Peer-to-Peer Botnets Taking Over the New Voronoi-Overlay

Joseph Montgomery
Research Experience for Undergraduates 2010
Utah State University

Abstract— **Peer-to-peer (P2P) botnets are the latest mutation of a plague that threatens every computer with access to the internet. The security community is inherently one step behind botnets with every new permutation seen in the wild. With recent research into employing a Voronoi overlay for P2P Networked Virtual Environments (NVE's) and Massively Multiplayer Online Games (MMOG's), the security community needs to adopt a forward-thinking approach to defending against new strains of P2P botnets and anticipate how these new Voronoi-based P2P networks may be utilized as a backbone for botnets. This paper proposes a modification to a current Voronoi-based NVE simulator to study the effects of a botnet infestation using this new technique.**

Keywords: P2P Botnets; security; Voronoi overlay;

I. Introduction

The world has become a smaller place because of the Internet. The Internet has connected people and ideas in a way that has never before been done. The amount of information and knowledge that is at our fingertips would be incomprehensible to people 100 years ago. In such a relatively short amount of time, the ability to communicate has increased exponentially. Unfortunately many have recognized the potential to do harm and exploit this new technology for personal gains. Hackers have been sending out malicious applications such as viruses, trojans and worms for a long time and for various reasons. The botnet is the latest evolution of malware today and poses the biggest threat to anybody that uses the Internet.

A botnet is a collection of infected computers, called "bots", that will do the bidding of the botmaster, which is the person that controls the botnet [1]. Computers can unwillingly become infected bots through any number of ways, whether by a direct attack on a specific vulnerability that is detected on the host system, or by social engineering through means of innocent-looking e-mail attachments or links. Botnets are dangerous because they are an effective tool in virtually every cyber criminal activity imaginable - identity theft, distributed denial of service (DDOS) attacks, click fraud, spam, etc. [2].

Botnets are generally accepted to have evolved from non-malicious bots developed to aid in the maintenance of Internet Chat Relay (IRC) servers. The most well-known of these early bots was known as *EggDrop*. Not long afterwards, the ability to automatically control hundreds of computers from a single location was exploited for monetary and political gains.

The original model for botnets followed the Command & Control model with a single server and several bot clients connecting to it [3]. This type of botnet is fairly easily mitigated since it offers a single point of failure for the entire botnet – the server. Botnets therefore have been moving to a P2P structure to become more resilient to defenses and further evade the security community. P2P Botnets are fairly new and most of the ones seen in the wild do not fully take advantage of the strengths of a true P2P network [4]. It is important that the security community anticipate the direction that botnets are heading in so that the world may be better prepared when the next generation of botnets is seen in the wild.

II. Related Work

There has been much research done in the areas of botnets and Voronoi-based networks. There is, however, a great lack of research in the area of botnets on Voronoi-based networks. Because Voronoi-based networks have very good potential for being widely used in NVEs and MMOGs, it is important to look ahead at how botnets might utilize this type of network for their own gains.

A. Botnets

There are many research projects that focus on giving an overview or case study on botnets. Cooke et al give a very broad report on botnets in general, including characteristics of several observed botnets and methods to mitigate those botnets [2]. This is a very helpful introductory report for those beginning research in the botnet field. A more recent report of this type was published by Liu et al and provides much of the same type of information, but with more recent occurrences of botnets found in the wild [3].

Grizzard et al offer a very comprehensive overview on P2P botnets, with a very in depth case study on a recent botnet called Peacomm [5]. Their research shows how botnets are evolving to avoid further mitigation and that they are doing so in the direction of P2P networks. Holz et al propose various methods to measure and mitigate some of the latest P2P botnets found in the wild at the time of their research [6]. They also offer an in-depth case study of the botnet StormWorm.

There is much research published on the topic of detecting botnet intrusions on networks because the nature of the security community is to react to strains of botnets found in the wild. Gu et al set a standard in this field of botnet research with their BotHunter software [7]. An improvement to their software is proposed by Sorensen et al [10]. Their research is more forward-looking in nature because they modify BotHunter to anticipate how it would detect a covert botnet. A covert botnet is one that purposely hides its actions inside a network so as to not appear as a bot to an edge-based detection system.

Going one step further than detection, Stone-Gross et al take the battle to the botnets by taking over the large botnet Torpig [8]. Torpig is a Command & Control botnet that uses a domain flux algorithm to constantly change the command server the bots will contact to get instructions from. The researchers hijack the botnet by anticipating what domain the bots will be contacting for a given period of time. Their research demonstrates the weaknesses of the C&C architecture and also shows the relative ease in which this type of botnet can be mitigated.

Starnberger et al break away from the reactive nature of the security community by proposing a stronger P2P network than what is presently found in the wild [4]. Their research is driven by the fact that most of the P2P botnets in the wild at the time of their research were relatively weak and did not utilize the strengths of P2P networks. Their demonstration is to present the community with a possibility of what P2P botnets can evolve into in the near future. This type of research is important because the security community needs to be prepared for the threats of tomorrow's botnets.

B. Voronoi-Overlay

There is also much research being done to apply a Voronoi-overlay to NVEs and MMOGs. Hu et al lay the groundwork for a Voronoi-based network by researching a scalable solution for MMOGs specifically [9]. Their work is added upon by Backhaus et al by making the Voronoi-based network more consistent [15]. Jiang et al also improve upon this design in much the same way [11]. More improvements to the architecture and P2P messaging are proposed through other research papers, making the Voronoi-based network a very real possibility for NVEs and MMOGs sometime in the not-too-distant future [12],[13].

Mathias is currently working on a simulator for a hybrid Voronoi-based network called Aubrey [14]. This network is hybrid because it uses a server for peers to log in to for security purposes. The current implementation of this simulation is contained in a single multi-threaded application that simulates the network and peers connecting to it. It does not produce any network traffic that can be captured or analyzed. The focus of Aubrey is to work out the mechanics and logic of the Voronoi-overlay.

III. Proposed Approach

The approach that this project takes is to modify the Aubrey simulator to simulate network traffic that can then be captured and analyzed. Once Aubrey uses network traffic, bots can then be introduced into the network for the purpose of finding what characteristics distinguish the infected peers from normal peers in the network. With that information, defenses can be put in place to prevent real botnet infections on future Voronoi-based P2P networks.

The method that this author intended to take was to have the messages sent back and forth between peers be handled by sockets. Aubrey is written in C#, which has built-in support for sockets. Each peer would be assigned a unique port (in the range of 49152 to 65535) to listen for messages on. When a peer wanted to send a message to another peer, it would first connect to the receiving peer's socket and then send the message over the network, addressed to "localhost" and the receiving peer's port. This would then create network traffic that can be captured and analyzed.

IV. Conclusions

Providing a platform to introduce and study botnets in a Voronoi-based network is important to defend against future botnets. Looking ahead at what botnets can become in the future gives the security community a leg up in the fight against botnets. This project will provide a tool that will provide valuable data to researchers interested in securing the upcoming Voronoi-based networks from future botnets.

V. Future Work

Work needs to be done to complete the network traffic simulation in Aubrey. Much of the supporting structure is there in the classes, but at present, there is no network traffic being generated when messages are sent among the peers in the network.

Beyond generating network traffic, the simulation should be modified to include infected peers. This would provide a chance to study the characteristics of bots inside a legitimate Voronoi-based P2P network. These characteristics and data can then be applied to making Voronoi-based networks in the future stronger against botnets from the get go.

Sponsors:
Chad Mano
Brandon Shirley

References

[1] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” in *Proceedings of the 6th ACM SIGCOMM Internet Measurement Conference (IMC 06)*, pp. 41–52, Rio de Janeriro, Brazil, October 2006.

[2] Evan Cooke, Farnam Jahanian, and Danny McPherson. The Zombie Roundup: Understanding, Detecting, and Disturbing Botnets. In *Proceedings of the first Workshop on Steps to Reducing Unwanted Traffic on he Internet (STRUTI)* , pages 39–44, July 2005.

[3] J. Liu, Y. Xiao, J. Zhang , ”Botnet: Classification, attacks, Detection, Tracing and Preventive measures” *URASIP journal of Wireless Communications and Networking*, Vol. 2009, article ID 692654, 2009.

[4] G. Starnberger, C. Kruegel, and E. Kirda, “Overbot - a botnet protocol based on kademlia,” in *Proc. of the 4th Int. Conf. on Security and Privacy in Communication Networks (SecureComm ’08)*, September 2008.

[5] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon. Peer-to-peer botnets: Overview and case study. In Proceedings of 1st USENIX Workshop on Hot Topics in Understanding Botnets, 2007.

[6] HOLZ, T., STEINER, M., DAHL, F., BIERSACK, E., AND FREILING, F. 2008. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. In Proc. 1st USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET) (San Francisco, CA). USENIX, Berkeley, CA, 1–9.

[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. In Proceedings of the 16th USENIX Security Symposium.

[8] B. Stone-Gross et al., *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, UCSB Tech. Rep., 2009

[9] S.-Y. Hu and G.-M. Liao. Scalable peer-to-peer networked virtual environment. In NetGames ’04: Proceedings of 3rd ACM SIGCOMM workshop on Network and system support for games, pages 129–133, New York, NY, USA, 2004. ACM Press.

[10] N. V. Sorensen, S. B. Sorensen, K. D. Feuz, G. Kerzhner and C. D. Mano. Detecting Covert Botnets Using Communication Patterns [unpublished]

[11] J.-R. Jiang, J.-S. Chiou, and S.-Y. Hu. Enhancing Neighborship Consistency for Peer-to-Peer Distributed Virtual Environments. In Proc. ICDCS workshops (CDS 2007), 2007.

[12] J.-F. Chen et al. A Forwarding Model for Voronoi-based Overlay Network. In Proc. P2P-NVE, 2007.

[13] S. Y. Hu, S. C. Chang, and J. R. Jiang. Voronoi State Management for Peer-to-Peer Massively Multiplayer Online Games. In *Proc. of the IEEE International Workshop on Networking Issues in Multimedia Entertainment*, 1134-1138, January 2008.

[14] D. Mathias. Audrey: A Hybrid P2P Approach for Massive Networked Virtual Environments [unpublished]

[15] H. Backhaus and S. Krause. Voronoi-based adaptive scalable transfer revisited: gain and loss of a voronoi-based peer-to-peer approach for mmog. In *Proc. of NetGames ’07*, pages 49–54, Melbourne, Australia, 2007.