TATA COMMUNICATIONS

MSS : MULTI-LAYER DDoS PROTECTION

DEFEATING THE EVOLVING MULTI-LAYER DDoS THREAT

STEP UP TO PROTECT YOUR BUSINESS AVAILABILITY

JUNE 2017

In 2017, a number of high profile cyberattacks have compromised the reputation and bottom-line of various multinational corporations – as well as affecting critical national infrastructure in several countries. As a result of their unprecedented size and scale, these recent cyber-attacks have transcended the business and security worlds and have broken through to the wider public consciousness.

A CLEAR, PRESENT AND INCREASING DANGER

As evidenced by high-profile attacks such as WannaCry and Petya, the cyber threat landscape has morphed into a far more dangerous and challenging place. And yet some tactics remain as popular as ever – reports of DDoS assaults being used to reignite the fading embers of ransomware continued months after the initial shockwave. 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.

DDOS ATTACKS ARE SKYROCKETING[1]

The first quarter of 2016 saw a:

125.36% increase in total DDoS attacks

138% increase in attacks over 100 Gbps in Q3 2016 from previous year

(source: https://www.theregister.co.uk/2016/12/16/ddos_in_2017_strap_yourself_in_for_a_bumpy_ride/)

48.2% increase in average attack duration: Q1 2016 vs Q4 2016

(source: https://securelist.com/kaspersky-ddos-intelligence-report-for-q1-2016/74550/ & https://securelist.com/ddos-attacks-in-q4-2016/77412/)

10% increase in number of countries targeted for DDOS attacks: Q1 2016 vs Q4 2016

(source: https://securelist.com/kaspersky-ddos-intelligence-report-for-q1-2016/74550/ & https://securelist.com/ddos-attacks-in-q4-2016/77412/)

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 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.[2]

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

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

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 67.8G bps 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 were breached as a result of the cyber-attack, with 38% suffering a loss of corporate intellectual property.[3]

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! [4]

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.[5]

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 organization. 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. [6]

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. [7]

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." [6]

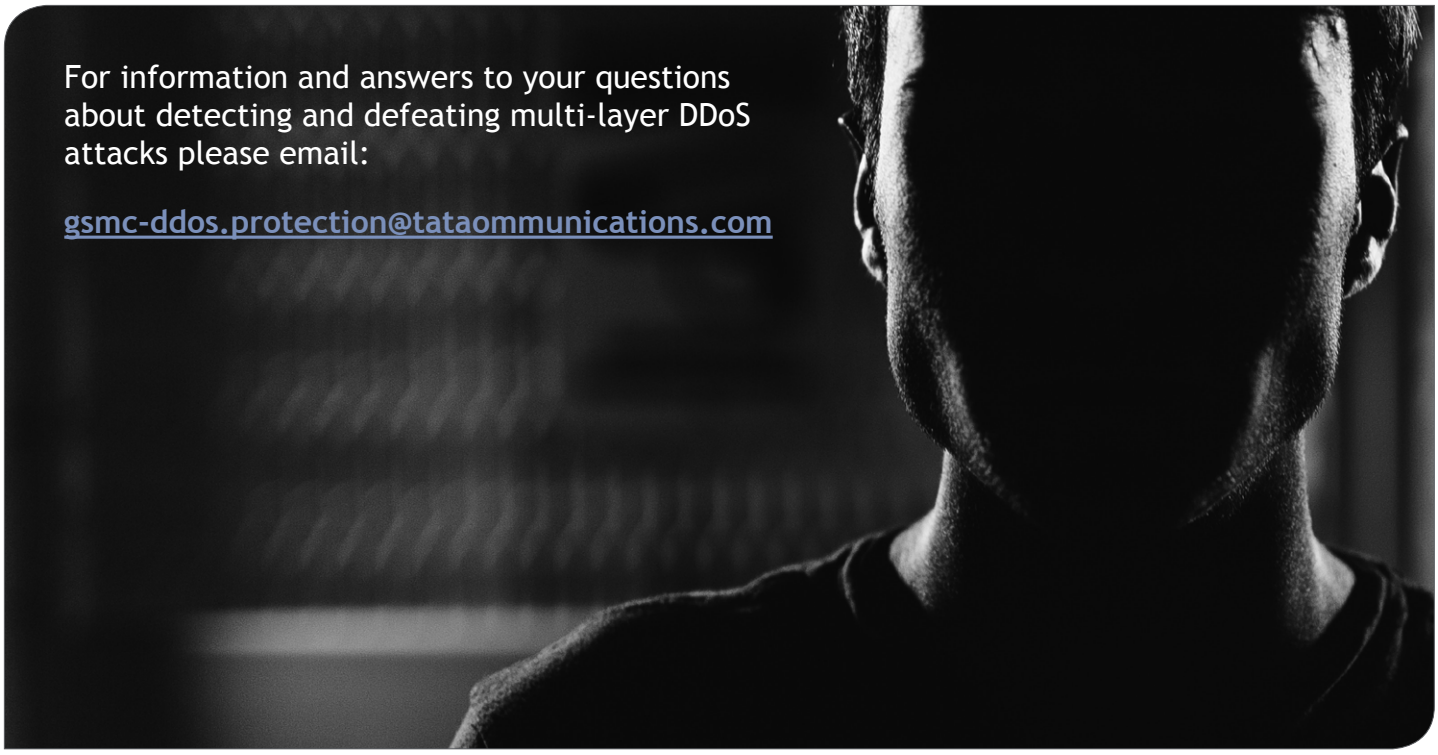
HOW TO COMBAT MALICIOUS, MULTI-LAYER DDOS ATTACKS

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.

"We believe that the best defensive posture against the modern DDoS threat is a layered approach that combines onpremise 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'



REFERENCES:

1. https://www.akamai.com/us/en/about/ourthinking/state-of-the-internet-report/global-stateof-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

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 | tata_comm
http://tatacommunications-newworld.com | www.youtube.com/tatacomms

For more information, visit us at www.tatacommunications.com