Reviewing the Current Threat Landscape of Botnets

Created by: Emmanuel C. Ogu
Version received: 20 April 2020

Botnets have been around for about three decades, and their sophistication and capabilities have evolved rapidly over the period. Originally simple codes that were used for the administration of IRC channels, botnets today pose very formidable threats to systems and network infrastructure. They have become one of the more-preferred options in the toolkit of hackers and cybercriminals; particularly due to their ability to subvert and overrun secure infrastructures within a relatively short time.

Research has greatly advanced in trying to keep up with the rapid evolution of the botnet threat. At this time, it is important to review the status of the threat, *vis-á-vis* the extent of research that has emerged in relation to the threat. This is crucial for understanding the future prospects of the threat, in terms of where it is headed next; as well as what research areas require more work.

This exploratory research serves this purpose. It introduces the botnet threat from its early origins; then it traverses the current status of botnets, and summarizes research efforts so far (highlighting some limitations of modern countermeasures). It further goes on to discuss the future trends of botnets and botnet research, before bringing it together to present the current threat landscape.

Introduction

Essentially, botnets are a network of compromised systems that are coordinated by a single channel for purposes that are often criminal. They generally feature a *bot herder* who controls the activities of the botnet; a *bot code* that is the malware used to hijack and enlist new machines; a *command and control (C&C) infrastructure* that provides the coordination and instructions for the botnet activities; and then the compromised machines themselves that are known as *the bots or zombies* [1].

In general, bot herders are able to evade detection using stepping-stones and surrogacy; bot controllers achieve the same objective through encryption methods; the bots, on the other hand, would adopt techniques of binary obfuscation, anti-analysis, security suppression or rootkit technology to hide their network presence; while the C&C servers & communication traffic evade detection by using IP & domain fluxes, rogue servers, anonymisation, encryption, and protocol and traffic tweaking, to mention a few [2].

But then, Botnets were not always malicious in their operations. They began as automated tools for administering large IRC chat rooms over remote channels. Today, however, they have been found to be engaged in various forms of attacks against Mobile Ad-hoc networks (MANETs), Voice over IP (VoIP) infrastructures, Autonomous Vehicular Networks (or Vehicular Ad-hoc Networks [VANETs]), as well as traditional TCP/IP and UDP network infrastructures [1].

The activities of botnets have featured denial of service (DoS) attacks, stock market frauds, data theft, various other financial crimes. They are particularly preferred by cybercriminals because they help to obfuscate their actual identities; especially in the era of stringent cybercrime legislation and cross-border coordination by several nation states for cybercrime prosecution.

However, the attackers who own botnets could be of various types. They could be *Hackers/Skilled Individuals* with limited resources; *Hacker Groups* with more coordinated skillset, objectives, and resource; or *Government/Nation-state Actors* with vast amounts of resources.

Current Status of Botnets

Today, we see botnet attacks displaying synchronous and asynchronous properties for coordination and control. While *Synchronous Botnets* rely on coordinated commands issued by botnet owners through central C&C servers, *Asynchronous Botnets* are self-sufficient units that carry their attack commands within their code binaries and do not rely on central command and control.

Botnet command and control architectures could be Direct, Centralized, Peer-to-Peer (P2P), or Hybrid. *Direct C&C* involves bot owners coordinating and instructing each bot in the botnet individually, irrespective of the size of the botnet. *Centralized C&C* relies on a C&C server as a central rendezvous for coordination and instructions for the botnet. *P2P C&C* is a sophisticated architecture that is decentralized; where individual bots are also able to provide control and coordination information for other bots in the botnet. *Hybrid C&C* tend to integrate one or more unique features / characteristics of the direct, centralized and P2P architectures; combining their individual advantages to create a more powerful command and control infrastructure.

Three stages characterize the lifecycle of botnets [3]:

1. At the *infection / doping stage*, vulnerabilities in machines are exploited using bot codes released into networks by attackers. Several techniques could be applied at this stage; including active procedures such as scanning, flooding, war driving and injection, or physical trans-loading/infusion, as well as passive procedures such as drive-by downloads, trans-loading from various removable media, or social engineering, emails, ads, cloned URLs, games, and bugged/pirated Software.
2. Then, the *recruitment and rallying stage* follows, where successfully compromised machines rallied for further instructions by the attackers. Techniques featured here include hard coded or generated Domain Name Services (DNS) commands; or hard coded IP Addresses
3. Finally, the *synchronization and reporting stage* would see new members of the botnet receive command and control instructions for their actions, and then reporting periodically on their activities via the same medium.

However, similar to this forward lifecycle is a reverse lifecycle, where a botmaster (who may not actually be the original owner of the botnet) might randomly release bot codes on the internet to re-infect previously previously compromised machines that may have been dislodged from other botnets, abandoned by their botmasters, or cut-off from a command and control source. These machines can be re-infected and reverse-rallied to a new command and control source to join a new botnet [3].

In addition, there are several types of botnets that have emerged in modern times. *Spam Botnets* are used to send millions of spamware daily, in an attempt to compromise machines via email. *Information Gathering / Reconnaissance Botnets* are used to mine information from the open Internet in large quantities. *Identity Theft Botnets* steal private user identity and information for fraudulent aims. *Click-fraud Botnets* mimic legitimate click-ad behaviors to amass revenue for cybercriminals through fraudulent click-advertisement web traffic. *Crypto Botnets* mine crypto currencies and resources for financial gains.

Botnet Research Efforts so far

The broad goals of research efforts towards countering botnet activities focus on *Prevention* – increased chances / possibility of averting the occurrence of a botnet attack; *Detection* – accurately spotting the presence of a botnet activities in a network; *Offense* – launching counter-attacks against botnets and other intrusion elements to take them down; *Reconnaissance* – monitoring botnet activities on a network, to gather useful information about their operation; and *Mitigation* – controlling and curtailing the extent of the damage to the network and hosts by a rampaging botnet.

Botnet countermeasures so far can be grouped as follows. *Spoofing* countermeasures aim to compromise certain parameters of the bot code, so that they are unable to return the results desired by the botmaster. *Analysis-based* countermeasures often use custom honeypot and darknet configurations to analyze network traffic in real-time to detect trends that reflect what is already known about botnet activities, using either signature-based or anomaly-based approaches. *Mining-based* countermeasures deploy data mining and machine learning models to deduce insights into botnet activities from already-acquired botnet data from networks.

However, spoofing and analysis-based countermeasures have sometimes been ineffective in detecting polymorphic botnets that are able to change their form, structure, and trail of operations across different outsets of the botnets. This is owing to the extent to which they typically rely on already known information about strains of existing botnets.

Future Trends of Botnets and Botnet Research

The advancements in mobile computing, combined with the growing proliferation of mobile devices presents a viable future landscape for botnets with wider prospects of reach. Already, there has been a growing popularity of botnets that have particularly focused on attacking popular mobile operating systems; such as the Symbian Java (Symbian/Yxes worm of 2009), the IoS (iKee.B botclient of 2009), and the Android (Geinimi malware of 2010) [4].

Traditional and mobile cloud environments also provide promising prospects for botnets to enhance their strength, ubiquity, patronage and coverage through a new paradigm known as botnets-as-a-service. In addition, with the dawn of the Internet-of-things and capabilities for cognizant computing, mobile and cloud botnets of the future would be able to learn and exploit vulnerabilities in the patterns of user interactions and operations, and then modify /re-configure themselves accordingly for more sophisticated attacks. In effect, botnets of the future might develop their own artificial intelligence by exploiting the capabilities of big data.

Also, as mobile computing continue to expand in terms of speed and computational power through the advances in 4G/LTE and 5G, botnets in this environments would be able to leverage such capabilities to amplify the efficiency of their activities with respect to speed and time.

Bringing it All Together

Based on the foregoing, Figure 1 summarizes the current threat landscape of the botnet threat.

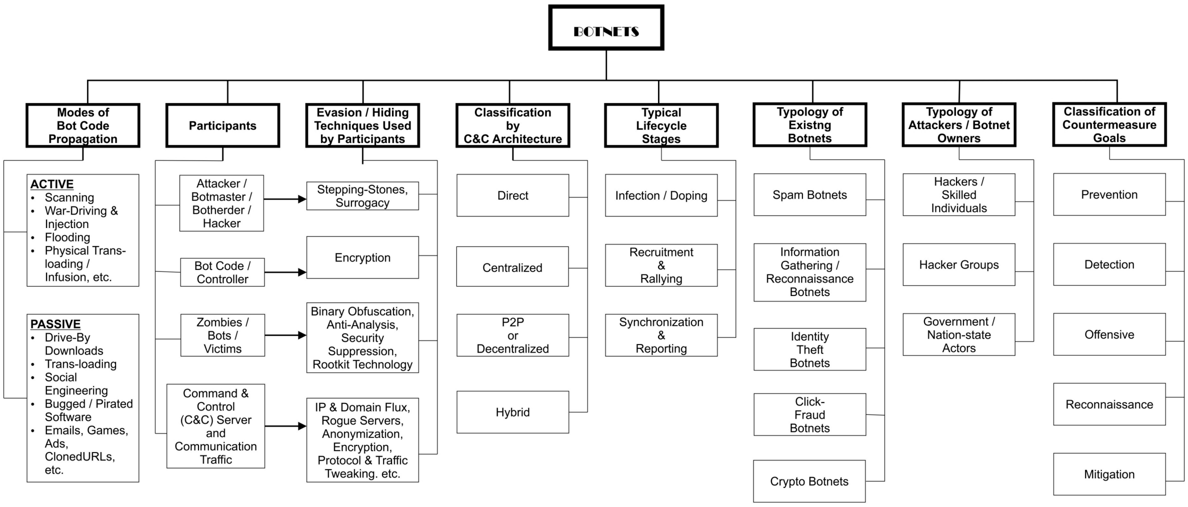
BOTNETS
Modes of Bot Code Propagation
Participants
Evasion / Hiding Techniques Used by Participants
Classification by C&C Architecture
Typical Lifecycle Stages
Typology of Existng Botnets
Typology of Attackers / Botnet Owners
Classification of Countermeasure Goals
ACTIVE
• Scanning
• War-Driving & Injection
• Flooding
• Physical Trans-loading / Infusion, etc.
PASSIVE
• Drive-By Downloads
• Trans-loading
• Social Engineering
• Bugged / Pirated Software
• Emails, Games, Ads, ClonedURLs, etc.
Attacker / Botmaster / Botherder / Hacker
Bot Code / Controller
Zombies / Bots / Victims
Command & Control (C&C) Server and Communication Traffic
Stepping-Stones, Surrogacy
Encryption
Binary Obfuscation, Anti-Analysis, Security Suppression, Rootkit Technology
IP & Domain Flux, Rogue Servers, Anonymization, Encryption, Protocol & Traffic Tweaking. etc.
Direct
Centralized
P2P or Decentralized
Hybrid
Infection / Doping
Recruitment & Rallying
Synchronization & Reporting
Spam Botnets
Information Gathering / Reconnaissance Botnets
Identity Theft Botnets
Click-Fraud Botnets
Crypto Botnets
Hackers / Skilled Individuals
Hacker Groups
Government / Nation-state Actors
Prevention
Detection
Offensive
Reconnaissance
Mitigation

***Figure 1*: The Current Botnet Threat Landscape**

As we expect to see botnets become even more sophisticated in the near future, further research is needed to unpack the internal workings of botnets that especially feature the decentralised/P2P control architecture. This remains one of the known formidable features of modern botnets, and botnet owners and attackers are expected to begin exploring technologies such as blockchain and advanced cryptography towards hardening these nefarious control structures and making them more impervious.

In addition, the exposition of the reverse lifecycle of botnets necessitates future research to explore the covert backdoor channels that help preserve the subsistence of botnets by acting as “open doors” for their reawakening. As modern approaches to sinkholing and darknet implementations continue to reveal valuable information regarding botnets and their key survival features, future research directions should hone these findings and provide robust insights that would help terminate the reverse lifecycle of botnets.

Furthermore, in the wake of brewing political tensions on the global scene, and fears of politically-motivated cyber-attacks, it is also crucial for future research to explore the power and operational dynamics that characterize the different types of attackers who own and control botnets. This is likely to lead to the discovery of new threat and attack categories/classes that would help the security community to better understand the distinguishable characteristics of cyber threats and attacks on a broader scale.

References

1. Ogu, E. C.; Ojesanmi, O. A.; Awodele, O.; & Kuyoro, S. O.; A Botnets Circumspection: The Current Threat Landscape & What We Know So Far. *Information* **2019**, *10(11)*, 337, https://doi.org/10.3390/info10110337.
2. Khattak, S.; Ramay, N. R.; Khan, K. R.; Syed, A. A.; & Khayam, S. A.; A taxonomy of botnet behavior, detection, and defense. *IEEE Communications Surveys & Tutorials* **2013**, *16(2)*, 898-924, https://doi.org/10.1109/SURV.2013.091213.00134.
3. Ogu, E. C.; Vrakas, N.; Ogu, C.; & Ajose-Ismail, B. M.; On the Internal Workings of Botnets: A Review*International Journal of Computer Applications* **2016**, *138(4)*, 39-43, https://doi.org/10.5120/ijca2016908797.
4. Anagnostopoulos, M.; Kambourakis, G.; & Gritzalis, S.; New facets of mobile botnet: Architecture and evaluation. *International Journal of Information Security* **2016**, *15(5)*, 455-473, https://doi.org/10.1007/s10207-015-0310-0.

Keywords

Cybersecurity; Information Security; Botnets; Cybercrimes; Network Security; Threat Landscape