ANAPAYA

Most significant BGP hijacks and DDoS attacks of 2022

BGP

3rd February 2022

Hackers stole roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a BGP hijack against the server infrastructure of one of the platform's providers.[1]

The attack lasted two hours, and KLAYswap's network was accessed through the third-party communication platform KakaoTalk.

DDoS

March 2022

A threat actor launched an HTTP-based DDoS attack using DanaBot against the webmail server belonging to the Ukrainian Ministry of Defense.[2]

The hacker used two stages of malware to attempt to steal credentials using download and execute commands. It is not yet known who was responsible for the attacks.

BGP

25 April 2022

Some Twitter traffic was briefly funnelled through a Russian ISP in either a BGP error or a deliberate attack.[3]

The incident lasted 45 minutes before RTCOMM, a leading ISP in Russia, stopped advertising its network as the official way for other ISPs to connect to the widely used Twitter IP addresses.

DDoS

June 2022

Hackers delayed the start of President Vladimir Putin's speech at the 25th St Petersburg International Economic Forum.[4]

A DDoS flooded its accreditation and admission systems with bogus traffic, and those responsible are thought to be pro-Ukrainian hacktivists. Internet connectivity and speeds suffered at the event, and Putin's speech was delayed by almost two hours.

BGP

26 July 2022

For 12 hours on July 26 and 27, internet users trying to access a portion of Apple's network were sent in the wrong direction by instructions issued by Russian operator Rostelecom.[5]

Apple quickly mitigated the problem by issuing routing instructions that countermanded those from Rostelecom; the issue raised questions regarding Apple's server security.

BGP

August 2022

Amazon lost control of the IP addresses it uses to host cloud services and took over three hours to regain control.[6]

An analysis showed that this lapse allowed hackers to steal $235,000 in cryptocurrency from users of one of the affected customers.

BGP

August 2022

Blockchain interoperability venue Celer network fell victim to a BGP hijack targeting its DNS servers, where perpetrators got away with around 128 ETH (roughly $240,000).[7]

In this attack, the hackers directly targeted the underlying infrastructure in the Internet architecture outside the Celer system and allowed cross-chain users to access a "phishing" front-end user interface within a period by deceiving the Internet's underlying routing protocol (BGP). The Celer network was able to limit damages due to its 24-hour monitoring system.

DDoS

October 2022

Wynncraft, one of the most considerable Minecraft servers, was recently hit by a 2.5 Tbps distributed denial-of-service (DDoS) attack.[8]

This multi-vector attack lasted for about two minutes. It consisted of UDP and TCP flood packets attempting to overwhelm the server to restrict hundreds of thousands of players from accessing the game.

DDoS

November 2022

Pro-Russia hacker group Killnet launched a DDoS attack against the website belonging to the Prince of Wales and warned that the UK healthcare system would be next.[9]

Killnet also threatened future attacks against the London Stock Exchange, the British Army, and more after claiming responsibility for attacks against Starlink and the White House earlier in the year.

DDoS

December 2022

State-owned Russian bank VTB was hit by the most significant DDoS attack in its history, which affected customers' ability to access its mobile app and website.[10]

However, bank representatives cited by the same source reassured clients that their data has remained safe. The attack is thought to have originated from pro-Ukrainian hacktivists.

The data shows that the number and sophistication of BGP hijacks and DDoS attacks is increasing. Cybersecurity is therefore gaining more importance in today's era. To safely secure your company and avoid financial damages or compromising your company's reputation visit Anapaya.net and learn more about SCiON.

Visit anapaya.net

Sources

1 The Record, *KlaySwap crypto users lose funds after BGP hijack*, February 14, 2022

2 Security Boulevard, *DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense*, March 2, 2022

3 itnews, *Russian network 'hijacked' Twitter traffic*, Mar 29 2022

4 Reuters, *Hackers crash internet as 'Russian Davos' adjusts to new reality*, June 17, 2022

5 AppleInsider, *Russia tried to hijack some of Apple's internet traffic for 12 hours*, Jul 28, 2022

6 Ars Technica, *How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000*, 23 September 2022

7 Binance, *Celer Network's Multi-Chain Bridge Under DNS Attack*, 19 August 2022

8 SiliconRepublic, *Minecraft server targeted by a major DDoS attack*, 17 October 2022

9 DarkReading, *Killnet Gloats About DDoS Attacks Downing Starlink, White House*, November 29, 2022

10 Infosecurity, *Russia's VTB Bank Suffers its Biggest Ever DDoS*, 7 December 2022