Execution Context in Anti-

Malware Testing

David Harley

Randy Abrams

In the day (DOS/Mac)…

• Nothing ran automatically except on boot

• No network based attacks

• On-access was little used

On-demand Testing Effective

• Manageable sample set

• Statistically valid

• Viable samples

• Pre-infection scanning was viable

• No Autorun

• Virus rarity

The Age of On-access

• >640K

• Prevalence

• Equivalent to on-demand in detection

• Same validity as on-demand

Disinfection is Bad

• Replace from backups

The Meteor Strikes

• New infection vectors add contextual heuristics

• Email

• Data=code

• CodeRed/automation/obfuscation

• Glut

• Disinfection required

• New testing methodologies needed

Execution Context?
•Execution contextof the scanner
•On –demand/on-access
•Execution contextof the malware
•Active/Latent/Alien
•Product context

Execution Context Testing?

• Testing on the holodeck

• Test the Scanner in its natural habitat

• Test the malware in its normal state of being

• Active/passive/vector used

The Scanner’s Habitat

• Single/Multi-Function Detection Testing versus

Whole Product Evaluation

• Firewall?

• Anti-spam?

• IDS/IPS

• Execution initiated analysis

The Scanner’s Habitat

• Basic Heuristic Analysis (Static/Passive)

• Active/Advanced Heuristics: Dynamic Analysis

• Emulation

• Sandboxing

• Dynamic Analysis

Malware State of Being

• Inactive

• Dormant

• Damaged

• Active

• Stealthed

• Virtually Aware

Fictional Malware
•Malware does not naturally mutate by
competent testing
•Autorun appears 1ston removable media
•Drivebys are downloads

Static Vs Dynamic

• Static testing looks easy: however, overall

detection is hard to measure accurately or

usefully

• Static testing is highly repeatable

• Dynamic testing is harder to do and resource-

intensive.

• Dynamic testing is almost unrepeatable

Challenges
• Sample Validation

• Delivery reproduction

• IP/Geo/Lan aware

• Browser aware

• OS aware?

Challenges
• Virtually aware

• Malcode may detect a VM (virtual machine)

and behave differently:

• Terminate

• Try to take advantage of virtual

environment to access host machine

Challenges
• Account for White listing

• Don’t infect others

• Repeatability

• Exploits

Importance
• True performance assessment requires dynamic

testing

• For a given test set where a product is capable of

detecting all samples, execution context may

sometimes limit detection.

Conclusions
• On-demand testing – still valid

• On-access testing – still valid

• Dynamic testing – valid and essential

Standards
• AMTSO: tests “where a PC is exposed to a live

threat (for example, by attempting to execute

the malware) as part of the test.”

• Academic rigor is required to make dynamic

testing as close to repeatable as possible.