Halting DDoS attacks in their tracks

In a world in which the number of connected devices continues to climb, exciting new business and growth opportunities are emerging in areas such as the Internet of Things (IoT), virtualization, online commerce and entertainment.

However, at the same time this opens more avenues for criminals to exploit with increasingly sophisticated cyberattacks. With the rise of IoT devices, many attacks are now in the form of distributed denial-of-service (DDoS) attacks, whereby a flood of traffic interrupts normal internet traffic flows and stops good traffic from getting through.

Such DDoS invasions come in various types, a common one being volumetric attacks. These are designed to consume available bandwidth by overwhelming the network with traffic and typically come from compromised devices or the exploitation of certain network protocols. Another type is application-layer attacks, which tend to target a specific service on the host network such as a search engine.

The threat is set to increase further as IoT proliferates with the drive towards 5G and its use for purposes such as connected cars, which could effectively create mobile hotspots from which attacks can be launched.

Content

03 DDoS trends

04 Combat strategy

04 Review and collaborate

05 Our DDoS protection

06 Extra assurance

DDoS trends

The past few years have seen some unprecedented DDoS attacks on the terabit scale. These have been aided by emerging methods such as the memcached technique used in early 2018, when a then record-breaking 1.7Tbps DDoS attack followed swiftly on the heels of a 1.35Tbps one just days before.

And 2020 then saw a DDoS attack that trumped even those, with Amazon Web Services reporting a 2.3Tbps event that resulted in three days of elevated threat and was 44% larger than any volumetric attack it had previously detected.

NETSCOUT, meanwhile, reported that there was a 16% increase in DDoS attack frequency globally in the second half of 2019 year-on-year. And although the organization noted a significant drop in regularity of attacks larger than 200Gbps, perpetrators have turned up the volume of smaller-scale activity while using an ever-growing array of new or increasingly popular attack vectors – with NETSCOUT highlighting that there were seven in 2019 alone.

COVID-19 has also shown evidence of the potential impact of sudden events that transform consumer behavior. Information services and technology company Neustar highlights that in the first half of 2020, a "precipitous" rise in DDoS activity mirrored a growth in internet traffic as people spent much more time online at home on activities such as shopping, gaming and working during the pandemic. In all, Neustar noted a 150% year-on-year rise in number of attacks in the first six months of 2020.

One recent trend has been the surge in DDoS attacks in the gaming arena, where it has become easier and much more accessible for regular users armed with a credit

card to cheaply access services that cause a lag in rivals' connections. Low-cost DDoS "booter" or "stresser" services can be used to knock other gamers offline. Or they can be used to launch attacks against targets such as financial services and regular IT or cloud services that may be hosting applications for other industries.

Another factor to consider is that these threats can afflict a wide variety of industries, meaning that companies simply cannot afford to let down their guard.

> "A recent trend has been the **surge in DDoS attacks** in the gaming arena. **DDoS "booter" or "stresser"** services can be used to knock other gamers offline.

> Automated mitigation with providers such as NTT can allow a rapid response in as little as **30 seconds.**

Combat strategy

To fight back against these threats, there is a variety of steps that carriers and enterprises can take to prepare themselves. One of the key measures is to identify assets that are critical to the business, such as name and base servers.

On top of this, it is advisable to harness network operations centers (NOCs) to monitor normal traffic levels so the impact of an attack can be more easily and rapidly identified before it has the chance to take hold and cause real chaos. Many companies still do not know their normal patterns, making it hard for them to identify unusual levels of activity.

Tools like NetFlow can be used to gather data and network traffic for analysis, with one big advantage being the provision of both commercial and open-source software to fit every budget. Such resources make it possible to accumulate historical data and help identify in the future whether there are any big spikes in traffic that might indicate an attack, and even where it may be coming from.

It also pays to keep detailed logs of any attacks to help properly prepare for similar events in the future, enabling the creation of a checklist and aiding a review of potential security services that can deal with the types of pattern flagged up.

Attack simulations can additionally be run to ensure NOCs are able to deal with threats and have a specific plan of action when they occur, helping identify critical assets in advance of the business coming under attack. Furthermore, establishing a close relationship with security teams of providers is an effective way of helping to relieve the stress when an attack breaks out. Our network security team (NST) can arrange and participate in these “war games”. Contact us if you would like to set up an exercise.

By taking such steps, organizations and network providers can work together to respond more rapidly to an attack. Teams can then work together effectively to stamp out any threats, using methods such as blocking traffic or scrubbing and cleaning it, depending on needs. Automated mitigation with providers can allow a rapid response in as little as 30 seconds, which is important given the rising number of very short attacks in areas such as gaming, where they often last less than five minutes.

Review and collaborate

The work should not stop once an attack is over. Then it’s time for a post mortem, analyzing what happened and identifying any equipment failures and holes there may be in defenses to be even more ready for attacks next time round.

In this way, factors can be assessed such as whether firewalls were able to handle bad traffic, whether there were compromised or vulnerable servers and whether there is a need to look at making upgrades or using a more intelligent mitigation service.

Documenting the type of attack can help NOC teams identify bad types of traffic in future as well, enabling a more rapid response. In the aftermath of an attack, it may also be possible to trace an attack back to the attacker and take action against them as a result.

On top of this, industry collaboration is key to reducing the impact of threats. The Global Leaders’ Forum seeks to gather carriers and people dealing with DDoS on a regular basis to share ideas and information, as well as help people get to know each other to form rapid points of contact. Online security groups such as NSP-SEC and Ops-Trust are further avenues for cooperation.

We collaborate with many groups and at events, and we are ready to arrange meetings to discuss better approaches to mitigating DDoS attacks.

Our DDoS protection

Making protection a central feature when launching new products and services remains a must. This is an area where we take a proactive approach. Doing this means that such threats can be stopped early, rather than taking a reactive approach when the damage is already done.

With a view to this, our DDoS Protection Services (DPS) provides intelligent DDoS mitigation capabilities that clean malicious traffic before it impacts the customer's internet connection.

This happens through traffic being diverted to the company's scrubbing centers, where it is analyzed and the attack traffic removed before the rest is forwarded on to the customer network. We have developed various levels of DPS that cater to the different amounts of protection customers require.

Our DPS Max service is aimed at customers wanting full protection, including attack detection and automitigation functions. The latter feature allows customers to receive immediate mitigation through the platform detecting attacks and automatically putting defensive measures in place based on customer-defined thresholds. Once an attack is over, the platform returns customer traffic to standard pre-attack routing.

Other tiers of our service are DPS Control, DPS Core and DPS Detect. The first of these is an entry-level service that enables customers to define permanent access control lists (ACLs) to block certain types of traffic on the network. This service is ideal for advanced users who understand their traffic profile and can largely mitigate attacks by themselves but want to reduce their exposure to specific types of threats.

An intermediate tier, DPS Core, takes things to the next level by offering a range of extra features compared with the basic service. A highlight of this service is the state-of-the-art technology that enables rapid responses to mitigation requests. It enables a response within 15 minutes for requests submitted via the company's DPS Portal - an exclusive portal for DDoS protection services.

The DPS Portal offers major benefits for customers apart from improving speed. As well as opening up tickets in our support structure, it immediately notifies an on-call security engineer to come to the customer's aid. Through the portal, customers can also request configuration changes such as adding prefixes for protection, and review mitigation history and graphs of attacks.

Meanwhile, another tier of the service is DPS Detect, which provides the features offered by DPS Core and adds services such as detection capabilities to notify clients of potential attacks and customer-initiated mitigation at the touch of a button.

We also offer customers selective blackholing to block traffic on the network and limit attacks on a geographical basis. This can be effective in preventing large-scale volumetric attacks from spreading.

Extra assurance

An additional layer of assurance is provided through support from our network security team, through which DPS subscribers can receive direct access to experts with an average tenure of 10-plus years, offering a wealth of experience to help mitigate attacks.

Our services are ideal for any business that requires a high level of internet availability, including e-commerce players, telecoms carriers and internet service providers, content providers such as video and gaming companies and social networking sites.

Overall, a multi-strategy approach is often recommended by vendors as the best, most comprehensive strategy for dealing with DDoS attacks nowadays. This employs a combination of filtering at the front end to block unused applications, selective blackholing and DDoS mitigation through intelligent scrubbing.

By taking the steps recommended above and working closely with us and our well established security mechanisms, we can make great strides in resolving DDoS issues together.

> “ Our DDoS Protection Services (DPS) provide intelligent DDoS mitigation capabilities that **clean malicious traffic before it impacts** your internet connection.

