

SECURITY THREATS AND TRENDS

MARCH 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 March Secode take a closer look at the future within IDS.

After the alert statistic showed that most alerts occur in Intra LAN last month, we now see that Internet is the most targeted zone. Intra LAN is still targeted by severe alerts, and many reported incidents are generated in this zone. The reason for this severe traffic is the Downadup/Conficker virus.

There has been a slight increase in the number of reconnaissance attacks. The traffic mostly targets well known Microsoft ports, and the service port 5900 (VNC). We also see an increase in the number of reconnaissance attacks towards port 3306 (MySQL). Some of the Microsoft 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

INTRODUCTION	4
NEWS OF THE MONTH	5
PUBLISHED VULNERABILITIES	5
IN THE NEWS.....	6
FOCUS OF THE MONTH – IDS TECHNOLOGY.....	7
SECODE FORESEES NEXT STEP IN IDS INFRASTRUCTURE APPLICATION	7
ALERT STATISTIC.....	8
HANDLED ALERTS	8
REPORTED INCIDENTS.....	9
THREAT LEVEL.....	10
RECONNAISSANCE ATTACKS FEBRUARY 2009.....	10
INTERNET WORMS AND SPAM.....	12

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

Firefox 3.0.6

<http://www.mozilla.com/en-US/firefox/3.0.6/releasenotes/>

VNC Multiple Integer Overflows

<http://www.securityfocus.com/archive/1/500632>

Cisco Releases Security Advisory for Cisco Wireless LAN Controllers

<http://www.cisco.com/warp/public/707/cisco-sa-20090204-wlc.shtml>

Java updates all round

<http://java.sun.com/javase/6/webnotes/6u12.html>

Trend Micro InterScan Web Security Suite Lets Certain Remote Authenticated Users Gain Elevated Privileges

<http://www.securitytracker.com/alerts/2009/Feb/1021694.html>

February Black Tuesday Overview

<http://isc.sans.org/diary.html?storyid=5836>

Sun Java System Directory Server Denial of Service Vulnerability

<http://www.vupen.com/english/advisories/2009/0409>

Multiple vulnerabilities in Firefox and Xulrunner for Ubuntu 8.04 and 8.10

<http://secunia.com/Advisories/33869>

Active Exploitation of Microsoft Internet Explorer 7 Vulnerability

http://www.us-cert.gov/current/index.html#malware_exploiting_microsoft_internet_explorer

Windows Live Messenger Charset Denial of Service Vulnerability

<http://www.vupen.com/english/advisories/2009/0466>

CERT Advisory VU#435052: An Architectural Flaw In Transparent Proxies

<http://www.kb.cert.org/vuls/id/435052>

Flash Player update available to address security vulnerabilities

<http://www.adobe.com/support/security/bulletins/apsb09-01.html>

IN THE NEWS

Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1

<http://www.cert.org/archive/pdf/CSG-V3.pdf>

Budget encrypted USB hard drives easily cracked

<http://www.heise-online.co.uk/security/Cracking-budget-encryption--/features/112548>

Malware infection that began with windshield wipers

<http://isc.sans.org/diary.html?storyid=5797>

What You Really Need To Know About Data Loss Prevention

<http://www.darkreading.com/insiderthreat/security/management/showArticle.jhtml?articleID=213300864>

The Top 10 Internet Registrars Hosting Spammers, Illicit Sites

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=213201931&cid=RSSfeed>

Malicious insider attacks to rise

<http://news.bbc.co.uk/2/hi/technology/7875904.stm>

F-Secure hit by SQL Injection attack, "not vulnerable due to IT security strategy"

<http://www.f-secure.com/weblog/archives/00001605.html>

The Essential Guide to Wireless Security

<http://www.itsecurity.com/features/essential-guide-wireless-security-071708/>

With global effort, a new type of worm is slowed

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127940&source=rss_topic82

Mobile manufacturers express security fears

<http://www.vnunet.com/vnunet/news/2236563/mobile-risks-rise-mcafee>

Top 8 Web 2.0 Security Threats

<http://www.secure-enterprise20.org/>

How to Improve Virtualization Security

<http://www.eweek.com/c/a/Virtualization/How-to-Improve-Virtualization-Security/>

New Symbian-based mobile worm circulating in the wild

<http://blogs.zdnet.com/security/?p=2617>

Conficker becomes a more flexible worm

<http://www.h-online.com/security/Conficker-becomes-a-more-flexible-worm--/news/112705>

VeriSign: We will support DNS security in 2011

<http://www.networkworld.com/news/2009/022409-verisign-dns-security.html?hpg1=bn>

FOCUS OF THE MONTH – IDS TECHNOLOGY

SECODE FORESEES NEXT STEP IN IDS INFRASTRUCTURE APPLICATION

IDS technology can be applied much more effectively

Over the years the application of IDS technology has grown to standardized common building blocks of every mature ICT infrastructure. Due to project pressure and lack of 'round the clock' availability of security specialists, many IDS infrastructures in use today are configured minimal in terms of detection and reporting capabilities. We all want smooth and fast implementations while any risk at potential problems (false positives, disrupted business processes) need to be prevented.

These are the main reasons why IDS infrastructures are tuned down causing low sensitivity, per definition. Therefore one could say that in the real world about 30% of the maximum and manageable effective value can be reached. In other words, most IDS infrastructures don't deliver enough, there too little value created out of the investment.

Now, the essence of 24/7 monitoring, analyzing and correlation of IDS output goes beyond further professionalizing of incident management, security management, compliance management, virtual patching and security operations. The powerful combination of available security specialists and in depth knowledge of the target infrastructures, enables IDS technology to maximize it's capabilities without risking to run into problems. This holistic IDS approach brings the 'next step' in IDS infrastructures in reach for almost every organization. And trust me, I've done the math many times, it's absolutely more cost effective as well.

Besides a much higher and consistent level of information security against a better price tag, additional benefits of such a 'next step' approach are mainly getting real value from the investments while your specialists become available for other important tasks which are much more visible to the higher management layers.

Rob M.M. Greuter
Secode Netherlands B.V.

ALERT STATISTIC

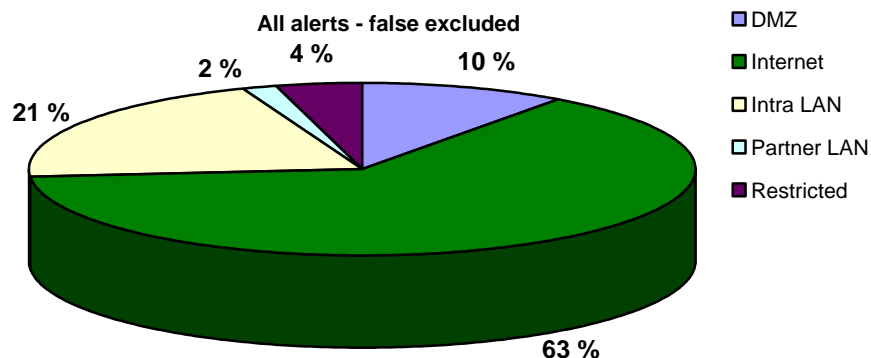
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

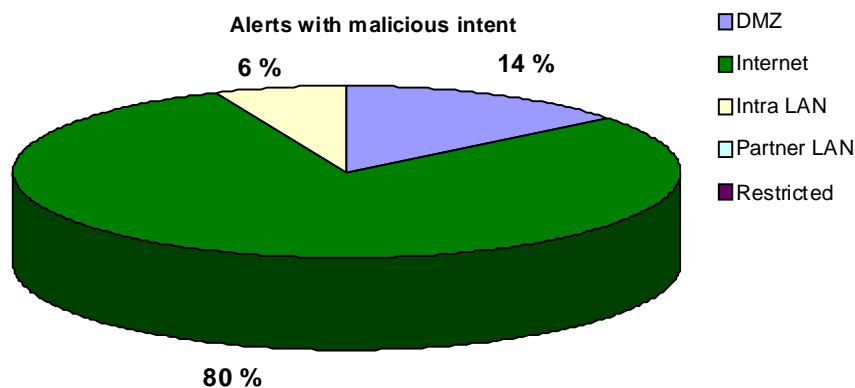
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

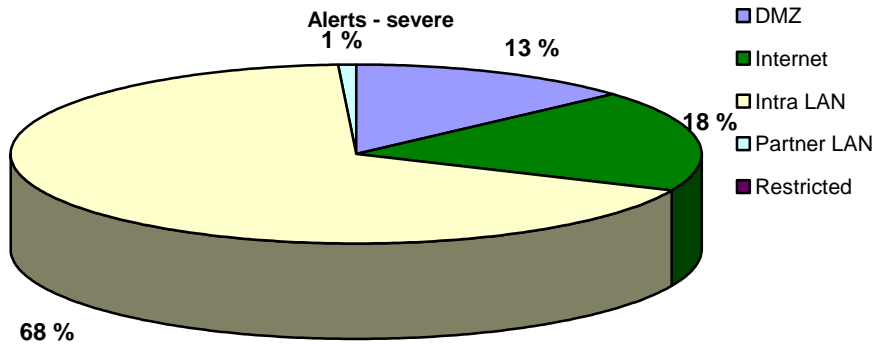
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



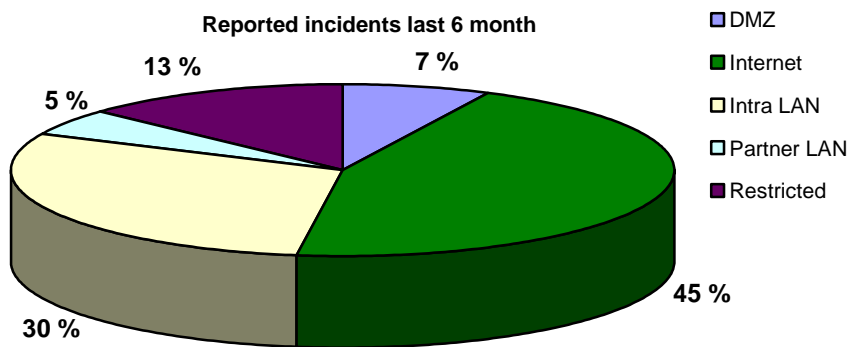
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

After we saw a great deal of alerts in the Intra LAN zone in January we this month see that Internet is the most targeted zone. We still see a great deal of severe alerts in the Intra LAN however, this is still due to infections of Downadup/Conficker virus.

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/Conficker 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, however we see that many incidents happen in Intra LAN as well.

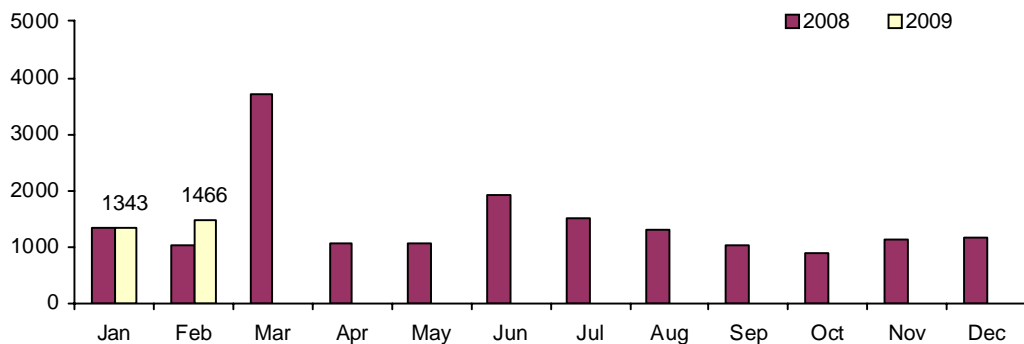
THREAT LEVEL

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.

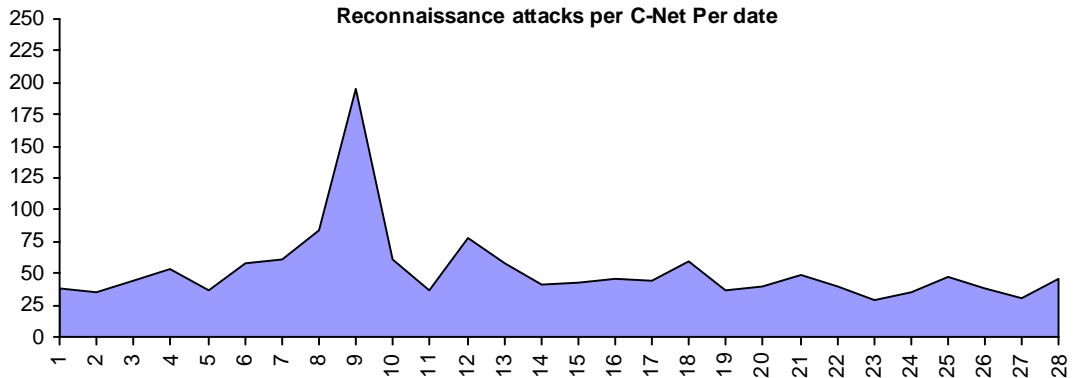
RECONNAISSANCE ATTACKS FEBRUARY 2009

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.

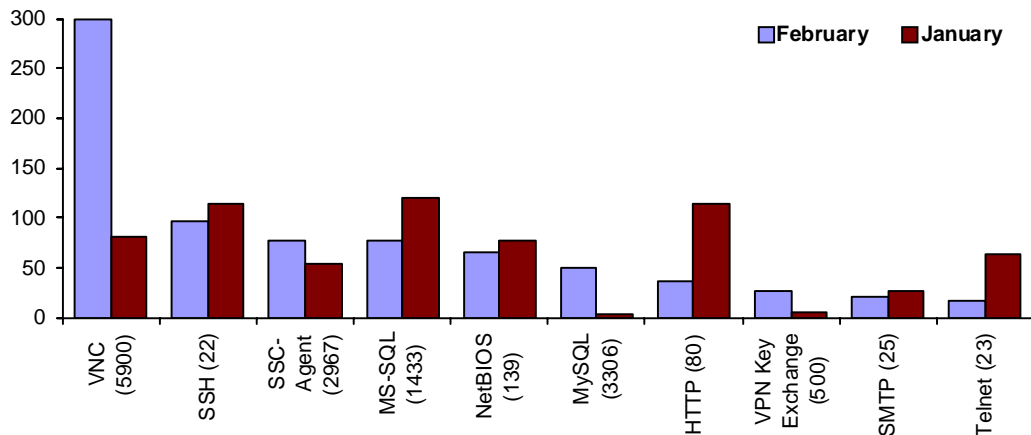
Reconnaissance attacks per monitored C-Net



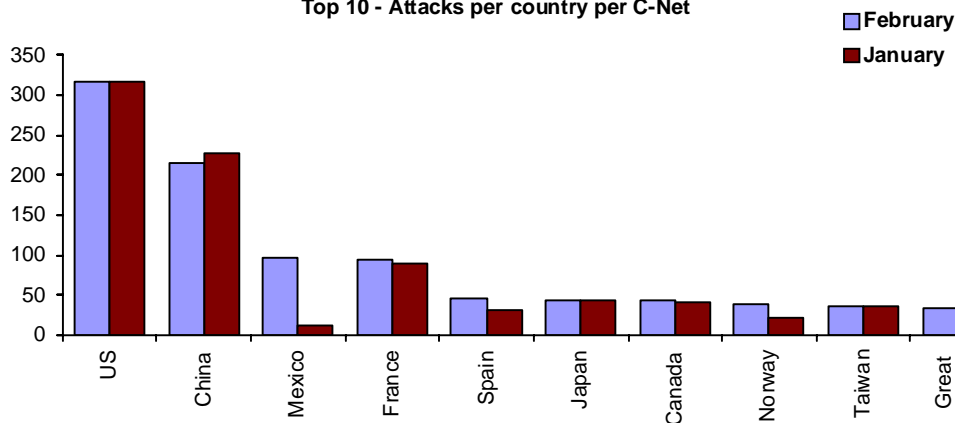
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net



The traffic level for February was slightly higher than for January. However, except for a peak of traffic on the 9th the level of traffic is pretty stabile. The peak on the 9th is caused by an increased traffic towards port 5900 (VNC) this day. We also see a great deal of traffic towards port 3306 (MySQL).

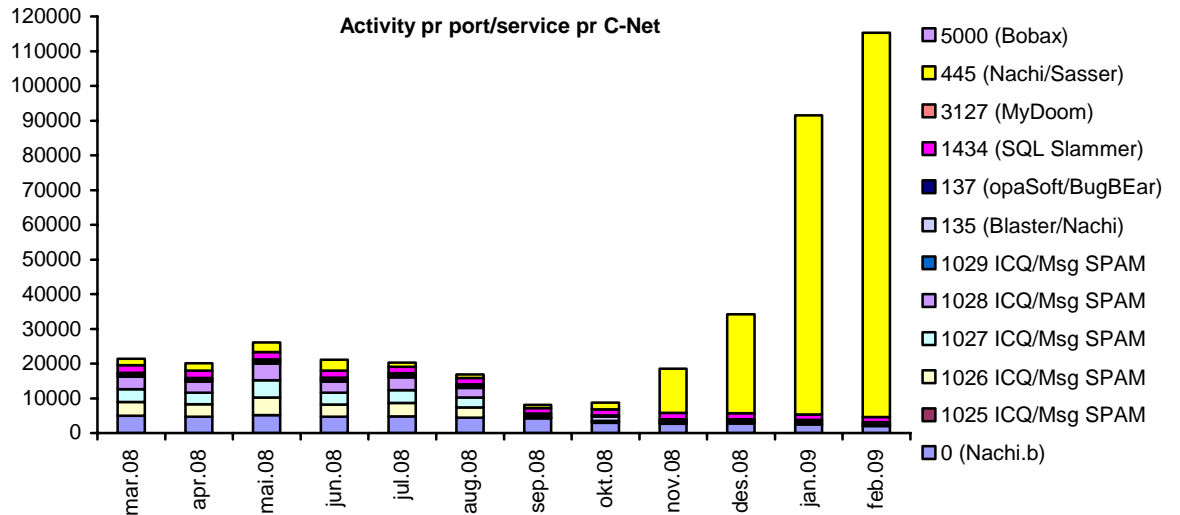
VNC is once again the main service of attack after being further down the list last month. We still see that well known services are attacked, and then especially Microsoft used ports. However, except from VNC the MySQL service has had the most increase in attack level this month. Several countries are behind this traffic, but the US is the main source. If we look at VNC there are several contries of origin, but South-American countries are mostly represented with Argentina, Mexico and Chile leading the way. Many of the attack also have its origin in Spain.

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. The main difference here is the increase in traffic from Mexico, and this may be due to the VNC attacks mentioned above. 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 increase in the level does not seem to stop. However, we now see that the increase has slowed down, so in a month or two we may see it leveling out. 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.