A Guideline to Anti-Malware-Software testing

Andreas Marx

Content

- Introduction

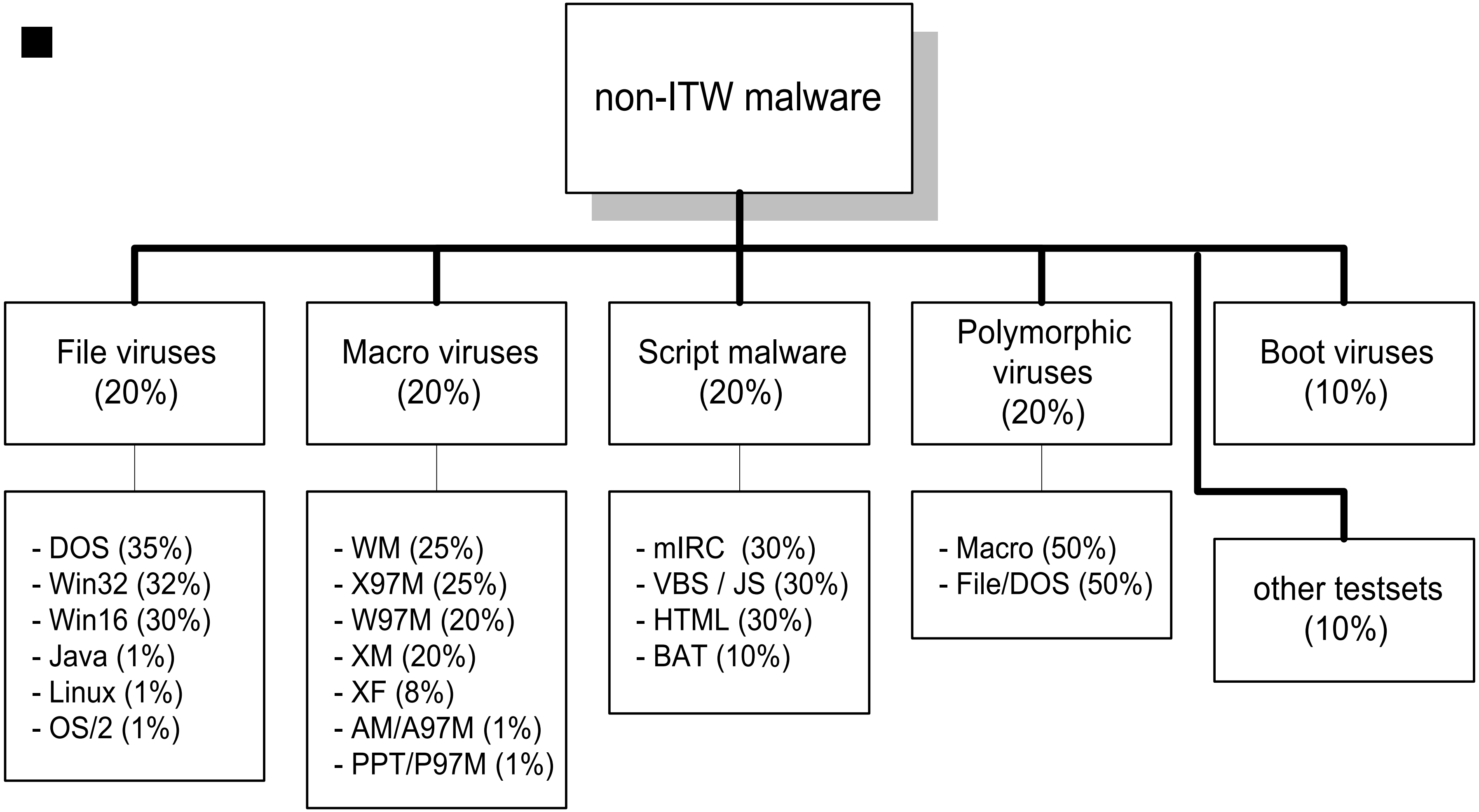
- Three main parts

  – Part 1: Prerequisites and Preparations
  – Part 2: Evaluation and Testing
  – Part 3: Editing and Documentation

Prerequisites and Preparations I

- Prerequisites
  - – Methodical foundations about testing, about viruses and anti-virus software
  - – Tester has to be independent from anti-virus companies, no sponsoring
- Preparations
  - – Creation of a project plan (time...)
  - – Test criteria and weights (schemes)

Prerequisites and Preparations I



non-ITW malware

File viruses (20%)

- DOS (35%)
- Win32 (32%)
- Win16 (30%)
- Java (1%)
- Linux (1%)
- OS/2 (1%)

Macro viruses (20%)

- WM (25%)
- X97M (25%)
- W97M (20%)
- XM (20%)
- XF (8%)
- AM/A97M (1%)
- PPT/P97M (1%)

Script malware (20%)

- mIRC (30%)
- VBS / JS (30%)
- HTML (30%)
- BAT (10%)

Polymorphic viruses (20%)

- Macro (50%)
- File/DOS (50%)

Boot viruses (10%)

other testsets (10%)

Prerequisites and Preparations I

- Prerequisites
  - – Methodical foundations about testing, about viruses and anti-virus software
  - – Tester has to be independent from anti-virus companies, no sponsoring

- Preparations
  - – Creation of a project plan (time...)
  - – Test criteria and weights (schemes)
  - – Acquisition of resources (humans, computers)

Prerequisites and Preparations II

- Information required by AV companies
  - Objective of the test
  - Deadlines for products and updates
  - What is going to be tested?
  - Which OS and what environments
  - What has to be delivered for the test?
- Getting the products from the companies
  - Which options/settings are recommended to test the software?
  - Package list
  - Contact persons

Prerequisites and Preparations III

- Creation of the test files
  - How to get the viruses? Virus simulators, generators, AV companies, Downloads...

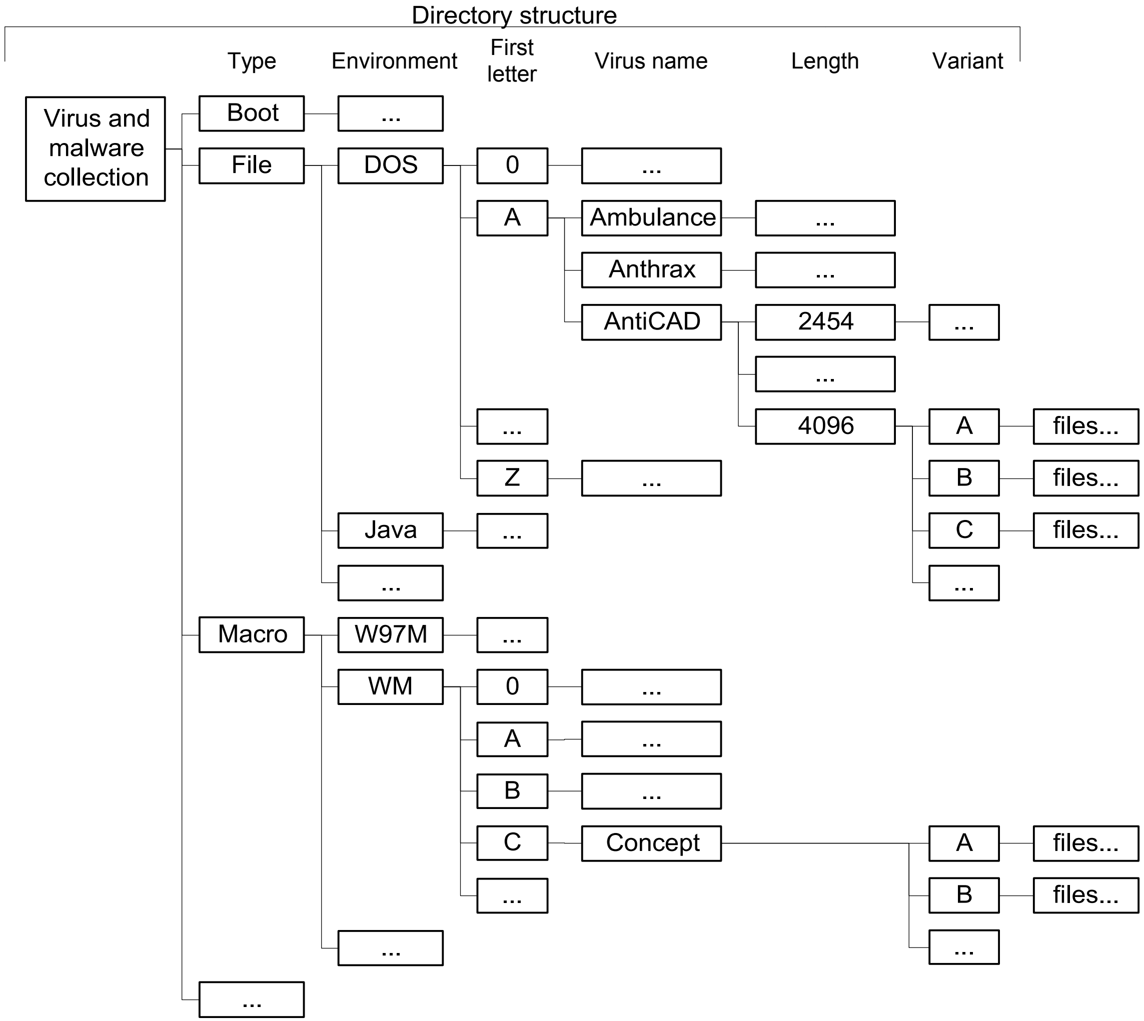
Prerequisites and Preparations III

- Creation of the test files
  - How to get the viruses? Virus simulators, generators, AV companies, Downloads... ☹

Prerequisites and Preparations III

- Creation of the test files
  - How to get the viruses? Virus simulators, generators, AV companies, Downloads... ☹
  - Virus Collections sorted after type and characteristics (e.g. File-, Macro viruses)

Prerequisites and Preparations III



Directory structure

Type | Environment | First letter | Virus name | Length | Variant

- Virus and malware collection
  - Boot
    - ...
  - File
    - DOS
      - 0
        - ...
      - A
        - Ambulance
          - ...
        - Anthrax
          - ...
        - AntiCAD
          - 2454
            - ...
          - ...
          - 4096
            - A
              - files...
            - B
              - files...
            - C
              - files...
            - ...
      - ...
      - Z
        - ...
    - Java
      - ...
    - ...
  - Macro
    - W97M
      - ...
    - WM
      - 0
        - ...
      - A
        - ...
      - B
        - ...
      - C
        - Concept
          - A
            - files...
          - B
            - files...
          - ...
      - ...
    - ...
  - ...

Prerequisites and Preparations III

- Creation of the test files
  - How to get the viruses? Virus simulators, generators, AV companies, Downloads...
  - Virus Collections sorted after type and characteristics (e.g. File-, Macro viruses)
  - Replicating samples: Test their ability to spread, prevent cheating
  - Preparing test files for compressed and archived files

Evaluation and Testing I

- Software and service quality features
  - Completeness
  - User-friendliness, program’s feedback
  - Security, robustness
  - Efficiency, compatibility
  - Adaptability, configuration
  - Documentation
  - Support, updates, costs
- Test strategies
  - Volume (mass) test and under heavy load

Evaluation and Testing II

- Virus-related tests
  - On-Demand (virus scanner)
  - On-Access (virus guard)
  - Disinfection of some viruses
  - Memory detection
  - Compressed and archived Files
  - Emergency-plan und -discs of the vendor

- Attention: Bugs in the OS (features?)

Editing and Documentation

- Representation of the results
  - Summarize of all results into managable tables
  - Getting the final results using the schemes which have been made before the tests starts
  - Writing the review by the tester
  - Publication

- After publication
  - Keep contacts, Discussions about test strategies

Summary

- Testing is a complex process, which is not objective in all parts (e.g. user-friendliness)
- Only a short part of the program’s life cycle can be tested
- Many things can be tested, but only the “Real Life” is important, which can only be simulated partly and incomplete
- Test as a help to come to a decision

Summary

- Any Questions?