McAfee
An Intel Company

Real-world testing, the good, the bad, and ugly

Craig Schmugar – Research Architect
Aditya Kapoor – Research Architect

October 3, 2013

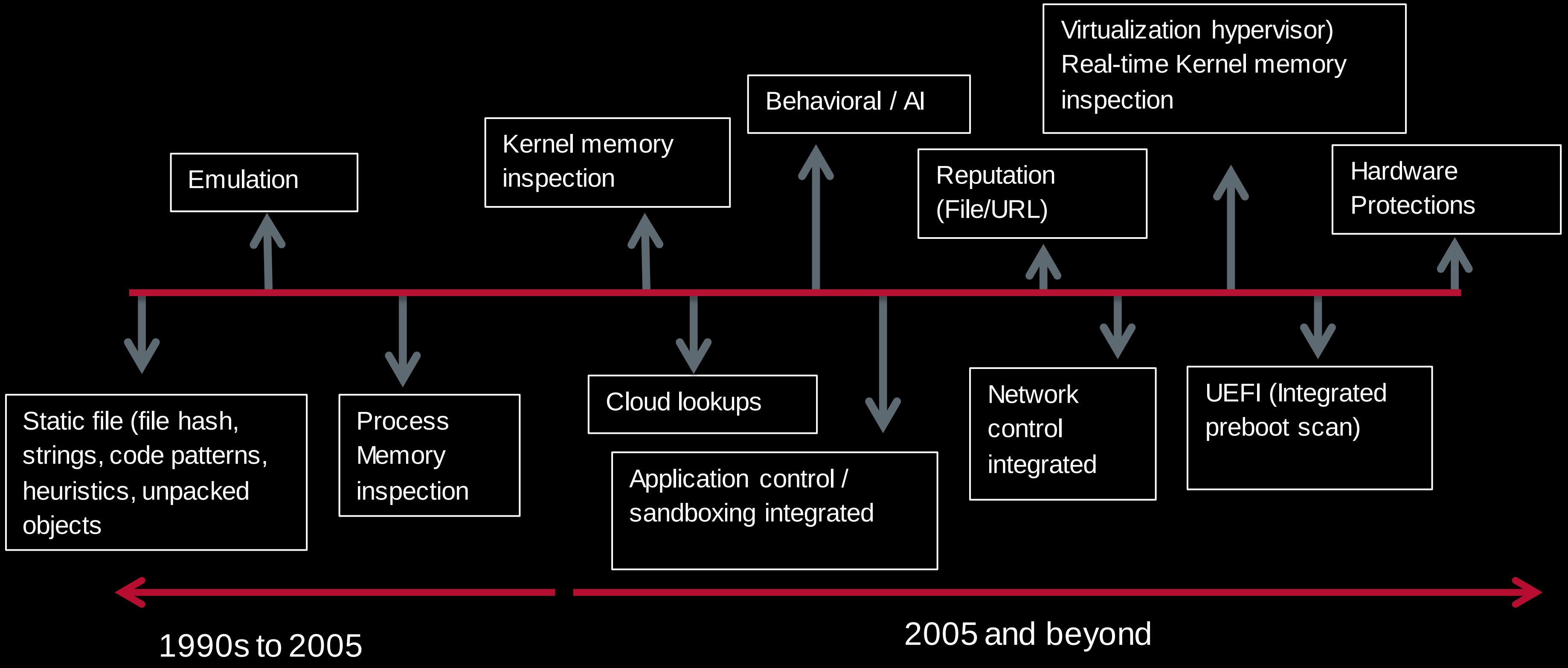
SAFE NEVER SLEEPS™

Introduction – Comparative Testing

- Anti-malware testing in general is hard.
- Comparative testing has evolved greatly over the years
- What is Real-world testing?

Real-world testing aims to evaluate anti-malware suites against in-the-wild malicious attacks, and general system usage, in a manor consistent with authentic user-experience.

Real-world Testing – Defense-In-Depth



Static file (file hash, strings, code patterns, heuristics, unpacked objects)

Emulation

Process Memory inspection

Kernel memory inspection

Cloud lookups

Behavioral / AI

Application control / sandboxing integrated

Reputation (File/URL)

Network control integrated

Virtualization hypervisor) Real-time Kernel memory inspection

UEFI (Integrated preboot scan)

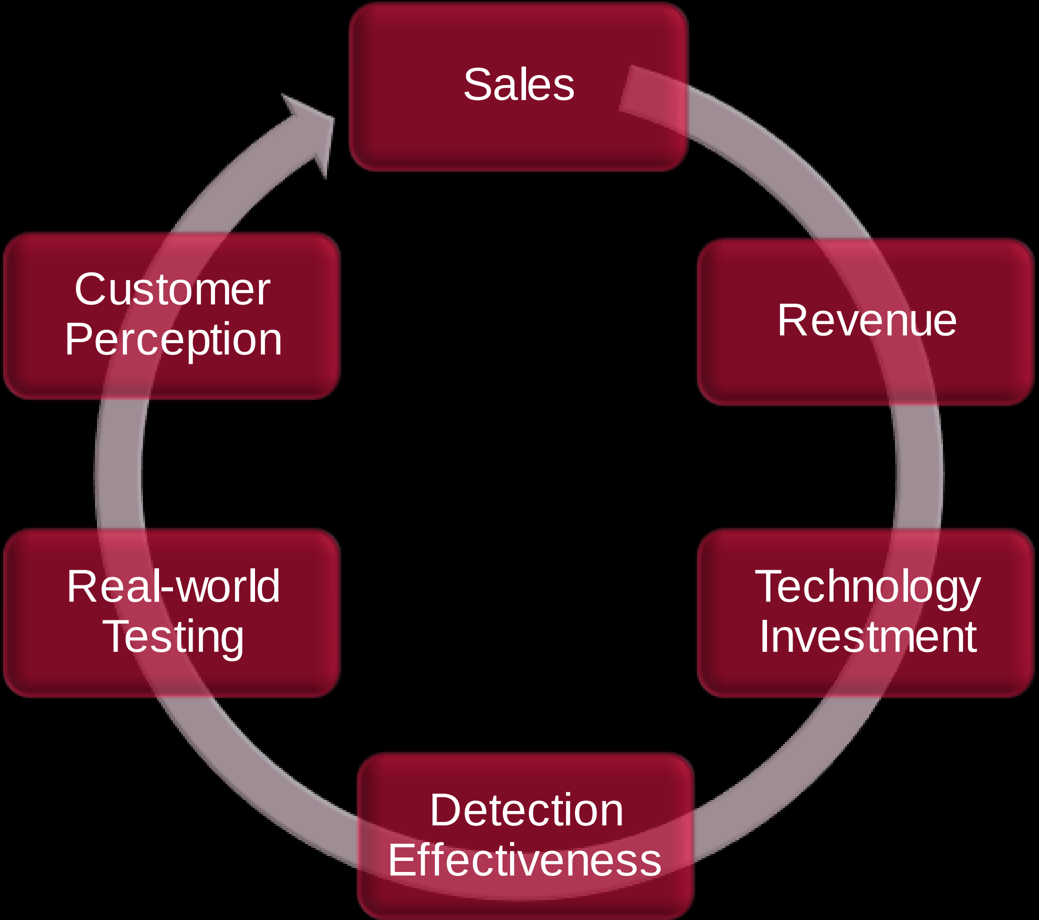
Hardware Protections

1990s to 2005

2005 and beyond

Major detection technologies over time

Real-world Testing – Business Case



Sales

Revenue

Technology Investment

Detection Effectiveness

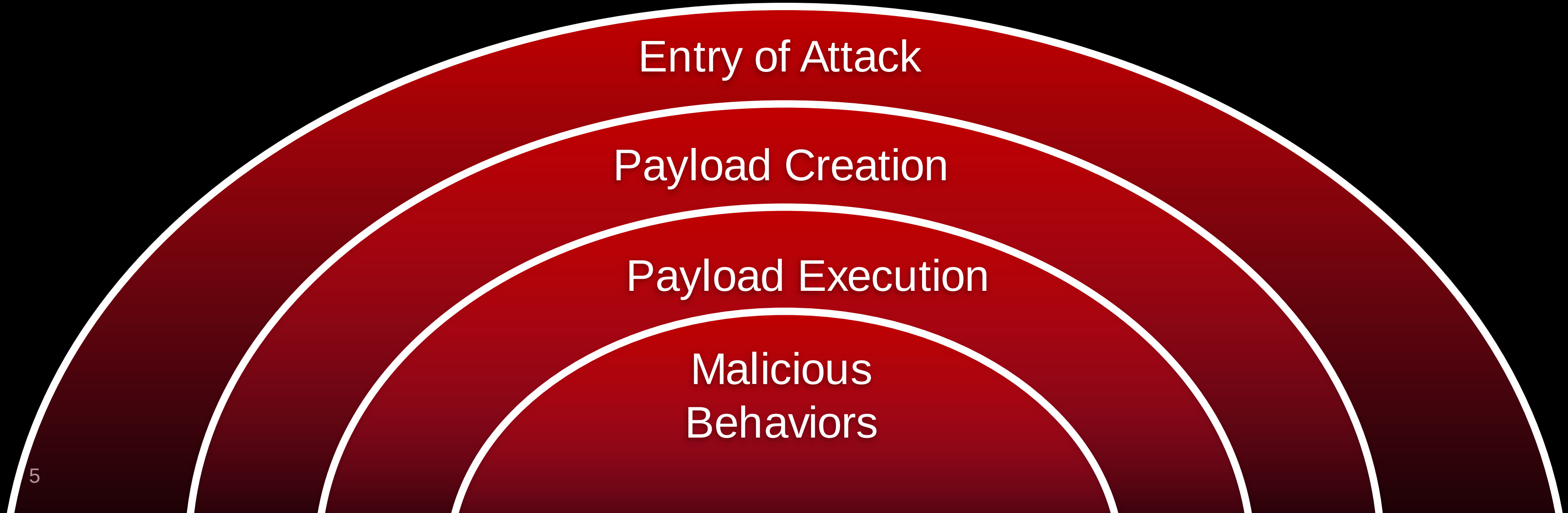
Real-world Testing

Customer Perception

Real-world Testing – Defense-In-Depth

LAN WAN USB

EMAIL WEB



Entry of Attack

Payload Creation

Payload Execution

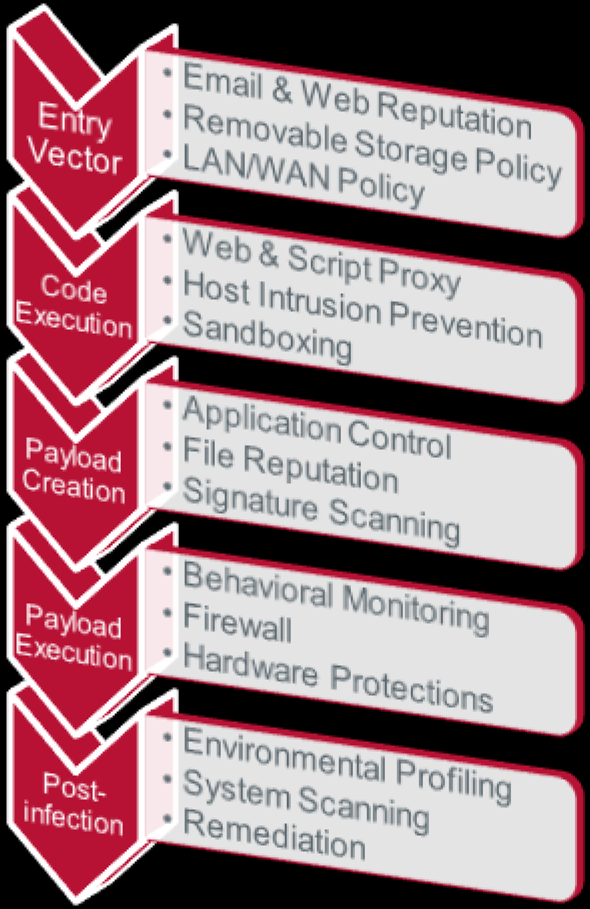
Malicious Behaviors

Real-world Testing – Defense-In-Depth

- What functionality is delivered in the product?

- Q: Does current testing represent the suite? How does one know?

- A: Read product log files
- A: Create a forensic timeline



Entry Vector
- Email & Web Reputation
- Removable Storage Policy
- LAN/WAN Policy

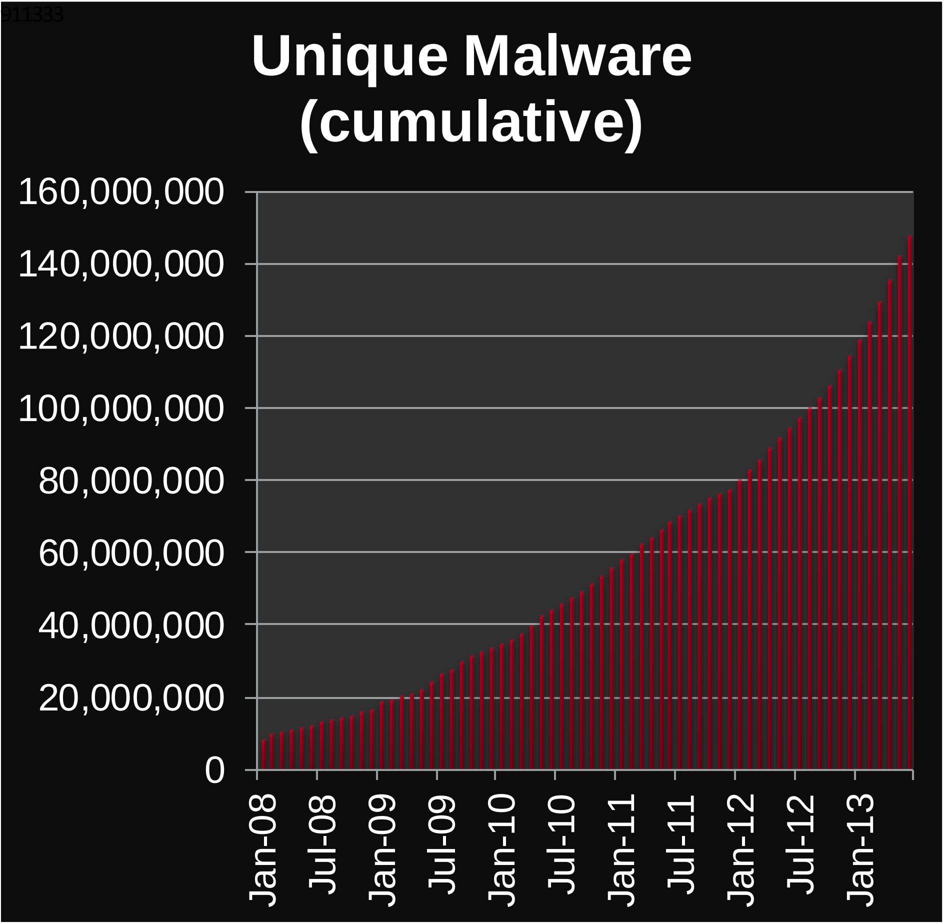
Code Execution
- Web & Script Proxy
- Host Intrusion Prevention
- Sandboxing

Payload Creation
- Application Control
- File Reputation
- Signature Scanning

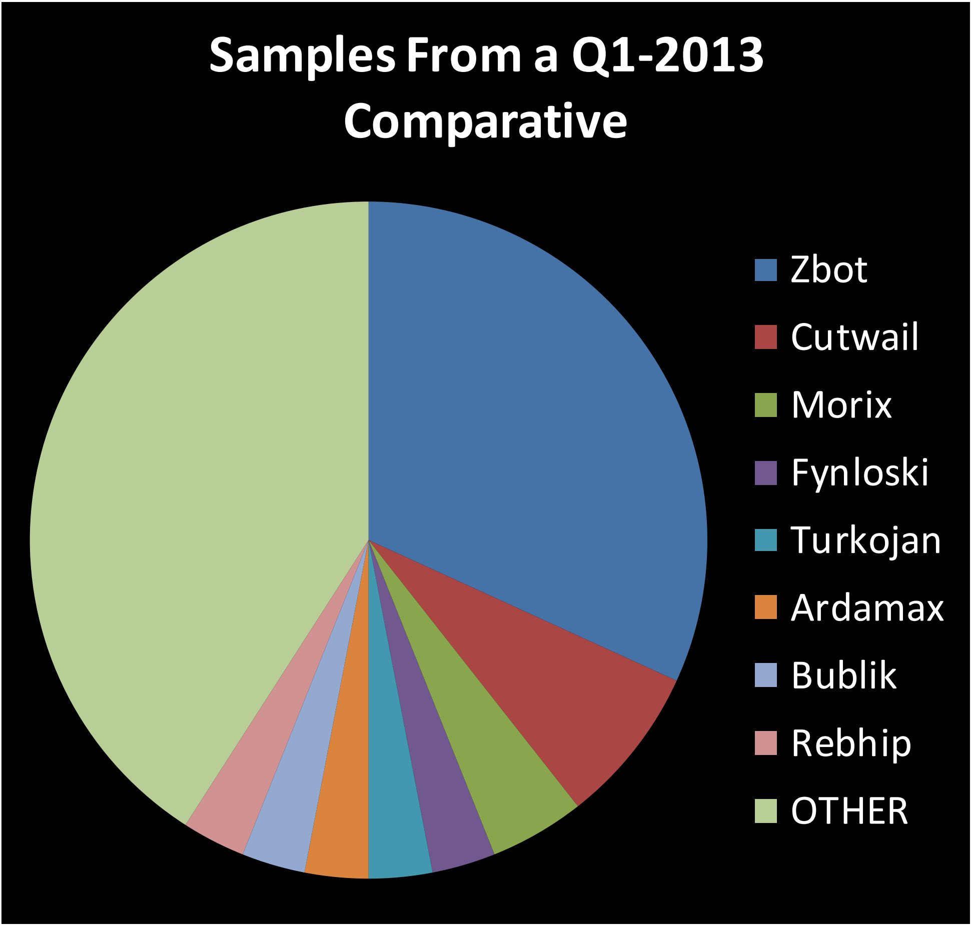
Payload Execution
- Behavioral Monitoring
- Firewall
- Hardware Protections

Post-infection
- Environmental Profiling
- System Scanning
- Remediation

Real-world Testing – Samples

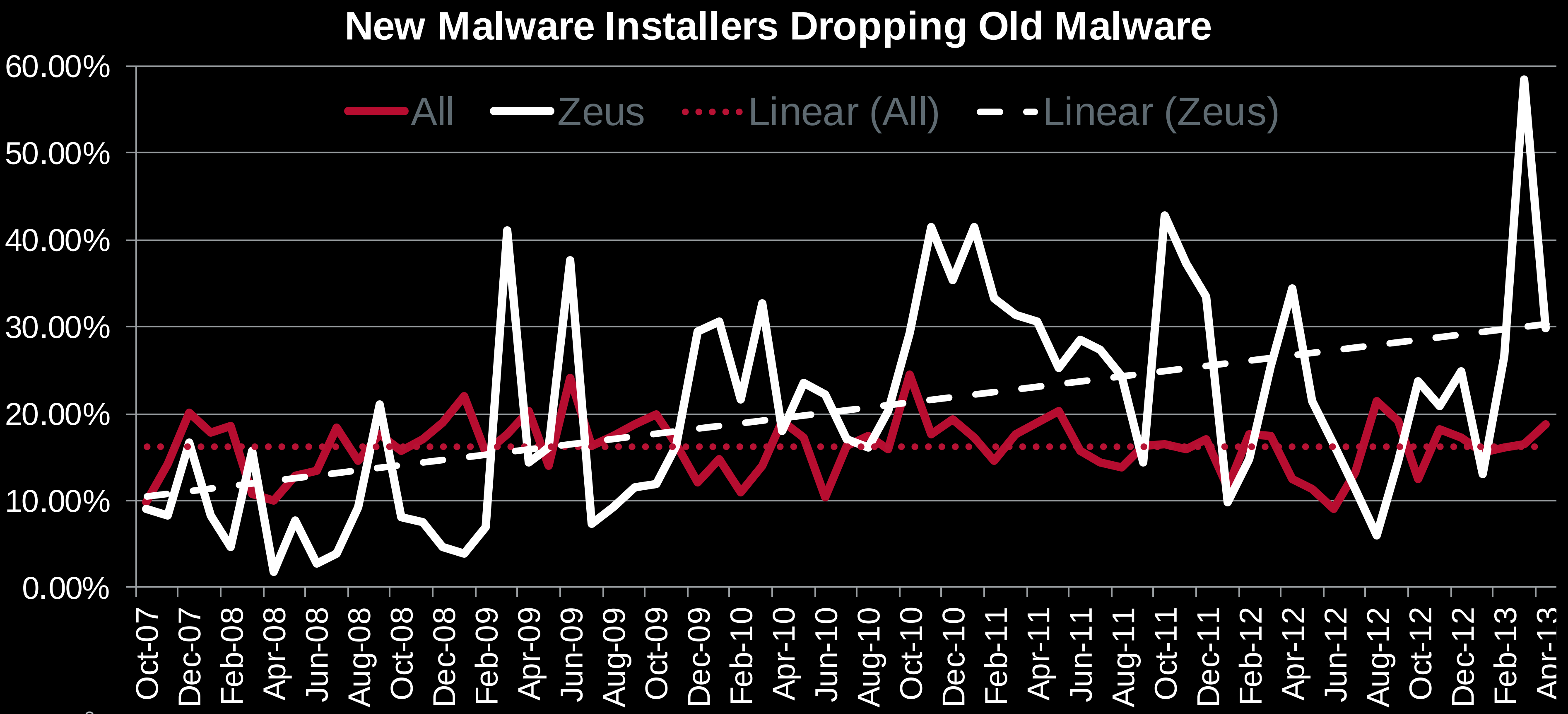


Unique Malware (cumulative)



Samples From a Q1-2013 Comparative

Real-world Testing – Samples



Real-world Testing – Samples

- Samples should meet the goals of the test
  - Wide-spread ?
  - Personalized ?
  - Targeted ?
  - Fresh ?
  - Independently source (not from a common source used by tested vendors) ?

Real-world Testing – Alternate Approaches

McAfee
An Intel Company

- Sample selection
  - Validate sample freshness across multiple sources
  - Lab-created/generated malware
  - Persistent adversary attacks (signed malware, trusted domains)

- Product effectiveness
  - Forensic threat protection analysis
  - Crowdsourcing

- What about attack age-based and prevalence-based protections?

Real-world Testing – Conclusions

- Full product real-world testing should test (a) the full product, exercising as many features as possible, (b) reward protection greater than detect/remediate and (c) test diverse real-world scenarios.

- Testing goals should be defined more clearly, represented in the methodology, and spelled out in publications.

- Test results should be made available on a granular level to allow readers to compare products under different circumstances.

Questions?