

# SECURITY THREATS AND TRENDS

## AUGUST 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 gives a short description on one of our biggest threats.

The alert statistics show that most of the triggered alerts are now situated in the DMZ-zone, and that the most sever alerts are triggered in restricted zones. Among incidents for the last 6 months we see that they are directed to some of Secode's customers, and then mostly customers in the financial sector.

There has been a decrease in the number of reconnaissance attacks this period, mainly because of decreased activity from infected computers in Poland towards the VNC service.

Spam and worm activity remain 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.....	5
<b>FOCUS OF THE MONTH – THE BIGGEST THREAT.....</b>	<b>7</b>
SOCIAL VIRUSES .....	7
USER TRAINING .....	7
<b>ALERT STATISTIC.....</b>	<b>9</b>
HANDLED ALERTS .....	9
REPORTED INCIDENTS.....	10
<b>THREAT LEVEL.....</b>	<b>11</b>
RECONNAISSANCE ATTACKS JULY 2008.....	11
INTERNET WORMS AND SPAM.....	13

## 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 deep 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 summaries from Secode's Managed Security Services (MSS). An alert appears when an IDS or IPS sensor recognizes network traffic that matches the implemented signatures/filters, and in these cases alerts will be transferred to the Secode SOC (Security Operation Center).

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, several vulnerabilities will be published, and there will have been many security related news. This chapter presents the most important vulnerabilities and the most interesting news. Most cases, if not all, have been presented in Secode Norway's newsletter during this month.

### PUBLISHED VULNERABILITIES

Wireshark GSM SMS, PANA, KISMET, RTMPT, and syslog Dissector Bugs Let Remote Users Deny Service

<http://securitytracker.com/alerts/2008/Jul/1020404.html>

Viktig sikkerhetsfix til Opera

<http://www.opera.com/download/index.dml?custom=yes>

Opera for Windows Unspecified Remote Code Execution Vulnerability

<http://www.frsirt.com/english/advisories/2008/1998>

Unpatched Word Vulnerability

<http://isc.sans.org/diary.html?storyid=4696>

Major fix to DNS vulnerability impacts Windows, Debian

[http://www.betanews.com/article/Major\\_fix\\_to\\_DNS\\_vulnerability\\_impacts\\_Windows\\_Debian/1215551008](http://www.betanews.com/article/Major_fix_to_DNS_vulnerability_impacts_Windows_Debian/1215551008)

Updates for Java eliminate many security holes

<http://www.heise-online.co.uk/security/Updates-for-Java-eliminate-many-security-holes--/news/111080>

Oracle to Release 45 Security Fixes

<http://www.eweek.com/c/a/Database/Oracle-to-Release-45-Security-Fixes/>

Ubuntu Security Update Fixes BIND Cache Poisoning Vulnerability

<http://www.frsirt.com/english/advisories/2008/2090>

Firefox gets security tune-up

<http://www.vnunet.com/vnunet/news/2221977/firefox-gets-security-tune>

Sun Solaris System Management Agent Buffer Overflow Vulnerability

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-239785-1>

High-priority patch fixes critical vulns in RealPlayer

[http://www.theregister.co.uk/2008/07/25/realplayer\\_vulns\\_patched/](http://www.theregister.co.uk/2008/07/25/realplayer_vulns_patched/)

Oracle ships emergency workaround for zero-day flaw

<http://www.eweek.com/c/a/Security/Oracle-Sounds-Alert-Over-Unpatched-WebLogic-Server-Flaw/>

### IN THE NEWS

Older Versions Of Firefox, IE Put 45% Of All Internet Users At Risk

<http://www.informationweek.com/news/internet/browsers/showArticle.jhtml;jsessionid=14LUPCFYDLYFGQSNDLRSKHOCJUNN2JVN?articleID=208801958&subSection=Security>

80 offentlige nettsteder sprer datavirus

<http://www.digi.no/php/art.php?id=777998>

Forty Percent of Web Users Surf With Unsafe Browsers  
<http://governmentsecurity.org/forum/?showtopic=29335>

Gartner: Seven cloud-computing security risks  
[http://www.infoworld.com/article/08/07/02/Gartner\\_Seven\\_cloudcomputing\\_security\\_risks\\_1.html](http://www.infoworld.com/article/08/07/02/Gartner_Seven_cloudcomputing_security_risks_1.html)

ISO certifies Adobe's PDF  
[http://www.theregister.co.uk/2008/07/03/pdf\\_iso\\_standard/](http://www.theregister.co.uk/2008/07/03/pdf_iso_standard/)

Europe drafts law to disconnect suspected filesharers  
[http://www.theregister.co.uk/2008/07/06/europe\\_drafts\\_law\\_to\\_disconnect\\_filesharers/](http://www.theregister.co.uk/2008/07/06/europe_drafts_law_to_disconnect_filesharers/)

Resellers: Cisco not tackling counterfeit products  
<http://news.zdnet.co.uk/security/0,1000000189,39443795,00.htm>

Firefox users shown to be safer  
<http://www.vnunet.com/vnunet/news/2220991/firefox-users-shown-safer>

Security Pros: Microsoft's July Patch Ratings Misleading  
<http://www.eweek.com/c/a/Security/Security-Pros-Rating-of-Microsofts-July-Security-Patches-Could-be-Deceiving/>

Stadig mer spam kommer fra naboens PC  
<http://www.digi.no/php/art.php?id=778944>

Alliance forms to fix DNS poisoning flaw  
<http://www.eweek.com/c/a/Security/DNS-Flaw-Leaves-Major-Internet-Security-Hole/>

5 Ways to Build an Indestructible Customer Data Fortress  
<http://www.technewsworld.com/story/63696.html>

Lanserer Visa-kort som lager egne koder  
<http://www.digi.no/php/art.php?id=779193>

How to plan a Penetration Test  
<http://passcisa.blogspot.com/2008/07/how-to-plan-penetration-test.html>

Facing the pain of passwords  
[http://news.cnet.com/8301-1009\\_3-9989071-83.html?tag=cd.blog](http://news.cnet.com/8301-1009_3-9989071-83.html?tag=cd.blog)

Filmbransjen selger mer til tross for piratene  
<http://www.digi.no/php/art.php?id=779818>

Romanian cops cuff 24 cybercrime suspects  
<http://www.networkworld.com/news/2008/071708-losses-likely-to-rise-from.html?hpg1=bn>

Facebook blunder exposes personal details  
<http://www.vnunet.com/vnunet/news/2221777/facebook-exposes-members>

Is Open Source Development Insecure?  
[http://www.internetnews.com/dev-news/article.php/10792\\_3760026\\_1](http://www.internetnews.com/dev-news/article.php/10792_3760026_1)

Security flaws in online banking sites found to be widespread  
<http://www.ns.umich.edu/htdocs/releases/story.php?id=6652>

Ny søketjeneste «lik Google ganger tre»  
<http://www.digi.no/php/art.php?id=780812>

## FOCUS OF THE MONTH – THE BIGGEST THREAT

---

When you work with IT-security, either as a Security Officer, a Security Consultant or as any other security related employee, the most important thing is to make the systems as secure as possible with the tools available. You will never get a system 100% secure. A totally secure system will be so little user-friendly that the system will be difficult to use at the everyday work. This is the reason why Security Officers use measures to make it more secure without interacting with the systems own user-friendliness. These measures could be antivirus solutions, surveillance either on network or the machine, firewalls, isolated networks zones and so on. All these solutions enhance the security, but sadly none of these are securing against our biggest threat, the users.

Expressions like “no system is more secure than its dumbest user” and “computers only do what they are asked” are constantly surfacing. Those expressions are due to the fact that computers are designed so the users input is the deciding factor for what the computers are to do, and therefore it is the user that is responsible for most problems and errors. This is certainly applicable for some security threats.

It is without a doubt the users and there ignorance that keeps viruses and Trojans alive, spreading them further and letting them infect the computers. It is users that make sure that spammers earn money on their actions and keep going. Actually research show that on securing online services like banking, games, web shops and so on, the user are a more important factor than many other elements.

### SOCIAL VIRUSES

In the beginning of August a new virus in Facebook was reported. The virus made out to be a greeting from one of your friends, writing on “the Wall”. In the message there was a link to an alleged video at Google, but upon clicking on the link you were asked to download a new version of the Flash player. In stead of getting Flash installed you got a Trojan that could be used for spreading malware and so on. This is a good example on how viruses are spreading with the help of ignorant users.

Facebook, MySpace, YouTube, MSN and so on are all exposed to a great deal of viruses. These viruses show that the users make a normal online-service interesting for hackers spreading viruses, just because the users are helping with the virus spread. A message with a link referring to a site passing as being from someone you know is enough to make a virus spread. The user himself is ignorant about the fact that the link may direct you to a virus, or the user really believes that it is a real link sent from the people he knows. Suddenly you then have a Trojan on the machine, spreading the virus further. This last year we have seen an increase in such viruses. MSN is still a popular target, and lately we have seen that Facebook and MySpace are more popular targets.

### USER TRAINING

To make the services more secure, and reducing spreading of viruses, Trojans, spam and so on, it is highly recommended to use some time to train the users. The users should get training in Internet use, generating passwords, e-mail and last but not least the systems they are going to use. You can not let a user handle an electronic cash register if they do not know the system well, or if not the system is design making it impossible to make mistakes. The latter is often hard to implement, and a course is therefore the best approach.

A personal computer should also have updated firewall and antivirus solution installed at any given point of time. A user will often surf the web, download seemingly legitimate files, and open links, without thinking about the consequences. The user should get some sort of training in how these system functions and how to conduct oneself to these systems. There are little use of getting a message that a virus is located on you computer if you are not able to make the right measures, if the antivirus is not able to delete it.



## ALERT STATISTIC

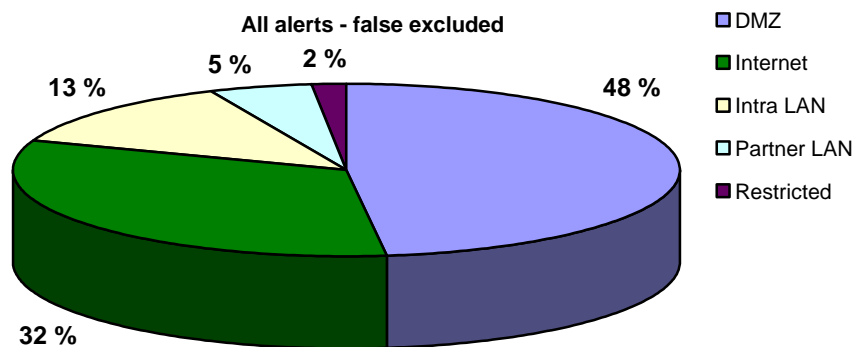
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

### HANDLED ALERTS

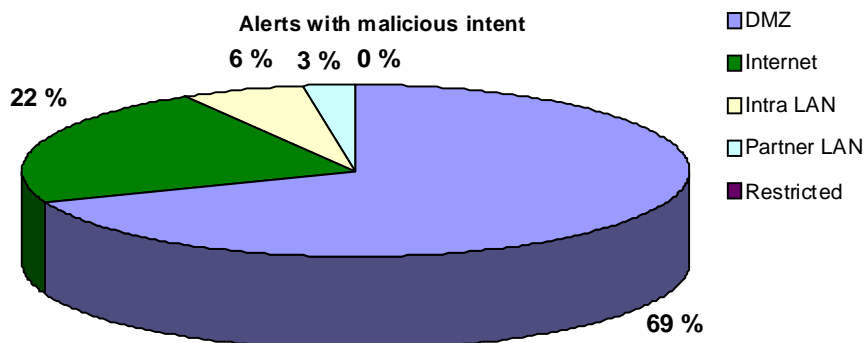
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

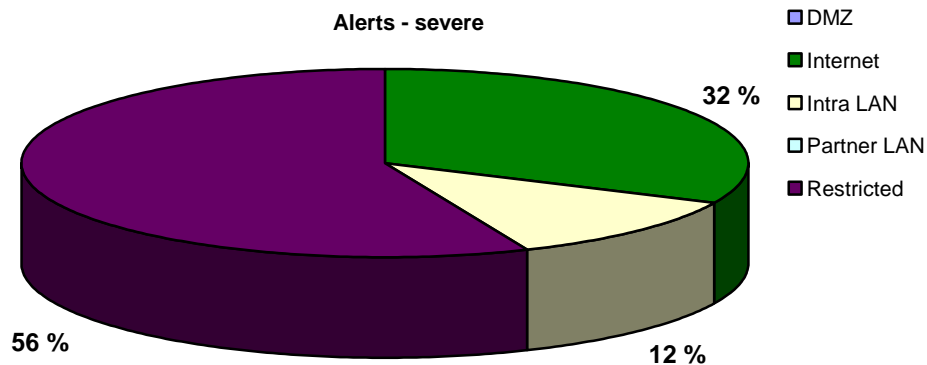
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

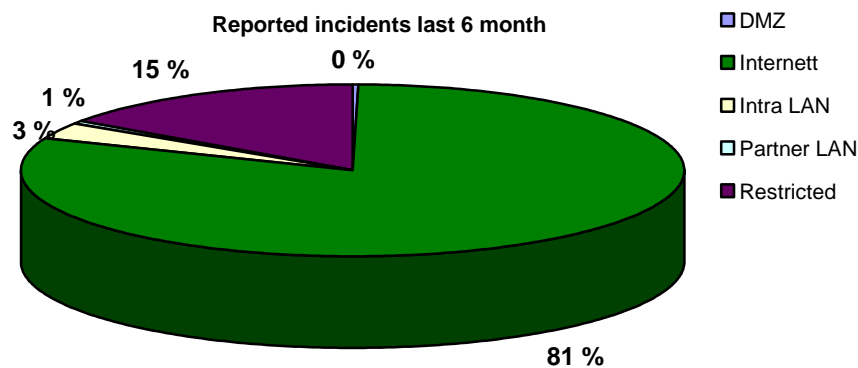


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

As in previous periods, there has been a large amount of alerts as a result of activity from the Internet, though we have seen a little less activity this month than earlier. Most of the activity is attacks against customer within the financial sector, where the attacker’s goal is to gain money. There has also been several alerts from “restricted” segments. All traffic within restricted segments are seen as severe if it violate with the normal traffic pattern.

**REPORTED INCIDENTS**

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



The main percentage of reported incidents from the Internet is mainly directed attacks towards financial institutions.

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

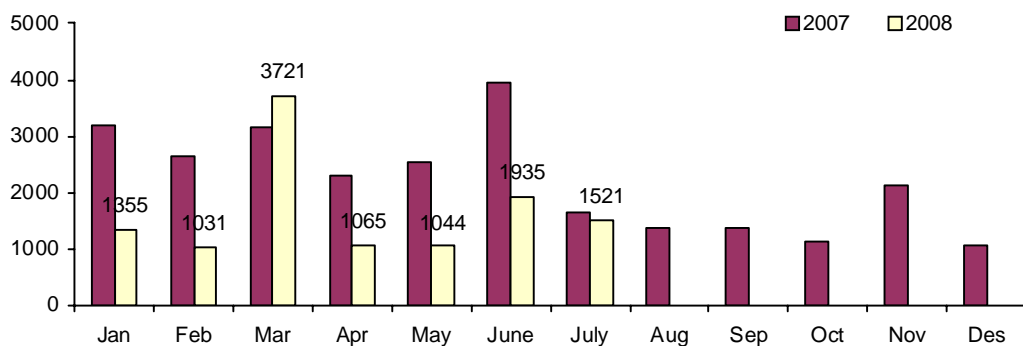
## THREAT LEVEL

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.

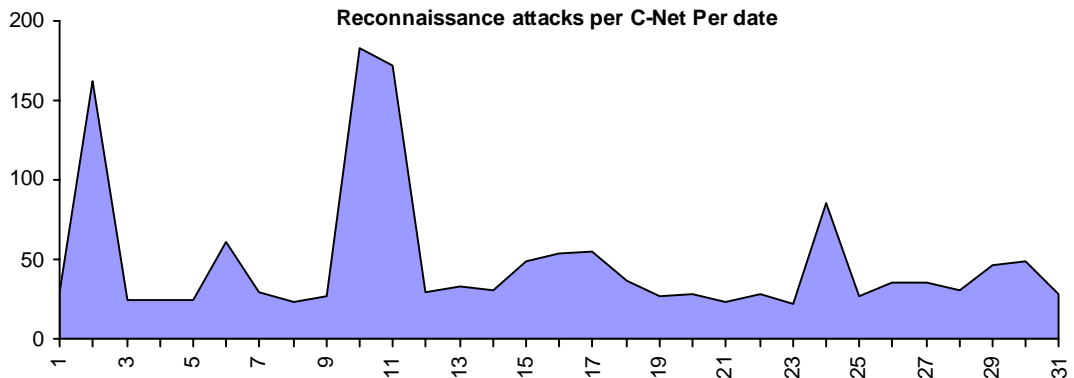
### RECONNAISSANCE ATTACKS JULY 2008

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.

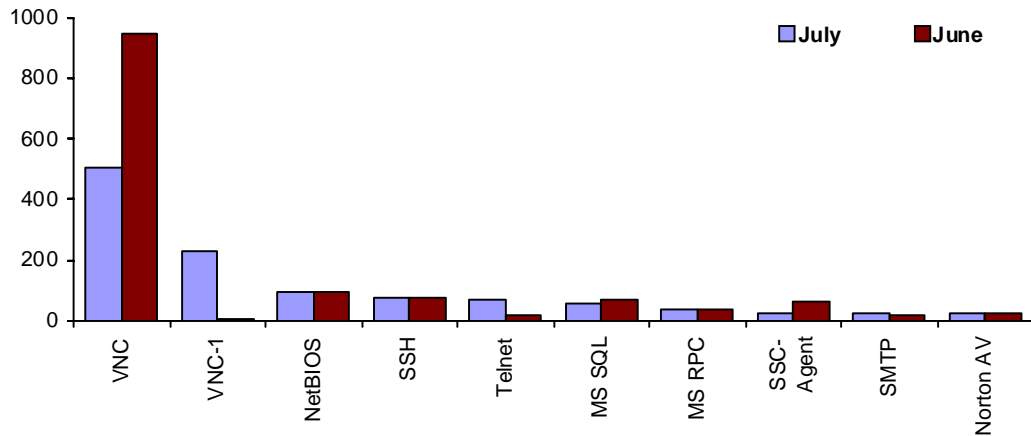
**Reconnaissance attacks per monitored C-Net**



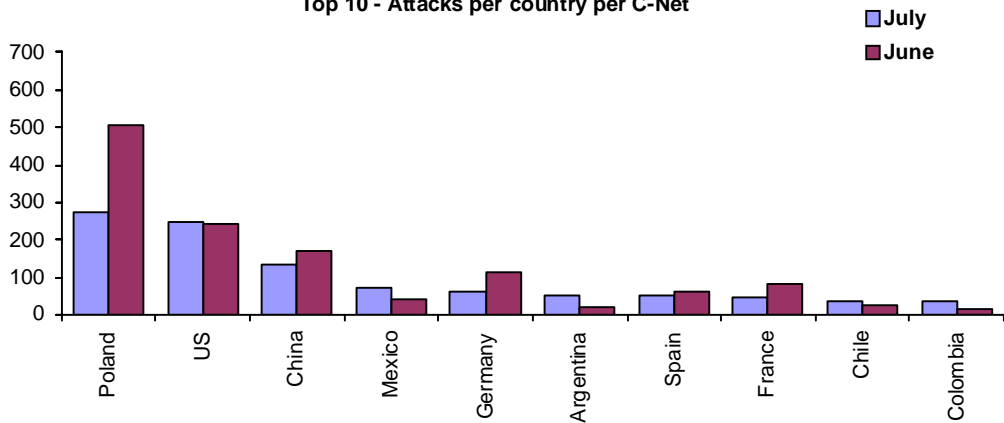
**Reconnaissance attacks per C-Net Per date**



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



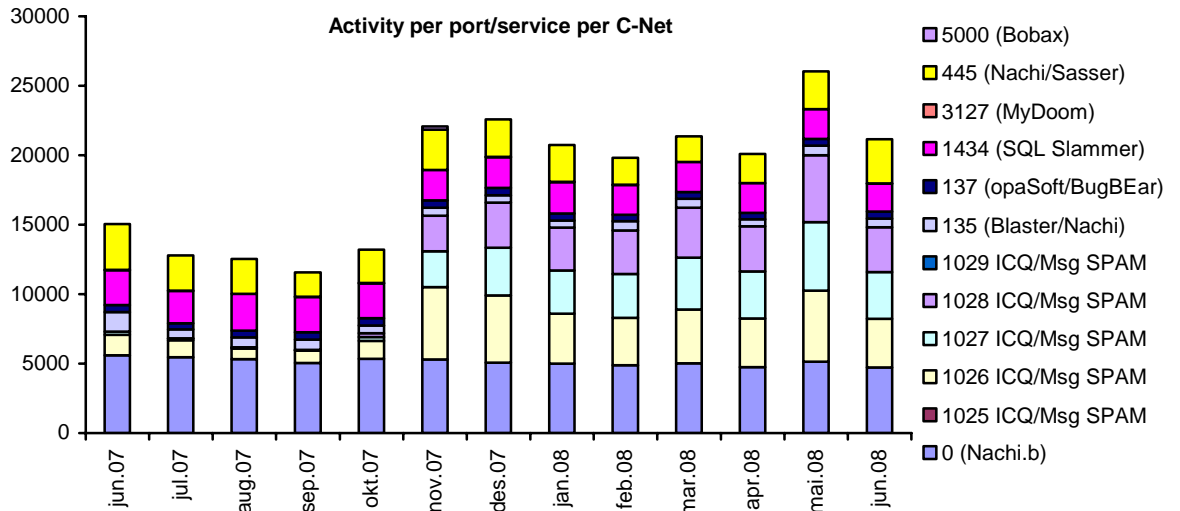
**Top 10 - Attacks per country per C-Net**



Compared to last month, it is observed a small decrease in number of reconnaissance attack. Last month there was a lot of activity towards the VNC service. This service is still hit in a large scale, but not as much as previous month. It is scans for VNC that are the reason for all the tops we see in the statistic "Per date". Otherwise there has been an increase in activity towards VNC-1. Poland is the source of the majority of the VNC and VNC-1 scans.

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.



The activity against the different services in the statistic above remains at a relatively stable level. As in previous periods, we see that Msg Spam is the most frequent type of incident within this category.