INDUSTRY TRENDS IN DDOS ATTACKS



Rapid growth in attack volume: DDoS incidents rose by 186% in early 2024, 75% of these were carpet bombing attacks, emphasizing the rise of a new attack vector.1



Shift to sophisticated methods:

Attackers increasingly use multi-vector and distributed techniques like Carpet Bombing to evade detection.



Soaring costs of downtime: DDoS attacks now cost \$6,000 per minute on average.²



Focus on key infrastructure:

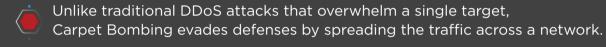
Cybercriminals are targeting critical industries such as finance, healthcare, and telecom with distributed DDoS techniques.



CARPET BOMBING



A distributed DDoS strategy that floods a network by targeting multiple IP addresses simultaneously.



Results in network-wide disruptions and is harder to detect using conventional methods.



Widespread downtime:

Interrupts services across multiple nodes, leading to operational inefficiencies and revenue loss.



Strained infrastructure:

Overloads routers, firewalls, and application servers, affecting legitimate users.



Financial impact:

Significant financial losses on victims and loss of consumer trust in the target company



CHALLENGES IN DETECTION



Hidden intentions: Broad targeting conceals the attacker's true focus.



Enhanced volume: Combines with amplification techniques for higher impact.



Stealthy nature: Traditional detection tools struggle with the



dispersed nature of traffic in Carpet Bombing attacks.



Increased damage: More disruptive than traditional DDoS methods.

HOW TATA COMMUNICATIONS CAN HELP

Profile-Based Detection:

A cutting-edge solution to effectively combat distributed and sophisticated attacks like Carpet Bombing while maintaining operational resilience. With Network-Wide Monitoring, it tracks traffic across the aggregated customer network to detect anomalies.



Aggregates NetFlow data from multiple distributed sites for holistic insights.



Customer-Centric Approach: Groups traffic based on customer IDs to ensure tailored detection.



Identifies lowvolume distributed attacks, including those targeting multiple IPs.

CUSTOMER BENEFITS



Proactive Threat Mitigation: Stay ahead of advanced threats with real-time detection and response.



Enhanced Network Stability: Prevent service disruptions and maintain smooth operations.



Tailored Protection: Customer-specific grouping ensures precise and targeted detection.

Operational Confidence: Minimise downtime, protect brand reputation, and safeguard user trust.

SECURE YOUR NETWORK TODAY WITH TATA COMMUNICATIONS' INDUSTRY-LEADING DDOS SOLUTIONS!

SOURCE: Vercara Bi-annual DNS and DDoS Traffic and Trends Analysis report Cybermaterial









CONTACT US in 0