

SECURITY THREATS AND TRENDS

JANUARY 2008



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 number of reconnaissance attacks is still at a low level. The three most searched services are http/alt. http, SSC-Agent and NetBIOS. A large part of the searches for http/alt. http originates from Norwegian addresses.

After an increase of spam and worm activity last month, this activity is now at a stable level.

Focus of the Month makes a summary of the most important attack trends in 2007, to try to determine what we have in prospect in the coming year.

TABLE OF CONTENTS

INTRODUCTION	4
THREAT LEVEL	5
RECONNAISSANCE ATTACKS DECEMBER 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 – A YEAR GONE BY, A YEAR AHEAD.....	11
ATTACK PATTERNS.....	11
WHAT ABOUT SECURITY?.....	11

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.

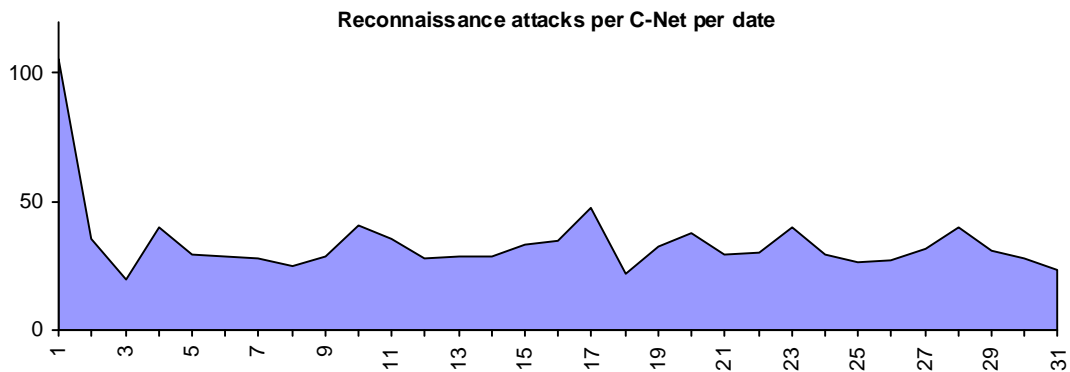
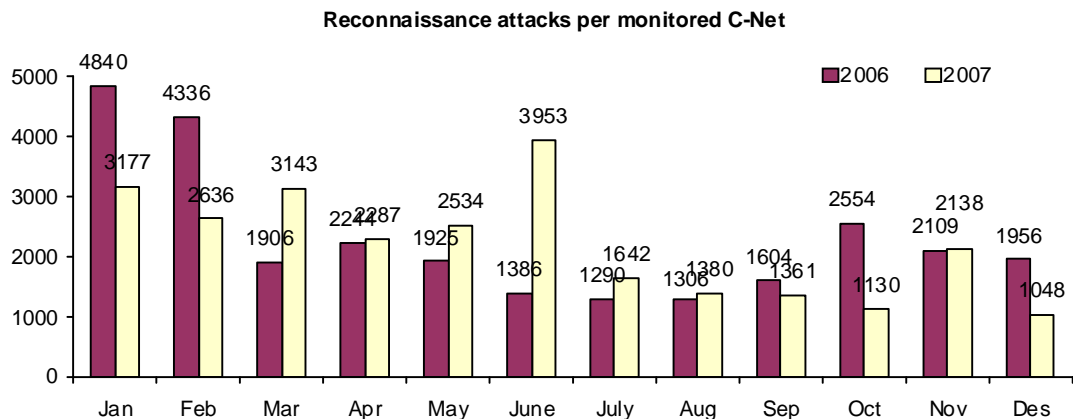
Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

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 DECEMBER 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.

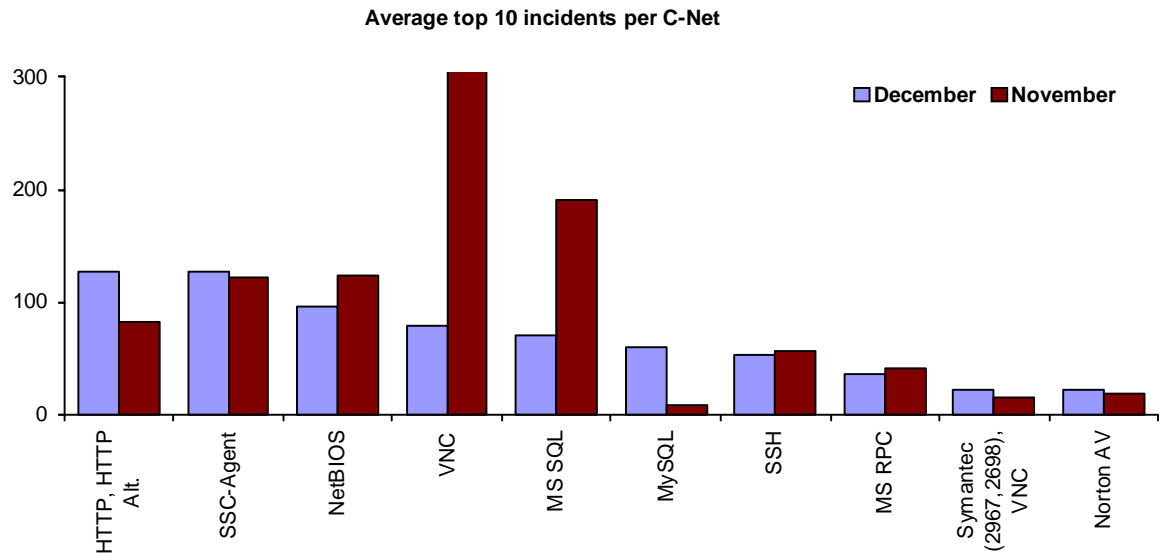


The trend shows that the number of reconnaissance attacks have stayed at a low level the last half-year. What 2007 concerns, it was recorded an activity top in June. This activity top was caused by several scans for MS SQL, something which probably was related to the launching of Microsoft's CTP (Community Technology Preview) version of SQL Server 2008 this month.

1st of December it was observed a distributed mapping attempt for Symantec Antivirus solution (SSC-Agent on port 2967), but besides this the activity has been at a stable level this month. It is normal that the traffic shows a decrease during the Christmas holiday when most people spend less time with their computers. This trend is also observed by Secode previous years.

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.

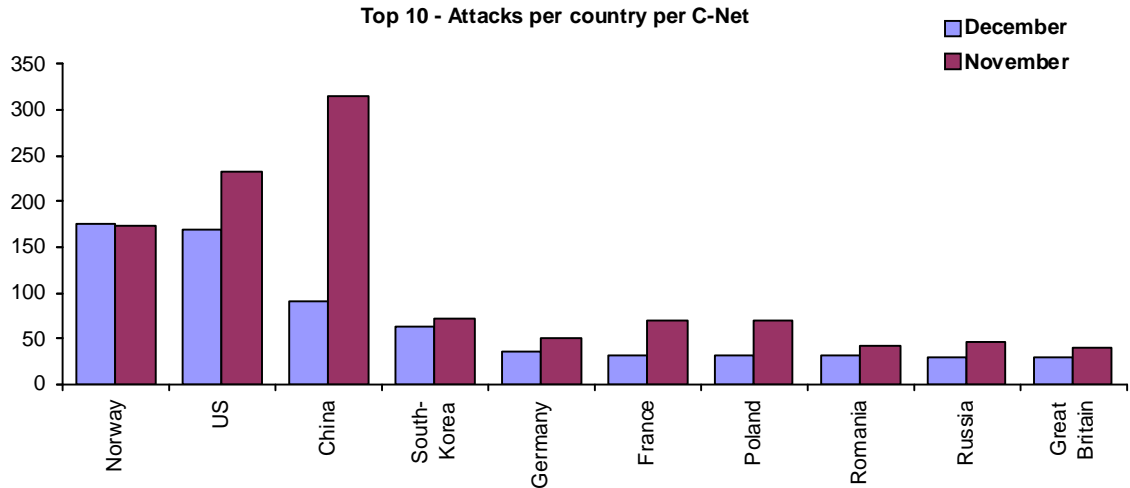


It is more or less the same services that have reoccurred at the Top 10 statistic the last months. For now, port scans for http and alt. http is the most frequent type of reconnaissance attack, followed closely by scans for Symantec Antivirus (SSC-Agent).

The dropping activity against the services VNC and MS SQL continues also throughout December. Scans for MySQL showed a slight, passing increase in the middle of the month.

RECONNAISSANCE ATTACKS PR COUNTRY

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

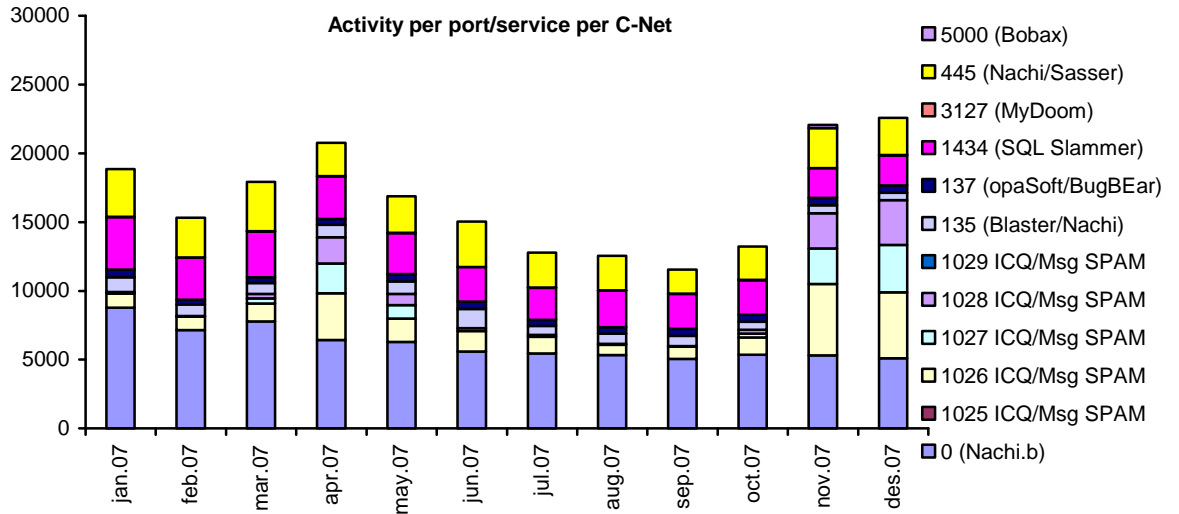


Norway is this month the most active source of reconnaissance attacks. A large part of the traffic from Norway is searches for port 80 and 8080 (http and alt. http).

Activity from the US and China has dropped during December, in accordance to the decrease in the total activity level.

INTERNET WORMS AND SPAM

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



Only minor changes are observed in spam and worm traffic this period. Besides ping, connection attempts against ICQ/Messenger (port 1027) are the most frequent type of worm activity.

ALERT STATISTIC

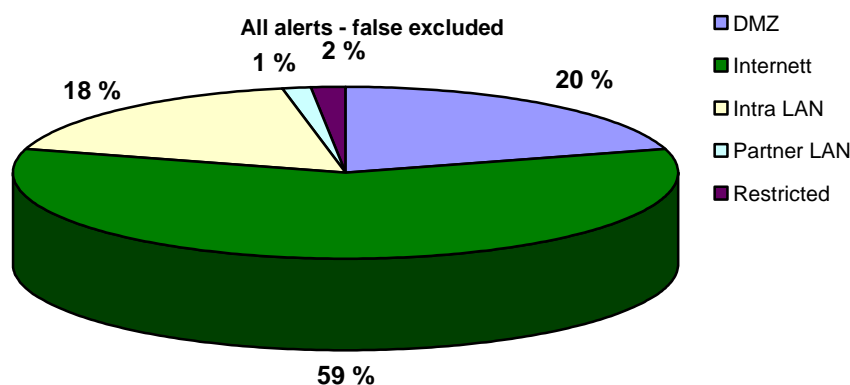
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

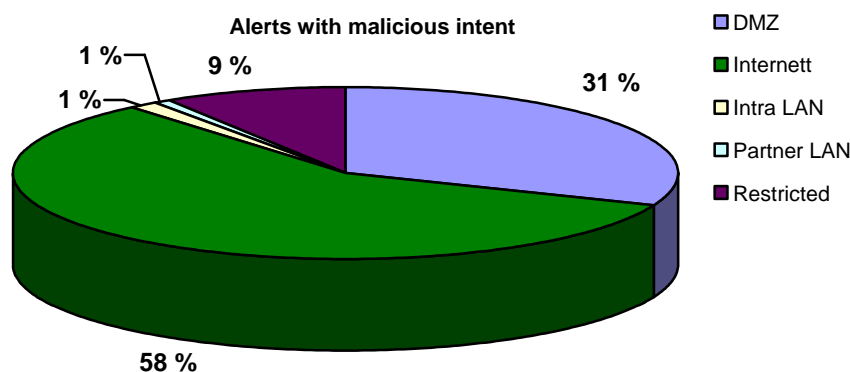
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

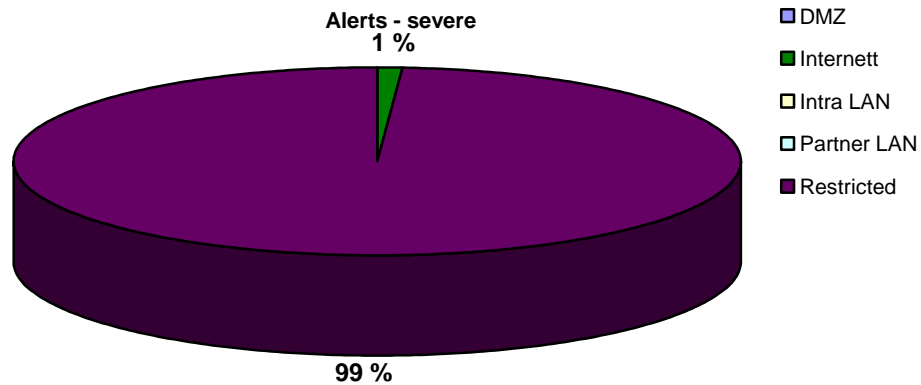
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



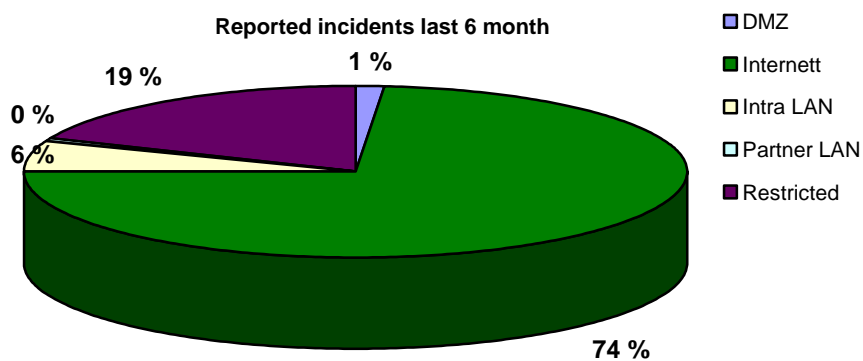
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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 – A YEAR GONE BY, A YEAR AHEAD

Trojans and phishing. Botnets, web attacks and spamming. These are all well-known terms that have made their impact on 2007, and which now are more important than ever.

ATTACK PATTERNS

There are much the same types of crime at the Internet as in the usual world; e.g. there are terrorism, vandalism, fraud and organized crime. A huge part of the Internet crime deal with economy, which influence the attack trends in the way that the attacks are getting more customized and directly targeted against organizations.

There are complete Trojans engines and virus writer kit for sale. Only a few changes are needed to get these to target a selected organization. For example, one Trojan engine alone can be adjusted to target several online banks. The criminal world is also hiring out botnets for spamming and for launching other large attacks. In other words; money is now by far the most controlling factor in e-crime, and there are no sign for this to decline.

If we look back at 2007 there are two attack trends that are especially distinctive, namely Trojans and phishing. Except this, there have also been botnets, Ddos attacks, web attacks and application attacks. None of these are to be considered as new, but the development of these threats has been huge the last year.

Example of successful attacks in 2007:

- January: The worm Storm is launched. This worm have built the largest botnet active at the Internet today
- February: The launching of a large Ddos attack against online game servers. 10 000 of users was affected
- June: A large, successful web attack against many of Italian web sites
- July: www.microsoft.uk.co was defaced by a SQL injection attack
- October: 4000 swedish sites was hacked by islamists
- September: The Trojan Mpack have infected half a million Internet users

...and more examples like this are expected in 2008. Trojans are expected to get more advanced and even harder to detect. At the same time Trojans will contribute to even more and larger botnets.

In 2007 we have also seen that attack through social networking sites as Facebook and MySpace have started. Such networks have become enormously popular, and have therefore formed a new channel for web attacks. Recently it was known that spyware was distributed through a Facebook application called Secret Crush. The users have been infected by downloading of what seemed to be a legitimate service. Because of the large popularity of such services, these types of attacks are believed to grow stronger in 2008.

WHAT ABOUT SECURITY?

Accordingly, Internet attacks are believed to become more and better in 2008. So what about security?

In a Nordic perspective, security has become a highly prioritized area. The last year we have seen several cases of severe and customized attacks towards Nordic organizations, something that in a high degree puts security at the agenda. Even though we can feel we are living in a small and relatively calm part of the world, we are still equally exposed to the same Internet crime as the rest of the world.

It is now a while since IPS started to be rolled out in the Northern as defend towards Internet threats, but Secode is now experiencing that organizations start to see the profits in using IPS as to address internal threats. Several of Secodes customers have in 2007 been hit by "good old fashion" worm infections that spread in the internal networks and created huge

problems and high costs. In such cases, IPS can do a great job in segmenting the network and prevent propagation.

Meanwhile as the security around external nodes are getting better, organizations are getting more mobile and opens more of their network for partners, something which makes virus- and worm threats still relevant. NAC(Network Access Control) is put to use by organizations that want better control of who connects to their network, such as consultants or employees with mobile units. A NAC scans units that connect to the net to determine whether they are fully patched etc., and can also isolate units that turn out to be infected.

A virus infection is usually easy to detect with security tools. However, this is not always the case with e.g. Trojans. Trojans investigated by Secode during the year, have turned out to be very advanced and sometimes almost invisible (e.g. Torpig). In such cases it is important with analysis competence and comprehension of the normal network traffic. It is also important to have the possibility to investigate traffic subsequently to find deviating patterns (e.g. IDS and logs).