RADAR™ For Telcos – Full DDoS Coverage

Background

The telecommunications industry keeps the world connected - building, operating, and managing complex network infrastructures used for voice and data transmission.

With an ever-growing customer-base and technology disruptions, Telcos are encountering constant pressure to deliver innovative services at lower costs to retain their customers in a highly competitive market. Along with facing challenges related to network optimization and performance, technologies such as SDN, 5G, and NFV, they are now encountering the biggest challenge of all times – **Distributed Denial of Service attacks (DDoS).**

In 2020, the percentage of DDoS attacks on the telecom industry has grown by 31%

Known Published DDoS Attacks on Telcos

2020	USA	T-Mobile, Metro by T-Mobile, Verizon, AT&T, and Sprint	100,000 customers from T-Mobile and 30,000 from AT&T suffered the impact along with several more from other providers.
2020	Iran	Iranian Telecommunications	The attack impact was so powerful that the internet was disrupted across the country.
2019	S. Africa	Liquid Telecom and Webafrica	Large-scale volumetric DDoS attack with a ransom demand of 4.0 Bitcoin, with a confidentiality breach threat.
2019	S. Africa	Cool Ideas	Connectivity affected for customers across South Africa.
2018	Cambodia	EZECOM, SINET, Telcotech, and Digi	Hit by large-scale DDoS attacks affecting connectivity for customers.
2018	UK	O2	Users were unable to make calls, texts, or surf the Internet.
2017	China	NA	DDoS siege spanning over 11 days (277 hours) disrupted services across all services offered by the telecom company.
2016	Liberia	Several ISPs	Attacks at roughly 500Gbps preventing customers from reaching more than 1,200 domains.
2016	USA	Dyn	Unavailability of major Internet platforms and services to users in Europe and North America.

The Telcos DDoS Problem

DDoS threat to the Telco network has a significant impact for various reasons:

- Telcos operate many of the services that are most vulnerable to DDoS attacks such as NTP or DNS, increasing vulnerability levels.
- Telcos sometimes become the vectors through which large outages are created. If a service provider is attacked and the services allowing them to operate their network are compromised, an entire region can be compromised.
- Attacks on Telcos can cripple customers' services and temporarily bring them down. For example, during the Dyn DDoS attack, nearly 70 enterprises suffered outages.

When Telcos are impacted by a DDoS attack, an entire ecosystem of partners, customers, and enterprises, and in fact, sometimes an entire city or region is impacted. As a result, Telcos face damages that are significantly higher than other industries.

Why Mitigation is Not Enough

Telcos often rely on two popular DDoS mitigation solutions:

Black-Hole Service

DDoS Black Hole routing is seen as a DDoS countermeasure where attack traffic is directed to a `black hole' server which absorbs the attack (ideally without disruption to other services). This is used as a method to block attack traffic and protect genuine traffic. However, sophisticated attacks might use changing IP addresses and attack vectors, which can limit this method's effectiveness. More importantly, the hacker has accomplished his goal of disrupting traffic to the network service, as legitimate traffic is blackholed as well.

Clean-Pipe service

Clean-Pipe provides real-time traffic monitoring of IP addresses of customers that need to be safeguarded in the event of an attack. Clean-Pipe redirects the attack traffic to a mitigation platform where it will be analyzed and cleansed before being re-routed through the network to customers. Very often Clean-pipe services are not automated, resulting in downtime and high latency for customers as the Telco tries to figure out the issues and troubleshoot.

Closing the DDoS Security Gap – Introducing RADAR™

Both solutions ultimately require correct and precise identification of attack traffic, to successfully differentiate it from legitimate traffic. These detection mechanisms must be validated and adjusted on the go, as the environments they are protecting evolve. Otherwise the gaps are only going to show when an actual attack comes through.

RADAR™ continuously & without disruption, detects DDoS risks before an attack happens, not after, thereby ensuring that all three layers, i.e. layers 3, 4, and 7 are continuously checked.

Leaping ahead, RADAR™ tests environments against over 100 different types of DDoS attack vectors, from layers 3, 4 & 7 attacks. By simulating DDoS attacks, RADAR™ simulates in a non-disruptive manner 50,000 to 100's of thousands of DDoS attack vectors a year. By taking a DDoS risk-based approach it prioritizes vulnerabilities to reduce the time and effort needed to close the highest risk vulnerabilities safeguarding all three layers.

Benefits of RADAR™ for the Telco Industry

Working as a top layer on any mitigation solution, RADAR™ eliminates in advance any chance of downtime if attacked. Giving Telcos a full risk-based DDoS protection, through continuous DDoS mitigation gap detection & remediation and zero impact on ongoing IT systems.

Where required, DDoS testing is drastically cut due to full ongoing DDoS intelligence reports, and DDoS defenses are at maximum effectiveness. RADAR™ provides a far superior ROI and performance for DDoS mitigation, risk management, ongoing vulnerability elimination, and infrequent Red team testing.

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com