

SECURITY THREATS AND TRENDS

FEBRUARY 2008

SECODE

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 News of the Month, which is a new chapter this month, collects some of the most important news and vulnerabilities this month.

In the Focus of the Month we look at the Data Retention Directive. We describe the directive from a Norwegian point of view. This is meant as a summary of the most important news about this directive, which has been in many news media this month.

Among the Alert Statistic we see that there are some brute force, scans and other attacks towards our customers from the Internet. These attacks do not form any real threat towards our customers. The alerted incidents are mostly directed attacks from Internet, or ignorant users at the customers' site.

There has been a slight increase in the number of reconnaissance attacks this month, in comparison with last month. This is mostly because there have been a great deal of traffic towards port 5900 (VNC) towards the end of the month. The traffic has its origin mostly in Poland and Hungary.

TABLE OF CONTENTS

| | |
|---|-----------|
| INTRODUCTION | 4 |
| NEWS OF THE MONTH..... | 5 |
| PUBLISHED VULNERABILITIES | 5 |
| IN THE NEWS | 6 |
| FOCUS OF THE MONTH – DATA RETENTION..... | 8 |
| WHAT IS THE DIRECTIVE OF DATA RETENTION?..... | 8 |
| PRIVACY | 8 |
| DATA RETENTION..... | 8 |
| POLITICAL AND CIVIL RESISTANCE | 9 |
| SOURCES | 9 |
| ALERT STATISTIC | 10 |
| HANDLED ALERTS..... | 10 |
| REPORTED INCIDENTS | 11 |
| THREAT LEVEL | 12 |
| RECONNAISSANCE ATTACKS JANUARY 2008 | 12 |
| INTERNET WORMS AND SPAM | 14 |

INTRODUCTION

This report is built on four main parts: News of the Month, Focus of the Month, Threat level, and Alert Statistic.

News of the Month is a chapter which presents the biggest IT security incidents registered by other media. This may be sensational analysis, new viruses, new vulnerabilities, or other IT security news.

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.

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.

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.

NEWS OF THE MONTH

During a month many vulnerabilities will be published, and there will have been many security related news. We wish to present the most important vulnerabilities and the most interesting news in this chapter. We will emphasize that this is only a small part of the news the last month. Most cases, if not all, have been presented in Secode Norway's newsletter during this month.

PUBLISHED VULNERABILITIES

Vulnerabilities discovered in several Windows media players

<http://www.heise-security.co.uk/news/101198>

RealPlayer Unspecified Data Processing Buffer Overflow Vulnerability

<http://lists.immunitysec.com/pipermail/dailydave/2008-January/004811.html>

http://www.us-cert.gov/current/index.html#public_exploit_code_for_realplayer

Novell ZENworks Endpoint Security Management Privilege Escalation

<http://secunia.com/advisories/28351/>

Apache "mod_proxy_balancer" Cross Site Scripting and Denial of Service

<http://www.frsirt.com/english/advisories/2008/0048>

IBM Lotus Domino Unspecified Denial of Service Vulnerability

<http://secwatch.org/advisories/1020009/>

Sun Java System Identity Manager Multiple Cross Site Scripting Issues

<http://www.frsirt.com/english/advisories/2008/0089>

Sun Java SE 6 Update 4 has released

http://java.sun.com/javase/6/webnotes/ReleaseNotes.html#160_04

Lotus Sametime Client Remote Cross-Site Scripting Vulnerability

<http://www-1.ibm.com/support/docview.wss?uid=swg21292938>

Citrix Presentation Server Buffer Overflow in IMA Service Lets Remote Users Execute Arbitrary Code

<http://support.citrix.com/article/CTX114487>

MyBB PHP Code Execution and SQL Injection Vulnerabilities

<http://community.mybboard.net/showthread.php?tid=27227>

HP Oracle for OpenView Multiple Vulnerabilities

<http://secunia.com/advisories/28556/>

IBM Tivoli Business Service Manager Discloses Passwords to Local Users

<http://www-1.ibm.com/support/docview.wss?uid=swg24017939>

Cisco PIX Firewall TTL Decrement Feature Lets Remote Users Deny Service

<http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml>

Cisco Application Velocity System Default Admin Passwords Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml>

Proficy Default Login Method Does Not Encrypt User Passwords

<http://support.gefanuc.com/support/index?page=kbchannel&id=KB12459>

Firebird Remote Memory Corruption

<http://www.coresecurity.com/?action=item&id=2095>

IN THE NEWS

Data Breaches, Thefts on the Rise

<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/01/AR2008010101714.html?hpid=topnews>

Report: Identity Theft Worse in 2008

http://www.cio-today.com/story.xhtml?story_id=0020002HDHGS

Social networking sites supply valuable information to criminals

<http://www.heise-security.co.uk/news/101248>

2007 worst ever year for data protection

http://www.theregister.co.uk/2008/01/07/lib_dems_data_losses/

Spam hits 97 percent of all email

<http://www.itnews.com.au/News/NewsStory.aspx?story=67677>

FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack

http://www.wired.com/politics/security/news/2008/01/dreamliner_security

Schoolboy hacks into city's tram system

<http://www.telegraph.co.uk>

Trojan targets over 400 banks

http://www.symantec.com/enterprise/security_response/weblog/2008/01/banking_in_silence.html

Home Sec in anti-terror plan to control entire web

http://www.theregister.co.uk/2008/01/17/home_office_smith_speech_web_terror_crackdown_insanity/

Two-thirds of Oracle DBAs don't apply security patches

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057226&pageNumber=1>

CIA Says Hackers Have Cut Power Grid

<http://www.pcworld.com/article/id,141564-c,hackers/article.html>

Storm worm anniversary brings fresh variants

<http://news.zdnet.co.uk/security/0,1000000189,39292265,00.htm>

First case of "drive-by pharming" identified in the wild

<http://www.networkworld.com/news/2008/012208-drive-by-pharming.html>

Windows Vista One Year Vulnerability Report

<http://blogs.technet.com/security/archive/2008/01/23/download-windows-vista-one-year-vulnerability-report.aspx>

Hacked embassy websites found pushing malware

http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/

Schneier: Cyber-extortion on the rise

<http://news.zdnet.co.uk/security/0,1000000189,39292357,00.htm>

Bush Order Expands Network Monitoring

http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html

New attack proves critical Windows bug 'highly exploitable'

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060118>

Schneier: Security vendors exploiting user emotions

<http://news.zdnet.co.uk/security/0,1000000189,39292505,00.htm>

IM attacks get nastier

<http://www.techworld.com/security/news/index.cfm?newsID=11279&pagtype=samechan>

FOCUS OF THE MONTH – DATA RETENTION

During the last weeks there have been debates on Norwegian Internet news sites. The debates have been related to the EU Directive 2006/24/EC, the Data Retention Directive. The directive is in itself not new, it was actually adopted march 2006, but until now the directive has not been implemented in Norway. Most countries in the European Union have approved the directive, with the Irish and Slovenian representatives being the only ones to vote against it. In this months focus we will try to collect information about this directive, so you as a reader may see the real meaning of implementing this directive, and why it is so highly spoken of.

WHAT IS THE DIRECTIVE OF DATA RETENTION?

In Norway the directive has gotten the name “Datalagringsdirektivet”, which will be “Data Retention Directive” if we translate it directly to English. The name is referring to the EU directive called 2006/24/EC (or 2006/24/EF in Norwegian). This directive treats with the issues around data retention. Information that is to be saved, in accordance with this directive, may be used in the fight against crime and terrorism. The data retention shall include e-mail, different kinds of telecommunication and Internet access.

Many people are in the belief that this directive give access to saving the entire communication stream, this is not the case. The information stored should only be identity and time of communication. For mobile phone communication, place of call are also to be stored. Data revealing the content of the communication are not to be stored. E-mail content may not be stored either, and web traffic is not to be stored. Only IP-address and the time of logon and logoff may be stored.

PRIVACY

We may be especially preoccupied by privacy in Norway. Every time something or someone in some way or another threatens our privacy, the population of Norway will object. This is the tendency we see now.

Privacy is defined as “restrictions to avoid misuse of personal information”. In the case of the directive of data retention many will argue that by saving identity for both parties in telecommunication we have a breach of privacy. Saving the data, and keeping it stored, is not the breach in itself. However, use of data later on may be. Several news media states, as the directive says, that the data are only to be used if there is suspicion of a crime. Practically this means; in stead of saving data for the suspects in a case, data will be stored for everyone and only data for suspects will be used.

So, why do people object to this directive? If you are not a suspect in a criminal case, or suspected for terrorism, the data will never be used. Well, it comes down to trust. People do not want this data to be stored, because they do not trust the government, the ISPs and others involved. The people in a country can never be sure that the data is stored securely enough. In addition, many feel that by inducting a directive of this kind the population are under “suspicion” at all times. In some ways you can say that this directive treats everyone as a criminal until “proven innocent”.

DATA RETENTION

The directive states that the data shall be retained from 6 months up to 2 years. It is up to each country to decide how long they want to retain the data. In Norway the police have stated that they want to save the data for 12 months. This also leads to debates in Norway, were many experts believe that the minimum amount of time should be used.

Another question that has been asked about data retention is of course exactly what is to be retained. The directive has clear guidelines on this point. The content of the communication shall, as previously stated, not be saved. There is however some concerns that inducting this directive will lead the way for retaining more information in the future. Several companies

have, in Norway at least, expressed a strong wish for communication content being retained. This can be used to reveal distribution of illegal content, for example copyright material.

POLITICAL AND CIVIL RESISTANCE

To begin with there were only one political party in Norway that were critical of inducting this directive. Now several parties are having the same opinion. The “youth parties” are mostly the parties being critical. It is expected that several critical questions will be asked when the Data Retention Directive is being submitted to a hearing in the Norwegian Parliament.

Civilians are also engaged in this matter in Norway. Over 9 000 Norwegians have signed a petition on the Norwegian site www.opprop.no. At Facebook, the Internet community, there are at least two groups showing their resistance for this directive. The two groups have, at this point, roughly 6 500 and 16 000 members. In other words, in a Norwegian perspective, we see a relatively large engagement among civilians to stop this directive.

Norway has basically no power in this matter. As a member of EEA (European Economic Area,) Norway must follow many directives stated by the European Union (EU). So, if Norway in some way set against this directive in a political state, it will only have a symbolic meaning towards the EU. Norway may also use the right to veto, but this requires political support from other countries in the EU, and the question is if this support is big enough at this point. The most impact Norway can make is to make the directive “thinner”, as they did with the Infosoc Directive.

It will be interesting to follow the development of this matter in the future.

SOURCES

- [1] EurLex – Directive 2006/24/EC
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>
- [2] Dagbladet – Alle nordmenn skal overvåkes (Norwegian)
<http://www.dagbladet.no/dinside/2008/01/10/523498.html>
- [3] Forbrukerrådet – Datalagringsdirektivet truer personvernet (Norwegian)
<http://forbrukerportalen.no/Artikler/2008/1201264304.64>
- [4] Datalagringsdirektivet.no (Norwegian)
<http://www.datalagringsdirektivet.no>
- [5] Digi.no – Politisk motstand mot datalagringsdirektivet (Norwegian)
<http://digi.no/php/art.php?id=507068>

ALERT STATISTIC

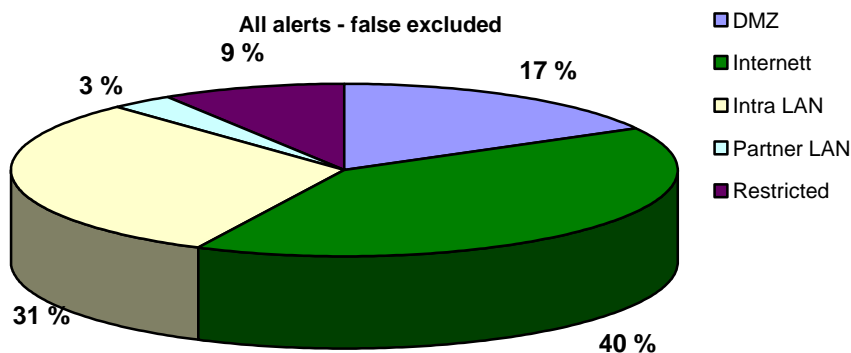
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

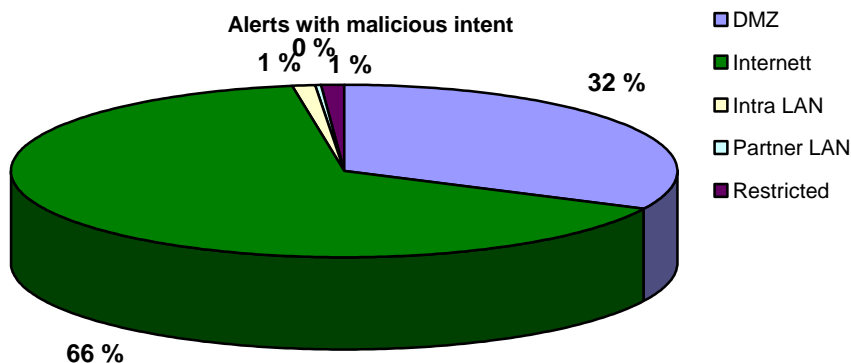
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

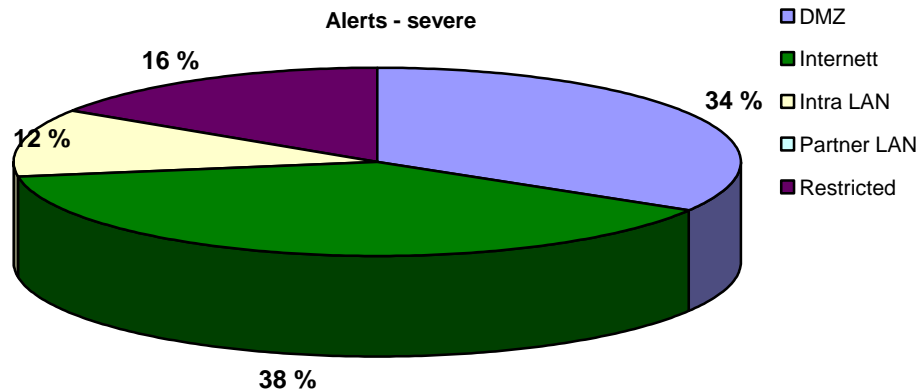
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

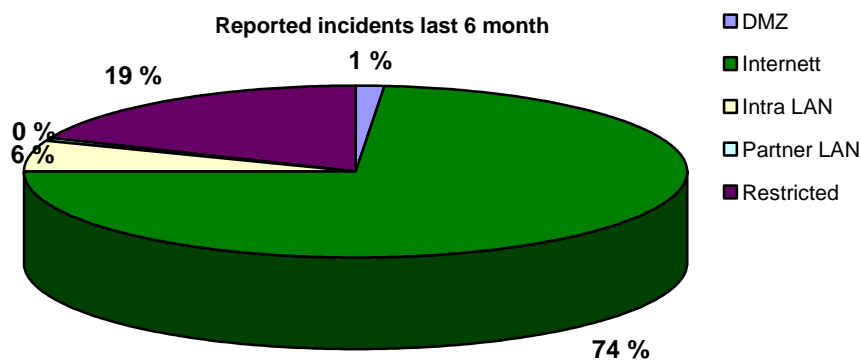


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

If you look at the distribution of alerts with malicious intent in comparison with severe alerts, you will soon discover that there are a bigger amount of alerts from Internet that are malicious than severe. This is mostly due to some brute force attacks, port scan and similar from different sources on the Internet, which will never form any big threat for Secode's customers.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



The big amount of reported incidents with Internet origin is mainly directed attacks towards financial institutions in Norway. The last couple of years, crime for profit have replaced other types of attacks, and many institutions and companies are then the goal of attacks.

The incidents in the restricted zone are mainly ignorant users breaching a company policy.

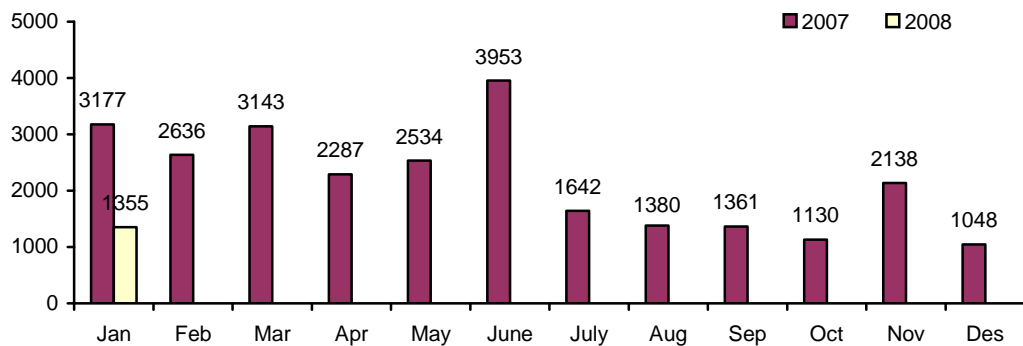
THREAT LEVEL

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.

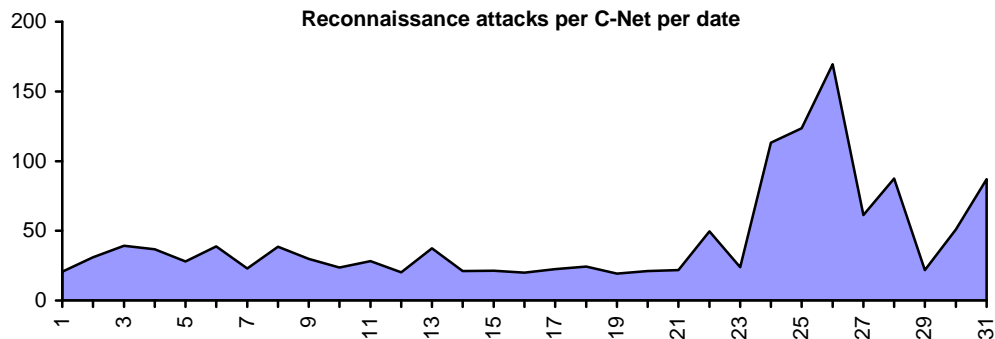
RECONNAISSANCE ATTACKS JANUARY 2008

The statistics in this subchapter gives an overview of the average number of reconnaissance attacks per network under surveillance. Top 10 average reconnaissance attacks contain a summary of the most common reconnaissance attacks; either the scan is for one single service or a combination of several services. The malicious activity in the statistics 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.

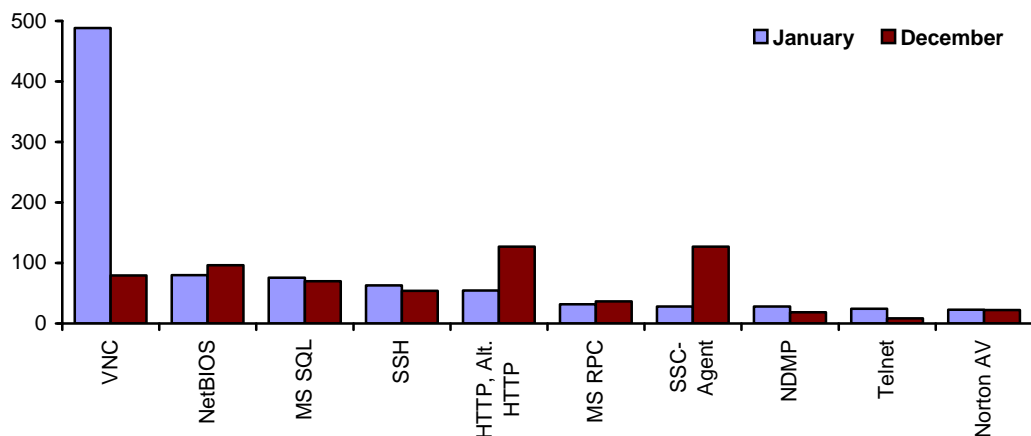
Reconnaissance attacks per monitored C-Net

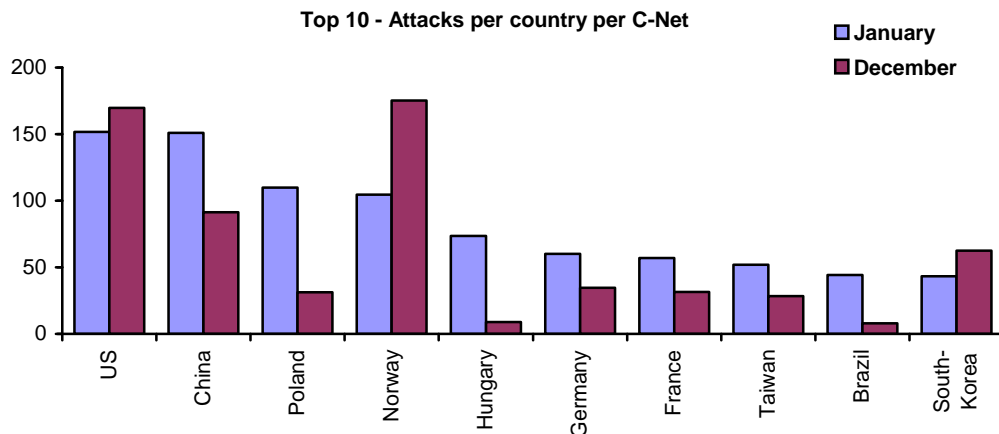


Reconnaissance attacks per C-Net per date



Average top 10 incidents per C-Net





The level of traffic is slightly higher than the level we saw last month, but it is still lower than the level we saw a year ago. We anticipate that we will continue to see a relatively low level of traffic throughout 2008, as we did the second half of 2007, or a further decrease in the level. This is because we see that the attacks are more and more directed towards specific companies, and reconnaissance attacks are therefore only used in the preliminary attacks.

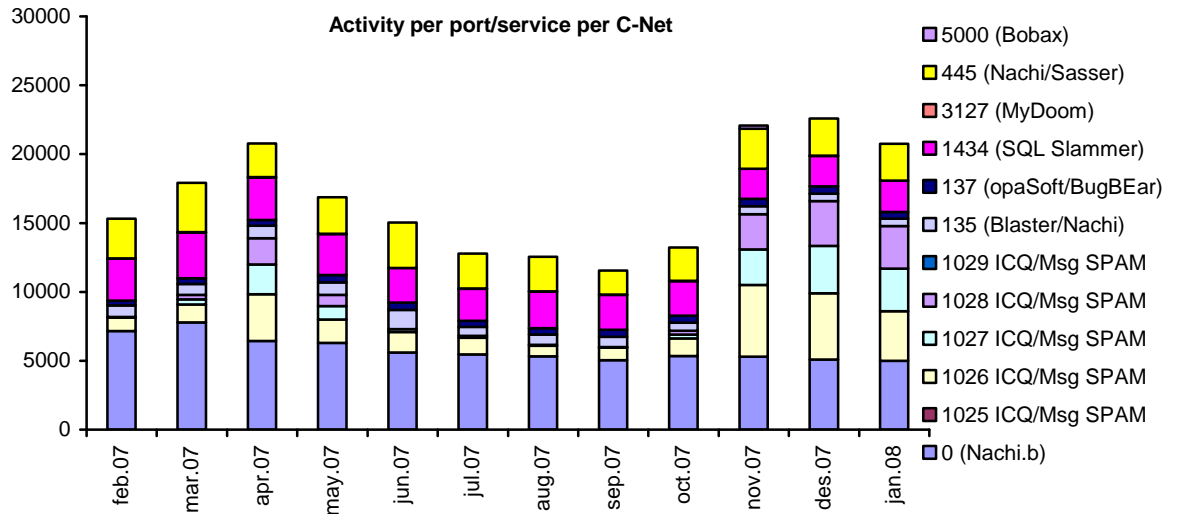
During this period there has been a stable level until the last week of the month. The traffic in this following period was mostly due to VNC traffic from Poland and Hungary. We can find this pattern in the other graphs as well, where VNC is the most exposed service this period, and Poland and Hungary have had the biggest increase in traffic since last month.

We also see an increase in searches from countries that were higher on the list earlier in 2007. This includes France and Brazil. Norway, on the other hand, has had a decrease in the level of traffic during this period, in comparison with last period.

If we exclude the previously mentioned changes, there are only minor differences in this month's traffic.

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.



During the last three months we have seen an increase in the level of ICQ/Msg Spam in comparison with earlier months in 2007. This is most likely due to the spreading of a new MSN virus in this period. The virus spread through messages claiming the user of MSN was on a picture found on an Internet Community site, for example Facebook. The user was asked to visit the site to see it. These messages have most likely triggered as spam.