

SECURITY THREATS AND TRENDS

MAY 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 once again shown a decreasing level. The level of traffic per day indicates that no new vulnerabilities have been released. Searches towards the service SSC-Agent have decrease again, while we see more spam and worm traffic this period.

No new trends have been detected this month.

The 'Focus of the Month' in this issue covers mobile security.

TABLE OF CONTENTS

INTRODUCTION	3
THREAT LEVEL.....	4
RECONNAISSANCE ATTACKS APRIL 2007	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 – MOBILE SECURITY	10
MOBILE THREATS	10
TEN SECURITY ADVISES.....	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.

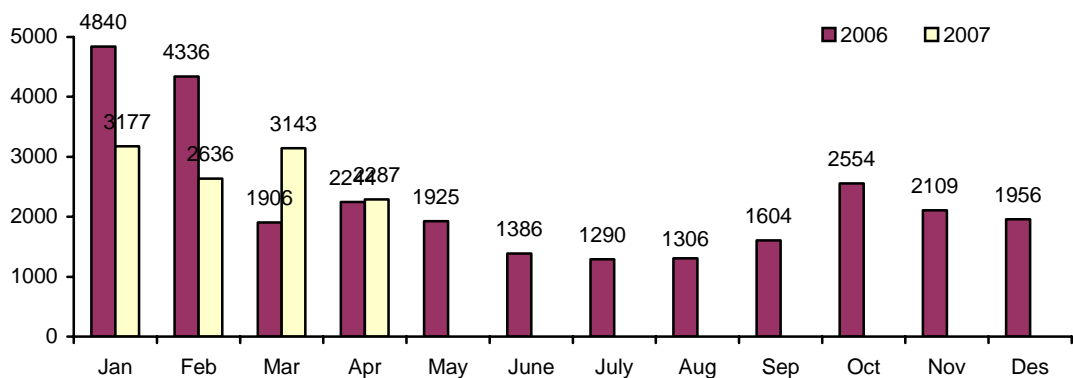
THREAT LEVEL

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.

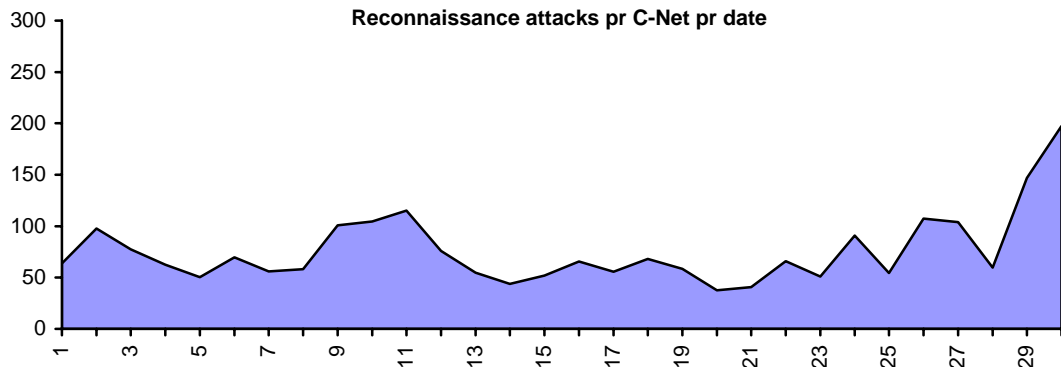
RECONNAISSANCE ATTACKS APRIL 2007

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

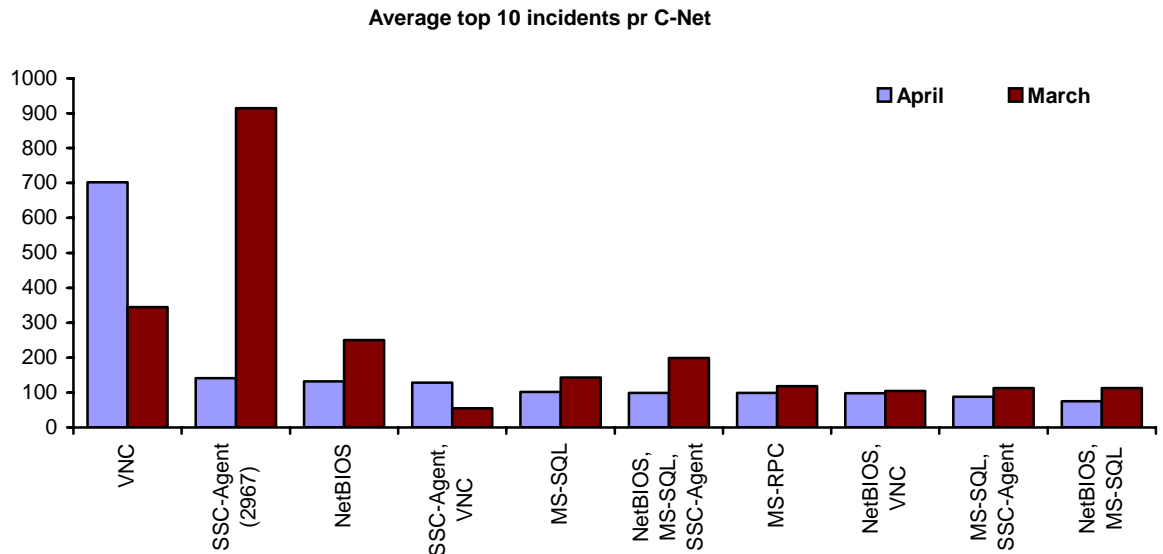


There has been a decrease in the total number of reconnaissance attacks from March to April. The traffic is widely spread over all days of the month, with no peeks, which is a good indication that no new vulnerabilities have been released. The level of traffic is quite variable, so it is not unusual that the level is now lower than last month.

There are no special attacks behind these numbers.

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.



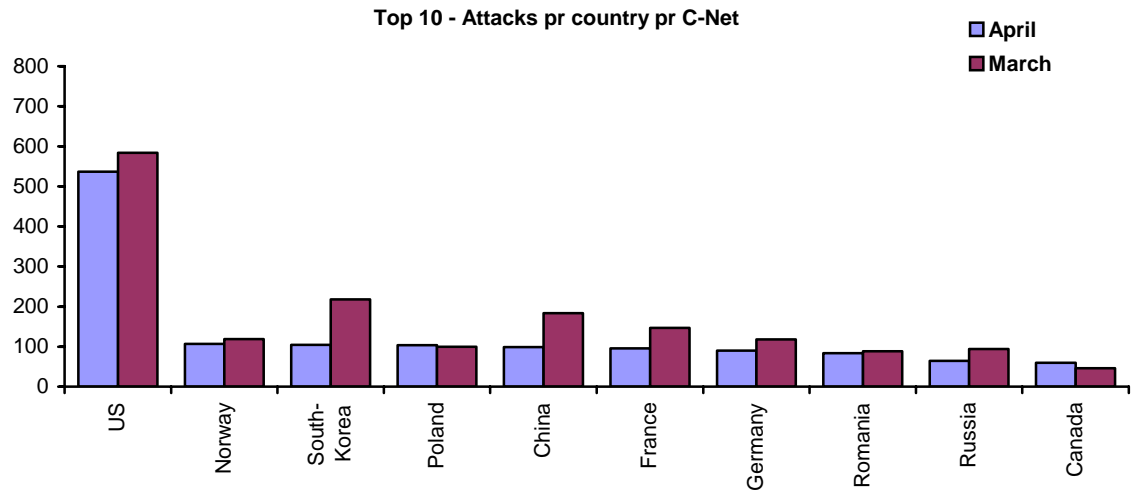
Scans for tcp port 2967 (Symantec AV) has once more relapsed during this period, while scans towards VNC has increased. As mentioned earlier, there is lots of variety in the level of traffic.

Scans for tcp port 2968 (ENPP, used by Symantec), which was on the top ten list last period, is once again decreased and is out of the list.

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 originates from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed.

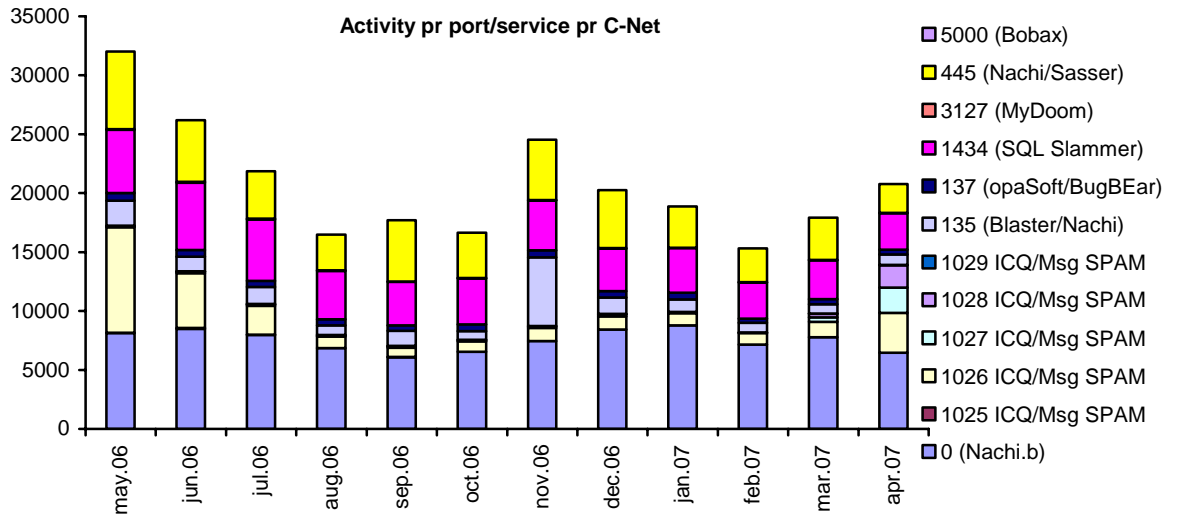


As in earlier periods, the US is the most aggressive source of reconnaissance attacks, but there has been a slight reduction this month as well as last month. Romania is still at the Top 10 list after the country entered it last month. Traffic from all countries is observed towards several of our customers, so there is no particular attack behind the statistic above.

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

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 this month differs from the latest periods. First of all the increasing trend continues this month. Secondly, we see an increase in activity against port 1026, 1027 and 1028 (Messenger spam ports). However, we can not connect this increase to new vulnerabilities or a certain attack method.

ALERT STATISTIC

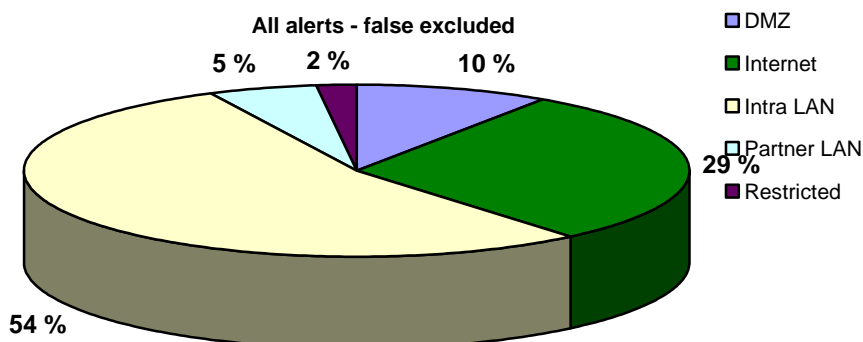
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

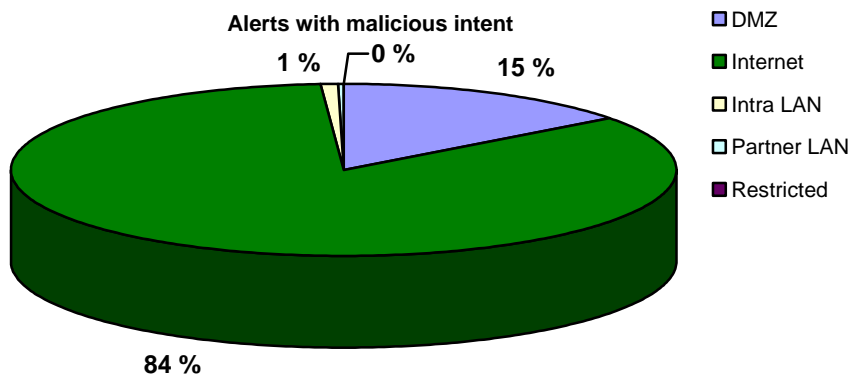
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

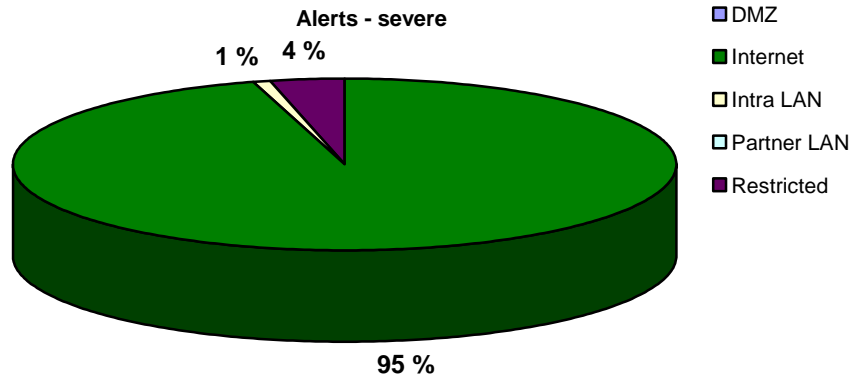
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



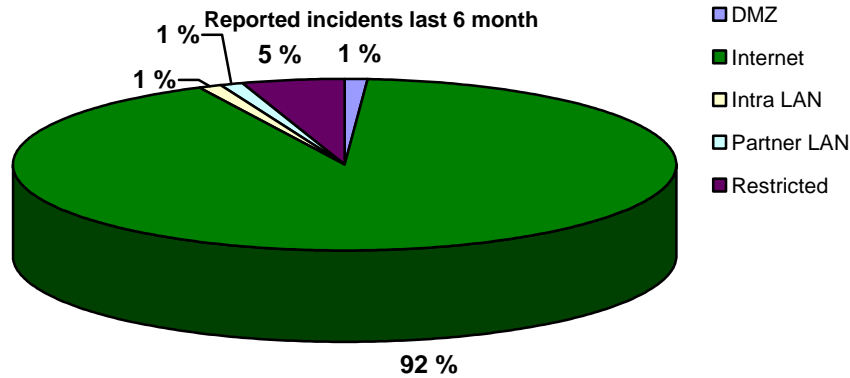
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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 – MOBILE SECURITY

Mobile security will normally include mobile phones, PDA, laptops and so on. In this article we will mainly focus on mobile phone security, because it is mostly in that area we see new development and new threats on a daily basis.

As our mobile phones become smarter, the security threats become bigger. We now store a huge amount of sensitive information on the mobile phone. It is almost as much sensitive information stored on a mobile phone as we find on a laptop, and this offers new challenges. The area of mobile security is bigger than we can grasp in this article, but we will scratch the surface to help you focus.

MOBILE THREATS

Threats against a mobile phone is similar to the threats of a laptop, which again is similar to the threats of a desktop PC. In other words, viruses, Trojans, hackers and so on could be a threat to a mobile phone as well as for a computer. However, there is one threat that is greater for a mobile phone than a computer, and that is the threat of physical access. As you may know, a mobile phone, PDA or laptop is carried with you, and that makes the physical security dynamic and difficult. Further, a mobile phone or PDA is easier to steal than other technical devices, because it is so small. A criminal may take it from you without your notice.

In addition there are some threats to a mobile phone that are not given enough attention. That is the ability to track or eavesdrop a device. It is not that difficult to tap a signal from a mobile phone communication. You only need some simple devices available for a small amount of money. Tracking the signal is as easy as taping the signal.

In latter time mobile phones are delivered with operating systems like Symbian and Windows Mobile. The included operating systems have support for several programs which again can be used to edit documents, spreadsheets, presentations and so on. There are also several Internet browser and e-mail clients developed for mobile phones at this point. In other words, the mobile phone is often used as a mini-computer, and files are transferred between the computer and the mobile phone. This interaction makes security issues more important than ever.

TEN SECURITY ADVISES

The area of mobile security is, as mentioned earlier, large. We could have written a thesis on the subject, but instead we will take a shallow look on most of the security aspects. This is best done by giving some security advises as we will here.

1. Guard your mobile phone like you would your wallet.

The physical access to a mobile phone is the most likely way to get information from it. If someone borrows your mobile phone for example, just think how much information they can gather from it. When you let someone borrow your mobile phone you have some indication on what information they gather, but just think how much information they can gather if they steal your phone. That leads me to advise 2.

2. Use password protection on your phone.

If your phone is turned on when it is stolen this will only help if you password protect files and services on your mobile phone. However, all password protection is better than no protection, so we strongly recommend that you password protect as much as you see fit at your mobile.

3. Data encryption

Data encryption is a higher level of "password protection". If you encrypt your files on your mobile phone it is difficult for others to access your data. The idea behind it is that if you

make it difficult to retrieve data in human readable form, it is less likely that the data will be retrieved.

4. Removable storage

This is actually an advice that has been introduced for PDA security, but it may be used for mobile phones too. If your mobile phone has the ability to store data at a removable memory card, you should store data (sensitive data and backups of other data) on this memory card. This card may then be located on a secure location while you are travelling, or you may use it to keep your phone and your data at separate location for a short amount of time.

5. Careful use

This is like telling someone that you should not do something stupid like giving your credit card to a criminal. The problem is that mobile devices are easy to eavesdrop, so you should not give away to sensitive information on the mobile phone. However, this is very difficult because mobile phones have become one of our main communication channels. Some restrictions around use are possible to follow though. First, do not give out sensitive information if you are afraid of misuse, and secondly, do not forget the people around you when you talk in your mobile phone. It is easy for people standing close by to listen to your conversation, and they may even hear what the other person is saying.

6. Software protection

It is likely that you would protect your laptop with one or several software programs, like antivirus and firewall. You should do the same thing with your mobile phone, because this has now become a mini-computer. There are several programs for use on mobile phones, and some vendors give you a full package similar to the "Internet security" package you would install on your computer.

7. Wireless security

Most mobile phones are delivered with some kind of wireless access option. This may be Bluetooth or Wi-Fi. You should always secure this as good as possible, and hopefully at the same level you would protect your laptop. Check your mobile phone for possibilities to secure this feature. You should not use access points that you do not know is probably secured either.

8. Disable Bluetooth and Wi-Fi

When you are not using it, disable it! You never know who is seeking out devices.

9. Monitor and Detection Software

If it is possible on your mobile phone, some monitoring and detection of activity on your device should be installed. This can let you know if someone is trying to access programs on your mobile phone.

10. Use e-mail wisely

The same rules that apply for an e-mail client on a computer should apply here. Do not open e-mails from people you do not know, and do not open attachments if you are not sure what the file content is. Remember that it may be easier to gather information from a mobile phone than other devices, so be careful to download e-mails with sensitive information to your mobile phone if it is not encrypted.