

*newsletter*

## Distributed Denial of Service-Attacks in the Internet

**Distributed denial of service attacks (DDoS) are an ever increasing risk for the internet. Such attacks are becoming more frequent and are now targeting central elements of the internet's infrastructure.**

### **DDoS on DNS servers**

At the end of November 2002 the internet provider UltraDNS (responsible for the administration of the Domain Name System (DNS) server of the top level Domain.info) was subject to a DDoS lasting 4 hours.

A month earlier on 21.10.2002, the root servers of the DNS were the target of a massive DDoS attack. DNS servers form an essential component of the internet, being a form of address book for the entire internet.

Every computer in the internet is assigned a specific address. The job of the DNS system is to categorise each computer and translate the user-friendly Web addresses (e.g. www.swissre.com) into numeric IP addresses that can be understood by computers (e.g. 193.246.224.28).

This attack, the most severe and complex to date according to US authorities, lasted for around an hour. 7 of the 13 root servers around the world crashed completely, while a further two were all but put out of action. Internet users noticed little of what was going on because the servers of local ISPs (Internet Service Providers) are able to buffer IP address allocations for a certain length of time. In the case of a lengthier failure, however, problems must be expected in terms of internet access and mail routing. To date, no one has been held accountable for the attacks.

### **Technical background**

DDoS attacks on the internet have been occurring for several years already. They exploit the weak-points inherent in the implementation and configuration of network functions of a variety of operating systems. Denial of service is a process that aims to disrupt network services (e.g. a web or mail server), thus rendering it difficult or impossible to use. The network link of the target is systematically bombarded with a large number of data packets which leads to overloading and, ultimately, failure of the system.

To achieve this end, the attacker must be in possession of a sufficiently large number of IT resources. An optimum method of generating enough resources is the so-called distributed denial of service attack.

In contrast to a simple denial of service, a DDoS attack is launched from several different sources simultaneously, i.e. numerous computers send data packets simultaneously in a co-ordinated fashion to a specific target address.

This is done using automated DDoS programs such as Trinoo, Tribe Flood or "Stacheldraht" that are readily available in the internet.

**How an attack works**

The DDoS attacker works in the background, activating other computers as tools in the operation. This is why it is so difficult to trace the instigator of this type of attack. The attacker first seeks out unprotected computers in the internet. He uses these as "hosts" for his weapons of attack, thus building up an entire network as the attack base.

In simple terms, an attack proceeds as follows:

- the instigator gives the attack command to the master programs in his attack network;
- the master programs route the command to the computers under their control (daemons);
- numerous daemons simultaneously attack a pre-arranged target system - the victim.

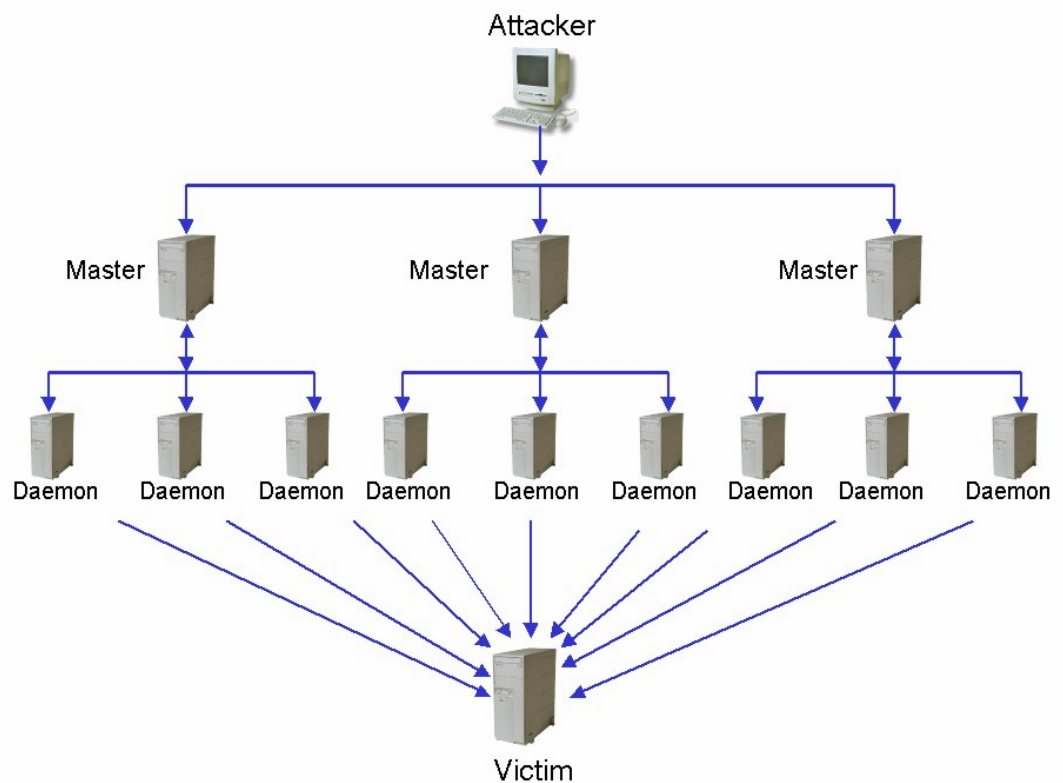


Fig.: overview of a DDoS attack

**Other examples**

Denial of service attacks are a major and ever-present security threat for companies. 40% of the companies which took part in the CSI/FBI's Computer Crime and Security Survey claim to have been hit by a denial of service attack in 2001.

Examples of DDoS attacks:

- in February 2000, renowned internet providers such as Yahoo.com, ebay.com, Amazon.com, and CNN.com were virtually incapacitated for up to 3 hours by a massive DDoS attack;
- a large number of Microsoft's Web pages were attacked in January 2001 and were unavailable for up to 24 hours;
- in February 2002, a long series of DDoS attacks resulted in the British internet provider, CloudNine, having to close down.

## **Conclusion**

These events highlight the risks in an ever highly networked digitised world economy that is becomingly increasingly dependent on the availability of IT infrastructures. DDoS attacks pose an ever greater risk to companies whose businesses rely on internet presence. Up to now, this attack technique has targeted, in the main, specific E-commerce providers and institutions. Selective attacks on the core elements of the internet's infrastructure, however, represent a much greater threat, given the potential for economic losses.

## **Information for the underwriter**

IT system failure due to denial of service attacks are not normally insured under standard property and liability covers. There are, however, special insurance products that cater specifically for IT and internet risks, including network failure. To reflect the seriousness of this risk, it is essential that underwriters conduct an in-depth assessment of each risk and conclude suitable time deductibles with the client.

Inadequate protection of information technology against unauthorised access makes it easier for such systems to be used as tools in an attack against a third party. This can lead to third-party liability claims by a victim against the operator of the violated system (downstream liability). During risk assessment of internet or IT liability covers, it is essential, therefore, that the degree of protection against attack is carefully examined.

Business interruption caused by the failure of external networks following a denial of service attack can lead to losses via supplier/customer extensions. Careful assessment of the risk is important here too, especially with regard to interfaces and interdependencies to internet service providers, hosters and carriers.

Further, there is a danger of accumulation exposure arising from attacks on internet infrastructures in cases where insurance programmes provide business interruption cover for IT systems without underlying material damage. This is particularly the case when central elements of the internet infrastructure fail. Up to now, however, a practicable method of regulating this accumulation scenario has yet to be found.

## **Contact**

AssTech GmbH  
Postfach 1211  
85766 Unterföhring bei München  
Telephone + 49 89 3844-1585  
Telefax + 49 89 3844-1586  
info@asstech.com  
www.asstech.com