

Surfing the web - a threat analysis,

for



by



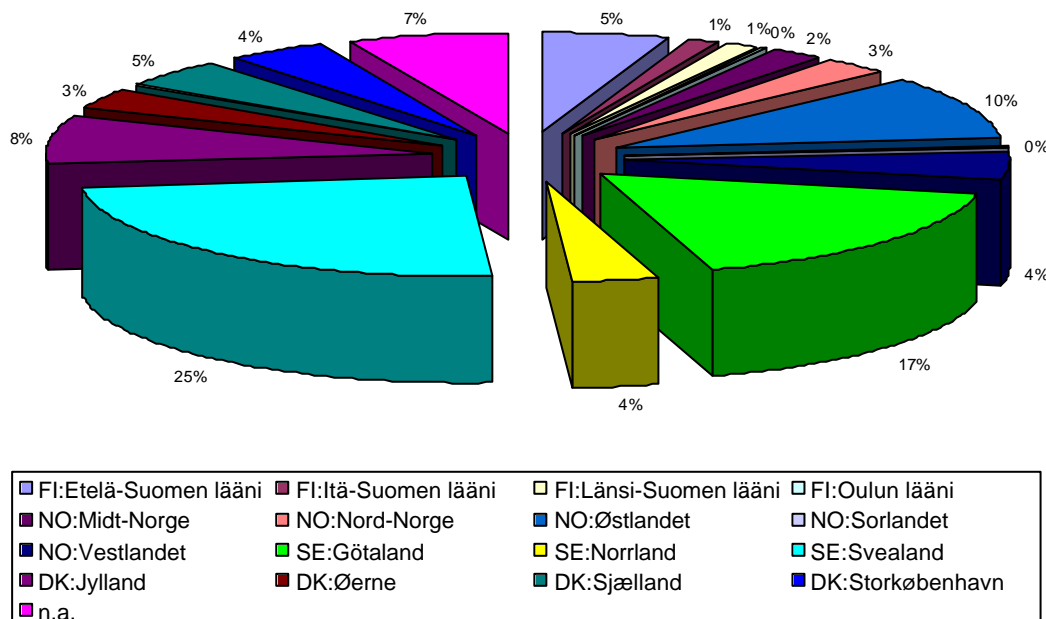
Situation

Surfing, e-mailing and chatting make the user subject of possibly harmful attacks on their systems. A survey for the Nordic region (Denmark, Finland, Norway, Sweden) reports surfing behaviour of the users, as well as a threat-analysis for using the web itself.

A total of 400 users showed their interest to be testpilots in the research via electronic newsletters to subscribers of IT-magazines. They described their surfing behaviour, techniques and programs being used, security means being used, damages already suffered and their general attitude for safety of data and data-transport.

300 valid reports from the testpilots were analysed for danger-evaluation in the Nordic region. Within this context, the users sent in log-files from Norton Personal Firewall 2001, with which they surfed the Internet during September 2001. This way, a comparison between objective dangers and subjective experience of danger was accomplished.

In what part of the country do you live?



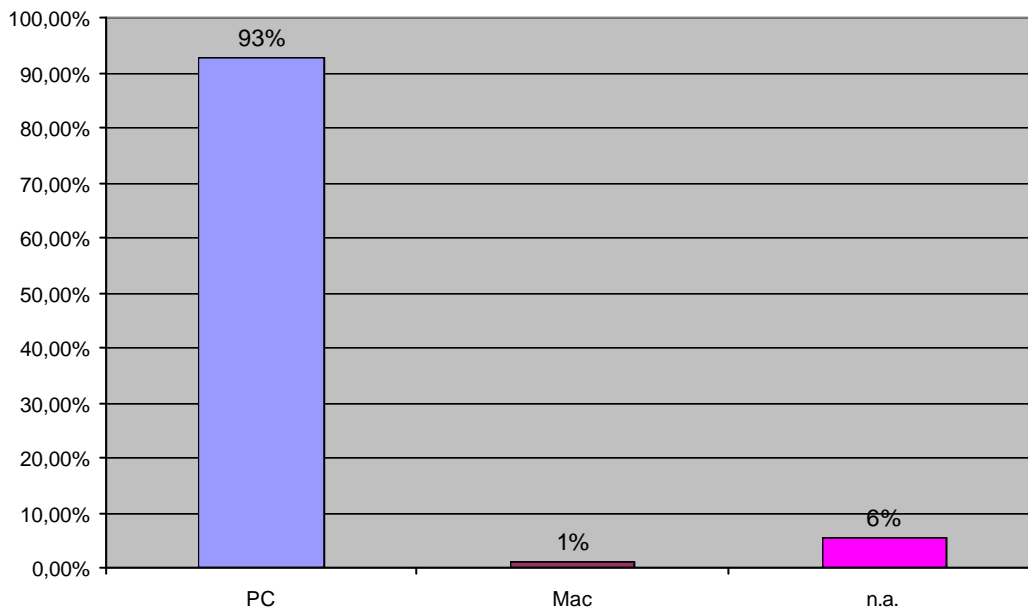
Survey for the Nordic's; divided by countries and regions

Systems

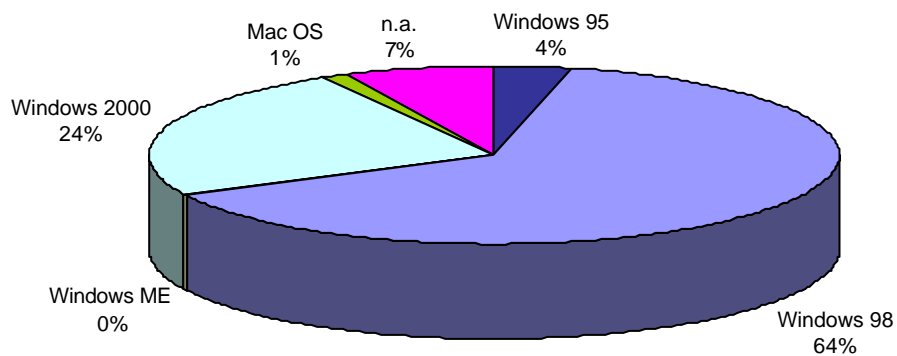
The great majority of users have Windows 98 as operating-system. Without patches and increased safety measures, an average Windows 98 system is to be regarded rather vulnerable. Especially for worms like NIMDA and Trojans, as they can cause major damages to the system, since they can take over the control of the computer. This is partly caused by programs of low security like an un-patched early Explorer or Outlook. Without Norton Personal Firewall being active, quite some systems would have been hacked with a high probability.

Platforms and operating-systems

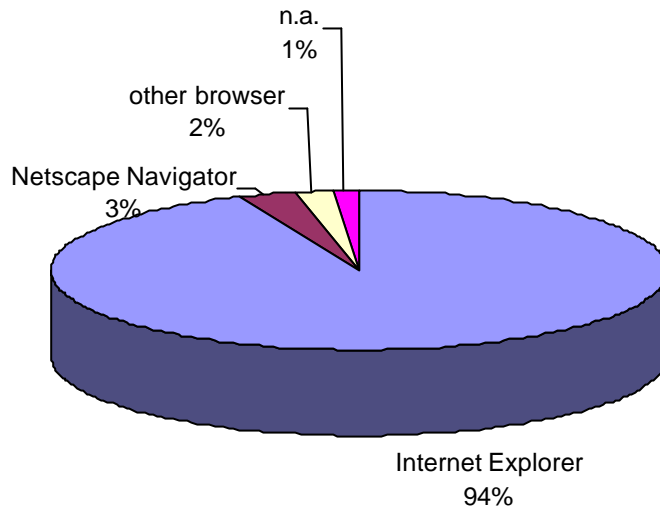
PC or Macintosh



Which Operating System are you using?

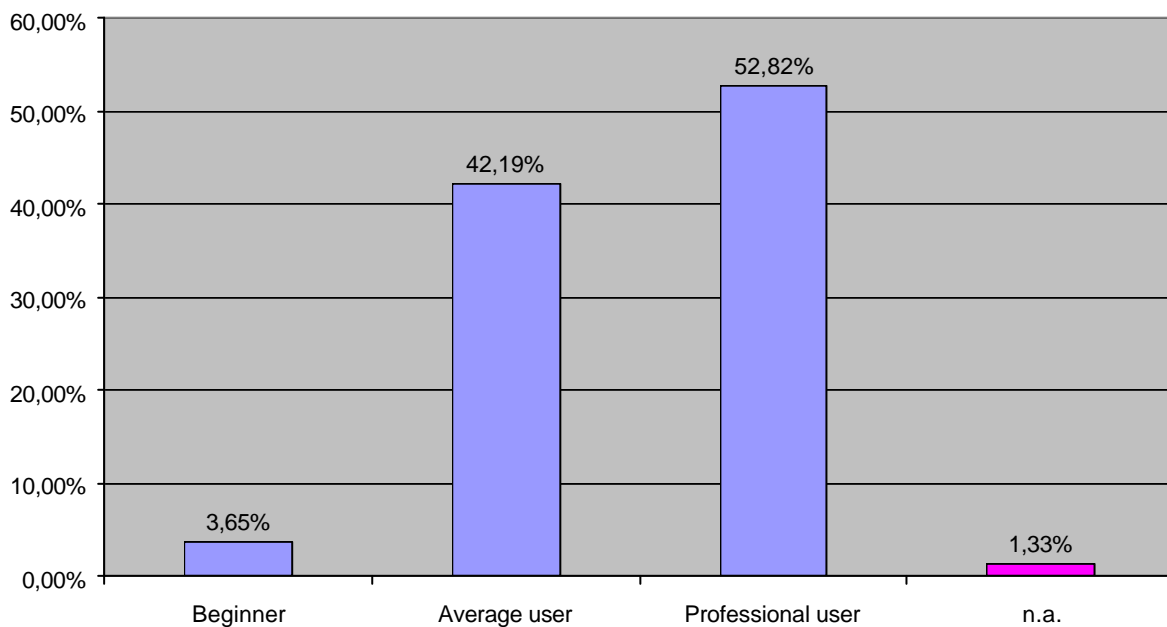


What type of browser do you use?



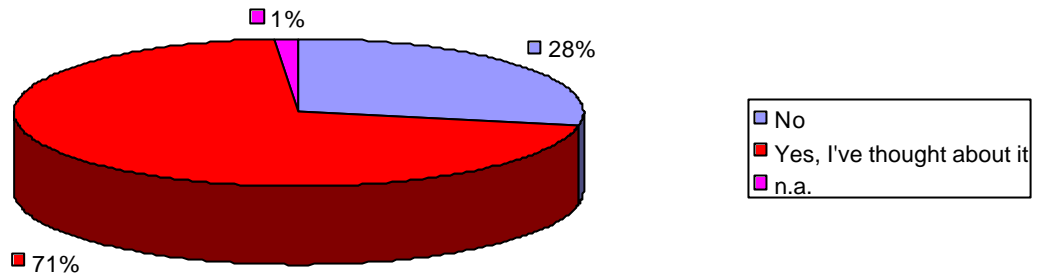
The majority of users have systems that are based on Microsoft-software only.

How would you describe your internet know-how?

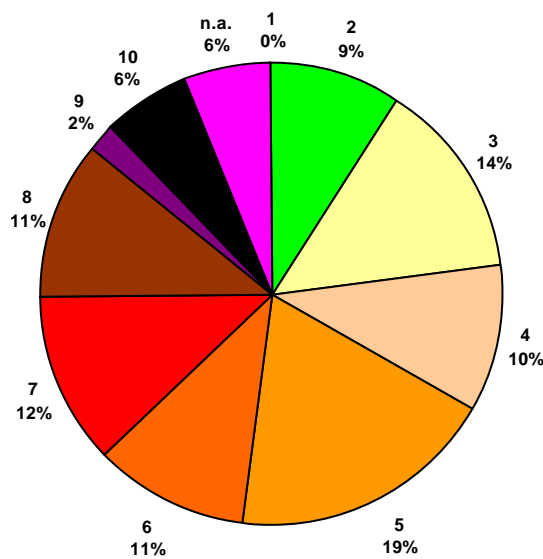


The testpilots in the survey are the essence average and professional users, both from own estimation and experience when analysing the log-files. Non-experienced users are more likely to be hacked.

Do you fear an attack on your computer?



On a scale from 1-10, how do you think the risk to be hacked is?

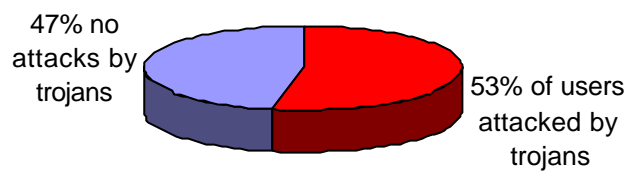


Subjective threat-experiences shows, that users are generally well aware of the dangers on Internet. Some bad experiences, as covered by the question for already suffered damages, will add to this. Quite some users already had security means installed.

Type of attacks

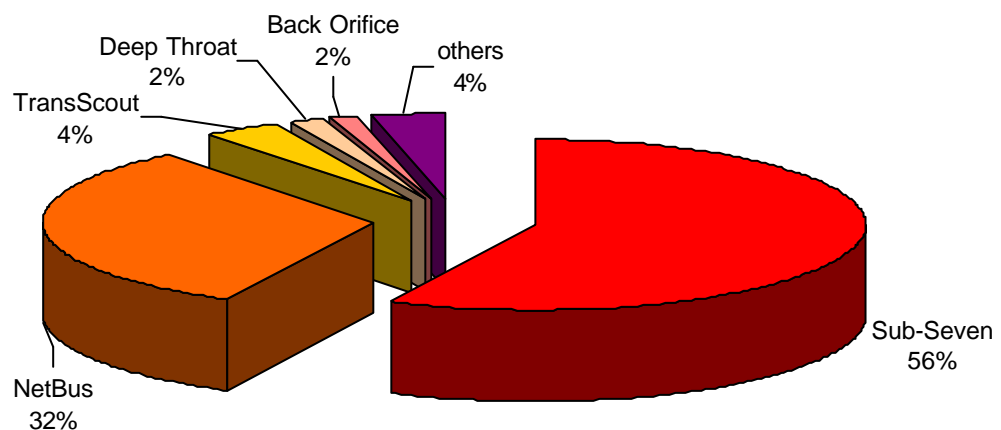
Of the 300 participants, 159 had contacts with possibly very harmful Trojans, plus intrusion attempts and port-scans. Together, about 240 users were seriously attacked. About all of the users were somehow molested by minor dangers. In addition to actively blocking known forms of attacks, Norton Personal Firewall filtered several thousand of non-valid data-packages.

Trojan attacks on users

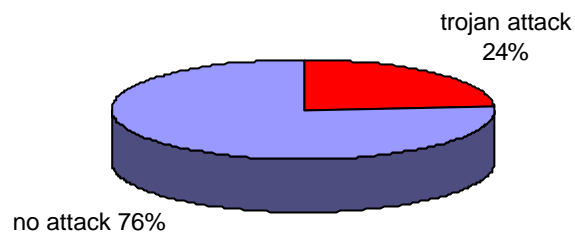


Trojan attacks, in total more than 1.500:

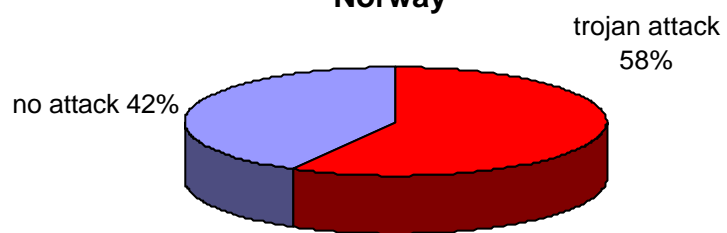
- ◆ Sub-Seven: 878
- ◆ NetBus: 493
- ◆ TransScout: 56
- ◆ Deep Throat: 26
- ◆ Back Orifice: 23



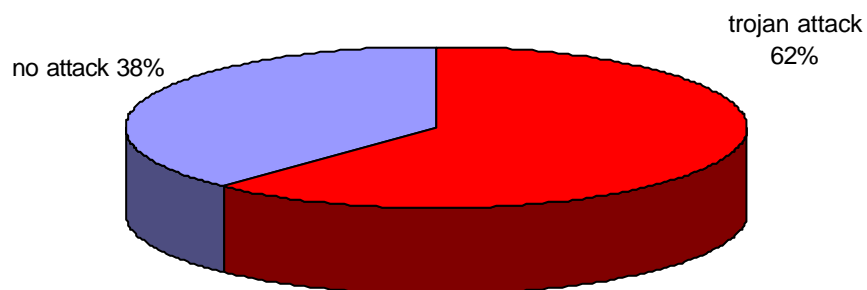
Finland



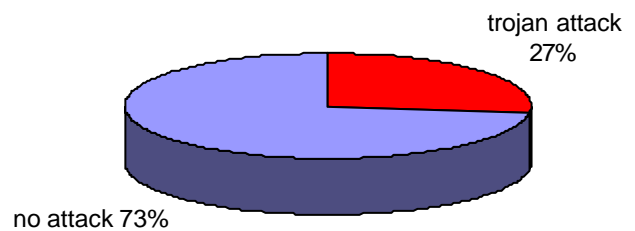
Norway



Sweden, most participants in the survey



Denmark



Swedish and Norwegian users are far more attacked by Trojans than Danish or Finnish users.

Sub-Seven

Sub-Seven is the most popular Trojan. It is able to take over the control of the infected system. There, Sub-Seven can do multiple damages. Its FTP-capability allows the attacker to upload or download files anytime at will. To do this, a Sub-Seven client can browse the computer just as a regular user. In addition to these already threatening capabilities, Sub-Seven can start or terminate programs or online-sessions. Also the manipulation of data in active use as take screenshots, altering the content of the screen (pop-up windows, additional direct data manipulation within programs), online-bugging and even the remote editing of the Windows-registry is possible.

A computer infected by Sub-Seven is dangerous for the network since Sub-Seven will find out passwords and gain access-rights to servers, so much more harm can be done than just by manipulating or deleting data on one local computer.

Nevertheless, the defences against Sub-Seven is rather simple. Its capabilities, the way of infection and handling the danger are well known.

NetBus and Back Orifice

Both Trojans are available as commercial harmless means to remotely manage a system, as well as malicious programs to intrude and take over a system. Their capabilities are similar to Sub-Seven. They can log all user-activities on the system. Also, they both can start and stop programs and even shut down the computer.

Their FTP-functions allow uploading and downloading of files. Together with the ability to execute any program, both systems are powerful and easy to maintain means of system-administration or massive threats to data-security.

Trans Scout, Deep Throat and others

Still pretty often found, these Trojans lack the wide spread in public. They are similar in terms of general abilities to the Trojans mentioned earlier. In terms of practical use, as means of attacks, they are less handsome for the hacker. Compared to the big number of Trojans, especially Sub-Seven, they are generally rare.

144 Trojan attacks in one month

Within the survey, two users from Sweden share the “record” for possible hacking attempts. During one month of surfing the worst exposed user had 144 “visits” from Trojans, 138 NetBus and 6 Sub-Seven. The second user had 139 Sub-Seven, 2 Deep Throat, 2 NetBus and one HackATack.

Danish users, smaller in numbers and therefore less likely to get extraordinary high attacks, have suffered up to 17 attacks per single user.

The biggest number of attacks to a Finnish user was 23.

A Norwegian user faced 118 attacks, followed by 76 attacks for the second one.

Together with minor numbers of Rat, Qaz, NetSphere, Blade Runner, Stealth Spy, ShockRave and Ultor, the total amount of possibly harmful Trojan-related events is beyond 1.500. Since some events could not be tracked to the definite occur of a Trojan, these were not added to the statistics.

Attacks from home

Not only websites were the source of attacks. Some 15 family-networks or small-business networks are infected by Trojans. Local computer addresses of Trojan attacks prove, that no direct connection to the web is necessary to get remotely controlled. A simple connection to an infected server is sufficient.

The survey could not find out, if those Trojans were intentionally installed to control a worker or a family-member. This seems unlikely and therefore those events have to be regarded as valid infections. So, defences have to be set up internally as well as towards the web.

Taken from a Norwegian user:

- ◆ *Regelen "Standardblokkering DeepThroat trojansk hest" blokkerte (krXXXXXX,2140).*

Swedish users most threatened

With 62 percent of the users attacked by Trojans, Swedish users are most threatened by Trojans. Norway is endangered almost at the same level. Denmark and Finland are relatively safe.

This may be a statistical deviation, since Swedish users were by far the majority in this survey. With rather few users from especially Finland, the real threat may be higher there.

Worms

There is no exact number of worm-attacks available. This is caused by two reasons. The firewall rejects most worms as non-valid communication of the system. An attack by a worm, will not be specified to the sample by most firewalls. Also, intensive media coverage of NIMDA, Code Red and Sircam forced most users to update their security-level.

Even if worm's only occurs in small numbers, possible consequences of worms are severe.

Once a worm gets hold of a system, it will spread itself to any contact in the address-book. This way, it spreads itself like an avalanche, infecting many users at the same time. The current threat-level of worms in the web has to be subdivided for Windows- and Unix-based systems.

Generally, worms are more harmful and more frequent for Windows. The worst sample active at this moment is NIMDA. It will go active by just previewing the infected message. Then, similar to a Trojan, it can take over control. In every case, NIMDA will spread by reading the address-book. It does not require Outlook or Outlook Express. Any MIME-compatible client will be used for reading the address-book and spreading the worm onwards.

The potential danger of NIMDA is its capability of jumping from server to the client and backwards. Classical worms were almost always limited to servers. With NIMDA and a new generation of worms, mass-infections can take place very fast.

The Norton Personal Firewall, as it was installed on the systems of the participants, blocks NIMDA reliably by denying it to address the system. Together with a virus-scanner, like included in Norton Internet Security, the threat of worms is minimized to almost nil.

Non-valid packages a possible danger

Possibly dangerous or useless data-packages were received in vast amounts. Several thousand events were recorded. Since worms or new Trojans could exploit security-leaks in operating systems or mail-programs by sending special packages, it is likely that numerous attacks were blocked.

Intrusion and port-scans

In addition to these automated attacks, a small number of likely menial-driven intrusion attempts were recorded. With deliberate aim, a computer is more likely to be successfully hacked.

More than 70 users experienced port-scans, a part of them done really profound.

A non-protected system with low security-standards is very vulnerable to port-scans. By directly addressing to system-services, a hacker will receive valuable information for further attacks. With some security-leaks especially in older systems like early Windows 95 or applications of that time, a hacker will be able to bore his way into the system.

To do this, hackers do not need high qualifications. Quite some websites or hacker-CDs provide an attacker with any means to do port-scans and to exploit them later on.

Two examples of port-scans, the first taken from a Swedish user, show how aggressively his computer was attacked. A complete scan was done on his machine:

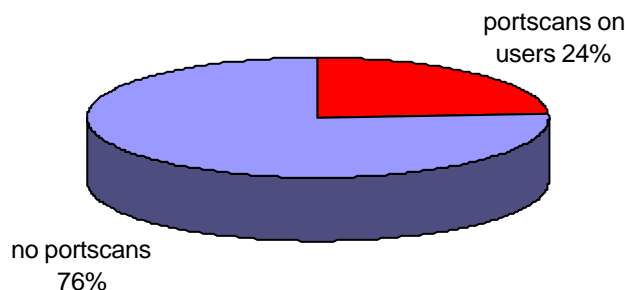
- ◆ *Portavsökning upptäcktes från adressen 192.168.10.X Minst 15 portar avsöktes.*

Users from other countries were massively scanned as well, as a Danish log-file proofs:

- ◆ *Portskanning konstateret fra adressen 192.168.1.X Mindst 11 porte prøves.*

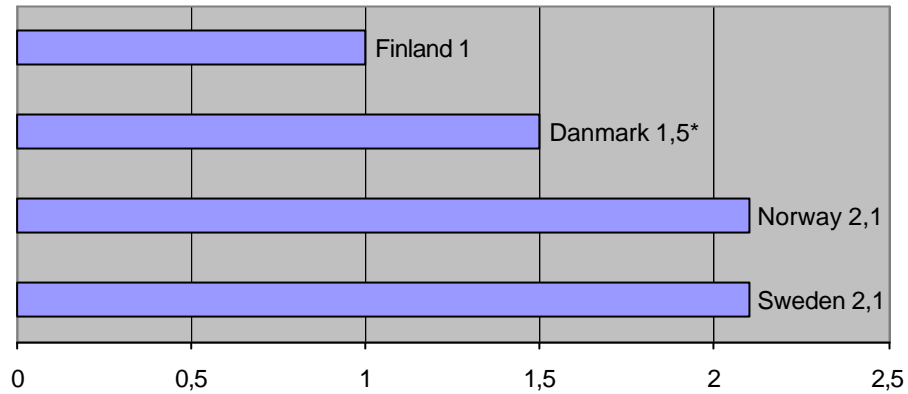
This user also suffered the most port-scans in this survey, about 40 valid events.

Portscans, all countries



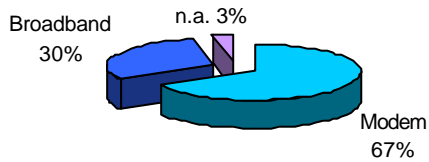
Port-scans and Broadband

Portscans per attacked user

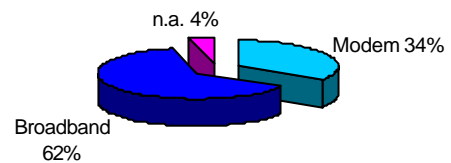


*One user suffered so many attacks, that the whole statistic would have been devaluated. He was taken out from the research-result.

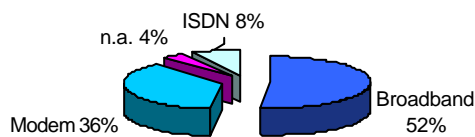
Connection Norway



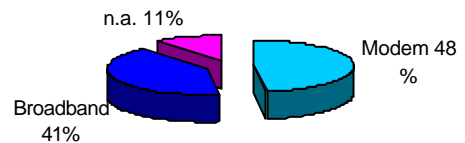
Connection Sweden



Connection Finland

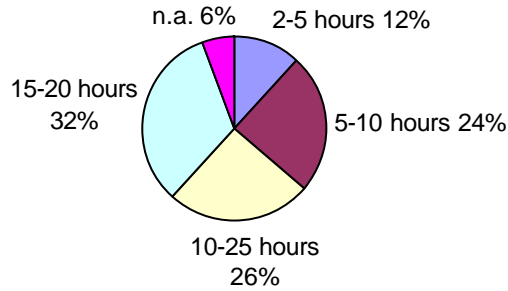


Connection Danmark

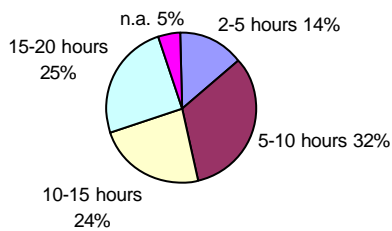


No direct-link can be established, comparing broadband and active port-scans. The threat-level for countries shows, that Sweden and Norway experiences most port-scans per attacked user.

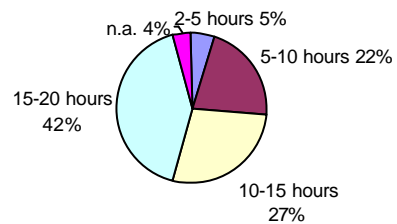
Surfing time per user / week, all participants



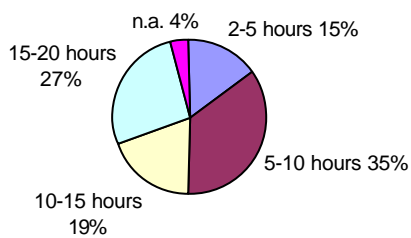
Surfing time Norway



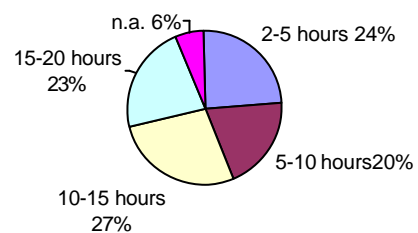
Surfing time Sweden



Surfing time Finland



Surfing time Danmark



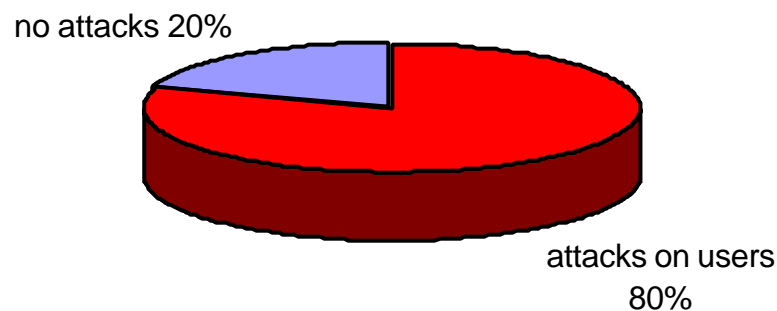
Swedish habitants spend more time online than the other countries in the Nordic. Together with the high number of broadband-users, they have the highest volume of transported data. This, and the likely often use of emails, number of changes of websites-addresses and general connection to the web make them most attacked.

Overall Threat

Surfing, e-mail or chatting can cause considerable damage to users by 80 percent. This is subdivided in different forms of attacks, from which direct-intrusions, worms and successfully placed Trojans will form the highest danger.

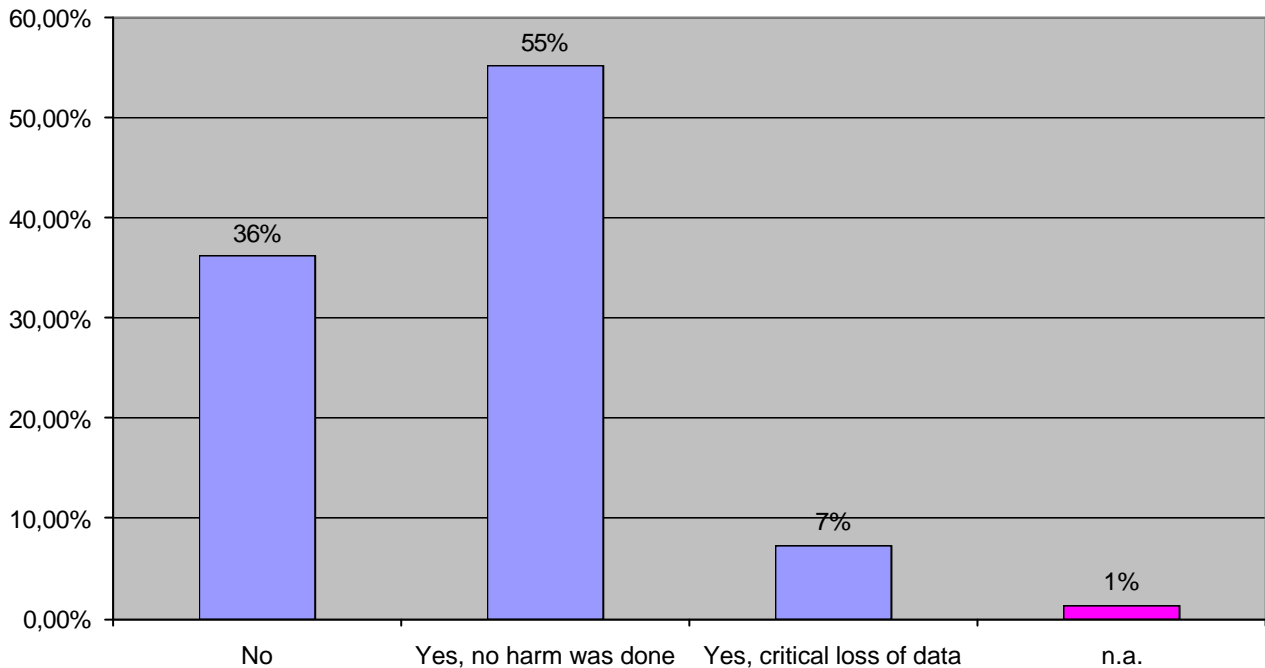
Without security-means, quite a number of participants would have suffered negative effects from attacks. Out of 301 participants, at least 240 were molested by serious threats. If it was possible to exactly track the kind of generally blocked communication for every single event, the numbers for serious threats would have been much higher. Especially with NIMDA, Red Code and massive infections of Windows networks, the actual number of threats could easily triple or quadruple.

Overall threat in the nordic



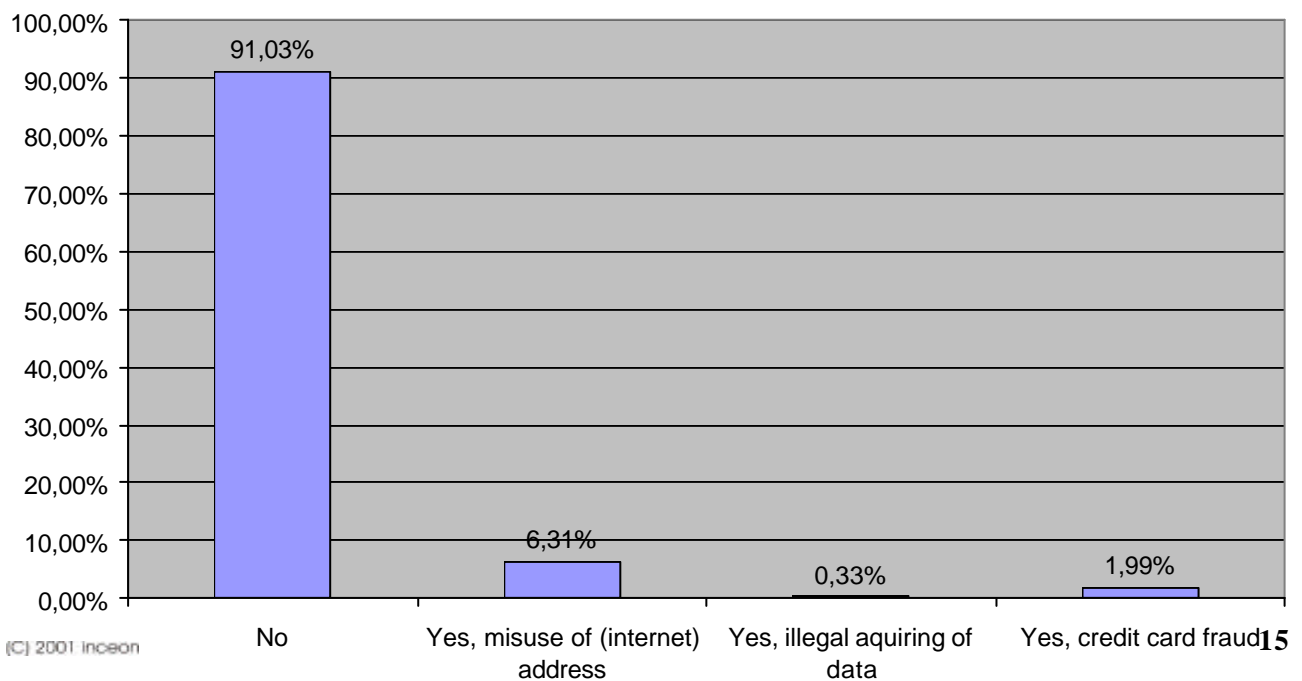
About all of the users faced doubtful communications of programs. Enough programs are available, which download advertising during a session and show it to the user. This is no case of classical danger for data. Nevertheless, the user suffers from delays in work and longer loading-time. These programs are normally being installed when users install certain shareware-programs.

Have you ever been attacked from the web?

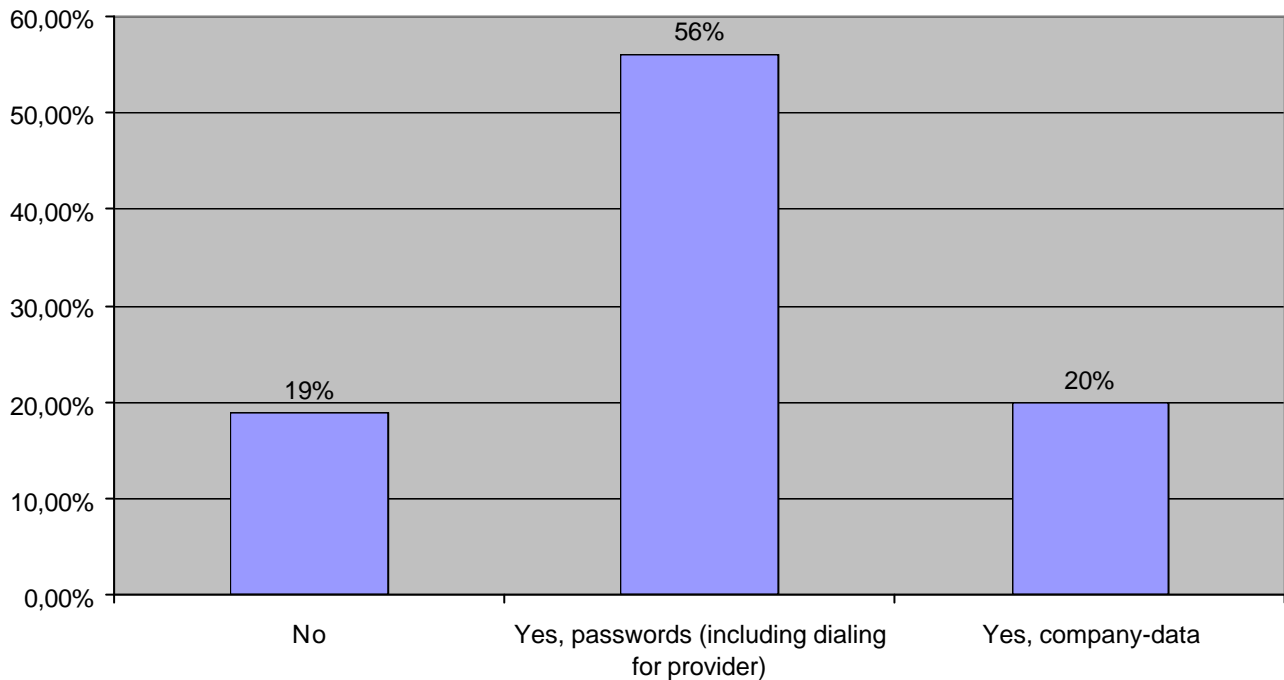


A relatively high number, 62 percent, of users already experienced attacks from the web. With 7 percent loss of system or critical data, the danger is also in historical view shown. The economical damage for cleaning a system is considerable, even if no lasting harm is done.

Did you experience any misuse of your data?*

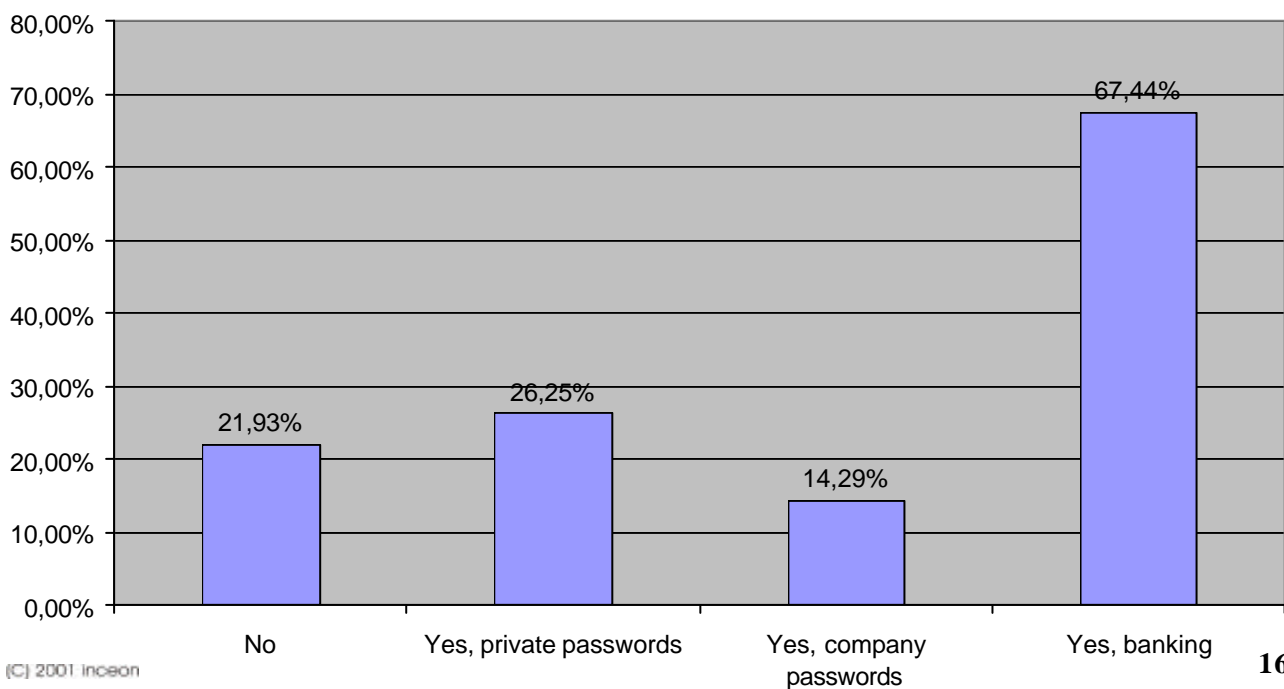


Do you store critical data on your computer?*



Threat scenarios as listed above can cause serious trouble, as a lot of users store important private or business-related data on their hard-drives.

Do you send critical data by internet?*



Development

Comparing to earlier research in other parts of Europe, the pure number of attacks per user seems decreasing. Nevertheless increases the danger by running multiple and more sophisticated attacks in short time.

In a research done four months ago in Germany, there were rather few different attempts especially with Trojan horses. Almost no other Trojans than NetBus, Sub-Seven, HackATack and BackOrifice occurred during the testperiod.

In the actual research, a great variety of Trojans and port-scans took place. Besides the Trojans mentioned above, additional attacks of DeepThroat, TransScout, ShockRave, QaZ, NetSphere, Spy and WinCrash happened in considerably high numbers. Not all of the attacks are listed in the Trojan-statistics, since some doubtful events could not be tracked down to a valid attack.

Port-scans today were partly done in a very consequent way. Almost every possible entrance was scanned, if the users went to very aggressive websites. All this happened fully automated. In addition some likely menial intrusion attempts occurred.

Since many users store sensitive data on their system or transmit sensitive data (banking, shopping, company-passwords..) a threat scenario must be taking serious. In addition to the threats that were recorded in the logfiles, about 10 percent of the users already suffered an attack or a virus-infection with hard to repair damage or loss of data or credit-card fraud.

Sweden most threatened, followed by Norway

Comparing the countries, both Norway and Sweden are most exposed to attacks. Denmark is safer and Finland experiences the least attacks.

This may be related to the number of people speaking the language. Finnish is, compared to the Scandinavian language family, more uncommon.

All countries together face the same threats, when they surf internationally. This also counts for security leaks in operating systems or applications.

The Nordic is no safe region for surfing. Only Finland has a bit fewer attacks to face.

Broadband + long surfing time most dangerous due to high traffic

Broadband itself is no more danger than other ways of getting into the web. But in combination with intensive surfing (especially Sweden), a constant connection and massive use of Internet services, the number of attacks is higher.

Results

Log-files show, that the web is generally polluted. Not depending on time or surfing habits, a danger of infection or intrusion is permanent.

Only for user's of languages with limited deployment, especially Finnish, dangers are a bit less threatening, if users stick to web-sites of their own language.

Advices

Without adequate means of security, home users face massive threats when they surf, chat or email. A good and always active virus-scanner is the absolute minimum for the protection of data. More recommendable is a firewall combined with a virus-scanner. A firewall system offers the biggest advantage by its ability to respond to unknown forms of attacks. Even if new worms or Trojans occur, the firewall will be able to block numerous attacks just by applying the defence rules. Protection has to be regarded as absolutely necessary, if the computer is not just used for gaming and the user will not mind loosing data or reconfiguring the system.

When sensitive data are stored on a computer or when they are being sent by web, firewall and virus-scanner will have to be up to date, set on high security level. This especially counts for home-office working. Every fifth user stores company data on his system. A security leak, especially when it is exploited by Trojans or new worm's, makes even the company vulnerable to home-hacking.

Comparing further statistic values, broadband users are the most likely victims of hacking. They spent the most time in the Internet and therefore take higher risks of being hacked. Like home-office users, they will have to choose high security levels.

Statistics of the survey

301 participants, testperiod: 1 month, September 2001.

Blocking and admitting of communications

Total occurrence Users affected

Denmark

Brugeren har oprettet en regel for at "blokere" kommunikation.	83	16
Brugeren har oprettet en regel for at "tillade" kommunikation.	1027	57
Denne ene gang har brugeren valgt at "blokere" kommunikation.	993	37
Denne ene gang har brugeren valgt at "tillade" kommunikation.	4212	60

Suomi

Käyttäjä on luonut säännön, jonka tarkoitus on "estää" yhteydet.	17	10
Käyttäjä on luonut säännön, jonka tarkoitus on "sallia" yhteydet.	399	22
Tällä kerralla käyttäjä on päättänyt "estää" yhteydet.	812	19
Tällä kerralla käyttäjä on päättänyt "sallia" yhteydet.	899	23

Norway

Brukeren har laget en regel for å "blokkere"-kommunikasjon.	25	14
Brukeren har laget en regel for å "tillate"-kommunikasjon.	1178	56
Denne ene gangen har brukeren valgt å "blokkere"-kommunikasjon.	1188	40
Denne ene gangen har brukeren valgt å "tillate"-kommunikasjon.	2418	53

Sweden

Användaren har skapat en regel för att "blockera" kommunikationer.	370	34
Användaren har skapat en regel för att "tillät" kommunikationer.	3919	127
Den här gången har användaren valt att "blockera" kommunikationer.	1860	88
Den här gången har användaren valt att "tillät" kommunikationer.	10092	113

The firewall-functions have restrictively controlled all data-traffic. All unknown events were recorded. The users were able to allow or deny programs or activity, in- or outbound from the firewall.

Within these parameters, normal functions of an e-mail client or a browser were allowed generally. This also counts for programs of entertaining purpose (e.g. web radio-services).

All suspicious activities were reported in the firewalls different types of log-files. With these high numbers of allowed communication it is likely, that some malicious programs got a permit granted by users.

For further statistics, an estimated number of 150 doubtful events will be used.

Depending on the level of personal judgement (Is a report of installed programs already a severe incident or is it to be regarded as harmless?..), the following values are rather conservative.

Trojans

◆ Sub-Seven	878
◆ NetBus	493
◆ TransScout	56
◆ Deep Throat	26
◆ Back Orifice	23
◆ Qaz	20
◆ Ultor	5
◆ Blade Runner	3
◆ Rat	3
◆ NetSphere	2
◆ Stealth Spy	2
◆ Master Paradise	2
◆ Portal of Doom	1
◆ Shock Rave	1
◆ WinCrash	1
◆ Bla	1

Total **1517**

Average per 159 users attacked by Trojans **9,5**

Average per 301users **5**

Port-scans

	Scans	Users affected
◆ Denmark	64	12
◆ Finland	5	5
◆ Norway	40	19
◆ Sweden	79	37

Total **184** **73**

Average per attacked 73 users **2,5**

Average per 301users **0,6**

Other attacks

- ◆ Direct intrusion 3
- ◆ Likely attacks, blocked by firewall approx. 150*

Total 153

Average per 301 users 0,5

*note: the estimation for non-specific attacks blocked by firewall is very conservative. With the amount of communication allowed or blocked plus several thousand blocked data packages, experience shows that a number of 1.000 or more is more likely but simply cant be proven.

Summary of attacks

- ◆ Trojans 1517
- ◆ Port-scans 184
- ◆ Other 153

Total 1854

Average attacks per 301 users 6,16

Users, actually affected 240

Attacks per user affected 7,72