Computer Security

Security incidents HW-1 (FALL 2020)

Adrien Colombier

Summary

1. Sony’s Playstation Network
2. AWS WAF misconfiguration

Playstation Network got hacked between 17th and 19th April 2011, the service was down until the 14th of May. It affected over 77 millions of users / players.It’s the biggest failure of PSN since the launch in 2006.

The 4th of May, Sony accused an anonymous group of being responsible for the attack.What they deny.

How did hackers manage to access these datas ? It turned out that the anonymous group was behind a DDoS attack. DDoS stands for ‘Distributed Denial of Service’. Generally, these attacks work by drowning down a system with requests of data. This could be sending a web server so many requests to serve a page that it crashes under the demand. It can also be a database hit by a very high volume of queries. The result is available internet bandwidth, CPU and RAM capacity becomes overwhelmed.

DDoS attacks can be sorted in 3 primary classes :

1. Volume-based attacks use massive amounts of bogus traffic to overwhelm a resource such as a website or server. They include ICMP, UDP and spoofed-packet flood attacks. The size of a volume-based attack is measured in bits per second (bps).
2. Protocol or network-layer DDoS attacks send large numbers of packets to targeted network infrastructures and infrastructure management tools. These protocol attacks include SYN floods and Smurf DDoS, among others, and their size is measured in packets per second (PPS).
3. Application-layer attacks are conducted by flooding applications with maliciously crafted requests. The size of application-layer attacks is measured in requests per second (RPS).

This happened in 2011 they probably had no idea they were going to be attacked or how to defend themselves against this kind of attack. Today many video games or services have a solution to block those attacks. When the service is receiving a request, it checks the IP and if the same IP is sending multiple similar requests they can block it thinking it’s not a human sending them. This happened recently during a competition event in France where a player forgot his Minecraft password and tried 10 different inputs (all wrong) and ‘Mojang’ service blocked the IP.

Another solution would be to slow down the traffic by refusing a certain amount of requests / queries in order to avoid a forced shutdown. The problem with this solution is that it doesn’t stop the attack, your service is running very slowly and if the attackers keep attacking you, your service will stay really slow.

An Amazon former employee was arrested and charged with stealing more than 100 million consumer applications for credit from ‘Capital One’.

The problem stemmed in part from a misconfigured open-source Web Application Firewall (WAF) that Capital One was using as part of its operations hosted in the cloud with Amazon Web Services (AWS).

Known as ‘ModSecurity’, this WAF is deployed along with the open-source Apache Web server to provide protections against several classes of vulnerabilities that attackers most commonly use to compromise the security of Web-based applications. The misconfiguration of the WAF allowed the intruder to trick the firewall into relaying requests to a key back-end resource on the AWS platform. This resource, known as the ‘metadata’ service, is responsible for handing out temporary information to a cloud server, including current credentials sent from a security service to access any resource in the cloud to which that server has access.

Johnson said AWS could address this shortcoming by including extra identifying information in any request sent to the metadata service, as Google has already done with its cloud hosting platform. He also acknowledged that doing so could break a lot of backwards compatibility within AWS.

There is no real solution to avoid this, it’s to the developer and user to be careful to what they are doing and to who you trust. Moreover, we have very powerful tools now to prevent bad code or misconfiguration and that could help a lot.

At the end we are just human and not machines, we make mistakes and it’s normal we just need to learn from them and try to no longer reproduce them.