

SECURITY THREATS AND TRENDS

JUNE 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

In this period there has been a slight increase in the total number of reconnaissance attacks. Especially we see an increase towards MySQL, which we unfortunately can not relate to any known vulnerabilities or attacks at this moment. Further, we see a marked decrease in the number of searches for Norway, in comparison with what we have seen earlier.

The 'Focus of the Month' in this issue covers new spam and Trojan trends on the Internet.

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 – NEW TRENDS	10
MEDIA PLAYERS.....	10
YOUTUBE TROJANS.....	10
SKYPE TROJANS	10
SPAM	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.

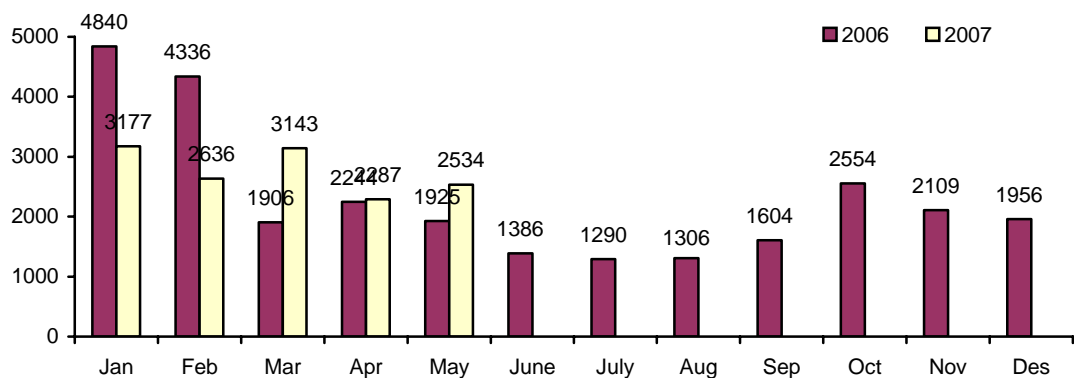
THREAT LEVEL

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.

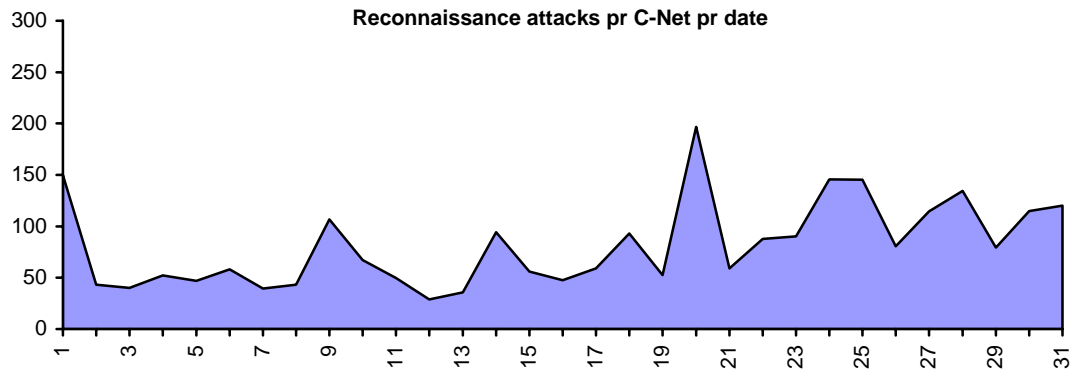
RECONNAISSANCE ATTACKS APRIL 2007

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

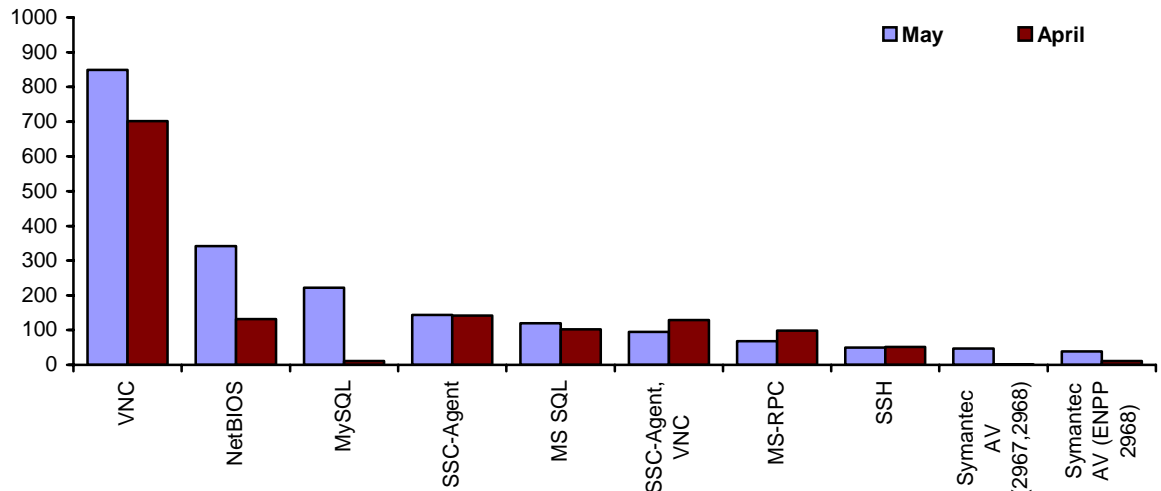


There has been an increase in the total number of reconnaissance attacks from April to May. There are no special attacks behind the peaks we see, but rather increased general traffic on the Internet. We have during the last months seen a more uniform distribution, and no distinct attacks running over a short amount of time.

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

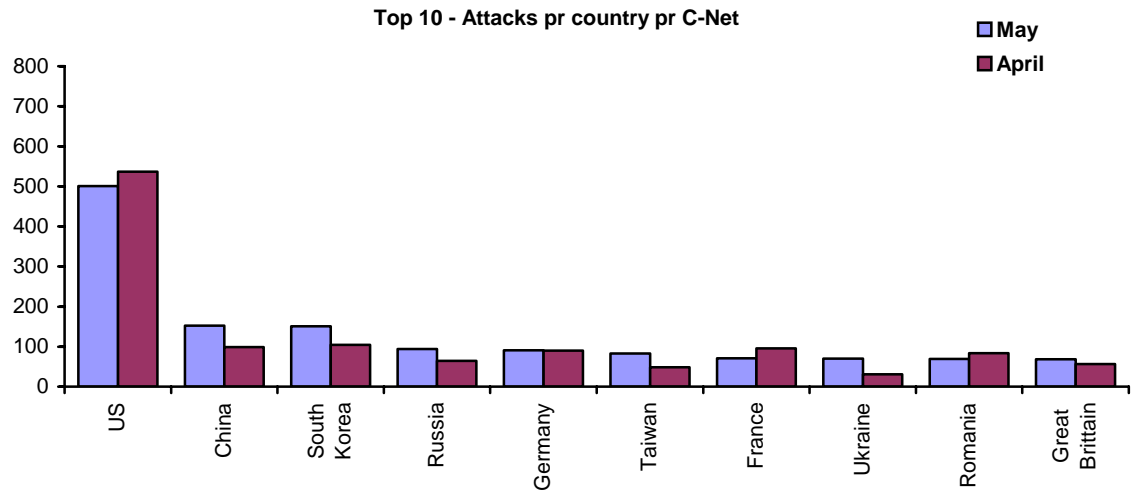


Scans for tcp port 2967 (Symantec AV) have now stabilised. We only see small differences in searches towards port 2967 in combination with other ports, while searches towards the port alone has kept pretty stable. Further we see an increase in searches towards VNC and NetBIOS. The biggest increase, however, we see towards tcp port 3306 (MySQL). It is for now not registered any worm or vulnerability which can be the source of this increase. However, in middle of May this increase has been registered by other companies as well.

With exception from searches towards MySQL, all services have been on the top 10 list during the last months.

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.



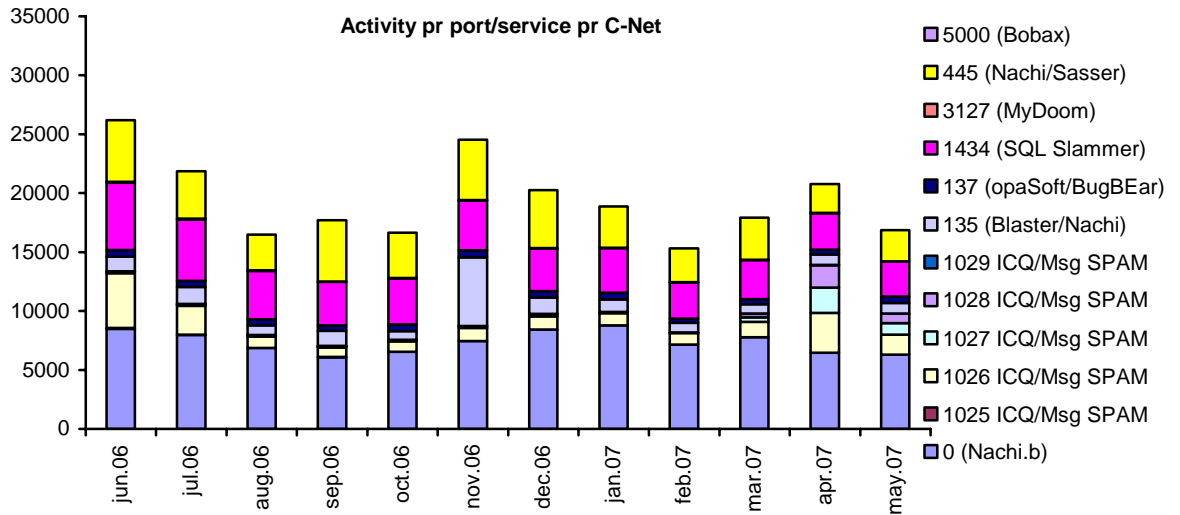
The reduction in searches from the US continues this month, as we have seen the last to-three months. Romania, which lately entered the list, has had a slight decrease this month, while we see an increase from Ukraine. Generally we see more traffic from East-European countries now than earlier. It is difficult to pinpoint the reason for this.

Our readers in Norway may also notice that Norway is out of the list this period. Norway is placed as number twelve, while we saw Norway at number two last month. This decrease may be due to the fact that we do not see any traffic towards MySQL, among others, from Norway at this point.

The US is this period followed by China 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.



Worm- and spam traffic have once again decreased. Especially traffic towards port 1026, 1027 and 1028 (Messenger spam) have been decreased, after we saw a relatively big increase last month. The other categories remain stable.

ALERT STATISTIC

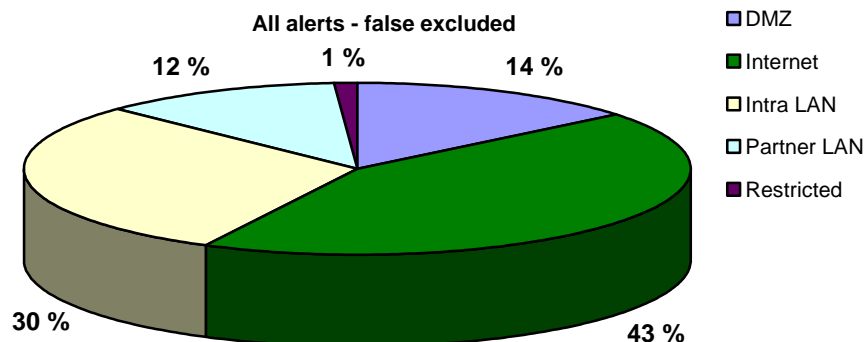
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

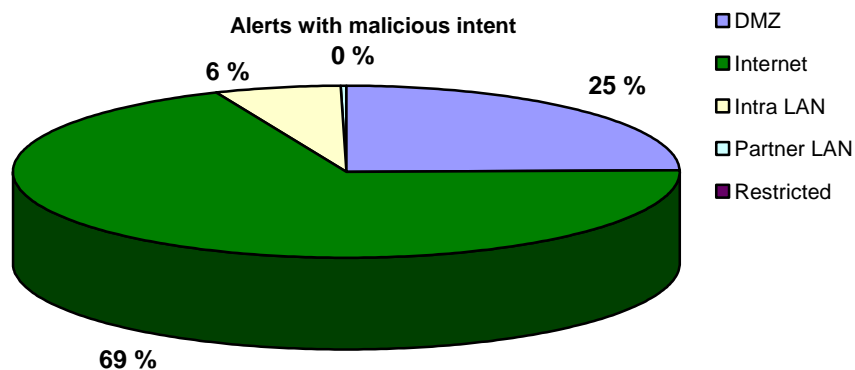
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

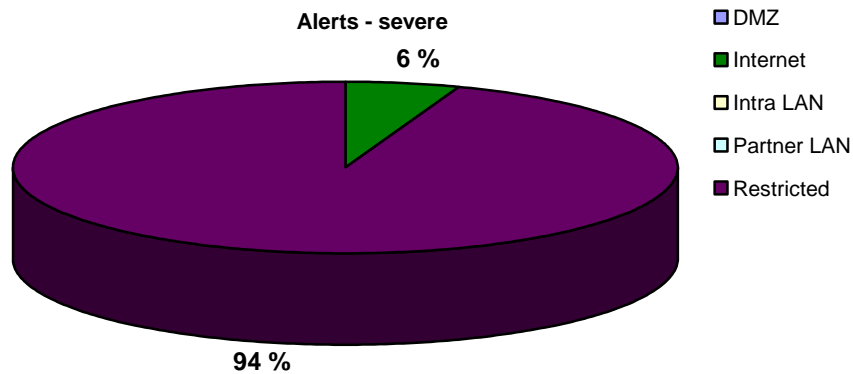
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



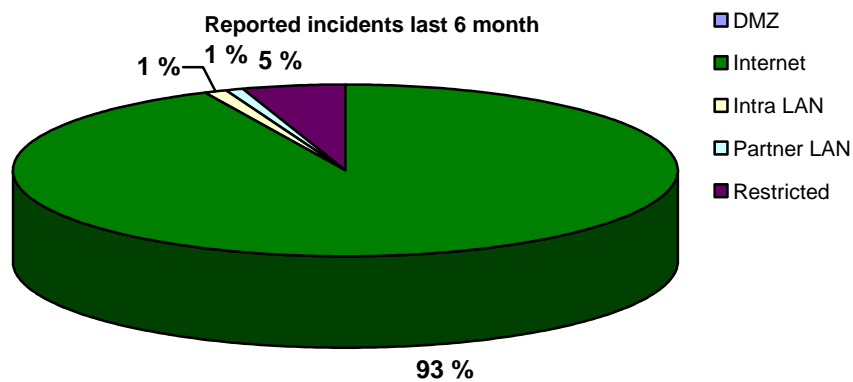
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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 – NEW TRENDS

The spreading of Trojans, spam and virus constantly finds new ways, and it becomes more and more difficult to reveal the new methods. In “Focus of the Month” we will look into these new ways to spread Trojans and spam. All methods described have surfaced during the last months.

MEDIA PLAYERS

So-called Bit Torrent clients including malware have surfaced lately. Torrent101, BitRoll, TorrentQ and GetTorrent are all examples on such clients. Lately it is registered that these kind of malware is spreading trough media players too. This happens in the following way.

1. The user downloads a movie, a TV show or similar from the Internet.
2. When the user tries to play the file, a message saying you have to have 3wPlayer to play the file appears (“This media file can only be played using 3wPlayer, that is completely FREE. Please visit playon.play3w.com to download.”)
3. The user downloads the player and gets malware with it.

This is the only kind of media player we have knowledge to at this point, spreading malware. This became known in late May, and it is therefore not unlikely that new programs of this kind will surface shortly.

YOUTUBE TROJANS

Websense registered only a few days ago a new way to spread crimeware through video clips on YouTube. Crimeware is small programs made to retrieve information which can be used to access online financial services. Some of the clips at YouTube will activate a Trojan, via a file called “YouTube04567”, which is loaded into the user’s computer. The Trojan will then copy information from the computer and transfers it to a remote server.

Earlier viruses and Trojans spreading through services like YouTube have been registered. These virus/Trojans is loaded as a so-called codec, which is “necessary” to play the files. This last Trojan registered on YouTube shows that new spreading methods are developed all the time, and that it only becomes more difficult to secure against this.

SKYPE TROJANS

Trojans spreading through Skype was first introduced in December 2006. After this new Skype Trojans has been registered many times, with some new features. Some of this Trojans exploit vulnerabilities in the Skype protocol, while others exploit user’s simple-mindedness and carelessness.

Mars 22nd a new Trojans was registered. This Trojan worked by giving the user a message marked “Check this up” and with a link to a website. On the website the user is requested to click on an executable file, which then will download and run malicious code. The code then spreads to other Skype users through the contact list on the computer.

Similar Trojans have also been seen in MSN, and the rule around this is clear: Do not click on any links in IM-messages if you are not 100% sure it is sent by someone you trust.

SPAM

At this moment one of the most discussed topics in IT news are spam. One of the reasons for this is an undergoing trial in the US, where it became known that the informant in the case made near to 40.000 dollar per week on spam. The defendant in the case, which pleaded guilty, had sent 1.27 million spam e-mails to AOL subscribers. The defendant have also spread spam in a large scale before he was caught for this, but there are no or few evidence for this and he his therefore not charged for it.

The battle against spam becomes more difficult every day that goes by, because the computers behind spam are getting more intelligent. While earlier the problem was biggest

for e-mail, we now see that free services on the Internet (forum, blog and so forth) are exposed more now. Internet-bots register false users, fills forums with spam-links or post spam-links as comments on blogs.

Earlier a solution to the problem would be to add a so-called CAPTCHA-block (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part). The problem with this solution is that in order to make them unreadable for computers the test must be so difficult that people would have problem with it too. In other words, the test must somehow “fool” the computer since it has not the ability to think by itself, it only does what it is thought to do. An example may be to use a simple intelligence question, where the answer could be one of several pictures.

Sadly, this is the area where it becomes clear; as long as the string-pullers make money the problem will not disappear.