

# **SECURITY THREATS AND TRENDS**

## **MARCH 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

Focus of the Month is about today's web attacks; the motive and techniques behind these.

The Alert Statistic shows that the majority of attacks against Secode's customers in March are observed in the Internet zone, while the most serious incidents occur in dmz and internal network zones.

There has been a slight decrease in number of reconnaissance attacks this month. Spamming attempts and activity from Internet worms remains at a stable level.

## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>4</b>
<b>NEWS OF THE MONTH.....</b>	<b>5</b>
PUBLISHED VULNERABILITIES .....	5
IN THE NEWS .....	6
<b>FOCUS OF THE MONTH – EVOLUTION OF WEB ATTACKS.....</b>	<b>8</b>
THE TECHNIQUES.....	8
SOURCES .....	9
<b>ALERT STATISTIC .....</b>	<b>10</b>
HANDLED ALERTS.....	10
REPORTED INCIDENTS .....	11
<b>THREAT LEVEL .....</b>	<b>12</b>
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

AIX LIBC INET\_Network Buffer Overflow

[http://www14.software.ibm.com/webapp/set2/subscriptions/ijhifoeblist?mode=7&heading=AX61&path=/200802/SECURITY/20080227/datafile123640&label=AIX%20libc%20inet\\_network%20buffer%20overflow](http://www14.software.ibm.com/webapp/set2/subscriptions/ijhifoeblist?mode=7&heading=AX61&path=/200802/SECURITY/20080227/datafile123640&label=AIX%20libc%20inet_network%20buffer%20overflow)

Java Runtime Environment lets Remote Applets and applications gain elevated privileges

<http://securitytracker.com/alerts/2008/Feb/1019308.html>

Trend Micro Office Scan multiple Remote Buffer overflow Vulnerabilities

<http://www.frsirt.com/english/advisories/2008/0702>

Symantec Decomposer: Multiple Denial Of Service vulnerabilities

<http://www.symantec.com/avcenter/security/Content/2008.02.27.html>

Critical VMWare Security alert for Windows hosted VMWare workstation

[http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=1004034](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004034)

Sybase Mobilink Data Processing Remote Buffer Overflow Vulnerabilities

<http://aluiqi.altervista.org/adv/mobilinkhOf-adv.txt>

IBM DB2 multiple Denial Of Service and Unspecified Vulnerabilities

<http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21255572>

IBM LOTUS NOTES JAVA PLUGIN SANDBOX Security Bypass Vulnerability

<http://www-1.ibm.com/support/docview.wss?uid=swg21257249>

FreeSSHd SSH Server Remote Denial Of Service Vulnerability

<http://aluiqi.altervista.org/adv/freesshdnull-adv.txt>

MySQL Multiple Code Execution and Security Bypass Vulnerabilities

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html>

CISCO Unified IP Phone Overflow and Denial Of Service Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-sa-20080213-phone.shtml>

Adobe Flash Media Server Edge Server Multiple Vulnerabilities

<http://www.adobe.com/support/security/bulletins/apsb08-03.html>

Adobe Reader

<http://www.frsirt.com/english/advisories/2008/0425>

Mozilla Firefox/Thunderbird/SeaMonkey Multiple Remote Vulnerabilities

<http://www.mozilla.com/en-US/firefox/2.0.0.12/releasenotes/#download>

Mozilla Firefox Lets Remote Users Obscure Web Forgery Dialog Warnings.

<http://securitytracker.com/alerts/2008/Feb/1019342.html>

Mozilla Firefox Stylesheet Processing Bug May Let Remote Users Obtain URL Parameters

<http://securitytracker.com/alerts/2008/Feb/1019341.html>

Mozilla Firefox Lets Remote Users Tamper with Security Dialogs

<http://securitytracker.com/alerts/2008/Feb/1019339.html>

Mozilla Firefox Lets Remote Web Sites Corrupt the Password Store in Certain Cases

<http://securitytracker.com/alerts/2008/Feb/1019334.html>

Mozilla Firefox Lets Remote Users Steal the Focus to Obtain Keystrokes

<http://securitytracker.com/alerts/2008/Feb/1019330.html>

Mozilla Firefox chrome: URI Directory Traversal Bug Lets Remote Users Load Local Files

<http://securitytracker.com/alerts/2008/Feb/1019329.html>

Mozilla Firefox designMode Frames May Let Remote Users Obtain Information and Potentially Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Feb/1019328.html>

Mozilla Firefox JavaScript Bugs Let Remote Users Conduct Cross-Site Scripting Attacks and Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Feb/1019327.html>

Mozilla Firefox Bugs in JavaScript Engine Let Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Feb/1019321.html>

Mozilla Firefox Bugs in Browser Engine Let Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Feb/1019320.html>

IBM DB2 Universal Database Administration Server Memory Corruption Vulnerability

<http://labs.idefense.com/intelligence/Vulnerabilities/display.php?id=654>

IBM DB2 Universal Database db2pd Arbitrary Library Loading Vulnerability

<http://labs.idefense.com/intelligence/Vulnerabilities/display.php?id=653>

IBM WEBSPHERE Edge Server Caching Proxy Cross Site Scripting Issue

<http://www.frsirt.com/english/advisories/2008/0446>

CISCO Wireless Control System TOMCAT "MOD\_JK.SO" Buffer Overflow

<http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.shtml>

## **IN THE NEWS**

Finjan Uncovers more than 8700 FTP servers credentials in the hands of hackers.

<http://www.finjan.com/Pressrelease.aspx?id=1868&PressLan=1819&lan=3>

IT Security skills falling short

<http://www.eweek.com/c/a/Careers/IT-Security-Skills-Falling-Short/>

McFee, Inc. teams with VMWare to advance virtualization security

<http://www.tradingmarkets.com/.site/news/Stock%20News/1140142/>

Microsoft's glasnost on interoperability means more bugs

<http://www.computerworld.com.au/index.php?id=570917725&eid=-6787>

Banks: Losses from computer intrusions up in 2007

[http://blog.washingtonpost.com/securityfix/2008/02/banks\\_losses\\_from\\_computer\\_int.html](http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html)

OpenID like sikkert som BankId

<http://www.digi.no/php/art.php?id=511041>

Online Gaming sites attacked by botnets

<http://www.casinocitytimes.com/news/article.cfm?contentID=171393>

Phishing attacks unleashed in UK banks

<http://news.zdnet.co.uk/security/0,1000000189,39292884,00.htm>

A powerful new Trojan horse causing concern

<http://www.scrippsnews.com/node/30747>

Mobile industry sees new security risks

<http://www.eweek.com/c/a/Security/Mobile-Industry-Sees-New-Security-Risks/>

Security vendors target mobile operators

<http://www.eweek.com/c/a/Security/Security-Vendors-Target-Mobile-Operators/>

MAYDAY! MAYDAY! Ruskies reinvent Cyber Crime

[http://www.theregister.co.uk/2008/02/13/new\\_botnet\\_advances/](http://www.theregister.co.uk/2008/02/13/new_botnet_advances/)

Encryption could make you more vulnerable, warn experts

[http://security.itworld.com/4341/encryption-makes-you-more-vulnerable-080211/page\\_1.html](http://security.itworld.com/4341/encryption-makes-you-more-vulnerable-080211/page_1.html)

RealPlayer users held to ransom

<http://www.daniweb.com/blogs/entry2060.html>

IT mot personvern: Grunnloven må endres

<http://www.digi.no/php/art.php?id=508639>

Remote workers ignoring security

<http://www.vnunet.com/vnunet/news/2209015/remote-workers-lax-security>

Spyware morphs into new treats

<http://www.computerweekly.com>

## FOCUS OF THE MONTH – EVOLUTION OF WEB ATTACKS

---

It is said over and over again; the attack pattern is now moving away from attacks against operative systems over to attacks against applications. Especially web attacks have been through an evolution where they have expanded both in number and attack techniques.

### THE MOTIVE

There are multiple reasons why attacks against web servers have increased. First is that web servers are easily available at the Internet. Additionally, organizations are putting more functionality out on the net, and some of these are developed too fast and not sufficiently tested. According to Gartner, 75 % of all security breaches at web sites were caused by poorly developed software.

Many web applications are vulnerable. Only during February it was published a high number of web vulnerabilities:

Cross-site scripting: 49 vulnerabilities  
SQL Injection: 133 vulnerabilities  
Web Applications: 85 vulnerabilities

According to the yearly Hacking Incident Database Report from WASC (Web Application Security Consortium), is data theft the main motive behind attacks. Thereafter follows surprisingly site defacing, again followed by attempts of planting malware at websites. One would believe that site defacing should be on a much lower level, considering that cyber crime now mainly are based on economic profit. A total of 67 % of all threats in WASC's report were designed to gain profit. Ideological hacking is listed as number two.

E-commerce sites and the databases behind them is a popular target for today's hackers. Such databases usually contains credit card numbers and expire date – information that easily can be used to empty the victims bank account. In addition to this, the tendency now shows an increase in attacks against new targets, including government and educational institutions. A reason for why hackers now turn to new targets may simply be that most e-commerce and transaction sites now have a better defense against web attacks.

### THE TECHNIQUES

SQL injection and cross-site scripting are the most well-known and still current methods for hacking web servers. Cross-site request forgery is on the other hand a technique that is not so much in use, but is considered to have a potential to increase. Probably can an equal high number of sites be vulnerable to Cross-site request forgery as to SQL injection.

Cross-site request forgery is in brief an attempt to hijack authorized net sessions to send unauthorized commands from the user to the web server. The clue in this attack is that the unauthorized commands come from a user approved and trusted by the web server. Potential victims for such attacks are web servers that perform instructions without further validation if the command comes from an already authenticated user.

Phishing have really made its impact on the attack pattern on the internet in the last couple of years, but is now outnumbered by hiding of malware at legitimate sites. This is done to spread malicious code and to hit end-users through their browsers. In this way are web servers becoming the source of virus- and Trojan propagation, and web servers are now replacing e-mail as the preferred channel to distribute malicious code.

Today's web attacks against browsers are very sophisticated with regards to how the attacks are designed to avoid security software. According to IBM's X-force Security 2007 Report only a small part of the web attacks were camouflaged, while at the end of 2007 almost 100 % of the exploits were either encrypted or based on obfuscation techniques.

AND IT IS HARD TO PROTECT ONESELF...

The fact that web attacks now just as well can come from legitimate sites as from the slightly more “scruffy” ones, makes it harder for users to protect themselves. The old advice to be aware of what sites to visit is not any longer a guarantee for safe surfing.

To mention one example; In February the downloading section of antivirus company AvSoft's website got hacked and was being used to install virus on the visitors' computers. Another example is the recent episode where Trend Micro was hacked in a massive web attack ([http://www.infoworld.com/article/08/03/14/Trend-Micro-hit-by-massive-Web-hack\\_1.html](http://www.infoworld.com/article/08/03/14/Trend-Micro-hit-by-massive-Web-hack_1.html)).

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

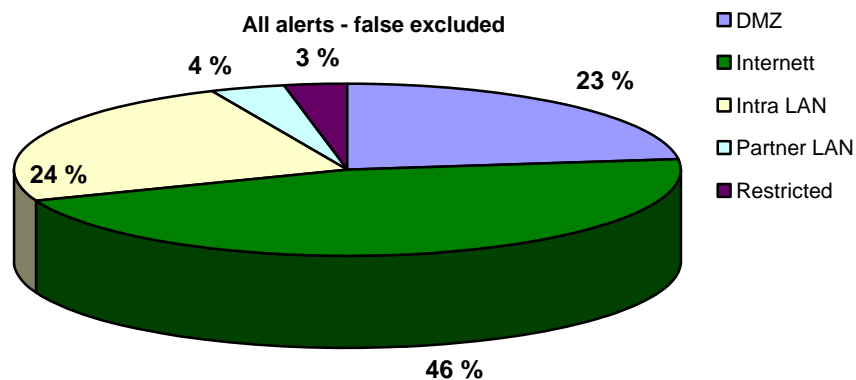
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

### HANDLED ALERTS

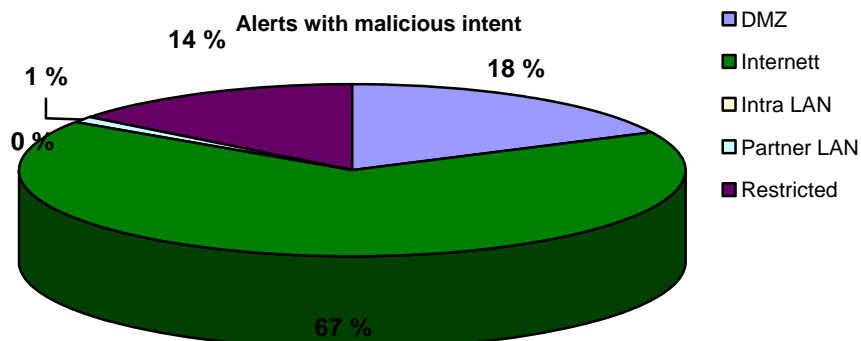
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

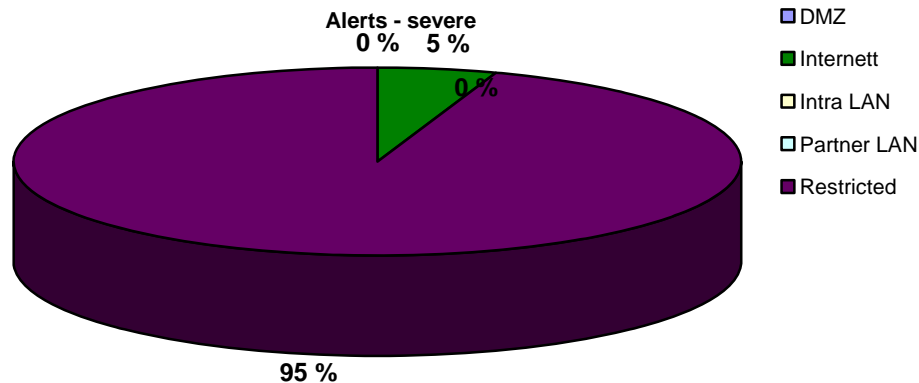
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

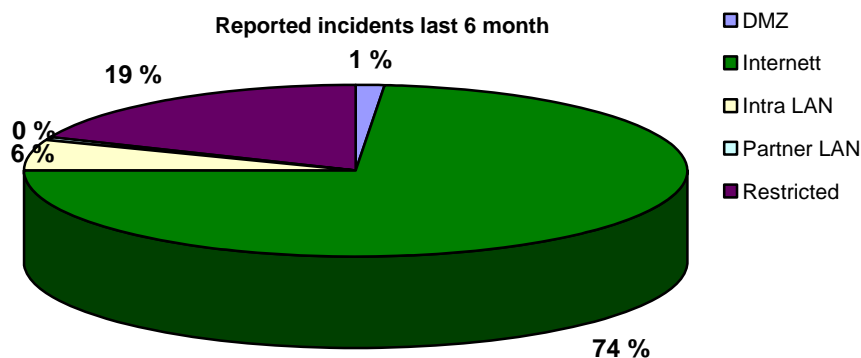


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

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 main percentage of reported incidents with Internet origin is mainly directed attacks towards financial institutions. 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.

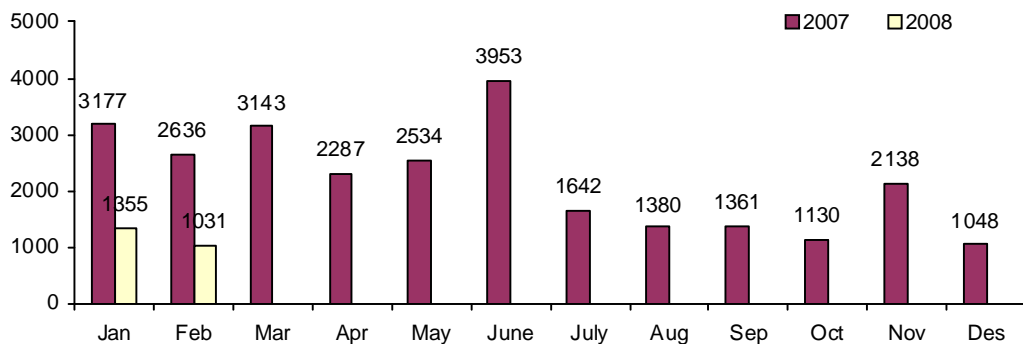
## THREAT LEVEL

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.

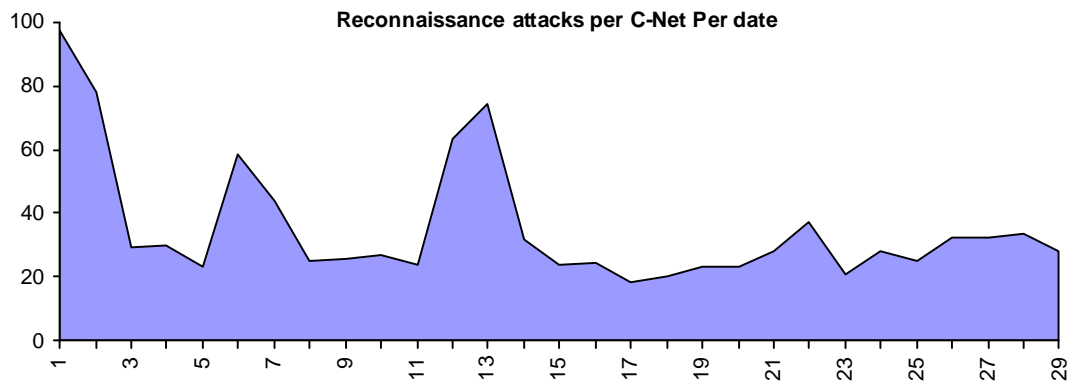
### RECONNAISSANCE ATTACKS JANUARY 2008

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.

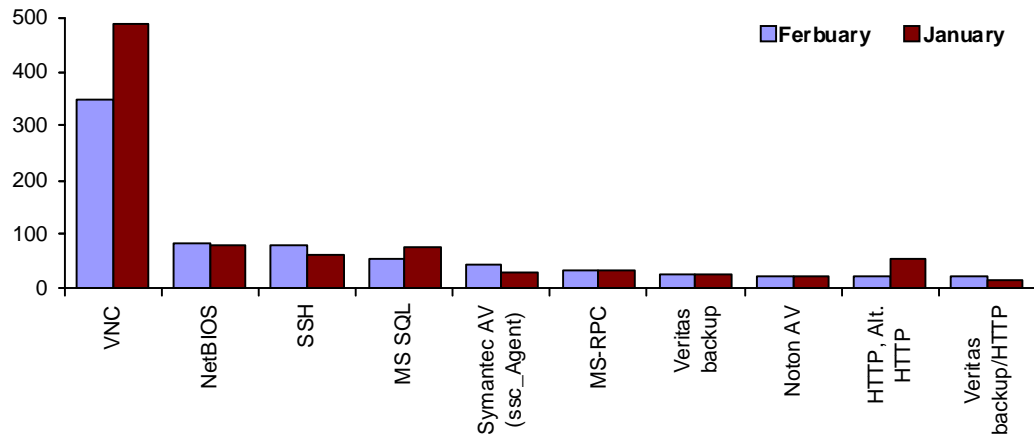
**Reconnaissance attacks per monitored C-Net**



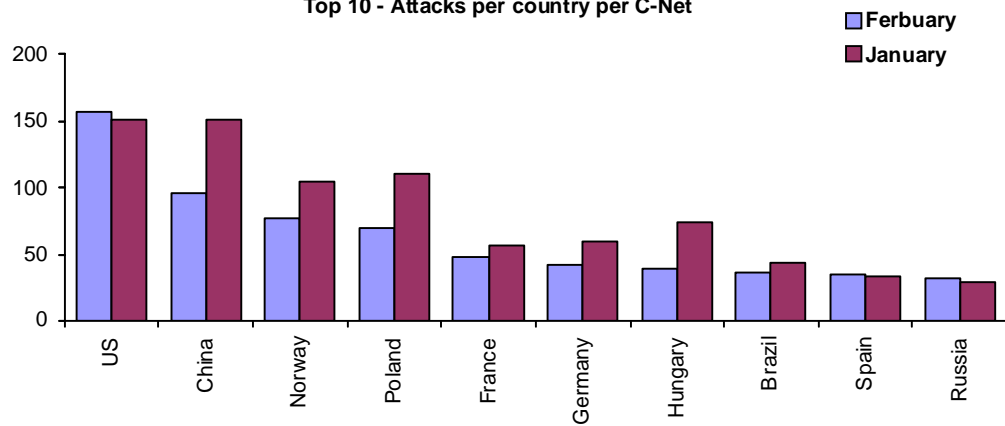
**Reconnaissance attacks per C-Net Per date**



**Average top 10 incidents per C-Net**



**Top 10 - Attacks per country per C-Net**

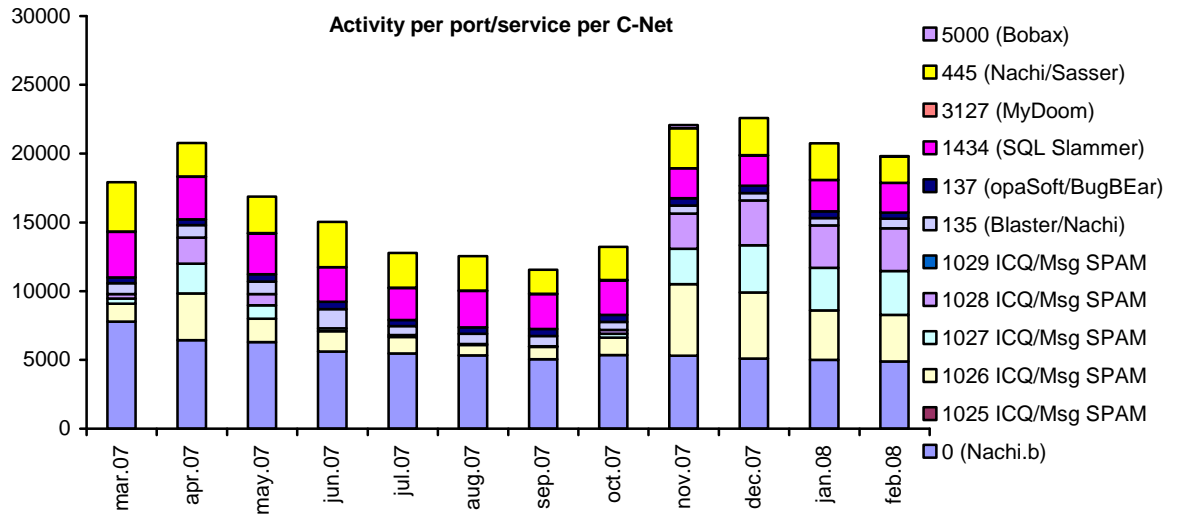


The number of reconnaissance attacks can vary on a daily basis, but the total activity is stable at a low level. It is observed only minor variations in the ten most attacked services. Despite a slight decrease, scans for VNC are still at a much higher level than the remaining services.

The US is the most active source of attacks, followed by China and Norway. Traffic from the Norwegian addresses is generally the same as observed from the other countries.

**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.



Activity towards the different services in the statistic above remains at a stable level. Still it is recorded lots of spam against ICQ and Messenger service.

The sources of traffic against ex. port 1434 is not necessary infected by the Slammer worm, but are probably rather parts of a bot net programmed to continuously send out attacks towards the regular worm services. This explains why we still see so much traffic from old worms that should almost be exterminated by now.