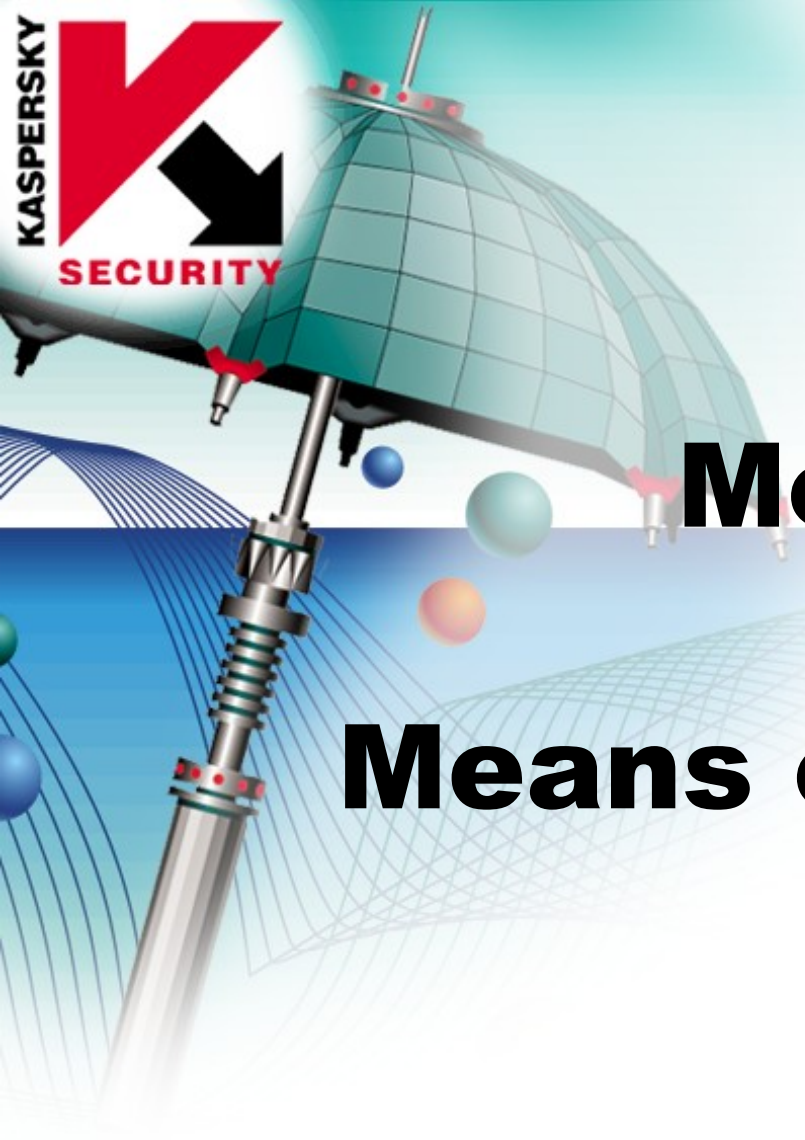


Modern IT-threats: Causes and Means of Neutralization

Eugene Kaspersky
Head of Anti-Virus Research
newvirus@kaspersky.com

KASPERSKY lab

Threat Classifications

- **Malware (worms, Trojans, viruses)**
  - Unauthorized data access
  - Hardware/software misuse
- **Spam (unwanted e-mail flooding)**
  - Risk of loosing valuable e-mails
  - Time (money) waste
  - Cheating and fraud
- **Global/Local Internet Attacks**
  - Network outage/visible slow-down
  - System crashes (client/server equipment)

Threat Classifications

- **Why malware?**
  - Teenage hooligans @computers
  - A way of self-affirmation
  - Anonymity
- **Why Spam?**
  - Spam is an easy legal business
  - Spam is anonymous
  - Spam is accepted
- **Global/Local Internet Attacks**
  - The best means of self-affirmation
  - The side-effect after “Flash Worms”
  - The worst thing to happen

Malware
[1/2]

1. **Behavior diversity**
   - Infector/destructor/stealer/spy-ware
   - Porno-dialers, clickers, downloaders
   - “Risk-ware” (FTP, IRC, proxy)

2. **Environmental diversity**
   - OS (Windows, Linux, Office, Palm)
   - Network apps (e-mail, SQL, games, pagers)
   - Non-network apps (HLP, archivers)

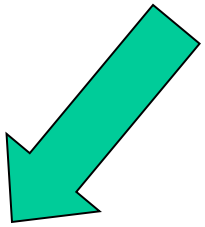
Malware
[2/2]

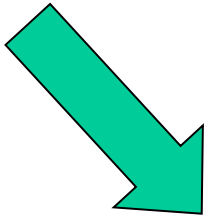
3. **Attack methods diversity**
   - Security breaches (buffer overflow)
   - Documented features (shared resources)
   - Human factor (social engineering)

4. **Spreading speed**
   - “Pure infectors” (removable media)
   - Network malware (e-mail, LAN, WAN)
   - “Flash worms”

Malware: Summary

- "Behavior x Environment x Infection x Speed" matrix: a huge number of combinations
- "Flash worms" worldwide infection in minutes





Anti-virus:

- Multi-purpose experts
- Attacks unpredictable
- Reaction: humans against machines

Malware:

- Guaranteed reception of malware within a given time frame
- Y200?: malware=50%

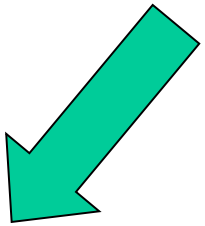
KASPERSKY lab

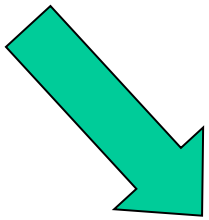
Spam

1. **Types diversity**
   - Advertising (products & services)
   - Fraud
   - Promotion
2. **Implementation diversity**
   - Text messages, web links, attachments
   - Graphic messages
   - Multiple languages
   - Countermeasures against anti-spam

Spam: Summary

- Diversity of types / implementation combinations
- Prompt reaction to new anti-spam technologies





Anti-spam:

- Multilingual support
- Immediate reaction
- Impossible forecast

Spam:

- Spam grows in number
- Spam grows in tricks
- Y200?: spam=50% email

Global Internet Attacks
[1/2]

1. **Implementation diversity**
   - Massive planned DDoS attack
   - Malware mass-mailing
   - Abnormal behavior of infected systems
2. **Consequence diversity**
   - Traffic slow-down / channels jam
   - Software/Hardware failure

Global Internet Attacks
[2/2]

3. **No way to protect against it**
   - Protected PCs will suffer from Internet failure
   - Protected regions will suffer from unprotected regions
   - 100% WW protection is touching a rainbow

4. **Side-effect diversity**
   - Home users – 100%
   - Governmental establishments – 0%
   - Others – in between

Behind the Threats

REASON

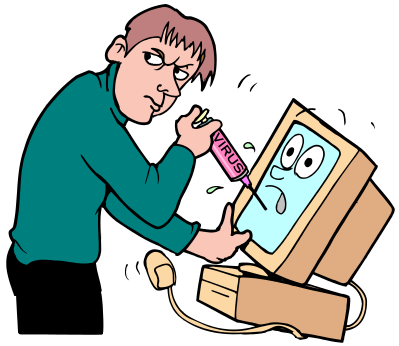
Human factor (virus-writers, hackers, users, spammers)

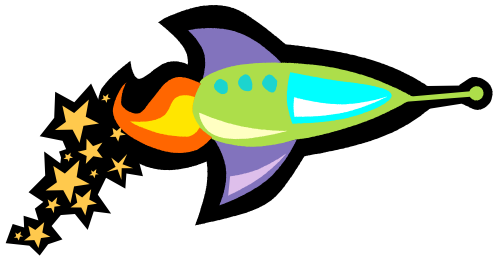
DELIVERY MEANS

Environment (networks, software, hardware)

CONSEQUENCES

Affected Victims (home users, enterprises)





slide 2

Protection

1. **Active defense**
   - Anti-virus, anti-hacker, anti-spam
   - More attention to corporate security
   - IT-security budgets increase
2. **Passive defense**
   - Transition to less popular SW (Linux, The Bat!)
   - Limited access (or disconnection) to the Internet

We will protect you against all threats until we are no longer able to.

Then we will start fixing their causes.

KASPERSKY lab

Fixing the Problem

1. **Fixing the environment (SW/HW vendors, IPSs)**
   - More security in products & services
   - Less redundant functionality – less vulnerability
   - More attention to Internet security needs
2. **Fixing the "human factor"**
   - Strong rules in public networks
   - Obligatory authorization
   - "Net-Police" / e-Interpol
   - Education and certification

F.A.Q.

Q.: Will it kill the anti-virus industry?

A.: No. There will be kamikazes and romantic, brainless hooligans regardless.

Q.: Should governments supervise the future network?

A.: Probably. However, more conceivable and less painful scenarios are also available.

Thank you
Спасибо
Danke schön
Dank ye vel
Merci
Gracias
Grazie
Shyeh shyeh
Arigato
Dhaniawad
Todah rabbah
Dankon
Shukran

Questions Please!

KASPERSKY lab