How Prophaze Secured Indian airports from Layer 3-7 DDoS attacks

Timeline of events leading to attack.

October 10 – 2022 - Cyberattacks reported at US airports.
https://www.theguardian.com/us-news/2022/oct/10/cyberattacks-disrupt-us-airport-websites

22-Feb-2023 - German airports hit with DDoS attack.
https://www.theregister.com/2023/02/17/german_airport_websites_ddos/

04-April-2023 - DDoS attacks rise as pro-Russia groups attack Finland, Israel
https://www.techrepublic.com/article/ddos-attacks-finland-israel/

08-April-2023 - DDoS attacks hits 6 Indian airports.
https://www.thehindu.com/news/cities/Kochi/cial-website-comes-under-attack/article66714841.ece

1) Airports Authority of India
2) Indira Gandhi International Airport
3) Mumbai International Airport
4) Hyderbad international Airport
5) Goa International Airport
6) Cochin International Airport

Background of the Attack

Anonymous Sudan is a famous hacktivists group. They had aligned with Russian hackers and planned attacks on countries like India and Israel stating religious activism as the motive behind the same.

On 8th April 2023 they launched an attack against all the major airports like Kochi, Delhi, Mumbai, Hyderabad, and Goa. They had launched a major Denial of Service Attack against these airport websites.

There were active discussions going on in the dark web and also on social media forums about the same. It was a politically motivated attack and was warned through Social Media posts that India would be the next target. This time it was the airport authorities, next could be some other sector as it is said that the attacks would continue until April 14th.

Layer 7 DDoS Attack

Denial of Service is an attack type where the intention is to shut down the operations of a network/ application by flooding the target with a large volume of traffic which can trigger a crash.

The ultimate goal is to deprive legitimate users of the service they are intending to use. This was majorly a layer 7 DDoS kind of attack. Layer 7 DDoS attacks are specifically targeted on the 7th layer or the topmost layer of the OSI model which is the application layer.

This layer usually handles request methods like HTTP GET and POST methods. Layer 7 DDoS attack usually does not require much bandwidth to execute the same and occurs very slowly. It only requires less than 1 Gbps of bandwidth.

This is why it is widely used to launch attacks on web portals as this minimal requirement makes them very effective and troublesome to handle as the resources required to fight back are much larger than those used to launch the same. This makes it very challenging to mitigate.

The HTTP traffic of layer 7 DDoS attack appears to be harmless peaks in HTTP traffic thus these spikes are confused with increased usage by the crowd. The Bots that provide the traffic spoof their IP addresses which seem to be regular addresses.

Layer 7 DDoS mitigation on Airport Infrastructure

According to several research, threat actors are co-ordinated via a particular telegram group, consists of 10000 members.

They use a particular DDoS Python script independently, which identifies open proxies on the internet and does an average connection of 200 requests per second from one script execution.

For instance, One of the IP involved in the current attack is.

138.68.190.172

Time	Method	Status	Request URI	Action
2023-04-09 13:28:55	HEAD	503	HEAD https://www.[redacted] HTTP/1.1	View
2023-04-09 13:28:55	HEAD	503	HEAD https://www.[redacted] HTTP/1.1	View
2023-04-09 13:28:55	HEAD	503	HEAD https://www.[redacted] HTTP/1.1	View
2023-04-09 13:28:55	HEAD	503	HEAD https://www.[redacted]	View

On a simple google search it is identified that this ip is listed in many open socks proxy list and one of them is

https://github.com/TheSpeedX/PROXY-List/blob/master/socks5.txt

Prophaze is continuously scrapping adding these types of proxy list in its global database.

A mass army of people of approximately 10k is doing the same and executing the scripts which creates a massive attack effect.

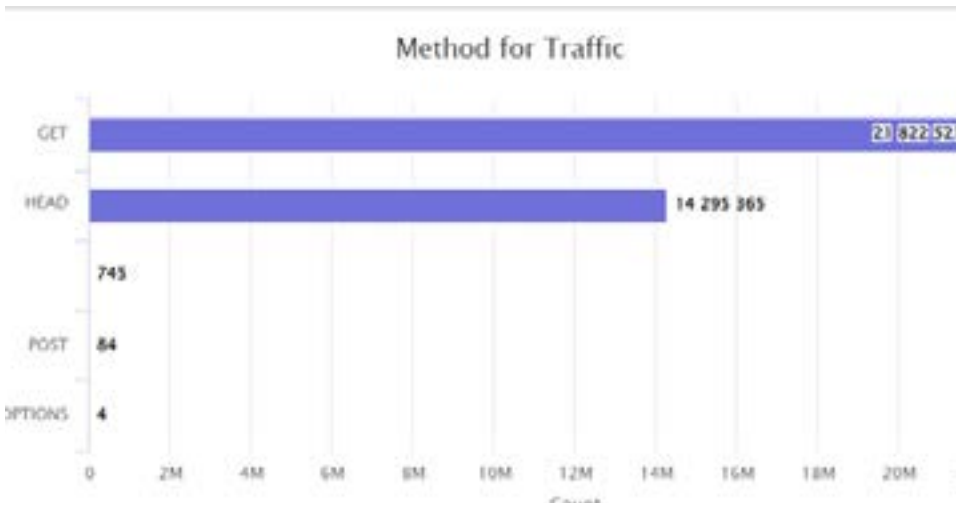
One peculiarity of the attack it is a combined effect of both Layer 3-4 DDoS and Layer 7 DDoS attack.

On a high level, the http flood attacks they are doing are.

1) GET flood.
2) HEAD flood
3) POST flood

In this case, they have used GET and HEAD flood continuously.

Potential DDoS Requests	
GET https://www.[redacted]/ HTTP/1.1	1748988
HEAD https://www.[redacted]/ HTTP/1.1	1222735
HEAD https://www.[redacted]HTTP/1.1	268577
GET https://www.[redacted]HTTP/1.1	162160
HEAD https://www.[redacted]HTTP/1.1	83643
[redacted]HTTP/2.0	63886



Referrer of the request is completely randomized so that the conventional rules and signatures cannot create a pattern based on the same.

User-Agents are also randomized, hence no way to block based on that parameter as well.

How Prophaze mitigated where other providers are failed to detect the same?

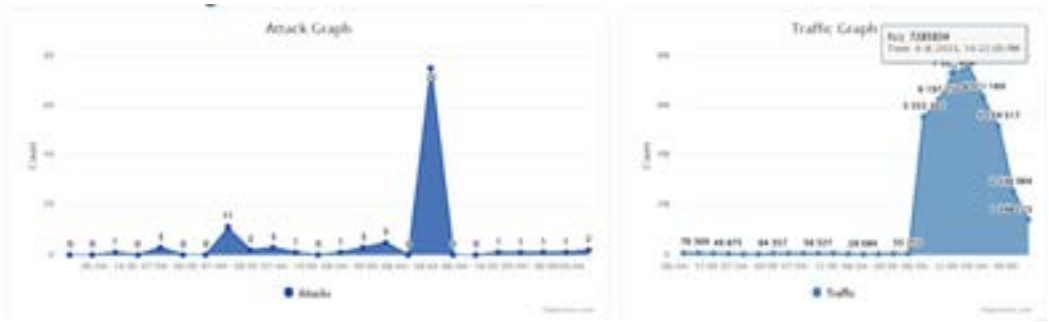
Prophaze alerting mechanisms are real time, whenever a spike in traffic happens beyond normal, systems can detect the same.

- As the load increased, Prophaze WAF instance were able to scale up dynamically to create a window to analyse the traffic pattern and enabled the dynamic DDoS Protection on Layer 7 .

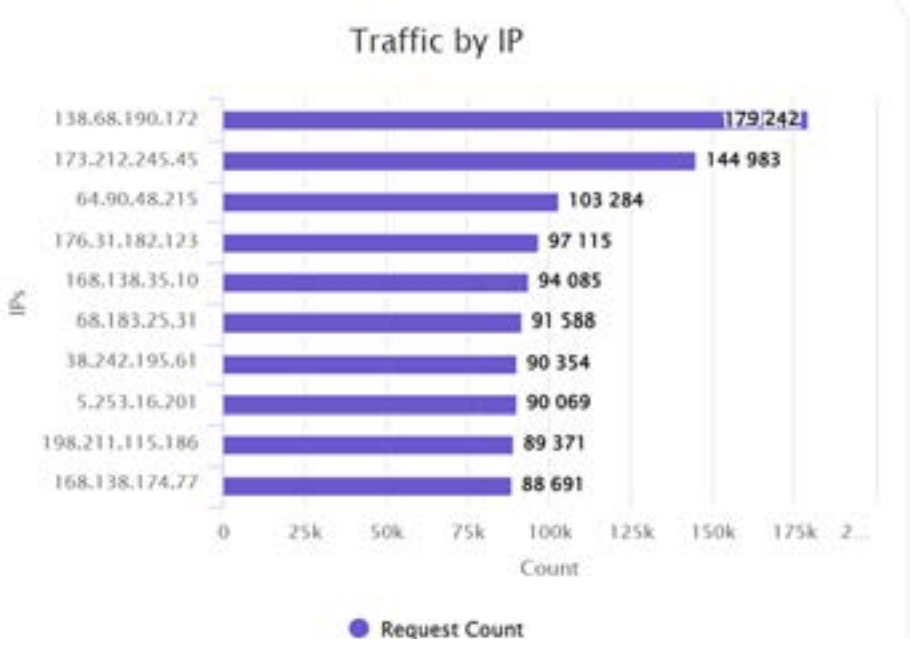
- Prophaze was able to send the API call to enable the Layer 3-4 protection on Infrastructure side.

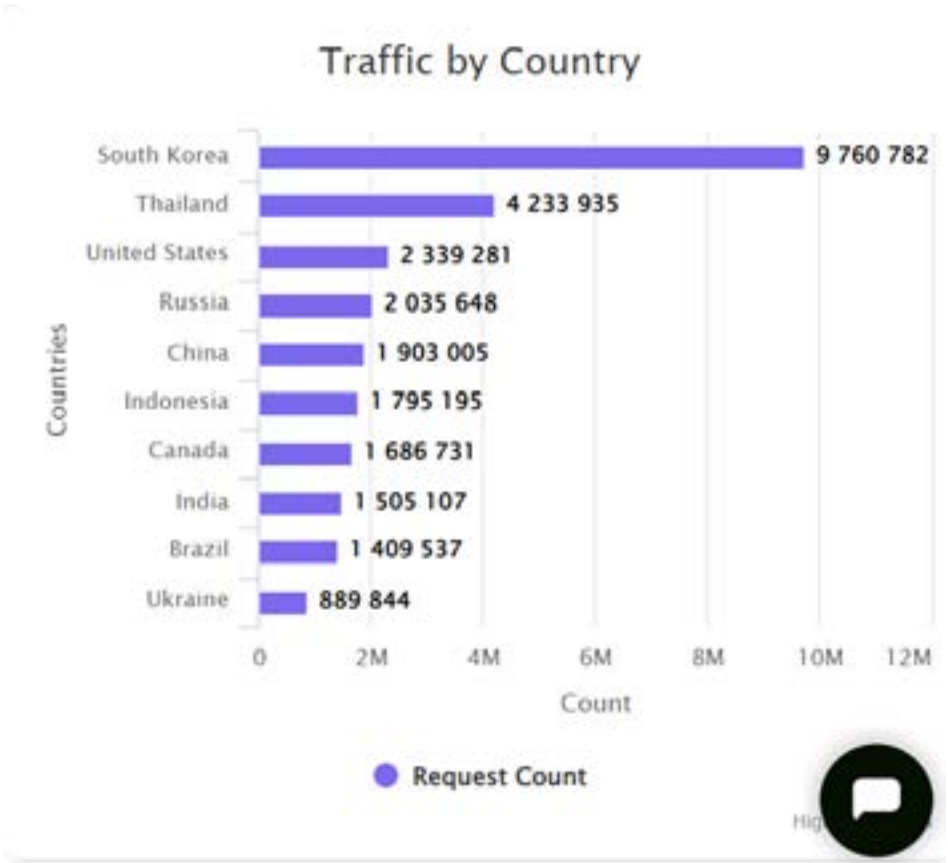
- Intelligence to analyse the attack and to deploy correct measures was the success factor for Prophaze to mitigate the attack in a span of minutes.

Attack started at around 3:40 PM on 08/04/2023 and reached its peak at 04:07 PM and ended around 1:00 AM and ended by 4 AM in the morning. The attack duration was around 42 Minutes, approximately 50 million sustained requests landed at Layer 7 DDoS for 5 hours.

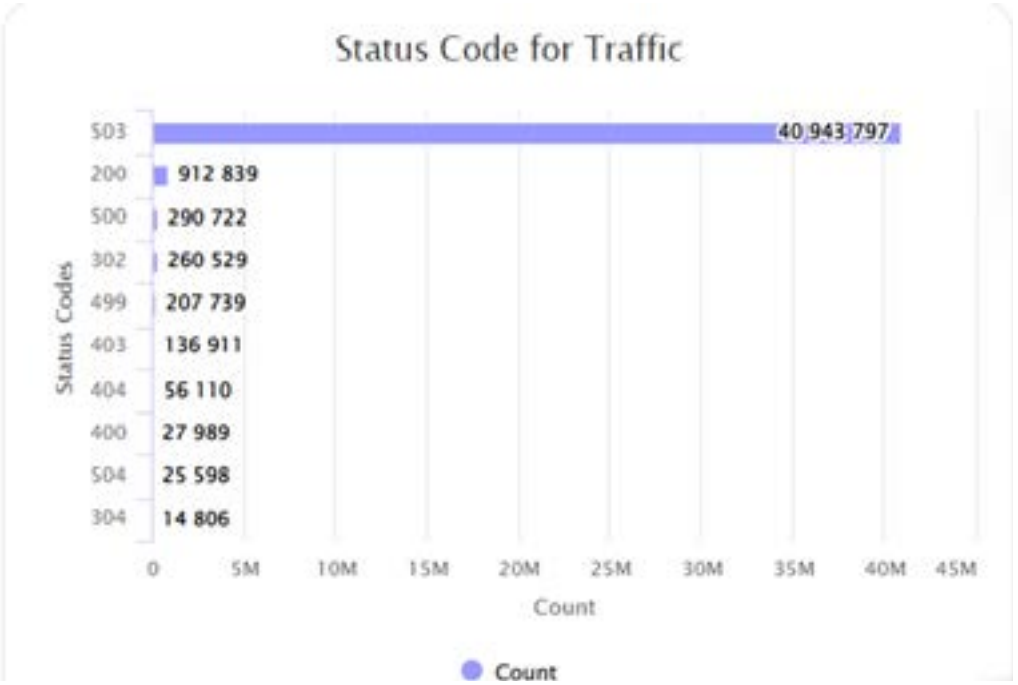


Attack was distributed from multiple countries, but predominantly from South Korea and Thailand and apart from 2 Ips involved in the attack,
Malicious requests were equally distributed around 50 Ip addresses.





Prophaze enabled a captcha less intelligence algorithm to detect the script traffic with out affecting the user experience on the website. All the malicious requests were served by a 503-status response and killed the connection.



Prophaze, Now and Beyond Security

Prophaze mission is to provide sophisticated technologies which creates value addition to its customers to secure the web infrastructure against global attacks and hence serving the people to have a hassle-free internet experience. As the technology is getting evolved Prophaze tagline is to provide a complete Web Security Platform which involves Web Application and API Protection (WAAP), Bot Protection, DDoS Protection, Virtual Patching in one umbrella. It is the first AI driven , Kubernetes WAF technology.