

SECURITY THREATS AND TRENDS

APRIL 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 taking a short look at piracy.

The Alert Statistic shows that most alerts behind attacks have their origin outside the customers net this month. The attacks are directed at customers, mostly towards financial intentions.

There has been an increase in the number of reconnaissance attacks this month, mostly because there was a great deal of searches towards VNC in the middle of the month. These searches have also had an impact on the statistics for the country of origin.

Spamming attempts and activity from Internet worms remains 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 – THE WAR AGAINST PIRACY.....	8
PIRACY.....	8
MONEY PERSPECTIVE.....	8
WAR STRATEGIES	9
WHAT ABOUT THE FUTURE?	9
SOURCES.....	9
ALERT STATISTIC.....	10
HANDLED ALERTS	10
REPORTED INCIDENTS.....	11
THREAT LEVEL.....	12
RECONNAISSANCE ATTACKS MARCH 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

phpMyAdmin "\$_REQUEST" SQL Injection Vulnerability
<http://secunia.com/advisories/29200/>

Squid Analysis Report Generator Buffer Overflow
http://sourceforge.net/project/shownotes.php?release_id=581212&group_id=68910

Adobe Acrobat Temporary File Race Condition in "acroread" Wrapper Script May Let Local Users Gain Elevated Privileges
<http://securitytracker.com/alerts/2008/Mar/1019539.html>

Sun Java Multiple Code Execution and Security Bypass Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/0770>

CheckPoint VPN-1 UTM Edge "user" Cross Site Scripting Vulnerability
<http://www.frsirt.com/english/advisories/2008/0788>

Red Hat Enterprise Linux Default IPSec Script Uses IKE Aggressive Mode
<http://www.ernw.de/download/pskattack.pdf>

Panda Products cpoint.sys Privilege Escalation Vulnerabilities
<http://www.trapkit.de/advisories/TKADV2008-001.txt>

Citrix Presentation Server Clients Information Disclosure Vulnerability
<http://support.citrix.com/article/CTX116227>

Adobe Form Designer/Form Client Remote Buffer Overflow Vulnerabilities
http://www.adobe.com/support/products/enterprise/support_knowledge_center_formclient.html

Cisco User-Changeable Password Remote Cross-Site Scripting and Arbitrary Code Execution Vulnerabilities
http://www.recurity-labs.com/content/pub/RecurityLabs_Cisco_ACS_UCP_advisory.txt

McAfee ePolicy Orchestrator Format String Bug Lets Remote Users Execute Arbitrary Code
<http://securitytracker.com/alerts/2008/Mar/1019609.html>

Red Hat update for kernel
<http://secunia.com/advisories/29387/>

CA BrightStor ARCserve Backup List Control Code Execution Vulnerability
<http://milw0rm.com/exploits/5264>

Multiple F-Secure antivirus products archives code execution
<http://www.f-secure.com/security/fsc-2008-2.shtml>

Mozilla Firefox vulnerabilities

- Mozilla Firefox URL Bug Lets Remote Users Spoof HTTP Referer Values in Certain Cases
<http://securitytracker.com/alerts/2008/Mar/1019703.html>

- Mozilla Firefox XUL Popup Bug Lets Remote Users Spoof Tabbed Pages
<http://securitytracker.com/alerts/2008/Mar/1019700.html>
- Mozilla Firefox Bugs in JavaScript Engine and Layout Engine May Let Remote Users Execute Arbitrary Code
<http://securitytracker.com/alerts/2008/Mar/1019695.html>
- Mozilla Firefox JavaScript Bugs Let Remote Users Execute Arbitrary Code
<http://securitytracker.com/alerts/2008/Mar/1019694.html>

Wireshark Multiple Remote Denial of Service Vulnerabilities
<http://www.wireshark.org/security/wnpa-sec-2008-02.html>

IN THE NEWS

RBN 'Rizing'

<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080301>
<http://www.shadowserver.org/wiki/pmwiki.php?n=Information.Whitepapers>

Six botnets pump out 85 per cent of spam

<http://www.computerworld.com.au/index.php?id=481069848&eid=-6787>

The Untold Cyber War

http://www.huffingtonpost.com/karen-salmansohn/the-untold-cyber-war_b_89104.html

Hackers attack MySpace and Facebook

<http://www.vnunet.com/vnunet/news/2210932/buffer-overflow-hacks-target>

Hackers Test Their Viruses Prior to Release

<http://news.softpedia.com/news/Hackers-Test-their-Viruses-Prior-to-Release-80034.shtml>

Measuring Identity Theft at Top Banks

<http://repositories.cdlib.org/bclt/lts/44/>

Hack into a Windows PC - no password needed

<http://www.theage.com.au/news/security/hack-into-a-windows-pc--no-password-needed/2008/03/04/1204402423638.html>

The State of Spam - A Monthly Report – March 2008

http://eval.symantec.com/mktginfo/enterprise/other_resources/SpamReport_March08.pdf

Fraudsters piggyback on search engines

<http://www.securityfocus.com/brief/695>

Hospital donor files compromised

http://www.bendbulletin.com/apps/pbcs.dll/article?AID=/20080306/NEWS0107/803060442/1006&nav_category=NEWS0107

Linux tool speeds up police computer forensics

<http://news.zdnet.co.uk/software/0,1000000121,39363098,00.htm>

FBI admits to internet spying

<http://www.vnunet.com/vnunet/news/2211460/fbi-admits-internet-spying>

Security Products: Suites vs. Best-of-Breed

http://www.schneier.com/blog/archives/2008/03/security_produc_1.html

To Aim Ads, Web Is Keeping Closer Eye on You

http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=2&pagewanted=1&hp&oref=slogin

Battle Against Fast-Flux Botnets Intensifies

http://www.darkreading.com/document.asp?doc_id=148002&WT.svl=news1_2

The malware menace – but not as we know

http://www.securitypark.co.uk/security_article260742.html

Casino insider tells (almost) all about security

<http://www.computerworld.com.au/index.php/id;270726757;pp;3;fp;4194304;fpid;1>

FTP Hacking on the Rise

http://www.darkreading.com/document.asp?doc_id=148143&WT.svl=news1_2

Cyber-attack launched from 10,000 web pages

<http://itnews.com.au/News/71994,cyberattack-launched-from-10000-web-pages.aspx>

Security skills still most valuable to IT chiefs

<http://news.zdnet.co.uk/itmanagement/0,1000000308,39366037,00.htm>

Second mass hack exposed

<http://www.itnews.com.au/News/72214,second-mass-hack-exposed.aspx>

Analysis: Cyberattacks on Tibet groups

http://www.upi.com/International_Security/Emerging_Threats/Analysis/2008/03/24/analysis_cyberattacks_on_tibet_groups/9260/

Most sites still hack-able

http://weblog.infoworld.com/zeroday/archives/2008/03/web_site_hack_e.html?source=rss

Linux: A Tempting Target for Malware?

<http://www.linuxinsider.com/rsstory/62275.html>

Users Still Worst Enemy to Endpoint Security

<http://www.eweek.com/c/a/Security/Panel-Users-Still-Worst-Enemy-to-Endpoint-Security/>

FOCUS OF THE MONTH – THE WAR AGAINST PIRACY

The arguments against piracy are many, and most of them are met with arguments from “pirates”. In this report we will take a closer look at the pro and cons of piracy and how this affects the Internet security today.

PIRACY

There are many definitions for piracy. Piracy in this content is a copyright infringement of software, movies and music, or in more lay terms, the act of stealing or distributing copyrighted software, movies and music. The distribution channel is mostly the Internet, but may be other channels as well. In this report we only discuss Internet distributed material.

The two main industries that are fighting piracy is “Hollywood”, movies and TV-series included, and the music industry. The main reason for fighting piracy is that the industries are afraid of losing money.

Most young people will say that they do not see it as wrong to download pirated material, and many of them will also help distribute the material.

MONEY PERSPECTIVE

The music and movie industry are using millions of dollars every week to make new material. If they do not get a good income they can not spend as much money on making this material, and in both industries you have to spend money to make money. This is the main reason for their arguments against piracy. For every file that is downloaded they will in some way lose income, or they at least believe so. The fact that a recent survey showed that “pirates” were more eager at going to the cinema, and several surveys showing that “pirates” are using at least as much money as others on music, is telling us something else.

You could question why they go more to the movies or buy more music if they download it, and the reason is very clear. If you are not certain that you will like some kind of music, or a movie, you can listen to it or watch before you decide. In addition, we see that “pirates” download music, movies and TV-series they normally have not even heard about. By doing so they widen their horizon, and start listening to bands they never heard before or watching movies or TV-series they did not know about. This will in turn make them buy music and movies they normally would not buy, because they now have opened their eyes for some new band, TV-series or movie. Things they do not like will not be bought. However, it would not be bought if they had not downloaded it either.

Of course there are “pirates” that never buy a DVD or a CD. However the effect of those buying more music because they are able to listen to it in their own home before buying is greater.

When we talk about software the positive effect is great here too. Young people download and start using software they can not afford while they are in school. After several years of using some kind of software in their own private home, for school or other work, they would like to use the same software when they start working. As most companies do not accept their employees using pirated software, they now have to buy software .

Even if we can argue that it is in some way positive to let people download this material, it is impossible to make the industry see that. They want to let people listen to music, see a movie or use software for a small fee instead of letting piracy happen, so the fight against piracy is still going strong.

WAR STRATEGIES

There are several laws implemented around the world aiming to stop piracy. Norway has a pretty liberal law, letting people copy their CDs to give a copy to their family or their closest friends. This law is more liberal than the law or the directive EU established. France however, has a strict law. In France you are of course not allowed to copy CDs, and if you get caught distributing or downloading copyrighted material three times you may lose your Internet access for the rest of your life. The EU has recently voted against a suggestion similar to this law, which may cause trouble for this law.

Making governments implement laws is one way of fighting piracy; another way is making it more difficult to copy the material. Several kinds of copy protections have been tested and implemented during the years, to big protest from the buyers. Some copy protections have made it more or less impossible to play a CD in some CD players; DVD protections have made it difficult to use DVD players in PCs and so on.

Another way of fighting piracy has been to make files available for download for a small amount of money. However, to protect the files from being distributed further they have been "blocked", making it difficult for some to play it on their own MP3 players or other kind of players. Making some singles, episodes of a TV-series or a movie available for a small amount of time have however been successful.

The most noticeable difference for many has however been the "Piracy is a crime" campaign. This campaign is in short a campaign where they are using advertising in the media to tell people what piracy is, and why you should not do this. The "Piracy is a crime" commercial is shown before every movie screening at the movie theaters, or at as a commercial on a DVD. Several are annoyed about this campaign however, because people buying legitimate material are sick of seeing this commercial. And the real "pirates" are not eager movie buyers or movie goers, if we shall believe the industry itself.

WHAT ABOUT THE FUTURE?

Many believe that the industry will give in after a while, but it is more likely that they will take advantage of the situation. Releasing movies, TV-episodes, singles and so on for a short amount of time on different Internet channels. Getting people to start listening to a band, see a TV-series or get interested in a movie that way. Several music bands and TV-series are using this way of distribution already.

The war against piracy will continue in years to come, and we can only hope that the morals for "pirates" changes. That is probably the only way for the industry to win.

SOURCES

- [1] EU avviste utestengelse av fildelere (Norwegian)
<http://www.digi.no/php/art.php?id=519896>
- [2] Wikipedia – Copyright infringement
http://en.wikipedia.org/wiki/Copyright_infringement

ALERT STATISTIC

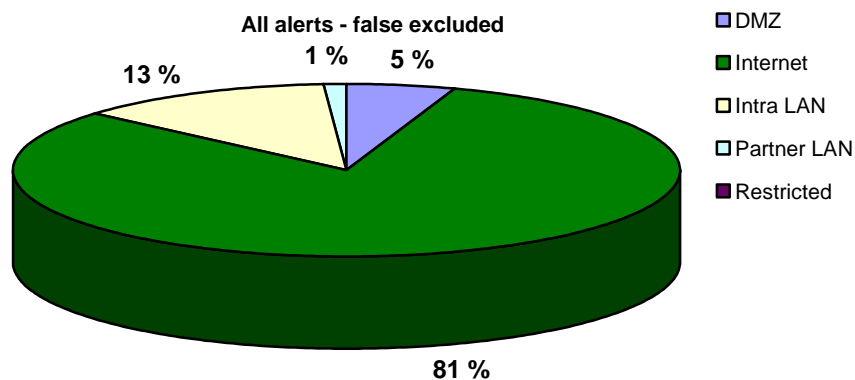
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

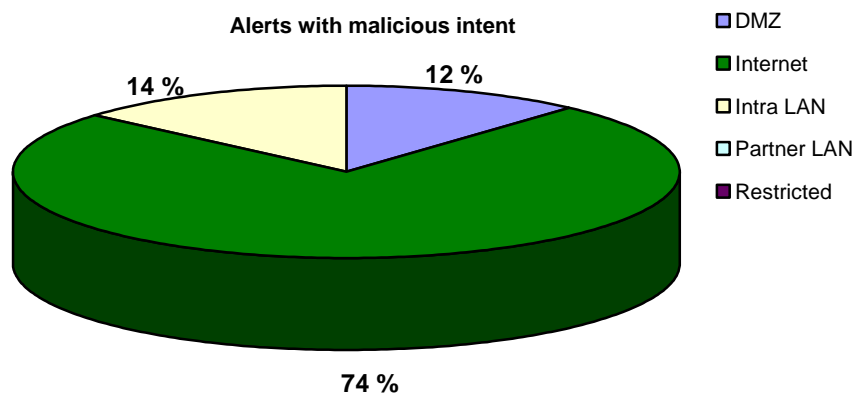
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

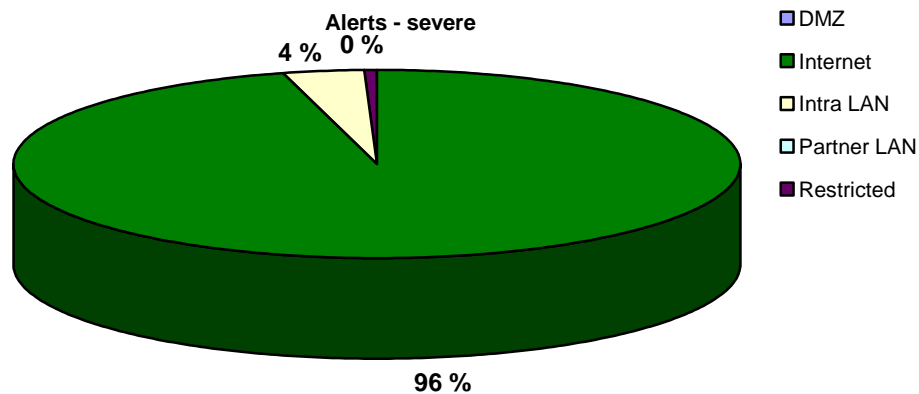
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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

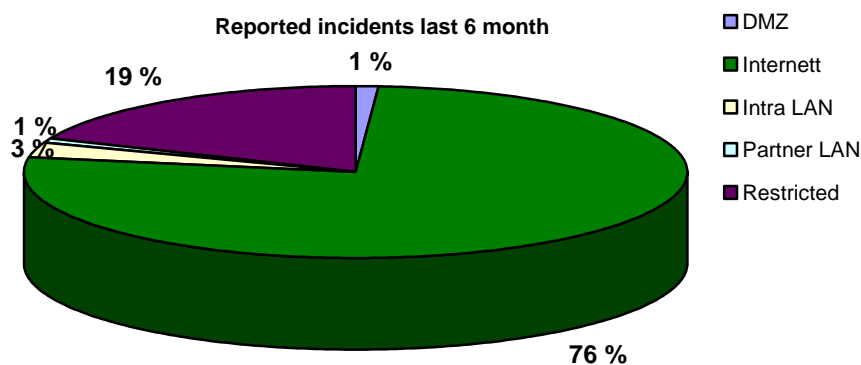


The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

There have been a lot of alerts from the Internet this month, and most of these alerts are part of directed attacks towards customers. In other words, these attacks are intended to attack that particular customer in order to get 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 with Internet origin is mainly directed attacks towards financial institutions.

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

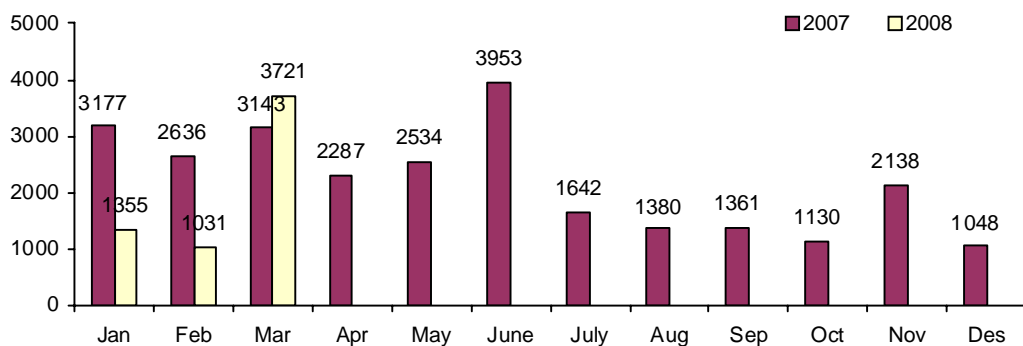
THREAT LEVEL

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.

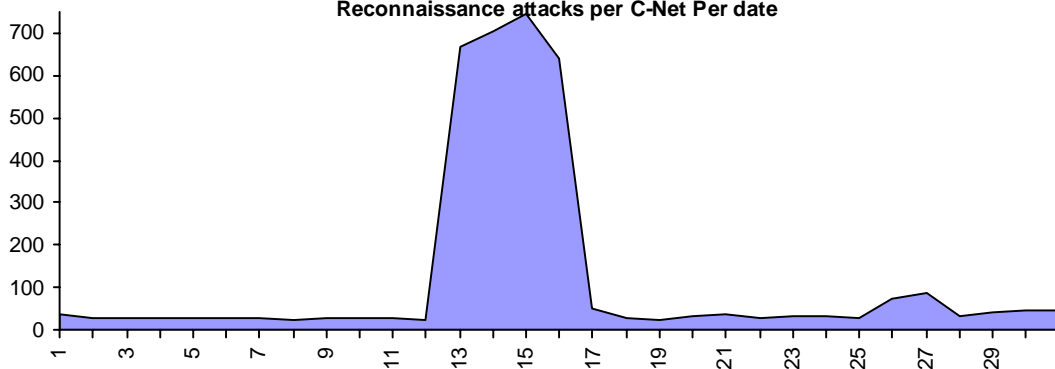
RECONNAISSANCE ATTACKS MARCH 2008

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.

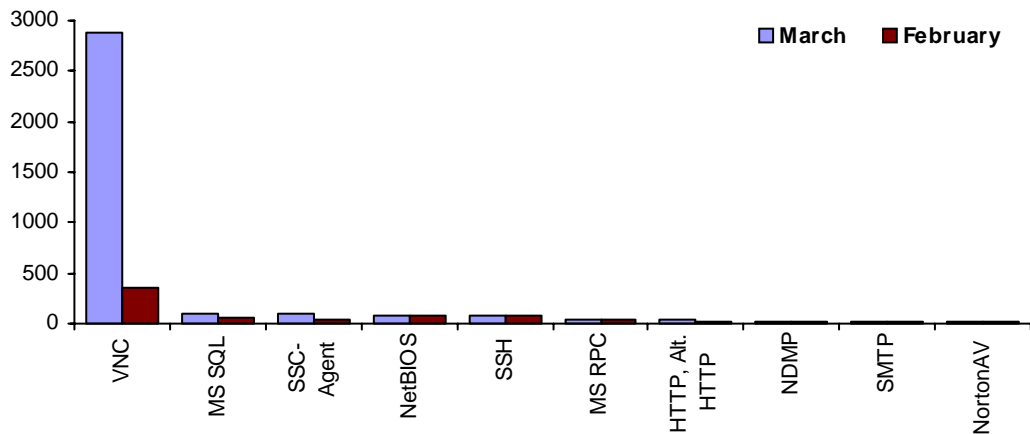
Reconnaissance attacks per monitored C-Net



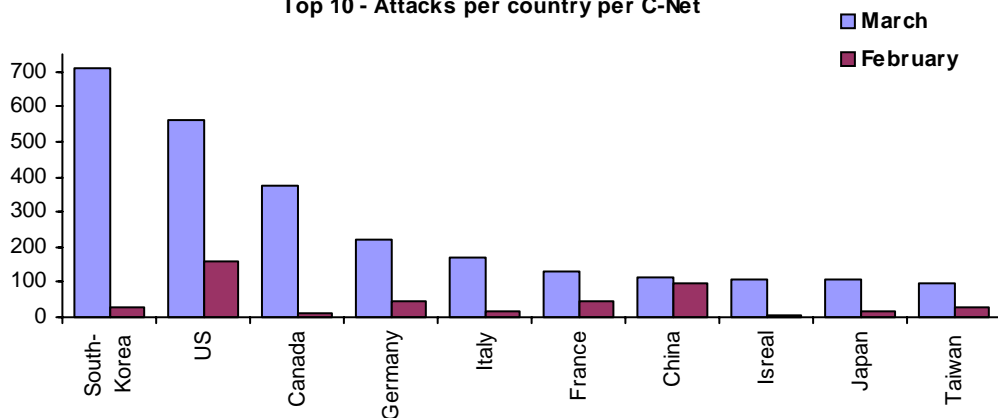
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net

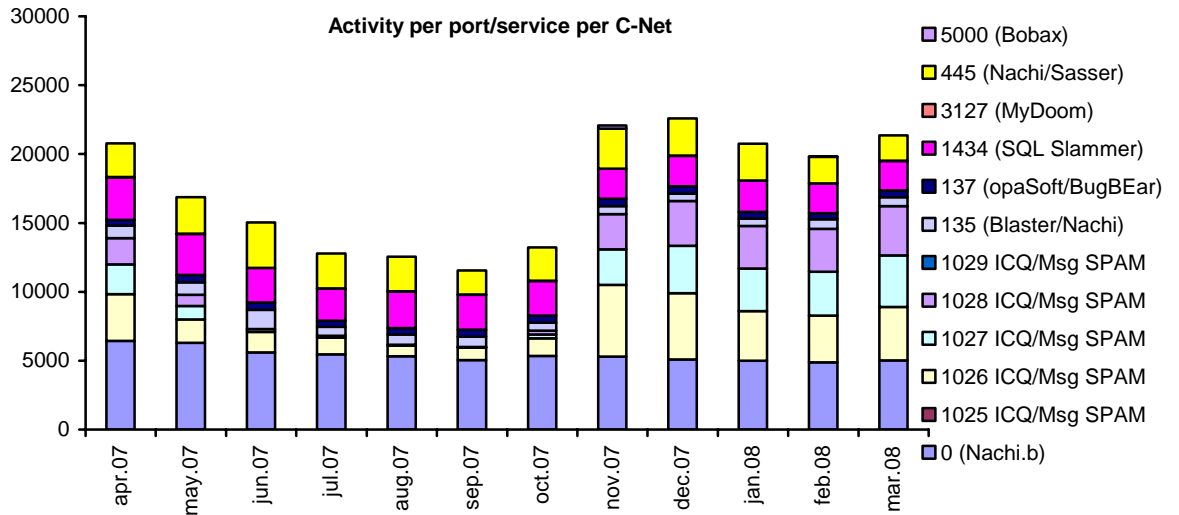


The number of reconnaissance attacks has been at a higher level this month than previous months. The reason for this change is that there has been a great deal of searches towards VNC from the 12th to the 17th of this month. We have not found why this service were attacked at this particular point, but the attacks came from several countries, and it may seem that a new exploit have been the reason of attack.

South-Korea were one of the most active countries behind the attacks towards VNC, and are therefore the most active country this month. The US, Canada and Germany follow and are also active in the VNC attacks.

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 we see that Msg SPAM is the most targeted services.