

SECURITY THREATS AND TRENDS

OCTOBER 2007

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and The Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

SUMMARY

The level of traffic is nearly at the same level as last period, but the traffic is more spread out through the entire month. Of the bigger reconnaissance attacks it is mainly MS SQL and VNC services that is exposed. VNC-1 is the service that had the most increase this period. China has now passed the US on the top 10 list. This is mainly due to searches towards MS SQL, but China has been active towards all services. Mexico has also had a big increase this period. When we look at worm and spam traffic there is, not unexpected, a small decrease this period as well.

Focus of the month presents DoS attacks, historically and today.

TABLE OF CONTENTS

INTRODUCTION	4
THREAT LEVEL	5
RECONNAISSANCE ATTACKS AUGUST 2007	5
TYPE OF RECONNAISSANCE ATTACKS	6
RECONNAISSANCE ATTACKS PR COUNTRY	7
INTERNET WORMS AND SPAM	8
ALERT STATISTIC	9
HANDLED ALERTS	9
REPORTED INCIDENTS	10
FOCUS OF THE MONTH – DOS ATTACKS	11
DENIAL OF SERVICE	11
DOS HISTORY	11
THE ATTACKS OF TODAY	12
COUNTERMEASURES AND RESPONSE	13
SOURCES	14

INTRODUCTION

This report is based on three main parts: Threat level, Alert Statistic and Focus of the Month.

Threat level is a presentation of what threats organizations are exposed to through their Internet connection. In this threat evaluation, reconnaissance attacks from the Internet against customers of Secode are analyzed and presented.

Alert Statistic is based on alerts from Secode's IDS and IPS tools. An alert appears when a sensor recognizes network traffic that fits the implemented signatures/filters, and in these cases alerts will be transferred to the Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handled by analysts at Secode.

Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

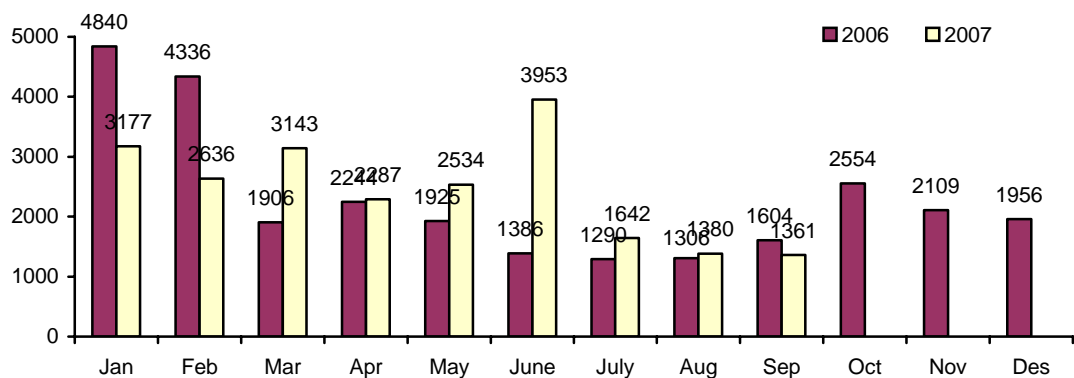
THREAT LEVEL

Due to high activity level, Internet worms and spamming are handled in a separate subchapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

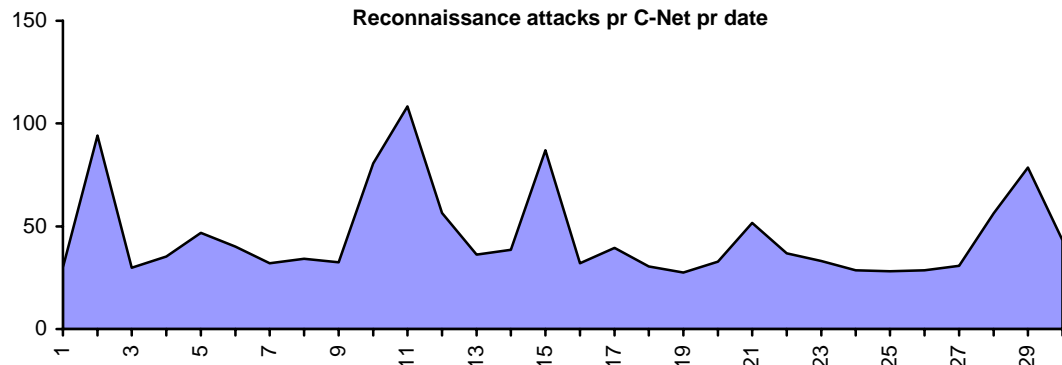
RECONNAISSANCE ATTACKS AUGUST 2007

The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different network areas.

Reconnaissance attacks pr monitored C-Net



Reconnaissance attacks pr C-Net pr date

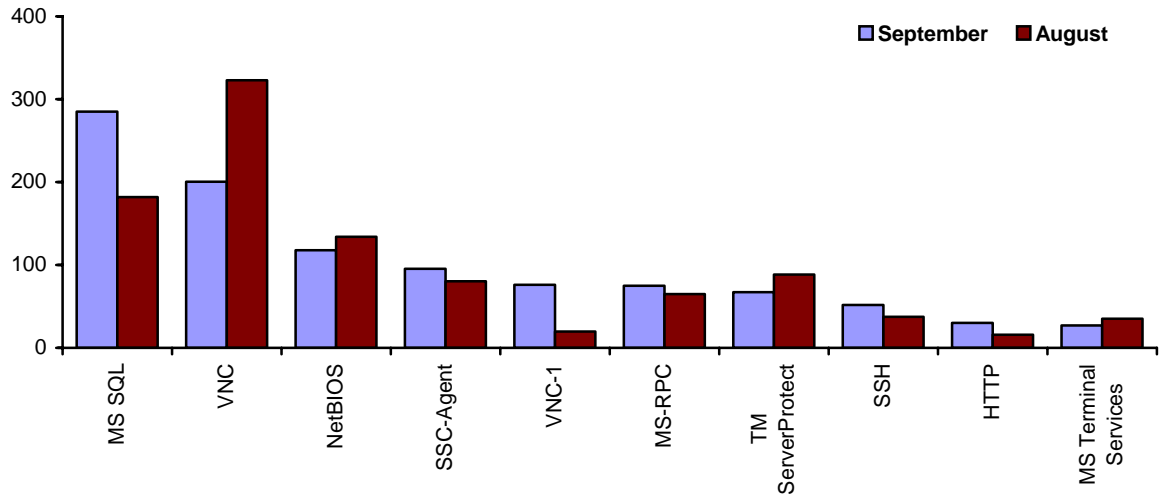


The traffic level this month is nearly at the same level as last period. However, last period there were two significant peaks during the period, while we in this period see that the traffic is spread more over the entire period. The peak on the 11th is related to a large number of searches towards MS SQL, mainly from China. The peak on the 15th is related to a large number of searches towards VNC-1, mainly from China, Mexico and Singapore. As for the last peak of the period, on the 29th, those searches are directed towards VNC.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months. The diagram does not separate scans for one single service from combined scans for several services.

Average top 10 incidents pr C-Net

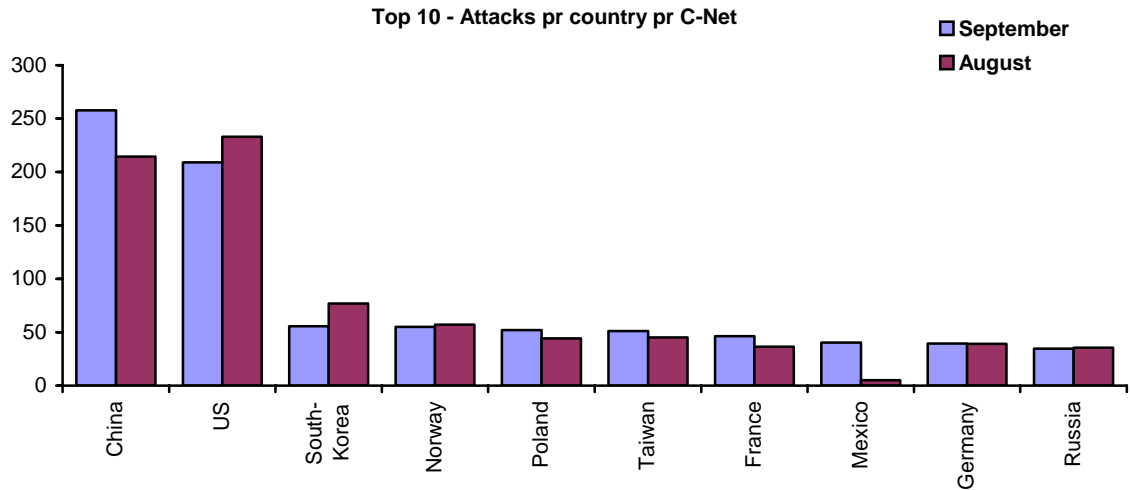


We continue to see a decrease in the level of traffic towards VNC this period, and this period MS SQL is the most exposed service.

The most distinct difference we see from last period is the increase in searches towards port 5901 (VNC-1). VNC services are under a large amount of pressure at all times, and during some time now searches have been directed towards port 5901 and 5902 (VNC-1 and VNC-2).

RECONNAISSANCE ATTACKS PR COUNTRY

The malicious activity in the statistic below is mainly automated attacks, which comes from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed.



China has passed the level of traffic seen from the US this period. Most of the traffic seen from China is searches for MS SQL this period, but China is active towards all services.

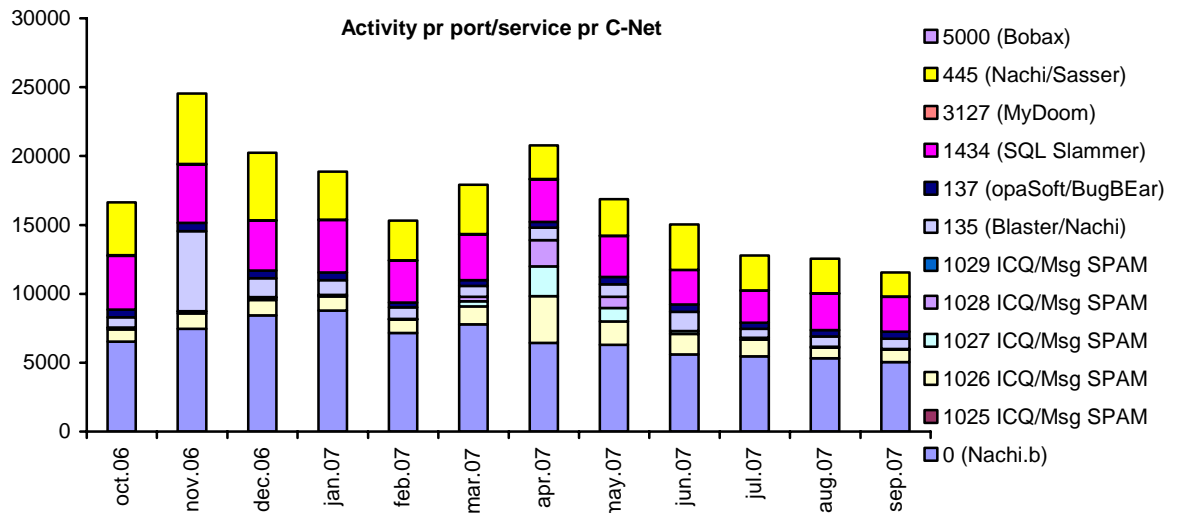
We can also see that Mexico has had a large increase of traffic this period, and is now among the top 10 countries of origin. Attacks from Mexico are, as previously mentioned, related to searches towards VNC-1.

There is still a decrease in searches from Norway, but Norway is still at the same placement as last period. New reports from other security vendors tell us that Norway is actually one of the most active sources in other countries as well.

China is followed by the US and South-Korea this period.

INTERNET WORMS AND SPAM

Because of a high level of activity against certain services, such traffic is presented in separate statistics. This applies for services most frequently targeted by Internet worms and spamming attempts.



The worm and spam traffic level is still decreasing slowly. There are only minor differences among the categories. There is a trend that the attacks are being executed by botnet or that the attacks are more direct. In other words, it is as expected that there will be a decrease here.

ALERT STATISTIC

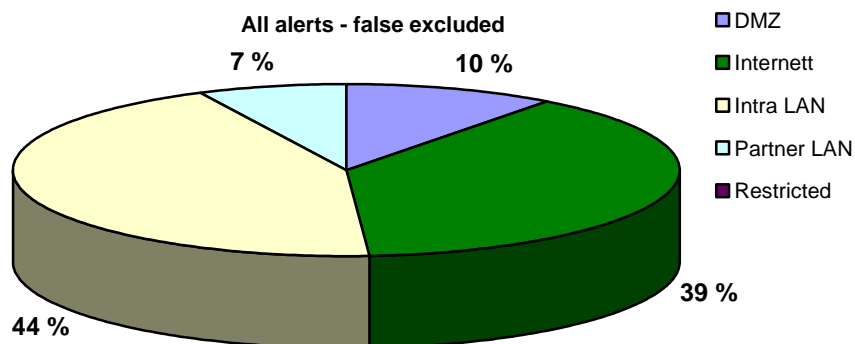
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

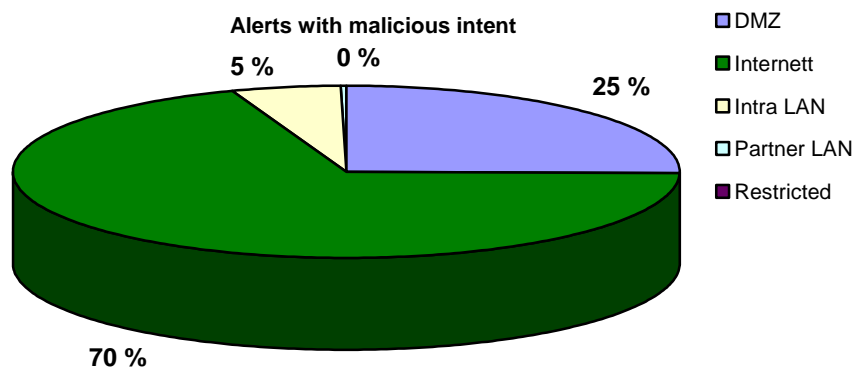
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located inside the network and monitors traffic between clients, servers and other network equipment
- Partner LAN: the measuring point is located in an environment that is used for communication towards external partners. The partner LAN is without Internet access
- Restricted LAN: the measuring point is located in a limited environment with a very well defined traffic pattern and without Internet access



The diagram above shows the distribution for all genuine alerts.



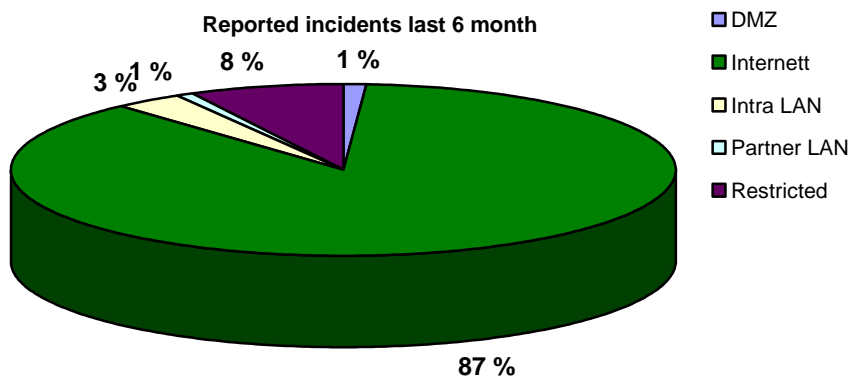
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



FOCUS OF THE MONTH – DoS ATTACKS

Denial of Service (DoS) attacks have been around for many years, but have developed during the years. In this month's Threats and Trends we will take a closer look at the history of DoS attacks and what today's trends are. Denial of Service attacks is today the type of attacks that have the potential to do most harm on the Internet. While other web attacks are more directed, and often have a financial motive, many DoS attacks are only after doing some harm.

DENIAL OF SERVICE

Today Denial of Service attacks are divided mainly into two areas; the "common" Denial of Service attacks, where the attack is from one source towards one system, and the so-called Distributed Denial of Service (DDoS) attacks, which consist of many computers attacking one system. The computers in a DDoS attack may either be a part of a botnet, or it may be compromised machines sending a large amount of data on the network.

A DoS attack is an attack where the goal is to make a computer system unavailable to its intended users. Attacks may happen in many ways, but the goal is to either force the computer to reset, it could also make services unavailable by using resources, or it is obstructing communication between user and victim.

DoS HISTORY

DoS attacks have developed along the IT development at large. There have been so many incidents and developments within DoS that it is difficult to get all in a timeline. Some of the most important events in history are retold here.

- Prior to 1995: No special methods were available at this point, but DoS attacks were executed. Attacks at this point were executed by using simple probing or scans. Some of the attacks were actually as simple as physically destroying computers or changing user rights and so on.
- 1995: "Chatters" are taking down machines by using the ping of death. Ping of death is sending a malformed ping packet with a size that exceeds the size of a normal IP-packet. Use of Nuke is also popular at this point. This attack is similar to the ping of death, but here the attacker sends a huge amount of small ICMP (ping) packets towards one target.
- 1998: Smurf attacks are getting more popular. Smurf attacks are executed by sending a large amount of ICMP echo packets to broadcast addresses, which results in a huge amount of echo replies in the network.
- 1999: A huge amount of data coming from computers under the control of hackers is discovered. This become known as Distributed Denial of Service (DDoS) attacks since most of the attackers uses hundreds, maybe thousands, of zombie computers distributed all over the Internet to execute the attack.
- 2000: A DDoS attack is taking down Yahoo.com, eBay, Amazon.com and mane other websites for several hours. Authorities arrest a 15-year old Canadian, "mafiaboy", after he brags about the attack on Internet. He had managed to get control over several computers at a lab on the University of California, which he then used to execute the attack. It is estimated that Yahoo.com lost \$ 500,000 due to downtime, and Amazon.com lost \$ 600,000.
- 2002: A DDoS attack hits 9 of the 13 servers that are the backbone of Internet. Even though the scale of the hour long attack was large, Internet users remained mainly unaffected by the attack. Security experts believe that if the attack was to continue for a longer period of time it would have a great impact on the electronic communication worldwide.
- 2003-2007: Several worm attacks have been executed with more or less success when it comes to Denial of Service. It will be too much to list all, but one example is the Blaster worm.

- February 2007: A large attack was executed towards online game servers, where more than 10,000 gamers were affected. The attack was initiated from the former Soviet Union.

The figure below tells us how DoS attacks have developed during the years from 1990 to 2000, and how it has become easier for attackers. Today you need minimal of knowledge to be a part of a DoS attack. This is because a lot of code and software is available online. The attacks, however, are more sophisticated than ever.

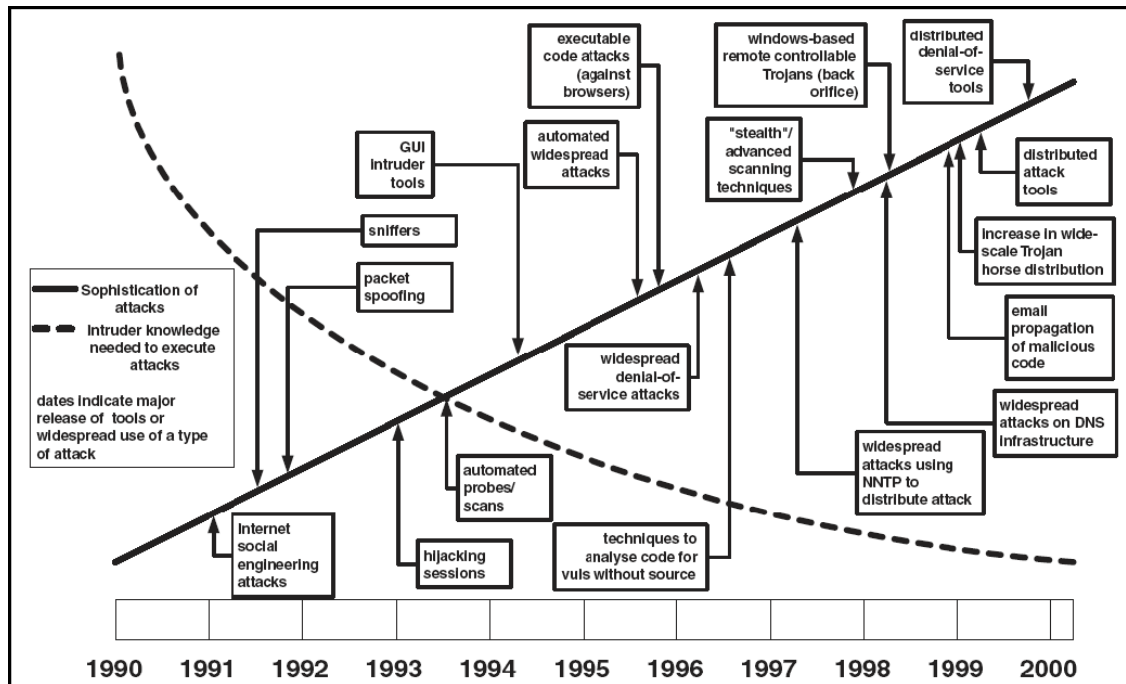


Figure 1 Evolution of DoS attacks

THE ATTACKS OF TODAY

Many of the attack methods which have surfaced over the last years are still in use today. However, there are slim chances for them to be successful, because IT-security has also developed during this time. Of Denial of Service attacks there is mostly DDoS attacks happening today, and these are usually from a zombie net, or a botnet as it is also called. The attacks are today often directed to bigger nodes or ISP level, so they hit a bigger part of the Internet.

A botnet consists of several zombie computers which have been compromised by a hacker, a virus or a Trojan. MPack solutions, or similar, may be used to compromise computers to become zombies. In addition to be used in DDoS attacks they will also be used to, among others, spam and phishing.

The figure below shows the different attack categories under DDoS attacks.

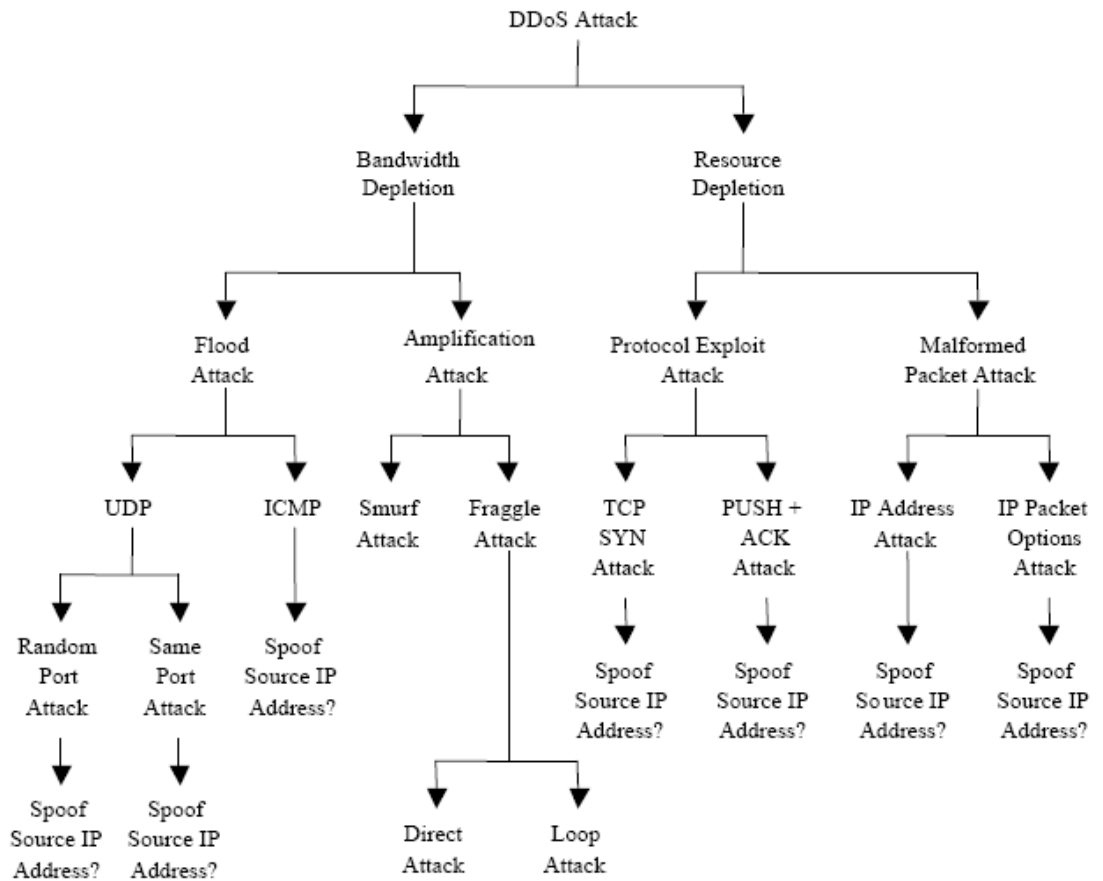


Figure 2 DDoS Attack Categories

COUNTERMEASURES AND RESPONSE

To be able to stop an attack as soon as possible there are some countermeasures that may be carried out. This may be:

1. Have the possibility to emergency block traffic from special IP-addresses. If using a botnet this may prove to be difficult, but if there are some known patterns it may be possible to block by content instead. Packet dropping may also be a solution.
2. Have an alternative route available which may be used to keep the service available under an attack.

To avoid attacks there are several possibilities as well:

1. Use of SYN cookies that makes sure that no resources are to be used before a client address has been verified.
2. Use of firewall reduces possibility for a DoS attack. Some attacks use legal services and addresses, only sending lots of packets or bigger packets, and they are harder to stop. However, a firewall may be useful to stop simple flooding attacks.
3. Many switches have built in possibilities to make DoS attacks harder. This may be Bogon filtering for example.
4. IPS may stop a great deal of DoS attacks by dropping packets or blocking traffic. However there are possibilities for legal packets, in large scale that may be allowed through an IPS.

The ISP (Internet Service Provider) may also implement countermeasures when under attack. This can be:

1. Blocking of fragmented packets
2. Blocking port 80 with Access Control Lists (ACL) towards IP addresses under attack

ISPs actually have a big responsibility for countermeasures being implemented, this because equipment at the companies under attack rarely have capacity to stop a bigger attack.

SOURCES

Security researchers uncover massive attack on Italian web sites

<http://arstechnica.com/news.ars/post/20070618-security-researchers-uncover-massive-attack-on-italian-web-sites.html>

Denial of Service - Brief History & Introduction to Defenses

<http://www.cs.unc.edu/~jeffay/courses/nidsS05/slides/3-DDoS-History-Defense.pdf>

Wikipedia - Denial of Service

http://en.wikipedia.org/wiki/Denial-of-service_attack

Wikipedia - Ping of Death

http://en.wikipedia.org/wiki/Ping_of_death

Wikipedia - Smurf Attack

http://en.wikipedia.org/wiki/Smurf_attack

Wikipedia - Zombie Computer

http://en.wikipedia.org/wiki/Zombie_computer

A Brief History of Denial of Service Attacks

http://www.castlecops.com/a3963-A_Brief_History_of_Denial_of_Service_Attacks.html

Defenses Against Distributed Denial of Service Attacks

<http://www.garykessler.net/library/ddos.html>