

CERT Polska

Przemysław Jaroszewski, Mirosław Maj
CERT POLSKA

info@cert.pl
http://www.cert.pl/



TF-CSIRT Meeting, Copenhagen, 23 May 2002

CERT
POLSKA

Agenda

- A bit of history
- Who are we?
- What do we do and for whom?
- Who do we work with?
- How do we do it?
- CERT Polska Report 2001



A bit of history

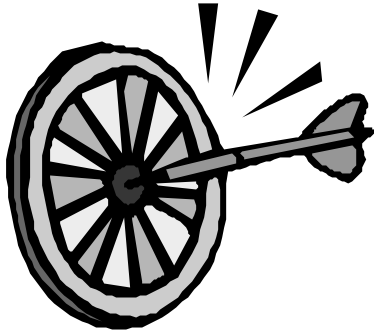
- CERT Polska founded in 1996 as CERT NASK
- NASK (Research and Academic Network in Poland) administers top-level domain .pl
- CERT was to handle security incidents for this domain
- Joined FIRST in 1997 as a full member
- Known as CERT Polska since 2001
- TERENA TI Level 2 since November 2001



Who are we?

- A „virtual” CERT until 2000
- Now a team within NASK structures separated from the internal security team
- Three people directly assigned to CERT backed with support of NASK engineers when needed





Our goals

- providing a single, trusted point of contact in Poland for the NASK customers community and other networks in Poland to deal with network security incidents and their prevention
- responding to security incidents in networks connected to NASK and networks connected to other Polish providers
- providing security information and warnings of possible attacks cooperation with other incident response teams all over the world

What do we do?

Handling internal incidents

- NASK is one of major Polish ISPs, connecting plenty of academic and governmental institutions
- CERT registers internal incidents reported by IDS systems, third-party or in any other way and coordinates their handling
- Close cooperation with NASK's security team and other teams
- Lack of shared ticketing system



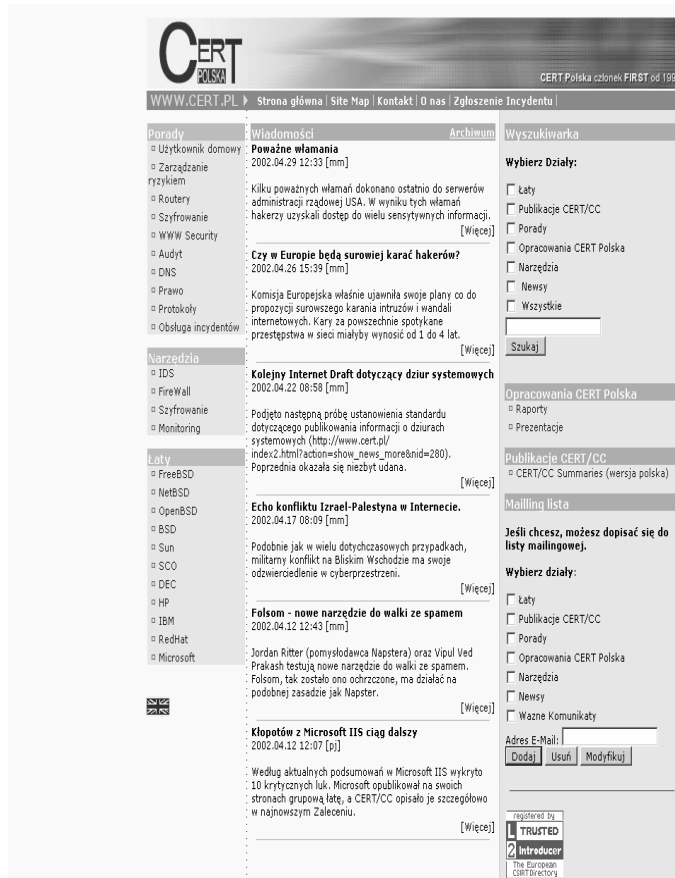
What do we do?

So far, CERT Polska is the only Polish CSIRT active on international arena.

- we act as a contact point to other providers and their security teams or CSIRTs
- we are widely recognized and respected in Poland by providers and other institutions as trusted point of exchange of information
- we register all incidents involving Polish networks reported to us
- however, most incidents are handled by other providers' own CSIRTs



What do we do?



The screenshot shows the CERT Polska website interface. The main content area displays a news article titled "Poważne włamanie" (Serious breach) dated 2002.04.29 12:33 [mm]. The article text reads: "Kilku poważnych włamań dokonano ostatnio do serwerów administracji rządowej USA. W wyniku tych włamań hakerzy uzyskali dostęp do wielu sensywnych informacji." Below the article, there are several other news items, including "Czy w Europie będą surowiej karać hakerów?", "Kolejny Internet Draft dotyczący dziur systemowych", "Echo konfliktu Izrael-Palestyna w Internecie.", "Folsom - nowe narzędzie do walki ze spamem", and "Kłopotów z Microsoft IIS ciąg dalszy". The website has a navigation menu on the left with categories like "Porady", "Narzędzia", and "Laty". On the right, there is a search bar and a "Wyszukiwarka" section with filters for "Wybierz Działy" and "Wybierz działy".

Education: <http://www.cert.pl/>

- popular source of information on IT security in Polish
- place to publish own advisories and links to other sources
- mailing list for alerts and periodical news updates
- guides for reporting the incident



What do we do?

Education: conferences and seminars: **SECURE**

- major annual two-day event organized by CERT Polska and NASK with great support from leading technology and methodology providers.
- guests from both Poland and abroad are invited to give speeches on various aspects of IT security (Tenn Nijsen, Damir Rajnovic, David Crochemore, Rob Thomas, Ian Cook to be mentioned)
- traditionally, two parallel blocks (for managers and technicians) are held
- great place to learn and establish contacts for many
- popularity of the event grows every year, attracting more than 100 people



What do we do?



Close cooperation with governmental institutions leads to plans for CERT Polska to play an important role in securing critical country infrastructure.

CERT Polska would act as an information exchange point and knowledge base.

- March 2002: Conference on Protection of National Critical Infrastructure - David Parker sharing his experience from UNIRAS

Who do we work with?

- Colleagues from NASK
- Law enforcement:
 - actively supporting each other on conferences and seminars, both organized by CERT Polska and the Police
 - knowledge base and expertises
- Inspector General for the Protection of Personal Data



Who do we work with?

Other Polish CSIRTs

- Polish Telecom (TP S.A. Abuse Team)
- AsterCity.net
- POL34-CERT
- and others...



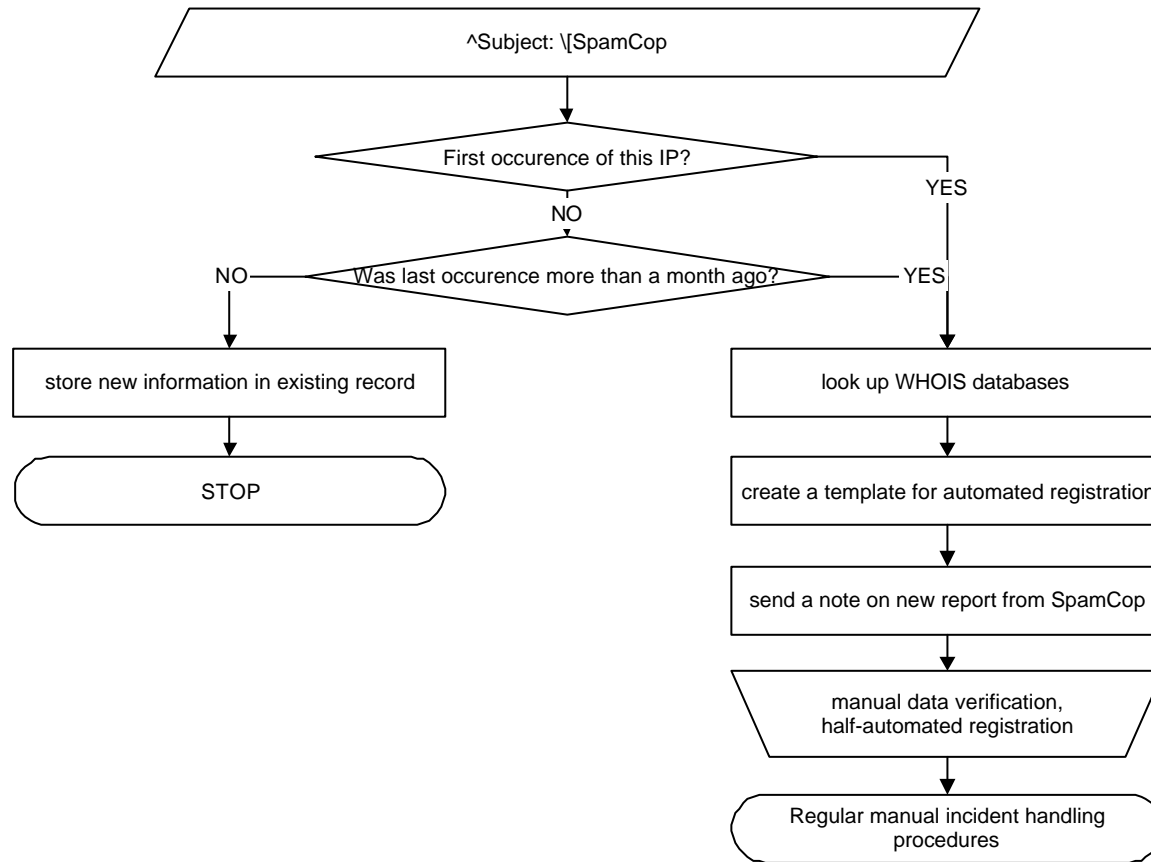
Quality of these contacts varies

How do we do it?

- Automated processing, as far as possible
 - CodeRed, Nimda
 - Klez
 - SpamCop notifications
 - spam
- Manual processing with Windows application
- Web interfaces for fast lookup in all databases



How do we do it?



How do we do it?

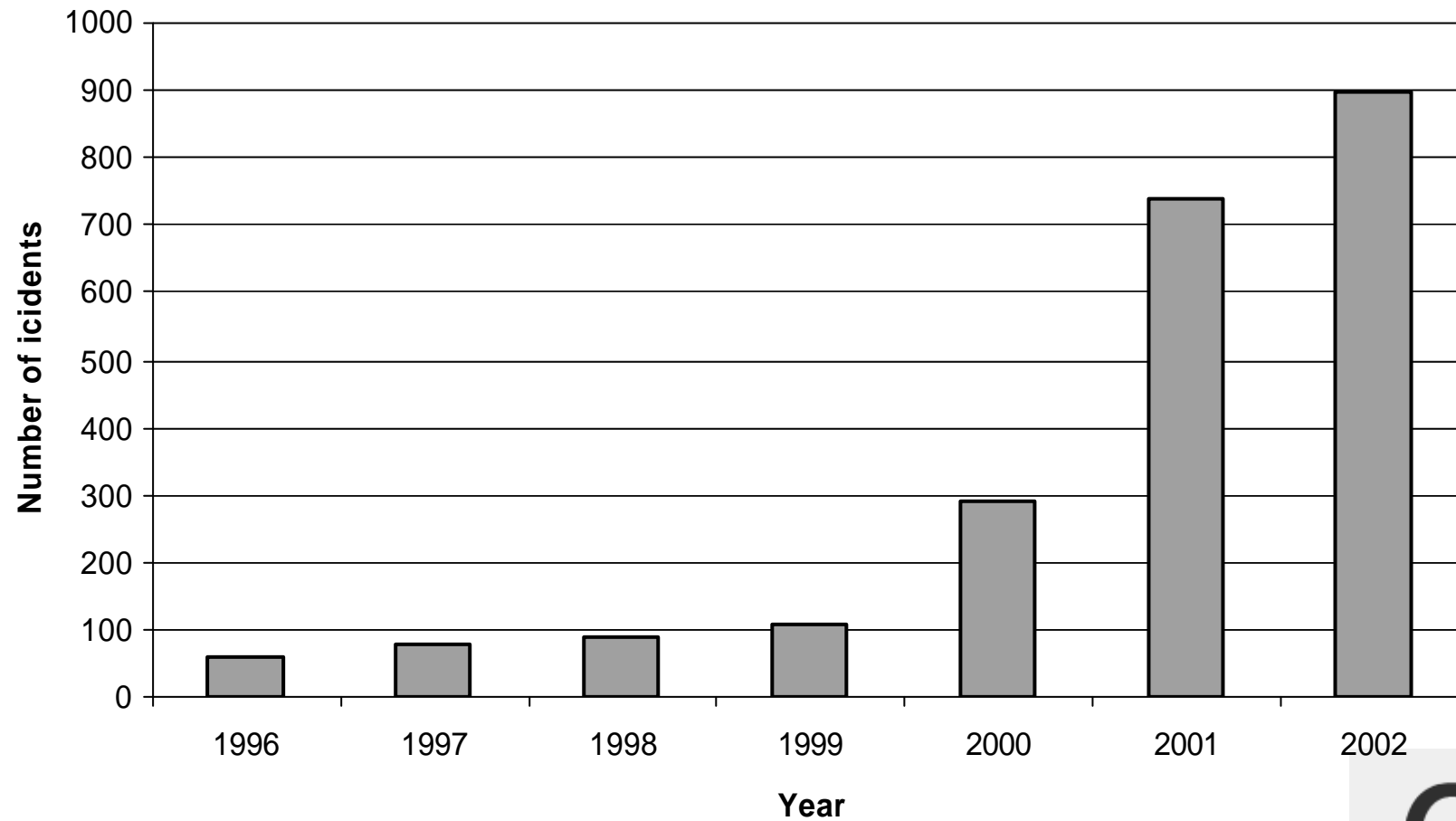
Manual processing: self-developed Windows application. Features:

- built-in contacts database management
- basic reports and statistics
- reminders
- SQL lookup front-end

Under permanent development

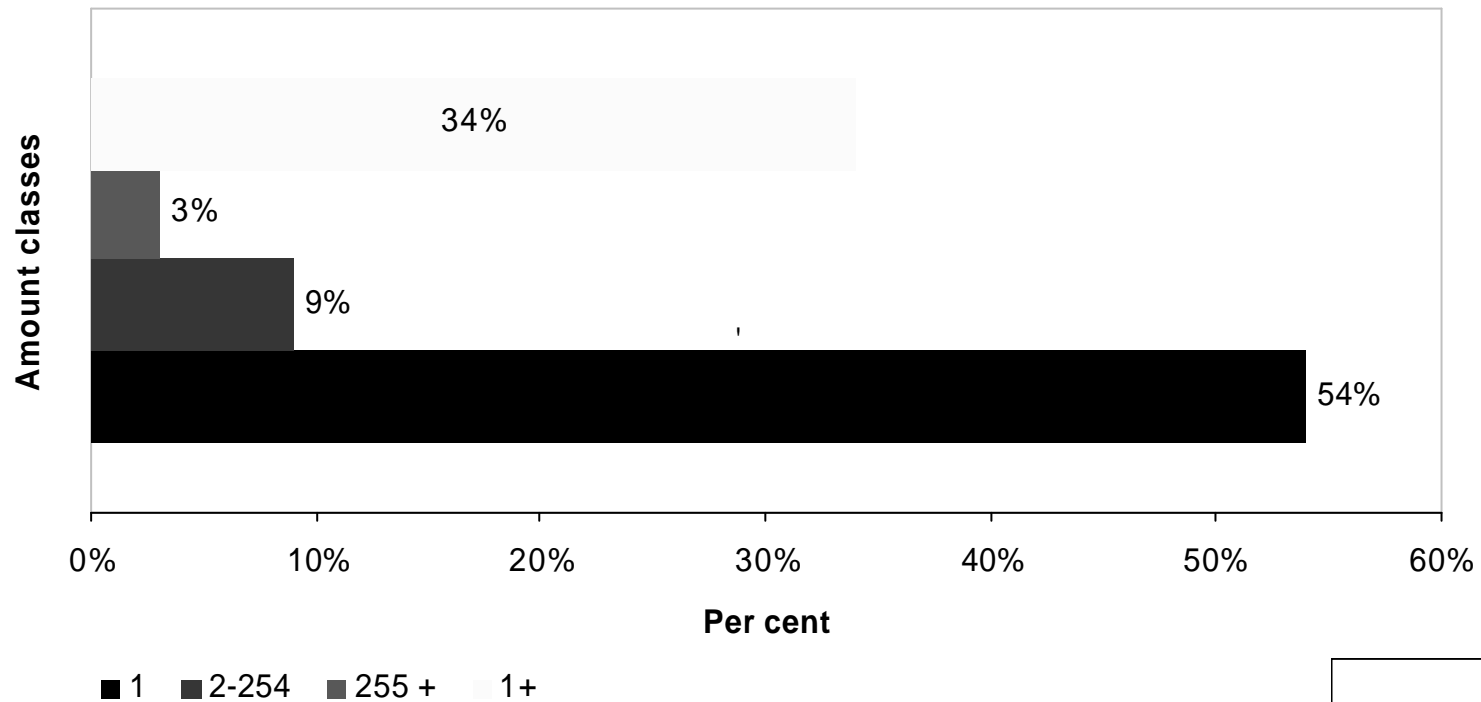


CERT Polska Statistics — 21/05/2002



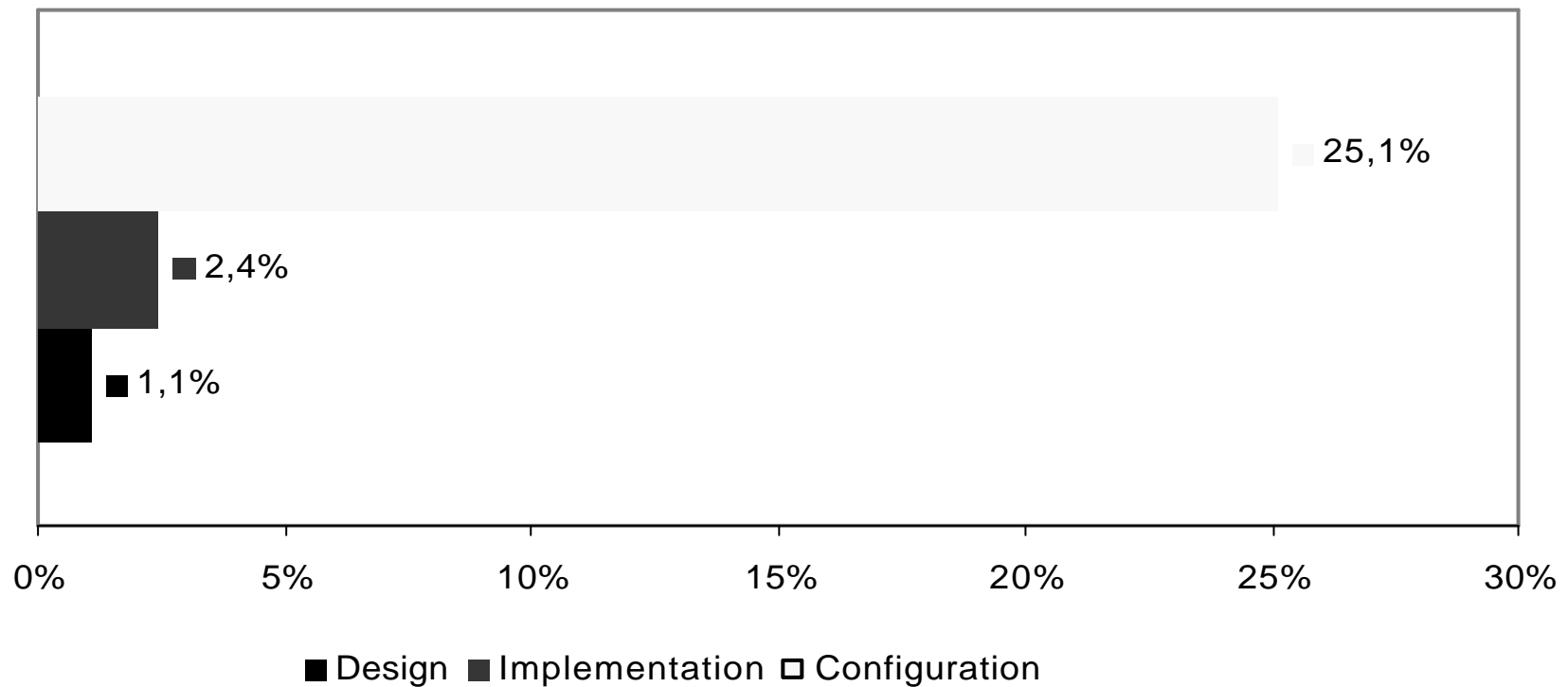
CERT Polska Report 2001

How many computers are attacked during a single incident?



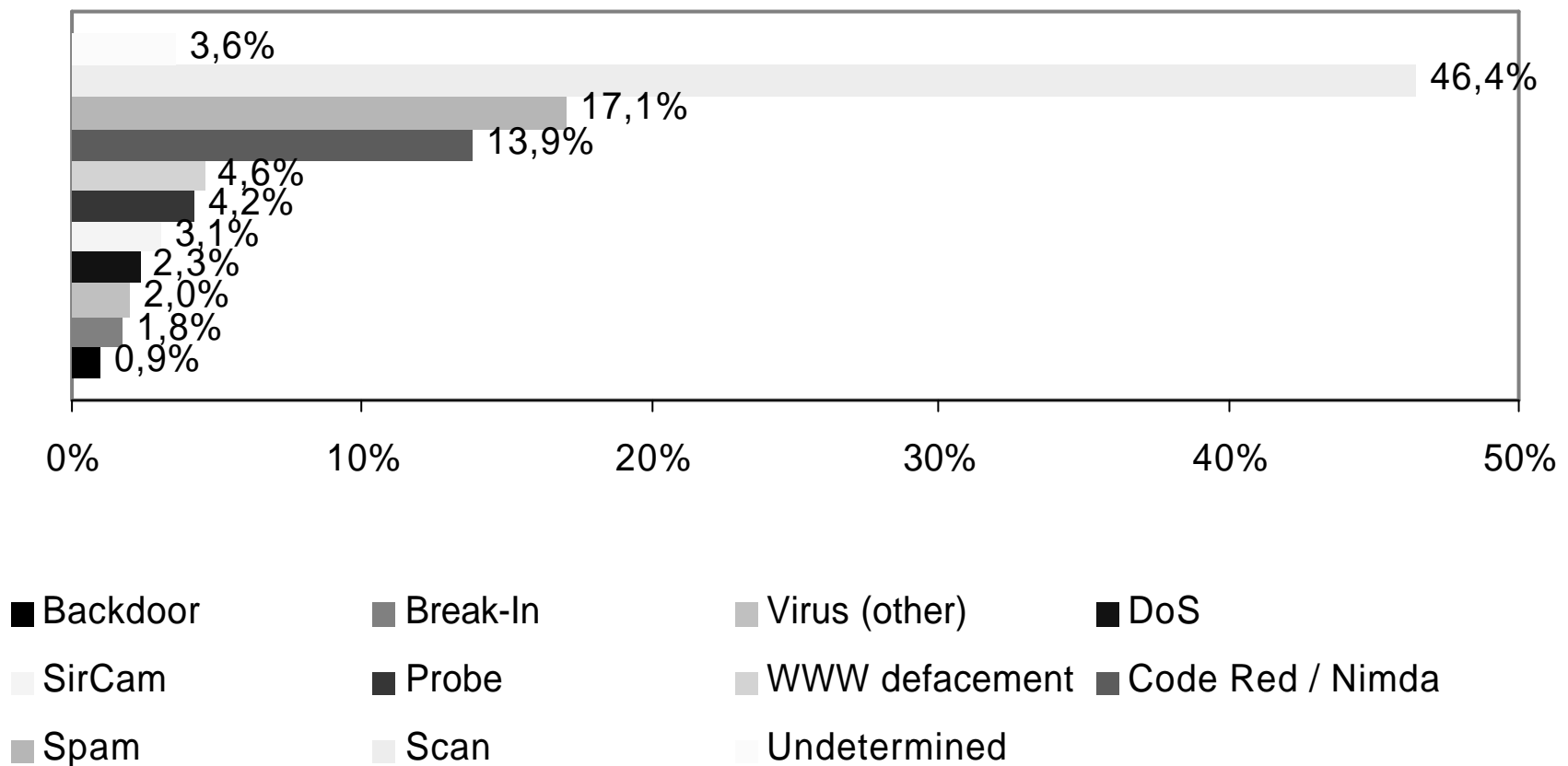
CERT Polska Report 2001

What is attacked?



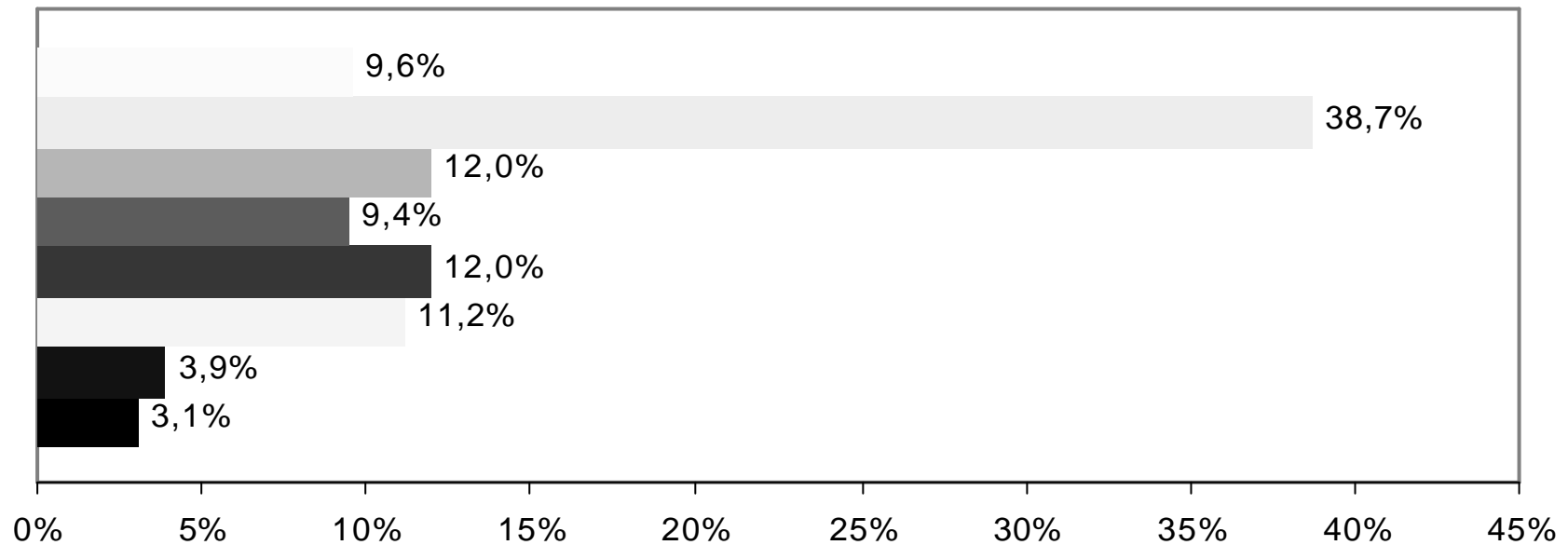
CERT Polska Report 2001

Most frequent attacks



CERT Polska Report 2001

Who reports to us?

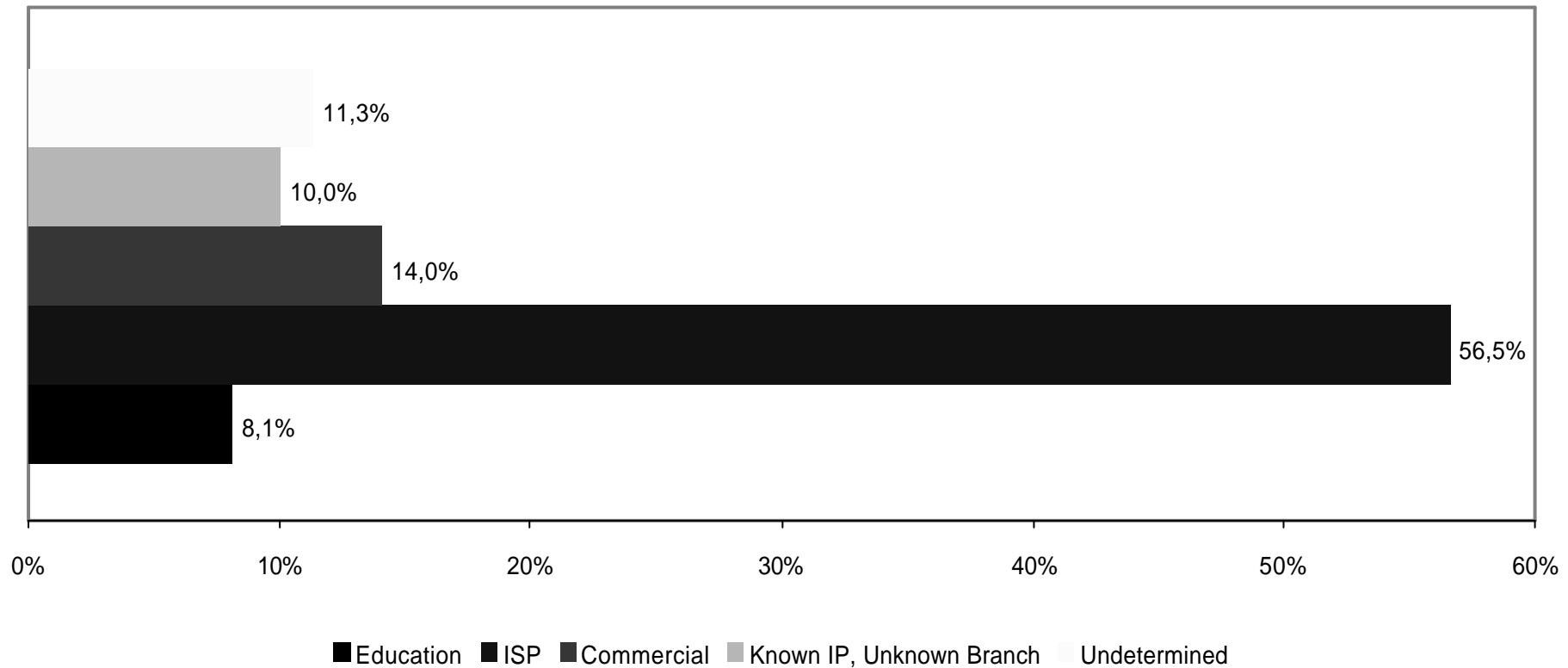


- Domestic Individual
- Foreign Individual
- Domestic CERT
- Foreign CERT
- Domestic Security Related Inst
- Foreign Security Related Inst
- Domestic Company, Inst
- Foreign Company, Inst



CERT Polska Report 2001

Who attacks?



Questions?

Comments?

info@cert.pl

phone: +48 22 523 1274

fax: +48 22 523 1399



Thank you!

