Computer Communications 000 (2016) 1–9

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# Exploiting Content Delivery Networks for covert channel communications

Yongzhi Wang[a,b], Yulong Shen[a,*], Xiaopeng Jiao[a], Tao Zhang[a], Xu Si[a], Ahmed Salem[a], Jia Liu[c]

[a] School of Computer Science and Technology, Xidian University, 2 South Taibai Road, Xi'an, Shaanxi, PR China
[b] Key Laboratory of Grain Information Processing and Control, (Henan University of Technology), Ministry of Education, PR China
[c] School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan

ARTICLE INFO

*Article history:*
Available online xxx

*Keywords:*
Content Delivery Networks
Covert channel
Information hiding

ABSTRACT

Content Delivery Networks (CDNs) became an important infrastructure in today's Internet architecture. More and more content providers use CDNs to improve their service quality and reliability. However, providing better quality of service (QoS) by using CDNs could also be abused by attackers to commit network crimes. In this paper, we show that CDNs can be used as a covert communication channel to circumvent network censorships. Specifically, we propose the CDN covert channel attack, where accessing contents through different CDN nodes can form a unique pattern, which can be used in encoding secret messages. We implemented a proof-of-concept covert channel based on our proposed attack on CloudFront, a commercial CDN service provided by Amazon Web Service. We showed that our constructed covert channel can transmit messages with various lengths with an average transmission efficiency as 2.29 bits per request (i.e., each *penetration request* transmits 2.29 bits of secret message on average). After presenting the CDN covert channel attack, we also discuss possible countermeasures.

## 1. Introduction

Content Delivery Networks (CDNs) have received a wide acceptance as a solution to provide on-demand capacity and faster content accessibility. Akamai [1], a leader CDN provider, has deployed 85,800 servers in about 1800 districts within a thousands of different ISPs in more than 79 countries. Today, most of the major content providers, such as CNN, Reuters, Yahoo, Youtube, utilize CDNs to achieve high speed content access.

CDNs enable the user to access the objects from the closest edge server, thus obtains a much higher access speed. On the other hand, due to CDNs' open characteristic, CDNs can be also abused by the attacker for illegal purposes. For instance, [2] described a denial of service (DoS) attack that makes a huge number of CDN edge servers serve as malicious content visitors, which can exhaust the original content server's resource. In our paper, we continue to play the devil's advocate to explore other possible attacks. By exploring vulnerabilities from a different perspective, we show that a *malicious content provider* (MCP) and a *malicious content visitor* (MCV) can use a CDN to construct a covert channel. Specifically, the MCV can access the MCP's contents through different CDN edge servers. Using different CDN edge servers generates different access patterns, which can be used to encode secret messages.

We call our proposed attack as the *CDN covert channel attack*. As far as we know, this is the first paper that describes such an attack. We performed a proof-of-concept CDN covert channel attack on a real commercial CDN, the *Amazon CloudFront*. In our experiments, we showed that secret messages with arbitrary lengths can be sent through this channel. Our experiments in Section 4 shows that the transmission efficiency can be 2.25 bits per *penetration request*. We also discussed the traditional HTTP-based covert channel attack and explored its possible attack scheme in an environment where the CDN is introduced. The ultimate goal of our research is to prevent proposed attacks. Therefore, after presenting the attack details, we discussed possible countermeasures regarding to the proposed attacks.

The paper is organized as follows. We declare the research motivation, the system model and the attacker model in Section 2. We describe the design of the CDN-based covert channel attack and the HTTP-based covert channel attack in the CDN environment in Section 3. We describe the experimental details and results in Section 4. We discuss possible countermeasures in Section 5. We

[*] Corresponding author. Tel: +862988201779; Fax: +862988202427.
*E-mail addresses:* yzwang@xidian.edu.cn (Y. Wang), ylshen@mail.xidian.edu.cn (Y. Shen), xpjiao@mail.xidian.edu.cn (X. Jiao), taozhang@xidian.edu.cn (T. Zhang), bryant123@foxmail.com (X. Si), engahmedsalem2@yahoo.com (A. Salem), jliu871219@gmail.com (J. Liu).

http://dx.doi.org/10.1016/j.comcom.2016.07.011
0140-3664/© 2016 Elsevier B.V. All rights reserved.

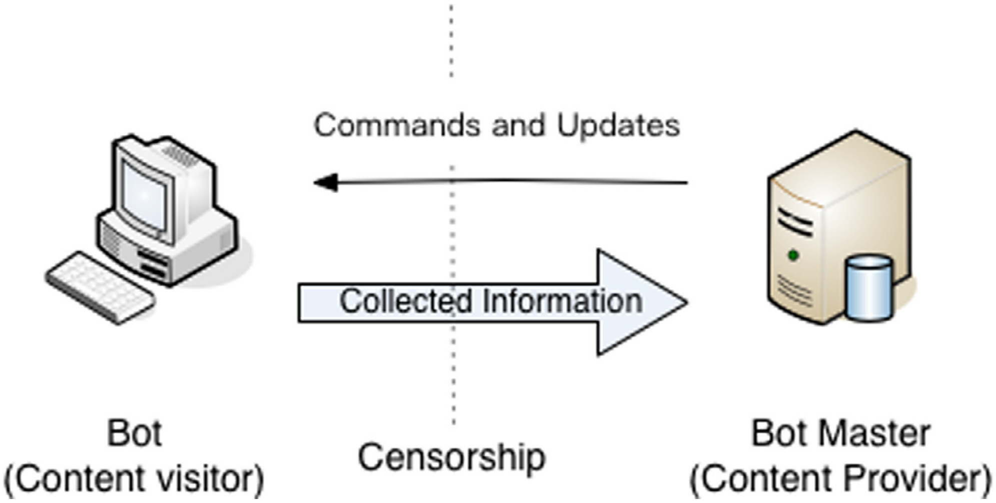

**Fig. 1.** The Scenario of CDN covert channel attack.

discuss the related work in Section 6. We conclude the paper and point out the future works in Section 7.

## 2. Research motivations, the system model and the attacker model

### 2.1. Research motivations

The covert channel communication is usually used for transmitting secret information while circumventing the Internet's censorship. One of the applications of the covert channel is the botnet command-and-control (C & C) as shown in Fig. 1. A botnet usually consists of a number of bots and a bot master. The bot master sends commands or updates to the bots. Each bot, according to the bot master's command, performs attacks or steals information from the infected host, and submits stolen data or attack results back to the bot master. The bot master can be deployed on the content provider's server. Bots can be deployed on the content visitor's machines. The botnet commands or updates can be sent to the bots when bots visit the content provider's server as a visitor. Given the high volume of the content to be transmitted from a content provider to the visitor, it is fairly easy to hide the botnet commands and updates in the transmitted content. However, the information sent from a content visitor to the content provider is usually limited. In many protocols such as HTTP and DNS, content visitors only send content requests to the content provider. The amount of information hidden in a request is usually quite limited. Besides, certain censorship mechanisms exist in the Internet to recognize such requests. On the other hand, in a botnet, the amount of information sent from the bot to the bot master are usually large. Therefore, finding an effective and safe covert channel that can transmit a large amount of information is still a challenging problem. Our research thus focuses on the secret information transmission in this direction, i.e., from the content visitor to the content provider. Attackers have constructed different covert channels on existing protocols for the message transmission, including Relay Chat Protocol (IRC), HTTP [3], Domain Name System (DNS) [4], email [5], etc. Our research propose a novel covert channel, which uses CDN services to transmit information from the bot to the bot master secretly.

### 2.2. The system model

A CDN can be modeled as in Fig. 2. A typical CDN consists of a large number of *edge servers* and *domain name system* (DNS) servers. Edge servers cache contents provided by content providers. DNS servers direct content visitors to the edge server that caches the requested content. As shown in Fig. 2, when a content visitor wants to access an object that is hosted on the content provider, the request is sent to the local DNS server (step 1). The server will return the IP address of the requested object if such information is cached in the local DNS server (step 4). Otherwise, it will forward the request to the CDN's recursive DNS server (step 2), which will return the IP address of the closest edge server to the content visitor (step 3). The IP address will be returned from the local DNS server to the content provider (step 4). With the edge server's address, the content visitor sends a request to the edge server and obtains the object if the object is cached in the edge server (step 5 and 6). If the object is not cached, the edge server will forward the request to the content provider to fetch the object and return the received object to the content visitor. Meanwhile, the edge server may cache the obtained object using different caching algorithms [1,6] to avoid future cache miss (step 7 and 8).

### 2.3. The attacker model

In our research, we assume that the bot master is deployed on a server, which provides contents through CDN services. Thus the content provider is a *Malicious Content Provider* (MCP). This server can belong to a benign content provider, which is compromised by being installed a bot master. It can also be a server belonging to a malicious content provider. In this case, the bot master is deployed intentionally by the malicious content provider. We assume that the bot is installed on the visitor's host. Thus the visitor is a *Malicious Content Visitor* (MCV). A benign visitor can be installed a bot when it visits a malicious content server. Our paper will show that when the visitor, i.e., the bot, accesses the content provided by the content provider, i.e., the bot master, it can send covert messages to the bot master through the CDN. In our paper, we mainly focus on the information transmission from the bot to the bot master. We assume that the information sent from the bot master to the bot can be hidden in the content provided by the MCP through traditional information hiding techniques [7].

## 3. Attack design

### 3.1. Architecture

The architecture of the CDN covert channel attack is shown in Fig. 3. A MCP (the bot master) hosts a server to provide contents