

SECURITY THREATS AND TRENDS

DECEMBER 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

In Decembers Focus of the Month we take a look at some of the trends we have seen the last year.

The alert statistic shows that most alerts occur in partner zone, but these are rarely severe. The most severe alerts this period has occurred from Internet, and are due to attacks towards web servers, mostly in financial institutions.

There have been a slight increase in the number of reconnaissance attacks. We see, however, that there is no difference from last month when it comes to attacks against VNC. Algeria have surprisingly entered the top 10 list of countries of origin.

Among spam/worm we see an increase in the traffic towards port 445 this month. This is due to new worms targeting this port, and then in particular W32.Downandup. A patch for this problem has been released by Microsoft.

TABLE OF CONTENTS

INTRODUCTION	4
NEWS OF THE MONTH	5
PUBLISHED VULNERABILITIES	5
IN THE NEWS.....	5
FOCUS OF THE MONTH – THE ART OF SECURITY WAR	7
ALERT STATISTIC.....	9
HANDLED ALERTS	9
REPORTED INCIDENTS.....	10
THREAT LEVEL.....	11
RECONNAISSANCE ATTACKS SEPTEMBER 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

Adobe Acrobat/Reader "util.printf()" Buffer Overflow
<http://secunia.com/advisories/29773/>

Novell Access Manager Session Termination Weakness
<http://www.novell.com/support/viewContent.do?externalId=7001788>

New critical vulnerabilities in VLC media player
<http://www.heise-online.co.uk/security/New-critical-vulnerabilities-in-VLC-media-player--/news/111900>

Solaris DHCP Daemon Bug Lets Remote Users Deny Service
<http://securitytracker.com/alerts/2008/Nov/1021157.html>

Microsoft XML Core Services Multiple Remote Vulnerabilities (MS08-069)
<http://www.microsoft.com/technet/security/Bulletin/ms08-069.msp>

SAP GUI MDrmSap ActiveX Remote Code Execution Vulnerability
<http://service.sap.com/sap/support/notes/1142431>

Trend Micro ServerProtect Multiple Code Execution Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/3127>

Apple Safari Code Execution and Security Bypass Vulnerabilities
<http://support.apple.com/kb/HT3298>

HP OpenView Network Node Manager Cross Site Scripting Issues
http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01607570

EMC ControlCenter Buffer Overflow and File Download Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/3220>

IN THE NEWS

Data Leak Prevention, DLP Security Vendors Grow Up
<http://www.eweek.com/c/a/Security/Data-Leak-Prevention-Market-Starts-to-Grow-Up/>

Stealthy Trojan Swipes Bank Log-ins, Financial Data from Thousands
<http://www.eweek.com/c/a/Security/Stealthy-Trojan-Swipes-Bank-Logins-Financial-Data-From-Thousands/>

Microsoft: Malware Threats Up 43%
<http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=212000055>

The end of an era - Windows 3.x
http://www.gss.co.uk/news/article/5584/The_end_of_an_era_-_Windows_3.x/

BotHunter tracks down zombie PCs on a LAN
<http://www.bothunter.net/>

Even more RPC worms for Windows hole

<http://www.heise-online.co.uk/security/Even-more-RPC-worms-for-Windows-hole--/news/111883>

WPA alleged to be crackable in less than 15 minutes

<http://www.heise-online.co.uk/security/WPA-alleged-to-be-crackable-in-less-than-15-minutes--/news/111906>

Thousands hit in broad Web hack

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=009119598>

Hackers exploit PDF security flaws

<http://www.heise-online.co.uk/security/Hackers-exploit-PDF-security-flaws--/news/111920>

Study: Storm botnet brought in daily profits of up to \$9,500

<http://arstechnica.com/news.ars/post/20081110-study-storm-botnet-brought-in-daily-profits-of-up-to-9500.html>

The Economics of Spam

http://www.schneier.com/blog/archives/2008/11/the_economics_o.html

Attacks On Banks

<http://www.net-security.org/article.php?id=1189&p=1>

Opera "file://" URI Handling Buffer Overflow Vulnerability

<http://milw0rm.com/exploits/7135>

Symantec sees spike in dangerous Microsoft attacks

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9121198&intsrc=news_ts_head

Security breach gives PayPal phish the personal touch

http://www.theregister.co.uk/2008/11/24/pamela_security_breach/

Europol to establish a centre to fight cyber crime

<http://www.heise-online.co.uk/security/Europol-to-establish-a-centre-to-fight-cyber-crime--/news/112044>

New report predicts massive increase in malware and phishing in 2009

http://www.message-labs.com/mlireport/MLI_Predictions_Annual2009_FINAL.pdf

FOCUS OF THE MONTH – THE ART OF SECURITY WAR

In late 2007 and early 2008 all security experts said the same thing. “2008 will be a year with a huge amount of cybercrime, and the crime will have financial motives.” They were right. However, we had no idea how right we all would be.

We have seen several sources of news indicating that this year there have been more viruses, the botnets have been bigger and the percentage of spam larger than we have ever seen before. Security experts are still one step behind the criminals, and several companies are even further behind, not implementing new technology fast enough. You may say that the battle is lost, but we believe the war is still going strong.

VIRUSES

2008 have gone down in history as the worst year of viruses ever. During this year the numbers of computer viruses have more than tripled. F-Secure have told that they receive more than 80 000 examples of malicious code every day. Trend Micro have told that they have found 5.4 million unique examples for malicious code during 2008. 800 examples are identified every hour. These numbers are larger than security experts could imagine for 2008.

The positive trend about these viruses is that they do not spread as fast and over as wide an area as viruses did a couple of years ago. The viruses do not live that long either, or they get modified. In other words, security professionals are successful in forcing cyber criminals to renew their code often.

BOTNETS

In November of 2008 the worst botnet attack of the year was presented. The botnet DDoS attack generated 40 Gb/second of traffic. The largest registered the previous two years was “only” at 24 Gb/second. Several botnets on sizes of multiple thousands of computers have also been registered. The Dutch police force got control over a botnet containing 100 000 computers in August of this year. This botnet may have been even larger at one time, probably up to 150 000 computers.

Botnets are in most cases possible to stop. However, the ISPs which would be responsible for stopping these attacks say that they are not able to stop them fast enough. Some of the attacks are also bigger than the Internet infrastructure can handle. In other words, we are falling behind here. The positive thing is that more botnets are discovered and stopped now. This may be because there are many of these botnets, but it is also possible that we have better detection now than earlier. Several reports indicate the latter.

SPAM

The numbers for spam is not better than other reports for 2008. IronPort have reported that 120 billions of spam messages are sent every day. That is near 20 messages per person on this earth per day. At one point this year a security company said that 98% of all e-mails sent was spam. Symantec have reported that the spam level is up to 90% at all times, however there have been a month now that we see a temporarily drop of spam. This is due to a hosting company used for spamming now have shut down. It is likely however that spam will increase during the holiday season, with false e-mails trying to sell products or make you donate money.

New methods for stopping spam are developed at all times, and most spam is now stopped at ISP level in stead of making its way to the end user. However, too much spam are processed, so shutting down hosting companies may be the next step. Telenor in Norway really got into trouble this fall when the amount of spam increased suddenly and with such amount that their e-mail systems more or less stopped. The spam e-mails actually worked as a Denial of Service attack.

THE NEW BATTLE

As you may understand security experts are one step behind the criminals at all time. However, we see now examples of experts taking control over botnets, learning how they work to easier make to stop them. We see that hosting companies known for spam or other criminal activities are shut down, either temporarily or for ever. We see layered security at several companies using anti-virus, web washers, packet shapers, proxy servers, anti-malware and so on. Layered security and attacking the trouble as near the source as possible seem to be the way to go now.

EXTERNAL SOURCES

- [1] Symantec – The State of Spam December 2008
http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_12-2008.en-us.pdf
- [2] IronPort – 2008 Internet Security Trends
<http://www.ironport.com/securitytrends/>
- [3] Digi.no – Frykter retro-virus (Norwegian)
<http://www.digi.no/php/art.php?id=797569>
- [4] Digi.no – Det verste virus-året noensinne (Norwegian)
<http://www.digi.no/php/art.php?id=796693>
- [5] NY Times – Thieves Winning Online War, Maybe Even in Your Computer
http://www.nytimes.com/2008/12/06/technology/internet/06security.html?_r=2
- [6] Digi.no – Kraftigste botnet-angrep noensinne (Norwegian)
<http://www.digi.no/php/art.php?id=794340>
- [7] Digi.no – Nederlandsk politi tok kontroll over botnet
<http://www.digi.no/php/art.php?id=782579>
- [8] USA Today – Botnet scams are exploding
http://www.usatoday.com/tech/news/computersecurity/2008-03-16-computer-botnets_N.htm

ALERT STATISTIC

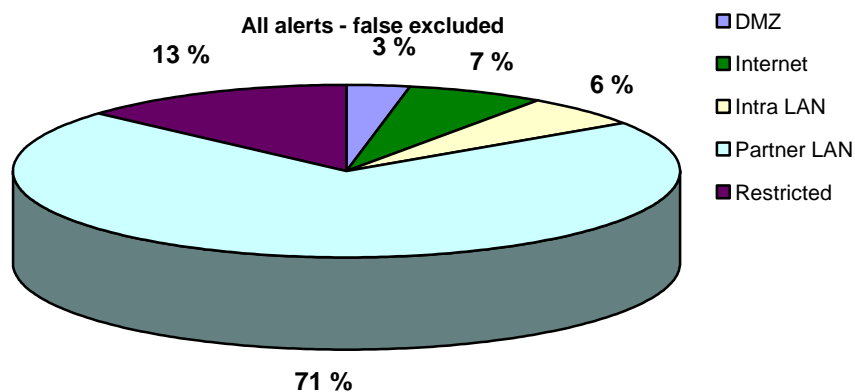
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

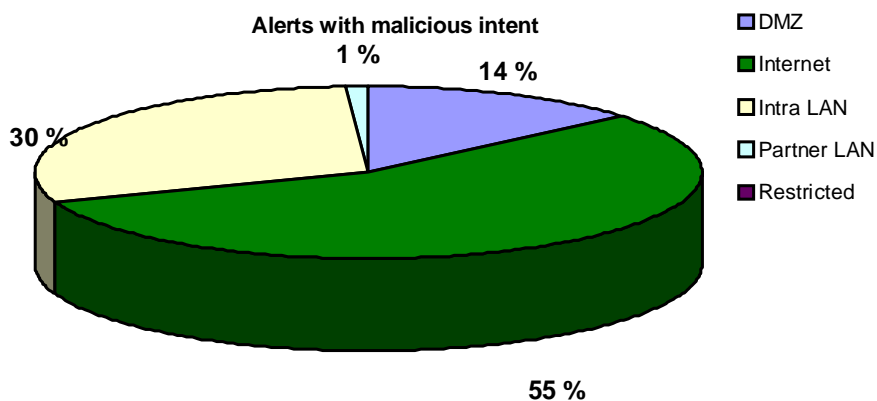
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

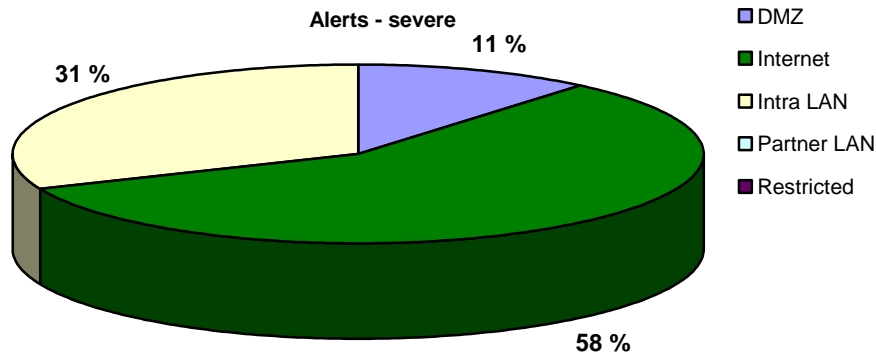
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



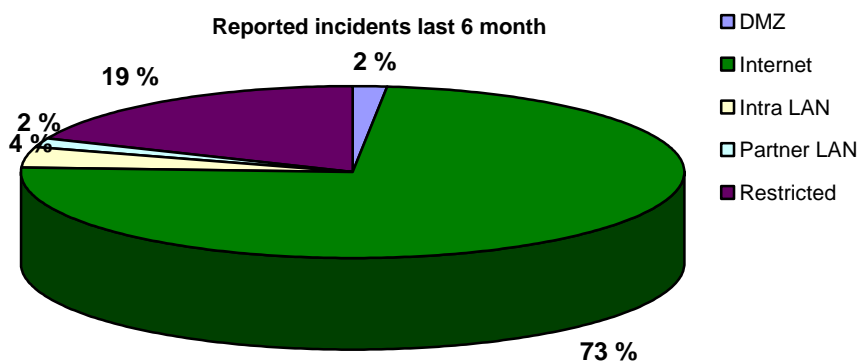
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

This month most alerts have been registered in the partner LAN. We see however that most of these alerts are of not severe character. Only a minor of these alerts have had a malicious intend. Severe alerts are still mostly seen from the Internet, registered on internet sensors or in the DMZ. Other severe alerts are mostly seen in internal zones, indicating that users are breaching the internal policy.

Most of the attacks from the Internet are mainly caused by web attacks against web servers.

REPORTED INCIDENTS

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



Incidents in restricted zone are mainly caused by users which violates the organization's internal security policy. The incidents from the Internet segments are mainly directly targeting attacks against the finance sector, using HTTP/HTTPS. We see that most of the attacks are directed attack from the Internet segment.

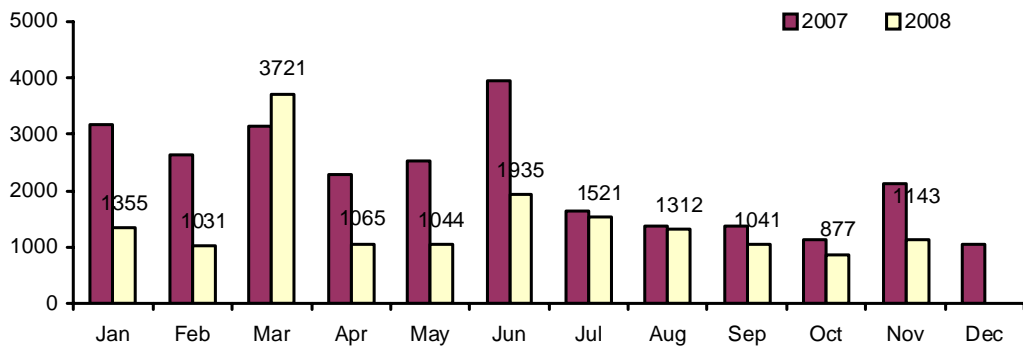
THREAT LEVEL

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.

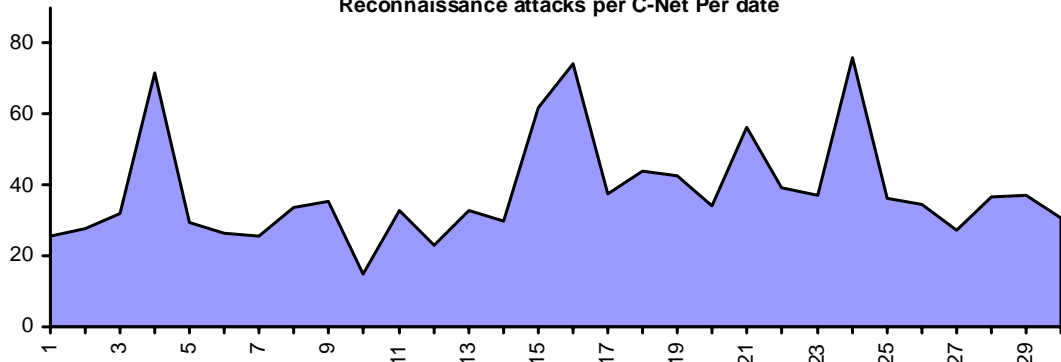
RECONNAISSANCE ATTACKS NOVEMBER 2008

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.

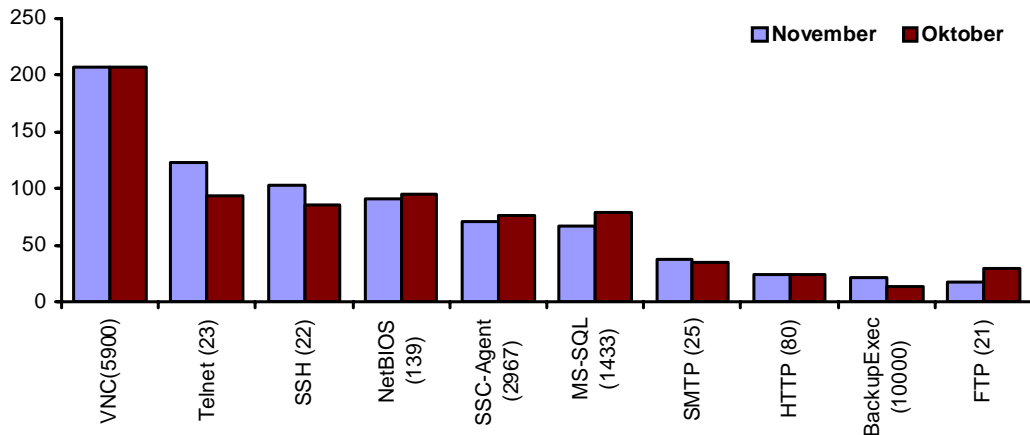
Reconnaissance attacks per monitored C-Net



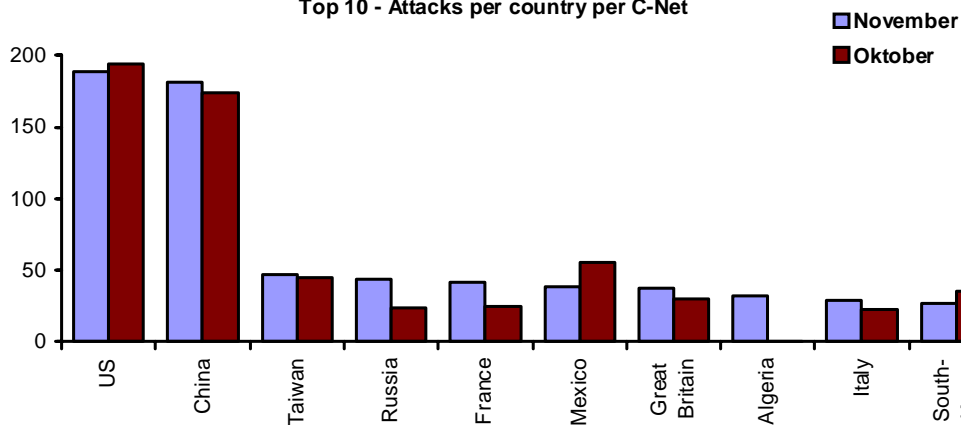
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net



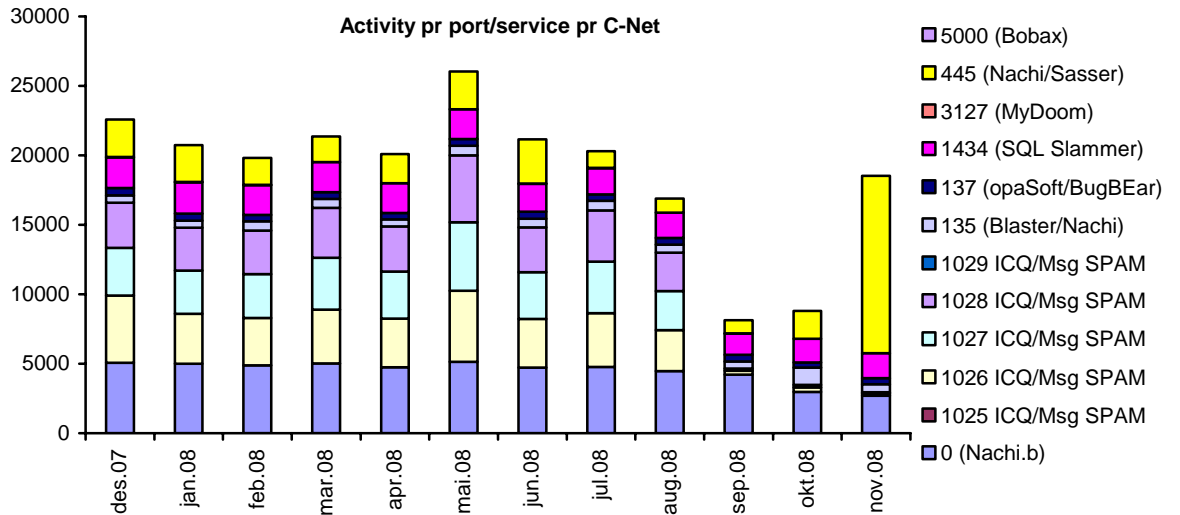
There was a slight increase in the number of reconnaissance attacks during November. However, we see that the main service of attack is still VNC, and there is no difference there from last month. As we see an increase in the total number of reconnaissance attacks there is probably an increase in several of the services that is not placed among the top ten target services.

Among countries of origin there is one surprise this month, with Algeria being on 8th place. The attacks from Algeria is almost only seen towards VNC (port 5900), and they hit all our customers. This indicates that these attacks are not intended to target any particular company.

All the service scans in the statistic above is targeting known services with known vulnerabilities and exploits.

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.



This month we have seen a big increase in traffic towards port 445. This traffic is seen towards all of our customers. This traffic seems to be related to worms which target this port in particular (W32.Downadup). In late of October a critical update was released from Microsoft, an update which Secode highly recommended to implement. This patch was released due to some attacks towards the Windows Sever Service, which uses the 445 port. Towards the end of November we have seen a huge increase in this kind of traffic, making Symantec set their ThreatCon level to two.

Most firewalls are configured to block port 445. In addition the patch released in October has been recommended for all. If your firewall is secured and the patch is implemented, you are in no danger.