

SECURITY THREATS AND TRENDS

JANUARY 2007

SECODE AB

Secode AB was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In year 2000, Secode started its 24/7 Managed Security Services and Security Consulting in Sweden. 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. Today, Secode helps many customers in private and public sectors, from five 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 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 the two areas: 24/7 Managed Security Services and Security Consulting.

SUMMARY

The total number of reconnaissance attacks has decreased slightly during December. At the end of the month, a new vulnerability in Symantec Antivirus and Firewall software was published resulting in a sudden rise in scans for this service.

The “Focus of the Month” gives a summary of the most usual attack trends in 2006.

TABLE OF CONTENTS

1. INTRODUCTION	3
2. THREAT LEVEL	4
RECONNAISSANCE ATTACKS DECEMBER 2006	4
TYPE OF RECONNAISSANCE ATTACKS	5
RECONNAISSANCE ATTACKS PR COUNTRY.....	6
INTERNET WORMS AND SPAM.....	6
3. ALERT STATISTIC	7
REPORTED INCIDENTS.....	8
4. FOCUS OF THE MONTH – ATTACK TRENDS IN 2006	9
PATH OF ATTACKS.....	9
BUG-A-DAY PROJECTS.....	10

1. INTRODUCTION

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

Threat level is a presentation of various threats that organizations are exposed to when connected to Internet. In this threat evaluation, reconnaissance attacks from the Internet towards 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. In such cases the alerts will be transferred to 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 that focuses on relevant topics within IT Security. For example topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

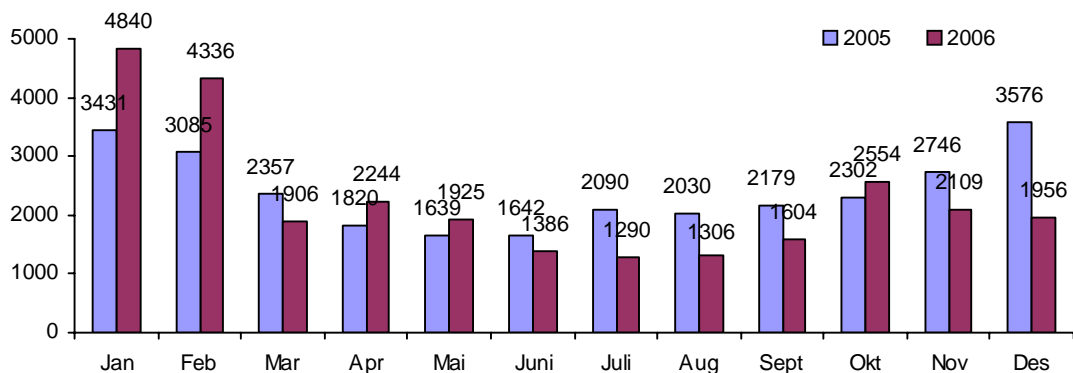
2. THREAT LEVEL

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.

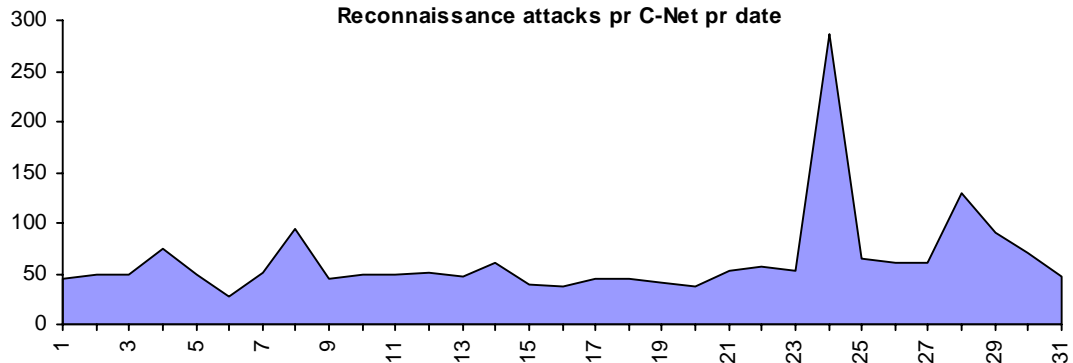
RECONNAISSANCE ATTACKS DECEMBER 2006

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



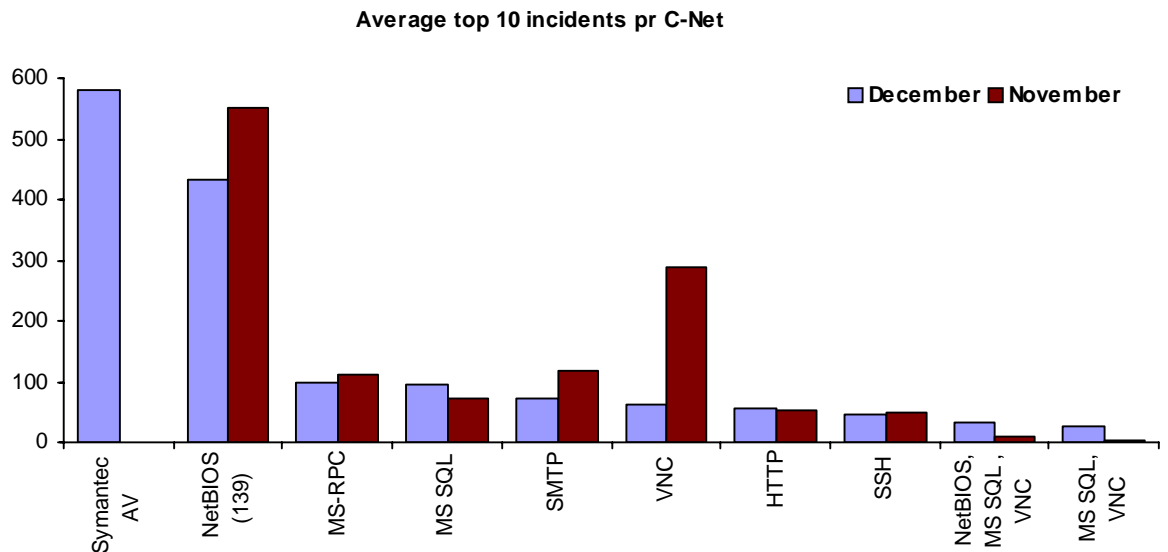
Reconnaissance attacks pr C-Net pr date



The total number of reconnaissance attacks has shown a small decrease during December. It is quite normal to see a reduction in malicious activity during the Christmas holiday, something that probably is related to the fact that many are on vacation from work and school, resulting in less people using their computers. In 2006 there is on the other hand observed an increase at the end of the month. This increase is caused by several reconnaissance attacks related to the publishing of new vulnerabilities.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months, regardless if the scan targets are a single service or several services.

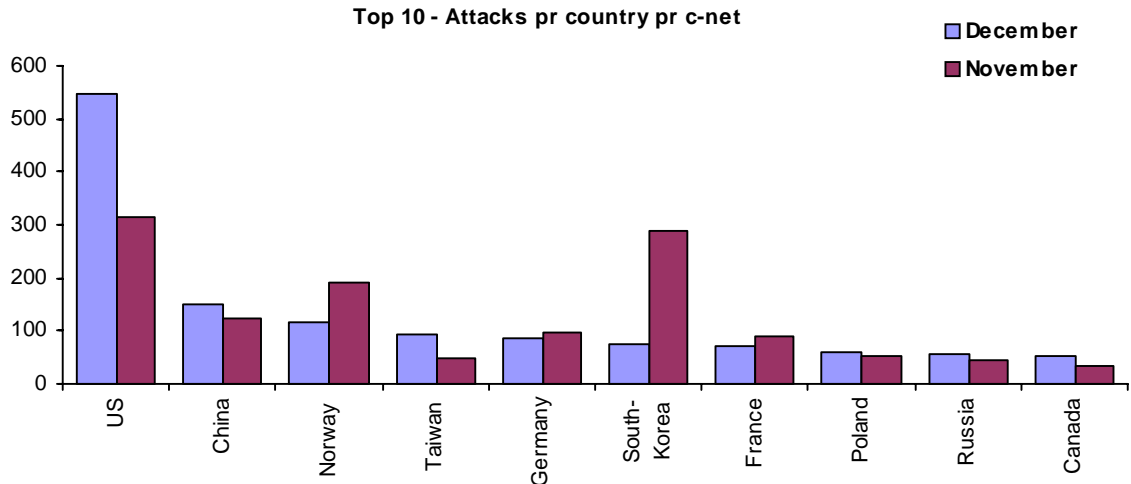


Towards the end of December Secode has observed a significant increase in scans for tcp port 2967. This port is used by Symantec Antivirus and Firewall software. Several vulnerabilities were published in these products late in December, and shortly afterwards, exploit code was available at the Internet. It also seems to be a worm out in the wild making scans towards port 2967, but the spread of this worm is limited, and so far it does not seem as the worm will increase in wide extent.

Otherwise it has not been any large changes in most common reconnaissance attacks. The NetBIOS Session Service is still frequently attacked, while the other services remain at a much lower level.

RECONNAISSANCE ATTACKS PR COUNTRY

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

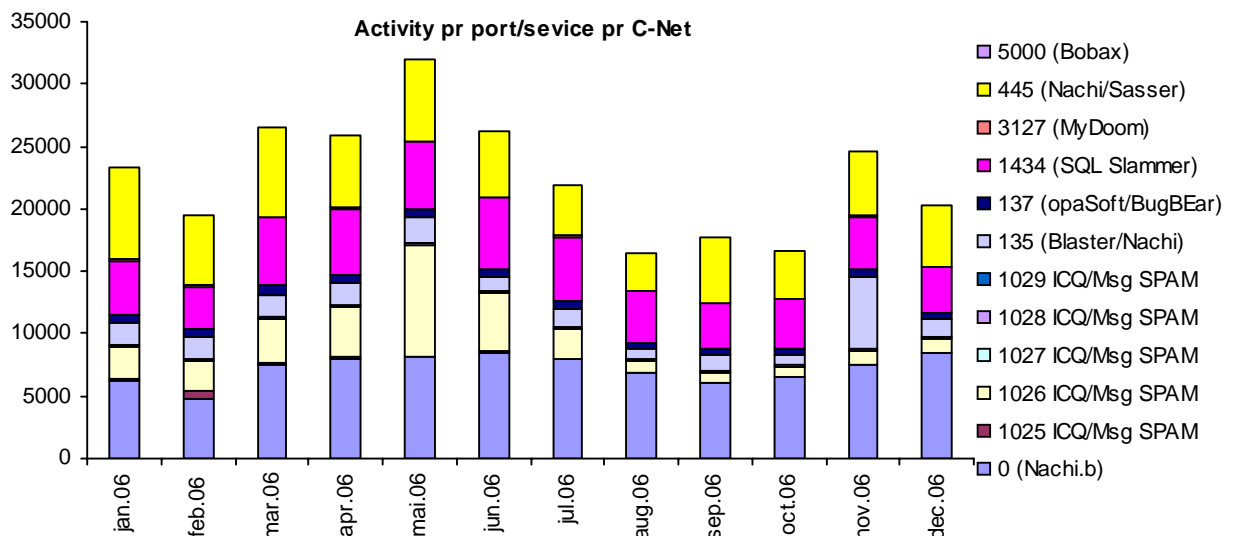


The US is still the most aggressive source of reconnaissance attacks, this month followed by China and Norway.

As observed also previous month, the decreasing activity from South-Korea continues out December.

INTERNET WORMS AND SPAM

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



As for the rest of the malicious activity, worm activity has also decreased the last month. It is still Microsoft-ds and Microsoft SQL server which are most frequently attacked by worms.

3. ALERT STATISTIC

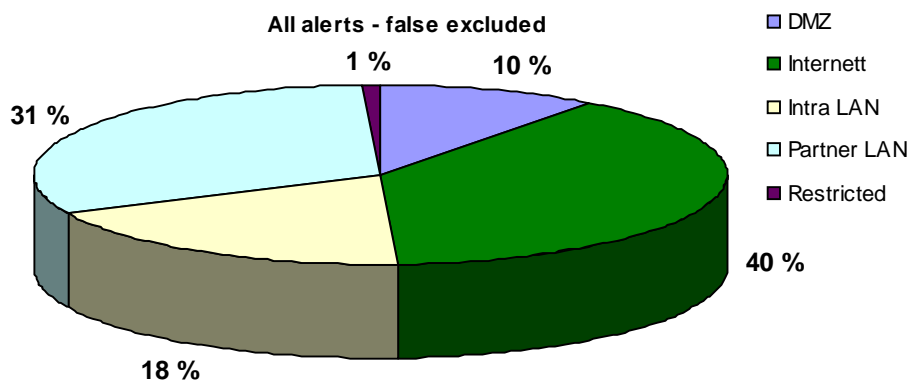
This chapter summarizes of alerts from IDS/IPS sensors. All alerts are analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment under surveillance.

HANDLED ALERTS

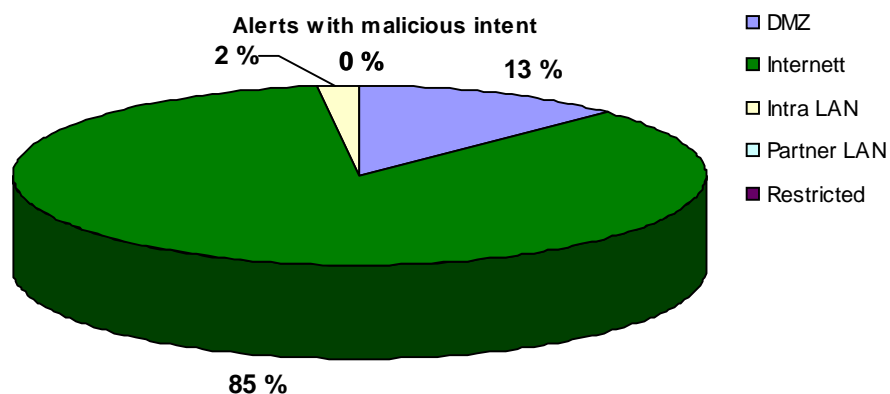
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are placed.

The network segments are divided into the following:

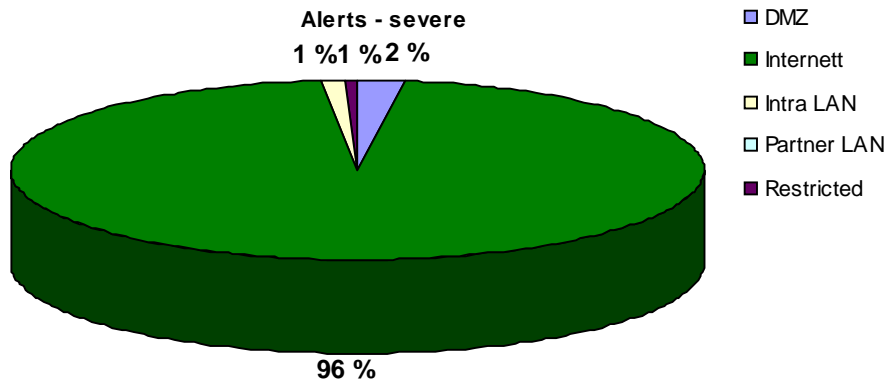
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is placed inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is placed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



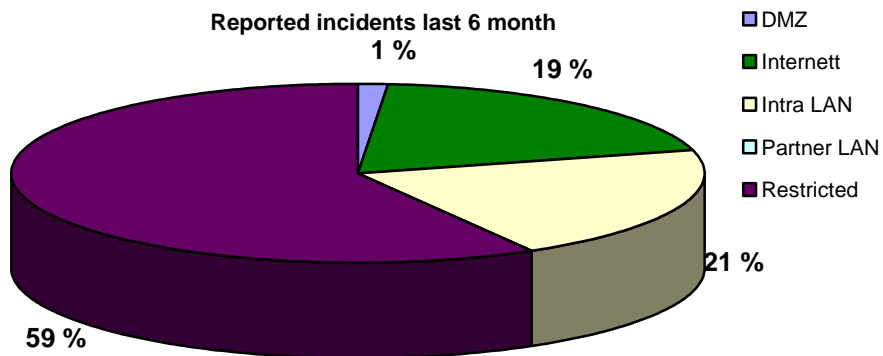
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



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.



4. FOCUS OF THE MONTH – ATTACK TRENDS IN 2006

Over the last year we have seen a development of the attack pattern, in the sense of new attack vectors and a development of the existing paths of attack. Organizations have now more units to protect, as for example PDA units, wireless access, mobile phones, etc. All together, this provides hackers an increasing number of attack targets and more complex interfaces to attack.

During 2006 there has been an increase in client-side attacks as exploits in web browsers, e-mail clients and in particular Office applications. Office files are popular attack vectors because such files are often not blocked by any security mechanisms and users are allowed to download and open these files. An infected Office document is therefore a natural way to attack as there is a great chance that it will reach the end user unmodified by security mechanisms.

Secode is of the opinion that both organizations and private persons in general have become more aware of security issues. This is reflected by the fact of limited worm and virus propagation in 2006.

As a security effort, some organizations are moving away from Microsoft products. But as a countermeasure, so does the attackers.

PATH OF ATTACKS

Phishing is by now a well-known phenomenon, but in 2006 there has been a significant improvement in the way these attacks are carried out. Phishing is a combination of social engineering and technical attacks, with an eye to lure people and unjustified get hold on their personal data. Phishing attacks basically consist of fooling people to visit a bogus website that pass itself off as for example an Internet banking service. Fooling people to visit the website can be performed by a spoofed e-mail, a false link or through DNS hijacking or poisoning. The claim regarding the improvement of phishing attacks during 2006 are based on the fact that the both the spoofed e-mail and bogus website now are improved in the way they are created. Phishing are also getting more targeted by objectives, meaning that the spoofed emails are not necessary spammed out to millions of people, but are sent to few targets.

The statistic below shows phishing reports in the period from Oct. 05 to Oct. 06



Source: www.antiphishing.org

Denial-of-Service (DoS) attacks make a significant and severe threat to organizations that are depended on their Internet availability. Attackers are now in possession of large resources, mainly in form of bandwidth and a high number of infected computers world-wide. These resources make them capable to damage/take down large net segments. DoS

attacks are hard to protect from. During 2006 it has been reported of several cases where large organizations are made unavailable because of a DoS attack. These attacks have hit organizations all over the world, included organization in Norway and Sweden.

A DoS attack can simply consist of a large number of computers making simultaneous connections toward a website. If the web server can't handle this large amount of traffic, it may crash.

Trojans have become a major concern for organizations in 2006. This doesn't apply to those Trojans that are mass-mailed out to millions of computer users, but rather the few special adjusted Trojans. Such special adjusted Trojans may e.g. install keystroke loggers and open the compromised system for remote access. The purpose of such Trojans is mainly industrial espionage and financial motivated crime. Security technology often detects attacks that arrives in large scales, but the small and specially crafted Trojans are harder to detect. When asked, organizations often point out these infrequently Trojans as one of their main concerns.

Zero-days attack is a term that frequently has appeared in media during 2006. As in earlier year, 2006 has also had its share of new vulnerabilities. Many have been rated as critical, and some have been a part of zero-days attacks, meaning that the vulnerability is exploited before a patch is available.

One example of this type of attack was the VML vulnerability (in Internet Explorer) which was highly exploited for quite long before a patch was made available. At the end of December another zero-day attack got focus, this time for exploiting an unpatched vulnerability in Word. Microsoft has as usual been under a lot of attacks, but also Apple has experienced exploits of vulnerabilities for which there are no patches.

Zero-day attacks are hard to detect with signature based surveillance technologies because an attack has to be discovered at least one time to make the security supplier able to create a suitable signature.

The increase in zero-days attack in 2006 can somewhat be related to the fact that it is now easier to discover vulnerabilities by use of *fuzzing tools* (software testing tool). Such fuzzing tools have also been used in the last half-year's much mentioned *Bug-A-Day projects*.

BUG-A-DAY PROJECTS

Bug-A-Day projects aim to release new unknown vulnerability on daily basis for a given period of time. In July we described the Browserfun project, which for each day in a week published exploit code for unpatched vulnerabilities in different browsers. Similar we have seen Month of Kernel Bugs, which released a kernel vulnerability each day for a whole month.

Year 2007 has also started off with a Bug-A-Day project, this time with the claim to daily publish an exploit for a new vulnerability in Apple.

The purpose of Bug-A-Day projects is to set focus on vulnerable software. Apparently the men behind the projects partly do it as a protest against the software suppliers' ignorance to security holes.

As a result of the publishing of vulnerability exploits, there has also been an increase in attacks against the current products. Similar, due to the new Bug-A-Day project, Secode expect to see a rise in attacks towards different Apple products in the near future.