

Virus Analysis

Techniques, Tools, and Research Issues

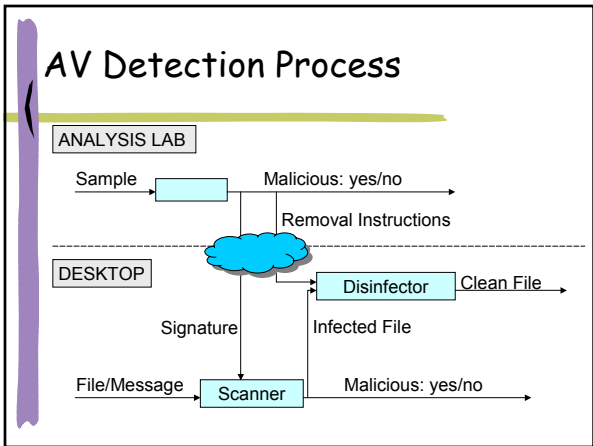
Part V: Research Issues

Michael Venable
Arun Lakhotia

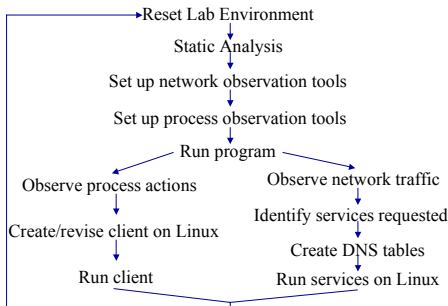
University of Louisiana at Lafayette, USA

Research Issues in Virus Analysis

- Revisit: Processes
- Classification of Problem Space
- Current State of Technologies
- Survey of Research
- Distributed Virus Analysis



Malware Analysis Process



Research Issues: AV Lab

- * Sample Collection and Filtering
- * Analysis
- * Fingerprint Extraction
- * Payload Identification
- * Signature Distribution
- * Evaluation of AV Scanners


Research Issues: Desktop

- * Prevention
- * Detection
 - Heuristic
- * Disinfection
- * Recovery

Current State of AV Technology

Copyright © 2004, Carey Nachenberg, Symantec
Presented: Worm 2004


- ✦ **Process**
 - Capture, Analyze, Create signature, Test, Roll-out
- ✦ **Detection technology - not just grep!**
 - *These technologies are used in client AV software; these are not back-end server technologies!*
 - Multi-String search
 - Scalpel scanning (precision scanning at the entrvnnint)
 - X-Ray (plaintext crypto attack on virus/worm)
 - CPU emulation
 - P-CODE-driven detection
 - Decide where and when to scan/emulate
 - Hand-code detections in P-CODE
- ✦ **Timeframe**
 - 5 minutes to several weeks (!) to write a signature
 - Several hours or more for false positive/negative testing



Current State: Desktop

Copyright © 2004, Carey Nachenberg, Symantec
Presented: Worm 2004


- ✦ **Heuristics**
 - **Dynamic heuristics**
 - Leverage CPU emulator to coax file-based threat into displaying bad behaviors
 - **Static heuristics**
 - Use signatures to detect known-bad sequences of code
 - Applied to macro, script, and binary threats
- ✦ **Behavior blocking**
 - 1st generation systems today
 - Stop threats by intercepting and blocking system calls
 - Policy-based blocking prevalent
 - Simple buffer-overflow protection (software/NX)



Current State: AV Lab

Copyright © 2004, Carey Nachenberg, Symantec
Presented: Worm 2004


- ✦ **Signature Updates**
 - **Volume**
 - We push up to **1.4B** (virus definition) updates every day
 - Up to **60 terabytes** of data sent down every day!
 - That's up to 6 times the total amount of printed material in the Library of Congress per day
 - **Scalability**
 - Leverage Akamai's 14,000 servers in 1,100 networks
 - **Compression**
 - Employ incremental update technologies and compression (~85-90% percent reduction)
 - Some vendors ship "single definition packages"



Current State: AV Lab

Copyright © 2004, Carey Nachenberg, Symantec
Presented: Worm 2004

- ⌘ Automation
 - Submission filtering
 - Automatic filtering of customer submissions (95%)
 - Application of super-sensitive heuristics for triage purposes
 - Analysis
 - Auto-replication of threats in VMs
 - ⌘ Macro-based threats, binary threats
 - Auto-fingerprint generation with provably-low false positive rates
 - ⌘ Leverages Markov chaining approach
 - Quality Assurance
 - Automated, parallel testing
 - Huge corpora of files for false positive testing



Survey of Research

- ⌘ TBD

Summary

- ⌘ AV Processes
- ⌘ Interesting problems along the processe
- ⌘ Rethinking AV Process
