

SECURITY THREATS AND TRENDS

SEPTEMBER 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 treat the term Cloud Computing.

The alert statistic shows that the majority of alerts occur in the Internet zone, while severe alerts mostly occur in restricted zone.

The number of reconnaissance attacks from the Internet remains at a stable level. The most searched service is VNC. Poland, the US and China are the three most attacking countries.

Spam and Internet activity remain 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 – CLOUD COMPUTING	8
ALERT STATISTIC.....	10
HANDLED ALERTS	10
REPORTED INCIDENTS.....	11
THREAT LEVEL.....	12
RECONNAISSANCE ATTACKS JULY 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. 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

AWStats Totals Code Execution and Cross Site Scripting Vulnerabilities
<http://userwww.service.emory.edu/~ekenda2/EMORY-2008-01.txt>

Ubuntu issues security patch for kernel flaw
<http://www.ubuntu.com/usn/usn-637-1>

IBM WebSphere Portal Remote Authentication Bypass Vulnerability
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK67104>

Sun rdesktop Code Execution and Denial of Service Vulnerabilities
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-240708-1>

VLC Media Player TTA Data Processing Integer Overflow Vulnerability
<http://www.orange-bat.com/adv/2008/adv.08.16.txt>

Vulnerability in Cisco WebEx Meeting Manager ActiveX Control
<http://www.cisco.com/warp/public/707/cisco-sa-20080814-webex.shtml>

VMware ESXi OpenSSL Vulnerabilities
<http://secunia.com/advisories/31489/>

Sun Java System Web Proxy Server Denial of Service Vulnerability
<http://www.frsirt.com/english/advisories/2008/2366>

August 2008 Black Tuesday Overview
<http://isc.sans.org/diary.html?storyid=4876>

Microsoft Security Bulletin MS08-051 – Critical
<http://www.microsoft.com/technet/security/Bulletin/MS08-051.msp>

Microsoft Security Bulletin MS08-041 – Critical
<http://www.microsoft.com/technet/security/bulletin/MS08-041.msp>

Ubuntu Security Update Fixes xine-lib Code Execution Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/2333>

Trend Micro Products ObjRemoveCtrl Class Buffer Overflows
<http://secunia.com/advisories/31440/>

HP-UX Unspecified libc Flaw Lets Remote Users Deny Service
<http://securitytracker.com/alerts/2008/Aug/1020637.html>

Gentoo Security Update Fixes Wireshark Denial of Service Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/2303>

Sun Solaris Adobe Reader Code Execution and Security Bypass Issues
<http://www.frsirt.com/english/advisories/2008/2289>

Apache Tomcat 6 Cross-Site Scripting and Security Bypass
<http://secunia.com/advisories/31381/>

Sun Java Update Component Lack of Digital Signatures
<http://securitytracker.com/alerts/2008/Jul/1020584.html>

OpenOffice Update Component Lack of Digital Signatures
<http://securitytracker.com/alerts/2008/Jul/1020583.html>

Apple Mac OS X Code Execution and Security Bypass Vulnerabilities
<http://www.frsirt.com/english/advisories/2008/2268>

IN THE NEWS

Revealed: The Internet's Biggest Security Hole
<http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html>

Laptop boot passwords vulnerable to attack
<http://www.heise-online.co.uk/security/Laptop-boot-passwords-vulnerable-to-attack--/news/111403>

Faren over etter virus-spredning på MSN.no
<http://www.digi.no/php/art.php?id=784099>

WhiteHat Report Finds Web Site Security Vulnerabilities Persist
<http://www.eweek.com/c/a/Security/WhiteHat-Report-Finds-Web-Site-Security-Vulnerabilities-Persist/>

Most organizations fail to stop interior network threats
<http://www.net-security.org/secworld.php?id=6454>

SSH Key-based Attacks
http://www.us-cert.gov/current/index.html#ssh_key_based_attacks

Phishers Bite Back with Malware Exploits Linked to Keywords
<http://www.eweek.com/c/a/Security/Phishers-Bite-Back-With-Malware-Exploits/>

Facebook Hacks Here they come. It was bound to happen.
<http://www.stephenbailey.com/business/082008-facebook-hacks/>

A Security Assessment of the Internet Protocol
http://www.schneier.com/blog/archives/2008/08/a_security_asse.html

X-Force 2008 Mid-Year Trend Statistics
<http://www-935.ibm.com/services/us/iss/xforce/midyearreport/>

SSLVPN Vulnerabilities - Client Certificates offer a superior defense over OTP devices
<http://www.networkworld.com/community/node/31124>

Thoughts on the Russia vs Georgia Cyber War
<http://isc.sans.org/diary.html?storyid=4903>

What is worse than reusing passwords?
<http://www.itworld.com/tech-society/54193/beware-meta-password-reuse>

DNS creator: It's time to add security
<http://news.zdnet.co.uk/security/0,1000000189,39459935,00.htm>

Mystery web attack hijacks your clipboard
http://www.theregister.co.uk/2008/08/15/webbased_clipboard_hijacking/

FOCUS OF THE MONTH – CLOUD COMPUTING

Cloud computing is a term used within the Internet world to describe the current evolution of how the web is used by people and organizations, and what direction the IT industry seems to take. But what is this really?

Cloud computing as a term refers to the metaphor of Internet being a “cloud”. There are some differences in how to define it, but generally Cloud computing are used as a description of an Internet based platform, with the belonging distribution utilities. Through Cloud computing, IT related resources (services, servers, capacity) are offered as a service through Internet.

Cloud computing are also mixed together with Web 2.0. Web 2.0 is neither a concrete product or technology, but are used as a description of “the new web”, ergo the changed way of how Internet are used for share of information, hosted services and social networks. Examples of Web 2.0 services are Facebook, YouTube and Google Apps.

Heading for the Clouds

Cloud computing is making its way both into private homes and into the business world. The technological progress has lead to more distributed environment, more high-speed lines, lower storage costs, wireless high-speed networks and a growth in handheld units with Internet access. All these factors are part of making it easy for users to access data and use applications placed at remote servers.

Cloud computing is also reckoned to be useful for large organisations that have many users on different locations, and that for example use specialized software to perform data- and resource intensive tasks.

A research made of Pew Research Center shows that 69 percent of the Internet users use one or another form of Cloud computing. 56 percent say they use a web mail service (f.ex. Hotmail). 40 percent say they use Cloud computing for at least 2 activities. The table below shows what services users use through Cloud Computing:

Cloud Computing Activities	
<i>Internet users who do the following online activities (%)</i>	
Use webmail services such as Hotmail, Gmail, or Yahoo! mail	56%
Store personal photos online	34
Use online applications such as Google Documents or Adobe Photoshop Express	29
Store personal videos online	7
Pay to store computer files online	5
Back up hard drive to an online site	5
<i>Source: Pew Internet & American Life Project April-May 2008 Survey. N=1,553 Internet users. Margin of error is ±3%.</i>	

The majority of users state simplicity and the possibility to access their data from any internet connected item as the main reason for why they uses Cloud Computing. An other important reason is the possibility to share information.

Despite the popularity of Cloud computing, 90 percent of the users say that they would be concerned if the vendor was sold to another party. 68 percent say they would be concerned if their data was used for targeted advertisement, and 49 percent say they would be concerned of their data was sold to others or given to law-enforcement bodies.

The high use of cloud applications combined with people's concerns shows "people use it more than they understand it", said John Horrigan, Pew's associate director for research.

Cloud Computing – security risks

For organizations there are several security risks by placing parts of their operations at the web. It is especially important to secure the information, since storage and processing of data will be excluded from physical and logic security within own locations. And the owner of the data is in the end responsible for the security and integrity of their own data.

The nature of Cloud computing makes it important to perform risk measurements within the areas of data integrity, data recovery and privacy, since these aspects constitute potential security risks.

Necessary security issues that should be raised before selecting a cloud vendor:

- Risk measurements from a 3rd party
- Avoid vendors that don't give out detailed information about the security. Ask for documentation on how the vendor have secured their servers and networks
- Description of how disaster recovery is handled
- Demand that the Cloud vendor must have a regulator compliance with external audit and certifications at the same level as a traditional vendor
- Provide for long-term viability of the data. If the vendor go broke or is bought by another company, the data must still be available

Web attacks

As the use of the Internet has changed, so has the Internet treaths:

- The attack focus have changed from operative system towards browsers and multimedia applications
- The number of vulnerabilities related to web server applications is increasing, and so are the numbers of attacks against these

The fact that data that normally was stored on a users PC now is moved out into web applications, has opened for a new trend of attack. This trend is a result of web-based applications being run in the browser, and the browser itself is highly exposed to vulnerabilities and exploits. During the first half-year of 2008, it was in 64 percent of the cases published exploit code the same day as browser related vulnerabilities was released. Plug-ins for browsers are particular exposed, and stands for 78 percent of the published browser-related exploits.

Sources

<http://www-935.ibm.com/services/us/iss/xforce/midyearreport/>

http://en.wikipedia.org/wiki/Cloud_computing

<http://www.networkworld.com/news/2008/070208-cloud.html>

<http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>

ALERT STATISTIC

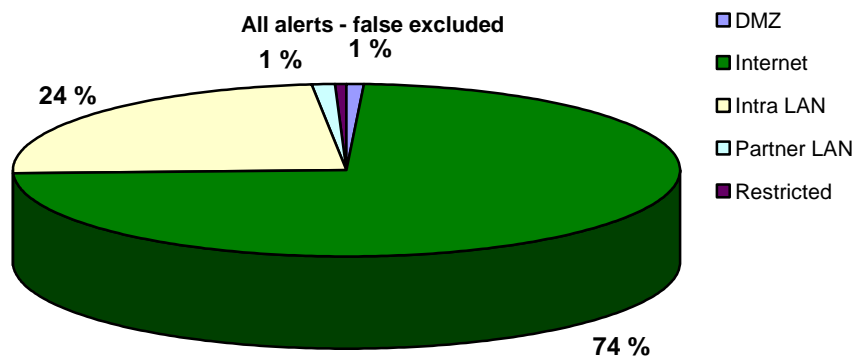
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

HANDLED ALERTS

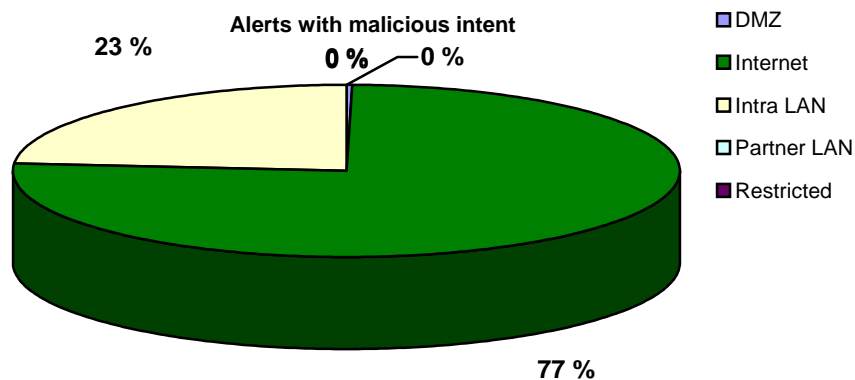
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

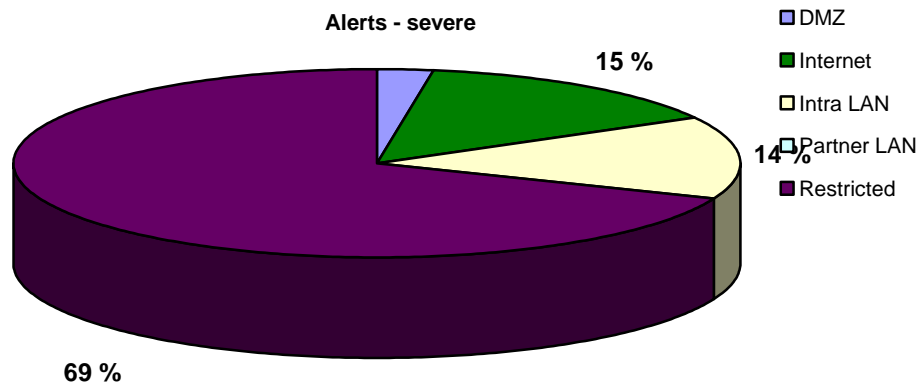
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



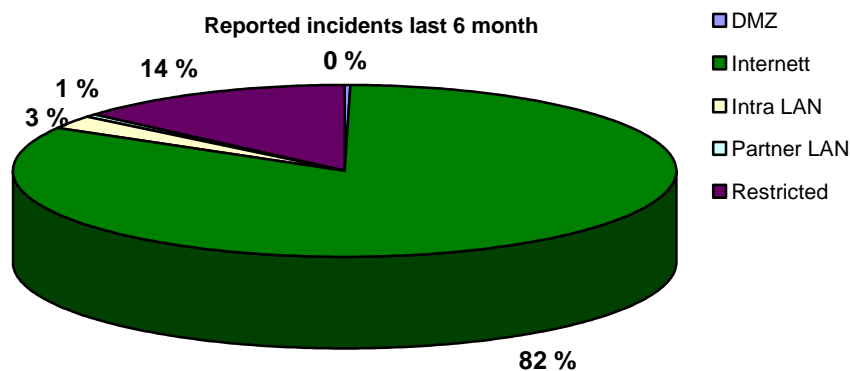
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

Most of the alerts occur in the Internet segment, but these are rarely of severe character. The alerts from the Internet segment are mainly web attacks, some of them are targeted while some of them are random Internet “interference”. None of Secode’s customers have been vulnerable to any of the recorded web attacks.

The majority of the severe alerts are detected within restricted zone. Typical for this zone, is that the traffic pattern is strictly defined, and everything that differ from this trigger off an alert.

REPORTED INCIDENTS

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



The main percentage of reported incidents from the Internet is mainly directed attacks towards financial institutions.

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

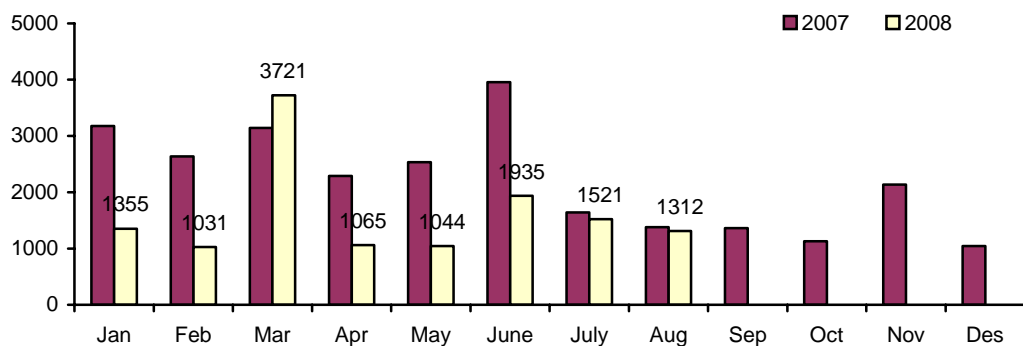
THREAT LEVEL

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.

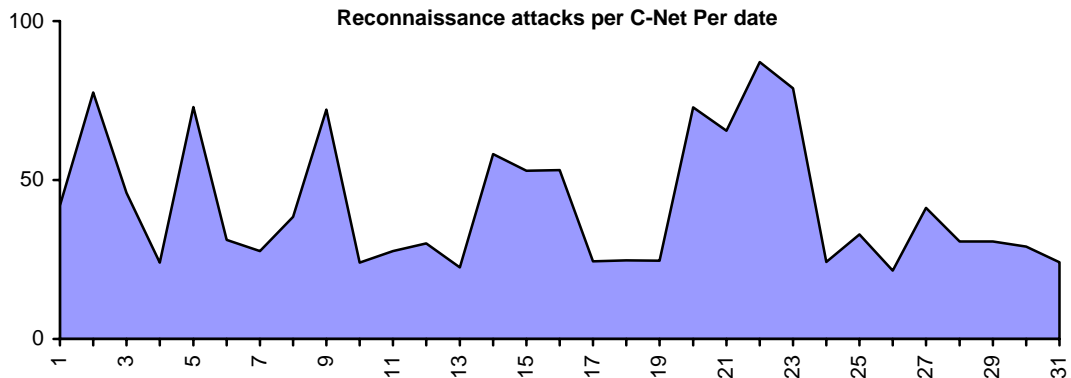
RECONNAISSANCE ATTACKS JULY 2008

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.

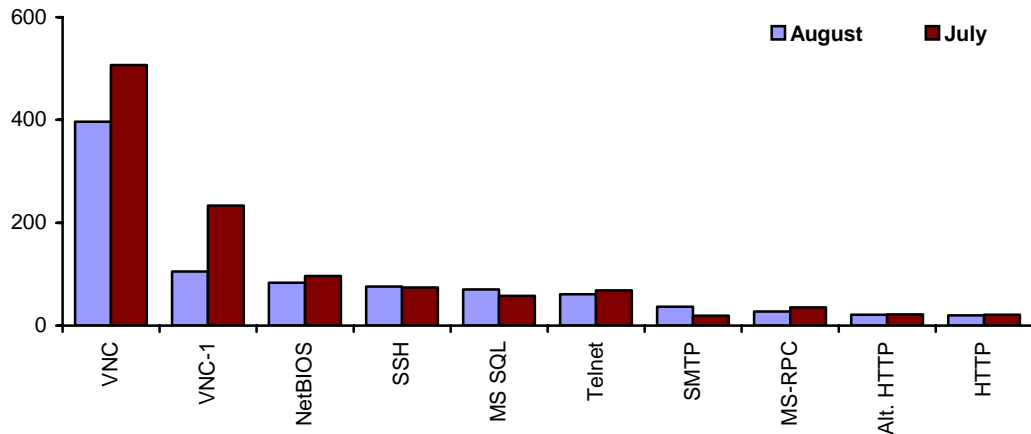
Reconnaissance attacks per monitored C-Net



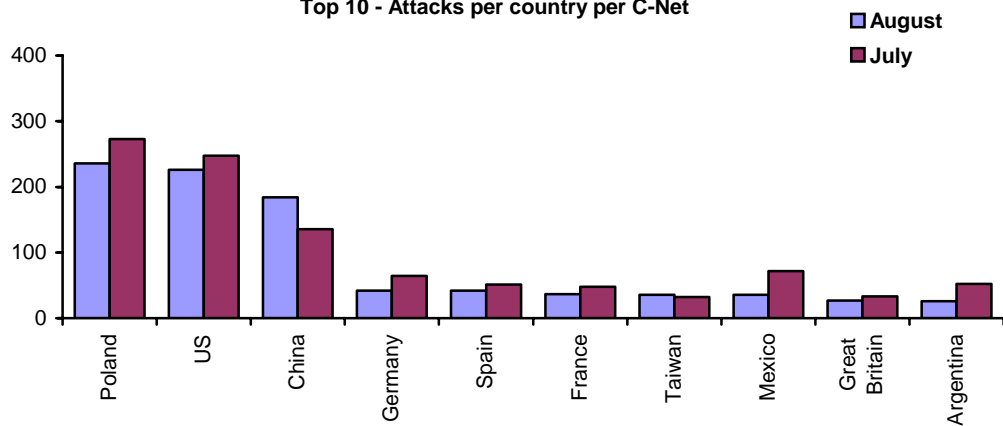
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net

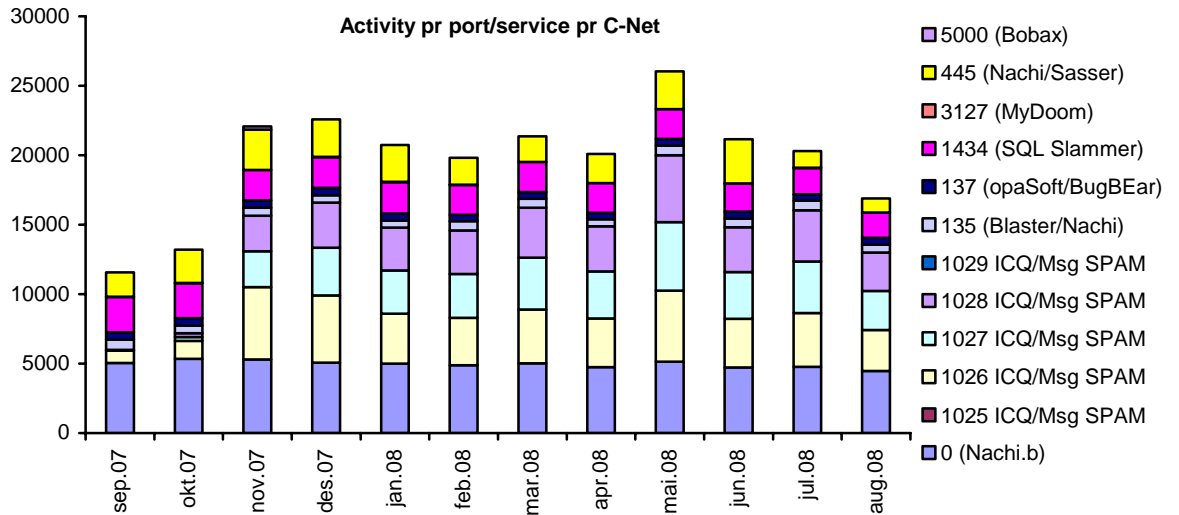


It is only observed minor changes within the reconnaissance attacks this month. The VNC is still the most attacked service (tcp port 5000 and 5001), and traffic towards this service occur all hours of the day. Poland is the most frequent source of attacks, followed by the US and China.

All of the services above are known to have severe vulnerabilities related to them. According to security researcher Fyodur - the creator of the scanning tool Nmap - it is the services HTTP (port 80), Telnet (port 23), SSH (port 22) og HTTPS (port 443) which are most frequently left open towards the Internet. He claimed this during the DEFCON hacking conference, after his last scanning of millions of Internet connected computers.

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 targeting the different services in the statistic above remains at a stable level. Besides pinging, the most hit services are messenger services (spam) and MS SQL server (slammer worm).

According to the mid-year report from X-force, “complex” spam (spam using pictures, pdf’s, html) is now on decline, while simpler URL spam is taking over. This is probably caused by the fact that URL spam is harder to detect by spam filters.