CARNet CERT
8th TF-CSIRT meeting
January 23rd 2003, Zagreb
CARNet – Croatian Academic and Research Network

• In 1991 - CARNet initiated as a Ministry of Science and Technology project
• In 1995 - CARNet institute established
• Funded by the Ministry of Science and Technology
CARNet backbone
CARNet network

- 169 faculties, research and other academic institutions connected to CARNet network
- Each institution’s system administrator serves as a security contact
- Dedicated security contacts at some larger institutions
CARNet CERT

- Established in 1996
- Currently three employers full time
- Constituency national based - .hr domain
CARNet CERT

- FIRST member since 1996
- TF – CSIRT participants
- TI – level 2 (accredited) team since September 2002
Cooperation with other teams

- CARNet CERT is currently the only CERT team in Croatia
- We act as a contact point to other providers and other security teams
- There are 10 ISP-s in Croatia
- Close cooperation with ISP’s abuse teams
Services we offer

- Announcements (vulnerability warnings and advisories)
- Vulnerability scanning on demand, (limited only to CARNet affiliates)
- Publishing security related documents
- Incident response
- Incident response support
- Incident response coordination
Handling incidents

• Incident handling according to priority
• Constant improvement of our “home made” incident tracking system
• Automate tasks as much as possible
main incident_handling() {
    new_mail_arrived();
    if (mail_about_incident) {
        if !(existing_incident || new_incident_reported_via_web) {
            open_new_incident();
            send_mail(inc_reporter, confirmation);
        }
        coordinate_incident();
        if (incident_solved) exit();
    } else if (ask_for_advice) answer();
    else general_respond();
}

function coordinate_incident() {
    if (first_mail_on_that_incident) {
        find_contact_of_source_network();
        send_mail(attack_source, report_incident);
    }
    else respond_or_contact_other_side();
}
Incidents handled by CARNet CERT

Number of incidents

Month

2000.
2002.

23.01.2003 8th TF-CSIRT meeting, Zagreb
Incident statistics

Types of incidents in 2002

- Other: 66
- Virus: 306
- Port scanning: 143
- Root account break-in: 19
- News spam: 5
- Unauthorized access: 44
- Mail spam: 61
- Mail relay: 12
- Denial of service: 44

23.01.2003 8th TF-CSIRT meeting, Zagreb
Incident statistics

Virus reports in 2002

- Opaserv: 33.6%
- Nimda/Code Red: 24%
- Yaha: 15.8%
- Klez: 7.9%
- Bugbear: 4.65%
- Hybris-B: 4.65%
- Other: 9.4%
Questions, comments?

- http://www.CERT.hr
- ccert@cert.hr