FACULTY OF SCIENCE
UNIVERSITY OF COPENHAGEN

Assignment 1

IT-security

May 28, 2015

Troels Thomsen qvw203
Department of Computer Science

Contents

1 Recent cases of attacks **1**

1.0.1 Greatfire.org 1

1.0.2 3F 1

1.0.3 SYN Flood attacks 2

2 Hands-on with SYN Floods **3**

2.0.4 Capture file 3

2.1 Simulated SYN Flood 3

1 Recent cases of attacks

1.0.1 Greatfire.org

On March 26th through March 27th 2015 an online repository for open-source software called GitHub, along with Greatfire.org mirror sites underwent a large-scale distributed denial of service (DDoS) attack. This attack was carried out presumably by the Chinese government through the state-owned companies China Telecom and China Unicom [2].

The attack did not target GitHub singularly, but its goal was to take down the code repositories `https://github.com/cn-nytimes` and `https://github.com/greatfire`. These repositories contains code for hosting mirror sites enabling internet users to circumvent the Great Firewall of China (GFW). The attack on the GitHub repositories was part of a larger attack on Greatfire.org and their mirrors hosted on Amazon Cloudfront [1].

The DDoS attack was conducted out as a so-called man-on-the-side attack [3]. Unsuspecting internet users from outside China accessing Chinese websites or websites containing content hosted in China, was used to perform GET requests to the GitHub repositories and the Amazon Cloudfront mirrors. This was done by injecting a piece of javascript code into an otherwise innocent file sent from the Chinese search engine Baidu. Users visiting sites with Chinese content would unknowingly request the very common Baidu's analytics software hosted inside China. Some of these requests (roughly 1%) were then intercepted as they went through the GFW, and extra packets containing the malicious javascript were added to the response.

The ultimate goal of these attacks was to prevent Greafire.org from helping Chinese internet users access material which has been banned by the Chinese government.

1.0.2 3F

On April 30th 2015 several people were convicted of having conducted a denial of service attack against the organisations 3F, HK and LO during June 2012 [4]. The attack was carried out by individuals claiming to be affiliated with the hacker group Anonymous, which later denied all such affiliations. The attack was primarily motivated by the fact that 3F and its associated unions was carrying out a blockade against a restaurant in Vejle, due to the restaurant having what 3F considered to be unacceptable working terms for its employees. The hackers considered this unjust and tried to retaliate on behalf of the restaurant by attacking 3F's website.

In both the case of the Chinese attacks and the attack on 3F, the motivation behind the attacks could be said to be political, as both of the attacking parties tried to threaten their adversaries into submission by attacking their online resources. The main difference between the two attacks however, is the fact that the attack on Greatfire.org and its services was carried out by the Chinese government, using their vast IT-infrastructure to enable a very sophisticated type of DDoS attack. The attack on 3F on the other hand was carried out by a small group of individuals acting on their own as the old-school rogue type of hackers often depicted in popular culture. The Chinese governments activities can be seen in a large context as part of a global shift towards more government-supported hacking, where the most notable proponent of this strategy is the United States National Security Agency.

1.0.3 SYN Flood attacks

SYN Flood attacks exploits the TCP three-way handshake to occupy resources on the targeted server and render it unresponsive to other clients. The attacker will send a large amount of SYN packets to all open ports, but not respond to SYN-ACK thus leaving the connection half-open. The connection will stay half-open for some duration on the server, and if enough SYN packets are received before the server reallocates the connection resource, the attacker can successfully make all available resources half-open thus preventing legitimate users from establishing a connection.

While the attack on GitHub was not strictly speaking a SYN flood attack, it shared some of the same characteristics. Like the changing ports in a SYN Flood, the payload of the GitHub DDoS attack carried a timestamp in order to generate random unique requests [1]. The main difference between the GitHub attacks and a SYN Flood is the fact that the Chinese attacks actually completed the requests waiting for the server to reply before continuing. When the server was ”slow enough” with its response, the script would switch to a different server [1].

2 Hands-on with SYN Floods

2.0.4 Capture file

We recognize the given packet capture as a recording of a SYN Flood attack by the fact that it contains 629000 SYN packets send within 4 seconds, and only a few SYN-ACK packets send from the server indicating that it is not used to that amount of traffic. Additionally we see no corresponding ACK from the clients.

2.1 Simulated SYN Flood

My working machine has a SYN backlog size of 256.

During the simulated attack i carried out on my own machine, netstat showed 256 connections with status SYNC-RECV. I recorded approximately 175000 SYN packets during the 1 second capture i did while the attack was ongoing.

I would regard the attack as successful since i managed to fill up the queue while at the same time slowing down the machine significantly taking up 40-60% of the processing power. I tried the attack with the SYN cookie both on and off, but did not notice any significant difference. It took slightly longer to fill up the que with SYNC-RECV while SYN cookie was on. With SYN cookie on the server is supposed to drop the connection until it receives ACK, and reconstruct the queue entry from the sequence number. It is difficult to assess based on the netstat dump, whether or not this was actually the case for my test attack.

While the SYN cookie mechanism can prevent the server from dropping some legitimate requests if the queue fills up, the server might still slow down significantly due to the excess traffic. Additionally, the server can not accept any other TCP options while SYN cookies is on, since it drops the queue entry while waiting for ACK.

References

[1] GreatFire.org. Using baidu to steer millions of computers to launch denial of service attacks. https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1, 2015.

[2] Erik Hjelmvik. China's man-on-the-side attack on github. http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub, 2015.

[3] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, and Vern Paxson. China's great cannon. https://citizenlab.org/2015/04/chinas-great-cannon/, 2015.

[4] DR Nyheder. Hackere skal betale 1,4 millioner kroner i erstatning til 3f. http://www.dr.dk/Nyheder/Indland/2015/04/30/152616.htm, 2015.