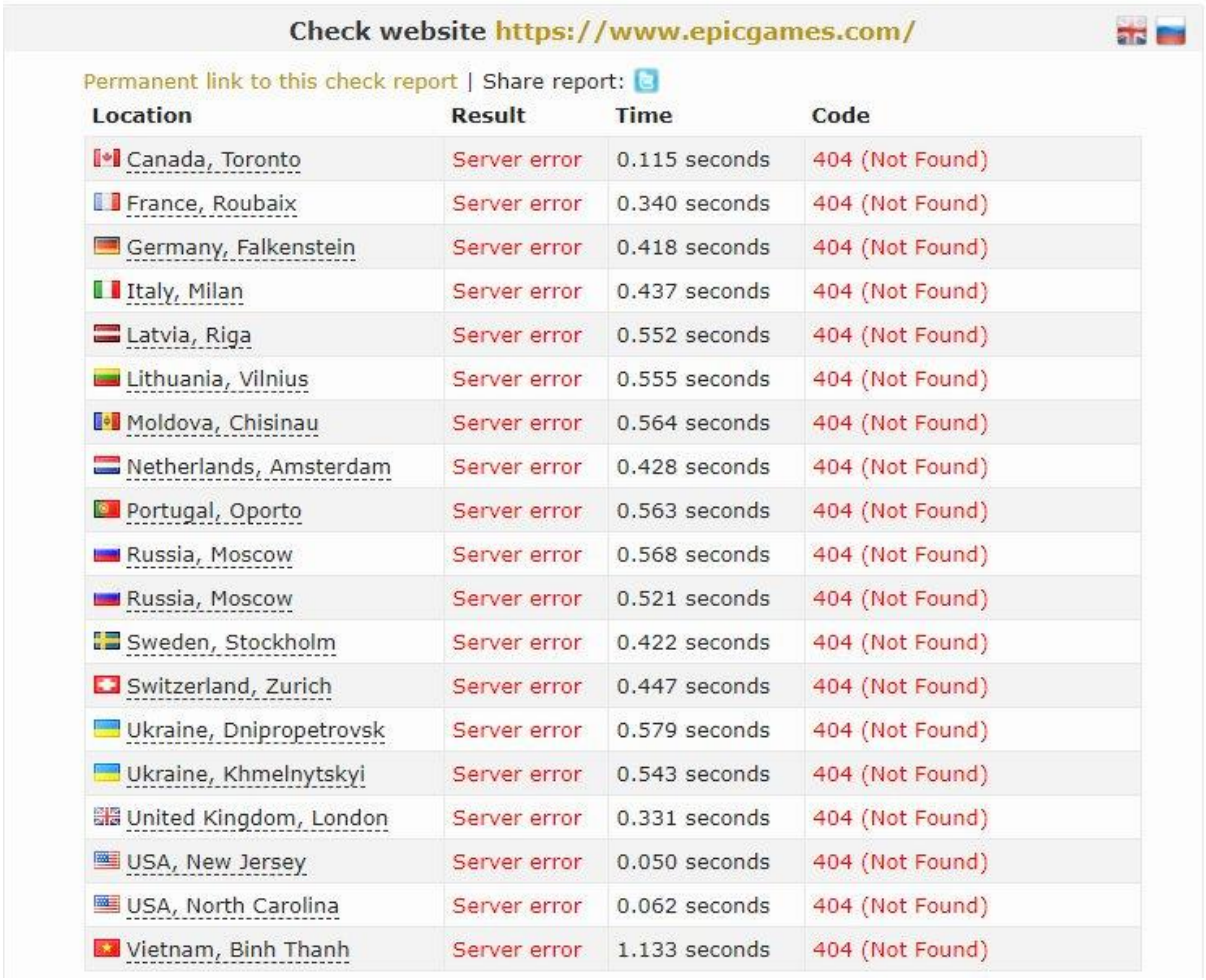
Defending Against Specific Denial of Service Attacks

1. A DDoS was claimed to be carried out by a hacker who goes by the name Restless (Flux0Flux) on Fortnite - Battle Royale servers on 12 April, 2018. Fortnite is an online multiplayer Battle Royale themed game developed by Epic Games.
2. How the attack was carried out is not very clear as both the hacker and the company didn't give out much information, but people have speculated that memcached servers were utilised to amplify the packets being sent to the game servers. The servers are distributed around the globe and aren't designed to handle heavy requests. Their only jobs include player data validation and relaying it to various other players in the same session.



Check website https://www.epicgames.com/

Permanent link to this check report | Share report:

Location	Result	Time	Code
Canada, Toronto	Server error	0.115 seconds	404 (Not Found)
France, Roubaix	Server error	0.340 seconds	404 (Not Found)
Germany, Falkenstein	Server error	0.418 seconds	404 (Not Found)
Italy, Milan	Server error	0.437 seconds	404 (Not Found)
Latvia, Riga	Server error	0.552 seconds	404 (Not Found)
Lithuania, Vilnius	Server error	0.555 seconds	404 (Not Found)
Moldova, Chisinau	Server error	0.564 seconds	404 (Not Found)
Netherlands, Amsterdam	Server error	0.428 seconds	404 (Not Found)
Portugal, Oporto	Server error	0.563 seconds	404 (Not Found)
Russia, Moscow	Server error	0.568 seconds	404 (Not Found)
Russia, Moscow	Server error	0.521 seconds	404 (Not Found)
Sweden, Stockholm	Server error	0.422 seconds	404 (Not Found)
Switzerland, Zurich	Server error	0.447 seconds	404 (Not Found)
Ukraine, Dnipropetrovsk	Server error	0.579 seconds	404 (Not Found)
Ukraine, Khmelnytskyi	Server error	0.543 seconds	404 (Not Found)
United Kingdom, London	Server error	0.331 seconds	404 (Not Found)
USA, New Jersey	Server error	0.050 seconds	404 (Not Found)
USA, North Carolina	Server error	0.062 seconds	404 (Not Found)
Vietnam, Binh Thanh	Server error	1.133 seconds	404 (Not Found)

3. Since the attack didn't require very large bandwidth the use of DDoS mitigation technologies provided by Cloudflare or Akamai could have easily prevented the attack. Also these networks can mitigate attacks amounting to even Terabytes of data per second.

Case Study

1. Firewalls aren't much good when it comes to DoS mitigation but still ip filtering and blocking communication on ports which don't require internet access can help cover up lose ends. Eg. A SQL server running on some port on a local network also visible on internet may become the vulnerability which a hacker may target. The hacker may Dos attack and send large no of login requests to completely block legitimate access to the SQL server. This can be prevented by blocking the port and its visibility outside the local network.
2. A pc with trojan horse installed provides a window to the hacker to illegally modify the pc. In case of a Distributed DoS the infected PC may be used in order to generate extra bandwidth to attack the target defined by the hacker, thus the word distributed. Large number of such smaller PC on the internet together constitute a large DDoS. So protecting devices against trojan horses on the global level will drastically reduce the number and intensity of DoS attacks.
3. SYN cookies, DoS cookies, Stack tweaking