CASE STUDY

ISP uses Border Gateway Protocol data feeds to improve DDoS protection

The challenge

Goldnet had been heavily hit by a DDoS attack that completely put their infrastructure offline for several hours and was only solved by de-localizing their DNS.

The organisation realized that DDoS attacks, even small ones, progressively intensified, slowing down, or temporarily blocking, part of their infrastructure and the services to their customers.

Goldnet started to look for a solution that could mitigate or definitively eliminate this problem without having to invest in new resources or install and maintain additional equipment.

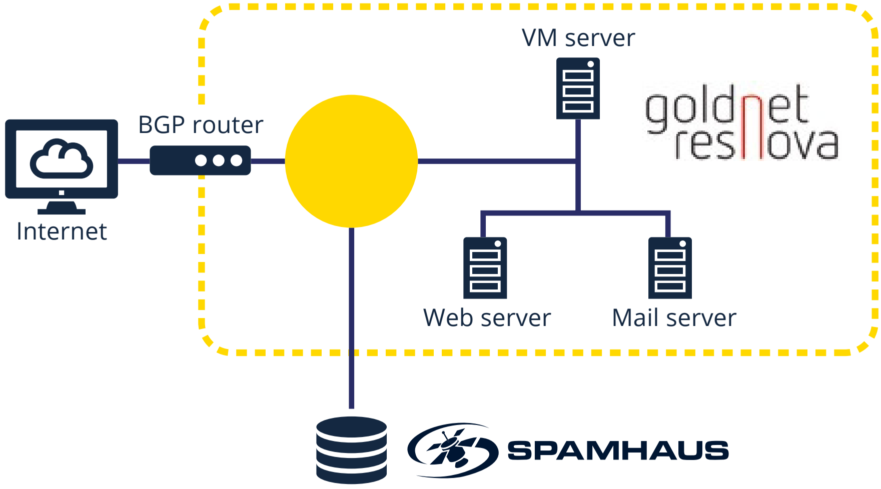
The solution

The security team identified the Spamhaus BGP data feed service as the best solution for their problem and simply configured their edge router with the parameters provided by Spamhaus.

BGP data feeds provides an additional layer in network security defenses. Any routers within your network that are peered with the Spamhaus BGP router will not be able to communicate with botnet C&Cs, preventing data egress and spamming from infected nodes on the network.

The results

Already after a few hours from the configuration on the edge router, the team noticed up to an 80% decline in spam traffic coming from infected or malicious servers. All this led to a reduction in workload for the company's servers and an increase in performance.



Who is Goldnet?

Goldnet is an Internet Service Provider operating since 1995 in the north east of Italy and hosts 100 Virtual Machines, over 2,000 domains and 5,000 mailboxes. It also offers connectivity, hosting, housing and web agency services.

Client environment

100
virtual machines

2,000
domains

5,000
mailboxes

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 Spamhaus 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 preventing any communication with listed IPs.

How it works

By taking just a few minutes to configure your edge router to peer with a Spamhaus 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 routing table, with a discard target, communication with 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.

Why Spamhaus?

IP addresses included within the BCL have been manually researched by a team of Spamhaus 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.

About Spamhaus

Spamhaus is the trusted authority on threat intelligence, uniquely placed in the industry because of our strong ethics, impartiality and quality of actionable data. This data not only protects, but also provides insight across networks and email worldwide.

With over two decades of experience our datasets are used by a wide range of industries including leading global technology companies, enterprise business and internet service providers. Currently our IP and domain datasets protect over three billion mailboxes globally.

Follow Spamhaus :

@spamhaustech
@spamhaus-technology-ltd
‘Spamhaus Technology’ channel

www.spamhaustech.com

About SecurityZones:
SecurityZONES is an authorized platinum distributor of Spamhaus and SURBL, providing datafeeds and solutions to improve your security defenses and prevent cyberattacks. As a trusted member of the internet eco-system for more than a decade, SecurityZONES works with customers around the globe to deliver the right data sets to best meet your cybersecurity needs. Learn more at SecurityZones.net

SECURITY ZONES
REALTIME THREAT INTELLIGENCE

SPAMHAUS