

# SECURITY THREATS AND TRENDS

## OCTOBER 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 Focus of the Month we look at Web 2.0 security.

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

The number of reconnaissance attacks from the Internet has decreased slightly this month. The most searched service is VNC, with a peak from the 8<sup>th</sup> to 12<sup>th</sup>. The US, China and Poland are the three most attacking countries.

For spam activity we see a decrease in the level of messenger spam. The other categories in spam and worm traffic remain stable.

## 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 – WEB 2.0 SECURITY.....</b>	<b>8</b>
WEB 2.0 .....	8
WEB 2.0 SECURITY .....	8
WEB 2.0 SECURITY ENHANCEMENTS.....	9
SOURCES.....	9
<b>ALERT STATISTIC.....</b>	<b>10</b>
HANDLED ALERTS .....	10
REPORTED INCIDENTS.....	11
<b>THREAT LEVEL.....</b>	<b>12</b>
RECONNAISSANCE ATTACKS SEPTEMBER 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

VMware ESX Server Multiple Vulnerabilities  
<http://secunia.com/advisories/31712/>

Carpet-bombing Vulnerability In Google Chrome New Browser  
<http://cyberinsecure.com/carpet-bombing-vulnerability-in-google-chrome-new-browser/>

Cisco PIX and ASA Information Disclosure and DoS Vulnerabilities  
<http://www.cisco.com/warp/public/707/cisco-sa-20080903-asa.shtml>

Gentoo Security Update Fixes RealPlayer Code Execution Vulnerability  
<http://www.frsirt.com/english/advisories/2008/2496>

Cisco warns of new security risks  
<http://www.vnunet.com/vnunet/news/2225515/cisco-warns-security-risks>

Google issues first patches for Chrome  
[http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9114287&taxonomyId=17&intsrc=kc\\_top](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9114287&taxonomyId=17&intsrc=kc_top)

Apple QuickTime Multiple Remote Code Execution Vulnerabilities  
<http://www.apple.com/support/downloads/quicktime755forwindows.html>

MySQL Empty Bit-String Literal Denial of Service  
<http://bugs.mysql.com/bug.php?id=35658>

Four vulnerabilities in Joomla eliminated  
<http://developer.joomla.org/security.html>

Serious vulnerability in phpMyAdmin [Update]  
<http://www.heise-online.co.uk/security/Serious-vulnerability-in-phpMyAdmin-Update--/news/111546>

Yahoo, Hotmail, Gmail all vulnerable to Palin-style password-reset hack  
[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9115187&taxonomyId=17&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9115187&taxonomyId=17&intsrc=kc_top)

### IN THE NEWS

Common usernames get more spam  
[http://www.theregister.co.uk/2008/08/29/spam\\_prevalance\\_research/](http://www.theregister.co.uk/2008/08/29/spam_prevalance_research/)

Cross-site hacks and the art of self defence  
[http://www.theregister.co.uk/2008/08/29/hijacked\\_browser/](http://www.theregister.co.uk/2008/08/29/hijacked_browser/)

Google 'starting from scratch' with own browser, Chrome  
[http://news.cnet.com/8301-17939\\_109-10029914-2.html?tag=mncol](http://news.cnet.com/8301-17939_109-10029914-2.html?tag=mncol)

Report: N. Korea Used Spyware, Sex in Targeted Attack on S. Korean Military  
[http://www.darkreading.com/document.asp?doc\\_id=162898&WT.svl=news1\\_1](http://www.darkreading.com/document.asp?doc_id=162898&WT.svl=news1_1)

Zombie network explosion

[http://www.theregister.co.uk/2008/09/02/zombie\\_surge/](http://www.theregister.co.uk/2008/09/02/zombie_surge/)

Secure Computing to Acquire Security to Drive Next-Generation Firewalls

<http://www.eweek.com/c/a/Security/Secure-Computing-to-Acquire-Security-to-Drive-Next-Generation-Firewalls/>

Open source release takes Linux rootkits mainstream

[http://www.theregister.co.uk/2008/09/04/linux\\_rootkit\\_released/](http://www.theregister.co.uk/2008/09/04/linux_rootkit_released/)

What You Really Need to Know About Data Leak Prevention

[http://www.darkreading.com/document.asp?doc\\_id=163021&WT.svl=news1\\_4](http://www.darkreading.com/document.asp?doc_id=163021&WT.svl=news1_4)

Trend virus update freezes some PCs

[http://www.theregister.co.uk/2008/09/08/trend\\_security\\_false\\_alarm/](http://www.theregister.co.uk/2008/09/08/trend_security_false_alarm/)

Survey says you can trust IT as far as you can throw it

<http://blogs.techrepublic.com.com/career/?p=396>

Threat to computers for industrial systems now serious

[http://www.infoworld.com/article/08/09/10/Threat\\_to\\_computers\\_for\\_industrial\\_systems\\_now\\_serious\\_1.html](http://www.infoworld.com/article/08/09/10/Threat_to_computers_for_industrial_systems_now_serious_1.html)

Internet Attack Fears Keep IT Security Spending on the Menu

<http://www.eweek.com/c/a/Security/Internet-Security-Fears-Keep-IT-Security-Spending-on-Menu/>

Hackers attack Large Hadron Collider

<http://www.telegraph.co.uk/earth/main.jhtml?xml=/earth/2008/09/12/scicern212.xml>

New tool creates fake YouTube pages for spreading malware

[http://news.cnet.com/8301-1009\\_3-10039974-83.html](http://news.cnet.com/8301-1009_3-10039974-83.html)

One Google data center idea that really floats

<http://www.networkworld.com/news/2008/091608-google-data-center.html?hpg1=bn>

Securing Your Network Premises With Endian

<http://www.linux.com/feature/147054>

Hackers prevent research on malicious code

<http://www.securecomputing.net.au/News/123066,hackers-prevent-research-on-malicious-code.aspx>

Identity theft bill set for approval

<http://www.vnunet.com/vnunet/news/2226560/identity-theft-bill-set>

85% of malware is now distributed through the Web

<http://www.net-security.org/secworld.php?id=6550>

Two-thirds of firms hit by cybercrime

<http://www.securityfocus.com/brief/825>

Clickjacking: Researchers raise alert for scary new cross-browser exploit

<http://blogs.zdnet.com/security/?p=1972>

Gartner: Security risks rise as smart phones get smarter

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9115782&taxonomyId=17&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9115782&taxonomyId=17&intsrc=kc_top)



## FOCUS OF THE MONTH – WEB 2.0 SECURITY

In an article released September 24<sup>th</sup> at Digi.no, Heidi Arnesen Austlid stated that companies have to relearn web-use from young people. The youth have grown up with the Web 2.0 systems at their side. They are used to sharing their private information on the web, leaving little information secret. The idea of making more company information available through the Internet is good and promising, but what about security?

### WEB 2.0

Web 2.0 is a term used to describe the changes in use of the World Wide Web. It does not refer to any technical update, but how the end-users and software developers utilize the web. Examples of so-called Web 2.0 “products” are blogs, wikis, podcasts, and social software and so on. eBay, Wikipedia, Facebook, YouTube and MySpace are all Web 2.0 sites.

Web 2.0 sites are characterized by the fact that users interact with the site rather than just retrieve information. Sites even encourage users to add value to the application as they use it. You can say that Web 2.0 characteristics are; rich user experience, user participation, dynamic content and scalability. The sites enhance creativity both from the users and from the service provider.



Figure 1 Tag cloud [1]

### WEB 2.0 SECURITY

As the Internet developed towards including the World Wide Web there were many questions about how to keep it secure. The development was carried out faster than the security measures were able to. This in turn made sites more complex to secure. We see the same development now. As new features, applications and possibilities surface at the web, the security issues are set aside to keep on developing at a great level. To keep up with the competition on the web the service providers need to speedily develop new features, and in terms they downgrade the security aspect of the development.

In the last couple of months, several articles have been published through different media about the insecurity we are facing in the applications. YouTube has malware in the videos, Facebook is facing malware in “plug-in” applications and so on. In addition, links that were previously shared by mail are now posted in guestbooks and the like. Many of these links are directing users to insecure websites. There are also some general articles about security in Web 2.0, and that indicates that security now has become an issue.

The security problems are many. The direct manipulation of code made by others is one problem, this since the code language in most cases is know and relatively easy. Other problems include the fact that “everybody” is able to contribute to Web 2.0 sites. Adding videos with malicious code is one example of such a problem. There is no strict

authentication for making contribute to the site; this means that people with malicious intent are let in the same as anybody else. Another problem is that these sites are mainly reviewed as trusted by different anti-malware systems. In other words, malware filters will probably not react on the malicious content since the site is trusted. Implementation of security is also pretty difficult, since the sites are supposed to be dynamic. The last problem is privacy itself. Because people are giving away information “here and there” hackers are able to gather much, if not all, of the information needed to carry out large attacks. Social engineering attacks have become easier after information started to become more available for instance. One good example of this is how users have started giving away work information on Facebook. It is no problem finding the name of an employee at a company and information about that person that “only friends” would know.

Certain technical security features are implemented in some of the sites however. Facebook has implemented a verification tool for applications. MySpace and Facebook are making it easier to keep your data only available for people you know. Other than this, most Web 2.0 sites rely on their users to discover, report and in some cases even remedy security issues. They hope that in making it a challenge, improving the site (including its security) will be appealing work for the users to demonstrate their skills and abilities.

## WEB 2.0 SECURITY ENHANCEMENTS

More Web 2.0 applications will be available in the future, and security will be a bigger problem. At this time we see that it is important to at least try and make security an issue in applications in the future. Verification of applications on all such sites is one possibility. Another one is to make “security tips” more available at the sites. Most sites have a security site warning about making too much information available, but they are often “hidden” in a submenu. What about new sites?

It is likely that there will be standardizations in the future, making it easier to implement security features at the sites. As more sites utilize common standards, developers can create “standard” security features as well. Web Content filtering systems are possible to filter out parts of a site (ads, pop-ups and so on). Use of IDS, anti-malware, log-systems and so on can help with some of the threats, and by letting security experts look at the logs from these systems, problems may be discovered more rapidly.

The most important thing however is that both users and companies are educated about how the use of these systems may affect their security.

## SOURCES

- [1] Wikipedia – Web 2.0  
[http://en.wikipedia.org/wiki/Web\\_2.0](http://en.wikipedia.org/wiki/Web_2.0)
- [2] Digi.no – Bedrifter må lære nettbruk av ungdom (Norwegian)  
<http://digi.no/php/art.php?id=787581>
- [3] Facebook – Application Verification Program  
<http://developers.facebook.com/verification.php>
- [4] MySpace – SafetyTips  
<http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips>

## ALERT STATISTIC

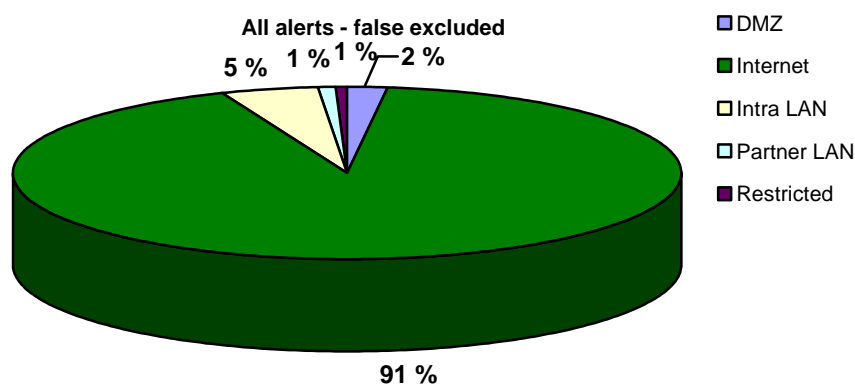
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts per net segment that are under surveillance.

### HANDLED ALERTS

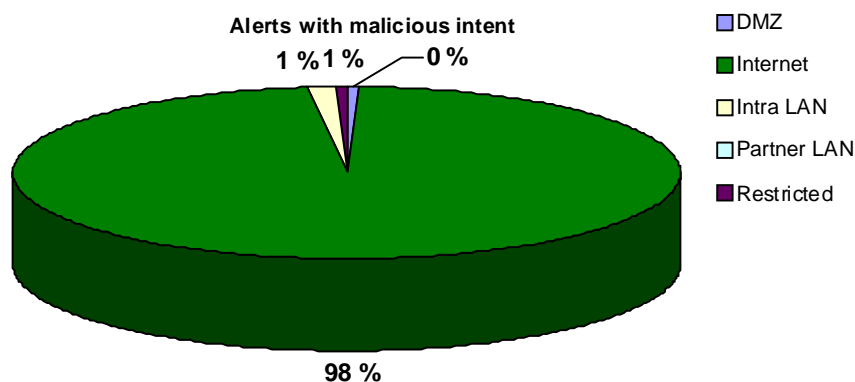
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are installed.

The network segments are divided into the following:

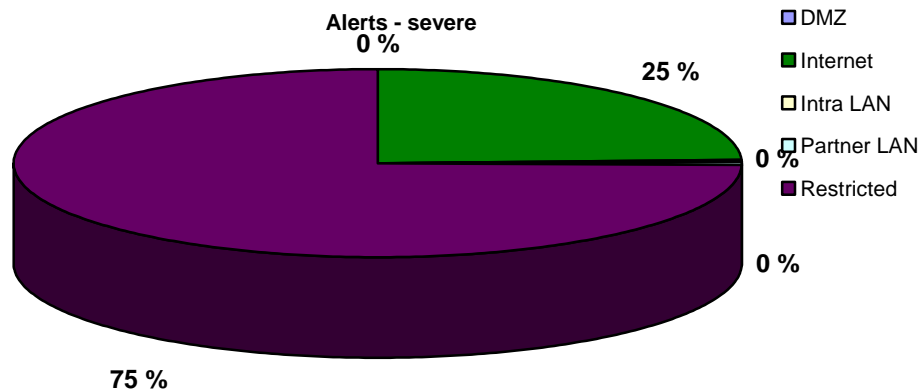
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is located inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is located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



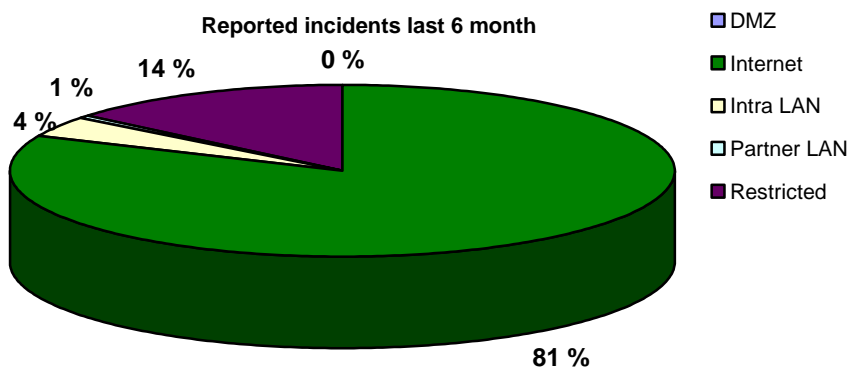
The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

Most of the alerts occur in the Internet segment, but these are rarely of severe character. This period we have seen an increase in the level of Brute Force attacks. These attacks originate from all over the world, and are not targeted against one particular customer or a group of customers. The attacks are automated and directed towards particular segments of the IP-address range. None of Secode's customers have been vulnerable to any of the recorded web attacks.

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

### REPORTED INCIDENTS

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



The incidents in the restricted zone are mainly ignorant users breaching a company policy. The incidents registered from the Internet are mainly directed attacks towards financial institutions.

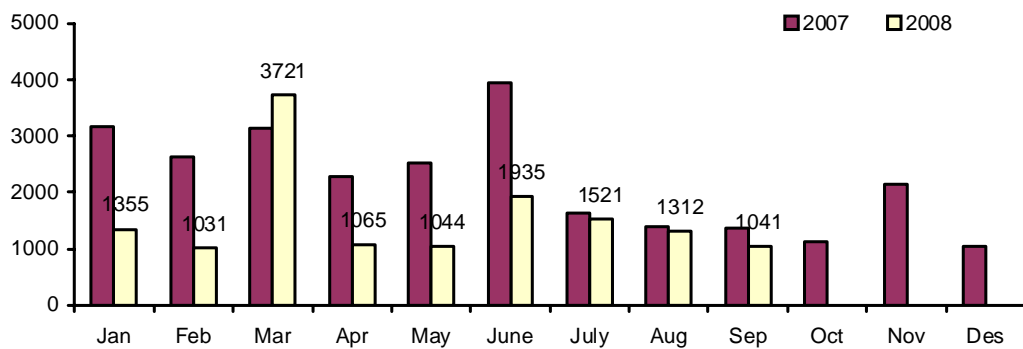
## THREAT LEVEL

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.

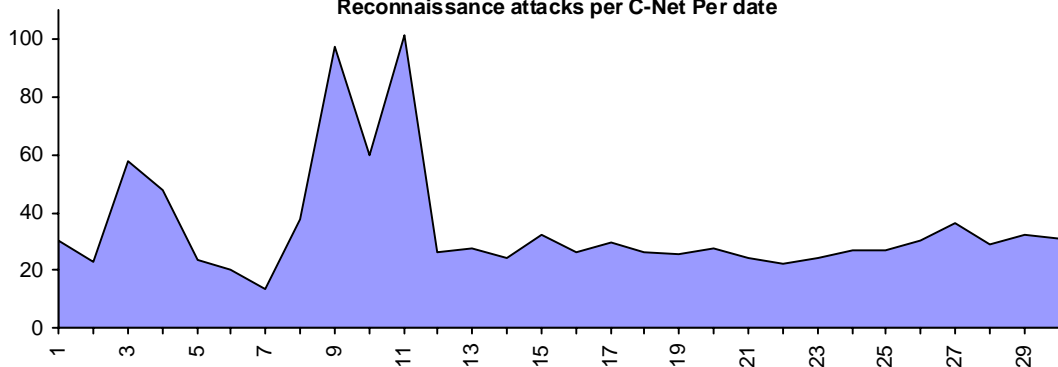
### RECONNAISSANCE ATTACKS SEPTEMBER 2008

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.

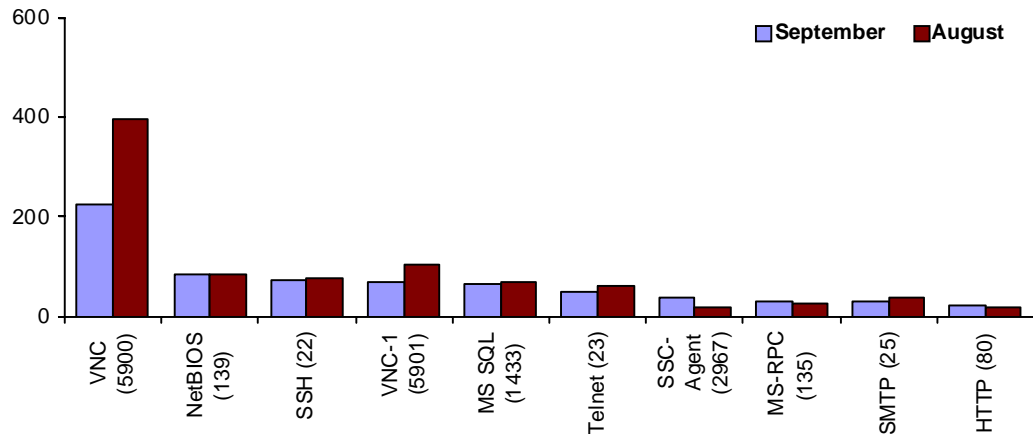
Reconnaissance attacks per monitored C-Net



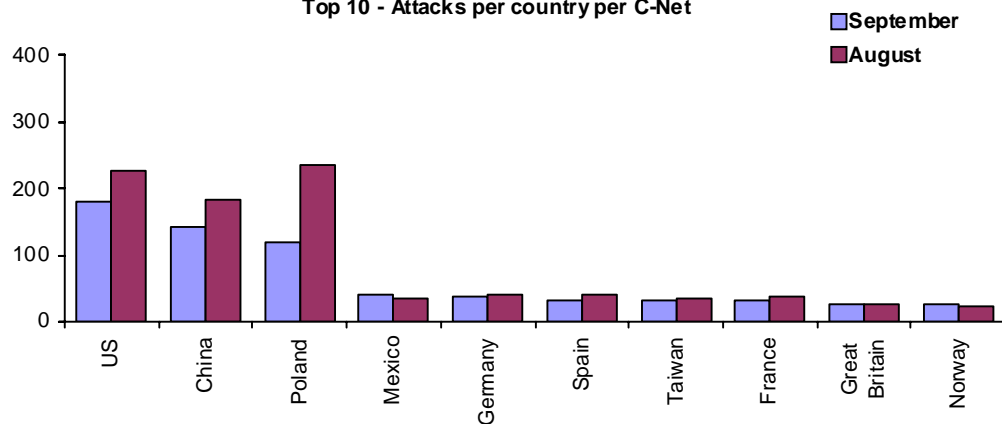
Reconnaissance attacks per C-Net Per date



Average top 10 incidents per C-Net



Top 10 - Attacks per country per C-Net

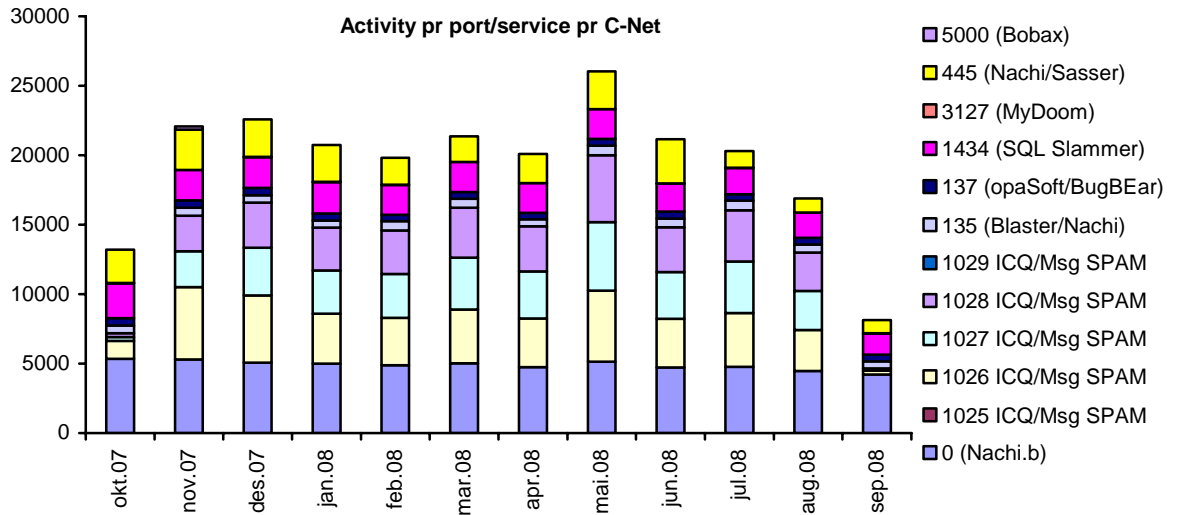


Only minor changes within the reconnaissance attacks have been observed this month. VNC is still the most attacked service (tcp port 5900), and traffic towards this service occur all hours of the day. There has been a peak in these attacks from the 8<sup>th</sup> this month until the 12<sup>th</sup>. The rest of the month we have seen a stable level of most kinds of attacks. The US is the most active source of malicious activities this period, followed by China and last months most active source, Poland.

All of the services in the statistics above are well-know services with known vulnerabilities. In other words, it is no surprise that these services are targeted.

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.



After several months with a lot of messenger spam we now see a drastic change in this category. There is almost no such spam registered this month. We have not found any indication why this change has happened at this point of time.

For the other categories, the traffic level remains stable.