efficient iP™
DEFINING SMART DDI

Press Release

Current DNS Filtering Security Solutions Won't Protect You!

Reading, UK, January 8th, 2015 : On Dec 22nd, Rackspace stated on their official Google+ page that their DNS suffered a DDoS attack on 3 of their data centers. Their services were restored after 12 hours. When they discovered the attack they tried to mitigate it by blocking inbound traffic. Most of the time the blocking mechanism is done through filtering of DNS queries; unfortunately, it is very difficult and almost impossible to filter legitimate versus non-legitimate traffic.

The impact of filtering can result in the blocking of legitimate traffic. Rackspace said that, "*In order to stabilize the issue, our teams placed the impacted DNS infrastructure behind mitigation services. This service is designed to protect our infrastructure, however, due to the nature of the event, a portion of legitimate traffic to our DNS infrastructure may be inadvertently blocked. Our teams are actively working to mitigate the attack and provide service stability.*" They added later on that, "*After blocking the majority of the inbound DDoS attack earlier in the morning some DNS servers that were sending both legitimate and DDoS traffic to Rackspace were blacklisted.*"

The filtering protection mechanism can even become a driving mechanism used by hackers at the expense of the customer it is supposed to protect. To avoid the risk of «false positive», the filtering system should be able to start doing the analysis at the DNS transaction level over a period of time in order to rebuild all DNS messages (queries, responses, fragments, recursions) and resolutions requested by customers. The system should store, index and analyze very large amounts of data while answering simultaneously to legitimate traffic, all without causing additional latency in time. With existing solutions, it is almost impossible to achieve and the unfortunate events that Rackspace experienced prove this.

The first thing to remember is that we want to ensure the availability of services to customers. To mitigate a DNS DDoS attack with existing filtering limitations, the DNS server will have to answer all queries. The DNS server should also be able to absorb all the traffic, up to the physical network capacity, if you want the DNS service to still answer to queries.

Answering all DNS queries will solve several problems: Cache poisoning because of a DNS time out Filtering wrong black list Crashing of the DNS server because of the workload Of course, it should be done without piling up dozens of DNS appliances, load balancers and/or firewalls to absorb the DDoS attack.

In June 2014 we announced SOLIDserver™ DNS Blast, the only solution available today that can answer up to 17 Million (17M) queries per second (QPS) with just one appliance; it's more than what any network can handle. With DNS Blast, there would have been no impact on the DNS service from the DDoS attack because the workload would have been absorbed. DNS Blast is the answer to ensuring DNS service availability to end users. To mitigate other DNS threats, SOLIDserver™ includes other DNS security features like RRL, Hybrid DNS Engine, Stealth DNS architecture and much more.

ABOUT EFFICIENTIP

EfficientIP, one of the fastest growing DDI vendors provides solutions to address organizations' needs to drive business efficiency through network services availability, security and performance. EfficientIP customers can ensure that their network infrastructure truly supports the business imperatives, ranging from business continuity and availability to reduce time-to-market for new products, services, and locations. Its unified management framework for DNS,DHCP & IPAM devices and network configurations enhances security, availability, and agility of the networks infrastructure. Customers worldwide across industries rely on EfficientIP offerings to enable policies to be applied and business processes to be automated that reduce operating costs and increase management efficiency. EfficientIP's offerings are complemented by technologies and services from global business partners. For further information, please visit: www.efficientip.com

EUROPE

EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes
FRANCE
+33 1 75 84 88 98

USA

Efficient IP Inc.
17 Wilmont Mews, Suite 400