DDoS – A Continuously Evolving Corporate IT Threat

iomart

> *"Organisations need to realise that advances in DDoS render simple firewall provisions insufficient. Instead security needs to be boosted through the use of an onsite Intelligent DDoS Mitigation System (IDMS), or a third party managed solution."*

Executive summary

A DDoS (Distributed Denial of Service) Attack is a malicious attempt to make a server or network resource unavailable to users by either temporarily interrupting or shutting down entirely the services of a host connected to the Internet. DDoS attacks use numerous computers and Internet connections and are often sent out globally in what is known as a botnet.

2014 was a record-breaking year in terms of DDoS attack severity as hacktivists, nation states and cybercriminals refined their techniques to cause more inconvenience and financial loss than ever before. DDoS as a concept is not new, but by using multiple attack vectors across several different surfaces, cybercriminals are still able to avoid basic-level protections and cause significant damage.

Businesses need to understand the different forms of DDoS attack and the four fundamental security factors that must be covered to reduce risk. Rather than becoming an outdated, outmoded form of cybercrime, DDoS continues to evolve, playing a vital role in hactivism and even modern cyber warfare between nation states.

Organisations need to realise that advances in DDoS render simple firewall provisions insufficient. Instead security needs to be boosted through the use of an onsite Intelligent DDoS Mitigation System (IDMS), or a third party managed solution that uses the same intelligent technologies.

Failure to prepare can be extremely costly. Your corporate integrity may be threatened because an outage can not only cause loss of revenue and productivity, it can also create major compliance and regulatory issues and seriously affect the way your brand is perceived by your customers, your partners and suppliers and the wider public.

In a survey of IT professionals conducted by Neustar, nearly two-thirds of respondents indicated that a DDoS attack would cost $240,000 in revenue losses per day. The same report showed that over 50 percent of respondents were concerned about the potential damage to their customer experience.

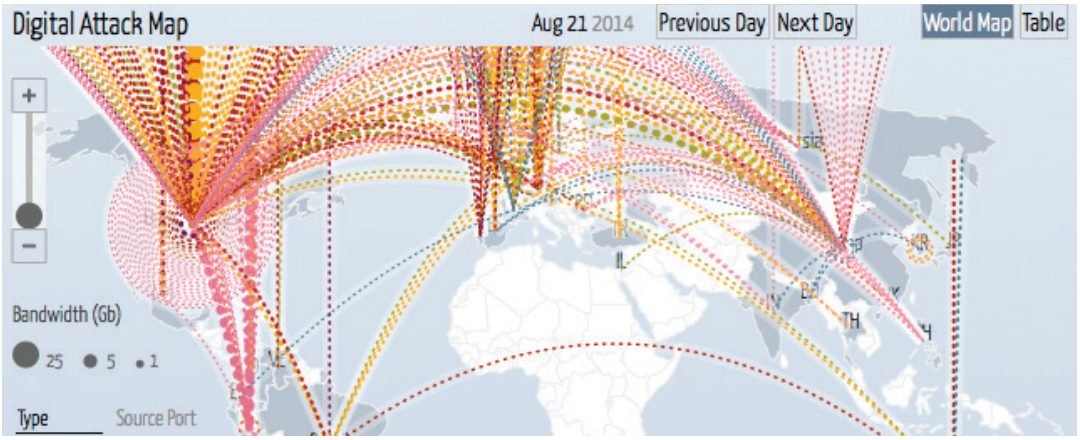
The current DDOS landscape

Historically Distributed Denial of Service (DDoS) attacks have simply flooded network resources with thousands of simultaneous resource requests, consuming all available bandwidth. Today they are growing in volume and changing in nature. The Akamai Q3 2014 State of the Internet report revealed a 22% increase in total DDoS attacks over the course of the year . The trend is for shorter, sharper durations but bigger packet per-second attacks.

Volume based attacks

Volume based attacks seek to overload a victim's network resources using various packet-flooding techniques to consume all available bandwidth. Measured by magnitude according to bits per second, attacks include UDP floods, ICMP floods and other spoofed-packet techniques.

The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).



Snapshot of DDoS Attacks

"The average peak packets sent per second during an attack increased by 366% over the course the year to Q3 2014."

Protocol attacks

A variation of Volume based attacks which also seek to saturate available bandwidth, protocol attacks are specifically engineered to consume server resources, or that of intermediate network equipment like network bridges, firewalls and load balancers. SYN floods, fragmented packets, Ping of Death and Smurf DDoS (among others) generate huge volumes of packets within such equipment so that legitimate traffic cannot be processed.

Consequently protocol attacks are measured in packets per second.

Application layer attacks

Known vulnerabilities within operating systems and server software can also be exploited to create DDoS-like behaviour. Application layer attacks generate seemingly legitimate traffic that uses Slowloris, Zero-day exploits and other techniques to cause key services to fail. The discovery of the Heartbleed, Shellshock and POODLE bugs during 2014 have opened a number of new avenues for hackers to exploit when launching DDOS attacks.

Application layer techniques are measured in requests per second.

In order to stay ahead of protective measures, DDoS attacks commonly use a combination of the above techniques which are then enacted by a globally distributed botnet. Using compromised PCs and servers a DDoS strike can be initiated within minutes. New threats emerge regularly with analysts finding incidences of hacked routers, customer premise equipment, mobile handheld units and even video conference devices being used to provide the sources for packet floods and more .

Virtually any Internet device can be exploited for use in a DDoS botnet if it meets one of the following conditions:

- The default configuration has not been changed and is insecure by design.
- The device is running outdated, vulnerable firmware.
- The device does not have any management or update facilities.

As measures to protect against DDoS attacks become more sophisticated, experts expect to see even more diverse devices being leveraged for use in botnets.

Who is most vulnerable to DDoS attacks?

As with most cybercrimes, there are three main motivations, financial gain, political ideology and general malicious intent. The type of business in question can often be used to determine motivations behind a DDoS attack, helpful for criminal investigations after normal service resumes.

Online entertainment providers were by the far most targeted sector in 2014, making up almost a third of all reported attacks. Media (24%) and software and technology (19%) were also extremely popular targets. Business service providers and health care and life sciences were much less attractive targets with less than 1% each .

Organisations subject to extortion and ransom

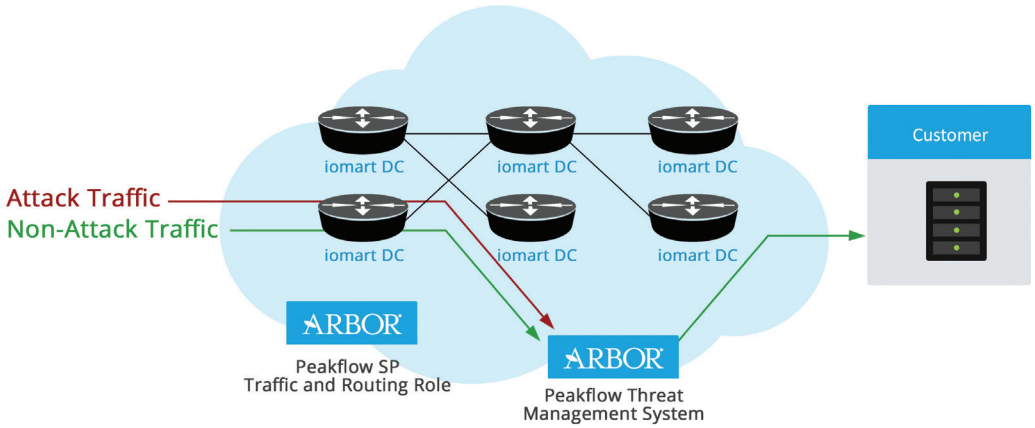
Mission-critical systems are so-called because organisations rely on them to conduct day-to-day business. Financially-motivated hackers may use DDoS techniques to limit or disable access to these systems. The criminals behind such an attack will make an approach to the affected organisation, offering to restore access in return for a large payment.

Financially motivated cybercriminals tend to target medium-sized businesses because:

- They are fully-reliant on systems.
- They are typically less well-equipped to handle DDoS attacks.
- They are (anecdotally) more likely to pay a ransom in order to restore access quickly.

Organisations subject to hactivism

In the age of the Internet collective, almost any organisation may find itself targeted by a group who take umbrage with profits, operations, ethics or ideology. World Cup sponsor companies were subjected to DDoS attacks by hactivist organisation



"There was a 44% decrease in application layer attacks between 2013 and 2014 ."

Anonymous campaigning against social inequality within host country Brazil last year for example . The same group have also pledged to mount a DDoS campaign to "take down" Jihadist websites in retaliation for the recent Charlie Hebdo terrorist attack in Paris .

There are also indications that DDoS may be being used by some nation states as part of their cyber warfare provisions. The largest DDoS attack ever observed was directed at two websites supporting pro-democracy protesters in Hong Kong . The attacks exceeded 500Gbps, with suspicion initially being directed at the Chinese government who were the subject of serious criticism on the affected sites. Revenge attacks were also perpetrated by Anonymous, targeting Chinese Government resources .

Organisations subject to malicious intent

Sadly it is relatively easy to launch even a basic DDoS attack. Indeed we have even reached the point where you can get 'DDoS for hire.'

Have you upset someone? Feasibly organisations of any size can be (and sometimes are), attacked by disgruntled customers, or those holding a personal grudge.

Small businesses, public sector organisations and even community groups can be taken offline relatively easily using DDoS attacks.

Ultimately no one is safe and any business could fall victim to a DDoS attack – the only difference will be organisation motivation behind the strike. So what is the solution?

Why firewalls and IPS devices are not the answer

The severity and complexity of DDoS attacks is often under-estimated, with many CTOs mistakenly assuming that corporate firewalls and Intrusion Preventions Systems (IPS) offer a sufficient level of protection.

Although firewalls and IPS are essential elements of a layered-defence strategy and can help mitigate some of the most simplistic DDoS attacks, emerging threats that use multiple vectors or techniques can often overwhelm such basic provisions.

Firewalls and IPS devices are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products. DDoS attacks consist of legitimate traffic from multiple sources targeted to exhaust critical resources, such as link capacity, session capacity, application service capacity (e.g. HTTP and DNS) or back-end databases. Because this traffic is authorised and does not contain the signature content of known malware it is not stopped by them. Therefore they fail to address the fundamental concern of DDoS - network availability – and often become targets for attacks themselves.

How to protect against DDoS attacks?

DDoS attacks are increasingly reliant on using a combination of techniques – most now use a mix of volumetric and application-layer methods to increase effectiveness. Enterprise organisations cannot afford to suffer an outage because an attack has overwhelmed the network. They need to be able to stay online while the attack is mitigated with the DDoS attack traffic directed away from their servers while the 'good' traffic needed to run their business is allowed through.

The only solution is to use an Intelligent DDoS Mitigation System (IDMS) capable of identifying and segregating legitimate network requests/traffic from that which is generated as part of a DDoS attack. A successful IDMS solution will implement:

1. Inline and out-of-band support to avoid providing another attack surface.
2. Broad network visibility to identify genuine distributed attacks, analysing traffic from each network segment.
3. Multiple detection techniques that update

regularly as new exploits are identified, including statistical anomaly detection and customisable threshold alerts.

4. Scalable mitigation capabilities that can handle attacks from 1Gbps (low end) to 40Gbps+ (high end).

Although the specific solution required will depend on the size and complexity of a given datacentre, these four factors will be essential to all.

"The Peakflow Threat Management System from Arbor Networks and iomart provides proactive scalable defence against mixed-mode DDoS strikes."

It is also extremely important to note that many DDoS attacks are relatively untargeted, presenting a serious problem in the form of collateral damage to third parties. Attacks on shared infrastructure, like that used for Cloud services or webhosting, often affect other parties and services that are not the primary focus of the strike.

Why choose Arbor from iomart?

Arbor Networks Inc. has been protecting the world's largest and most demanding networks from DDoS attacks for over a decade. The Arbor Security Engineering Research Team (ASERT) is a recognised leader in the field of DDoS research and protection and uses the anonymous traffic data shared with it by nearly 300 service providers across the globe to provide actionable network intelligence. As a result, solutions built using Arbor's knowledge and experience, provide world class protection to customers against DDoS and other attacks by cybercriminals

The Peakflow Threat Management System from Arbor Networks and iomart provides proactive scalable defence against mixed-mode DDoS strikes, adding additional processing and bandwidth capacity in line with an organisation's own growth. Placed at the edge of a protected network, network traffic is sampled regularly and compared to 40+ known attack signatures to proactively protect against DDoS attacks.

As ASERT discovers new vulnerabilities and attack vectors, updates are distributed to Peakflow platforms automatically, reducing the window of opportunity for cybercriminals. This is backed by fully configurable analysis and filtering capabilities, allowing packet rules to be created according to business needs. The same tools also allow for manual adjustments to help mitigate attacks at their peak.

When a DDoS attack is detected – many can exceed 300GB/sec - Peakflow mitigates it by surgically removing the illegitimate traffic while re-injecting the legitimate packets back into the network. Peakflow consists of multiple devices with specific tasks to block one or more types of attacks (DDoS, Flood etc) and depending on the nature of the attack, one or more of these tasks will be given to each device.

Peakflow can detect 'fast flood' attacks within as little as one second and can mitigate and stop them within 30 seconds.

iomart offers a complete end-to-end service for Arbor Peakflow units, from installation, initial configuration and attack mitigation, ensuring your mission-critical system stay online, all the time.

Network protection – an unavoidable essential

The first incidences of DDoS attack were recorded in 1999, with the best-documented case seeing a 227 node botnet being used to take down a single computer at the University of Minnesota with a basic volumetric attack . 15 years later and DDoS remains a significant tool in the cybercriminal's kit.

As shown above, firewalls can help provide a very basic level of protection against DDoS. However relying on a single system could, in the end, result in the firewall becoming another factor in a multi-vector strike (using protocol level weaknesses) increasing the damage done to your corporate systems.

With new zero-day exploits being discovered on a regular basis, and the potential of leveraging vast botnets for a relatively small fee, cybercriminals have a large array of new attack vectors that can be used to cause massive problems for their victims. The only way to stay ahead of these challenges is through the use of a scalable security solution that can continuously adapt to address and mitigate new threats.

The low-cost, high effectiveness of DDoS means that organisations of any size can and do fall victim to attacks. DDoS protection is no longer the preserve of Fortune 500 companies and government bodies. Instead all reputable organisations now need to seriously consider their exposure and how best to mitigate attacks that could take their business offline – permanently.

Bibliography

1. What A DDoS Can Cost – Dark Reading - Information Week

2. Akamai Q3 2014 State of the Internet report

3/4/5/6/7. Ibid.

8. World Cup 2014: 'Hacktivist' group Anonymous plan cyber-attack on sponsors including Coca-Cola, Budweiser and Emirates Airlines – **The Belfast Telegraph** – 2nd June 2014

9. Charlie Hebdo Paris massacre: Anonymous vows to avenge victims with cyber-war on jihadists – **International Business Times** – 9th January 2015.

10. Largest Cyber-Attack in History Hits Pro-Hong Kong Protest Websites – **International Business Times** – 21st November 2014

11. Charlie Hebdo Paris massacre: Anonymous vows to avenge victims with cyber-war on jihadists – **International Business Times** – 9th January 2015.

12. **Defenses Against Distributed Denial of Service Attacks** – Computer Security Book - Gary Kessler.

Lister Pavilion, Kelvin Campus, West of Scotland Science Park, Glasgow, G20 0SP