

# SECURITY THREATS AND TRENDS DECEMBER 2006

## 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 two areas: 24/7 Managed Security Services and Security Consulting.

## TABLE OF CONTENTS

<b>1. IDS – SECURITY THREATS AND TRENDS.....</b>	<b>3</b>
SUMMARY .....	3
IDS – INTRUSION DETECTION SYSTEM .....	3
BASIS .....	3
<b>2. THREAT LEVEL.....</b>	<b>4</b>
RECONNAISSANCE ATTACKS NOVEMBER 2006 .....	4
INTERNET WORMS AND SPAM .....	5
TYPE OF RECONNAISSANCE ATTACKS .....	5
RECONNAISSANCE ATTACKS PR COUNTRY .....	6
<b>3. FOCUS OF THE MONTH – BLOGGING SECURITY.....</b>	<b>7</b>
THE POSITIVE SIDES .....	7
THE NEGATIVE SIDES .....	7
USERS RESPONSIBILITY .....	8
CONCLUSION .....	8
SOURCES OF INFORMATION .....	9

# 1. IDS – SECURITY THREATS AND TRENDS

---

## **SUMMARY**

This month there have been registered a decrease in the total level of reconnaissance attacks. The traffic is normal, with only some minor differences from earlier months.

The Focus of the Month looks at the usage of blogs. We debate some pros and cons for blog security. Blogging has become more popular everyday, and therefore we find this area interesting.

## **IDS – INTRUSION DETECTION SYSTEM**

The main purpose of IDS is to reveal and prevent intrusion attempts or abuse of an organization's IT-systems. To do this, Secode has placed out IDS sensors that measures and analyses activity to find attack from the Internet. IDS can be compared to a digital guard and alarm service, where a sensor is like a video camera or a movement sensor.

## **BASIS**

From our Security Operations Center in Arendal and Gothenburg, Secode offer 24/7 Managed Security Services that encompass real-time traffic analysis and maintenance to sustain each customers' specified level of security. Real-time traffic analysis is done by use of sensors placed outside and/or inside the customer's network. This report is based on data collected from sensors in our Norwegian customer's network. These sensors are placed in different IP-address segments, in different geographic sites. All data are made anonymously to protect the customer's confidentiality.

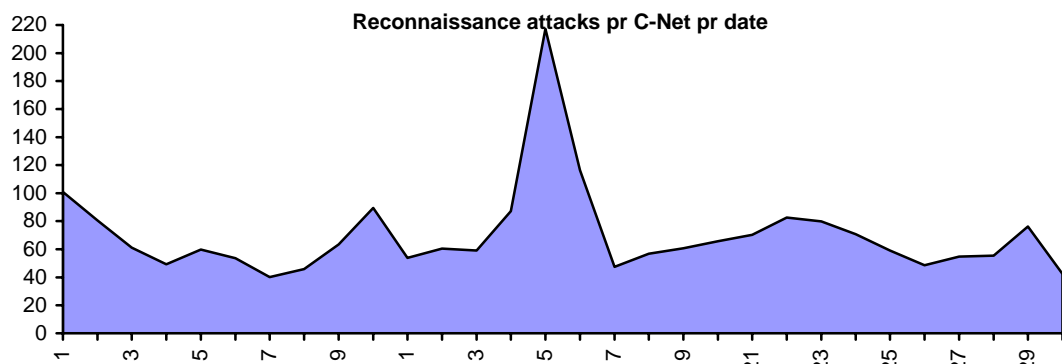
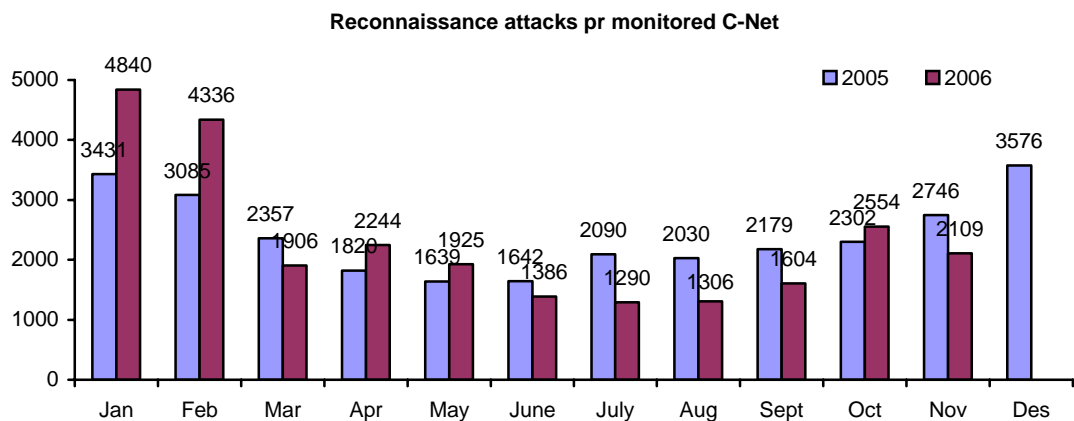
This report represents the normal threat picture, which all organizations that are connected to the Internet, are exposed to.

## 2. THREAT LEVEL

The evaluation of 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 Norwegian customers of Secode are analyzed and presented.

Reconnaissance attacks are searches for ports/services. Due to a high activity level traffic from Internet worms and spamming are handled in a separate chapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

### RECONNAISSANCE ATTACKS NOVEMBER 2006



The statistics above 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.

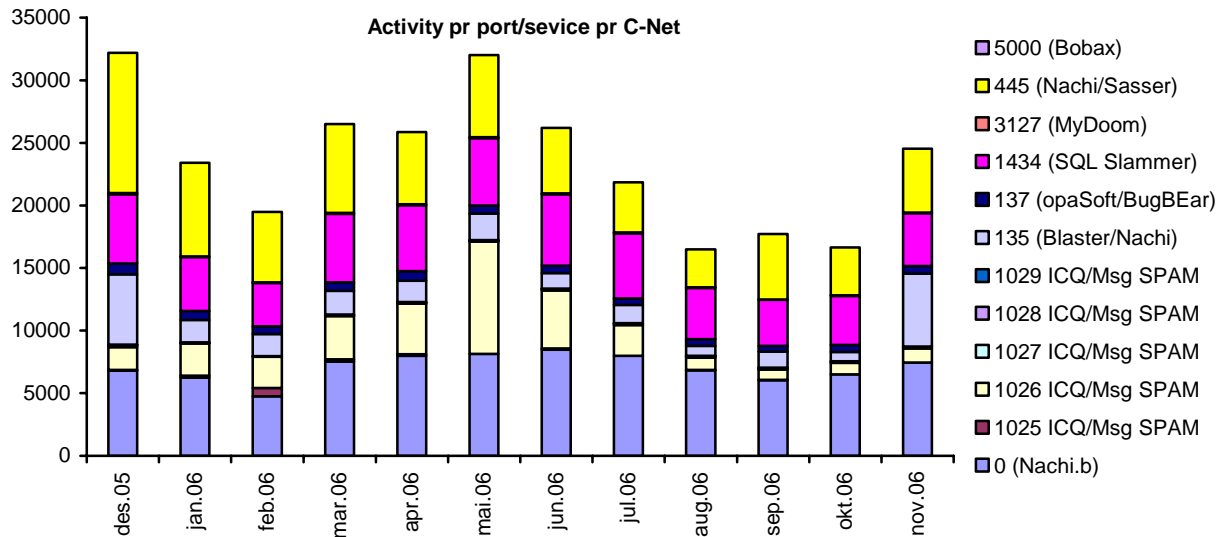
It is registered a decrease in the number of reconnaissance attacks this month. If we look at this in combination with the Internet worms and spam level, it seems like reconnaissance attacks are shadowed by the level of worms and spam. However, the decreasing level of reconnaissance attacks may only be a normal variation in the traffic level. October is the only month since May which the level was higher than 2005, which may indicate that October was an exception of the trends we have seen this year.

The number of reconnaissance attacks is widely spread over each day of the month, but with some extra weight around the 15<sup>th</sup>. This is mostly due to searches against NetBIOS

(port 139) and MS-Streaming (port 1755), but does not seem to be a part of one specific attack.

## 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.

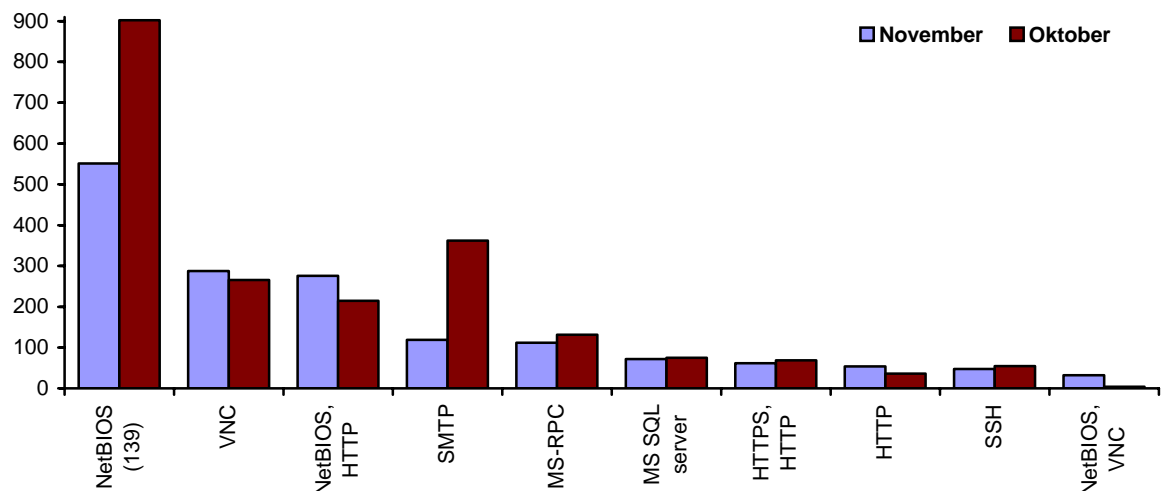


The number of spam and worms has increased this month, and are now, once again, at a fairly high level. Especially the Blaster/Nachi worm (port 135) has increased. The change in traffic is seen against all our customers, and is therefore not a part of an attack against one customer. Spam level have also increased, but this is probably just a normal variation in the traffic level.

## TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months.

Average top 10 incidents pr C-Net



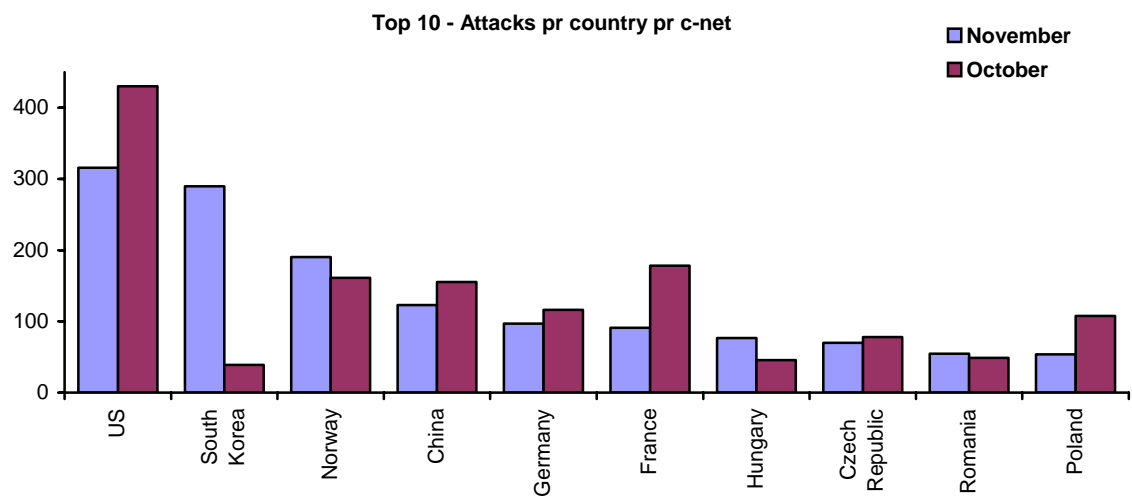
The statistic above shows the most common service scans that appear, whether it is scans for one single service or combined scans for several services.

It is registered a decrease in searches against NetBIOS (port 139) and SMTP (port 25) this period. Searches against these services will always differ from one month to another. In fact, these searches are mostly what define if there have been a high or a low level of reconnaissance attacks. As the total level decreased this month, searches against these services did to.

The other categories remain at a fairly stable level, with only minor differences.

No new special trends are registered this month. All services above have been on the Top 10 list before.

## RECONNAISSANCE ATTACKS PR COUNTRY



The malicious activity in the statistic above 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, but are rather a secondary effect.

South Korea is this month back at the top 10 list after the low amount of traffic last period. From the other countries there are registered either a decrease or a stable traffic level this period. Israel, which surprisingly entered the top 10 list last month, is out of the list again.

### 3. FOCUS OF THE MONTH – BLOGGING SECURITY

---

Blogging is the new phenomena in the IT-world today. It is registered a rapidly increase in the number of bloggers, even though only about one out of ten computer users are bloggers at this moment. The question now is; does this new trend bring security threats? The Focus of the Month will present some pros and some cons around the usage of blogs, and look at this in a computer security and privacy perspective. Some of the arguments in this article will be based on first hand experience.

#### THE POSITIVE SIDES

There are many advantages blogging brings into the IT-world. Blogging is popular within all levels of society and education, and this will bring more users to the computers. Media has covered several stories about bloggers all over the world, which has written about anything from their life as a prostitute at the streets of Brazil, to articles that revealed misuse of information in one of the world's biggest news channels. Blogging has become the new way to express opinions. It has become the new media, the new news channel and the modern kind of diary. But what are the positive sides in a security perspective?

As blogging becomes more popular more security blogs surface. Security blogs are different blogs that discuss vulnerabilities, threats and other issues in or against different areas of information technology. The blogs can be about software, computer hardware, communication technologies and so forth. The vulnerabilities that are presented in these blogs are often unknown for the companies in question, and therefore these blogs are helpful. Not only do the companies get information about vulnerabilities, but the users do to. In other words, users become aware of problems and may try to avoid the problems in question.

There are several examples of such blogs. In July 2006 Secode wrote about the *bug-a-day* blog in the Norwegian version of Security Threats and Trends. This blog was used to publish new vulnerabilities in web browsers every day for one month. Another blog of this kind is the *Month of Kernel Bugs*. In this blog kernel vulnerabilities have been published every day the last month (November 2006).

As mentioned before, the bloggers are from all kinds of society and educational levels. In other words, people who normally would not use the computer may now use it to write blogs. This enhances computer skills and awareness of the computers possibilities. We can in fact say that people who would normally not start using a computer now gets a push into the usage. As you have to have computer skills for almost any job in the western world today, this is an important development.

#### THE NEGATIVE SIDES

There are at this point probably more direct negative sides than positive sides around the use of blogs, but the blogs are full of potential and may bring more positivity in the future. Some of the negative sides of the blogs may not be severe, but they are often more visible to the public.

Several blogging sites have problems with spamming among the comments. This is mostly links to other sites, such as porn sites, casinos, hacker sites, illegal downloading sites, drug sellers and so on. Hundreds of such links may be covered by seamlessly good links, others are shown without a doubt of what it is. The spamming by itself is not dangerous for computer security, but the links may be. If a user is unaware of what the link is all about, viruses may enter his or her computer. The site, which the link refers to, may also be a phishing site, which can ask for personal information.

Privacy is an issue in itself when it comes to blogging. Many bloggers write about their own life masquerading as anonymous persons. However, they do not always have the knowledge needed to keep it anonymous. With all the information available at the Internet today, you don not have to have a lot of information about a person to figure out who he or she is, the home address, phone numbers and other information.

Let us present an example of how easy it is to give information that can tell others who you are. You enter a blog and write something like the following: "Yesterday I started my day by taking a horse ride around the area here. It is lovely to ride among the sheep and near the small farms. I love the fact that I live in a small place up north at the countryside. After a short breakfast at the diner by the main road here in town I went to my job as a security analyst within computer engineering. My colleague, John, and I did some work around some new technology our company develops. We are developing a new security device, which we are going to release next month. Anyway, after work I took some time going to Karate practice..." So what have you actually told the reader? Well, after that short story about your day the reader knows that you live in a small town at the countryside. There are several small farms outside this town, and there is a computer security company and a Karate dojo in town. There is also a diner by the main road. Even though the name John is masqueraded, a smart person would figure out where this is by just using Google (given that the country which the blogger came from is not that big), and you gave away some sensitive information about your own company. As you may see, this is probably the most dangerous aspect of blogging.

We have not even discussed the cons around security blogs yet. Many experts will state that these blogs make vulnerabilities known to the hacker, and should be stopped. This is part of the ongoing discussion around making vulnerabilities known or keeping them hidden. This discussion is a chapter by itself actually. Of course there may be negative sides about letting hackers, script kiddies and others know about vulnerabilities, but should people who discover them keep them hidden?

## **USERS RESPONSIBILITY**

As a blogger you have some responsibility. The blogger should try to keep critical information anonymous. There have been cases of people loosing their job after it has become known that a blogger have given away information about employees, or the company itself. A good rule would be not to write anything about people at work or information about the company that may be misused. Keep to the issue if you write in a serious blog, and do not give away to much information if you write about your life in personal blogs like MyBlog.com.

Visitors to other blogs should be careful what links they enter if there are links in comments. These links may be malicious.

## **CONCLUSION**

Blogging is still relatively new, but have become widely used by different users. This brings both positive and negative sides at this moment. In a computer security perspective we once again find ourselves discussing the pros and cons of publishing information about vulnerabilities. As long as this discussion exists, we can not tell you if the security blogs are positive or negative. The problem is that there are probably as many opinions about that issue as it is security experts in the world.

Blog spam however is a problem which may be fought. It is probably hard to win this battle, as it is for e-mail spamming, but the problem can be reduced. The main thing is, spammers do not earn anything if the links are not visited. In other words, the best way to fight this spam is to not click on their links. Anti-spam features are also developed.

Blogging will probably be even more popular in the future. Companies start to see the positive sides of communicating with their customers this way, and normal everyday users use this to express their opinions. Others use it just to get some feedback to their thoughts, in an anonymous way.

As you may see, the blog in itself is secure, but the content may not be.

### **SOURCES OF INFORMATION**

The Month of Kernel Bugs blog:

<http://projects.info-pull.com/mokb/>

Wikipedia – Spam in blogs:

[http://en.wikipedia.org/wiki/Spam\\_in\\_blogs](http://en.wikipedia.org/wiki/Spam_in_blogs)