Automated detection of antivirus coverage

Kris-Mikael Krister
krismika-at-stud.ntnu.no

NTNU
Innovation and Creativity

Agenda

What?

Terminology

- What is a “virus”?
- We will use the term “malware”.

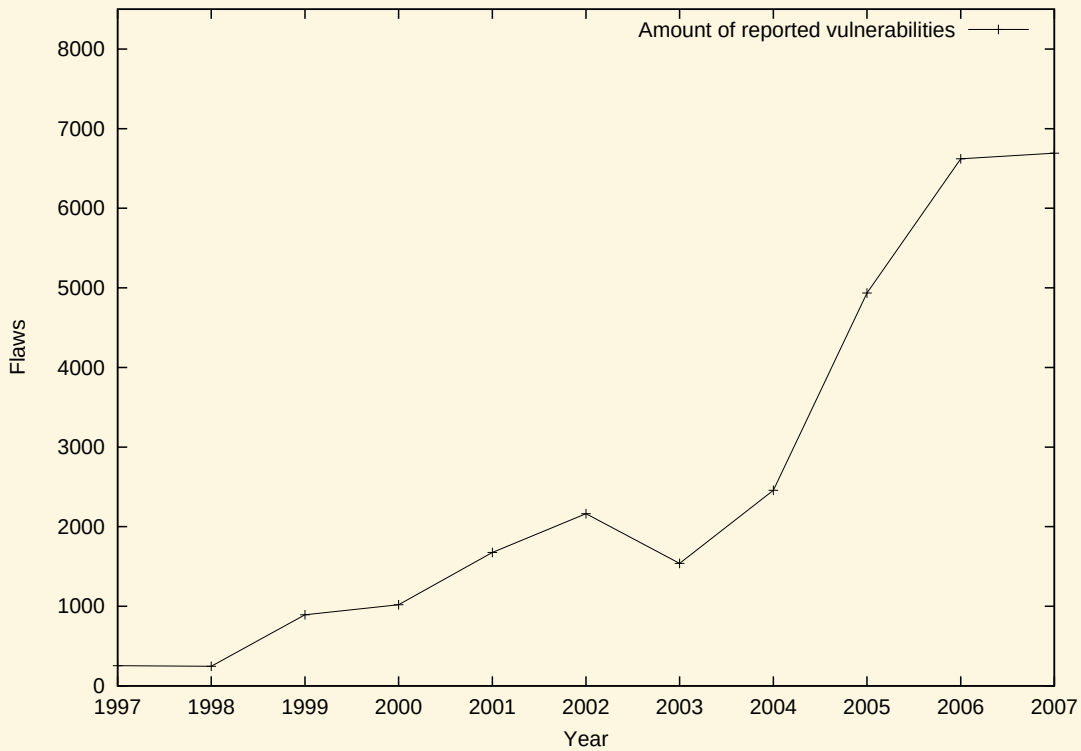
Content of this project

- An arbitrary amount of antivirus applications running the same types of operations with centralized control - possible?
- . . . if so, implement such a system

The amount of malware increases

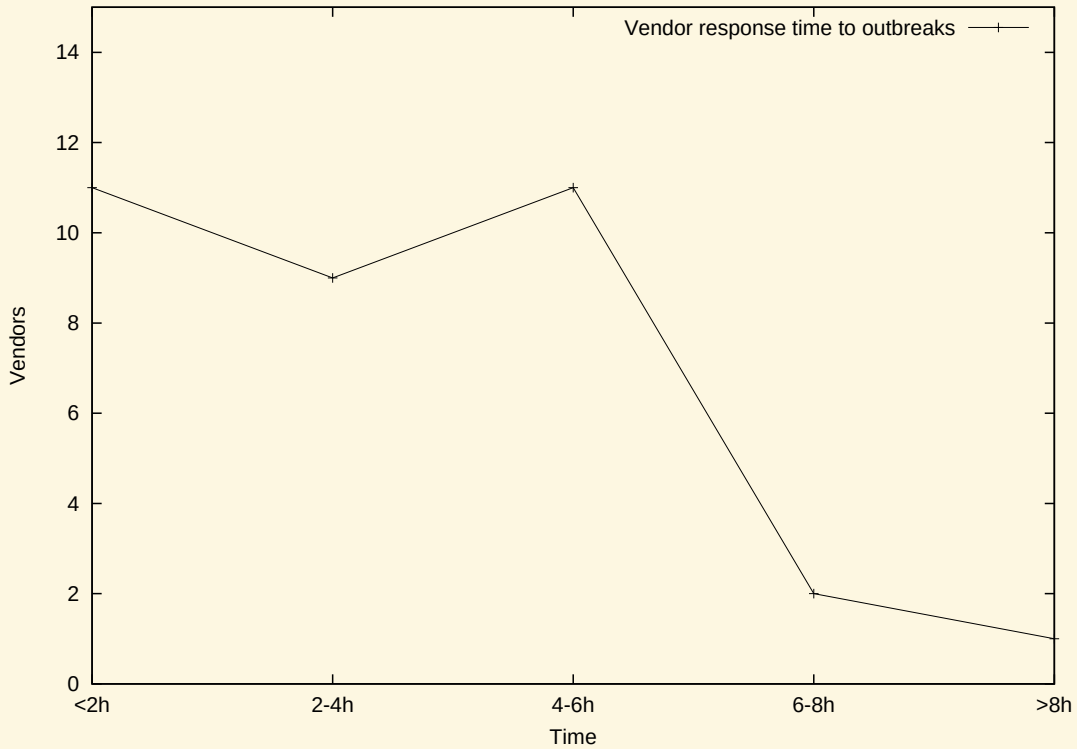
- The Internet grows → More targets
- There are existing solutions, but none of them are optimal
- A malware market has been established
  → Economic values
  → Sophisticated-hard-to-detect malware
- Complexity of software rise → More bugs/flaws

The amount of malware increases



Source: `http://nvd.nist.gov`

Detection rates



Source: `http://www.av-test.org`

Naming of malware

Product	Virus signature name
AhnLab-V3	Win-Trojan/Agent.20480.KQ
AntiVir	TR/Agent.46592.C
BitDefender	Backdoor.Generic.58074
Ikarus	Backdoor.Pigeon.6620
K7AntiVirus	Trojan.Win32.Agent.Family
NOD32v2	Win32/Agent.OBH
Sophos	Generic Patcher
Symantec	Trojan Horse
TrendMicro	PAK_Generic.001
Webwasher-Gateway16	Trojan.Agent.46592.C

Possible solutions

- Multiple antivirus applications on the same computer
- `metascan`
- `virustotal.com`

Requirements and fulfillment

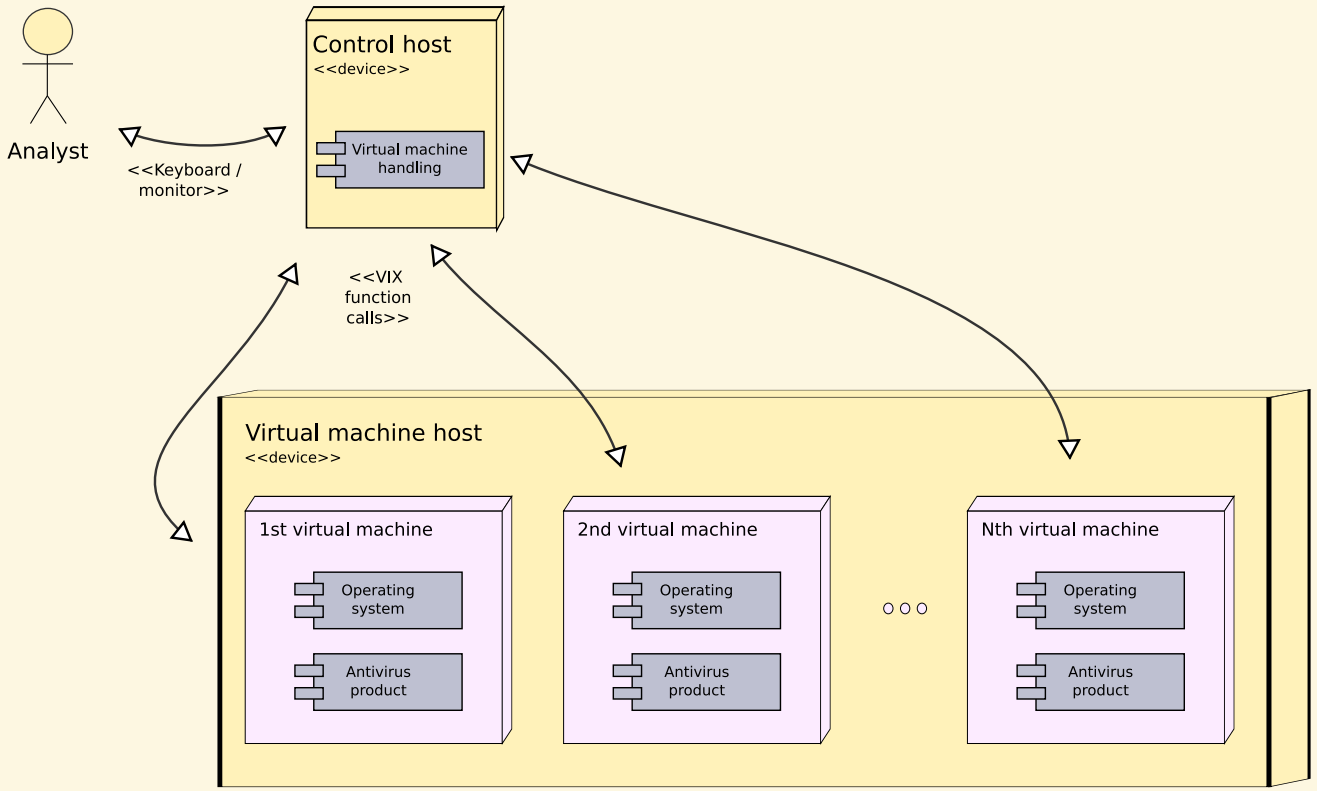
Requirements

- Centralized control
- Automated scanning with result aggregation
- Support for scanning and virus definition updates
- Reversing any infections to the system(s) scanning the files

How to fulfill the reqs

- Virtualization - `VMware server`
- The automation API - `VIX`

Implementation



Demo

Problems

- Memory
- False negatives/positives
- Command line requirement

The future

- Exponential growth of polymorphic malware samples make signature based antivirus scans a dead end (?)
- Heuristic scanning broken by design
- Dynamic analysis on the fly?

Questions?

?