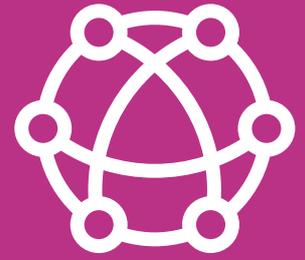


Border Gateway Protocol feeds: Block connections from malicious IP addresses at the network edge



What it is

Quick, automated traffic routing is essential for internet communications and Border Gateway Protocol (BGP) has become an industry standard enabling users to have a seamless experience.

By design, routers running BGP will accept advertised routes from other BGP routers by default. The automated nature of the system means that IP addresses with routing privileges are highly valued by cyber criminals but there is a way to block traffic at your network edge from the hijacked and malicious IPs used by criminals.

BGP feeds from Deteque provide an additional layer in your network security defenses by blocking connections to IPs involved in the most dangerous cybercrime and DDoS attacks.

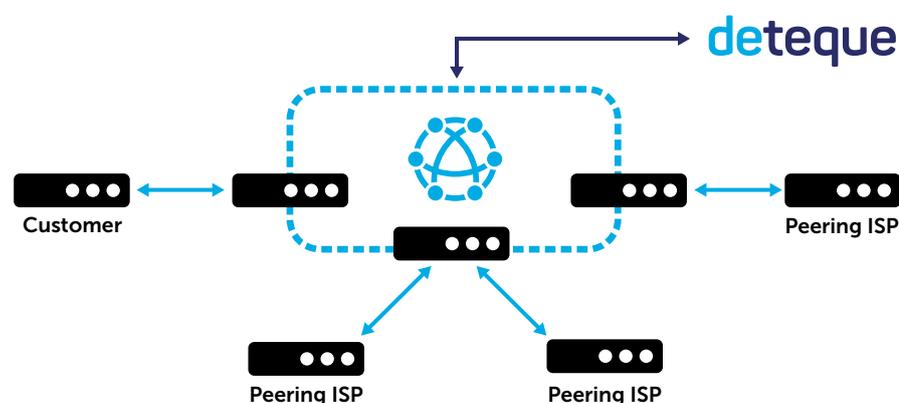
The BGP feeds include the latest Botnet Controller Lists (BCLs) and Do Not Route or Peer (DROP) data delivering almost instant updates to your edge router's DENY table and preventing any communication with listed IPs.

How it works

By taking just a few minutes to configure your edge router to peer with a Deteque BGP router and a null route, you can provide your network with the most up-to-date protection against botnets, phishing and external attacks on your organization's servers.

After installing BCL and DROP in your router's DENY table, all communication from, and to, C&C servers is blocked. This prevents infected computers within your network from receiving instructions and malware updates. BCL also prevents sensitive data from being sent from botnet nodes to C&C servers. Disrupting communication with the C&C servers neutralizes botnet nodes within your network and stops data egress, even though the devices have not yet had the malware removed.

When used in conjunction with intrusion prevention servers (IPS) and intrusion detection servers (IDS) such as Snort and Suricata, BCL identifies IP addresses of infected devices that are trying to contact botnet C&Cs and blocks traffic to and from these devices.



Data Feeds from Deteque disrupts communication with C&C servers, neutralizing botnet nodes within your network.

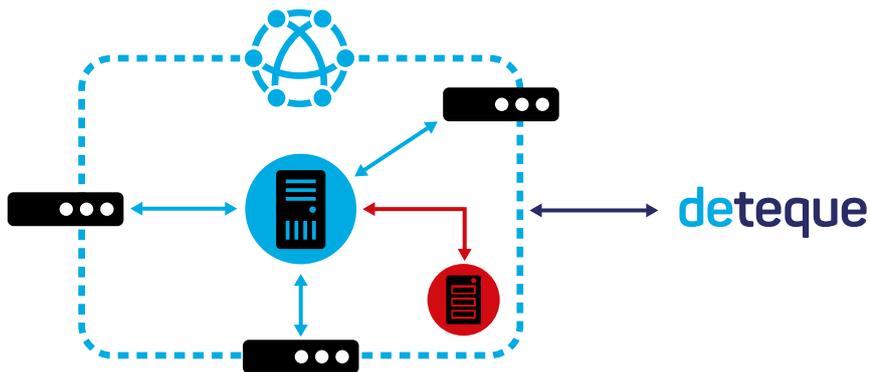
Why Deteque?

IP addresses included within the BCL have been manually researched by a team of Deteque security experts and is maintained as a zero false positive list. The IP addresses listed have been carefully researched and observed to be solely used for malicious activity and sending no legitimate email traffic.

BGP Case Study

A multi-national company with a dedicated IT subsidiary in charge of the local IT infrastructure for the home country, as well as being a large hosting provider for the organizations's online services and web portals. The IT subsidiary manages approximately 3,000 clients, mostly desktop and mobile systems as well as operating nearly 2,000 servers for the various online services and portals.

The organization's IT infrastructure was hit by a series of Distributed Denial of Service attacks (DDoS) aimed at bringing down parts of the network. The attacks lasted for several months with the IT team managing to mitigate the impact, finally tracking down the attacks which were associated with infected computers within the organisation's internal client network. The criminals had tried to exfiltrate data from inside the organisation with the DDoS attacks launched as a distraction from the actual crime being committed.



Client environment



3,000 clients
desktop and mobile



2,000 servers
eCommerce and portals



6,900 employees
in 30 countries worldwide

The results

As part of their protection strategy, the company subscribed to BGP data feeds and implemented both lists, DROP and BCL on their network.

The IT team 'sinkholed' the rogue IPs to a separate server under their own control which revealed several infected computers within the internal network that were infected with different pieces of malware. By using the sinkhole techniques, the IT team was able to identify up to ten infected computers on their internal network on a weekly basis, most of which turned out to be infected with a variant of the Zeus Trojan.

As soon as they implemented BGP data feeds and began sinkholing the malicious traffic, they reported that the DDoS attacks suddenly stopped and have registered a substantial decrease in subsequent DDoS attacks.

About Deteque

Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of security researchers who are dedicated to combating DNS abuse. Since 2008, Deteque has been at the forefront of securing networks by collecting, collating and delivering DNS-related threat intelligence to protect organizations in real-time. In addition to Passive DNS, Deteque also collates and delivers Response Policy Zones (RPZ) threat intelligence to block malicious domains and IPs used by cyber criminals to steal data, carry out fraud and exploit legitimate systems.

Follow Deteque:

- @deteque-llc
- @deteque
- 'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of
SPAMHAUS