Security Lab
Lab Assignment No. 1

Aim: Identify any one major security threat/issue from the internet and write in your own words.

Major security threat: DDoS Attack

Active attacks involve modification of a data stream or creation of a false stream of messages. Here, the attacker's aim is to corrupt or destroy data as well as the network itself. Active attacks are divided into four categories:

1. Masquerade
2. Replay attack
3. Modification of messages
4. Denial of service

We will be talking about **Denial of service** (DoS) attacks. **Denial of service** attack means making the network unavailable for the user who wants to communicate securely. It is generally done by interrupting the network connection between the users or making some services unavailable for users or disrupting the entire network by overloading with unwanted messages, so that the network becomes slow and unavailable for users.

A DoS attack can occur in two ways:

1. Flooding
2. Malformed data

DDoS attacks are **Distributed Denial of service** attacks. It occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The attacker floods the target computer with internet traffic to the point that the traffic overwhelms the target system. The target system is unable to respond to any requests or process any data, making it unavailable to legitimate users.

A DDoS attack uses more than one unique IP address or machines, often from thousands of hosts infected with malware. The scale of DDoS attacks has continued to rise over recent years, by 2016 exceeding a terabit per second. Here are some of the DDoS attacks:

1. First DDoS attack was on Panix, the third oldest IPS in the world. Due to the attack on September 6 1996, it brought down its services for several days while the hardware vendors figured out a proper defense.
2. In June 2019 in Hong Kong, the messaging app Telegram was subjected to a DDoS attack. The founders of Telegram have stated that this attack appeared via IP address originating from China.

3. In February 2020, Amazon Web Services experienced an attack with a peak volume of 2.3 terabits per second.

Now, we will be focusing on the most sophisticated and largest DDoS attack in the site's history.

March 2015 - GitHub Attack

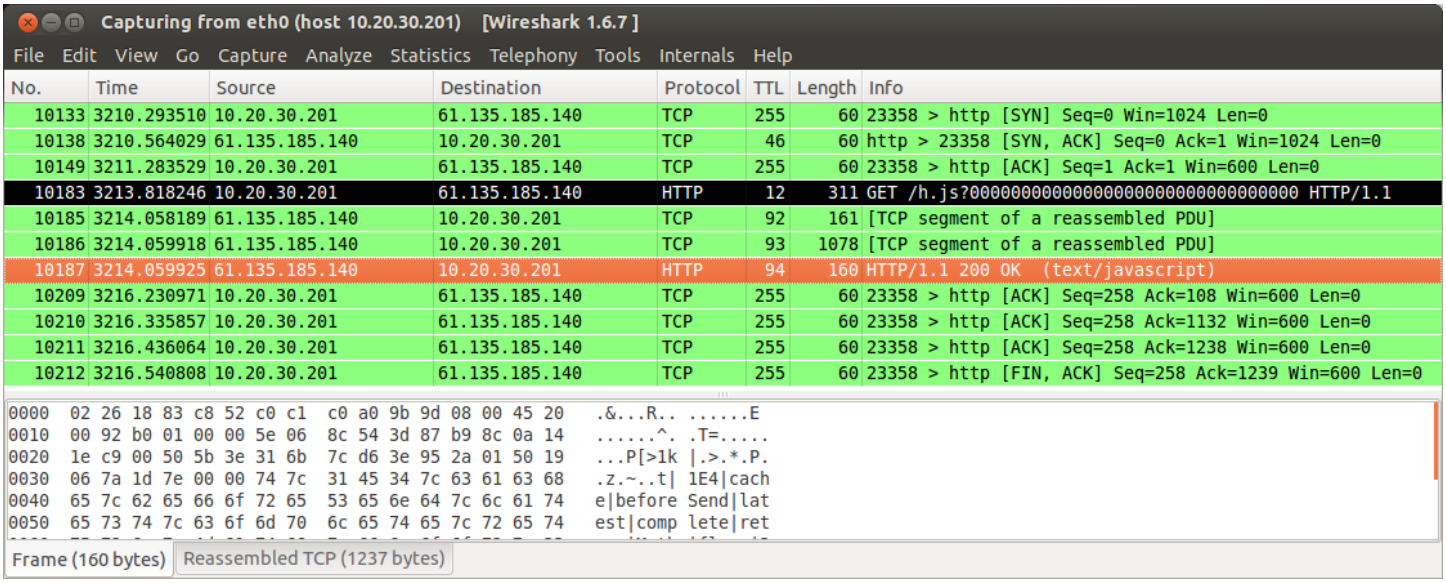
The DDoS attack targeted the URLs of two GitHub projects that were helping Chinese citizens circumvent China's state censorship. One of the URL pages was run by GreatFire and another mirroring Chinese translations of *The New York Times*.

Purpose and duration of the attack:

The purpose of the attack was to push GitHub into closing down these two projects. The result for GitHub was massive flood of traffic, which built for more than 24 hours before causing partial outages. Server logs showed a sudden drop in app server availability and page failures rate spiking to 100% just before 3am. The DDoS attack vector evolved gradually, during the six days of attack.

Process of the attack happened:

A large percentage of Chinese websites use Baidu Analytics to keep the track of their visitors. When a visitor views one of these sites, the browser normally loads a JavaScript file to keep track of each user.



DDoS attacks that crippled GitHub linked to Great Firewall of China

A certain device at the border of China's inner network and the Internet had hijacked the HTTP connections that went into China, replacing some "normal" JavaScript files from Baidu with malicious files - one which instructed the user's browser to continuously reload those two specific GitHub HTTP requests. It was believed that the attackers gained access to a highly authoritative data center. Additionally, all the traffic to Baidu Analytics is unencrypted. Thus, the attackers leveraged the weakness.

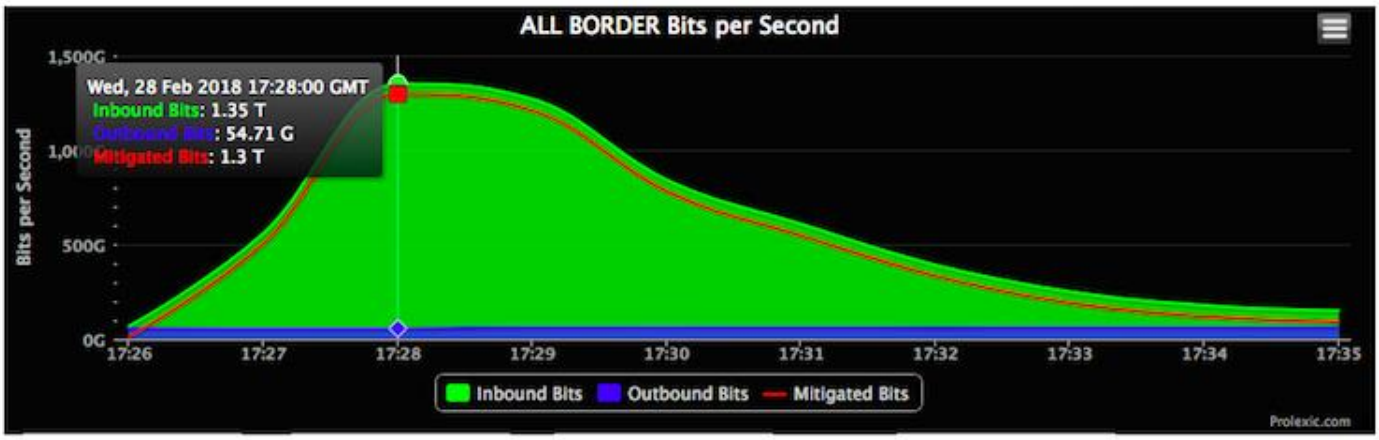
Observations:

When thousands of users were opening Chinese sites, they were unwillingly participating in the attack. A rogue JavaScript was injected into their client. The observers were speculating that the attack was meant to enforce Chinese web censorship, knocking out any way for Chinese citizens to circumvent the country's Great Firewall.

GreatFire's mirror sites came under a similar DDoS attack, which threatened to knock the service offline. Because GitHub is served over HTTPS, countries can't block individual pages without blocking the entire site, a feature that's proved extremely useful for anti-censorship services like Great Fire.

Another GitHub DDoS attack:

GitHub was the target of a large volumetric attack in February 2018. The DDoS attack sent packets at a rate of 126.9 Mpps and reached 1.35 Tbps.



Real-time traffic from the DDoS attack (AKAMAI)

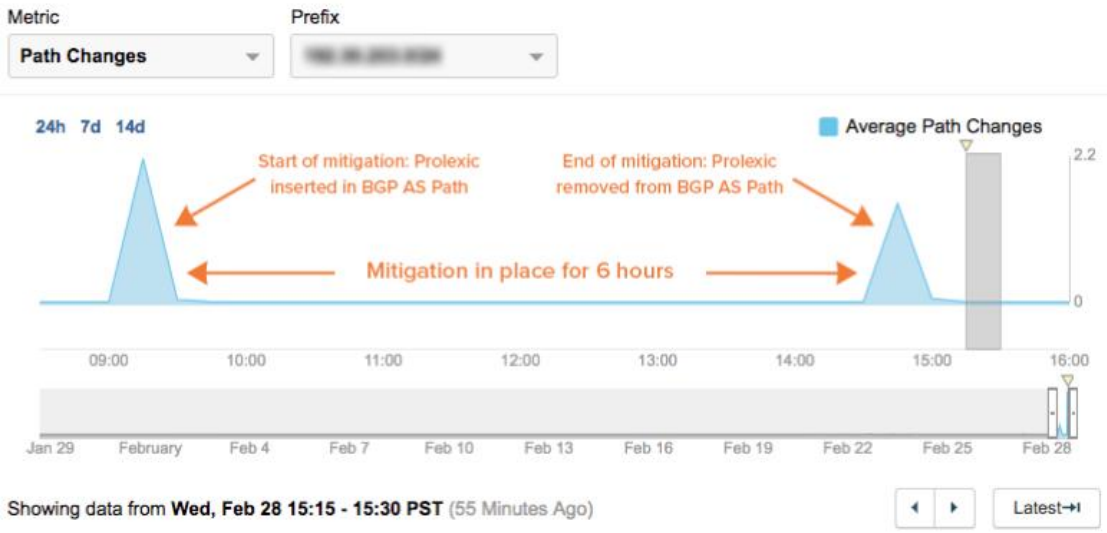
The 2018 Github attack is known as a Memcached DDoS attack. The attackers exploited a vulnerability on a command from the database caching system known as Memcached. The attackers spoofed the source within UDP packets to the GitHub servers and set the destination to vulnerable Memcached servers. The attackers were able to amplify the response size to more than 50,000x.

GitHub briefly struggled with intermittent outages as a digital system assessed the situation. Within 10 minutes it had automatically called for help from its DDoS mitigation service, Akamai Prolexic. Prolexic took over as an intermediary, routing all the traffic coming into and out of GitHub, and sent the data through its scrubbing centers to weed out and block malicious packets. After eight minutes, attackers relented and the assault dropped off.

According to GitHub, "the traffic was traced back to over a thousand different autonomous systems across tens of thousands of unique endpoints." Fortunately, GitHub already had anti-DDoS systems in place, so they were able to detect the attack within 10 minutes and mitigate it in 20 minutes.

Mitigation of attack by GitHub:

GitHub was quite efficient in mitigating the DDoS attack. Within minutes, the attack was identified and DDoS defense mechanisms kicked in. Given how quickly DDoS mitigation started, it is highly probable that the entire detection and mitigation process was automated. While the impact of the attack did not last for more than 15 minutes, GitHub-destined traffic continued to flow through Prolexic scrubbing centers up until 6 hours after the attack. The two spikes in the BGP path change timeline below represent the various points in time when Prolexic was introduced in the AS-path and subsequently removed.



Traffic destined to GitHub was sent to Prolexic scrubbing centers upto 6 hours after the DDoS attack.

DDoS attacks can be prevented by equipping your network, applications, and infrastructure with multi-level protection strategies. This may include prevention management systems that combine firewalls, VPN, anti-spam, content filtering and other security layers to monitor activities and identify traffic inconsistencies that may be symptoms of DDoS attacks.

Conclusion: Thus, we have studied and understood a major security threat/issue from the internet.