EIN PRESSWIRE

DDoS Attacks and How to Protect your Web Resource from DDoS Threat

Cloudcom is an Europe based company offering DDoS Protected Dedicated Servers and specializing in protection from oversized DDoS attacks.

DDoS Attack and ANTIDDOS

ZURICH, SWITZERLAND, SWITZERLAND, May 14, 2014 /EINPresswire.com/ -- The today's world is a world of rapidly evolving informational technology. The internet provided a new dimension for modern commerce. Most companies have an online presence, businesses are gaining access to new markets, more and more people are opting to work remotely from home. Of course, not all innovations of this brave new world are applied towards constructive goals. And for IT professionals responsible for security and operation of internet servers every day brings another challenge.

On the one hand, the online business owners are aiming for the optimal price/quality trade-off when choosing hardware and software equipment to ensure a well-functioning company.

On the another, a growing number of companies with online offerings are faced with IT threats that are unknown to brick-and-mortar businesses. No online business is immune to becoming a target of a cyberattack.

Today, the DoS (Denial of Service) attack or the DDoS (its distributed variant) - is considered to be one of the gravest problems affecting performance of virtual resources. In this respect, the government and bank websites are just as vulnerable as online gaming sites or even websites promoting magic services.

In 1988 the creation of the first worm virus foreshadowed the danger of informational technologies becoming the instrument of perpetrators. However, cyber attacks became widespread only ten years later. By 1998, the widespread adoption of high-speed Internet combined with a large variety of cheap and readily accessible tools for attacks became the chief factor in rapid advancement of cyber crime. The beginning of the 21st century was marked by the famous case of a 15 year old high school student, who in February 2000 initiated a number of attacks under the name "Project Rivolta" directed against such mega-sites as FIFA, Amazon, Dell, eBay, and CNN. By 2003, following several successful and disruptive attacks against Microsoft, internet DNS-servers, and LiveJournal.com, DoS/DDoS gained a reputation of the most pressing challenge of all online threats.

Today, every developed nation has adopted legislation penalizing cyber crime. These measures are especially crucial due to the widespread accessibility of DoS/DDoS blueprints and tools on the internet today. The power amplification of attacks has changed from 10-20 Gbit/s a couple years ago to 300 Gbit/s today.

DoS and Distributed DoS.

DoS and DDoS cyber attacks vary in their objectives and methods of realization. Nevertheless, this type of activity is always intentional, involving one or a large number of participants. The main objective of the attack is to infringe upon the network circuits or the whole system in order to bring down its performance. In turn, the legitimate users can not connect to the attacked website, receiving browser error "403 Forbidden" or "500 Internal Server Error." Quite often this disruption of service will result in web resource downtime, will inflict damage to the business' reputation and lead to loss of clients and revenue.

Classification of DoS and DDoS.

In general both DoS and DDoS attacks aim to flood the bandwidth or deplete the system resources. DDoS is the more comprehensive, distributed version of the attack. Distributed DoS engages not one, but many zombified computers, located all over the internet, making it extremely difficult to identify the source of the attack. At the present day, the advanced technology of networks and operating systems can repel some types of DDoS attacks, but only if the machines delivering the attack do not number in hundreds or hundreds of thousands.

There are two types of DoS and DDoS: local and remote.

Among the local attacks there are certain types of exploits, fork-bombs and viruses opening dozens of files or initiating an endless cycle of duplicating themselves, consuming processor and memory resources. The remote network attacks subdivide into two categories:

1) Remote attacks that exploit security holes and errors in the operating system in order to bring down the server;

2) Flood attacks aim to overwhelm the victim server with enormous amounts of meaningless IP packets.

While security wholes can be fixed once they've been exposed, it is a lot harder to guard against a flood attack. The flood works in two distinguished ways: in the first scenario the flood of IP packets fills up the connection line, not allowing for the server to process necessary information.

In the second case, the attack is directed not at the whole site, but at the specific segment that is running a resource-intensive application. A ton of requests is sent to this segment's address which leads to resource overload and performance slow down of the whole site.
The most common types of floods include: ICMP-flood (ping, smurf), UDP-flood, SYN-flood and HTTP-flood. The advanced types of DDoS can combine some or all of these attacks.

Let's see how these attacks work.

ICMP-flood is considered to be the most primitive and the most dangerous type aiming to clog the bandwidth and overload the internet protocol stack of TCP/IP.

"Ping" is called a flood attack that sends ICMP packets of the echo request (?ing), demanding the computer-addressee to reply with ICMP packets of echo reply. Once the connection is confirmed the victim-computer receives an enormous amount of ping packets depleting its CPU's resources and the availability of the bandwidth.

SMURF combines the echo request mechanism with IP spoofing to initiate a distributed attack. The attacker sends ping requests to a large number of random computers (a broadcasting network) switching the victims' IP address as the "reply to" address of the request. As a result, every machine in the broadcasting network sends back an echo reply to the victim computer ?exhausting the capacity of its connection. This attack is very effective and widespread.

UDP-flood is similar to ICMP, but instead of using ICMP-packets it delivers requests through the UDP protocol layer. A typical method of exhausting the system resources and availability of the bandwidth is based on directing a never-ending traffic of UDP packets to the ports 7 (echo request) and 19 (chargen request) of the target computer. The UDP protocol does not require a full communication handshake to exchange data, making UDP attacks difficult to detect and extremely effective.

Today the SYN-flood is considered the most well-known type of flood. It is based on the idea of establishing a large number of TCP-connections by sending SYN ("open connection") requests with spoofed source IP address. The victim-computer tries to process the requests by sending a SYN/ACK ("confirm open request") message back and waits for confirmation which never arrives.

Unlike ICMP and UDP attacks, the aim of SYN-flood is not only to clog the communication line, but also to sabotage the network stack forcing it to process and wait on multitudes of falsified requests. This renders the victim unable to accept valid connections.

HTTP-flood is also a very popular type of flood. It often attempts to sabotage the work of a server by targeting a script that accesses a database. The HTTP-flood initiates requests of type GET or POST causing the server to respond with data that is hundreds of times larger than the initial request. While responding to the malicious requests the server is forced to consume its resources and available bandwidth.

One can think of Distributed DoS as a result of the DoS attack harnessing the full power of the internet. The DDoS is the most widespread type of botnet activity. A botnet is a network of several computers (hosts) running bot software. Bots aim to infect the victim computer's and use them to send spam, steal personal information and initiate other DoS attacks.

The largest botnets are:

Kraken - 400,000 computers.
Srizbi - 315,000 computers.
Bobax - 185,000 computers.
Rustock - 150,000 computers.
Storm - 100,000 computers.
Psybot - 100,000 ADSL - routers running on Linux.
Botnet BBC - 22,000 computers. (experimental prototype created by BBC)

A plain DoS attack uses a small number of computers. It is easy to detect because the resource demands on the target system grow while the number of connections ("users") stays low. It is much harder to recognize and defend against the Distributed DoS because it causes no noticeable abnormalities in the system's performance pattern. Each computer in the attacking botnet is indistinguishable from a legitimate visitor to the site. The number of "users" increases - so does the system's resource utilization.

A famous example of legitimate users "causing" a DDoS attack is when Twitter became unresponsive in 2009, right after the news of Michael Jackson.

Cloudcom S.L.
Cloudcom S.L.
+34931731456
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.