

Robert Vibert

robert@avien.org

AVIEN

AVI-EWS

Administrator

Anti-Virus Information Exchange Network

www.avien.org

Anti-Virus Information & Early Warning System

www.avi-ews.org

What's up

- ▢ Overview of AVI-EWS
- ▢ Co-operation
- ▢ Information sharing
- ▢ Future plans and projects

Copyright 2003 Robert S Vibert

AVIEN

AVI-EWS

Two largest independent anti-malware organizations

- operated as not for profit
- cooperative
- grassroots

Anti-Virus Information Exchange Network

Anti-Virus Information & Early Warning System

WWW.AVIEN.ORG

AVIEN

- ▢ Anti-Virus Information Exchange Network
- ▢ What's it all about?
 - ▢ Grassroots
 - ▢ AV specialists in large organizations
 - ▢ Sharing info daily
 - ▢ Member in size from 1500 to 1.5 million

Copyright 2003 Robert S Vibert

WWW.AVI-EWS.ORG

AVI-EWS

- ▢ Anti-Virus Information & Early Warning System
- ▢ What is the AVI-EWS?
 - ▢ Member-to-member
 - ▢ Early Warning Alerts
 - ▢ Advisories
 - ▢ Fast - often 3 hours in advance

Copyright 2003 Robert S Vibert

WWW.AVI-EWS.ORG

AVI-EWS

- ▢ Anti-Virus Information & Early Warning System
 - ▢ Follow-up information and trend tracking
 - ▢ In depth analysis
 - ▢ Growth trends from various sources
 - ▢ Discussions on viruses & protection

Copyright 2003 Robert S Vibert

Anti-Virus Information & Early Warning System

Two main discussion lists

Virus-discussion

- Talk about viruses, new and recurrent
- Analysis
- Hype-busting

AVI-EWS-talk

- How to protect
- News of interest

Anti-Virus Information & Early Warning System

Two alert advisory lists

Advisory

- Concise info on new malware
- Analysis is discussed in virus-discussion
- Approximately 5 per month

Alert

- Fast-breaking malware
- Concise
- Many people have it linked to their pagers

Anti-Virus Information & Early Warning System

Backup alert list

Alert 2

- Different list provider
- High Bandwidth & availability
- In case the primary alert list fails

Anti-Virus Information & Early Warning System

Other lists

AVI-EWS Vuln-Discuss

- Talk about security vulnerabilities which may be connected to malware

Product certification

- Discussions on how to test and evaluate anti-malware products

Anti-Virus Information & Early Warning System

Other lists

Free tools

- Discussion on free software tools which can be used to fight malware

Cooperate

- Discussions on how we can work together to make it a safer computer world

Anti-Virus Information & Early Warning System

Other lists

SMB Lure tool

- Discussion on the SMB lure software tool which is used to track worms
- The author of this tool participates

Certify

- Discussions on projects related to certification of anti-virus professionals

Cooperation

- AVI-EWS is the **only** place with
 - Major customer representatives
 - Major anti-virus software specialists
 - Independent researchers
 - Testers
 - Law Enforcement
- All working towards the same goal

Copyright 2003 Robert S Vibert

Cooperation

- AVI-EWS is the **only** place with
 - No flaming
 - No sales pitches
 - Reasonable signal to noise ratio
 - No trolls
 - No wannabes

Copyright 2003 Robert S Vibert

Information sharing

- Keeping track of growing threats
 - new threats require new counter-measures
 - new tools
 - new configurations
 - new policies

Copyright 2003 Robert S Vibert

Information sharing

- In AVI-EWS, everyone helps each other
 - anyone can ask questions
 - no such a thing as a dumb question
 - multiple responses typical

Copyright 2003 Robert S Vibert

Information sharing

- A partial listing of AV organizations involved in the AVI-EWS project
 - Aladdin, AV-Test.org, Ahnlab, Central Command
 - Clearswift, Command Software,
 - Computer Associates, EICAR, ESET
 - F-Secure, Fortinet, FRISK Software
 - GeCad, GFI, H+BEDV, ICSA Labs
 - Idefense, InDefense, Intego

Copyright 2003 Robert S Vibert

Information sharing

- A partial listing of AV organizations involved in the AVI-EWS project
 - MessageLabs, Network Associates, Norman
 - Panda, PestPatrol, Proland
 - SoftWin, Sophos, Sybari
 - Symantec, Tarari, Trend Micro
 - Virus112

Copyright 2003 Robert S Vibert

Future plans

- ▮ Increase membership in Asia
- ▮ Continue increase in coverage
- ▮ Respond to member wishes

Copyright 2003 Robert S Vibert

Questions?

- ▮ Robert Vibert
 - ▮ Administrator
 - ▮ Anti-Virus Information Exchange Network
 - ▮ www.avien.org
 - ▮ Anti-Virus Information & Early Warning System
 - ▮ www.avi-ews.org

Copyright 2003 Robert S Vibert