Botnets and the Threat to Network Security and Social Network Integrity

FORI BARKA TATAMA[1], MAIKORI JENOM[2], ONU EGENA[3], LAWAL IBRAHIM[4], IPOLE-ADELAIYE NANCY[5]

[1, 2, 3, 4, 5] *Department of Computer Science, Bingham University, Karu, Nasarawa State, Nigeria.*

Abstract- ***Botnets or Bots are a menace to cyber-security and social integrity, they are several computing devices that are remotely controlled by an attacker to carry out malicious acts. They are used to carry out several attacks and deceitful acts on social networks to scam several people online from faking number of followers, number of likes on social networks. On a larger scale, botnets are used for setting off distributed denial of service attacks which is very dangerous for any business that falls victim to this attack, several business services are lost during these attacks which in turn leads to loss of money. Botnets takes two stages to form, first is the creation stage, in this stage the attacker creates a virus responsible for infecting computers and recruiting them to the network, this virus can be created from scratch or in certain cases the source code is gotten online and edited to suite the new purpose, after the development of the virus is completed we then proceed to the propagation stage which is the stage where a virus infects the computer being recruited to join the network, when the computer is infected and recruited the propagation continues to other computers till a vast network is created and ready to attack. Once several computers have been recruited as part of the botnet, the botmaster can proceed to rally the botnet to carry out attacks like distributed denial of service attacks, click fraud and identity theft, and other social network attacks like hashtag hijacking, trend jacking or click farming. These attacks are always dangerous for people or victims that are affected as it could lead to their identities being stolen or losing business services for long time. Due to the difficulty of detecting botnet attacks and difficulty in getting rid of botnets several techniques have been designed to detect botnet attacks, one of which is the honeypot technique, this technique means the use of traps to lure out the botnet to observe strange trends and patterns, these patterns are then use to the inform security personnel on the decision to take to prevent the botnet from carrying out attacks that drops business services.***

Indexed Terms- ***Botnet, Malware, Cybersecurity, Social Networks.***

I. INTRODUCTION

The rapid growth of the internet and importance of the internet and computer networks in daily activities and businesses has also led to the raise of bad actors that leverage the internet with malicious intent. These attacks range from a spamming, key logging and denial of service. Botnets or Robot Network is a modern type of cyber security threats, it involves the process of recruiting infected computing devices to carry out attacks on behalf of the botmaster (Hadianto & Purboyo, 2018).

Once a computer is recruited into the botnet it becomes a slave for the botmaster and carryout the purpose of the botmaster without the knowledge of the device owner. This infection spreads from one device to newer devices and this creates a vast network that can carry out massive attacks like distributed denial of service attacks (DDoS), spamming, cyber bullying, click fraud and other forms malicious attack (Tariq Banday & Qadri, 2009).

The attacker leverages several methods of infecting computing devices like phishing and compromised pirated software. When a device is recruited it becomes difficult to detect and uses more computing resources to carry out the tasks of the botmaster. One of such tasks is manipulating social media metrics to either boost an item on the internet, like website

visits, image likes, videos and so on, this goes a long way to manipulate several metrics that informs what get served to users on the internet as the more visits a website gets the more search engines tend to recommend it (Allan Liska, 2014).

The raise of botnets has led to the raise DDoS attacks and people paying attackers to boost the metrics of their social media content and other internet-based metrics. Due to deception of botnets and other dangers related to botnets techniques have been developed to properly detect botnets with major techniques being Honeynet detection and Intrusion detection which will be discussed in later sections of this study.

A. Entities Of A Botnet

A botnet is typically made of entities that carry out the attacks on the victim and they:

1. The Botmasters: these are the devices in charge of rallying the recruited bots in the network to carry out an attack, they are normally manned by a human attacker that orchestrates the entire attacks.
2. The handlers: these are communication devices and channels used by the botmaster to communicate with the bots on the network, this makes the attacker difficult to trace as there is no direct communication the botmaster and bots.
3. The bots: these are the infected systems that are rallied to carry out the botmaster's attacks. They are first infected and wait for the botmaster's command through the handles on what malicious attacks to carry out (Barse & Tidke, n.d.).

B. Botnet Creation

The first stage of creating a botnet is when the attacker develops the virus to infect computing devices by writing the program from scratch or by forking an existing project on platforms like github.com, these projects mainly hosted for educational purposes can be used by attackers for malicious intent. This makes it very easy for people with little technical knowledge to develop and deploy a botnet. The software holds software about port information, directory of the stored infected software on the bot system, credentials of botmasters and commands for the virus to hide itself from antivirus. The virus leverages several Command-and-Control methods to instruct the botnet on how to carry out attacks (Tariq Banday & Qadri, 2009).

C. Botnet Propagation

At this stage the infected computing devices are used to spread the infection over HTTP, FTP or TFTP protocols to grow the botnet to a level where it can create problems for victims. This propagation stage is usually achieved by the attacker using vulnerabilities in software or through infected pirated software. This infection can be spread through peer-to-peer networks using torrent, file sharing or direct download. When enough devices have been infected, they wait for commands from the botmaster to carry out the instructed attacks(Tariq Banday & Qadri, 2009).

D. Major Botnet Attacks

Botnets are serious threats to network security and having services running normally for delivering business needs, some major threats the botnets pose to cyber-security are Distributed Denial of Service attacks, click fraud and identity theft.

1. DDoS using Botnets: This is a form of attack where the computing system is overwhelmed by requests from an attacker or attackers that it can no longer service legitimate requests sent to it. With a botnet a botmaster can rally several computers to send many requests to the victim computer, in the process reducing the bandwidth necessary for providing necessary business requirements and other important computational services. Botnets are efficient at carrying this form of attacks because removes the need to spoof or fake IP address of the bots since in the case of a botnet the bots are real computers with their IP addresses (Anwar et al., 2014).

This attack goes a long way to affect daily business proceedings and in turn leads to financial loss. Businesses also must spend extra resources to reduce the chances of being attack by DDoS via botnets.

2. Click Fraud: One major use of botnets if to fake engagements, this can be advert engagement or social media engagement. Some advert companies pay subscribers based on the amount of engagement the advert gets and, in most cases, the

preferred form of engagement is clicks and this can be faked by a botnet where the botmaster orders the botnet to repeatedly click and advert and generate revenue for the attacker without really engaging with the product. This also give the advert company a false image of user engagement with the product, thinking it has wide reach not knowing its interactions are mostly fake (Zhang et al., 2016).

3. Spamming and Identity Theft: A person's IP address is their identity on the internet, computing device is recruited to a botnet they are also assuming the identity of the owner of computer and can get access to their contact list and spam their contact with phishing mail or malware to expend the botnet, in other cases they can sell the data on the dark web for other malicious activities. Platforms like twitter have and continue to struggle with fake accounts run by botnets, these accounts assume the identities or real people with images but with the intention of scamming people out of money or hijacking their account into the botnet (Hadianto & Purboyo, 2018).

Social Botnets on Social Media integrity

Social is a place where people and businesses share their thoughts, ideas, and time, for businesses, time spent on social media is mainly to promote their products and increase sales. The reliance on social media for communication and to get products in front of customers has made it a major target for bad actors. These bad actors range from social engineering scammers, spammers and botnets, botnets are notorious on social networks because they can be used to falsify social media metrics (Zhang et al., 2016). Botnets can be used to gain fake views to make an item or post seem more popular than it is, it can also make people seem more credible than they are. The botnet attacks are vast on social networks, but the overall target is to leverage the vast number of users on social media and the need to be aware of rapidly shared in certain cases unverified information. The fast create and consumption nature of social networks makes it easy for botnets to hide in plain sight by impersonating real people or promoting whatever the botmaster decides to promote. Amongst the numerous malicious activities of botnets here are the most common botnet social media attacks and they are:

1. Hashtag Hijacking: Hashtags are methods of identifying digital content on social network platforms especially twitter, when a hashtag gains high traction, it leads to having the topic trending, this could be used for advert campaigns which could make products popular. Hashtag hijacking is when a botmaster uses the botnet to target certain groups or organizations, by leaching onto their hashtag and promoting malicious links and content. The information being promoted will be linked to the organization that promoted the hashtag and the botnet will hijack the hashtag and in turn get some their customers to click the malicious links(Zhang et al., 2016).
2. Trend-jacking: Like hashtag hijacking, trend-jacking looks at current hot topics on social media and the attacker plants their trap within the context of the trending topics and waits for clients to fall for the bait. Trend-jacking guarantees a higher pool of potential victims as trends normally have high traction to begin with. When a botnet is trend-jacking it might also make the trend seem bigger than it is (Foster, 2015).
3. Click Farming: This is one of the most used botnet attacks on social media integrity, this is situation where people or organizations buy "followers" on social media that are not real users but botnets, these botnets can also be used to click links making them go viral, "like" a person's post and make that post reach more people thinking it has genuine "likes". This is often used by scammers to gain the trust of their victims since people often believe that people with more "followers" or "likes" is credible and can be trusted by the public (Barse & Tidke, n.d.).
4. Spray and Pray: This is derived from the shotgun gaming lingo where you shoot and hope the enemy is affected. In this case the botnet they post several malicious links; the spray, hoping any of the links get clicked; the pray. In this attack the, the attacker only needs one or two links to be clicked and they can proceed to stealing user data or spreading the botnet virus (Foster, 2015).

E. Botnet Detection

Botnets pose a huge danger to cyber-security, from DDoS attacks, trend-jacking, click fraud to click

farming botnets are notorious for these attacks and due to their peculiar nature and behavior there are two main techniques for detecting botnet activities. Social network companies and security agencies can adopt these detection techniques to blacklist their IP address and accounts to reduce the effect of the botnet. The two techniques are honeypot technique and intrusion detection.

F. Honeypot based detection

Honeypots are vulnerable systems that are used to lure a botnet to make their attacks, when the botnet attacks and tries to recruit the honeypot system the malware from the botmaster then retrieved and studied to learn how the botnet behaves (Seungjin et al., 2020). This technique can also be used on social media where certain posts can be used to lure out botnets that try to trend-jack or hijack a hashtag, when the post has unnatural behavior the social network company can lean in to suspend suspicious accounts relating to the post that served as the honeypot. Social media companies also employ moderators that can also read through distinct content or suspicious accounts that post content that can be used lure users to loosing their accounts or spending money against company policies.

With respect to cyber-security, there are three types of honeypot strategies companies employ and they are:

1. Low-interaction honeypot: These are easy to implement and uses two sandboxes to analyze the activities of a connecting devices without allowing the attacker to gain control of the honeypot, but services and necessary protocols are emulated to deceive the botnet, captures the attempts and notifies the relevant security agencies if any notorious behavior is observed (Seungjin et al., 2020; Wang et al., n.d.).
2. High-interaction honeypot: This is a bit more difficult to implement because the attackers are given full access to the honeypot, this gives the attackers more confidence to act naturally without any suspicion that they are being monitored and observe by security personnel. The attacker is then monitored, and behavior recorded for further study of the botnet patterns.
3. Honeytoken: Unlike the previously mentioned honeypot techniques that are service, and network based this technique is file based where a file containing fake data that is inaccessible by legitimate users. This file is made to be attractive to attackers like login credentials and credit card information. When the bots download such files, they are suspended till investigation is completed (Barse & Tidke, n.d.; Wang et al., n.d.).

G. Intrusion Detection System (IDS)

This technique monitors the traffic monitors the flow of data and traffic searching for malicious network activities, if any strange trends are observed by the Intrusion Detection System the security personnel are notified to take the proper actions. There are two IDS botnet detection techniques, there are:

1. Anomaly Based Detection: This is metric based system that checks for behaviors outside the normal expected behavior within the network, an example is getting frequent connections from a particular address and some security systems will find this to be anomaly and trigger a captcha asking the user to prove they are human (Barse & Tidke, n.d.; Hadianto & Purboyo, 2018).
2. Signature Based Detection: The signature-based intrusion detection system is a bit simpler to implement, this method needs the security personnel to know the signature of the attacker and watch out for the signature in the malware data packet and triggers the security system to blacklist the attacker (Barse & Tidke, n.d.).

H. Machine Learning

The raise of big data has also brought the raise of machine models that can detect patterns from data and give insight on the data.

II. RESEARCH FINDINGS

After studying the literature presented in previous sections of this study, we noticed a great increase in detecting botnets which includes the use of IDS and the honeypot techniques. In the case of IDS detected botnets captcha is used to perform further verification to show the person is human while the honeypot technique can be trusted enough to suspend attackers till further action is needed. In situations of DDoS attacks scaling up the service to frustrate the attacker can be the best option this till proper prevention techniques is gotten stop this type of attack. DDoS

attacks are a major type of botnet attacks, and this could be a major problem for business and botnets make them very dynamic and very difficult to detect and address (Brezo et al., 2011; Kaur Chahal et al., 2019).

On the social network attacks, it was observed that honeypots work well as most attackers can be drawn out using a chance to hop on a trend or person of influence. This is also not fool proof and is susceptible to a lot of false alarms and can get a lot of innocent real people being punished. Besides honeypot and IDS techniques, machine learning techniques are also being used to study the behavior of botnet attacks and adapt to their changes to keep up with the dynamic nature of botnets (Limarunothai & Amin Munlin, n.d.).

There is no definitive way to detect and address botnets as more research and studies are still being carried out in this field and so far, machine learning and artificial intelligence has shown promises for long term sustainable botnet detections.

Existing Challenges to Preventing Botnet Attacks

The solution to botnets is being heavily researched by top technology companies like Twitter, CEO of Twitter has made fighting bots on the platform his primary objective and like many companies and researchers they have faced their own challenges. After the study of several literature on botnet attacks, types and detection techniques several challenges are highlighted and reported by several researchers that are summarized into following challenges:

1. Dynamic nature of Botnets: One of the IDS techniques is anomaly-based detection, one of the major challenged posed here is the issue being there is no way of telling if an activity is actually and attack or a legitimate event. Users on slow internet services will tend to refresh often and this might trigger a captcha verification which is a false alarm and might frustrate the user to leave the website. The dynamic nature of botnets makes it difficult to detect or identify as we might have our suspicion but not real evidence in most cases to say the attack is real. This is the major research challenge of botnets, this dynamic nature of botnets leads to false alarms, obsolete detection techniques and eventually high business expenses trying to combat the botnets (Brezo et al., 2011; Limarunothai & Amin Munlin, n.d.).
2. BotCloud: This is a technique used by botmasters that leverage the scalability of the cloud to create a botnet that scales to large extents and are always active and online to carry out attacks, this is challenge as scaling up servers and computing power might be too expensive for the researcher and small businesses. Accommodating the attacks is also difficult as the attacks might carry out a DDoS attacks that scales beyond the available business resources (Kaur Chahal et al., 2019).
3. Mobile Botnets: Mobile devices have exploded in adoption and usage as most internet users access information via smart phones, the diverse natures of mobile phones have created a major challenge for researchers as one solution does not in most cases work for the vast number of mobile device types and platforms available (Brezo et al., 2011).

CONCLUSION

There is no denying the dangers posed by botnet to cyber-security or internet integrity. With the growth of internet coverage and users has also brought about the increase the number of bad actors that attempt to expand their reach using sophisticated tools techniques like botnets. From the findings of this study, it is obvious that botnets pose a huge challenge to businesses and individuals, and this has led to a lot of research in this domain and while progress is being made the dynamic nature and range of possible attacks posed by botnets makes it very difficult to detect and address this issue. These botnets impersonate real people and carry out attacks on behalf of the attack, this makes the botnets difficult to detect and allows them to fake social media user interaction which can affect businesses and help perpetuate scams. With easily accessible botnet code on the internet the raise of this type of security threat is ever increasing, this has led to the need to detect anomalies and block malicious actors, though the methods are not perfect they have come a long to reducing the effect of botnets.

REFERENCES

[1] Allan Liska. (2014). Building an Intelligence-Led Security Program (1st ed.).

[2] Anwar, S., Zain, J. M., Zolkipli, M. F., Binti, J., Zain, M., Fadli, M., Zulkipli, B., & Inayat, Z. (2014). A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing New chaos RADG cryptographic algorithm View project Android Device Security View project A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing. https://www.researchgate.net/publication/283257776

[3] Barse, Y., & Tidke, S. (n.d.). A Study on BOTNET Attacks and Detection Techniques. Issue 3 Ser. II, 15, 1–05. https://doi.org/10.9790/1676-1503020105

[4] Brezo, F., Santos, I., Bringas, P. G., & del Val, J. L. (2011). Challenges and limitations in current botnet detection. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 95–101. https://doi.org/10.1109/DEXA.2011.19

[5] Foster, J. (2015, July 7). The rise of social media Botnets. Https://Www.Darkreading.Com/Attacks-Breaches/the-Rise-of-Social-Media-Botnets.

[6] Hadianto, R., & Purboyo, T. W. (2018). A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking. In International Journal of Applied Engineering Research (Vol. 13, Issue 1). http://www.ripublication.com

[7] Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed Denial of Service Attacks: A Threat or Challenge. In New Review of Information Networking (Vol. 24, Issue 1, pp. 31–103). Routledge. https://doi.org/10.1080/13614576.2019.1611468

[8] Limarunothai, R., & Amin Munlin, M. (n.d.). Trends and Challenges of Botnet Architectures and Detection Techniques. In JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY (Vol. 5).

[9] Seungjin, L., Abdullah, A., Jhanjhi, N. Z., & Jaya, S. (2020). A Review on Honeypot-based Botnet Detection Models for Smart Factory. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 11, Issue 6). www.ijacsa.thesai.org

[10] Tariq Banday, M., & Qadri, J. (2009). Study of Botnets and their threats to Internet Security Book captioned "Cryptographic Security Solutions for the Internet of Things" to be published by IGI Global, USA View project. http://sprouts.aisnet.org/9-24

[11] Wang, P., Wu, L., Cunningham, R., & Zou, C. C. (n.d.). Honeypot Detection in Advanced Botnet Attacks. In Int. J. Information and Computer Security: Vols. x, No. x (Issue x).

[12] Zhang, J., Zhang, R., Zhang, Y., & Yan, G. (2016). The Rise of Social Botnets: Attacks and Countermeasures. http://arxiv.org/abs/1603.02714