



# Technical & Educational Strategies for combating Spyware

BSI  
Federal Office for Information Security  
Germany

Thomas Veit

# Outline

---

- \* Definition Spyware
- \* Current situation & trends

=> Comprehensive approach:

## *Culture of Security*

Government / Organizations	Citizens
Vendors	Providers

# 1st: What do we call Spyware ?

---

(very) general suggestion for a definition:

Spyware is:

**Any program that does send local information to some remote system without the users consent**

*Bots / Trojans / Viruses*

might be included by this definition in principle

*"Adware"*

would not be included in this definition, since the user is presumed to give consent before or while installing respective software

*System Management*

*Software*

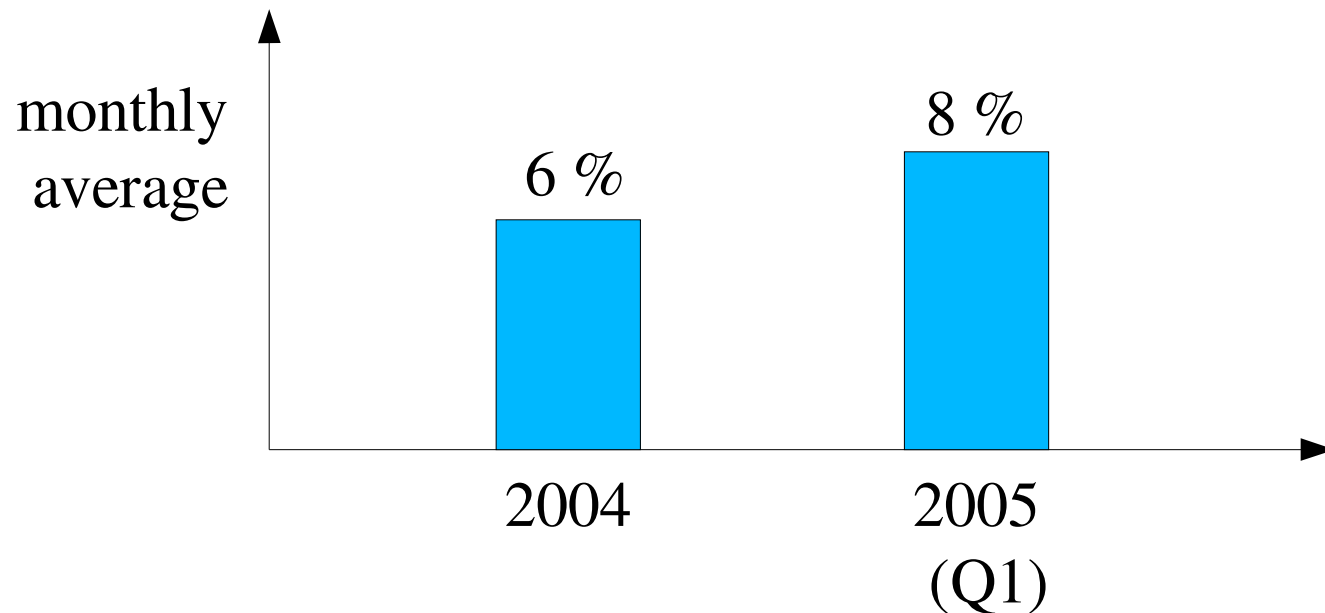
would not be included as well, since a general consent by the user is presumed as given

# Current Situation / Trends ...

recent BSI Status report:

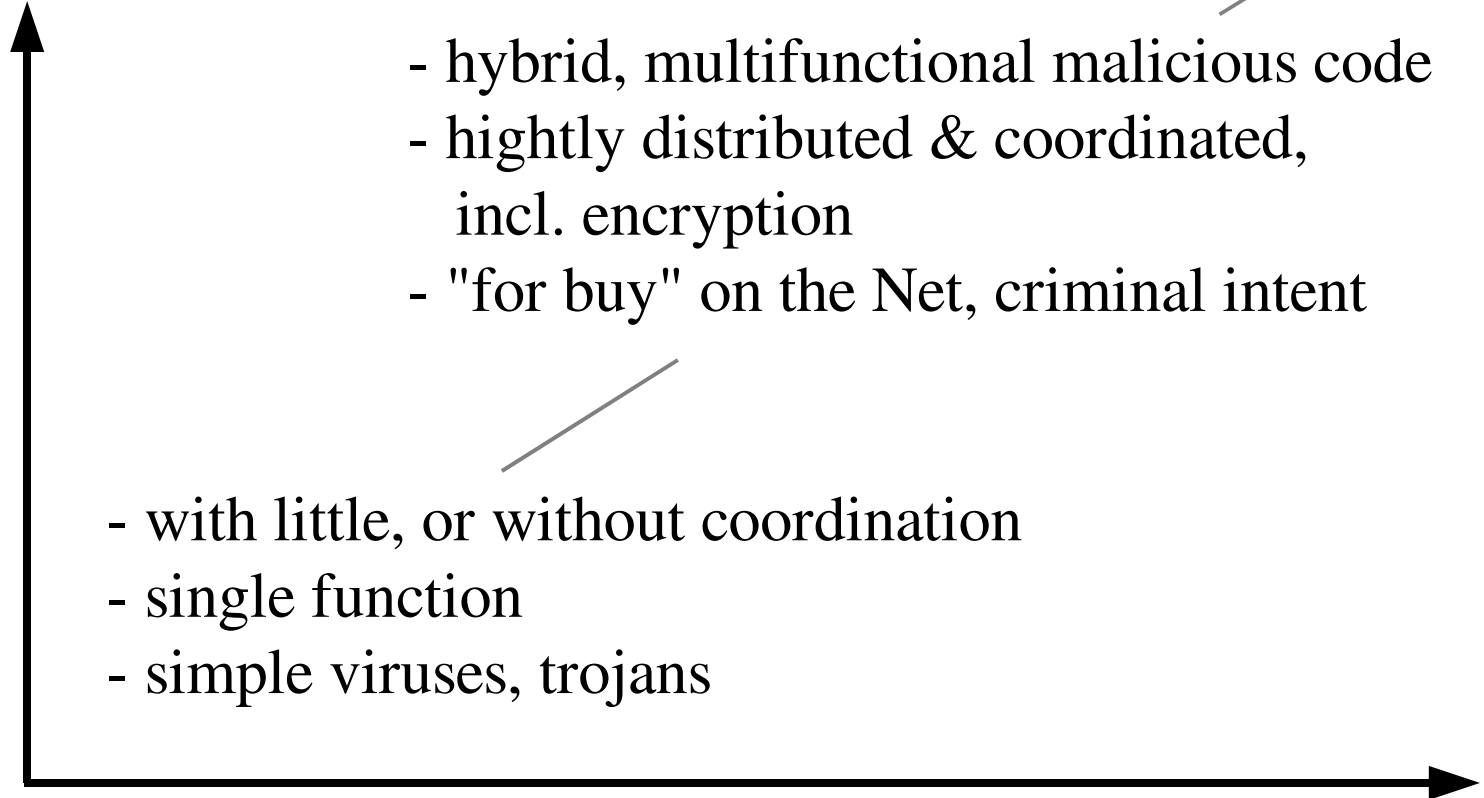
Information Security in Germany / 2004

Percentage of infected Emails, discovered at central gateways  
of Federal Government Network (IVBB)



## ... Evolution of Malicious software

sophistication



~ 1990

2005

# Multiple Infection Vectors

---

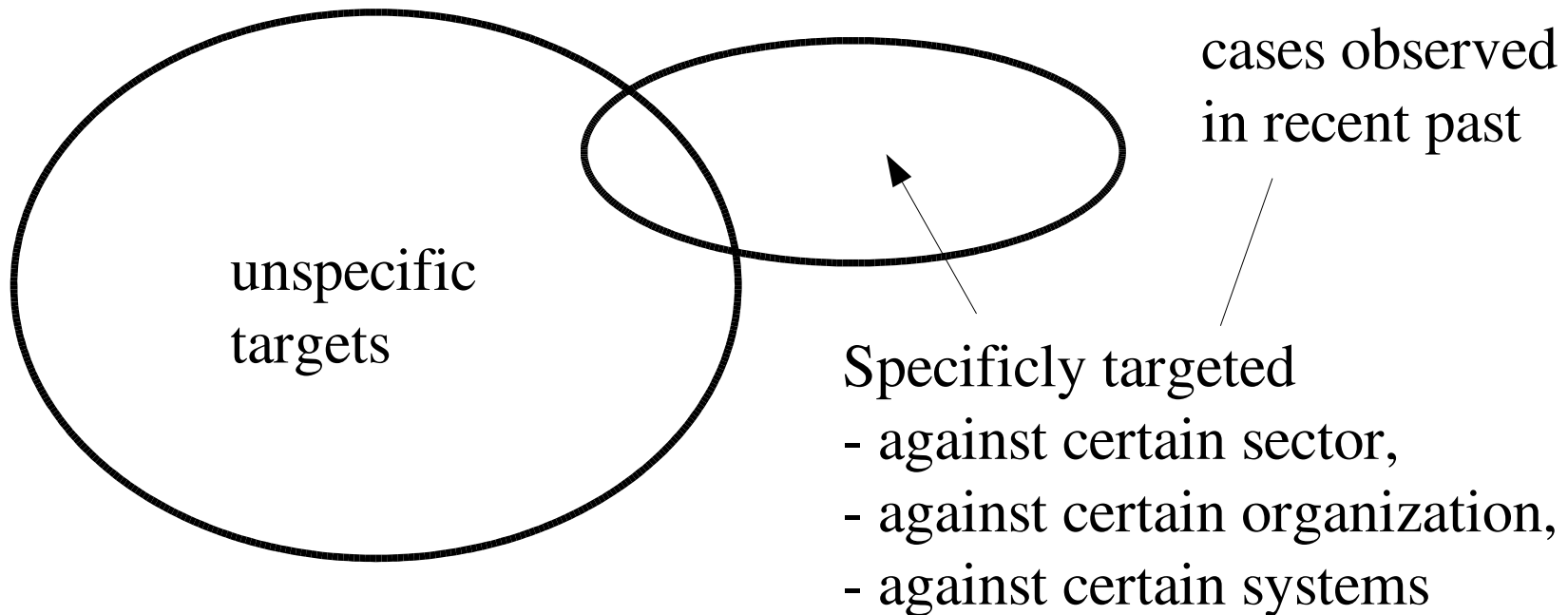
Variety of vectors for compromise of systems

- \* Automated execution of malicious WebScripts
- \* Execution of malicious Email-Attachments
- \* Direct intrusion via open port / vulnerability
- \* download malicious software & execution,

& combinations

# Evolution of targets

- specific & unspecific selection of systems to compromise



# Status / Threat - Summary

---

convergence of  
malicious features

variety of vectors  
to compromise  
systems

seemingly  
significant  
amount of  
criminal intent  
& money  
involved

lots of  
"easy  
targets"

significant **quantity**  
of compromised  
systems

significant **quality**  
of distributed  
malicious architecture

**=> Comprehensive approach necessary ...**

... single/isolated technical measures are not enough

## ... by all responsible actors

---

Government / Organizations	Citizens
Vendors	Providers

# Vendors / Suppliers

---

Security of products, suggested actions:

*(preventive)*

- built-in security by design
  - \* not just single features, but structural
  - \* caveat: complexity
- pre-configure products with appropriate balance between security and functionality (examples)

*(reactive)*

- implement vulnerability management procedures
- recognize cooperation with CERTs

# Government / Organizations

---

- Implement Comprehensive Security Framework
  - \* policy / guidelines / architecture / international cooperation
  - \* education of users on how to work securely on the Net
    - e.g. awareness campaign
  - \* include security requirements for the procurement of software
  - \* apply technical measures
    - central security management of clients
    - in principle, multiple security checks
      - \* e.g. central + client AntiVirus / Firewall
  - \* implement vulnerability management procedures

# Citizens

---

- get informed about security issues  
(e.g. <[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)> in Germany)
- \* behave accordingly (Email, Scripting, Download)
- \* use technical measures
  - AntiVirus, Personal Firewall

# Providers

---

- provide a  
    "secure Internet access package"  
for those customers who want it
  - \* including "basic port filtering"
  - \* provide recommendation for up2date  
    AntiVirus & Personal Firewall

# Summary

---

**If all players act together:**

=> a significant reduction of  
spyware &  
malicious program dissemination  
would be possible

BSI / Germany

T. Veit

+49 228 9582 - 236