COUNTERING THE THREAT OF VOLUMETRIC & APPLICATION DDOS ATTACKS

N4PROTECT DDOS SERVICE

PUBLIC

NODE4 LIMITED

26/11/2015

INTRODUCTION

This whitepaper lays out some of the history and reasoning as to why these trends and types of attack are prevalent and also describes the different types of attacks and the techniques attackers are using to thwart standard responses to DDoS (Distributed Denial of Service) attacks. The paper describes what best practices organisations need to adopt in order to mitigate against such attacks.

Recent headline news has brought hacking attacks such as DDoS firmly into the media spotlight. In October 2015 a fifteen-year-old boy from Northern Ireland was arrested under the Computer Misuse Act, he was believed to have been involved in a recent DDoS attack against TalkTalk. In turn, TalkTalk saw around 12% fall in their share price after a series of security breaches over an eight month period. Subsequently customers complained of losing money from criminal scams which allegedly purported to be from TalkTalk customer services. It is expected that TalkTalk will have to pay millions of pounds in compensation as well as fines to the ICO (Information Commissioner Office) for admitted data breaches. This was just the latest of DDoS attacks to make the news, the increase in attacks has substantially grown over the past twelve months and currently sees no signs of diminishing.

The rules around the way we should hold data are also set to change which should make the issues of DDoS and data breaches high on the radar as the implementation of the EU's new General Data Protection Regulations (GDPR), which is due to come into force sometime in early 2016 with full enforcement by early 2018. The new legislation exceeds the remit of the 1995 Data Protection Directive and eventually will affect most companies inside the EU and those outside who operate inside. Initially it will affect all organisations with more than 250 employees processing over 5,000 records per annum although by the full implementation small enterprises of all sizes and records will eventually subject to the legislation. Breaching the new regulation will see fines of at least 2% of global turnover or 1 million Euros, whichever is greater.

HISTORY

Since the early '90s DoS (Denial of Service) has been used as weapon in the arsenal of online activists motivated against various companies and local government departments for a variety of political and individual reasons. Back in 1995 an Italian collective called *Strano Network* launched a DoS attack against the French government as a protest against their nuclear policy. Back in the 1990's DoS attacks were a heavily manual affairs to orchestrate, requiring hackers to constantly input command strings at a computer terminal, thus attacks were fairly short lived. Also in the 90's a hacktivist group called the Electronic Disturbance Theatre attracted media attention when they organised "virtual sit-ins" and recruited computer programmers to attacks web sites associated with oppressive regimes.

In 2005, 18-year-old Farid Essabar, was arrested for distributing MyTob. The MyTob worm opened a backdoor on infected MS Windows hosts that opened the door for massive DDoS attacks that could compromise an untold number of hosts infected by the worm and execute commands sent over IRC. CNN covered the outbreak live, even as the station's own computers fell victim.

In recent years an organisation has emerged known as *LulzSec,* a black hat computer hacking group responsible for several high profile attacks including Sony Pictures in 2011 and also taking the CIA website offline. In October 2015 they claimed responsibility for some of the DDoS attacks on TalkTalk.

CURRENT TRENDS

It is not just over the last twelve months that DDoS attacks have increased. Akamai's 2015 report "*State of the Internet*" indicates that there was a 35% increase in DDoS activity in 2015 Q1 compared to 2014 Q4. Of the reported attacks (of which it is assumed that these fall far short of actual attacks), the Gaming industry accounted for 35.32% of attacks, followed by Software & Technology industries with 25.19% of the attacks. Today there is a far more sinister and organised backdrop to attacks including organised crime syndicates using DDoS as an extortion tool, as well as anonymous DDoS attack services providing cheap automated assaults which non-technical malcontents can purchase online for the price of a pint of beer. The proliferation of anonymous attack services and non-technical attack applications has created a much larger pool of miscreants of which have accessible, cheap and easy methods of executing attacks.

Who are the criminals and what is the purpose of attacks? Not all are perpetrators like the politically motivated "hacktivist" groups such as "Anonymous" or even cybercriminals such as DD4BC. Recent attacks have indicated that some industry sectors whose sole income is transacted via web servers are looking at "freezing out" the competition during key periods by orchestrating multiple DDoS attacks at their competitors thus scooping up customers left bereft of their regular providers.

In the past it might have been valid for a small company or organisation to claim that they were too small or did not have the profile to be targets for DDoS attacks, but increasingly aggrieved ex-employees or even amoral competitive companies can orchestrate almost instantly attacks against any URL or IP address they wish.

DDoS attacks usually make the headlines when they target high-profile institutions. Earlier in 2015 the websites affiliated with the football World Cup were brought down by a DDoS attack in protest against FIFA. Also in 2015 there were a series of extortion attempts when a group called DD4BC (DDoS for BitCoin) threatened to incapacitate a variety of business enterprises in the UK and US. Most of the companies threatened were not high-profile organisations but had highly integrated business processes inside IT systems which were integral to revenue streams. DDoS perpetrators are using social media to embarrass and advertise their targets inability to prevent.

Android Phone Screenshot of LOIC

2012 saw a sharp increase in volumetric DDoS attacks; one of the reasons for this is the advent of one of the most prevalent of DDoS attack tools; LOIC (Low Orbit Ion Cannon) which can be downloaded for free and automates DDoS attacks from many platforms, including mobile phone.

Like so many IT technologies, DDoS has moved on to become a more sophisticated disruptive methodology forming one of the many hacking tools in the kitbag of criminals. Protecting against such risks has now become a mandatory consideration every business must consider. DDoS has evolved into two distinct attack methods; the traditional flood or *volumetric* attack and the newer *application* level attack. The latter is targeted to specific applications; for example such as a database where again multiple request obfuscate legitimate traffic and cause the database server to fail to respond. The problem now is that it is no longer the domain of the professional criminal who provides the bulk of these attacks, the tools for sustaining crude DDoS attacks are available for anyone with even a smartphone to initiate.

WHAT IS DDOS?

In simple terms a DDoS attack is a crude tactic which involves sending so many requests to a target web site or server that it is unable to cope with any requests. The reality is that revenue services can be curtailed, which, for many companies can be a significant proportion of their business, and also damage a brand reputation when services become unavailable.

A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A distributed denial-of-service (DDoS) is where the attack source is more than one – and often thousands of unique IP addresses.

There are two main types of attack:

- Volumetric (flood level)
- Application Level (Layer 7) – otherwise known as "low-and-slow"

Attacks can occur for several minutes or several hours, they can either be a single occurrence or a regular occurrence over a number of days. Node4 have seen volumetric attacks of over 30Gbps. Generally attacks last a few hours and average 2–4Gbps. Our network has basic DDoS filters in place to help protect from volumetric attacks. We limit the volume of UDP traffic at the network edge and within our Data Centres, this helps protect Node4's network.

VOLUMETRIC (OSI LAYER 3 & 4) DDOS

A volumetric DDoS attack occurs when multiple comprised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic – usually UDP traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge. The targeted server is either overloaded with connections so that new connections can no longer be accepted, or the internet access circuit to the server or system becomes congested.

The major advantages to an attacker of using a DDoS attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behaviour of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defence mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. It's becoming more and more difficult to "out bandwidth" the attackers.

Managing volumetric attacks within transit links is dependent on which protocols and ports the attacks are aimed at as well as the incoming bandwidth. Adding packet filters on the network to limit the impact of the attack to individual customers is a viable tactic. Whilst providing a best effort support service to customers when they are attacked we are able to route customer's traffic through a packet-scrubbing service which strips out the DDoS attacks and returns valid data packets back through to the customer's servers. This switching of customer's transit link traffic containing the DDoS attack can take a few minutes to implement but is the best method of maintaining services in the minimum amount of time. Attacks are measured in Gbps and about 70% of them last a few hours whilst 20% last longer than five days.

According to Incapsula's 2015 report "*Global DDoS Threat Landscape*" the largest attack peak at around 253Gbps and the longest attack lasted 64 days. UDP is the most common attack vector whilst Large-SYN flood

is the most high-damage attack vector. They also reported that roughly 40% of all attacks are orchestrated with temporary hired Botnets.

APPLICATION (OSI LAYER 7) DDOS

An application DDoS occurs when a relatively small volume of bandwidth is used to consume the resources of a web server or service. For example this attack can occur when a valid request is made to a web server numerous times consuming processing resource on the server. Take the case where a request comes in to a web site to download a price book, each time the price book is requested a DB query is actioned. The system has been planned for the price book being requested once a minute, but the attacker requests the price book ten times a second. The DB server goes to 100% CPU attempting to deal with the requests resulting in an outage. This type of attack is very difficult to mitigate as you can't easily differentiate between the legitimate requests and the attackers requests.

Attacks are measured in RPS (Requests per Second), Incapsula's 2015 report "*Global DDoS Threat Landscape*" stated that the largest reported attack peaked at 179,712 RPS, the longest attack lasting 8 days. On average targets are attacked every ten days and the *Nitol* botnet was responsible for around 59% of all attacks.

N4PROTECT DDOS

N4Protect DDoS is a mitigation service from Node4 which protects against application based DDoS and can disrupt flood DDoS attacks by rerouting streams through a packet-scrubbing service. Providing a complete solution to companies who not only want to protect their online revenue but also the brand value such an attack – the cost of which is beyond measure.

There is a need to mitigate against both types of DDoS attack; volumetric and application level as in some cases the volumetric flood is used to hide a more targeted application attack. Whilst application level attacks can be heuristically analysed and pro-actively mitigated against the volumetric attacks by their nature have to be reactively countered.

Volumetric attacks include:

- TCP SYN Floods *SYN, SYN ACK, etc.)
- ICMP Flood Attacks (Ping Barrage, Smurf, etc.)
- UDP Flood Attacks (UDP Barrage, Fraggle, Etc.)
- Reflection Attacks

Volumetric attacks are reacted to when increased bandwidth triggers alerts and data streams are re-routed via packet-scrubbing services. This removes the DDoS attacks and returns a clean data stream back into the customer's servers. Once the DDoS attack abates, Node4 restores the original inbound routing and uses the data collected during the mitigation, to address any underlying issues uncovered as a result of the DoS attack.

Application layer attacks include:

- HTTP-GET Attacks
- HTTP-PST Attacks
- SSL Attacks

N4Protect DDoS proactively protects against every DDoS attack including Layer 7 Application, and SSL/HTTPS attacks. Our service uses a 100% heuristic/behaviour-based method to identify threats compared to competitors that rely primarily on signature-based matching. Instead of using pre-defined signatures to identify attack patterns, N4Protect DDoS builds a baseline of normal activity and then monitors traffic against it. Should an attack begin, N4Protect DDoS sees this as an anomaly and then immediately takes action to mitigate it. Customers are protected from known attacks and from the unknown "zero-day" attacks as N4Protect DDoS doesn't need to wait for a signature file to be updated. We are able to support customers requiring up to 1Gbps of Centralised Internet Bandwidth.

CONCLUSION

DDoS attacks are commonplace and occur on a minute-by-minute basis across the world, the tools to implement these attacks are freely available for any unskilled person with internet access to download and start attacking any known URL. Many businesses will not even realise they are being attacked; the lack of response of servers or web sites is often accredited to "IT anomalies" or a "busy" network. These attacks are shrugged off in some cases with businesses unable or unwilling to investigate because of a lack of understanding or a lack of access to basic tools or monitoring which would assist in identifying the attacks. Other DDoS attacks are advertised by their perpetrators as they wish to exploit ransom techniques to leverage maximum discomfort and afford victims time to pay up.

With the nature of the duality of DDoS attacks, it is clear that a single solution of mitigation at either application or volumetric levels is problematic. In order to properly contend with the risk it is vital to provide a solution for both elements as it is clear that in some cases the volumetric attacks obfuscate the application attacks.

Node4 can provide a comprehensive DDoS mitigation service which deals with both volumetric and application level attacks. The service is provided on an OPEX basis with an annual contract; this means that customers do not have the very expensive CAPEX outlay, nor do they need to equip themselves with the staff, training and processes to monitor and alleviate the attacks. The cost of preventing DDoS attacks is minuscule compared to the potential loss of income and the loss-of-face for a customer's brand.

Please contact Node4 for any questions relating to this whitepaper or enquiries regarding N4Protect DDoS services; please email sales@node4.co.uk or call 0845 1232222.