Poster: Mongoose, A Novel Lightweight Cross-Platform Botnet Over TOR

Joshua Pritchett[1]
[1]Department of Computer Science
Keene State College, USNH
Keene, NH, USA
joshua.pritchett@ksc.keene.edu

Wei Lu[1,2]
[2]Department of Electrical and Computer Engineering
University of Victoria
Victoria, BC, Canada
wlu@keene.edu

***Abstract*— "Botnets" consist of a network compromised machines controlled by an attacker ("botmaster"). Traditionally botnets have been integrated with computers, and have been the primary cause of many malicious Internet attacks. However, with emerging technologies such as tablets, cellphones, and other mobile devices; have presented new challenges in simulating what a modern botnet could look like, and how effective they can be executed with the limited resources provided by such technologies. With this poster presentation, we present a lightweight cross-platform (mobile, tablet, and computer) botnet that takes advantage of the TOR network. Compared to most traditional botnets, the proposed botnet allows the bots to phase in and out of networks due to their mobile nature, encrypted communications between bot and master, to use user agents to hide control traffic dispersion over the TOR network, with emphasis on a minimal deployment time and resource usage.**

I. Introduction

Over the past thirty years, we have witnessed a strong convergence of human activities with computing and communication, increasing dramatically the opportunities for new businesses. It, however, has also paved the way for a large number of criminal activities to thrive. While these crimes are being committed in the 'cyberspacial' domain, they are nevertheless having strong implications in the real world. One of the biggest of these security threats recently has been botnets, responsible for such criminal activities such as key-logging passwords, unauthorized recovery of credit-card numbers, personal account information, emitting spam emails or phishing scams, and generating click fraud to swindle large sums of money from online-advertising firms (as reported in a recent Symantec research report [1]).

The concept of a botnet refers to a collection of infected computers (bots) that interact to accomplish some distributed task for illegal purposes. The bots are controlled by an attacker, also known as the botmaster or botlord, through various command and control (C&C) channels. These channels can operate on different communication protocols (e.g. HTTP, IRC) and use various botnet topologies: server-client centralized or peer-to-peer distributed ('P2P'). In practice, detecting and blocking traffic from a centralized botnet, is not a difficult task since the whole botnet can be deflected by blacklisting the centralized communication server. Moreover, to prevent their intranet workstations from becoming viable bots, network administrators can simply block the appropriate outbound connections to the central botmaster. In response, more and more botnets are now evolving away from the centralized-communication approach, and toward the more-advanced strategy of distributed communication. Most of these distributed communications, however, have been used with mainly personal computers. Newer innovations have been led to new multi-platform technologies; most are mobile based changing the scope of distribution possibilities. These new machines allow for maximum portability and compact designs, but offer minimal resources for processing power, battery life, security, and software compatibility.

II. Related Work

Examples of traditional botnets include the early Sinit [2], Phatbot with WASTE command [3], Nugache [4] and the recent Peacomm (Storm worm) [5]. Compared to the traditional centralized C&C model, a distributed P2P botnet is much harder to detect and destroy because the bots' communication has no heavy dependence on any few selected servers. Thus, liberating even a large number of bots may fail to destroy the function of the overall botnet. Previous attempts at detecting botnets have been based mainly on honeypots [6,7,8,9,10,11], traffic-application classification [12,13,14,15] and passive-anomaly analysis [16,17,18,19], with limited success. The ineffectiveness of these solutions relates directly to the quickly evolving strategies employed by botmasters. Recent studies in 2013 have shown that the TOR network has been employed by botmasters in order to achieve to stealthiness and untraceability, thus being more difficult to be taken down considering the anonymous C&C servers provided by the TOR hidden services [20].

III. Proposed Solution

Addressing the challenge of investigating cross-platform botnets over Tor, we can simulate a lightweight botnet that accesses the full capabilities of Tor, called *Mongoose*, in order to discover the mystery hidden behind the TOR network and to extract the networking characteristics relevant to the C&C traffic of botnet using TOR. Figure 1 is the general topology of *Mongoose*. Some of the main features of *Mongoose* are:

- A lightweight system that requires minimal resources from the device at hand and can be deployed in less than two minutes.

- Can be extended with social media to allow quick distribution and giving the botmaster full access to collect traffic as much as possible.
- Based on KIVY architecture thus can be deployed cross-platform (personal computer, mobile phone, tablet, to name a few).
- Uses modern hybrid P2P/client server architecture, allowing for multiple servers to control multiple clients with no centralized server.
- All communications are encrypted via asymmetric encryption.
- Client and servers are hard to be traced, due to mobility, encryption, and user agents hiding control traffic dispersion over the TOR network.

Mongoose is an effective simulator of botnet over TOR. The preliminary results are promising in which we observed a large amount traffic on the ingressing and egressing TOR nodes. We believe combining the fingerprints of encryption algorithms applied to access TOR network and traffic information entropy during setting up networking connections is an effective way to detect the botnet over TOR.

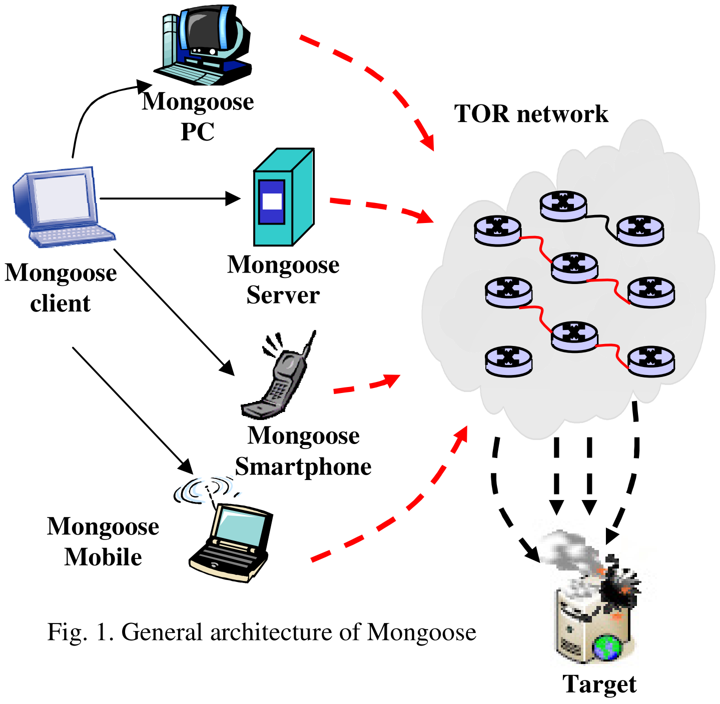

Fig. 1. General architecture of Mongoose

REFERENCES

[1] Symantec.http://www.symantec.com/security_response/publications/threatreport.jsp. Retrieved Apr 1 2015

[2] Sinit,http://www.symantec.com/security_response/writeup.jsp?docid=2003-100910-5701-99 Retrieved Apr 1 2015.

[3] Phatbot, http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20658 Retrieved Apr 1 2015.

[4] Nugache, http://www.symantec.com/security_response/writeup.jsp?docid=2006-043016-0900-99 Retrieved Apr 1 2015.

[5] Peacomm, http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99 Retrieved Apr 1 2015.

[6] M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," In *Proceedings of the 6th ACM SIGCOMM Conference on Internet measurement*, pp. 41-52, 2006.

[7] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling, "The nepenthes platform: an efficient approach to collect malware," In *Proceedings of Recent Advances in Intrusion Detection*, LNCS 4219, Springer-Verlag, 2006, pp. 165-184, Hamburg, 2006.

[8] V. Yegneswaran, P. Barford, and V. Paxson, "Using honeynets for internet situational awareness," In *Proceedings of the 4th Workshop on Hot Topics in Networks*, College Park, MD, 2005.

[9] Z.H. Li, A. Goyal, and Y. Chen, "Honeynet-based botnet scan traffic analysis," Botnet Detection: Countering the Largest Security Threat, in Series: Advances in Information Security, Vol. 36, W.K.Lee, C. Wang, D. Dagon, (Eds.), Springer, ISBN: 978-0-387-68766-7, 2008.

[10] F. Freiling, T. Holz, and G. Wicherski. "Botnet tracking: exploring a root-cause methodology to prevent Denial of Service attacks. In *Proceedings of 10th European Symposium on Research in Computer Security (ESORICS'05)*, 2005.

[11] T. Holz, M. Steiner, F. Dahl, E. Biersack and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm", In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, San Francisco, California, 2008.

[12] T. Strayer, R. Walsh, C. Livadas, D. Lapsley, "Detecting botnets with tight command and control," *Proceedings 2006 31st IEEE Conference on Local Computer Networks*, pp. 195-202, 2006.

[13] T. Strayer, D. Lapsley, R. Walsh, and C. Livadas, "Botnet detection based on network behavior," Botnet Detection: Countering the Largest Security Threat, in Series: Advances in Information Security, Vol. 36, W. K. Lee, C. Wang, D. Dagon, (Eds.), Springer, 2008.

[14] C. Livadas, R. Walsh, D. Lapsley, T. Strayer, "Using machine learning techniques to identify botnet traffic," In *Proceedings 2006 31st IEEE Conference on Local Computer Networks*, pp. 967-974, Nov. 2006.

[15] J. Goebel and T. Holz, "Rishi: Identify bot contaminated hosts by irc nickname evaluation," In *Proceedings of USENIX HotBots'07*, 2007.

[16] A. Karasaridis, B. Rexroad, and D. Hoeflin, "Wide-scale botnet detection and characterization," In *Proceedings of the 1st Conference on 1st Workshop on Hot Topics in Understanding Botnets*, Cambridge, MA, 2007.

[17] J. R. Binkley and S. Singh, "An algorithm for anomaly-based botnet detection," *USENIX SRUTI: 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet*, 2006.

[18] G.F. Gu, J.J. Zhang, and W.K. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," In *Proceedings of the 15th Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2008.

[19] G.F. Gu, R. Perdisci, J.J. Zhang, and W.K. Lee. "BotMiner: clustering analysis of network traffic for protocol- and structure-independent Botnet detection," In *Proceedings of the 17th USENIX Security Symposium (Security'08)*, San Jose, CA, 2008.

[20] Y. Klijnsma, Large botnet cause of recent Tor network overload, http://blog.fox-it.com/2013/09/05/largebotnet-cause-of-recent-tor-network-overload/ Fox-It, 5 September 2013.