

SECURITY THREATS AND TRENDS

NOVEMBER 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 Man-in-the-Browser attacks, and Trojans exploiting this attack method.

The alert statistic shows that most alerts occur in the Internet zone, but these are rarely severe. The most severe alerts this period has occurred in internal zones, and is caused by users making unwanted file downloads.

It is only observed minor variations in the monitoring of reconnaissance attacks from the Internet. Towards the end of the period it was recorded some smaller distributed attacks from countries in the South-America, a region from where it in previous periods have been recorded lesser attacks.

TABLE OF CONTENTS

INTRODUCTION	4
NEWS OF THE MONTH	5
PUBLISHED VULNERABILITIES	5
IN THE NEWS.....	6
FOCUS OF THE MONTH – MAN-IN-THE-BROWSER.....	7
BANKER TROJAN.....	7
A NORDIC VARIANT.....	7
EXTERNAL SOURCES	8
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

WinZip GDI+ Library Multiple Code Execution Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/2696>

Trend Micro OfficeScan Buffer Overflow and DoS Vulnerabilities
http://www.trendmicro.com/ftp/documentation/readme/OSCE8.0_SP1_Patch1_CriticalPatch_3087_Readme.txt
http://www.trendmicro.com/ftp/documentation/readme/OSCE_8.0_SP1_Win_EN_CriticalPatch_B2439_Readme.txt

Juniper NetScreen ScreenOS Cross Site Scripting Vulnerability
<http://www.layereddefense.com/netscreen01oct.html>

VMware Privilege Escalation and Multiple Code Execution Vulnerabilities
<http://www.vmware.com/security/advisories/VMSA-2008-0016.html>

IBM Lotus Quickr Denial of Service and Security Bypass Vulnerabilities
<http://www-01.ibm.com/support/docview.wss?rs=3264&uid=swg24018711>

Sun Java System Web Proxy Server FTP Heap Overflow
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-242986-1>

Opera Remote Code Execution and Information Disclosure Vulnerabilities
Link: <http://www.frsirt.com/english/advisories/2008/2765>

Oracle and BEA Products Multiple Code Execution Vulnerabilities
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
https://support.bea.com/application_content/product_portlets/securityadvisories/index.html

VLC Media Player XSPF Playlist Memory Corruption Vulnerability
<http://www.coresecurity.com/content/vlc-xspf-memory-corruption>

Adobe Flash CS3 SWF File Handling Code Execution Vulnerabilities
<http://www.adobe.com/support/security/advisories/apsa08-09.html>

Cisco Response to Outpost24 TCP State Table Manipulation Denial of Service Vulnerabilities
http://www.cisco.com/en/US/products/products_security_response09186a0080a15120.html

Multiple Vulnerabilities in Cisco PIX and Cisco ASA
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a183ba.shtml

Microsoft out-of-band patch MS08-067 - Severity Critical
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>
<http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx>

OpenOffice.org WMF and EMF Handling Heap Overflow Vulnerabilities
<http://download.openoffice.org/2.4.2/index.html>

Adobe PageMaker Key Strings Stack Buffer Overflow Vulnerability
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=749>

IBM Tivoli Storage Manager Express for Microsoft SQL Heap Overflow Vulnerability
<http://www.zerodayinitiative.com/advisories/ZDI-08-071/>

IN THE NEWS

Private Wi-Fi more secure than corporate wireless networks
<http://www.heise-online.co.uk/security/Private-Wi-Fi-more-secure-than-corporate-wireless-networks--/news/111837>

DoS Attack reveals (yet another) crack in net's core
http://www.theregister.co.uk/2008/10/01/fundamental_net_vuln/

Skype admits to storing China text messages
<http://www.eweek.com/c/a/Messaging-and-Collaboration/Skype-Admits-to-Storing-China-Text-Messages/>

Free tool hacks banking, webmail and social networking sessions
http://www.darkreading.com/document.asp?doc_id=165303&WT.svl=news1_1

Researcher publishes two iPhone vulnerabilities that Apple just wouldn't patch
<http://cyberinsecure.com/researcher-publishes-two-iphone-vulnerabilities-that-apple-just-wouldnt-patch/>

Gartner highlights the nine most contentious IT issues for the next two years
<http://governmentsecurity.org/forum/index.php?showtopic=30383>

A comparison of virtualization features of HP-UX, Solaris, and AIX
http://www.ibm.com/developerworks/aix/library/au-aixvirtualization/?ca=dgr-lnxw07CompareFeatures&S_TACT=105AGX59&S_cmp=GRsiteInxw07

WPA cracked
<http://isc.sans.org/diary.html?storyid=5315>
<http://www.theregister.co.uk/2008/11/08/wi-fi-protected-access-attack/>
<http://www.heise-online.co.uk/security/WPA-alleged-to-be-crackable-in-less-than-15-minutes--/news/111906>

FOCUS OF THE MONTH – MAN-IN-THE-BROWSER

Man-in-the-Browser is a term used on malware that is able to change what the user sees and does in their browsers. MitB is not a new phenomenon, but these attacks have the last year evolved to become more sophisticated. MitB attacks are also starting to get more international attention due to their capability to bypass extra security layers such as two-factor authentication (included physical tokens).

MitB is based on trojans that is installed at the victim's computers. Such Trojans uses the browser as attack channel, and is able to modify online transactions on-the-fly and yet show the user his/hers intended transaction. The Trojan is transparent to the user and does neither interferer with the normal use of the browser. Not until the user is visiting defined websites (usually eBanking sites), does the Trojan execute its commands.

MitB is structured in the same manner as a man-in-the-middle attack, but instead of hijacking a session, MitB attacks gets between the user and the security in the browser, and manipulate the interaction between the users and the server. This also differs from previous phishing attacks based on bogus websites, as MitB attacks use genuine services and sites, the user is logged in as normal and there is nothing unusual to notice. The data input from the user gets modified before it is encrypted and sent to the server. In the same manner is the answer from the server modified back to what the users expect it to be before presenting it in the browser.

MitB attacks are both expensive and highly technical advanced, and because of the high use of resources, this technique is first of all used in attacks which bring financial gain, ergo; attacks against financial organizations.

Successful MitB attack is detected against different browsers, including Firefox, Internet Explorer and Opera.

BANKER TROJAN

The Banker Trojan is one example of a Trojan that is based on Man-in-the-browser attacks. There are several variants in this Trojan family, and it is also known under different names (SilentBanker and Patcher is two examples).

The Banker Trojan manipulates online transactions and changes the recipients' account number in payments done through the eBanking solution. The manipulation does not affect the SSL certificate, something that may give the users a false sense of security that the transaction is safe. The Trojan has also keylogger functionality and steals login- and account information and sends this to an extern server.

The Banker Trojan is not a new threat, but the newest variants has now become more stealthier by the fact that it is added rootkit functionality which lets the Trojans be loaded into the system before antivirus software. Trojans combined with rootkits is extremely dangerous and hard to detect and remove.

A rootkit is [malware](#) which consists of a [program](#) designed to take fundamental of a computer system, without authorization by the system's owners and legitimate managers. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system [security](#) mechanisms (<http://en.wikipedia.org/wiki/Rootkit>)

A NORDIC VARIANT

Secode has received reports of a new variant of the Banker Trojans that attacks a few eBanks in the North. This variant is based on MitB and is a combination of Trojans and rootkits, something which makes it very hard to detect. Below is an example of how this Banker Trojan work:

- The Trojan/rootkit copies itself to the system
- The Trojan/rootkit adds itself to the the Reloaction Table (http://en.wikipedia.org/wiki/Relocation_table)
- The Trojans/rootkit waits for the user to restart the system so it gets activated
- The code is dependent on several system behavior to start up
- The Trojan modifies system files and adds a BHO – Browser helper Object (http://en.wikipedia.org/wiki/Browser_Helper_Object)
- When the user log in to the eBanking site, the Account Values, Last Login and Failed transfers is changed
- The Trojans disables the possibility to use Java, Firefox and Opera to force the users to use Internet Explorer
- The Trojans has a C&C server to which it transfer the users account information. The domain for the C&C server is generic

EXTERNAL SOURCES

- [1] F-secure
http://www.f-secure.com/v-descs/trojan-spy_w32_agent_bnp.shtml
- [2] Authentium.blogspot.com
<http://authentium.blogspot.com/2008/06/man-in-browser-attacks-worse-than.html>

ALERT STATISTIC

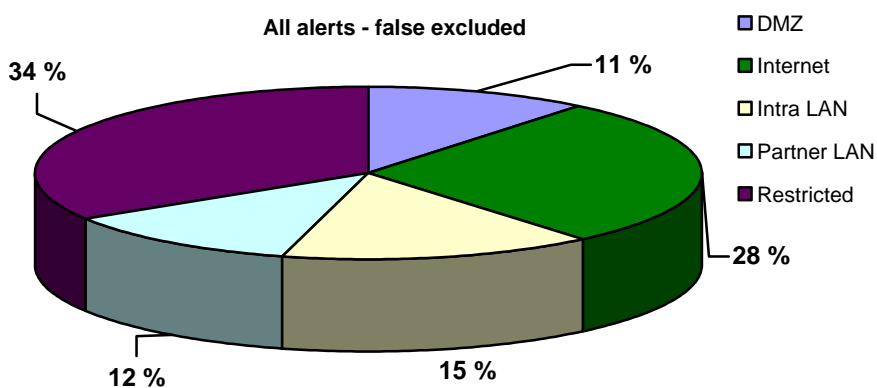
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

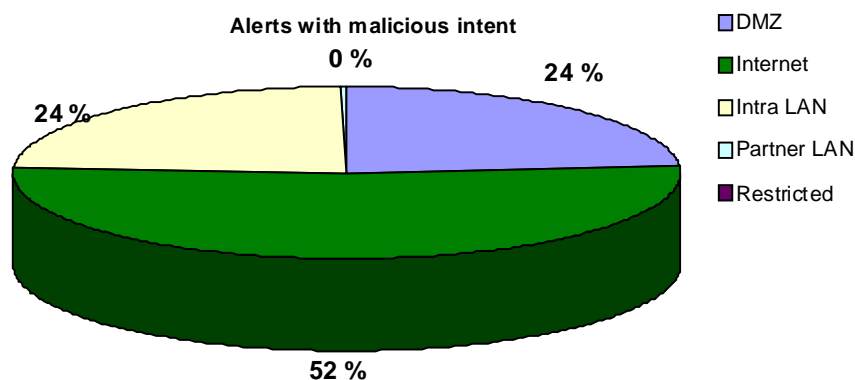
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

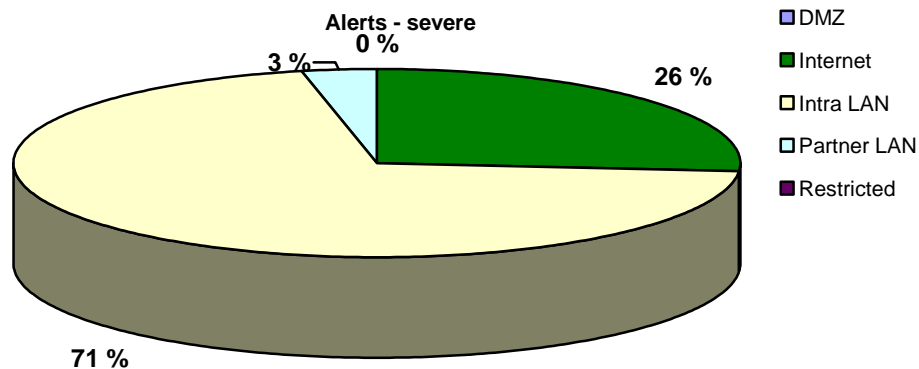
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



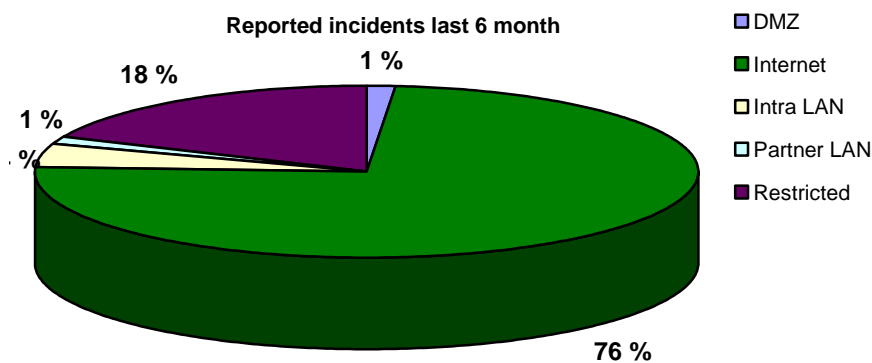
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

Most of the alerts with malicious content occur in the Internet segment, but they are rarely of severe character. The most severe alerts this month have occurred in internal zones, and is caused by unwanted file downloads performed by users at Secode’s customers.

Most of the attacks from the Internet is 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.

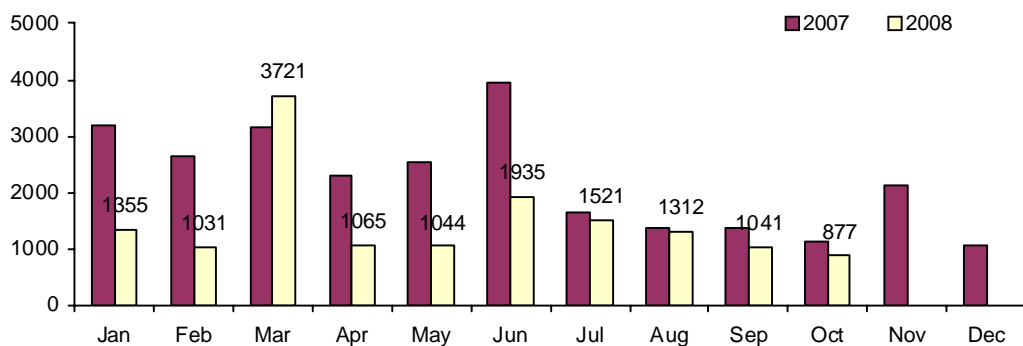
THREAT LEVEL

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.

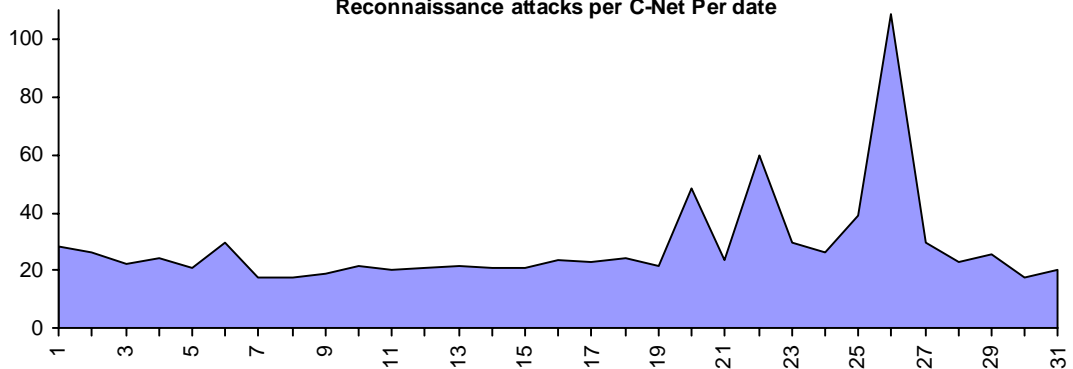
RECONNAISSANCE ATTACKS SEPTEMBER 2008

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.

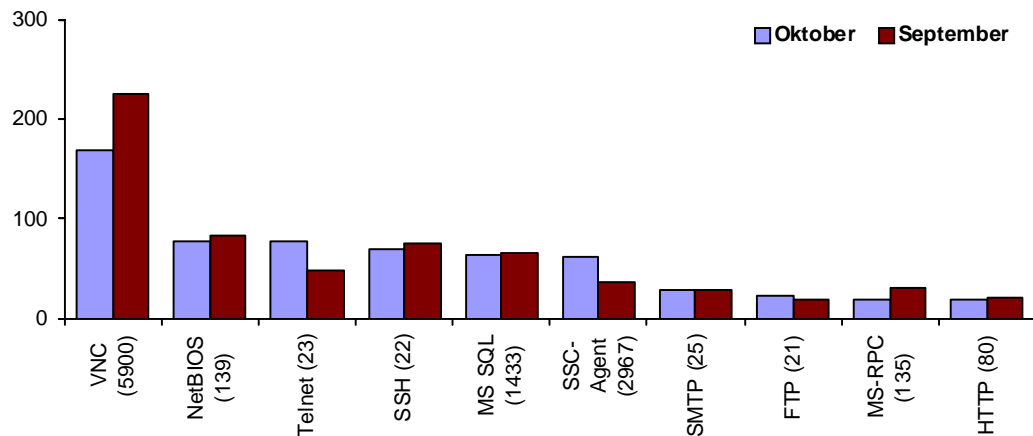
Reconnaissance attacks per monitored C-Net



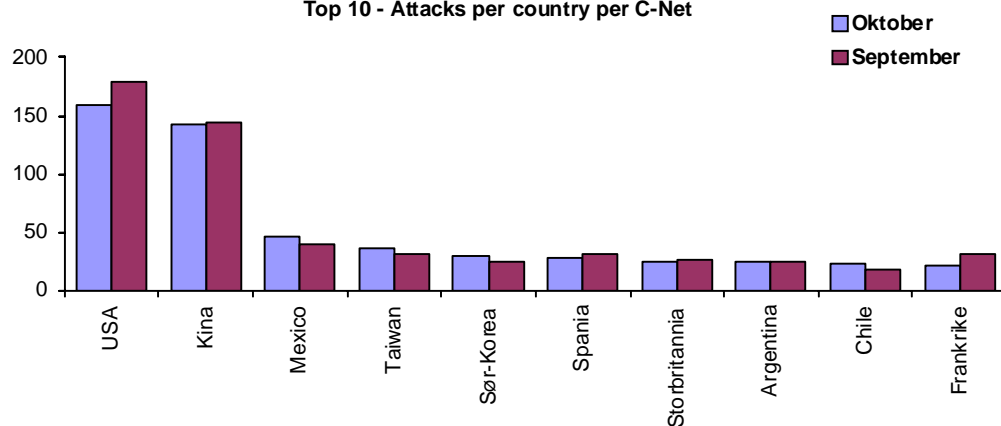
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net

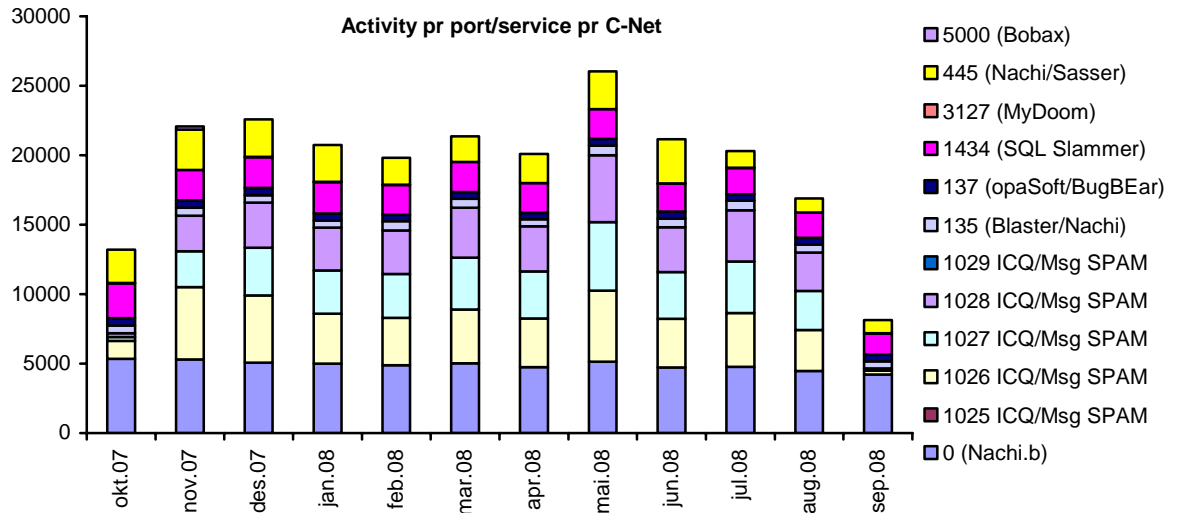


It is observed a slight decrease in number of reconnaissance attacks this month. The searched services are in general the same as previous periods, with VNC as the most frequent type of incident. The VNC scans increased towards the end of the period, something that is reflected in the "Attacks pr date" chart. This increase was caused by the fact that it has been several small distributed scans from countries in the South-America. These scans are the main cause to Mexico, Argentina and Chile appearing in the Top 10 list over attacking countries.

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.



The worm activity continues to decrease this month. Microsoft SQL Monitor and Microsofts er the most frequent searched services. As previous month, it is observed very little messenger spam.