Bennett Cyphers, Joshua Blum, Ofir Nachum, Louis Sobel
tweetnet@mit.edu

Project Proposal: Tweetnet

March 21, 2014

1 INTRODUCTION

Twitter is a centralized feed subscription service. The social network boasts over 500 million users as well as 340 million daily tweets and 1.3 billion daily search queries. Any user can send or broadcast a *tweet*, a 140 character message that can be synchronously or asynchronously read by either registered users or anonymous browsers. Twitter can be accessed through web browsers, SMS, and a developer API.

Twitter is a public, fast, free, robust, and reliable communication mechanism. Therefore, we posit that Twitter is a good tool for command and control of unknown sets of servers such as a botnet. A botnet controller can rely on Twitter's infrastructure to persist communication to nodes, alleviating the need to build and maintain such mechanisms themselves.

2 RELATED WORK

In recent years, botnets and spamnets have been found on Twitter by individual investigators. In 2009, Arbor Networks reported finding a Twitter account which periodically posted base-64 encoded commands [1]. These commands would direct presumably infected computers to download certain malicious files which would leak data from the victim's computer.

In 2010, Trend Micro discovered another application of the technique, in which a botnet known as Mehika used a binary called `WORM_TWITBOT` to hijack victims' computers [2]. The infected machines used the victims' Twitter account to send commands among the infected machines.

In 2013, a group of San Jose University researchers designed and implemented what they call a SocialNetworkingBot [4]. This system uses Twitter for command and control - a bot master tweets commands which are acted on by individual bots. The botnet serves as a proof of concept and shows that building such a botnet is possible.

In similar fashion, Nagaraja et al. introduce a sophisticated botnet termed Stegobot [11]. This botnet is novel in the way that it communicates: via a model of covert communication through image sharing. Specifically, communication is hidden via image steganography. This implementation shows how powerful social networks can be for botnet communication.

In addition to these very sophisticated botnet designs, researchers are also hard at work developing methods that uncover botnet activity. A group of Georgia Tech researchers recently hypothesized ideas for network-based anomaly detection as botnet detection mechanisms [7]. They propose that bots of the same botnet should have temporally correlated network activities - for example, a botnet might be programmed to tweet predictably every 15 minutes. This type of behavior would result in a flood of network traffic every 15 minutes, which may be detectable.

3 Project Goals

The goal of our project is to detect the use of Twitter for botnet command and control. We first have to reason about how such a botnet would look like. What are the key characteristics and patterns? Is there a defining feature that can easily identify a botnet on Twitter?

To test these theories, we will analyze Twitter's Firehose, a real time data stream of tweets as they are published. We categorize different techniques as follows:

Scalar Techniques
Applied to one tweet. Does a specific tweet look like something a botnet would understand? If a link is present, we can examine the content to see if malicious.

Vector Techniques
Applies to a set of tweets. Analyze based on user, hashtags, or retweet patterns.

Graph Techniques
Applies to followers, retweets, and view of the network from different users' perspectives.

Using models based on these three techniques, we suspect that a Twitter command and control channel will be detectable. We expect the communications to have identifiable patterns, either in content or in retweet networks. To help figure out what these patterns may be, we intend to design a botnet communication protocol of our own. We will design the protocol with the following traits desirable in a social network-utilizing botnet:

Stealth
The botnet's activities on Twitter should not be detectable by Twitter admins.

Authenticity
The botnet's slaves can only be controlled by the specified master. The botnet cannot be stolen by a rogue master.

Robustness
Loss of communication with a number of slaves or the master does not destroy the botnet.

Confidentiality
The communication should only be readable by bots within the network.

We will test a protocol using Twitter, or a similar service as a communication channel. Using the results of our models, we can build upon our protocol, extracting desirable features from any networks we find.

4 Conclusion

The project will consist of initial infrastructure to process the Firehose data as well as a suite of machine learning models using the scalar, vector, and graphical techniques. In addition, we intend to develop our own command and control protocol using Twitter to help us detect any such protocols that are currently in use.

There are two risks to the project. One is that we may not be able to detect a botnet on twitter. In this case, working through how we would go about finding one will still be a significant portion of the project. A second risk is that designing and prototyping a botnet could be unethical. However, there is precedent in the literature for this [11, 12, 4], and reasoning through how one could be built is essential to understanding how they can be detected.

5 Bibliography

[1] http://www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command-channel/

[2] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_discerning-relationships__mexican-botnet.pdf

[3] http://cryptome.org/2014/03/massive-twitter-botnet.htm

[4] http://www.mecs-press.org/ijcnis/ijcnis-v5-n6/IJCNIS-V5-N6-2.pdf

[5] http://trojan7malware.blogspot.com/2013/06/botnet-using-twitter-as-c.html

[6] http://www.intego.com/mac-security-blog/flashback-mac-malware%2Duses-twitter-as-command-and-control-center/

[7] http://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1006&context=cse

[8] http://link.springer.com/chapter/10.1007/978-3-642-13708-2_30

[9] http://link.springer.com/chapter/10.1007/978-3-642-25560-1_9

[10] http://www.sciencedirect.com/science/article/pii/S1389128612003568#

[11] http://www.cs.utexas.edu/~amir/papers/IH11-Stegobot.pdf

[12] http://link.springer.com/chapter/10.1007%2F978-3-642-14215-4_5