nccgroup
freedom from doubt

An NCC Group publication

Application Layer Attacks – The New DDoS Battleground

Prepared by: **Akhilesh Mathur**
Paul Vlissidis

Table of contents

Management summary

Distributed denial of service (DDoS) attacks, which are designed to flood organisations' servers preventing sites from functioning efficiently or at all, have become increasingly more sophisticated and targeted in the approach employed to bypass current defences.

It takes an average of 10 hours before a company can even begin to resolve a DDoS attack

Despite their ease of execution by cyber miscreants, the fallout from a successful DDoS attack can be significant. The short-term effects are clear - customer service disruption and online revenue loss – but the lingering impact can affect share price, company reputation and customer retention.

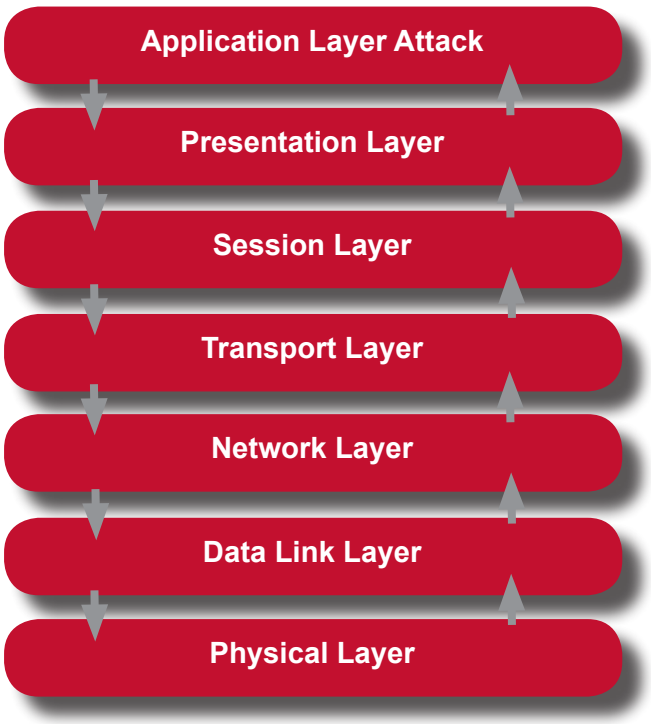
DDoS attacks have been on the up for a number of years which resulted in significant increases in the variety and availability of mitigation services designed to deal with such threats. In response to this, as well as the increasing reliance businesses have on 24/7 online presence, the DDoS threat landscape has evolved with more noticeable shift from basic network level flooding to highly targeted web application attacks.

With advancements in attack techniques comes the requirement for mitigation providers to adapt detection and scrubbing methodologies. We see an inevitable future shift towards attack vectors which will be increasingly problematic for current defence methodologies to detect and mitigate.

In this climate being prepared and knowing how your current DDoS mitigation solution and procedures will respond to such attacks is vital.

Current threat landscape

Previous DDoS attacks have predominantly used the lower levels of the OSI network model. Utilising Layer 3 (Network Protocol) and Layer 4 (Transport Protocol), attacks have concentrated mainly on either TCP attacks on server sockets or simply attempting to overwhelm network bandwidth. The infamous Low and High Ion Orbit Cannon DDoS tools used basic network requests to attack their targets. Until recently very few attacks used any sophisticated techniques although some network amplification attacks using DNS and more recently NTP have started to become more prevalent. Other amplification opportunities (eg SNMP) have yet to be seen in the wild.



In 2013 the average size of a DDoS attack was reported to be 2.64Gbps, a significant rise on previous years and thus, in a time of limited networking capabilities, volumetric attacks have quickly became the industry standard.

Attacks utilising traffic at Layers 3 and 4, even when using traffic amplification proxies, cannot be considered particularly sophisticated in nature and are designed to consume resources at a network level rather than the service itself. Often volumetric in nature, attacks aim to take down network infrastructure and servers by employing high-bandwidth flooding.

Due to the lack of complexity in the network and transport protocols and the generic profiles associated with DDoS traffic of this nature, defence solutions been refined over the years to effectively deal with such threats. Techniques such as challenge response and SYN cookies have been proven to cope well with the detection and mitigation of these increasingly archaic attack vectors.

With the general improvements in network bandwidth and widespread availability of malware controlled botnets, attackers overcome mitigation defences by utilising higher and higher traffic levels. Brute force volumetric flooding, publicised by the recent re-

1 http://threatpost.com/high-volume-ddos-attacks-top-operational-threat-to-businesses-service-providers/103933

emergence of DNS Amplification attacks, have produced a spate of DDoS floods commonly running into the +100Gbits . In turn the DDoS mitigation industry shifted to cloud-based solutions capable of off-ramping huge amounts of attack traffic before they have a chance to reach and overwhelm their target's networking thresholds.

As general bandwidth capabilities improve and the theoretically unlimited network capabilities cloud computing can provide for absorbing volumetric floods, DDoS techniques have adapted, replacing brute force for a more targeted approach.

Application layer attacks

Relocating attacks further up the OSI model to the Application Protocol (Layer 7) is a logical move for perpetrators to make due to most DDoS defence systems focusing primary detection and mitigation powers on lower layers.

As more and more businesses rely on a permanent online presence due to business design (such as online gambling) or customer preference (such as e-banking), targeting weak areas within web applications has provided a multitude of soft targets for attackers to exploit.

While traditional network level DDoS attacks have focussed on volumetric styles of attack, application level DDoS employs a targeted approach whereby initial scoping and research of the target site(s) is often performed to identify weak points (any element that will consume significant resources) resulting in much more effective attack methodology. Asymmetric attacks are designed to stress and overload either the service itself or any of the backend systems serving content, thus circumnavigating the need for even higher levels of traffic bandwidth.

With more and more functional complexity and user interaction being seen in modern web applications, the range of weak points that can be leveraged to stress the service becomes more diverse. These areas of weakness (pinch points) represent functionality that results in relatively large responses or intensive backend processing in comparison to the small repeated requests made by each bot, resulting in an ever increasing resource overhead.

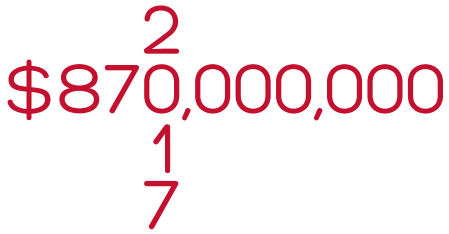
Typical pinch points can range from search queries, login pages and form submissions to PDF and Flash video downloads, all of which can be considered basic components of any web application. The effects of targeting these areas are dependent on the pinch point itself. Repeated login or search requests can cause lookup bottlenecks on database servers, while techniques such as Slow Read and Slow Post can result in

exhausting server connection tables. In the use of large PDF file downloads, an attack vector seen in the spate of attacks against US banks in 2013, traffic amplification effects can be created where the outgoing network bandwidth is saturated long before incoming traffic levels hit abnormally high levels. Knock on effects of application exploitation attacks utilising scripting vulnerabilities, XSS, hidden-field manipulation and SQL injection can result in numerous unexpected side effects to other parts of the business.

Often with web applications a complete denial of service is not even required. Web performance best practice states a five to ten second delay in a Website's response time often results in the user going elsewhere, presenting a loss in potential earnings for companies and highlighting another advantage of this resource light attack methodology.

Mitigation effectiveness

Traditional network level DDoS detection methods are unable to be effectively applied for web application DDoS attacks due to the traffic belonging to a different layer. Application Layer DDoS attacks utilising legitimate HTTP requests require completion of the three-way TCP handshake thus bypassing Layer 4 anomaly detection techniques.



The DDoS mitigation market is projected to hit $870 million in 2017

Targeting Layer 7 services also requires considerably less bandwidth and attack resources, and as such may fall far below the mitigation trigger 'thresholds' designed for more common volumetric attacks. Traffic appears well formed and legitimate, and often the traffic spike associated with the attack is not always distinguishable from flash crowd events (abrupt increases in legitimate user requests).

With the customisable complexity offered by the Application Layer, attackers can exploit this by randomising aspects of HTTP requests such as the header information and variable values so as to circumnavigate signature-based detection and scrubbing methods. We have seen that public websites contain many pinch points, providing a list of attack vectors which can be cycled through presenting the victim with a constantly changing attack front. In the case where poorly implemented functionality and coding practices have been identified, attacks can be customised to exploit these weaknesses causing victims to suspect other reasons such as infrastructure or application failure.

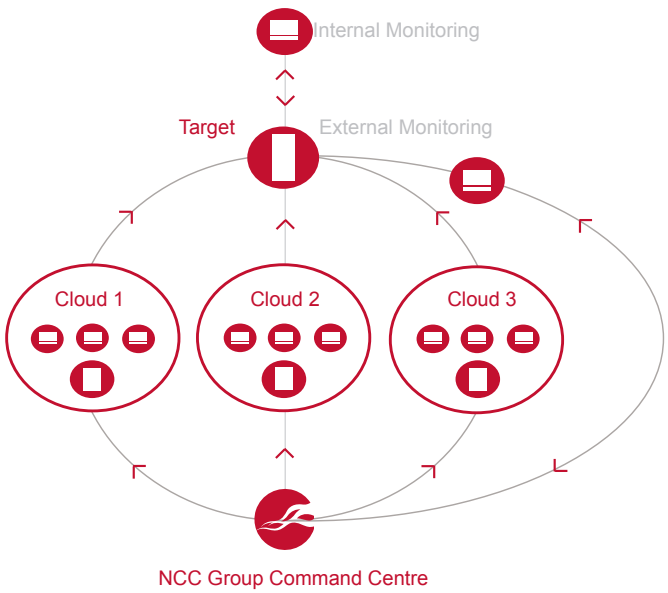
Sometimes security features can cause issues with mitigation of a DDoS attack. SSL encrypted traffic poses a problem due to many businesses' understandable reluctance to lodge their SSL certificates with third party mitigation providers, thus rendering detection and mitigation solutions unable to crack open traffic to analyse content using deep packet inspection. With requirements to ensure customer confidentiality, and increasing public awareness of man-in-the-middle internet traffic surveillance, forcing the use of encryption on web applications is a popular practice utilised by both providers and users.

More intelligent methodologies (such as behaviour profiling) to distinguish between legitimate and malicious HTTP requests can be instrumental in leading to effective DDoS detection and mitigation. Predefined behaviour profiles extrapolated from statistical attributes such as user session duration, request rates, geographical locations, response latency and response type, as well resource consumption monitoring, can provide a baseline to compare to traffic monitoring data. If anomalous behaviour is detected further analysis from either an automated or human perspective can be deployed to determine whether the suspicious traffic is a result of a legitimate or malicious application usage.

User challenge-response techniques (such as CAPTCHA) are extremely effective at identifying and whitelisting legitimate users who respond correctly to simple random challenges. However, these are considered to be very intrusive in their nature and are used sparingly, either to protect a few key areas of the web application or as an activated defence.

DDoS Assured Test Findings

According to statistics gathered from NCC Group's DDoS Assured service, many of our clients do not know the capabilities nor effectiveness of their DDoS mitigation solutions until they are under attack despite the considerable investments they they make each year.



NCC Group's DDoS Assured seeks to provide clients with a service to test their mitigation solutions in a

controlled environment against a real life DDoS attack, thus allowing them to assess both the technological implementations and capabilities of their solutions, with a primary focus on Application Layer HTTP attacks.

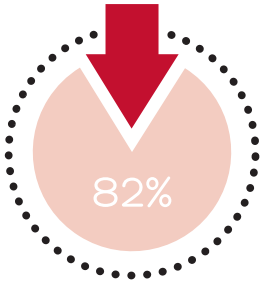
Using information fed back directly from our clients throughout DDoS Assured exercises, combined with data collected from our botnet monitoring processes, NCC Group's analysis exposes the limitations of mitigation solutions and often highlights the lack of understanding clients have in relating the service level agreements (SLA's) of purchased protection to the range of DDoS attacks experienced in the wild.

We also predict an inevitable future shift from volumetric network level floods to highly targeted, application level attacks, an area where confusion over mitigation solution capabilities occurs most often.

Successful DDoS Attack Statistics

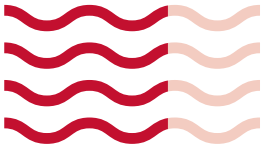
We have managed to create a denial-of-service state on **70%** of our client's targets. This denial-of-service effect resulted in a slow and unresponsive and in some cases completely unreachable target service. In many cases this was achieved despite mitigation being present and active. In 25% of these attacks, related infrastructure and services were also impacted as an unexpected side-effect. Many of our tests are specifically designed to stay well below this threshold so these have been discounted from the figures.

In **82%** of our DDoS Assured exercises where a denial-of-service effect was created, attacks were successful due to deployed mitigation solutions not being effective at protecting a client's infrastructure. In some cases, the client was unaware of exactly what level of protection their mitigation SLA's provided.



82% of our DDoS tests have been successful due to ineffective mitigation solutions

In **28%** of our DDoS Assured exercises where a denial-of-service effect was created, attacks on infrastructure were successful due to other unexpected factors. These factors ranged from mitigation that was in place but had not been configured correctly to unexpected bottlenecks identified in infrastructure either inside or outside our client's network perimeter.

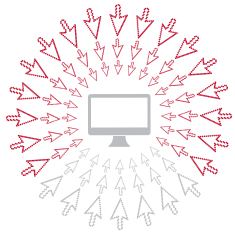


In 64% of our DDoS tests, the mitigation solution failed to protect against more advanced Layer 7 HTTP(s) Floods, despite mitigating Layer 4 floods

In **64%** of our DDoS Assured exercises where a denial-of-service effect was created, our client's mitigation solution failed to protect against more advanced Layer 7 HTTP(s) Floods, despite providing effective mitigation against network Layer 4 floods.

In **73%** of our DDoS Assured exercises where a denial-of-service effect was created, our botnet did not reach full strength before a denial of service effect was experienced on the target by the traffic flood. 89% of these were the more advanced HTTP(s) floods.

Statistical data presented has been extrapolated from +30 tests carried out by NCC Group's DDoS Assured testing platform across a variety of business sectors.



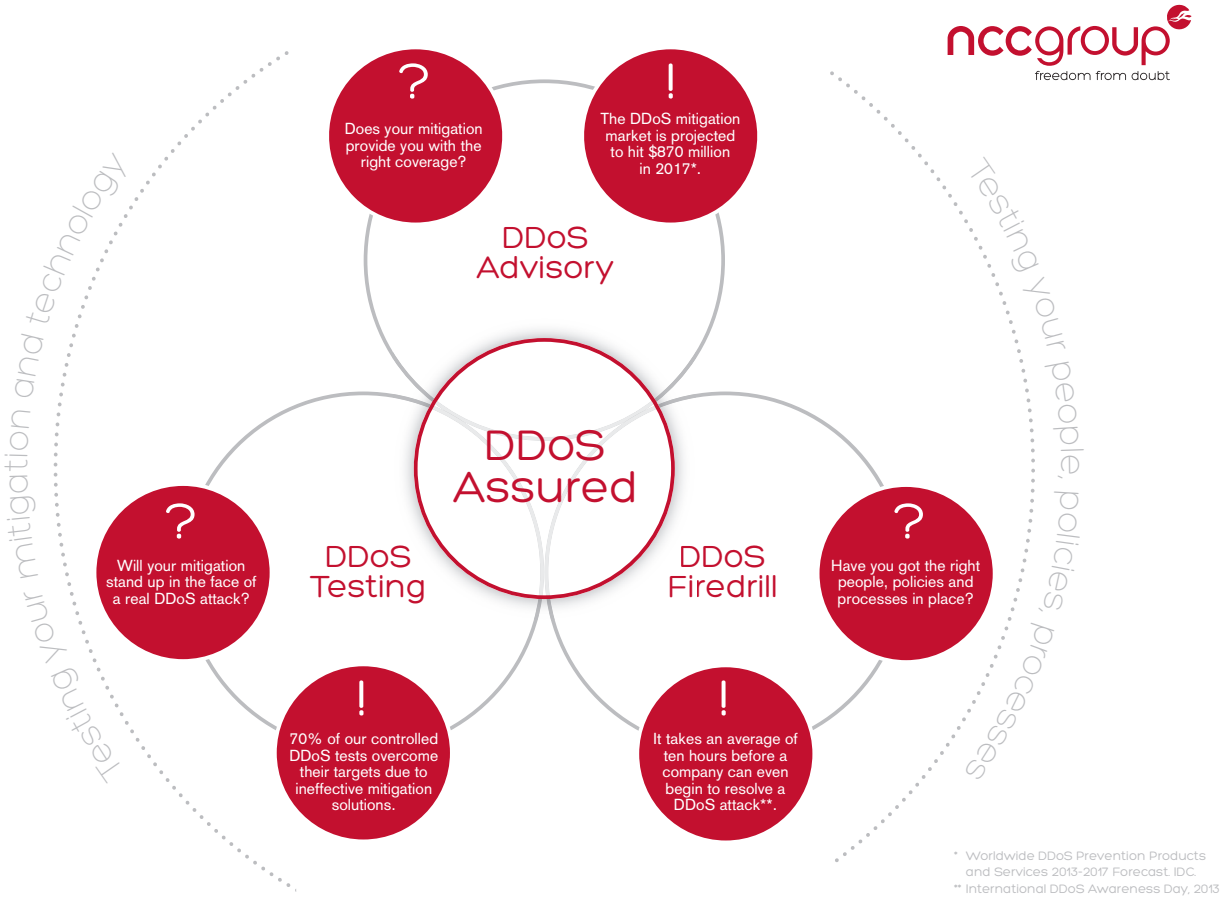
In 73% of our DDoS tests, our botnet did not reach full strength before a DoS effect was experienced on the target by the traffic flood

Conclusions

As seen from the statistical data gathered from our DDoS Assured attack simulation exercises, in 64% of the cases where the mitigation solution failed to protect a target's infrastructure the attack was utilising Application Layer attack vectors. In some cases the client was not aware of the distinction between the network layer and application layer protection solutions.

When buying DDoS mitigation services customers should be careful to ask if they are getting application layer detection as part of the package. In many cases volumetric bandwidth protection alone may not work. Intelligent buyers will insist on regular testing (and/or DDoS fire drills) to make sure they are getting the mitigation they are expecting.

As trends suggest, Layer 7 DDoS attack techniques will become the norm with reconnaissance and targeted attacks becoming the primary tools in the bot master's arsenal. Given the difficulty in differentiating Layer 7 DDoS attacks from legitimate and non-malicious connections is it imperative to undertake regular independent testing to check that current mitigation services are able to provide effective detection and protection against the adapting DDoS threat.



Details of NCC Group's DDoS Assured service can be found at http://www.nccgroup.com/en/our-services/security-testing-audit-and-compliance/security-and-penetration-testing/ddos-assured/

