

# SECURITY THREATS AND TRENDS

## FEBRUARY 2009

## 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 the focus of the month this February we are taking a closer look at the Downadup/Conficker virus. Trying to give you an overview of how it works.

The alert statistic shows that most alerts occur in intra LAN this time, mostly because several of the customers which this statistics is based on have been infected by the Downadup/Conficker virus. In other words, these alerts are registered as severe. Incidents reported for Intra LAN have also increased as a result of the virus.

There has been a slight increase in the number of reconnaissance attacks. We see, however, that the level is not abnormally high. The traffic mostly targets well known Microsoft ports. Some of these ports may be used for the Downadup virus.

Among spam/worm we continue to see an increase in the traffic towards port 445. This is due to the Downadup worm targeting this port.

## 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 – DOWNADUP/CONFICKER.....</b>	<b>7</b>
THE BEGINNING.....	7
HOW IT WORKS .....	7
THE FUTURE.....	8
PREVENTION .....	8
SOURCES AND MORE INFORMATION.....	8
<b>ALERT STATISTIC.....</b>	<b>9</b>
HANDLED ALERTS .....	9
REPORTED INCIDENTS.....	10
<b>THREAT LEVEL.....</b>	<b>11</b>
RECONNAISSANCE ATTACKS JANUARY 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

25C3: SMS "killer application" for many Nokia mobiles

<http://www.heise-online.co.uk/security/25C3-SMS-killer-application-for-many-Nokia-mobiles--/news/112335>

System Hardening Process Checklist

<http://www.shortinfosec.net/2009/01/system-hardening-process-checklist.html>

Microsoft Urges Organizations to Patch Server Vulnerability as New Attacks Surface

<http://www.eweek.com/c/a/Security/Microsoft-Urges-Organizations-Patch-Vulnerability-as-New-Round-of-Attacks-Surface/>

Samba Grants Remote Authenticated Users Access to the Root Filesystem in Certain Cases

<http://samba.org/samba/security/CVE-2009-0022.html>

OpenBSD update for OpenSSL

<http://www.openbsd.org/errata44.html>

Cisco removes vulnerabilities in its Global Site Selector

<http://www.cisco.com/warp/public/707/cisco-sa-20090107-gss.shtml>

Oracle Releases Critical Patch Update with 41 Fixes

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

Cisco Security Response: Cisco IOS Cross-Site Scripting Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml>

Trend Micro vulnerabilities

<http://secunia.com/Advisories/33609>

<http://secunia.com/Advisories/31160>

mod-auth-mysql SQL Injection Vulnerability

<http://www.openwall.com/lists/oss-security/2009/01/21/10>

### IN THE NEWS

Mobile Work Force, Mobile Threats: Strategies for Preventing Mobile Security Breaches

<http://www.itsecurity.com/features/mobile-work-force-threats-090408/>

With Gaza conflict, cyberattacks come too

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124658&intsrc=news\\_ts\\_head](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124658&intsrc=news_ts_head)

Spamhaus Statistics: The Top 10

<http://www.spamhaus.org/statistics/networks.lasso>

VeriSign transitions all new RapidSSL certificates to SHA-1 algorithm

<http://www.net-security.org/secworld.php?id=6885>

14% of SSL Certificates signed using Vulnerable MD5 Algorithm

[http://news.netcraft.com/archives/2009/01/01/14\\_of\\_ssl\\_certificates\\_signed\\_using\\_vulnerable\\_md5\\_algorithm.html](http://news.netcraft.com/archives/2009/01/01/14_of_ssl_certificates_signed_using_vulnerable_md5_algorithm.html)

2008 Data Breach Totals Soar

[http://www.idtheftcenter.org/artman2/publish/m\\_press/2008\\_Data\\_Breach\\_Totals\\_Soar.shtml](http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml)

Researchers Aim to Fortify CAPTCHA Against Spammers

<http://www.eweek.com/c/a/Security/Spammers-War-Against-CAPTCHA-Requires-New-Approaches/?kc=rss>

Sacked IT admin sentenced for hacking ex-employer

[http://www.theregister.co.uk/2009/01/07/it\\_admin\\_sentenced/](http://www.theregister.co.uk/2009/01/07/it_admin_sentenced/)

Choosing a Secure Password - The Linux-Tip Approach

<http://www.linux-tip.net/cms/content/view/365/27/>

CWE/SANS TOP 25 Most Dangerous Programming Errors

<http://www.sans.org/top25errors/>

Botnets' Landscape Changes as Spammers Get Back in the Swing of Things

<http://www.eweek.com/c/a/Security/Botnets-Landscape-Changes-as-Spammers-Get-Back-in-the-Swing-of-Things/>

Targeted social engineering

<http://isc.sans.org/diary.html?storyid=5707>

DNS queries for "."

<http://isc.sans.org/diary.html?storyid=5713&rss>

Shrinking Patch Timelines – The Need For HIPS

[http://www.governmentsecurity.org/SecurityHackingNews/Shrinking\\_Patch\\_Timelines\\_The\\_Need\\_For\\_HIPS](http://www.governmentsecurity.org/SecurityHackingNews/Shrinking_Patch_Timelines_The_Need_For_HIPS)

Cybercrime cost firms \$1 trillion globally, McAfee study says

[http://news.cnet.com/8301-1009\\_3-10152246-83.html?tag=mncol](http://news.cnet.com/8301-1009_3-10152246-83.html?tag=mncol)

## FOCUS OF THE MONTH – DOWNADUP/CONFICKER

---

Almost every day we get updates that the Downadup (or Conficker as it may be called) virus gets upgraded. The infection rate of the worm is massive. We will in this article look at how it began and how the virus affects us. We will also try to look at possible future outcomes for the virus.

### THE BEGINNING

In October of 2008 the Microsoft Corporation stated that a vulnerability in their Windows Server Service could be used to allow remote code execution. The vulnerability affected most of their Operating Systems (OS). Microsoft stated that they already had seen some attempts to exploit the vulnerability, and on October 23<sup>rd</sup> Microsoft released a patch that fixed the problem. However, the problem is that many do not implement the patch at once.

In November we started to register an increase in the number of automated attacks towards the port 445, one of the port which the vulnerability affected. At the same time we started to see the first articles about the Downadup/Conficker virus in the media and especially in alerts from security vendors. As the virus would have been stopped by implementing the patch and use firewall best practices on the perimeter firewalls, nobody expected that the virus would continue spreading for long. However we saw an increase in the automated attacks every day from that time on.

### HOW IT WORKS

The virus has several ways of spreading, which makes it a more successful worm than many others we have seen surfacing during the last couple of years. The four ways of spreading are:

- Through unpatched Windows systems that are connected to a network. Mostly through the port 445, but it may also spread through other Windows ports.
- By infected USB drives (thumb drives), using the autorun functionality to its advantage.
- Use Windows scheduled task and autorun to re-infect cleaned PCs.
- Brute Force dictionary attacks towards administrator passwords, cracking weak passwords.

The first two ways of spreading is the most well-known, a probably the most used as well. In Norway the policies for using thumb drives seems to be pretty strict, and many seem to keep these drives separate between work and home, keeping this spreading low. Unpatched systems however you will find lots of in Norway. Many companies have policies stating that no patch are to be installed until it is approved by the operational administrator, and they have not got the time to approve them. Others just do not have policies for patching at all, making an unpatched system pretty ordinary. At this point more than 15 million computers world wide have been infected.

So what does the virus do once it has infected a system? Well, several things. The reported things are:

- Copies itself into the Windows system folder
- Modifies the registry in Windows
- Changes access rights and registry keys so users can't change or delete them
- Sets itself to restart when Windows starts
- Connects to a public site for retrieving IP address to get the address of the computer.
- Downloads modified versions of itself from a long list of web sites. These lists are changed daily and are "randomly" generated by algorithms. The lists for some time forward are now known to some security vendors.
- Starts a web server on a random port of your PC to host a copy of the modified worm.

In other words, the only thing it does is to infect machines, making the computer available for remotely execution of code. It does not seem like it tries to do any more harm on the computer or try to download other viruses.

### THE FUTURE

No one knows what will happen with this virus in the future. Nobody knows how many computers will be infected, if the virus will alter to download other malicious code or if the virus will be used for a botnet. The latter have been predicted to be a possible outcome, and that would make it the largest botnet in the world, making it more or less impossible to shut down. The only thing we can say at this point is that the spreading does not seem to slow down.

We have seen an increase of about a couple of hundred automated attacks per week to about 90 000 per day for port 445, and the increase continues. There are no signs of the increase slowing down at this point either. Several other security vendors are reporting an increase of infected computers per day.

### PREVENTION

To prevent your self or your company from getting infected, remember the following:

- Keep all software updated. Especially critical updates from Microsoft should be implemented until the worm is more under control. At this point the worm finds new ways to spread almost daily, and many of the patches for Microsoft are related to this worm.
- Keep you network secure. In other words, configure your firewall to only let through the traffic it needs to. Consider using other network security products like IDS, IPS, log management, network flow, and anomaly based detection and so on. If you already have a product like this, make sure it is up to date and that the logs are processed as often as possible.
- Use strong passwords. This goes for a lot of different viruses.
- Have a full security suite on all clients surfing the web. Antivirus is not enough, but with malware protection, client firewalls and so on you are more secure. A client based IPS system may also be a good idea.

### SOURCES AND MORE INFORMATION

[1] All info about Downadup

<http://www.downadup.com/>

[2] Virus strikes 15 million PCS

[http://www.upi.com/Top\\_News/2009/01/25/Virus\\_strikes\\_15\\_million\\_PCs/UPI-19421232924206/](http://www.upi.com/Top_News/2009/01/25/Virus_strikes_15_million_PCs/UPI-19421232924206/)

[3] SANS – More tricks from Conficker and VM detection

<http://isc.sans.org/diary.html?storyid=5842&rss>

[4] SANS – Some tricks from Conficker's bag

<http://isc.sans.org/diary.html?storyid=5830>

[5] SANS – Conficker autorun and social engineering

<http://isc.sans.org/diary.html?storyid=5695>

[6] CNN – Downadup virus exposes millions of PCs to hijack

<http://www.cnn.com/2009/TECH/ptech/01/16/virus.downadup/index.html>

[7] F-Secure – Calculating the size of the downadup outbreak.

<http://www.f-secure.com/weblog/archives/00001584.html>

## ALERT STATISTIC

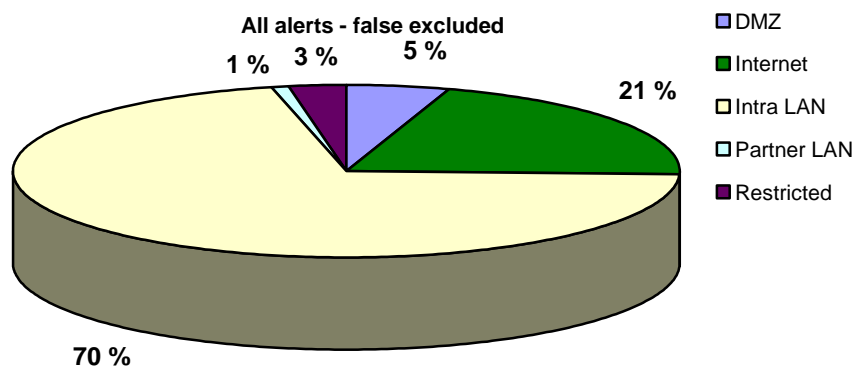
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

### HANDLED ALERTS

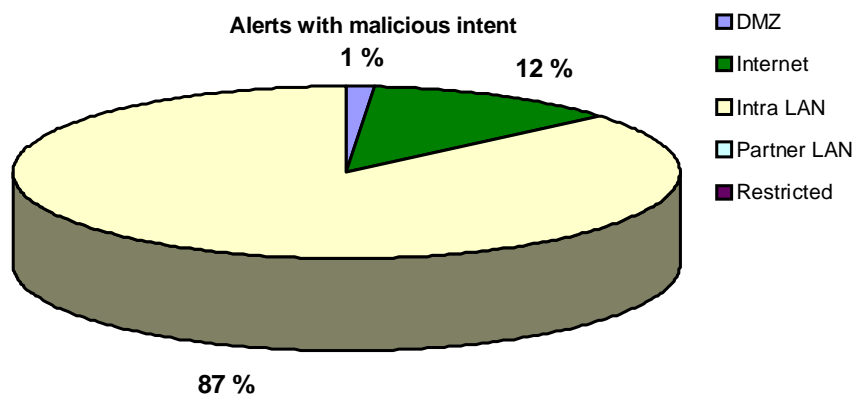
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

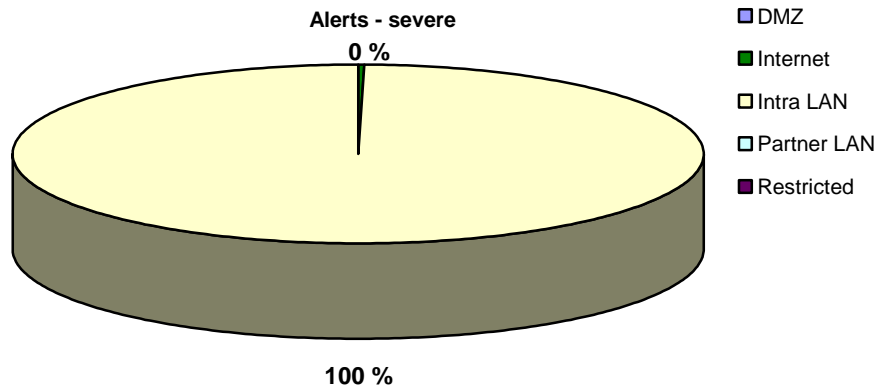
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



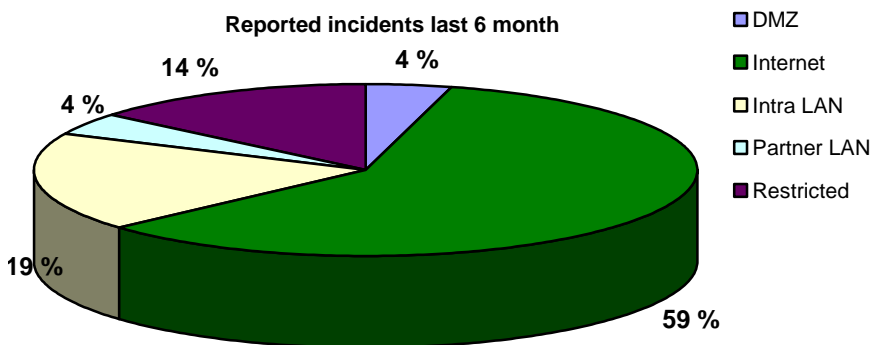
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

Most of the alerts in January were registered in the Intra LAN. This is due to infections of the Downadup virus at some of our customers. Most of the traffic on the Internet is also related to this virus. The virus generates a lot of traffic, both as a general alert and as an increase in the reconnaissance attacks and worm/spam traffic.

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 registered in the Intra LAN are in most cases related to the Downadup virus. 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.

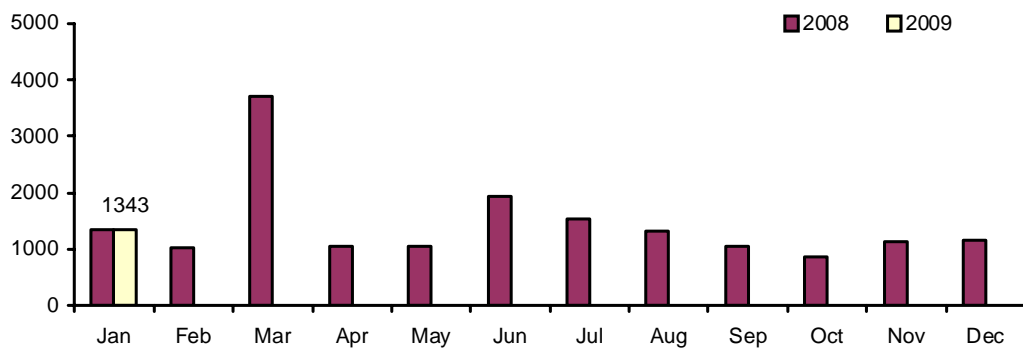
## THREAT LEVEL

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.

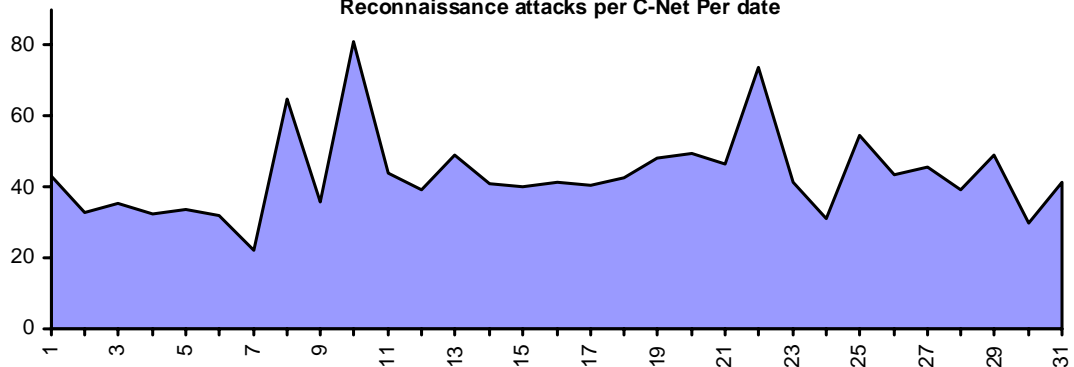
### RECONNAISSANCE ATTACKS JANUARY 2008

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.

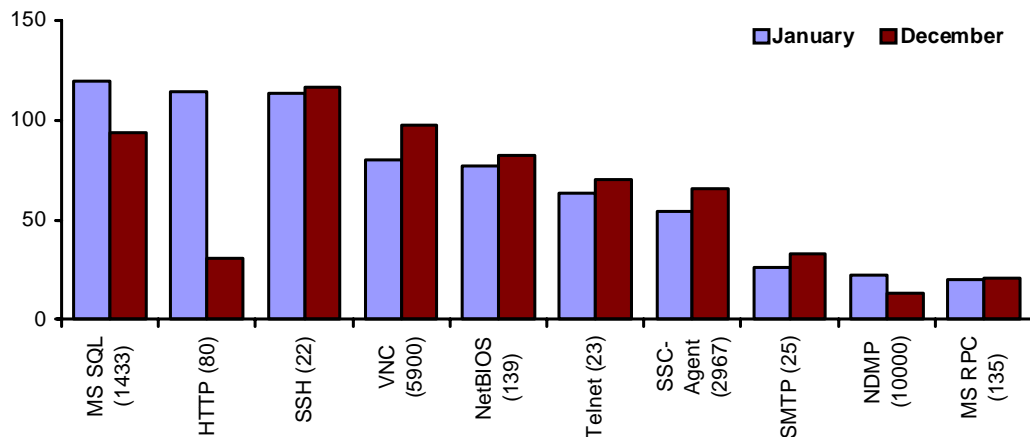
Reconnaissance attacks per monitored C-Net



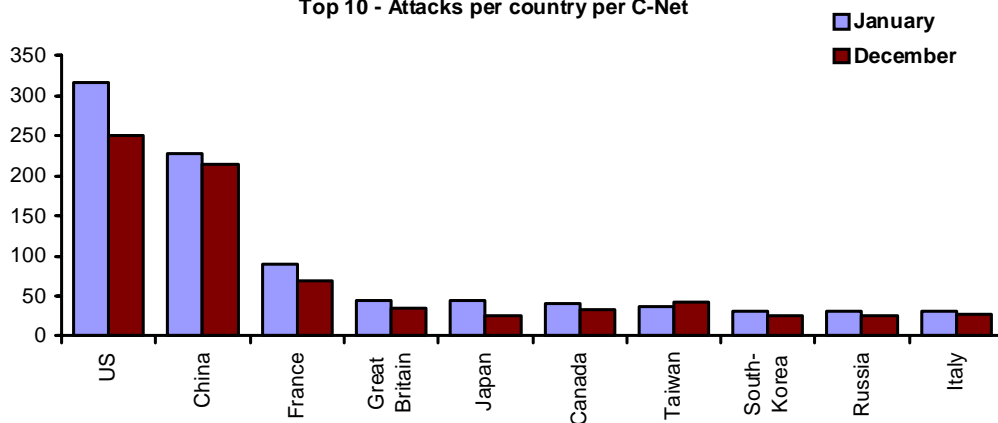
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net



The traffic level for January was slightly higher than for December. However, we see that the level in January 2009 is similar to the level a year ago, so the traffic level is in other words not abnormally high for this time of year.

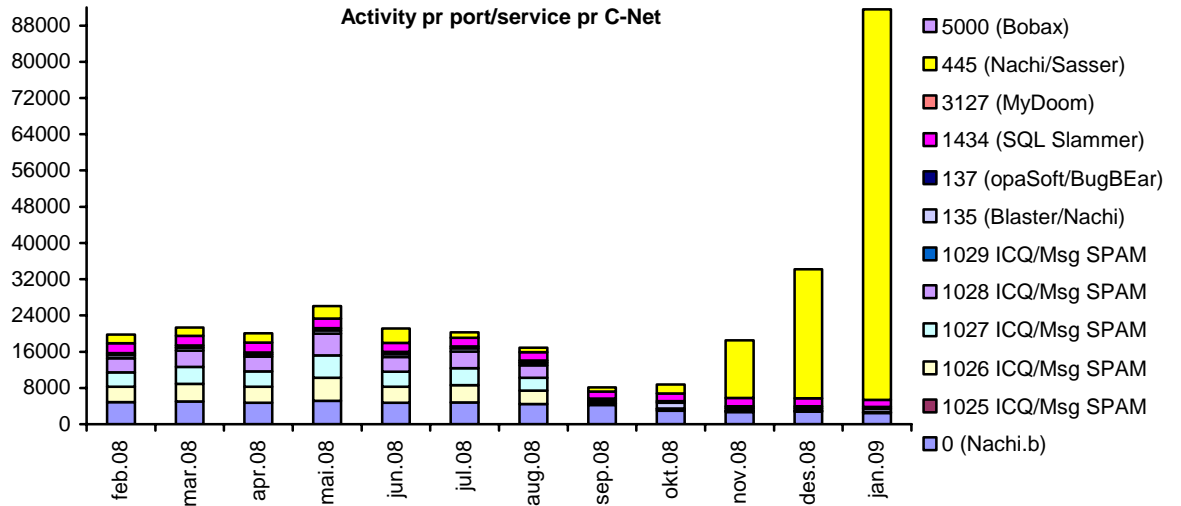
VNC is not the main service of attack this month. We see that more of the well known and well used services are targeted now. This includes the Microsoft used ports 1433 (SQL), 139 (NetBIOS) and 135 (MS RPC). The latter port may be used for spreading versions of the Downadup virus.

Among countries of origin there is no surprise this month. All countries have been on the top 10 list before, and many of them are on the list more or less every month. These numbers are coexistent with numbers registered by other security vendors.

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.



We have lately seen an increase in traffic towards port 445 related to the Downadup virus, and the traffic level is now sky-high. The statistics above displays the average level of traffic on c-net. We see however that some of the c-nets have a lot more traffic than others. The traffic towards other ports has decreased and is now insignificant.

As previously mentioned you should not be in any danger of getting the Downadup virus if you windows systems are updated and the firewall is configured to block port 445. We refer to the Focus of the month for more information about the Downadup virus.