DDoS mitigation

Background

A distributed denial-of-service (DDoS) is a coordinated attack where the resources of a target system are overwhelmed by an attacker, making it unavailable. Attackers may make use of large numbers of hosts on the Internet to carry out these attacks, resulting in serious adverse effects for the target systems.

How to prevent DDoS attacks?

DDoS attacks can be extremely difficult to guard against. Currently, there is no technology available that completely eliminates the risk of a DDoS attack, as demonstrated by large enterprises and governments that fall victim to such attacks.

There are varying techniques and levels of sophistication for DDoS attacks. Modern techniques, such as "reflected amplification", have provided unprecedented increases in attack capacity, overwhelming even the largest networks and organisations. When overloaded with a massive number of simultaneous requests, target systems often become unresponsive and unable to serve legitimate users.

How can Catalyst help me to mitigate the risk of DDoS attacks?

Catalyst has monitoring systems in place that allow us to detect anomalies in our networks and quickly react to them. These systems allow us to block certain types of attacks, preventing the targeted web property or other customers from being affected by it.

For larger or more sophisticated DDoS attacks, we have the ability to blackhole traffic to the targeted web property, with our upstream network providers. This causes the targeted site to go down, but avoids collateral damage and impact to other customers.

As a customer, how can I mitigate the risk of a DDoS attack further?

Customers that have valuable or critical web properties can contract additional DDoS protection services from companies like CloudFlare, Fastly and Incapsula. These systems provide globally distributed reverse proxies for websites. When a DDoS is identified, they have the ability to drop malicious traffic as close as possible to the country of origin, preventing this traffic from reaching your web properties hosted with Catalyst in New Zealand.

These solutions must be implemented and configured on a per site basis, as they require you to change your DNS records to point to their system's IP address instead of your own website.

While considered the state of the art in DDoS protection, these solutions do not eliminate the risk of a DDoS attack and introduce their own risks. For example, a motivated attacker may be able to find out the IP address of the servers behind the reverse proxy and find a way to attack them directly. There have also been

occurrences of DDoS protection service providers being compromised[1] and attackers being able to drop genuine network traffic to all web properties protected by their systems.

The future of DDoS protection

Network vendors like Cisco, Juniper, NTT and Arbor Networks have proposed an extension to the Internet's Border Gateway protocol called Flowspec (https://tools.ietf.org/html/rfc5575). Flowspec will allow Internet service providers to specify more sophisticated rules to match unwanted network traffic, such as matching on protocols, ports and source addresses. This will permit finer-grained control over filters for unwanted traffic compared to the remotely triggered blackhole route techniques currently employed, which filter on packet destination IP addresses only. Once more widely implemented it will increase the types of DDoS attacks that can be mitigated directly and easily by operators such as Catalyst.

The Defence Advanced Research Projects Agency (DARPA) has launched a research initiative called Extreme DDoS Defence to find further revolutionary ways to mitigate the risks of DDoS attacks. More information on this research programme can be found at http://www.darpa.mil/program/extreme-ddos-defense.

Both government and industry leaders recognise the existing issues of Internet technology and the increase in the number and variety of cyber attacks. Catalyst will continue to increase the levels of DDoS protection offered to our customers as new technologies become available to mitigate the risks of this modern threat.

1 http://www.ibtimes.co.uk/staminus-hack-2300-customers-impacted-ceo-admits-cyberattack-1549321