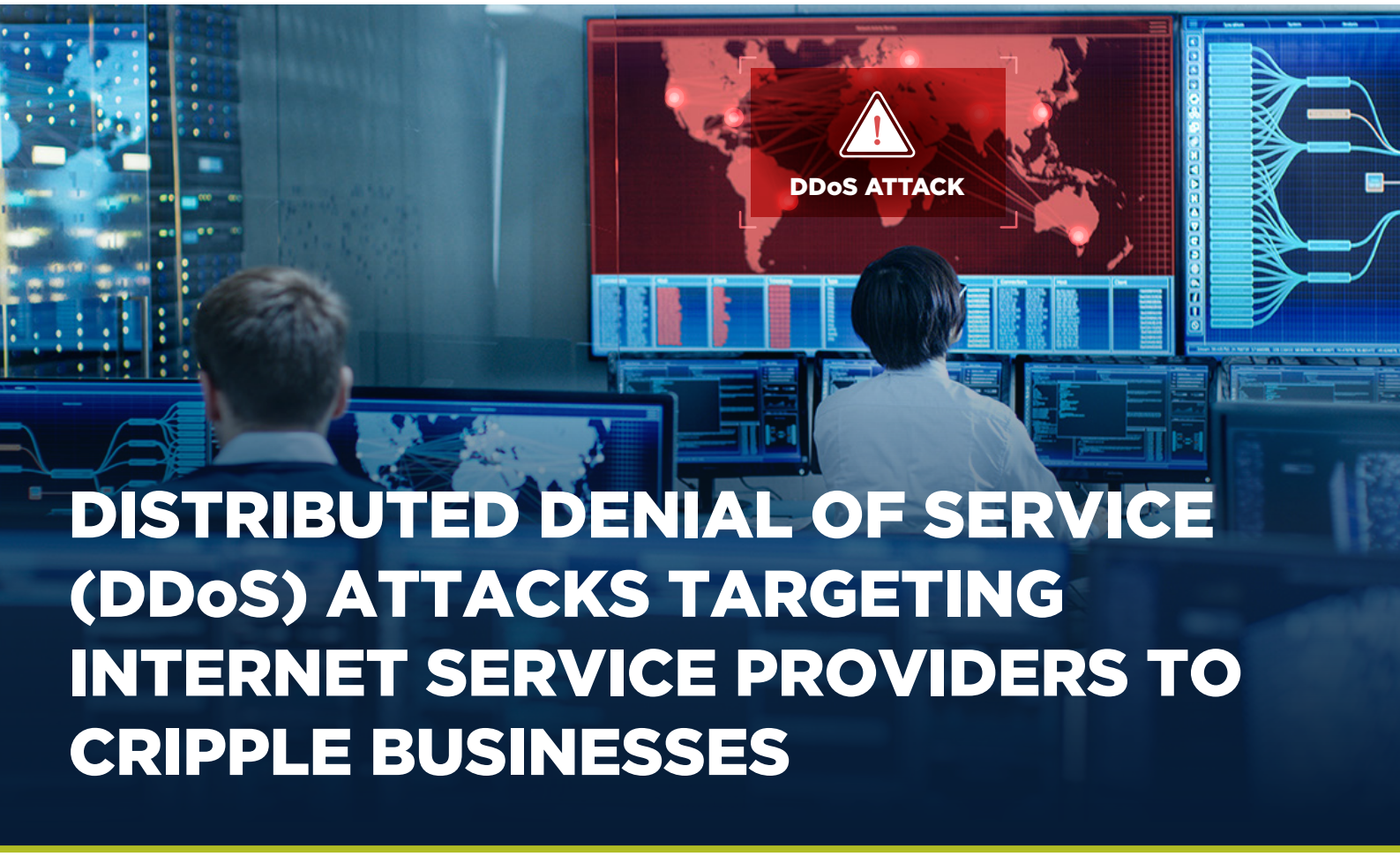

DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS TARGETING INTERNET SERVICE PROVIDERS TO CRIPPLE BUSINESSES

Internet Service Providers (ISPs) are a prime target for DDoS attacks in a world that's increasingly dependent on the Internet for learning, entertainment, shopping, communications, and work. In the first half of 2021 alone, cybercriminals launched approximately 5.4 million DDoS attacks. During this period, multiple ISPs in Europe were targeted, causing major operational disruption for the businesses connected to them. In fact, the DDoS attack on the Belgian ISP Belnet adversely affected 200+ institutions connected to the Belnet network, including the Belgian parliament. Similar attacks have been observed in other parts of the world including India. These attacks have gained momentum in the last month and seem to be systematic attempts to derail critical infrastructure and services around the festive season. This shift can be seen as another mutation of the recent spurt in 'supply chain attacks' whereby attackers attempt to breach the integrity or availability of critical providers in the enterprise value chain, eventually leading to high impact on businesses that depend on these critical services.

Tata Communications cybersecurity analysts have been closely monitoring this trend and have successfully thwarted several such attacks targeting ISPs in India. We've found that while the attacks started with a few targeted broadband providers in early October 2021, the pattern has evolved, so that by the end of the month, attacks were targeting multiple broadband providers simultaneously. Most such attacks were designed to flood an ISP's network with malicious traffic – consuming all available bandwidth and rendering the network unavailable to legitimate users.

Furthermore, our analysts observed a 30-fold increase in DDoS attacks in October 2021, compared to the volume recorded in September 2021.

> A deeper analysis of the data found that these attacks were focused on services that are used extensively during the festive season, including media streaming, Internet phone services and online gaming.

Potential impact on ISPs

The downtime caused by a successful DDoS attack can inflict tremendous damage upon any organisation, including:

- Lost revenue
- Loss of brand reputation
- Decreased productivity

The consequences can be much more serious when it comes to ISPs that form part of a nation's critical infrastructure. The stakes have become even higher in the wake of the pandemic, with enterprises relying heavily on their networks to maintain business continuity.

How can ISPs protect themselves

- Understand and baseline your current environment – in particular regular volumes of traffic – and put appropriate logging mechanisms in place at frequent intervals
- Review traffic patterns and logs to detect anomalies in network and application-level floods
- Stay vigilant to sudden surges in inbound traffic to critical servers or services, such as ICMP or UDP/TCP floods
- Enable alerts to act as soon as anomalies are spotted, before any major damage occurs.
- To achieve the above, deploy an appropriate intrusion/DDoS prevention solution through a reputable provider
- As recent DDoS attacks are becoming bigger, ensure you have scalable service contracts to adequately protect you against larger-volume threats
- Update your critical incident management processes, and keep an updated contact and escalation database to maintain lists of contacts for vendors of network and security devices

In these challenging times, it's crucial to stay aware of the ongoing DDoS threat targeting ISPs and to put in place best practices to defend against attacks. Working with an experienced partner like Tata Communications will help strengthen your business defences.

How Tata Communications world-class anti-DDoS solution is protecting customers

As you read this article our DDoS protection is probably mitigating a minor or a major attack for our customers globally. Our DDoS mitigation starts almost instantaneously when you subscribe to our auto mitigation feature. Our globally distributed Tier1 scrubbing farms mitigate attacks close to source thereby thwarting attempts to disrupt your business. Our 24x7x365 AI/ML based CSRC continuously monitors for anomalies and feeds the intelligence for quick, faster protection. In nutshell, a comprehensive DDoS protection that gives you peace of mind!

To know more and discuss your DDoS defence strategy, contact us today.