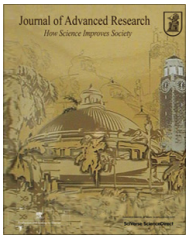
Journal of Advanced Research (2014) 5, 473–479

Cairo University

Journal of Advanced Research



ORIGINAL ARTICLE

Fast Flux Watch: A mechanism for online detection of fast flux networks

Basheer N. Al-Duwairi *, **Ahmad T. Al-Hammouri**

CyberSecurity Research Laboratory, Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid 22110, Jordan

ARTICLE INFO

Article history:
Received 1 September 2013
Received in revised form 2 January 2014
Accepted 3 January 2014
Available online 17 January 2014

Keywords:
Network security
Botnets
Fast flux networks
Bloom filter
Correlated TCP SYN

ABSTRACT

Fast flux networks represent a special type of botnets that are used to provide highly available web services to a backend server, which usually hosts malicious content. Detection of fast flux networks continues to be a challenging issue because of the similar behavior between these networks and other legitimate infrastructures, such as CDNs and server farms. This paper proposes Fast Flux Watch (FF-Watch), a mechanism for online detection of fast flux agents. FF-Watch is envisioned to exist as a software agent at leaf routers that connect stub networks to the Internet. The core mechanism of FF-Watch is based on the inherent feature of fast flux networks: flux agents within stub networks take the role of relaying client requests to point-of-sale websites of spam campaigns. The main idea of FF-Watch is to correlate incoming TCP connection requests to flux agents within a stub network with outgoing TCP connection requests from the same agents to the point-of-sale website. Theoretical and traffic trace driven analysis shows that the proposed mechanism can be utilized to efficiently detect fast flux agents within a stub network.

Introduction

Botnets, networks of compromised machines under an attacker's control, are the source of so many security threats including distributed denial-of-service (DDoS) attacks, spam, and identity theft [1–8]. Fast flux networks (FFNs) represent a special type of botnets that are being used by cybercriminals—in a way similar to that used in Content Distribution Networks (CDNs) and Round Robin Domain Name System (RRDNS)—to provide high availability and dynamicity for their malicious websites (usually online scam websites). The main idea of fast flux networks is to use bot machines as proxies that relay user requests to backend servers (i.e., the content servers). A frequent and fast change of proxies (known as flux agents) is required to evade detection and blocking, and to ensure high availability at the same time because these bots are often typical PCs that go online and offline at different times.

Fast flux networks represent a new trend in the operation and management of online spam campaigns. In these campaigns, spammers flood email inboxes of thousands of email users with advertisements about different products or services (e.g., pharmaceutical, adult content, phishing, etc.). These advertisements usually include hyperlinks to websites that represent the point-of-sale for the campaigns. Until recently, each point-of-sale website is used to map to a single IP address that

* Corresponding author. Tel.: +962 2 7201000x23366; fax: +962 2 7201077.
E-mail address: basheer@just.edu.jo (B.N. Al-Duwairi).
Peer review under responsibility of Cairo University.

Production and hosting by Elsevier

2090-1232 © 2014 Production and hosting by Elsevier B.V. on behalf of Cairo University.
http://dx.doi.org/10.1016/j.jare.2014.01.002

remains static for considerable amount of time, and thus giving defenders the opportunity to block access to the corresponding website, or even track it for the sake of legal pursuits. With FFNs, the domain name of the point-of-sale website maps to several IP addresses that keep changing at a fast rate. Fast flux domains are characterized by the very short TTL values for their A records, and by the frequent change-of-mapping to multiple IP addresses that usually belong to different autonomous systems [9,10].

Previous work in the area of FFNs has mainly focused on detecting and characterizing FFNs by analyzing Domain Name System (DNS) records of suspicious domain names. In this context, DNS records could be collected by actively querying the DNS system for domain names found in spam email messages (this approach was followed by Holz et al. [9]). Alternatively, the DNS records can be collected through passive monitoring of DNS traffic of an Internet Service Provider (ISP) network (an approach that was followed by Perdisci et al. [11]). Both approaches require collecting massive amount of information for analysis, and they do not provide a real-time detection of fast flux agents.

In this paper, we propose a novel mechanism for real-time detection of flux agents within an organizational network without requiring the collection of DNS traffic information. The proposed mechanism, called Fast Flux Watch (FF-Watch), is envisioned to exist as a software agent at leaf routers that connect stub networks to the Internet. The core mechanism of FF-Watch is based on the inherent features of fast flux networks where flux agents within stub networks take the role of relaying/redirecting client requests to point-of-sale websites of spam campaigns. Therefore, the basic idea is to correlate incoming TCP connection requests to flux agents within a stub network with outgoing TCP connection requests from the same agents to the point-of-sale website.

The rest of this paper is organized as follows. In 'Fast flux networks', we provide the relevant background about fast flux networks and their role in hosting online scam. 'Methodology' section describes the proposed FF-Watch mechanism. Then we present the evaluation of the proposed FF-Watch mechanism and discuss the results. Finally, conclusions and future research directions are outlined.

Fast flux networks

The issue of fast flux networks was reported for the first time by the Honeynet project [12] in 2007. However, Holz et al. [9] were the first to study this phenomenon systematically in 2008. Basically, FFNs can be considered as a special type of botnets that are used by botmasters to provide high availability to their malicious websites (known as mothership servers) while hiding their location and identity (i.e., IP addresses) to avoid blacklisting. These networks consist of compromised nodes called flux agents that serve as proxies to the mothership servers. A request to a fast flux domain will go through one of the flux agents before being forwarded to the mothership server. The flux agent will relay the response back to the client as shown in Fig. 1.

There have been considerable research efforts focusing mainly on detecting and characterizing FFNs. Previous work mainly relied on collecting domain names from e-mail's spam traps as the primary source of information, with the main goal

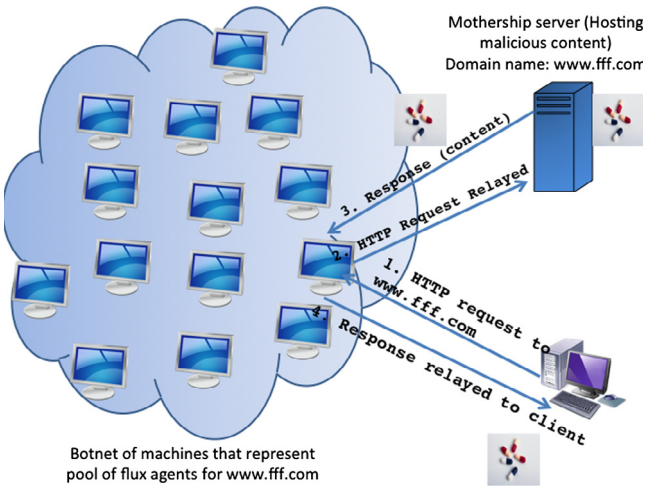


Fig. 1 The basic idea of fast flux networks. Fast flux domain resolves to multiple IP addresses that correspond to compromised nodes serving as proxies for the content server. Domain-name-to-IP-address mapping keeps changing over time.

is to classify domains into fast flux domains and non-fast flux domains based on certain features and characteristics that distinguish fast flux domains using different machine-learning algorithms. Generally, the research done in this area can be categorized, based on the approach followed in identifying flux agents, as follows.

- *Active detection*: In this approach, domain names of scam websites are extracted from spam archives, which were obtained from various spam traps. For each domain name, several DNS queries are performed (e.g., using the dig tool) to collect information about the set of resolved IP addresses. DNS answers for these queries are then examined to determine whether the domain name is being either legitimate or fast flux. The decision is based on observing certain features that characterize FFNs, and is usually done using artificial intelligence algorithms. This approach was adopted by most of the previous work in this field [13].
- *Passive detection*: This approach was proposed Perdisci et al. [11]. In this approach, live traces of DNS traffic (queries and answers) are collected by placing monitors at various strategic locations in an ISP network. The traffic is then analyzed searching for FFNs' footprints. The premise here is that it is possible to capture DNS information of domain names not only present in spam emails, but also in any other online applications, such as chat rooms, and malicious websites. The advantage of this approach is that it does not pose additional load on network resources to make active DNS lookups, as in the active approach. Additionally, it cannot be detected by botmasters who may suspect high DNS lookup rates on their infrastructure.
- *Real-time detection*: Recently, Hsu et al. [14] presented a system to detect FFNs in real-time with the goal to cut the detection time to few seconds without affecting the detection accuracy. The idea relies on the observation of the longer delays for HTTP responses as a result of relaying the requests via fast flux agents. Relaying requests through fast flux nodes typically requires additional time because of the