

SECURITY THREATS AND TRENDS

MAY 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 of the Kraken bot net – so far the biggest bot net detected.

The alert statistics show that most of the alerts are triggered by attacks from outside the customer's network. These attacks are especially targeted against customer within the financial sector.

It has been a decrease in reconnaissance attacks this month, mainly because of less activity towards the VNC service. Spam and Internet worms remain at a stable level.

TABLE OF CONTENTS

INTRODUCTION	4
NEWS OF THE MONTH	5
PUBLISHED VULNERABILITIES	5
IN THE NEWS.....	6
FOCUS OF THE MONTH – KRAKEN BOT NET	8
KRAKEN BOTNET	8
A MORALLY DILEMMA	8
USE BAD TO DO GOOD	9
KILDER	9
ALERT STATISTIC.....	10
HANDLED ALERTS	10
REPORTED INCIDENTS.....	11
THREAT LEVEL.....	12
RECONNAISSANCE ATTACKS APRIL 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 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. 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

Novell Groupwise Buffer Overflow in 'MailTo:' ULS handler lets remote users execute arbitrary code.

<http://securitytracker.com/alerts/2008/Apr/1019942.html>

IBM Lotus Expeditor URI hanler command execution vulnerability

<http://www.securityfocus.com/bid/28926/info>

A new class of vulnerability in Oracle: Lateral SQL injection

<http://www.databasesecurity.com/dbsec/lateral-sql-injection.pdf>

CA Secure Content Manager ECSQDMD Daemon can be crashed by remote users

<http://aluigi.altervista.org/adv/ecsqdamn-adv.txt>

Firefly Media Server Content Length Buffer overflow

http://sourceforge.net/project/showfiles.php?group_id=98211&package_id=105189&release_id=593465

OpenOffice Multiple Code Execution vulnerabilities

<http://www.openoffice.org/>

Clam AntiVirus Heap Overflow in Processing PeSpin Packed Files Lets Remote users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Apr/1019851.html>

IBM Lotus Notes Buffer Overflows in Applix Viewer Lets Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Apr/1019844.html>

IBM Lotus Notes Buffer Overflows in HTML Speed Reader Lets Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Apr/1019843.html>

IBM Lotus Notes Heap Overflows in EML Reader Lets Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Apr/1019842.html>

IBM Lotus Notes Stack Overflows in Folio Flat File Viewer Lets Remote Users Execute Arbitrary Code

<http://securitytracker.com/alerts/2008/Apr/1019841.html>

HP OpenView Network Node Manager Input Validation Flaw in 'OpenView5.exe' Lets Remote Users Traverse the Directory

Link: <http://securitytracker.com/alerts/2008/Apr/1019838.html>

HP OpenView Network Node Manager ovalarmsrv and ovtopmd Bugs Let Remote Users Deny Service

<http://securitytracker.com/alerts/2008/Apr/1019839.html>

Critical Hole in Cisco products

<http://www.heise-online.co.uk/news/Critical-hole-in-Cisco-products--/110481>

Oracle warns of critical DB server vulnerabilities

<http://www.eweek.com/c/a/Security/Oracle-Warns-of-Critical-DB-Server-Vulnerabilities/>

IN THE NEWS

Whitehats tackle the great botnet dilemma

http://www.theregister.co.uk/2008/04/29/kraken_botnet_infiltrated/

Malware carries end-user agreement

<http://www.vnunet.com/vnunet/news/2215490/malware-carries-user-agreement>

the new e-spying threat

http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

FSA warns banks: Shap up on security

<http://news.zdnet.co.uk/security/0,1000000189,39406491,00.htm>

Interop labs test result: Microsoft gets IT NAC act together

www.networkworld.com/research/2008/042808-ilabs-nac.html?fsrc=rss-security

Bluetooth Security danger ignored, say experts

<http://news.zdnet.co.uk/security/0,1000000189,39397480,00.htm>

Patches pose significant risk, researchers say

<http://www.securityfocus.com/news/11514>

Procure and Microsoft team up on security

<http://news.zdnet.co.uk/security/0,1000000189,39397451,00.htm>

SSMTP: A simple alternative to SendMail

<http://www.linux.com/feature/132006>

The cybercrime economy

<http://www.informationweek.com>

The rise of the malware mafia

http://www.theregister.co.uk/2008/04/11/organized_crime_embraces_net/

Gartner: Windows collapsing under own weights

<http://news.zdnet.co.uk/software/0,1000000121,39384073,00.htm>

Every second web application contains between one and ten holes

<http://www.heise-online.co.uk/news/Every-second-web-application-contains-between-one-and-ten-holes--/110515>

"The security business has no future" says IBM

<http://www.itpro.co.uk/security/news/186540/the-security-business-has-no-future-says-ibm.html>

<http://www.scmagazineus.com/From-RSA-Point-security-products-doomed-exhibitors-say/article/108801/>

New warning over imminent Internet meltdown

<http://www.computerworlduk.com/management/online/isp/news/index.cfm?RSS&NewsId=8384>

New attack kit targets bag of ActiveX bugs

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9075378&intsrc=hm_list

New crimeware-As-A-Service market thriving

http://www.darkreading.com/document.asp?doc_id=150319&WT.svl=news1_3

Europe asks ISPs to help battle cybercrime

<http://www.securityfocus.com/brief/714>

<http://www.coe.int>

Web attacks wont's stop

<http://www.computerworld.com.au/index.php?id=1562691283&eid=-144>

Unusual banking Trojan found today

<http://www.f-secure.com/weblog/archives/00001411.html>

FOCUS OF THE MONTH – KRAKEN BOT NET

With a view to the last month's news, this article sets new focus at bot net, and especially the Kraken bot net.

Several researches which attended the RSA Security Conference in San Francisco in the beginning of April, claimed that bot net is the biggest threat at today's internet. This is mainly because of the Ddos threat that increases proportional with the size of the zombie networks.

KRAKEN BOTNET

The Kraken bot, which share name with the legendary sea monster, was in April estimated to have created the largest bot net ever. Accurate size is impossible to calculate, and it has circulated several different versions regarding it's size. Still, the reports say that Kraken have created a bot net twice as large as the Storm network that is previously thought to be the largest bot net.

Kraken is special in it's method to attempt to avoid antivirus, firewall and IPS solutions. Kraken take use of a domain generator algorithm, which is designed to allow that infected computers search for possible control servers, instead of using one single server. Infected computers communicate to their control server through HTTP instead of IRC, because IRC normally is thought to be more suspect. Additional, the commands sent from a Kraken infected computer to the control server, is encrypted.

The latest variant of Kraken was probably distributed by MSN. The Kraken contains a method to generate different random filenames to the infected files. This makes it more difficult for spam- and antivirus filter.

A MORALLY DILEMMA

The Kraken is calculated to be the largest bot net ever, something that made to researches at TippingPoint want to try to infiltrate the bot net. This has ended in a very interesting morally dilemma.

The two researches Pedram Amini and Cody Pierce accomplished to create a fake Kraken server that could take control over Kraken infected computers. Straight away when the server was up and running, zombie computers from all over the world tried to connect to this server. During a week, it was recorded connection attempt from 25 000 unique computers, a number which still is growing. From this, TippingPoint think that the entire Kraken net might consist of up to 600 000 zombies, and that their two researches can take control over up to 14 % of the total Kraken bot net.

The possibility to take control over so many zombies, constitute to a morally dilemma: shall this control be used to clean ten thousands of infected computers, or shall one just let them be?

It is inside disagreement in TippingPoint of what they are to do. The pros think that they should distribute an update that removes Kraken from the infected computers since they now have the seldom opportunity to do something with the largest, active bot net. With simple means a large amount of spam spreading computers can be removed. The opponents are sceptical to what such an update can bring, especially in connection with what an eventually system crash can result in for the unknowing user.

USE BAD TO DO GOOD

To use same techniques as the bad guys to do good work is often up to discussion. Below follows a few examples from the last month's news on how the large threat of bot net can be dealt with:

- Possibility to install patches through control servers in bot net as mentioned in previous section. This method part from the friendly worms idea in the way that you loose control over friendly worms when they first is released, while you in this example can control and stop the updated whenever you want
- A team at University of Washington wants to fight bot nets by using swarms of good computers to neutralize the bad bot computers. Their system called Phaland, use large networks of computers to shield the protected server. All information to the server must pass through the protective computers, instead of the server being direct accessed. For more information, see: <http://technology.newscientist.com/article/dn13753-to-defeat-a-malicious-botnet-build-a-friendly-one.html>
- Bot net Pollution is another method to fight bot nets; vulnerabilities in the bot net's p2p protocol are exploited to add polluted content into the bot net to disrupt the communication between the bots. This method is tested at the Storm network with positive result. For more information, see http://www.darkreading.com/document.asp?doc_id=151862&f_src=drdaily

KILDER

- [1] Krakens
http://www.theregister.co.uk/2008/04/28/kraken_botnet/
- [2] Move over Storm – there's a bigger, stealthier botnet in town
http://www.theregister.co.uk/2008/04/07/kraken_botnet_menace/
- [2] Kraken botnet infiltration
<http://dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration>

ALERT STATISTIC

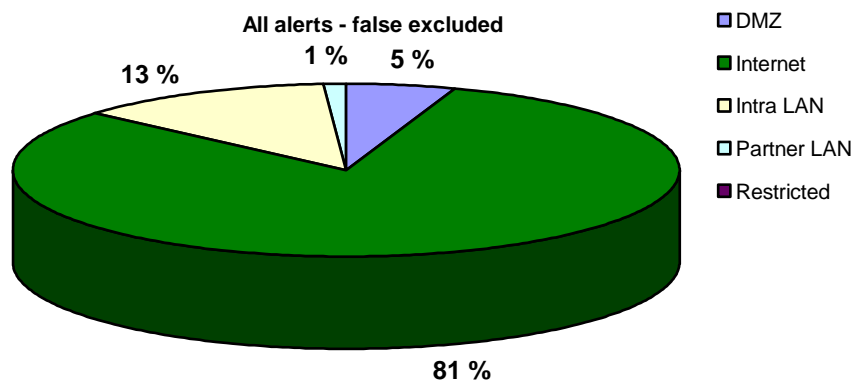
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

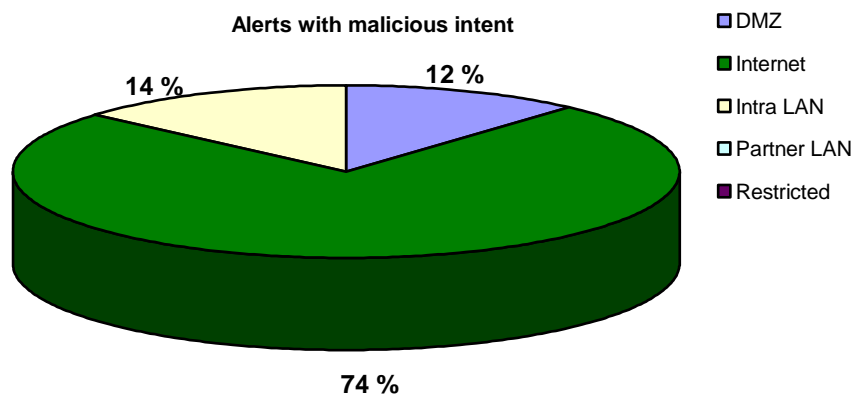
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

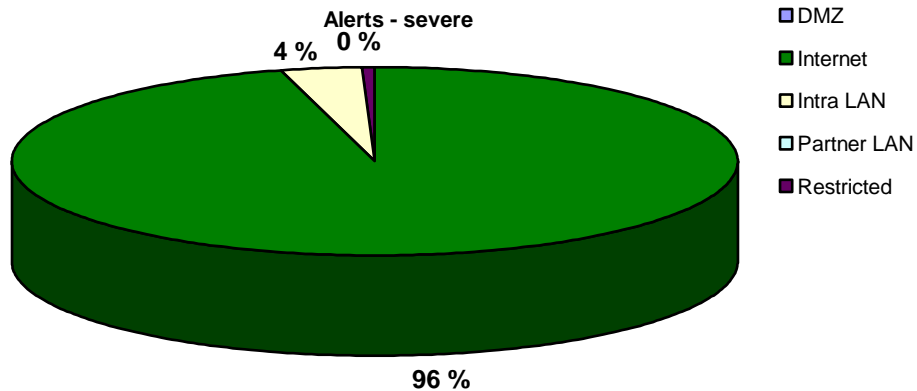
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

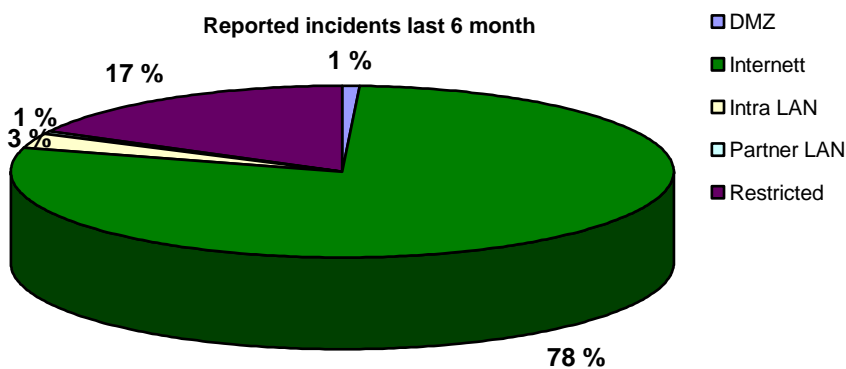


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

There have been most alerts caused by attacks from the Internet this month, and the majority of these are parts of directed attacks towards 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.

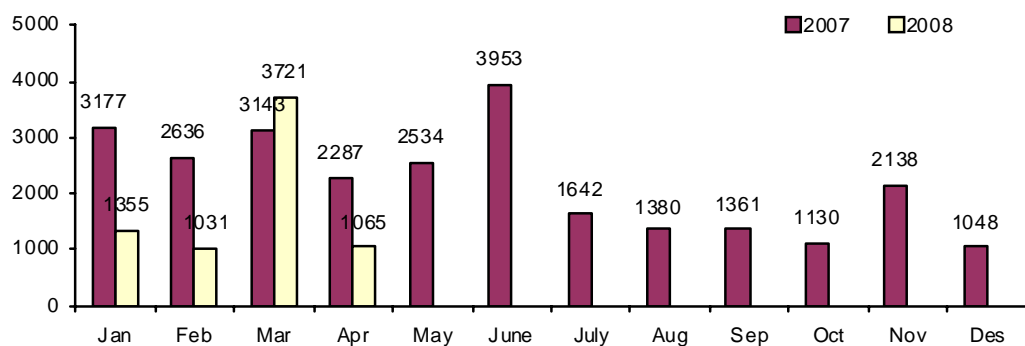
THREAT LEVEL

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.

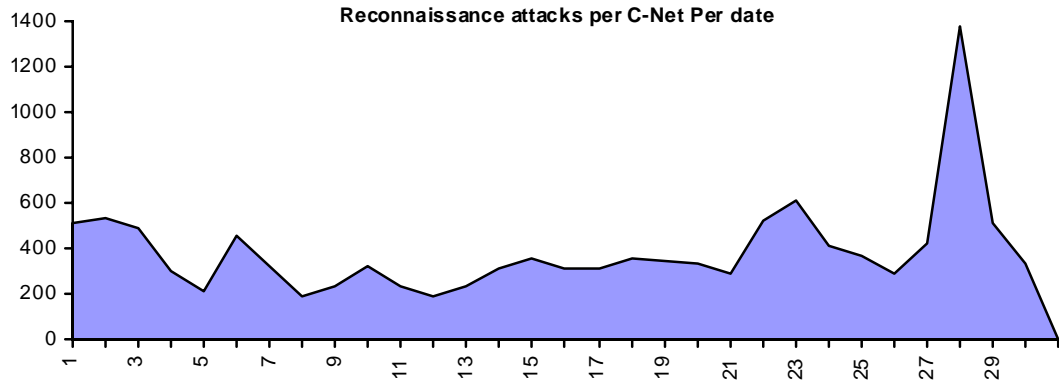
RECONNAISSANCE ATTACKS APRIL 2008

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.

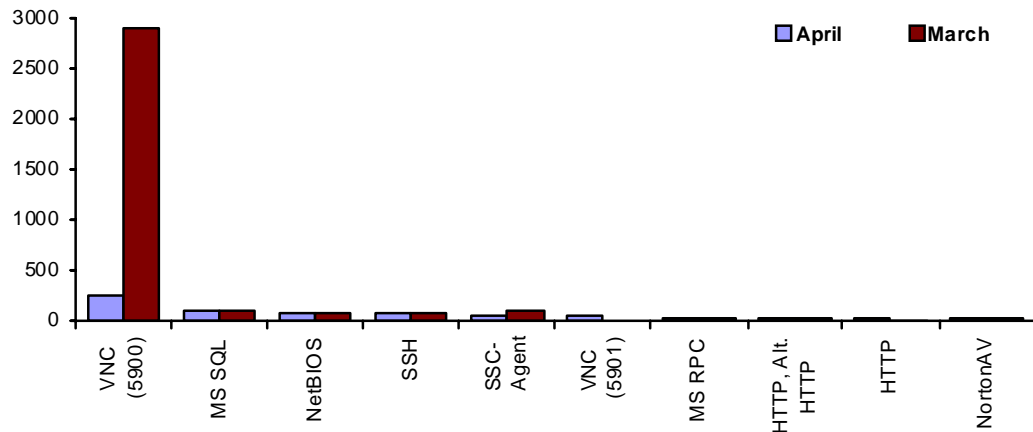
Reconnaissance attacks per monitored C-Net



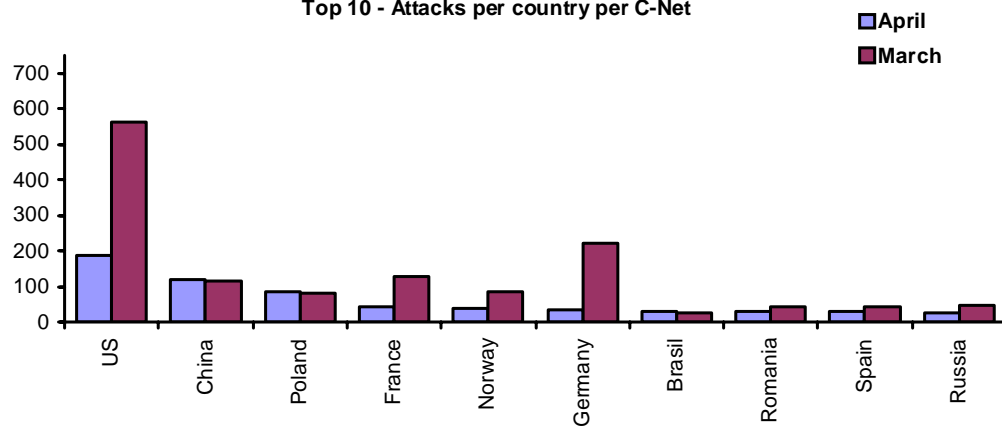
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



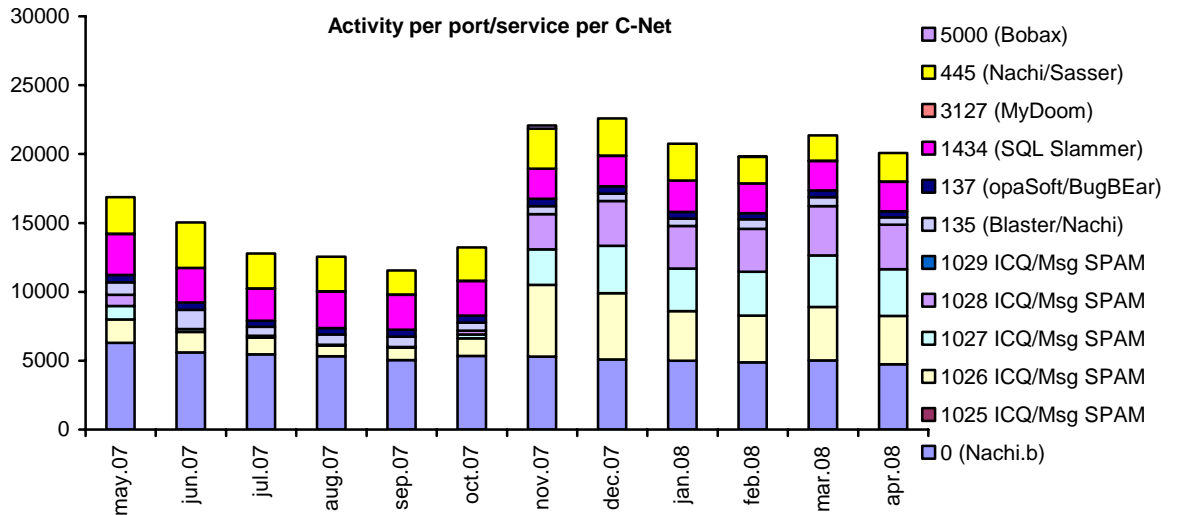
Top 10 - Attacks per country per C-Net



The total number of reconnaissance attacks has shown a decrease this month. This is caused by lesser activity targeting the VNC service. However, VNC is still the most frequent searched service. A large portion of the VNC scans was recorded 28th of April, something that clearly is shown in the statistic above.

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 towards the different services in the statistic above remains at a relatively stable level. As for previous periods, Msg SPAM is still the most targeted service.