every correspondence to stiffer the botnet location instrument.

BOTNET DETECTION TECHNIQUES

Detection of botnet at initial stage is not easy, therefore there are various techniques used to detect bot.

A. BotTracer

A bot like malware has represented a monstrous risk to PC security. A normal bot shows three invariant highlights along its beginning (1) the startup of a bot is programmed without requiring any client activities (2) Bot must build up a charge and control channel with its botmaster and (3) Bot will perform nearby or remote assaults at some point or another. BotTracer recognizes these three stages with the help of virtual machine Techniques. BotTracer has effectively identified every one of the bots in the trials with no false negatives.

B. BotMiner

This is a Botnet location framework that depends on a structure made of three primary stages; checking, grouping and relating. Initially, in the observing stage, two checking motors specifically C&C correspondence movement motor and action motor are utilized. Every motor keeps logs of its movement investigation. The C-plane screens both TCP and UDP stream to figure out who is conversing with whom. The A-plane screens organize exercises to figure out who is doing what by identifying strangely high sweep rates or weighted fizzled association rate. Second, in the bunching stage, C-plane grouping is performed by searching for groups of hosts that offer same correspondence designs. These bunches are defrauded by ascertaining four irregular factors, to be specific; various streams every hour, number of bundles every hour, normal number of bytes every second. In A-plane grouping, a host is first bunched in light of movement highlights. At long last, a cross-plane relationship is performed to discover a convergence between the two groups in the past stage. The convergence implies that these hosts are a piece of a botnet.

C. BotSniffer

BotSniffer can catch this spatial-worldly connection in organize movement and use factual calculations to distinguish Botnets with hypothetical limits on false positive and false negative rates. BotSniffer can recognize true Botnets with high exactness and has a low false positive rate. BotSniffer has two principle segments, the screen motor, and the connection motor. The screen motor is sent at the edge of an observed system. It looks at arrange movement, creates association record of suspicious C&C convention and recognizes action reaction conduct and message reaction conduct in the checked system. In the connection arrange, BotSniffer first gatherings the customers as per their goal IP and port combine. That is, customers that interface with a similar server will be put into a similar gathering. BotSniffer at that point plays out a gathering investigation of spatial-transient connection and similitude.

D. BotHunter

This is a Botnet recognition framework that depends on a predefined botnet contamination life-cycle. This framework works continuously and can recognize bots paying little heed to the system convention or C&C structure as long as the botnet's conduct takes after a predefined contamination cycle exchange demonstrate. BotHunter is contained three motors; Statistical Scan Anomaly Detection Engine (SCADE), Statistical Payload Anomaly Detection Engine (SLADE) and Signature Engine. SCADE is in charge of the discovery of inbound and outbound sweep exercises. SLADE distinguishes variations from the norm in byte-conveyed payloads. BotHunter is an application intended to track the two-way correspondence streams between interior resources and outer elements, building up a proof trail of information trade that match a state-based contamination arrangement display.

BOTNET ON ONLINE SOCIAL NETWORKING

Online Social Network (OSNs), such as Facebook, Twitter, and Google+, facilitate the interactions and communications among people. It becomes the most important social platforms for online communication and medium for opinions exchange.

A growing number of people regard popular OSNs as their main information sources. There have been writes about different assaults in light of social bots, for example, become a close acquaintance with casualties and afterward getting their own data, directing the spam crusade which prompts phishing, malware, and tricks.

A. STEGOBOT

Stegobot, another age botnet that imparts over probabilistically undetectable correspondence channels. It is intended to spread by means of social malware assaults and take data from its casualties. Stegobot activity does not present new correspondence endpoints between bots. Rather, it depends on a model of secretive correspondence over an informal organization overlay-bot to botmaster correspondence happens along the edges of an interpersonal organization. Further, bots utilize picture Steganography to shroud the nearness of correspondence inside pictures sharing conduct of client connection.

B. FRAppE

FRAppE-Facebook's Rigorous Application Evaluator-apparently the main device concentrated on distinguishing noxious applications on Facebook. FRAppE utilize assembled by watching the posting conduct of 111k Facebook applications seen crosswise over 2.2 million uses on Facebook. FRAppE can recognize malevolent applications with 99.5% exactness, with no false positive and a high evident positive rate (95.9%). FRAppE is a stage towards making a free guard dog for application evaluation and positioning, in order to caution Facebook clients before introducing applications.

BOTNET ON SMARTPHONES

The cell phone is presently all around coordinated with cutting edge capacities and advances, for example, the web. Portable Security has turned into an all-around basic issue because of the high use of cell phones, their accommodation, and versatility. Versatile Botnets have not yet been completely investigated as they have just as of late relocated to portable foundations.

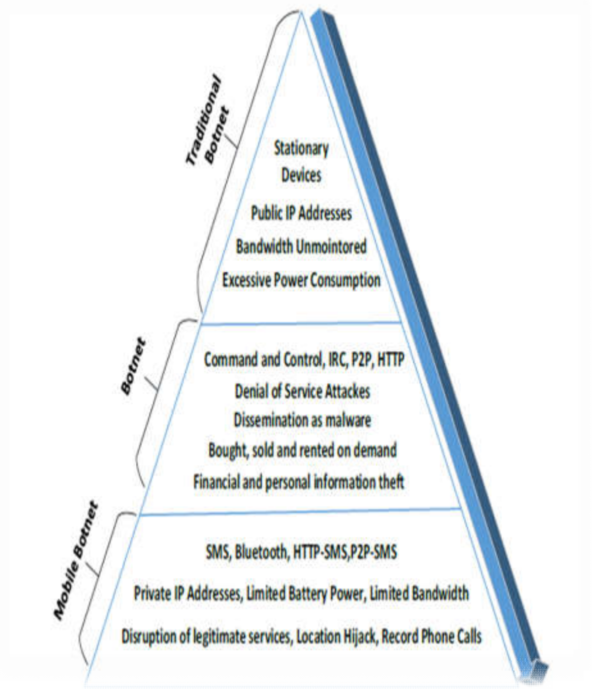
Traditional Botnet
Stationary Devices
Public IP Addresses
Bandwidth Unmointored
Excessive Power Consumption
Botnet
Command and Control, IRC, P2P, HTTP
Denial of Service Attackes
Dissemination as malware
Bought, sold and rented on demand
Financial and personal information theft
Mobile Botnet
SMS, Bluetooth, HTTP-SMS,P2P-SMS
Private IP Addresses, Limited Battery Power, Limited Bandwidth
Disruption of legitimate services, Location Hijack, Record Phone Calls

Figure 2: Botnet on Smartphone

A. Different type of Mobile Botnet

Compared different type of mobile botnet and their impact on Smartphone.

Table 1: Mobile Botnet

Name	Propagation Method	Attack	Mobile OS
Zeus	Social Engineering, Infected SMS messages	Mobile Banking Attack, TAC thefts, Illegal Transaction	Symbian, Blackberry, Android
DroidDream	Exploit Techniques, Trojanized Application	Theft of Private Data, Download Malicious Application	Android
SmartRoot	Exploit Techniques, Trojanized Application	Revenue generation, Theft of Private Data	Android
AnserveBot	Social Application, Trojanized Application	Theft of Private Data	Android
IkeeB	Self-Propagation	Revenue generation, Theft of private Data	Android
TigerBot	Trojanized Application	Theft of Private Data, Change Device Setting	Android
RootSmart	Exploit Techniques	Gain Root Access	Android

COMPARATIVE ANALYSIS

A. Botnet Categories

Compared Botnet Categories based on few key words: Structure, Strength, Weakness and Example.

Table 2: Botnet Categories

Type of Botnet	C&C Protocol Channel	Structure	Strength	Weakness	Example
IRC	IRC	Centralized	Flexible, Low latency communication	Collapsed once the server is shutting down	GTBot, SpyBot, SDBot, AgoBot etc.
P2P	P2P, Self-defined	Decentralized/ Distributed	Free from single point failure	High latency communication	Nugache, Storm etc.
HTTP	HTTP	Centralized	Bot hide their communication flows in the HTTP traffic	Collapsed once all botnet shutting down	ClickBot etc.
Mobile Botnet	SMS	Tree topology	Difficult to detect bot	Require a node list to be operate	IkeeB, SoCelBot etc.
Social Networking Sites	HTTP, IRC, P2P	Decentralized/ Distributed	Stealing personal information	Proper botnet detection approach should be used to detect bot.	SocialNetworking Bot, StegoBot.

B. Botnet Detection Techniques

Compared botnet detection approaches based on key features like Unknown bots, Botnet protocol and structure, Botnets with encrypted C&C channels, real-time detection, and accuracy.

Table 3: Botnet Detection Techniques

	Unknown Bot Detection	Protocol & Structure Independent	Encrypted Bot Detection	Real-time Detection	Low-False Positive
Signature-Based Detection	NO	NO	NO	NO	NO
Anomaly-Based Detection	YES	NO	YES	NO	YES
DNS-Based Detection	YES	YES	YES	NO	YES
Mining-Based Detection	YES	YES	YES	NO	YES

CONCLUSION

There are various botnet detection techniques available with very low false positive rate but no technique is capable of detecting bots in real-time. Also, mitigation and defensive techniques are ineffective given the advanced developments in botnet capabilities.

REFERENCE

[1] Reema Sharma,Deepshikha."Social Networking Sites: A New Platform for Botnets A short Case Study to prove that how today's Social Networking is a New Platform for Cyber Criminals", International Journal of Emerging Technology and Advanced Engineering, Volume 4 ,Special Issue 1, February 2014.

[2]A.Karim ,Rosli Bin , Muhammad S. , Syed Adeel Ali Shah, Irfan AWAN, " Botnet Detection Techniques: Review, Future Trends, and Issues", Journal of Zhejiang University-SCIENCE C(Computer & Electronics),Oct.2014.

[3]Maryam Feily, AlirezaShahrestani, SureswaranRamadass,"A Survey of Botnet and Botnet Detection",International Conference on Emerging Security Information, Systems and Technologies IEEE, 2009

[4]Amirmohammadsadeghian, MazdakZamani," Detecting and Preventing DDoS Attacks in Botnets by the Help of Self Triggered Black Holes", Asia-Pacific Conference on Computer Aided System Engineering, 2014

[5] Pierce M Gibbs,"Botnet Tracking Tools", GIAC (GSEC) Gold Certification, August 2014

[6] Lei Liu,songqing chen, Guanhua Yan and Zhao Zhang,"BofTracer: Execution-bassed Bot-Like malware Detection",Department of Electrical and Computer Engineering,2011.

[7] Muhammad Mahmoud, Manjinder Nir and Ashraf Matrawy,"A Survey on Botnet Architectures, Detection and Defences", International Journal of Network Security, Volume 17, Number 3, PP.272-289, May 2015.

[8] Hien T. Nquyen, Huiling Zhang," Mointoring Placement To Timely Detect Misinformation In Online Social Networking", IEEE ICC SAC Social Networking, 2015.

[9] Ashutosh Singh , Annie H. , Kevin R. ,Mark S. ," Social Networking for Botnet Command and Control", Modern Education and computer Science Press , I.J.Computer Network and Information Security,2013.

[10] Shishir Nagaraja, Vijit Kumar, Pragya Agarwal and Nikita Borisov,"Stegobot: A Covert Social Network Botnet", Indraprastha Institute of Information Technology, 2011.

[11] Sazzadur Rahman, Ting-Kai, Harsha V and Michalis Faloutsos,"Detecting Malicious Facebook Application", IEEE/ACM TRANSACTIONS ON NETWORKING, PP 1063-6692, 2015.

[12] Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar,"MoBots: A New Generation of Botnets on Mobile Devices and Networks",International Symposium on Computer Application And Industrial Electronics (ISCAIE),2012

[13] Heloise Pieterse, Martin S Olivier,"Android Botnets on the Rise: Trends and Characteristics", Computer Science Society, 2012.