

MSS : MULTI-LAYER DDoS PROTECTION

# DEFEATING THE EVOLVING MULTI-LAYER DDoS THREAT

STEP UP TO **PROTECT** YOUR BUSINESS AVAILABILITY

NOVEMBER 2016 | TATA COMMUNICATIONS

On New Year's Eve 2015, the world became a much more perilous place when a group calling itself New World Hacking brought down the main BBC website and associated services such as the iPlayer catch-up service and iPlayer Radio app. Even more disturbing, the group claimed that the attack was only a test, saying that "We didn't exactly plan to take it down for multiple hours."

## A CLEAR, PRESENT AND INCREASING DANGER

As evidenced by the BBC and similar attacks in 2016, the cyber threat landscape has morphed into a far more dangerous and challenging place. In the early days of DDoS attacks, hackers simply flooded network pipelines with traffic, overwhelming connections to servers. These high-bandwidth "volumetric" attacks were simply designed to take down servers and networks. Today, the emerging trend in DDoS is the multi-layer attack that combines flood attacks with application and state exhaustion attacks, all targeted against infrastructure devices in a single, sustained onslaught. Since these attacks generally consume less bandwidth, they're easier to launch, stealthier, and far more difficult to detect and defeat compared to volumetric attacks. What's more, they can have a catastrophic impact on business availability by threatening critical HTTP, DNS, VoIP, and SMTP applications, and shutting down websites and web-based services.

has increased four times more than attacks on other industries. And it's getting worse by the day. Verisign's "Distributed Denial of Service Trends Report" for the first quarter of 2016 found that the financial sector experienced a 15% increase in DDoS attacks from Q4 2015, with an average attack size of 23 Gbps. These attacks are also incredibly damaging and costly. A bank under DDoS attack can lose up to \$100,000 US an hour.<sup>2</sup>

**"No matter how prepared an organisation thinks it may be, DDoS attacks continue to take organisations by surprise and take websites offline, rendering them inaccessible for hours or sometimes for days."**

— Verisign "Distributed Denial of Service Trends Report" (Q1 2016)

## DDOS ATTACKS ARE SKYROCKETING

The first quarter of 2016 saw a:

- 125.36% increase in total DDoS attacks
- 142.14% increase in infrastructure layer (layers 3 & 4) attacks
- 34.98% decrease in the average attack duration: 16.14 vs. 24.82 hours
- 137.5% increase in attacks greater than 100 Gbps: 19 vs. 8

## Media and entertainment CSOs: after a DDoS attack, the show won't go on

In Q2 2016, media and entertainment companies were the target of a string of DDoS attacks reaching 67.8Gbps in magnitude according to a report from Verisign. Though media executives are reluctant to admit security problems, 28% of survey participants said their organisations have experienced a cyber-attack or data breach. Almost all indicated that one or more of their corporate web sites were forced offline because of the incident. A quarter of those surveyed also said that their corporate data was breached as a result of the cyber-attack, with 38% suffering a loss of corporate intellectual property.<sup>3</sup>

Not only that, DDoS attacks are being launched against consumers as well. Just one example is what happened to Gabriel Menezes Nunes. While running an hping command on his Sony Bravia TV, Mr. Nunes was stunned to discover that his TV was under a DDoS attack at that very moment!<sup>4</sup>

## WHO IS MOST AT RISK?

### Financial Services CSOs: protection against DDoS attacks — a wise investment

According to a new report from Websense Security Labs, the average number of attacks against Banking, Financial Services and Insurance (BFSI) enterprises

For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Contact us

Share



© 2016 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries. 105110 v10

## Gaming Industry CSOs: hackers are competing to bring you down

Gaming continues to be one of the most desirable targets of DDoS attackers. These attacks are not only focused on pure gaming sites, but on any company associated with online gaming or gaming-related content. Aside from financial gain, hackers are targeting these sites to gain notoriety and respect from other hackers. DDoS attacks are also being used by game players to gain a competitive advantage, as well as by malicious actors seeking to steal personal data from players.

Hackers, such as the Lizard Squad, are using attacks as a business strategy. They successfully launched a DDoS attack that overloaded the networks of both the Playstation Network and Xbox Live. The attack was staged to promote their new online attack tool, LizardStresser, which can only be described as “DDoS attacks as a service.” Offered to anyone who is willing to pay for it, the LizardStresser service is available in various packages, ranging from \$6 to \$500, depending on the length of attack.<sup>5</sup>

## CEOs: your enterprise, brand, and reputation are at risk

Today, concern about DDoS attacks goes beyond the purview of CSOs, CIOs, and the IT department. CEOs are now deeply worried about the potentially devastating consequences of these attacks. The 2015 Neustar DDoS Attacks and Protection Report that surveyed more than 500 senior executives confirms the depth of this concern: 40% believe that DDoS attacks are an increasing threat to their organisation. 30% of the enterprises have been attacked more than 10 times a year. And 26% of those attacked have suffered a loss of customer trust and damage to their brand image.<sup>6</sup>

## CFOs: the bottom line – it’s all about money

One of the most feared consequence of a DDoS attack is lost revenue according to 34% of the executives polled in Corero Network Security’s second annual DDoS Impact Survey. Nearly 45% also indicated that the most damaging effect was a loss of customer trust and confidence. Today, the median annual cost of a cyber attack is \$3,800,000 and increasing according to the Ponemon Institute’s 2015 Cost of Data Breach Study. In fact, the cost has increased 23% since 2013.<sup>7</sup>

## CMOs: protecting your customers is now a marketing initiative

A sophisticated, devastating DDoS attack can spell disaster for any company, destroying years of brand building. The results of the Neustar 2015 DDoS report confirm that fact,

finding that fully 40% of companies that suffered a DDoS attack lost customer trust and incurred damage to their brand. “When a customer visits a website, they expect an experience that is both responsive and secure,” said Margee Abrams, CISSP, director of security services at Neustar. “A security breach or website that’s inaccessible or sluggish as a result of a DDoS attack can have a devastating effect on consumer trust and equity that the brand spent time and treasure to once establish.”<sup>6</sup>

## HOW TO COMBAT MALICIOUS, MULTI-LAYER DDoS ATTACKS

Application-layer attacks can be especially difficult to proactively detect in the cloud since they’re hard to differentiate from genuine traffic. Many security experts believe that the solution to this dilemma is a multi-layered defence. On-premise protection at the network perimeter can react immediately to prevent infrastructure and service availability from being impacted by an application-layer or state-exhaustion attack. But on-premise protection alone does not provide a complete solution. An attack can escalate in size, saturating Internet connectivity, at which point network perimeter defences will not help. A cloud-based service is required to deal with higher magnitude attacks, where sufficient capacity and capability exists to deal with these high-volume attacks.

### The Arbor Networks Availability Protection System (APS)

Tata Communications has partnered with Arbor Networks to offer a uniquely effective cloud signalling approach that combines the Tata Communications cloud with on-premises DDoS protection - the Availability Protection System (APS)

**“We believe that the best defensive posture against the modern DDoS threat is a layered approach that combines on-premise and cloud-based protections. Only then will your organisation be protected against the full spectrum of DDoS attacks”**

—Gartner, ‘Master These Eight Steps to Control the Damage from DDoS Attacks’

This innovative solution augments the Tata Communications MDDoS service to detect and block DDoS threats in real time. Deployed at the enterprise network perimeter, APS disrupts botnet communications while detecting and blocking application-layer DDoS attacks, including those designed to compromise stateful inline tools such as firewalls.

For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Contact us

Share



© 2016 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries. 105110 v10

The Cloud Signaling™ functionality in APS provides a faster, automated way to prevent DDoS attacks. An efficient and integrated way of connecting the enterprise with the Tata Communications cloud, Cloud Signaling functionality connects the on premise APS device with the Tata Communications DDoS Protection cloud. Arbor believes that the best way for enterprises to have optimal protection against DDoS attacks is through this combination of on-premise and in-cloud defences which provide a multi layered security architecture.

“Hybrid defence scenarios (on premise equipment married with cloud services) will become more prevalent as organisations seek to defend against all vectors of DDoS attacks and as solution providers and product vendors work more closely together to deliver joint solutions.”

– IDC, Worldwide DDoS Prevention Products and Services 2013-2017 Forecast

Here’s how it works. When enterprise or data centre operators discover that they are under a service-disrupting DDoS attack, they can mitigate the attack in the cloud. Using the Cloud Signaling system, they simply click

on a drop down menu, triggering a signal to the Tata Communications cloud/SOC. This fast, efficient, proactive approach allows them to stay in command of the event. A volumetric DDoS attack congesting upstream links will immediately diminish or completely disappear from the data centre access links, protecting service availability. Both enterprise and managed services customers benefit from this real-time monitoring of the attack mitigation, followed by granular post mortem reports that provide details of the attack.

### A LONG AND CLOSE PARTNERSHIP DEFEATING SECURITY THREATS

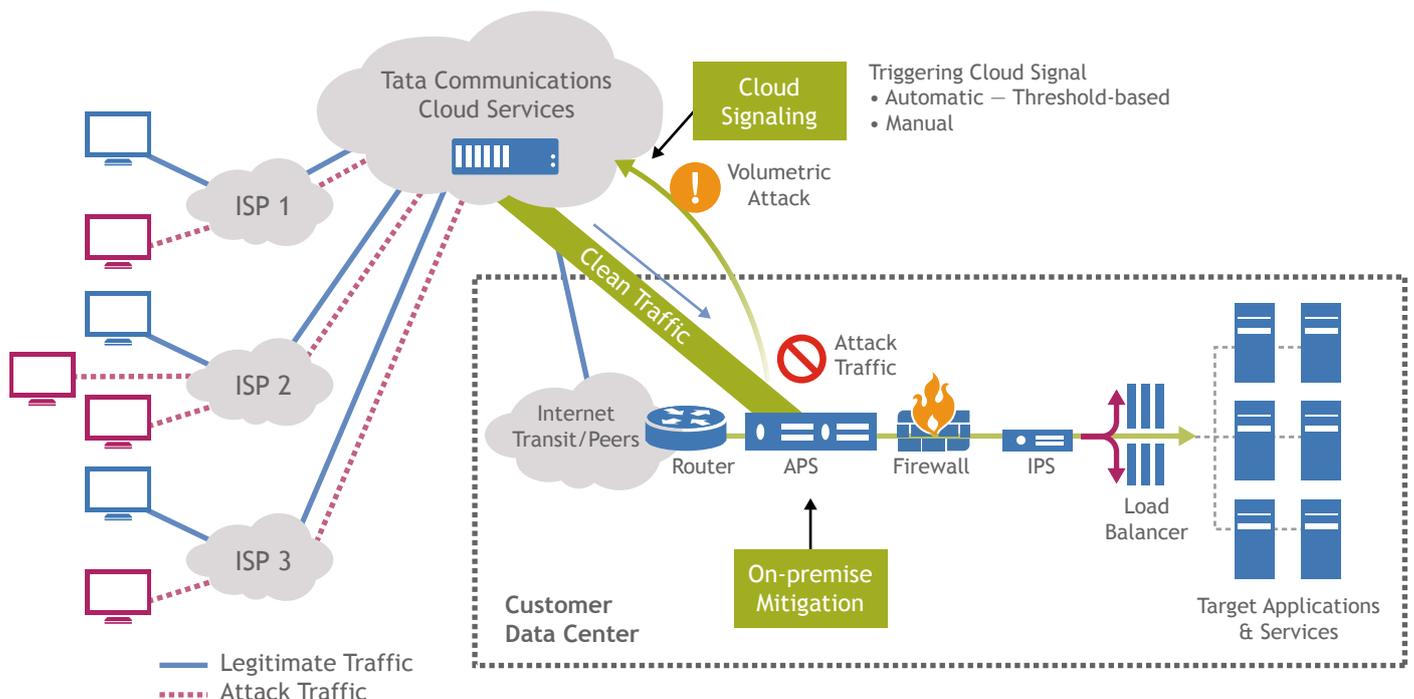
TATA COMMUNICATIONS



The strong working relationship between Tata Communications and Arbor Networks goes back many years. Tata Communication was Arbor’s first customer in India, protecting its infrastructure from DDoS attacks using the Arbor SP/TMS platform. After seeing how successful the combination was, Tata Communications was then able to confidently offer DDoS protection to its enterprise customers.

Since then, Arbor and Tata Communications have worked together to evolve the solution to meet the increasing security needs of today’s enterprises. Hackers and hacking tools have become very sophisticated and target specific

### A TYPICAL DEPLOYMENT OF THE TATA COMMUNICATIONS CLOUD & ARBOR APS SOLUTION



For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Contact us Share

applications. As a result, multi-vector attacks have become commonplace with the size of the attacks growing in magnitude.

In order to protect their customers against such sophisticated attacks, Tata Communications and Arbor Networks have together developed this multi-layer DDoS architecture to defend enterprise networks and defeat these attacks in real time. The two companies have created excellent synergy and feedback mechanisms to develop, test, prove, and implement the technology needed to protect your enterprise from the ever-evolving universe of threats.

**For information and answers to your questions about detecting and defeating multi-layer DDoS attacks please email:**  
[gsmc-ddos.protection@tatacommunications.com](mailto:gsmc-ddos.protection@tatacommunications.com)

## REFERENCES

1. <https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp>
2. <http://www.cutimes.com/2016/05/26/ddos-attacks-up-15-in-financial-sector-verisign>
3. <https://digitalcontentnext.org/blog/2016/01/05/security-concerns-in-the-media-and-entertainment-industry/>
4. <http://arstechnica.com/business/2012/04/tv-based-botnets-ddos-attacks-on-your-fridge-more-plausible-than-you-think/>
5. <http://www.pcmag.com/article2/0,2817,2474386,00.asp>
6. <https://www.neustar.biz/resources/whitepapers/ddos-attacks-protection-report-us-2015>
7. <http://www.firstpost.com/business/cost-data-breach-time-high-3-8-mn-climbing-2272564.html>

---

For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Contact us

Share



© 2016 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries. 105110 v10

Tata Communications Limited  
VSB, Mahatma Gandhi Road,  
Fort Mumbai, 400 001  
India

### About Tata Communications

Tata Communications Limited (CIN no: L64200MH1986PLC039266) along with its subsidiaries (Tata Communications) is a leading global provider of A New World of Communications™. With a leadership position in emerging markets, Tata Communications leverages its advanced solutions capabilities and domain expertise across its global and pan-India network to deliver managed solutions to multi-national enterprises, service providers and Indian consumers.

The Tata Communications global network includes one of the most advanced and largest submarine cable networks and a Tier-1 IP network, as well as nearly 1.5 million square feet of data centre and collocation space worldwide.

Tata Communications' depth and breadth of reach in emerging markets includes leadership in Indian enterprise data services and leadership in global international voice.

Tata Communications Limited is listed on the Bombay Stock Exchange and the National Stock Exchange of India.

[www.tatacommunications.com](http://www.tatacommunications.com) | [tata\\_comm](https://twitter.com/tata_comm)  
[tatacommunications-newworld.com](http://tatacommunications-newworld.com) | [www.youtube.com/tatacomms](http://www.youtube.com/tatacomms)

---

For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Contact us

Share



© 2016 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries. 105110 v10