

# SECURITY THREATS AND TRENDS

## JULY 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 summary of malware trends the first half-year of 2008.

The alert statistics show that most of the alerts are triggered by attacks from outside the customer's network. Secode observes that the financial sector is hit by more attacks than other sectors.

There has been an increase in number of reconnaissance attacks this period, mainly because of increased activity from infected computers in Poland.

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 – MORE MALWARE .....</b>	<b>7</b>
2008 SO FAR .....	7
MALWARE WORTH NOTICING .....	7
KILDER.....	8
<b>ALERT STATISTIC.....</b>	<b>9</b>
HANDLED ALERTS .....	9
REPORTED INCIDENTS.....	10
<b>THREAT LEVEL.....</b>	<b>11</b>
RECONNAISSANCE ATTACKS JUNE 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

Important Opera Update

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

VLC Media Player Integer Overflow In Processing WAV Files

<http://www.videolan.org/vlc/>

Mozilla Products Remote Code Execution And Security Bypass Issues

<http://www.mozilla.com/firefox/>

Internet Explorer 6 Cross-Domain Scripting Vulnerability

<http://www.f-secure.com/weblog/archives/00001463.html>

Nortel Media Processing Server OpensSSL Multiple Vulnerabilities

<http://support.nortel.com/go/main.jsp?cscat=BLTNDetail&id=738400>

<http://support.nortel.com/go/main.jsp?cscat=BLTNDetail&id=738962>

Fedora Update For Ruby

<https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00925.html>

<https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00937.html>

HP-UX HP CIFS Server Multiple Vulnerabilities

[http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr\\_na-c01475657](http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657)

Adobe Reader And Acrobat 8.1.2 Security Update

<http://www.adobe.com/support/security/bulletins/apsb08-15.html>

Apple Safari Code Execution And Information Disclosure Vulnerabilities

<http://www.apple.com/support/downloads/safari312forwindows.html>

Apple Mac OS X Command Execution and Security Bypass Issues

<http://www.frsirt.com/english/advisories/2008/1697>

Updates to VMware resolve critical security issues

<http://www.vmware.com/security/advisories/VMSA-2008-0008.html>

### IN THE NEWS

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)

Researcher Faults Apple iPhone On Security Updates

[http://news.cnet.com/8301-10789\\_3-9984017-57.html?tag=cd.blog](http://news.cnet.com/8301-10789_3-9984017-57.html?tag=cd.blog)

Unstructured Data At Risk In Most Firms, Survey Finds

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage&articleId=9105818&taxonomyId=19&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage&articleId=9105818&taxonomyId=19&intsrc=kc_top)

Recent Potential Email And Web Threats

<http://www.mxlogic.com/pdf/forecast/threatforecast0708.pdf>

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>

Tech Giants Team Up On Security  
<http://www.vnunet.com/vnunet/news/2220277/tech-giants-team-security>

Intelligent Access Control For Wireless LANS  
<http://www.net-security.org/secworld.php?id=6264>

The Evil Side Of Google? Exploring Google's User Data Collection  
<http://www.seomoz.org/blog/the-evil-side-of-google-exploring-googles-user-data-collection>

Top 15 Free SQL Injection Scanners  
<http://www.security-hacks.com/2007/05/18/top-15-free-sql-injection-scanners>

IT Attacks: Insidersvs. Outsiders  
[http://www.schneier.com/blog/archives/2008/06/it\\_attacks\\_insi.html](http://www.schneier.com/blog/archives/2008/06/it_attacks_insi.html)

Hyper-V vs. VMWare  
<http://www.computerworld.com.au/index.php/id:134302705:fp:16:fpid:2>

What Privacy Policy  
[http://www.forbes.com/technology/2008/06/21/privacy-security-marketing-tech-security-cx\\_ag\\_0623privacy.html](http://www.forbes.com/technology/2008/06/21/privacy-security-marketing-tech-security-cx_ag_0623privacy.html)

Most Corporate Networks Vulnerable To Cyberattacks  
<http://www.networkworld.com/news/2008/062308-most-corporate-networks-vulnerable-to.html?hpg1=bn>

SSL Encryption Coming To The Pirate Bay  
[http://www.slyck.com/story1691\\_SSL\\_Encryption\\_Coming\\_to\\_The\\_Pirate\\_Bay](http://www.slyck.com/story1691_SSL_Encryption_Coming_to_The_Pirate_Bay)

Ruby Flaws Send Security Researchers Into Shock  
[http://www.theregister.co.uk/2008/06/23/group\\_patches\\_ruby/](http://www.theregister.co.uk/2008/06/23/group_patches_ruby/)

## FOCUS OF THE MONTH – MORE MALWARE

---

Malware ravage the Internet as never before. According to F-Secure has the number of malware detections increased from a total of 500 000 in 2007 to 900 000 so far in 2008. Never has it been observed a likewise fast increase. A contributing factor to this is probably that criminal groups see online crime as a lucrative and low risk alternative to robbery and break-ins out in the “real” world.

### 2008 SO FAR

First half-year of 2008 has been marked by more multi-component malware. Multi-component malware means malicious software consisting of several, complex components that usually attack different weaknesses within an enterprise. One simple example of multi-component malware is software that includes a keylogger, a Trojan and a backdoor (bot). In brief; several threats rolled into one.

Often multi-component malware involves a series of attack stages that use each other’s result and depend on one another. As a first stage, the malware writer may tap information from blogs or social networking sites as Facebook.

Security employees experience both opportunities and challenges by securing the enterprise against multi-component malware. The challenges are first of all that when an attack component is detected, it is hard to tell if this is the only one, or if it is part of a larger series of threats. And on the contrary, because of the dependency between the components, it may be easier to prevent an attack by blocking just one small part of the total attack stages.

Multi-component malware have existed for a long time, but the last half-year they have become considerably more complex, with several more components and more functionality to improve the odds for a successful attack. The malware also contains security technology to make detection harder, something which really shows the increasing professionalism in the criminal malware groups. The criminals also use IT infrastructure and enterprise system in their operations, underlining that they are in possession of large resources and expertise. The attacks become more directly targeted against enterprises, and sometimes even down to single persons. Defense against such personalized attacks are hard and require a strong security policy and –culture within the enterprise.

### MALWARE WORTH NOTICING

**Mebroot** is a very advanced example of malware, and are considered by F-Secure to be the stealthiest malware produces so far. Probably it has taken several months to develop this malware. Mebroot holds the number of system modifications down to a minimum and is very hard to detect within a system.

Mebroot’s most distinctive character is that it replaces the infected systems Master Boot Record (MBR). MBR holds the first code to be loaded and executed during the boot process. For F-Secure’s analysis of Mebroot, see <http://www.f-secure.com/weblog/archives/00001393.html>

**Zlob**, also known as DNSChanger, is a variant of malware that changes the settings in wireless routers. Zlob is camouflaged as a video decoder needed to watch content in particular web sites, but when downloading, you also get malware that changes the router settings so that all future web traffic are routed through a server controlled by the attacker. Zlob tries to get access to the router settings by guessing usernames and password. This guessing is based on built-in list of default usernames/password.

Security researchers have for long warned that attack against hardware routers can be built into malware, but this variant of Zlob is probably the first case where such functionality is released in the wild. First of all this is worrying because previous variants of Zlob are one of the most common malware downloaded to Windows machines. In addition, after an infection, it won't be sufficient to remove Zlob from the compromised computer; the system will stay infected until the router itself is reset. If several computers use the same router, they all will suffer under the infection even if it is only one computer that has downloaded Zlob.

The last month it is also observed at least two cases of **Apple OS Trojans**. These have arisen after the publishing of several severe vulnerabilities in OS X. The most critical security hole is in Apple Remote Desktop Agent (ARDAgent). Exploitation of this vulnerability can lead to malware being installed at a MAC without having the user to enter administrator password. Since the publishing at Slashdot, it has circulated exploits at the Internet. By infection of the MAC Trojan, it is installed a keylogger at the system, together with a server for remote access and a DNS service to make MAC easy to find. It is uncertain how widespread this Trojan is.

## KILDER

- [1] F-Secure IT Security Threat Summary for the First Half of 2008  
<http://www.f-secure.com/2008/1/index.html>
- [2] Malware Silently Alters Wireless Router Settings  
[http://blog.washingtonpost.com/securityfix/2008/06/malware\\_silently\\_alters\\_wirele\\_1.html](http://blog.washingtonpost.com/securityfix/2008/06/malware_silently_alters_wirele_1.html)
- [3] The ARDAgent Security Hole: What you need to know  
<http://dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration>

## ALERT STATISTIC

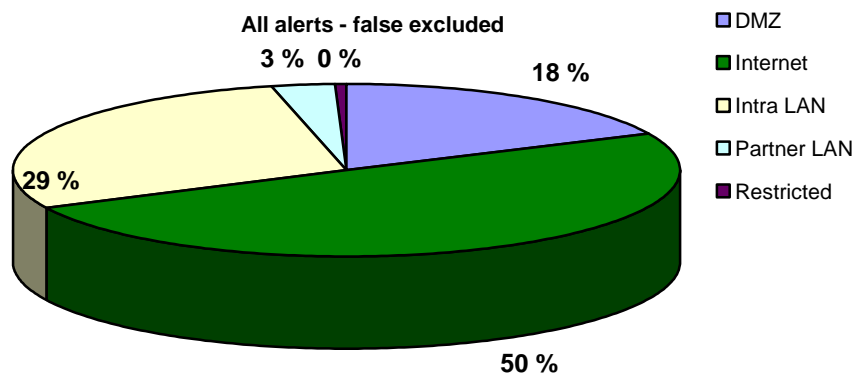
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

### HANDLED ALERTS

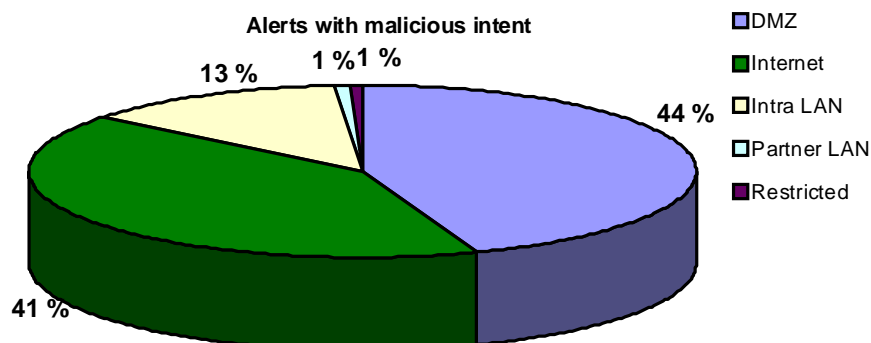
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

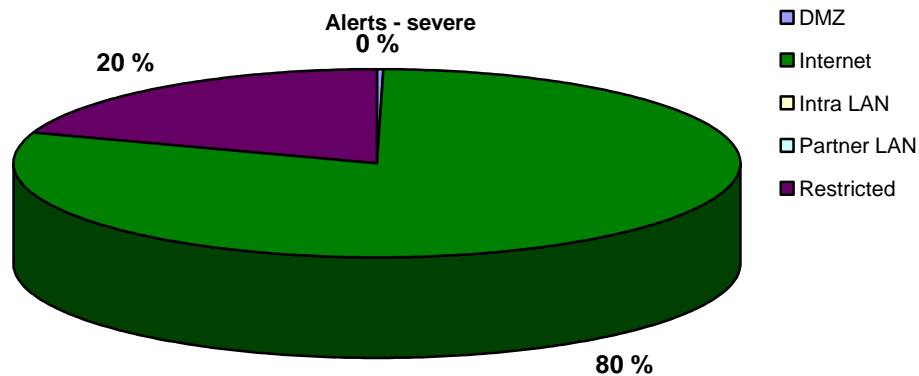
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

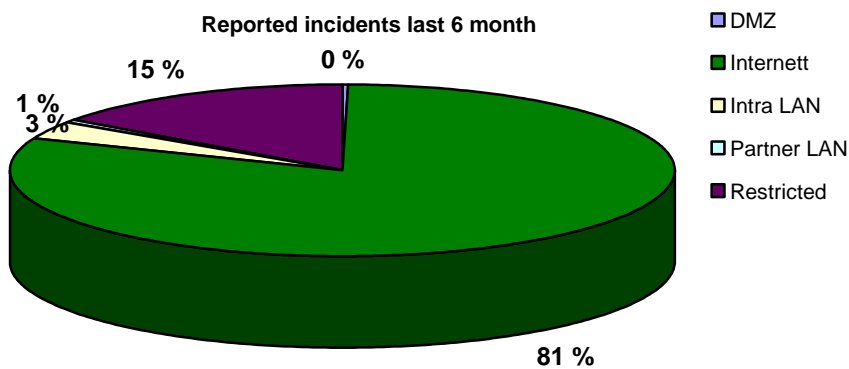


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

As in previous periods, there has been a large amount of alerts as a result of activity from the Internet. Most of this is directly targeted attacks against customers within the financial sector, where the attacker's goal is to gain money.

**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.

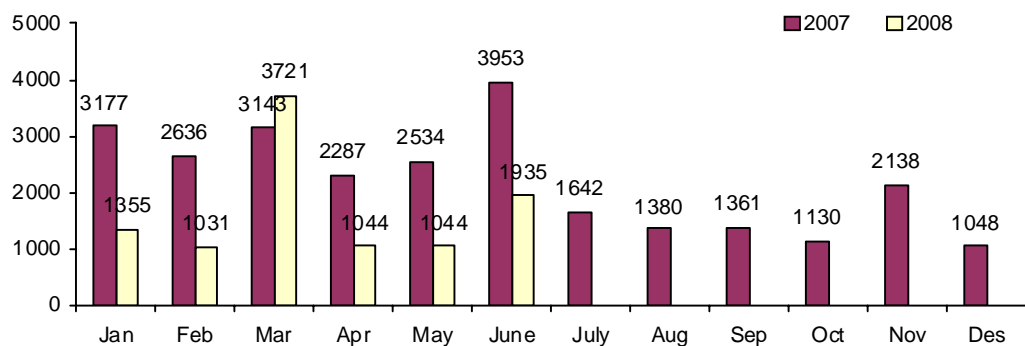
## THREAT LEVEL

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.

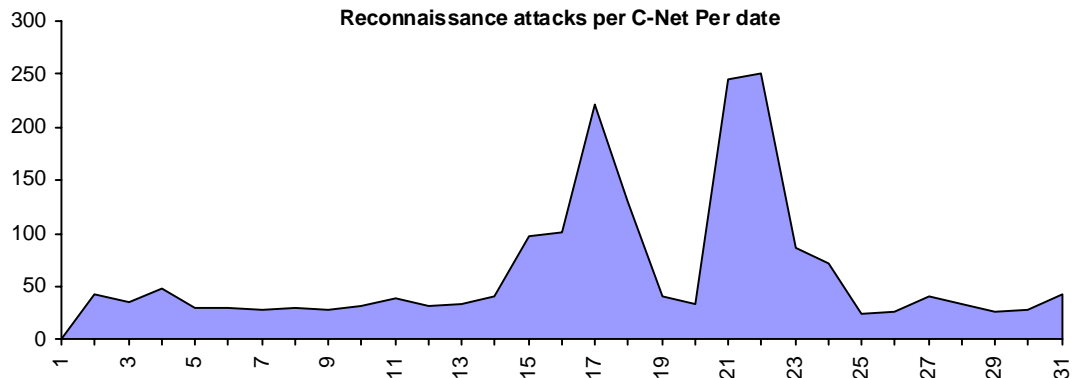
### RECONNAISSANCE ATTACKS JUNE 2008

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.

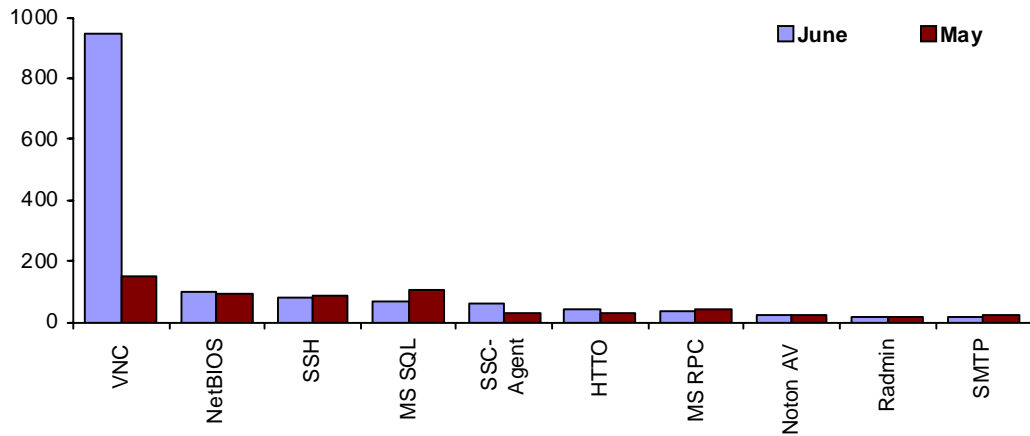
**Reconnaissance attacks per monitored C-Net**



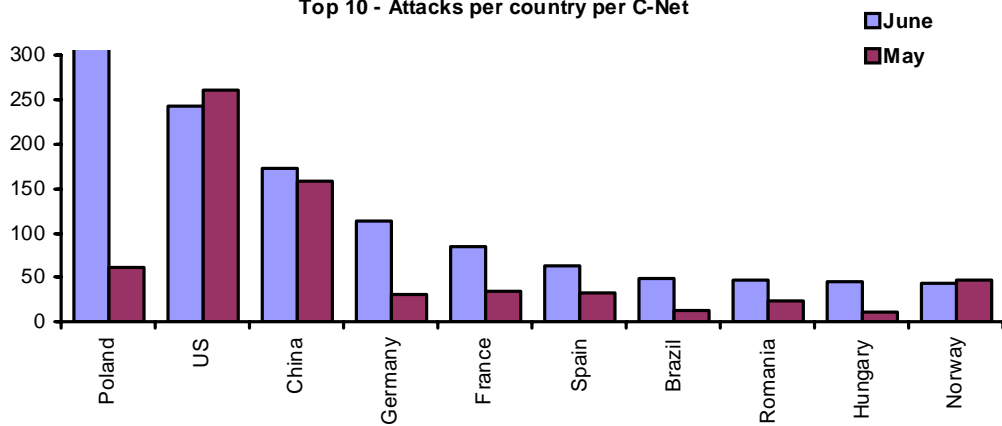
**Reconnaissance attacks per C-Net Per date**



Average top 10 incidents per C-Net



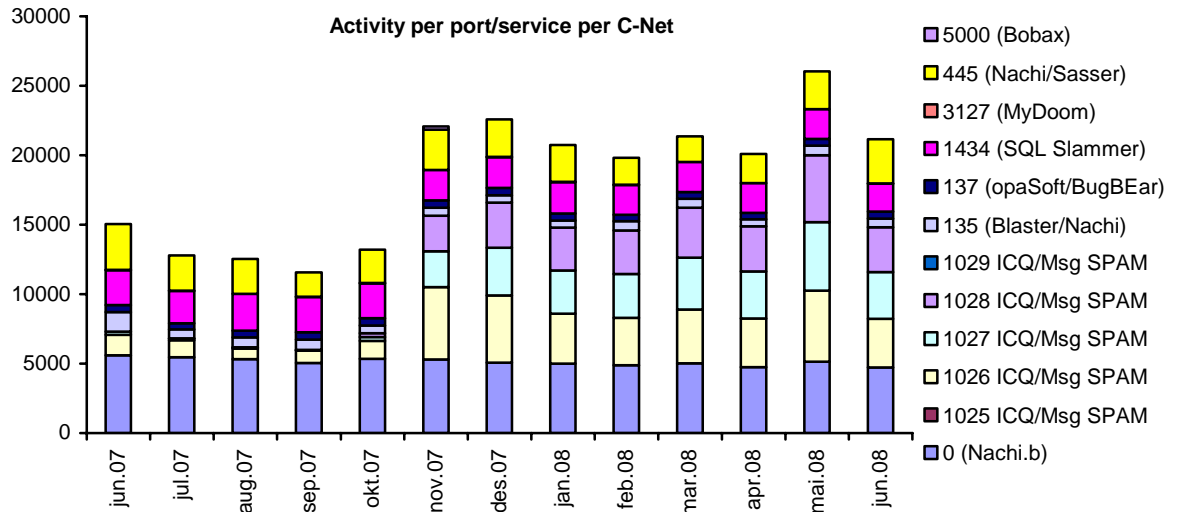
Top 10 - Attacks per country per C-Net



It is observed an increase in number of reconnaissance attacks this month, but compared to the same period last year; the activity level is still at a low level. The increase observed in June 2008, are due to several scans for the VNC service from infected networks in Poland.

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.