

SECURITY THREATS AND TRENDS

APRIL 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 year 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 reconnaissance attacks have shown an increase during March. However, compared to January, which has the same number of days, the activity level is at a relatively stable level.

No new trends have been detected this month.

In 'Focus of the Month', we discuss cyber terror.

TABLE OF CONTENTS

INTRODUCTION	3
THREAT LEVEL.....	4
RECONNAISSANCE ATTACKS MARCH 2006.....	4
TYPE OF RECONNAISSANCE ATTACKS	5
RECONNAISSANCE ATTACKS PR COUNTRY.....	6
INTERNET WORMS AND SPAM.....	7
ALERT STATISTIC.....	8
HANDLED ALERTS	8
REPORTED INCIDENTS.....	9
FOCUS OF THE MONTH – YOUTH TRENDS	10

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 appear when a sensor recognizes network traffic that fit the implemented signatures/filters, and in these cases alerts will be transferred to Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handles by analysts at Secode.

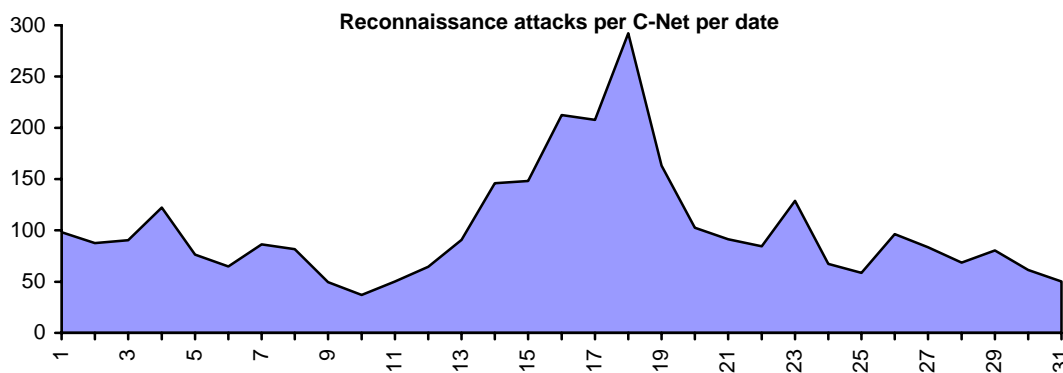
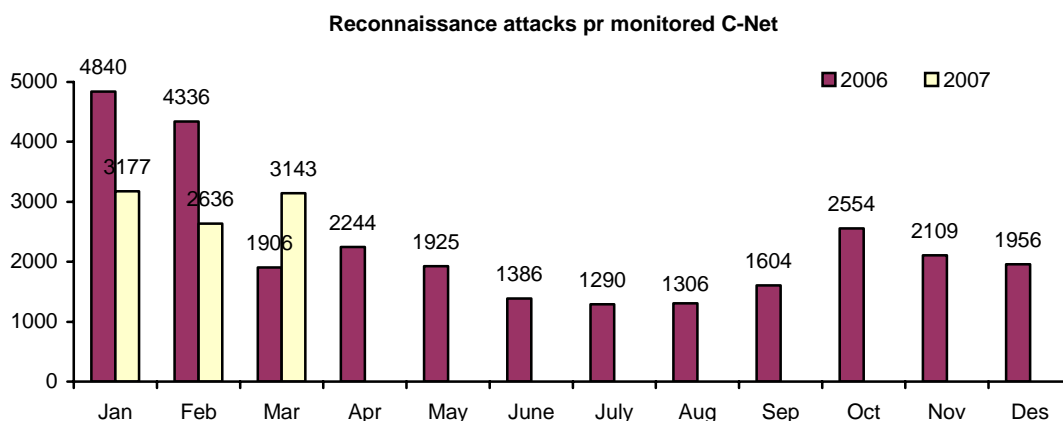
Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

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 MARCH 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.



There has been an increase in the total number of reconnaissance attacks from February to March, but with a view to the fact that February has a lower number of days, the activity level still seems to remain at a stable level. When comparing January and March (which has the same amount of days) there is only a minor change.

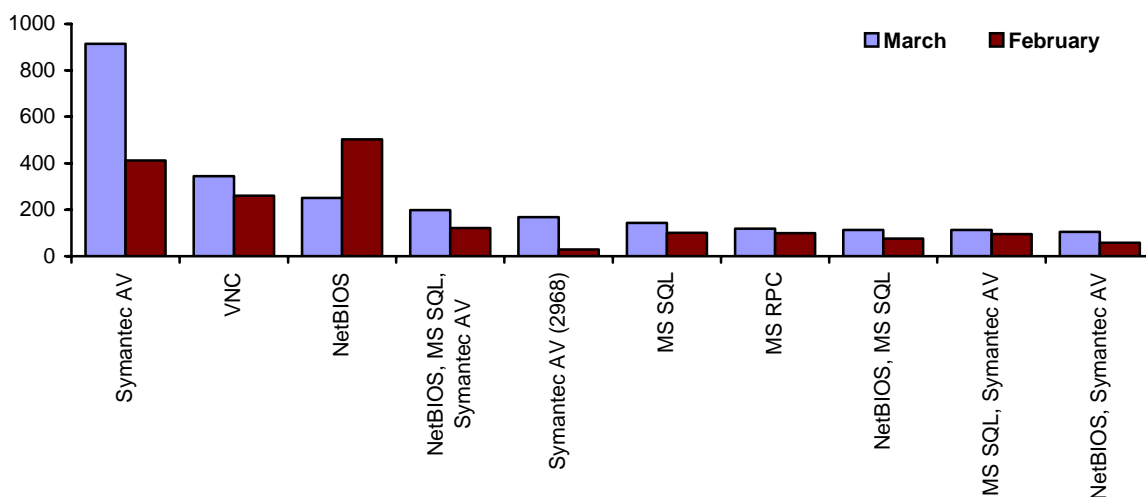
There has been an increase in the number of scans for port 2967. Besides that, there is a small scanning increase for most services, something that implies that there are few direct targeting scans .

There is no special attack behind the activity top around the 18th of March.

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 per C-Net



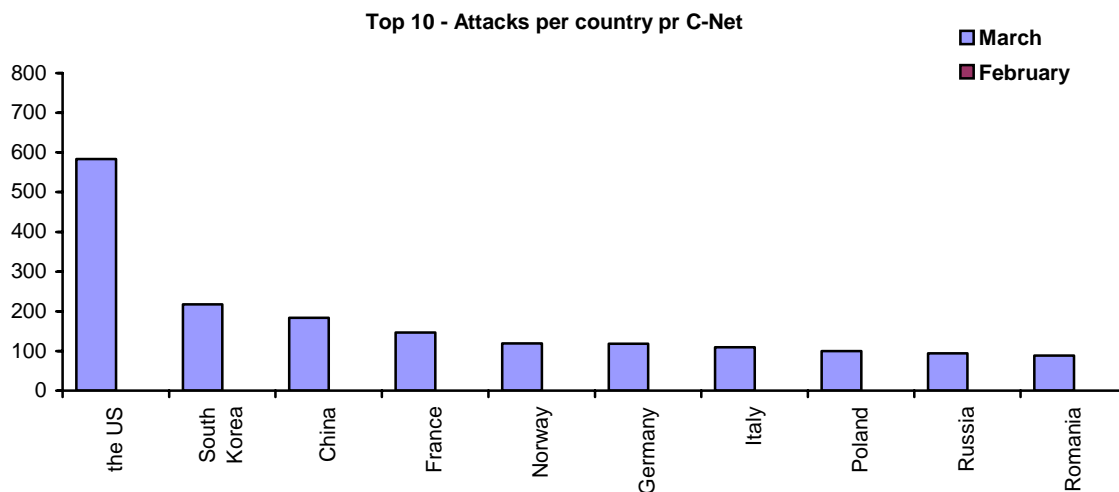
Scans for tcp port 2967 (Symantec AV) has once more increased after a considerable relapse last period. Scans for tcp port 139 (NetBIOS) is on the other hand reduced, which makes it the only service among the Top 10 that has been decreasing during March.

Scans for tcp port 2968 (ENPP, used by Symantec), has also decreased slightly. Otherwise there are only minor differences comparing with Top 10 lists from previous periods.

All the services above have previously been at the Top 10 list.

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.

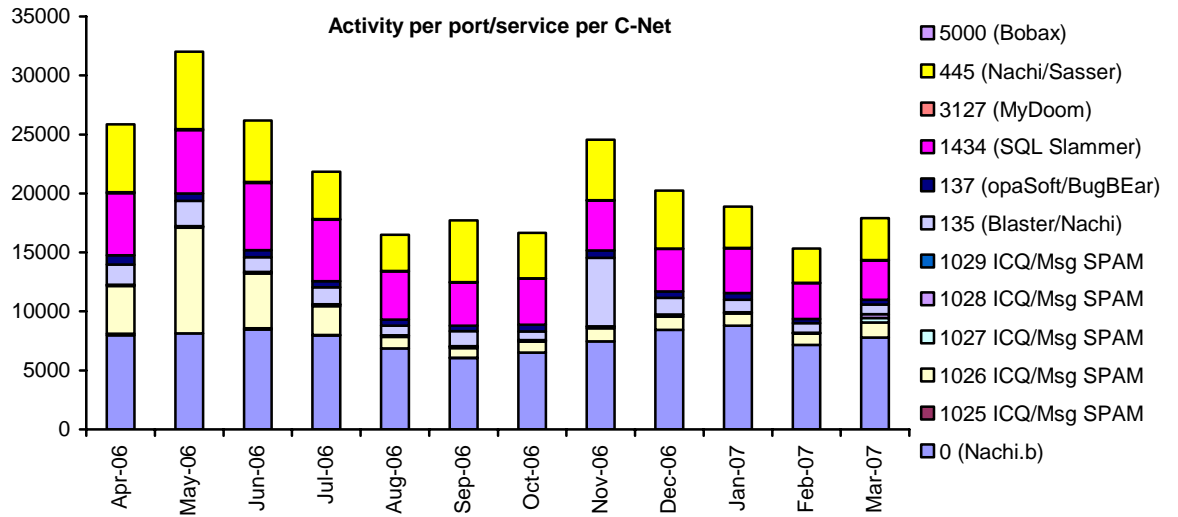


As in earlier periods, the US is the most aggressive source of reconnaissance attacks, but there has been a slight reduction this month. Romania is new to the Top 10 list of March. Traffic from this country is observed towards several of our customers, so there is no particular attack behind this new element in the statistic above.

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

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.



There has been a slight increase in worm- and spam activity this month. This increase is caused by more traffic towards ICQ/Msg Spam.

ALERT STATISTIC

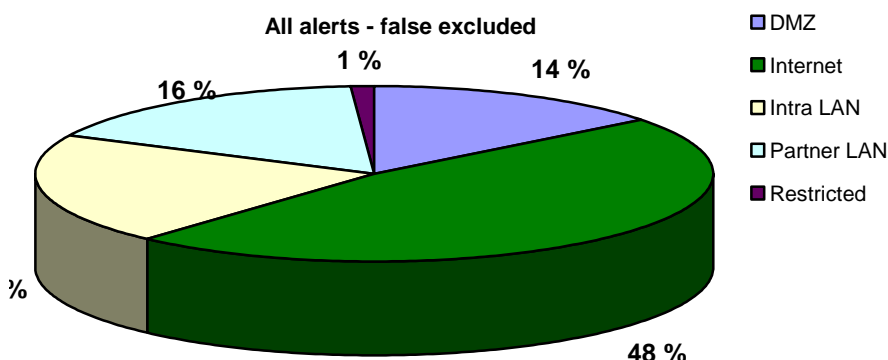
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

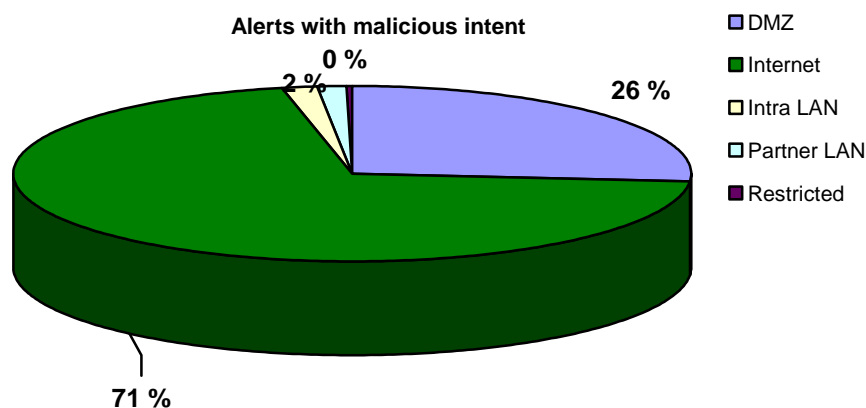
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

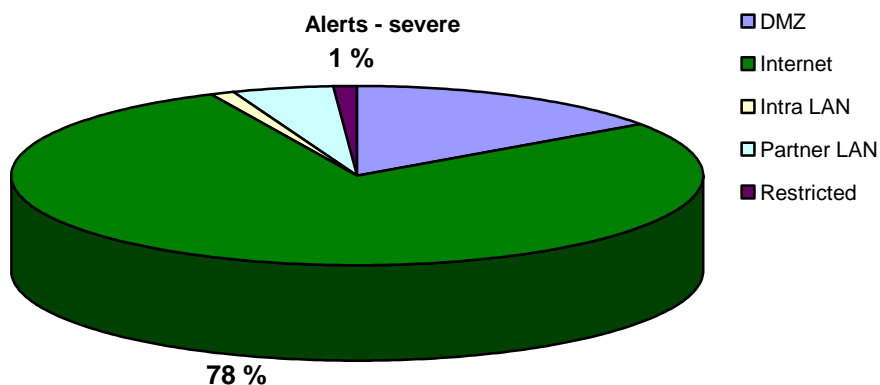
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located 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.



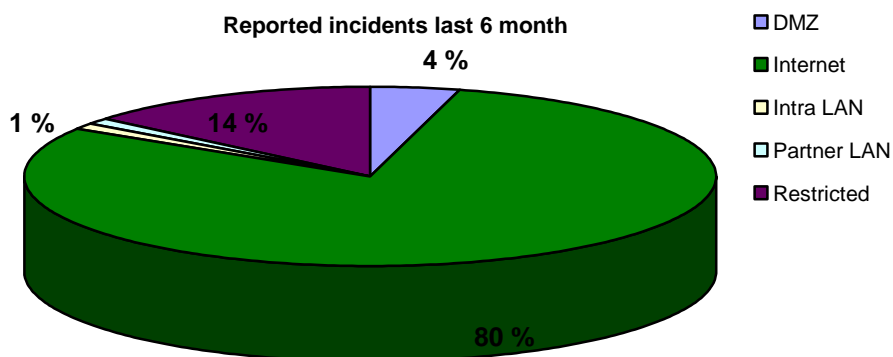
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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 – CYBER TERROR

Cyber terror was mentioned in the last Focus of the Month. This month we take a closer look at this phenomenon, and try to define exactly what cyber terror is and how it is being used.

During the last years we have got an impression that people relate terror to large destructions in the shape of bombs, airplane hijacking, and so on. This picture of terror has arisen from many years of media focus. Terror is much more, and here we try to give a more complete picture of this.

GENERAL TERRORISM

To define cyber terror, it might be O.K. to start by defining terror as a general concept. However, today no such clear definition of terror or terrorism exists. Terror is often used to describe the ability to create fear, while terrorism is terror used to achieve a political, religious or ideal measure. Other definitions say that all destruction of property or use of terror to achieve a political, religious or ideal measure is terrorism.

With other words, it is not necessarily so that the destruction of property has to make people frightened, as long as it is done with an intention to promote a political, religious or ideal goal.

As a pointer to the different definitions, here follows the definitions of the FBI and the American Department of Defence:

FBI

Terrorism - Illegal use of force or violence against people or property; to frighten or enforce a state, civil population or parts of this, to declare political or social opinion.

Department of Defence

Terrorism – calculated use of violence or threats of violence to impress fear; planned to enforce or frighten a state or society to achieve a goal of political, religious or ideal means.

Cyber terror

The definition of cyber terror follows the general description above, but applies for digital property. Cyber terror occurs in many different degrees of severity, where the most serious might be to influence the digital equipment in an airplane and make it crash, while the least serious is to redirect web sites to other sites showing political, religious or ideal messages (cross-site scripting attacks).

Many people will most likely disagree in this definition, mostly because this definition is so far away from how the media presents terror. Still we choose to follow this definition, as it is the most appropriate way to include the general definitions.

DEFINITION OF CYBER TERROR

Illegal destruction or disruption of digital property to frighten or enforce a state or a society, to achieve a political, religious or ideal measure.

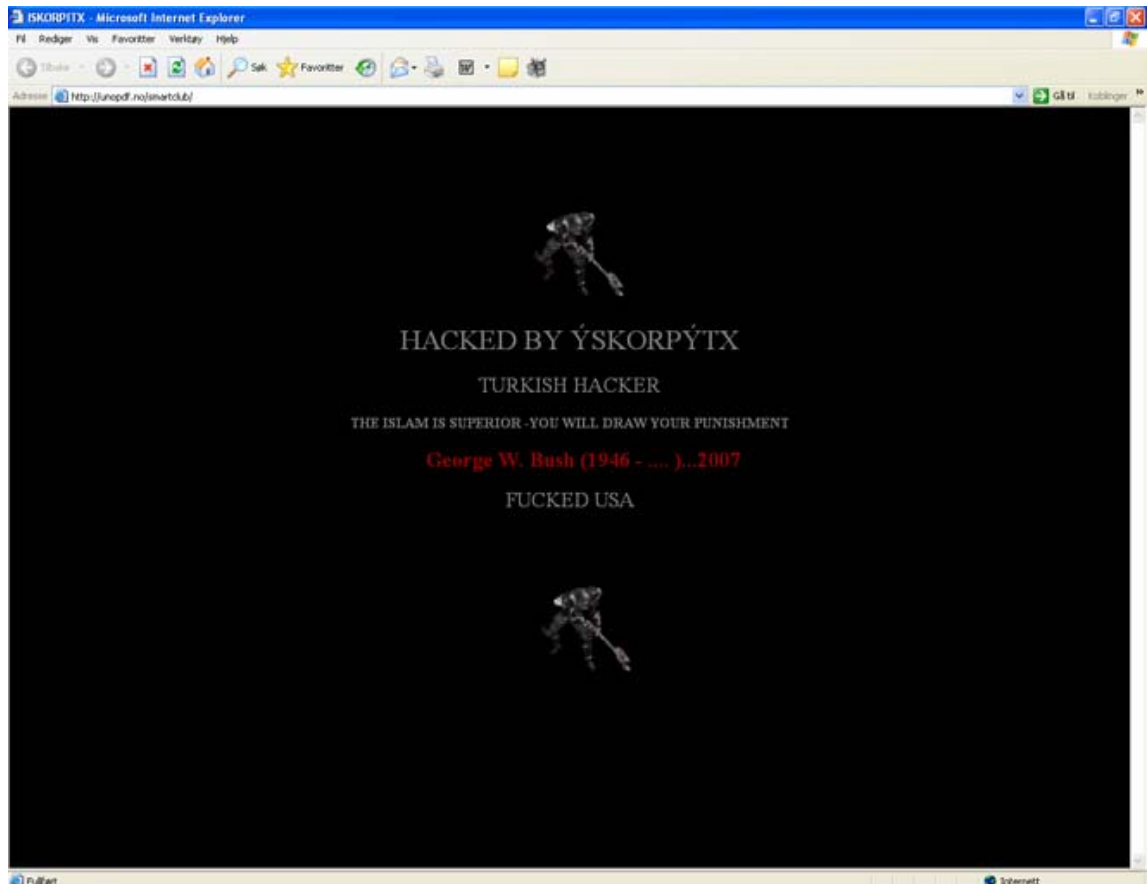
In addition to this, a new definition, called cyber terror support, has arisen. This includes use of information systems, which is not meant to have an enforcing effect on the targets, by terrorists. E.g. use of sniffer software to get information that later can be used in terrorist actions.

USE OF CYBER TERROR

Searching the Web for cyber terror, we find few examples on how this is used in practise. The only good example we found, was of hackers who have used cross-site scripting

against large amounts of web sites, to promote a point of view. E.g. a Turkish hacker called YSKOPYTX has hit several Norwegian sites, and given his/hers point of view on the US.

Below is an example of this towards the Norwegian Smart Club.



Some people may claim that since we do not see more cyber terror, it is likely that terrorists do not get full profit for this activity, but this does not mean that it will stay this way in the future. Since the society is getting more vulnerable to technical errors, the potential for cyber terror actions is continuously increasing.