UPTIME. ALL THE TIME. GUARANTEED.

www.vistnet.com

DDoS Protection Company

whitepaper:

DDoS Attacks 101

The turn of the 20th century marked the birth of DDoS Attacks - a major network threat, relentlessly gaining speed and affecting growing numbers of victims. Prominent sites are no longer the only targets of the onslaught - nowadays anyone with an online presence may fall prey to intentionally inflicted null or lackluster online performance.

Contents

Introducton

Today's World Wide Web spans over millions of computers scattered throughout the world with millions of people using the Internet for professional and personal needs. The everlasting necessity to maintain billions of connections uninterrupted, thus ensuring access to sites and services turns main internet nodes into attractive targets for violators who flood this structure or parts of it with all kinds of "bad" traffic, rendering it inaccessible to legitimate traffic. Even a short-lived denial of service attack can cause serious disruptions in revenue streams and may have devastating consequences for both private and public online entities.

The turn of the 20th century marked the birth of this major network threat, relentlessly gaining speed and affecting growing numbers of victims. Prominent sites are no longer the only targets of the onslaught - nowadays anyone with an online presence may fall prey to intentionally inflicted null or lackluster online performance. Recent evidence suggests that it is becoming increasingly easy and inexpensive to launch such assaults, whereas protecting one's site or service, without employing external expert services, is becoming almost impossible to achieve due to the associated infrastructure and software investment.

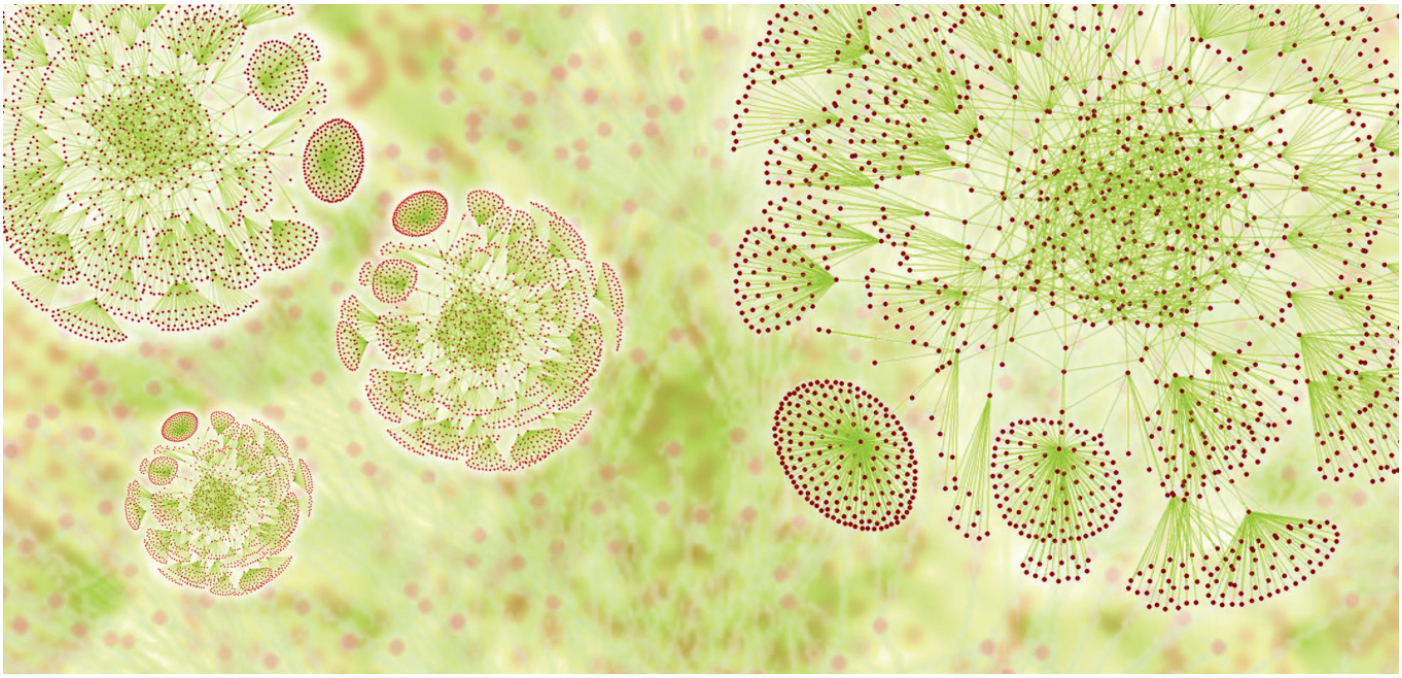


Image based on *"Digital dandelion or new semi-random Internet map?"* - courtesy of Jacobs School of Engineering, UCSD.

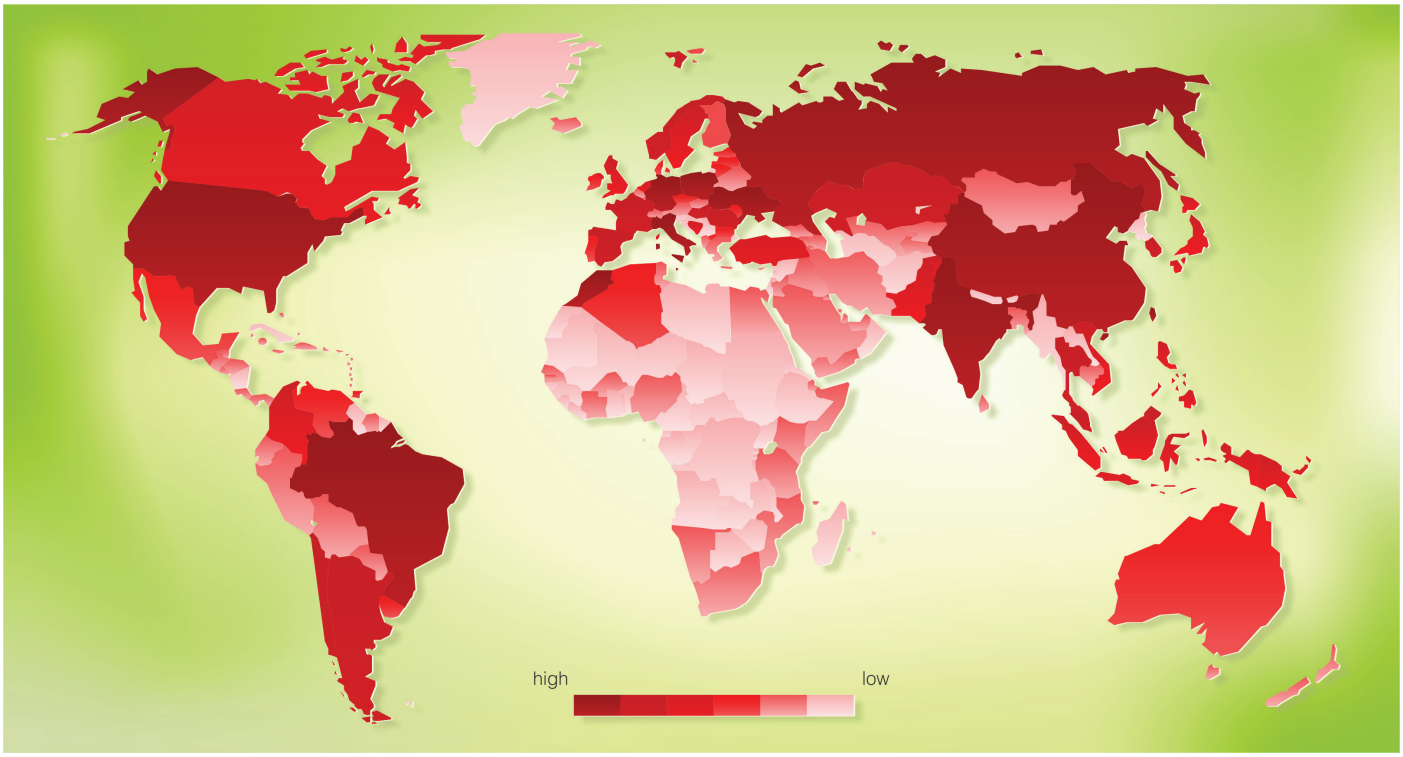
"Defending against denial of service attacks and large-scale worm outbreaks depends on network topology. Our work allows computer scientists to experiment with a range of random graphs that match Internet characteristics. This work is also useful for determining the sensitivity of particular techniques – like routing protocols and congestion controls – to network topology and to variations in network topology," - Priya Mahadevan, Jacobs School of Engineering, UCSD.

What is a DDoS Attack?

The Denial of Service (DoS) attack is a particular class of network threat designed to cripple or render completely inaccessible an online service to valid, clean traffic. Typically, such an attack is affected by initiating a horrendous amount of connections to a victim server, thus flooding its resources or the connection to it. Such invasions are easily detected and the initiator of the attack identified, or at least his actions efficiently blocked. To shed these faults, this type of attack evolved into a new generation of network plague - the Distributed Denial of Service (DDoS) attack. The violator remotely commands and controls a number of hacked computer systems (collectively called "botnet"). The botnets are dispersed all over the world, concealing the attacker's own location, boosting the attack's power and effectiveness.

DDoS type attacks work well due to achieving effective depletion of the targeted object's most vulnerable resources: network capacity, processor time, main memory. Resource depletion is achieved in most cases by employing various methods to emulate legitimate user flow in amounts that render the victim incapable to deal with.

Historical analysis of data accumulated over the past years, shows the average number of attacking hosts in a single attack to vary between 10 to 20 thousand individual machines, each sending 1-2 requests per second. Few systems are capable of maintaining continuous service when faced with an excess of 200-500 requests/sec.simultaneously, every request specially built to convey a maximum load.



Map: Worldwide Botnet Spread Actively Engaged in DDoS Invasions

How are DDoS Attacks organized?

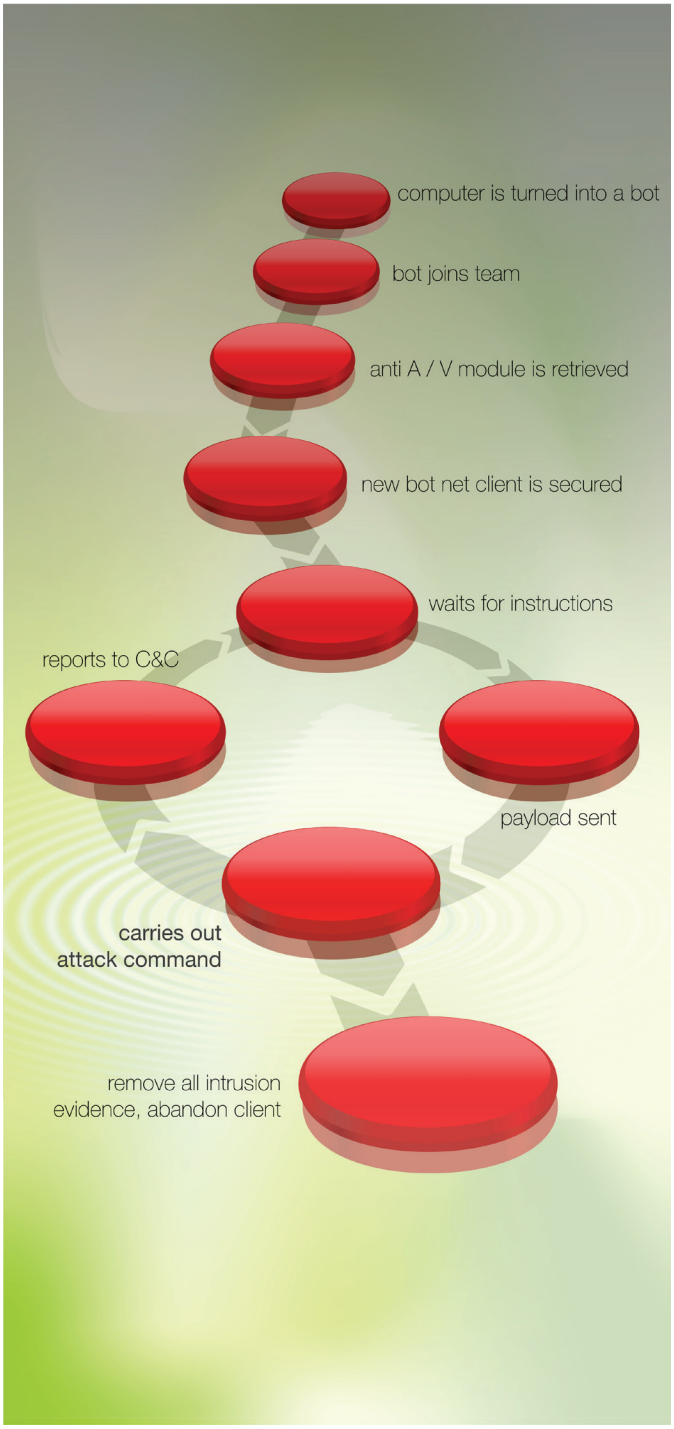
As explained before, DDoS attacks are first and foremost bulk raids by design and intended impact. In order for the attacks to be effective, an enormous collection of computer resources must be secured. This is usually done in advance, not by the DDoS attackers but by other agents, whose job is to make available and sell to the interested parties the bulk of compromised resources.

The process of obtaining access to mass computer muscle involves infecting hundreds of thousands of innocent users' machines with special software devised to enable DDoS attack launch. According to research, the most likely and easy prey to infection are the home computers – one, they are the most wide-spread and numerous on the net, and two – in most cases, unlike most business machines, they lack serious protection against such interventions.

Quite frequently, the infection of a computer is carried out through inadvertent and oblivious to the possible dangers access to a compromised web resource. When accessing such a resource, the victim computer's browser client is subjected to a severe attack whose intent is to exploit one or more of hundreds of existing vulnerabilities within the software. Once the browser is exposed – the job is done.

The victim machine then receives a "loader" – an application that enables the loading and execution of any other code delivered by the violator. Currently, scripts forcing loader installation are successful 80% of the cases. Eight in ten computers that accessed the compromised web resource are converted into zombie-machines - standing by to be controlled and commanded into launching DDoS attacks as members of the collective botnet.

Once the loader is in place, violators use it install special DDoS attack software (DDoS Bot) on the zombie-machines. With this, the preparatory stage is concluded and all that's left for the violator is to direct the onslaught to a victim. The figure on the right shows how a bot is "hooked up" and exploited after it has been compromised



Map: Worldwide Botnet Spread Actively Engaged in DDoS Invasions

Key types of DDoS Attacks

What does the DDoS Bot do? It all depends on the attack objective. There are around 20 types of DDoS attacks, classified by their directivity concept, that are known today. In general, all DDoS attacks could be split into two main groups – those that target connection bandwidth, and those aiming to discontinue a service.

Depending on the attacker's wish, attacks vary in duration - from a short-lived racketeer attack, to a prolonged detrimental invasion.

Attacks aiming to deplete available bandwidth try (and usually succeed) to sever connectivity between the victim and legitimate users by overloading of the data transfer channels and/or the servicing equipment. This is achieved by initiating transmission of a huge amount of packets through the most vulnerable segments of the victim's infrastructure and, in most cases, these packets are specially generated in order to effect greater loading of the target network equipment. Thus, all network equipment resources are used up and the connection appears to be non-existent for valid traffic because it's busy routing "trash" packets. In some instances, it also excludes itself from the routing process, breaking victim's connectivity with the world including legitimate users. The most popular bandwidth oriented DDoS attacks types are Syn Flood (using three-way handshake of TCP protocol), UDP Flood, and ICMP Flood, using UDP and ICMP protocols respectively.

Service- oriented attacks focus on crippling specific network services (most often web services.) The invasion emulates legitimate user activity in quantities that force the victim computer to commence providing access only to attacking machines, thus effectively denying its service to valid traffic.

DDoS Attacks - today's main network threat

One of the key factors making DDoS attacks the most popular threat nowadays is that, by and large, this activity requires no special qualification. In fact, any criminal who wishes to commit a DDoS attack could easily find all instruments needed in the course of an evening, just browsing the net. And he doesn't need to have any IT degree. Unfortunately, this is a 10 dollar bomb that anyone can buy in the nearest drugstore... Also, there are a lot of manuals and know-how readily available on the internet for DDoS attacks organization. Logically, DDoS attacks are becoming an increasingly popular weapon in the hands of students, political hacktivists, supporters of international terrorism, etc.

Criminals, harvesting networks of infected machines (Botnets) and powering DDoS attacks, more and more rarely work alone but often join traditional criminal communities. Most of them don't shy from entering partnerships, thus pooling their resources for guaranteed victim elimination.

The second reason why DDoS attacks are so dangerous and prolific comes from "internal" competition among criminals that drives prices lower. On average, a 10,000 machine botnet attack costs less than USD 400 today, and prices are falling by the day. The process is to be expected and is irreversible due to the ongoing expansion of the Internet with growing numbers of computers that could be used for criminal aims, "fresh" ones, appearing by the thousands daily in the global network.

The two factors combined, cater to an extremely low entry threshold for all interested parties, greatly diminishing the possibility for the attack occurrences to decrease in number. On the contrary, this number will most likely continue to rise to unprecedented levels.

In the meantime the quality of DDoS attack software is improving; criminals use virtual machines with specifically designed algorithms that make zombie-machines almost indistinguishable from real users. Criminals use peer-to-peer technologies for controlling Botnets that makes tracing them very difficult and almost impossible. All of the above accomplishments of the hackers make investments in DDoS attacks more and more effective.

DDoS attacks remain the single most horrendous threat for organizations with an online business. A small-scale inaccessibility of important resources greatly impacts an organizations' prestige, customer loyalty, severing vital revenue streams, inflicting significant, and sometimes irreparable financial losses. So how does one protect their business effectively, without wasting valuable resources at costs that could run astronomically high?

Methods for DDoS attack mitigation

For convenience, existing DDoS attack mitigation and protection methods can be examined in two groups: (i) protection that the victim company decides to build internally, and (ii) such provided by various DDoS Protection companies - one should keep in mind that these companies fairly often copy each other's solutions and market approach, with varying degrees of success.

Historically, most methods deployed by victim companies have displayed and alarming tendency to suffer from grave shortcomings that can be summarized as follows:

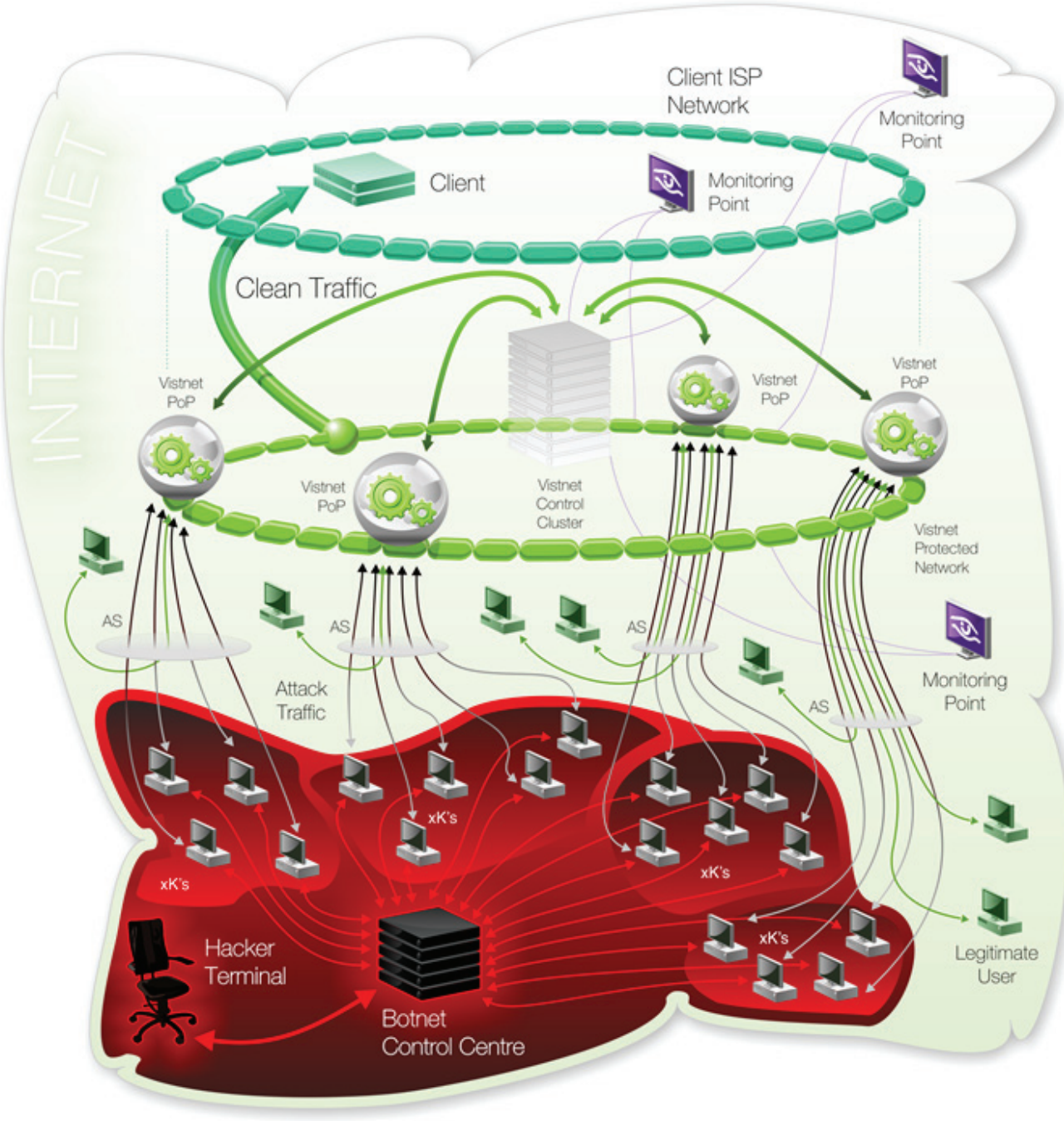
- the protection is limited within the site of the protected network: neighboring network elements and border segments are not affected or controlled
- lack of possibility for immediate deployment - if the protection is not in place at the time of the attack, the company has no means to respond to it as it happens
- inability to mitigate various attack types - usually, the protection covers a limited range of attack types.
- limited resource availability - the most detrimental DDoS invasion types require enormous financial, labor and time investment in network infrastructure, specialized software solutions and connectivity
- the considerably high cost of setting up, maintaining and staffing a protection scheme usually makes it not feasible.

As a result these self-protection techniques and endeavors are typically not merited with outstanding efficacy and expectations are not met duly. The attempted elimination of these defects, in most cases, surpasses in costs the aftereffects of the attack and makes no sense, especially when implemented within the bounds of a single attack target.

Methods employed by core-business DDoS protection providers are safe from these shortcomings but manifest others, equally annoying in some cases:

- case-specific customers receive access to a default configuration of the protection system that does not necessarily reflect service requirements, target groups, and other needs adequately. This is generally due to intended large-scale and mass-market product design, trained on maximizing general compatibility
- lack of well organized and timely feedback, leading to misunderstandings and in the customer-provider chain, resulting in disgruntled customers in need of extensive information on attacks and measures taken
- in some rare cases, protection providers engage in attack statistics juggling and manipulation, aiming at blowing up of estimates for obvious reasons

With customers in the dark for lack of complete attack information, it is not impossible to still experience denial of service, while paying excessive charges for protection.



Typical DDoS Attack Organization and Schematics of the Vistnet DDoS Protection Network

Vistnet DDoS Protection Solution

On the diagram above, one sees a typical DDoS Attack being filtered by the Vistnet Protection Network layer. Hacker(s) sit at a remote terminal connected to a Control & Command Centre, which in turn commands individual user machines en masse – the botnet. Bad/Attack traffic is directed to our protected network, which consists of a number of Points of Presence (PoP) placed around the world, ensuring ubiquitous, adequate and uninterrupted connectivity with your visitors, allowing us to receive and balance malicious traffic globally. To ensure effective functioning of the filtering and cleaning processes in our PoP's, Vistnet use a Decision-Making Control Cluster, which monitors the work of the PoP's, analyses the data and sends fresh and/or revised instructions as necessary. In addition, Vistnet have dispatched Monitoring Points scattered throughout the globe that report client site status from real valid visitor locations. These also send information to the Control Cluster, thus effecting corrective action.

Vistnet Point of Presence (PoP) - how it works:

The Pop is one of several similar structures in the DDoS mitigation network, carrying out direct transit traffic filtering, guided by rules and applying policies defined for it by the decision-making cluster.

So, how is traffic processed inside the PoP?

First, clearly non-targeted traffic is seethed out - often this happens at the border router. For example, UDP traffic is cut off if the specific client does not use UDP-based services. Next, traffic comes to the core-router, where, depending on the rules, it is determined whether to carry out additional filtering or traffic should pass directly to the PROXY / VPN server farm, from where it is sent to the target destination.

As needed, traffic is sent for additional filtering to the filtering server farm - dozens of servers running on high-performance software.

The structure allows not only to perform a series of inspections of incoming traffic, but also to gather additional statistical information, based on which a decision is made - i.) traffic is terminated as malicious, ii.) additional checks and parameterization are performed, iii.) traffic is sent to the recipient.

Additionally, the PoP's house a number of support structures:

- Server recovery - comprehensive configuration data for speedy recovery of under-performing components,
- Server for statistical data preparation - collects and processes "raw" statistics. Ready reports are sent via a secure channel to the decision-making cluster,
- Local monitoring server system - gathers statistics on the technical serviceability of all elements of the PoP.