eEye Digital Security®

Know your vulnerabilities. Know you're protected.

Agenda

- Today's Threat Landscape
- Zeroday Vulnerability Trends
- Attack Surface/Configuration
- Security's Cultural Shift
- Security in Context

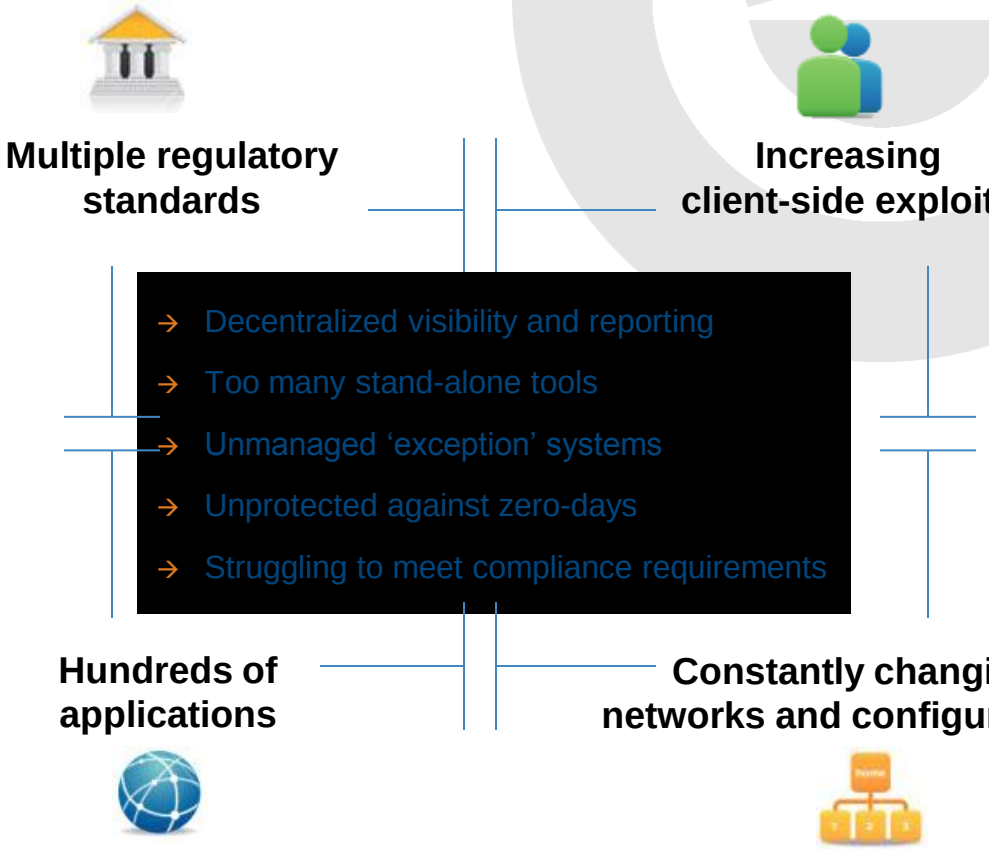
eEye Digital Security®

Time-Consuming Vulnerability Management

2011 VM Trends

- Managing **compliance initiatives** takes IT Security Pros up to 50% of their work week.
- **Centralized visibility** is key to vulnerability management with 73% of organizations having as many as 100 applications deployed.
- 31% of IT pros do not have enough personnel to **patch vulnerabilities** - a challenge intensified by lack of integration between scan and patch solutions.

Source: eEye 2011 VM Survey of 2,000 IT Security Professionals

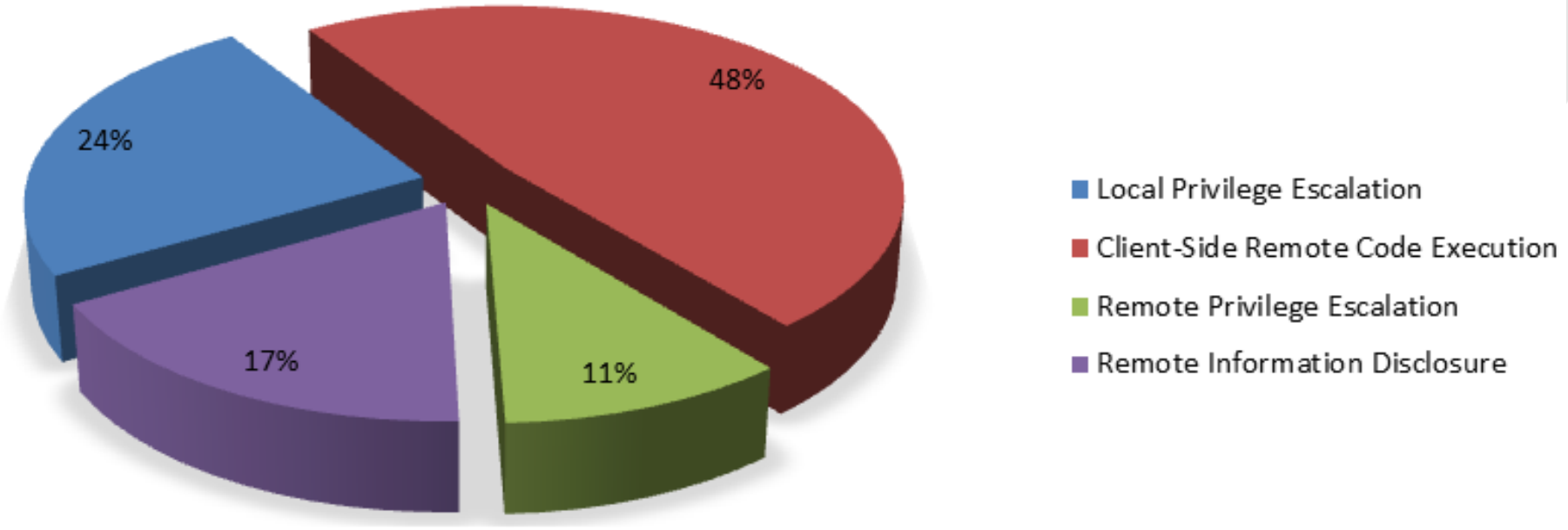


eEye Digital Security®

Zeroday Vulnerability Trends

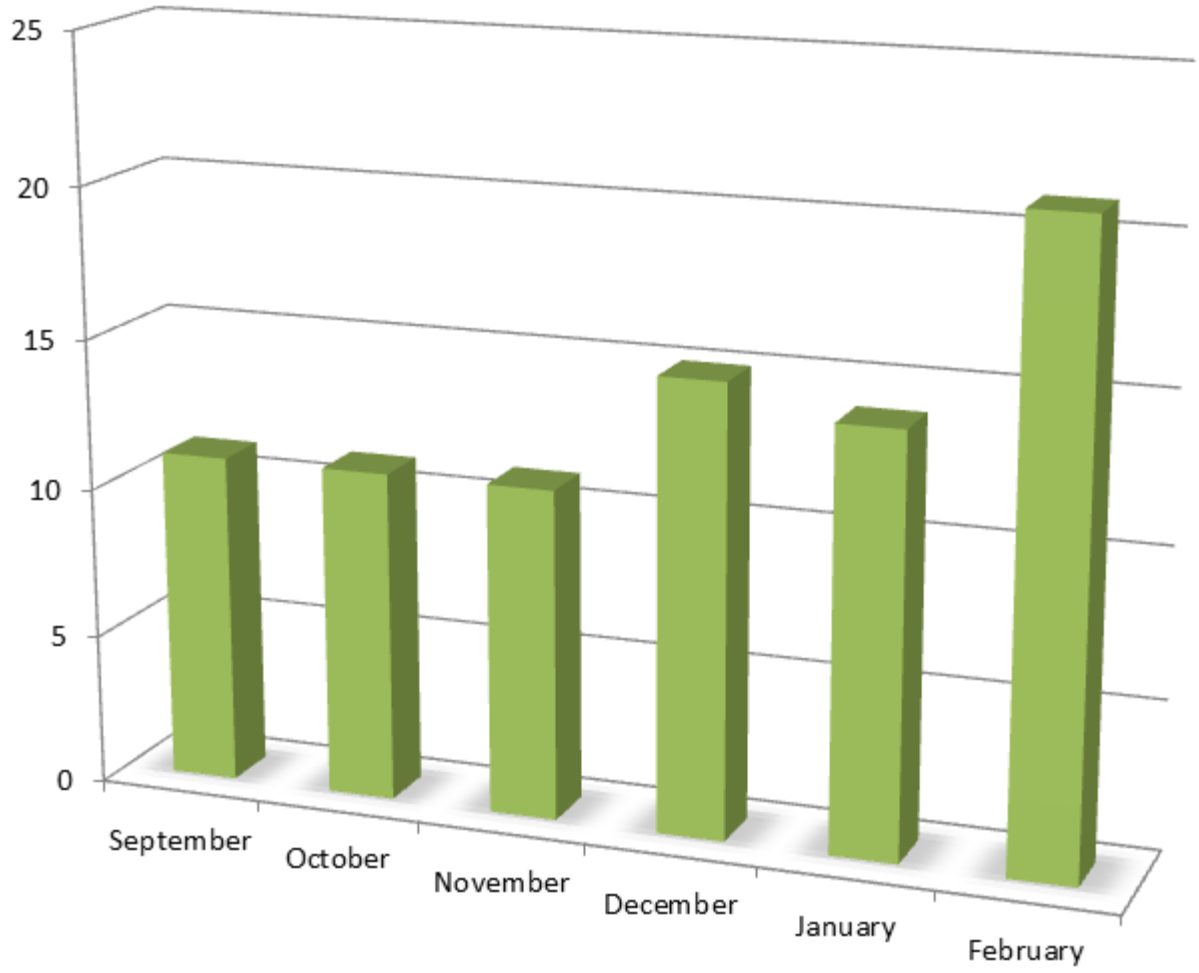
http://www.**eEye.com/ZDT**

Zeroday Vulnerabilites by Type



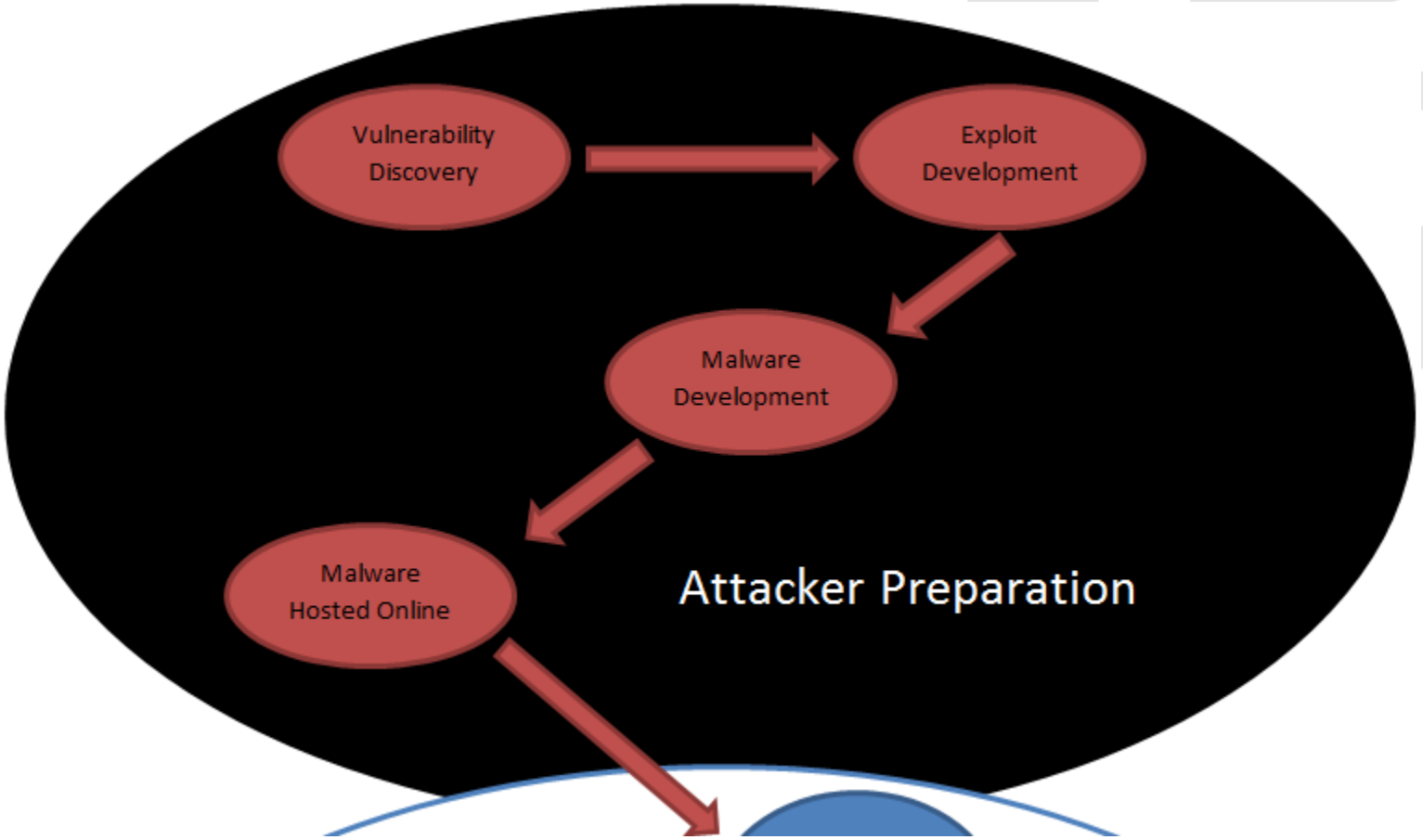
eEye Digital Security®

Zeroday: Tip of the iceberg



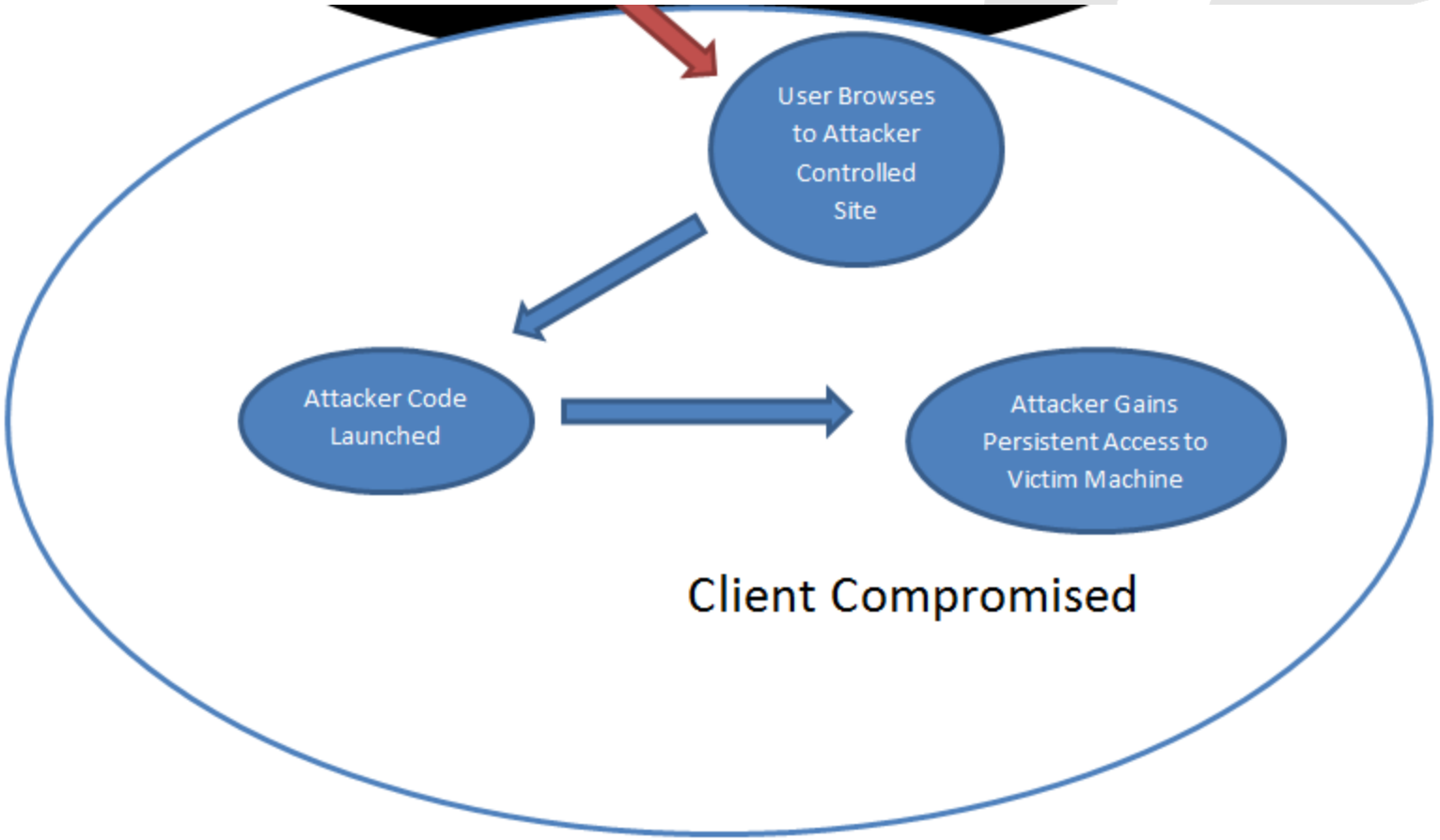
eEye Digital Security®

Anatomy of an Attack – Attacker Preparation



eEye Digital Security®

Anatomy of an Attack – Data Compromised

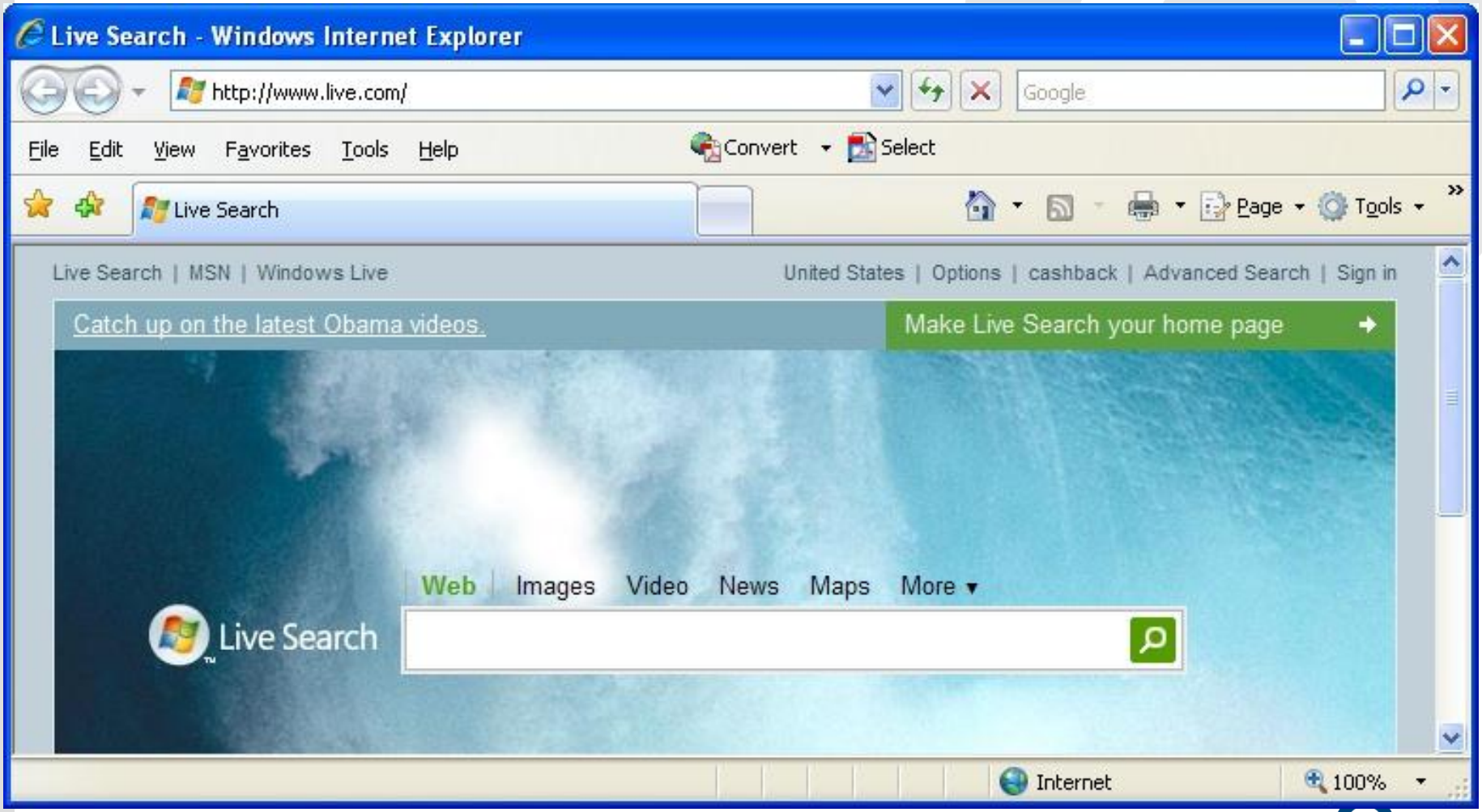


eEye Digital Security®

Attack Surface

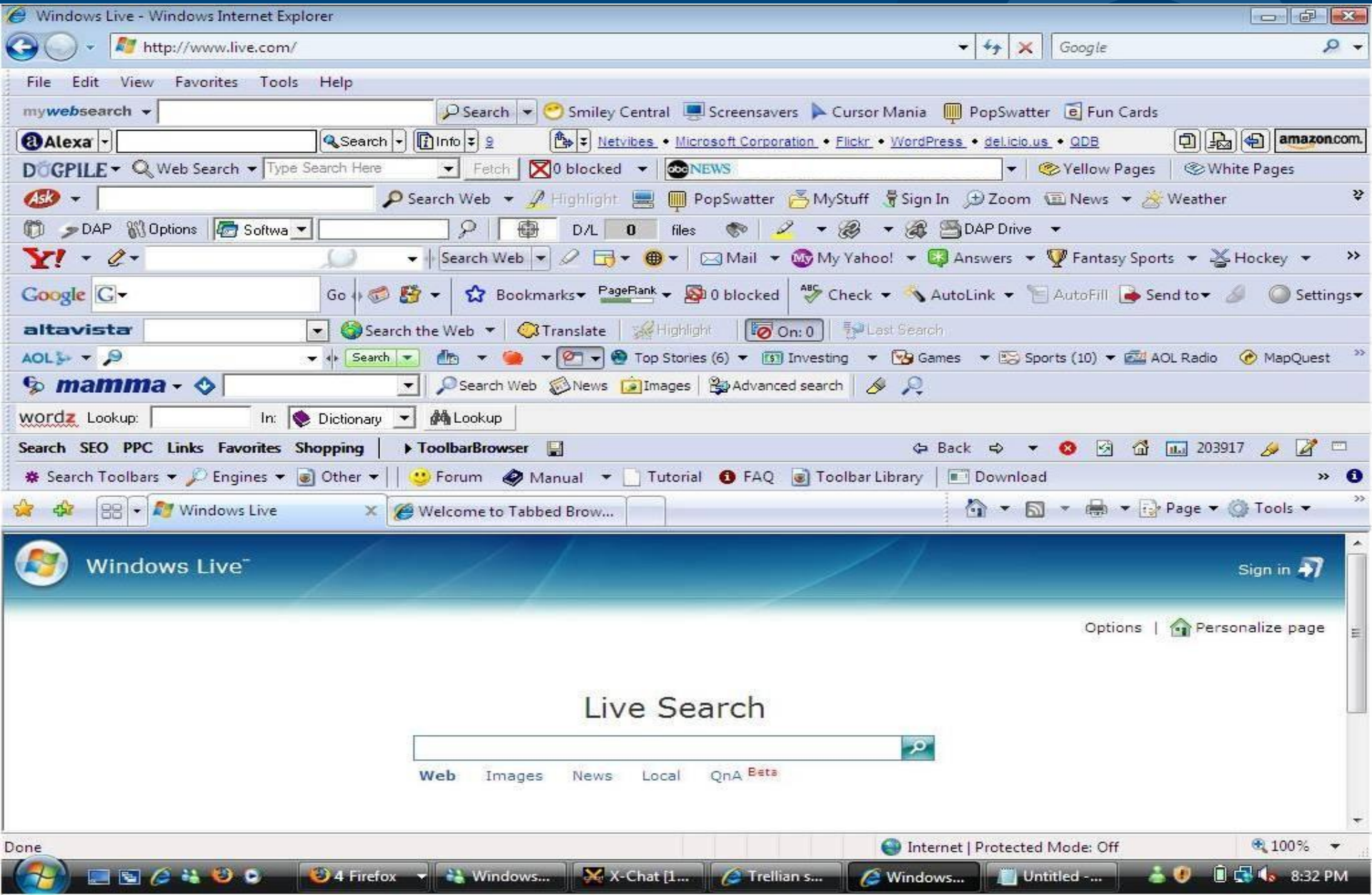
Where security begins and ends.

Attack Surface



eEye Digital Security®

Attack Surface



More Than a Microsoft World

- Adobe Acrobat
- Apple iTunes
  - iPhone's anyone?
- IBM Laptops
- Backup Software (Symantec)
- Custom web applications
- Quicktime, Realplayer, Java, Oracle, SAP, GreatPlains, Quicken, McAfee, Symantec, and many more…

Buzzword Bingo

Unified Endpoint Security Management

Malware Detection

Application Control

Database Security

Cloud Security and Compliance

Zero Day Protection

Next Generation Threat Protection

Data Loss Prevention

Next-Generation Firewall

Application Whitelisting

Behavioral Monitoring

Intrusion Prevention

UNIFIED CONTENT SECURITY

EndPointSecurity

eEye Digital Security®

How many products do we really need?

- Signal vs. Noise

eEye Digital Security®

Back to Basics

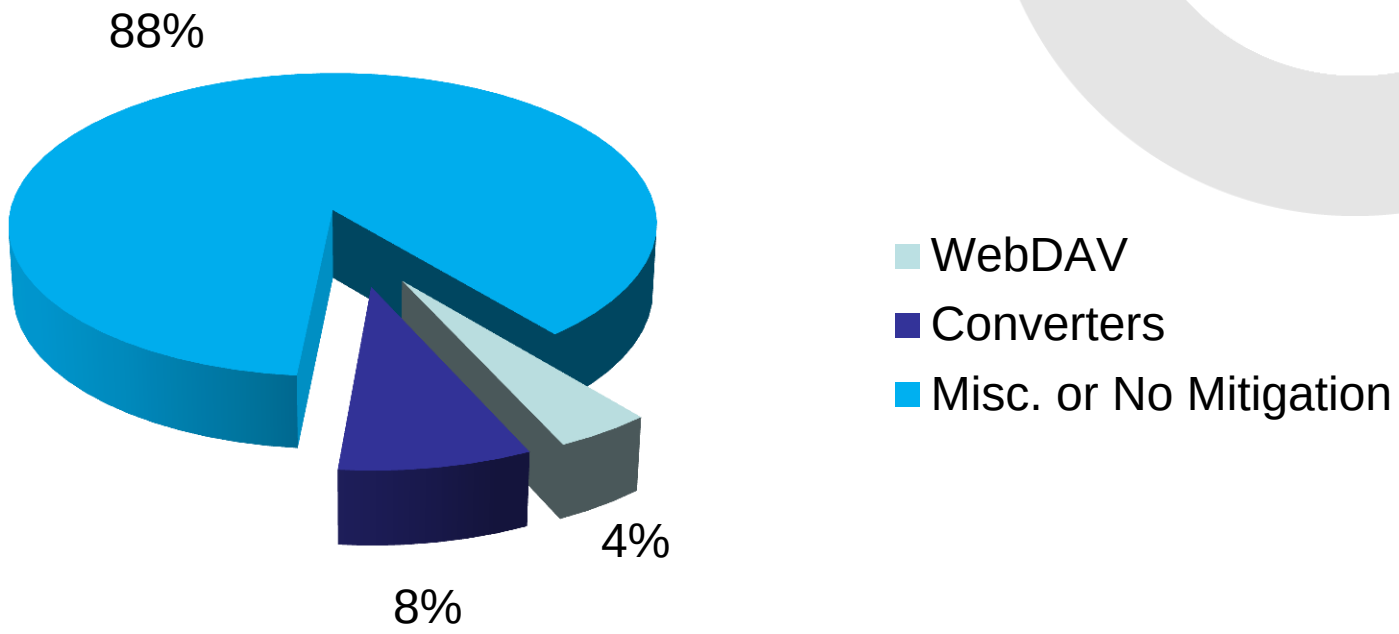
Good Configuration > Security Product

Why our security fails us?

- Monoculture
  - Not just an operating system problem.

Top 2 Mitigations vs. Microsoft 2010 Vulnerabilities

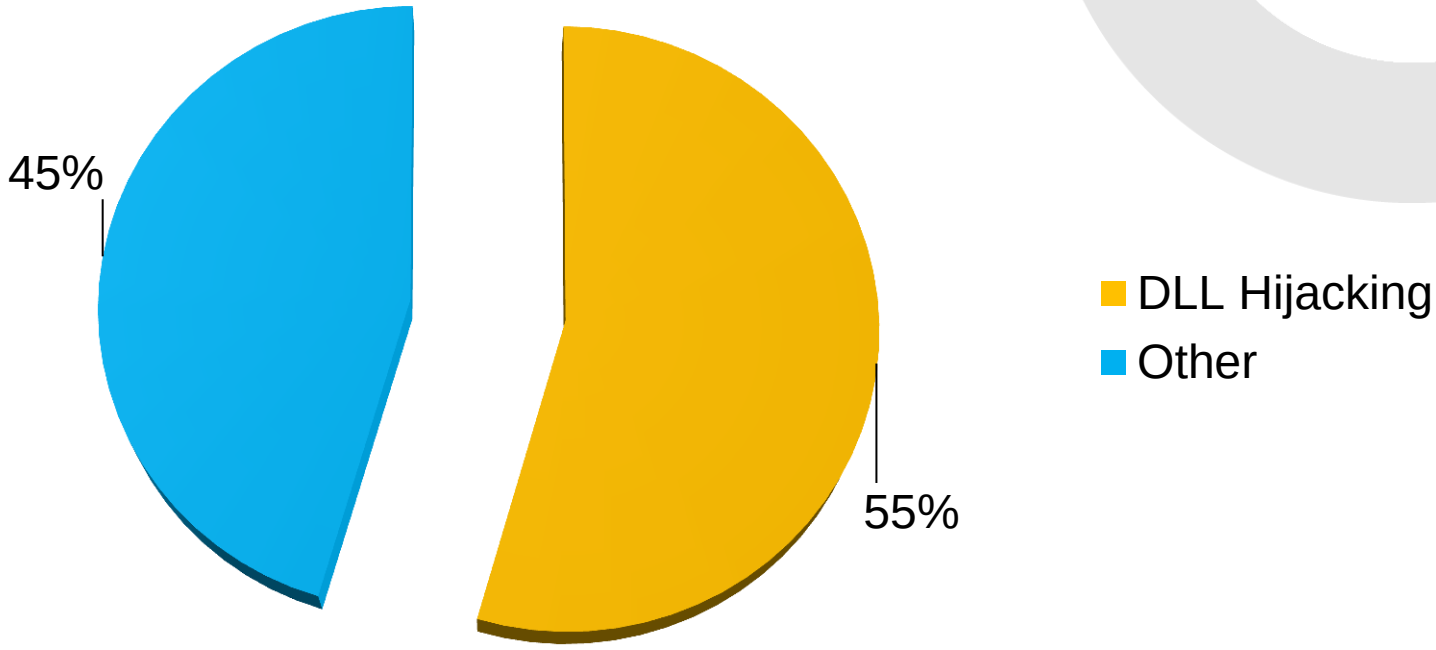
Types of Mitigation for 2010



eEye Digital Security®

Microsoft 2010 Patches - WebDAV

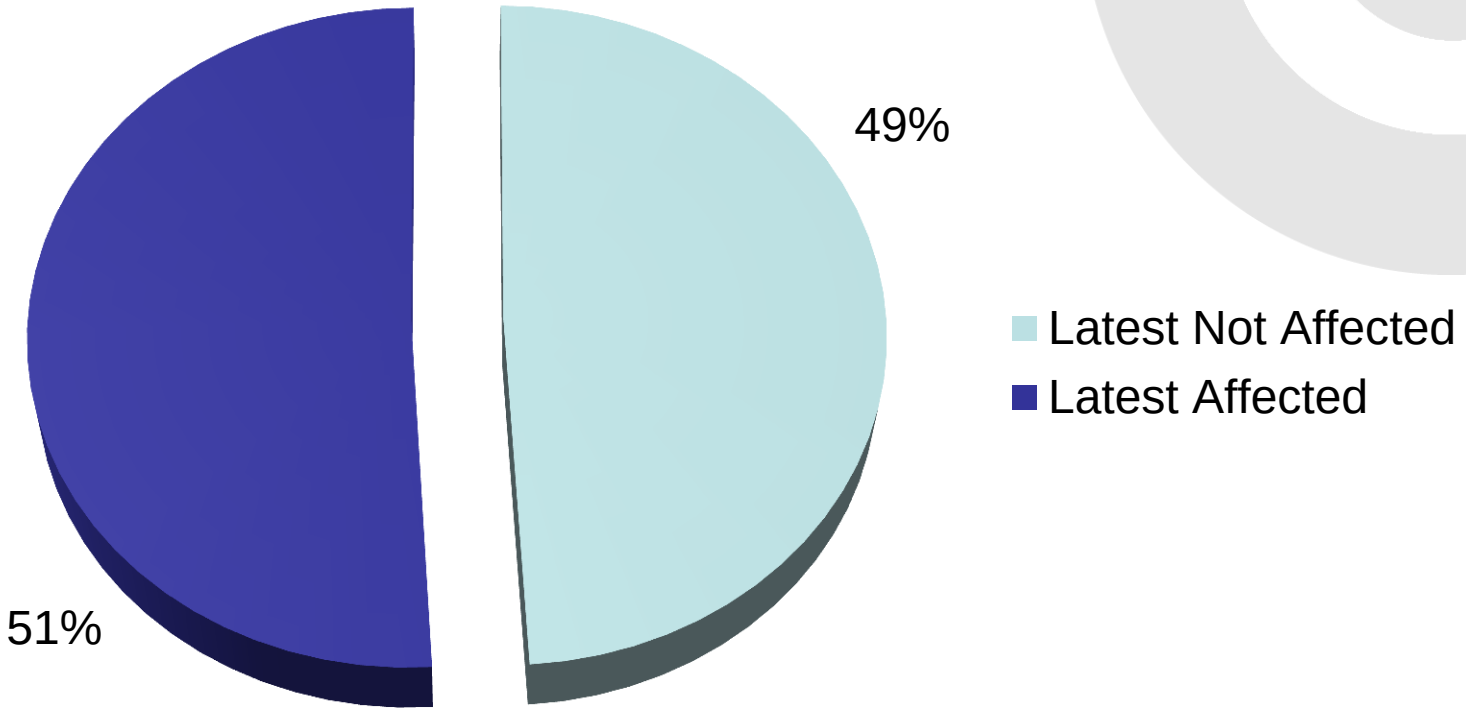
DLL Hijacking Breakdown



eEye Digital Security®

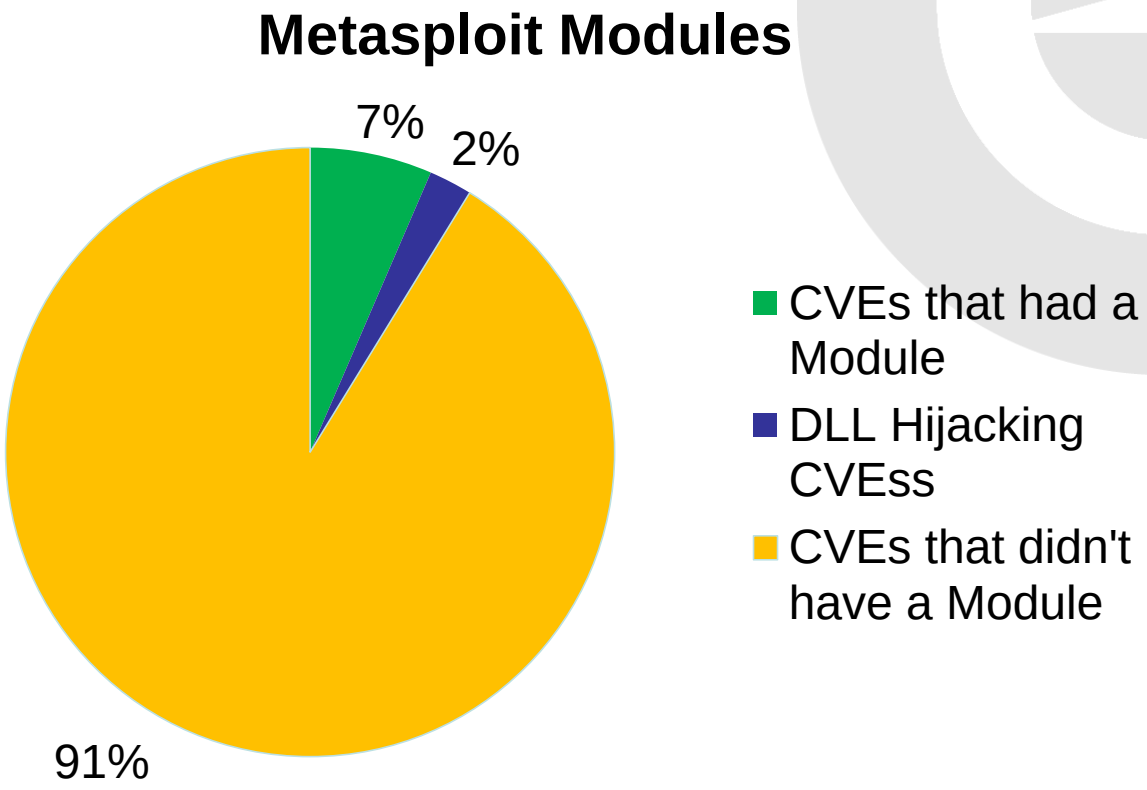
New = Better

Microsoft 2010 Patches vs. Latest Products



eEye Digital Security®

Metasploit vs. Microsoft 2010 Vulnerabilities



eEye Digital Security®

Security's Cultural Shift

- What's hype and what's a real concern with:
  - Stuxnet
  - Night Dragon
  - Aurora
  - Nation-sponsored hacking
  - Advanced Persistent Threats
- Security / Social Media / Mobile Computing..
  - Sliding scale, push back and find a balance or fail.

eEye Digital Security®

Security in Context.

Advanced Threat Protection (Stuxnet)

- Network anomaly detection
- Host based behavioral software
- File system permission hardening
- Neural network fuzzy logic uber security
- System disconnected from network

eEye Digital Security®

Mobile Security, which is worse?

Jailbroken? OR Client-side Exploit?

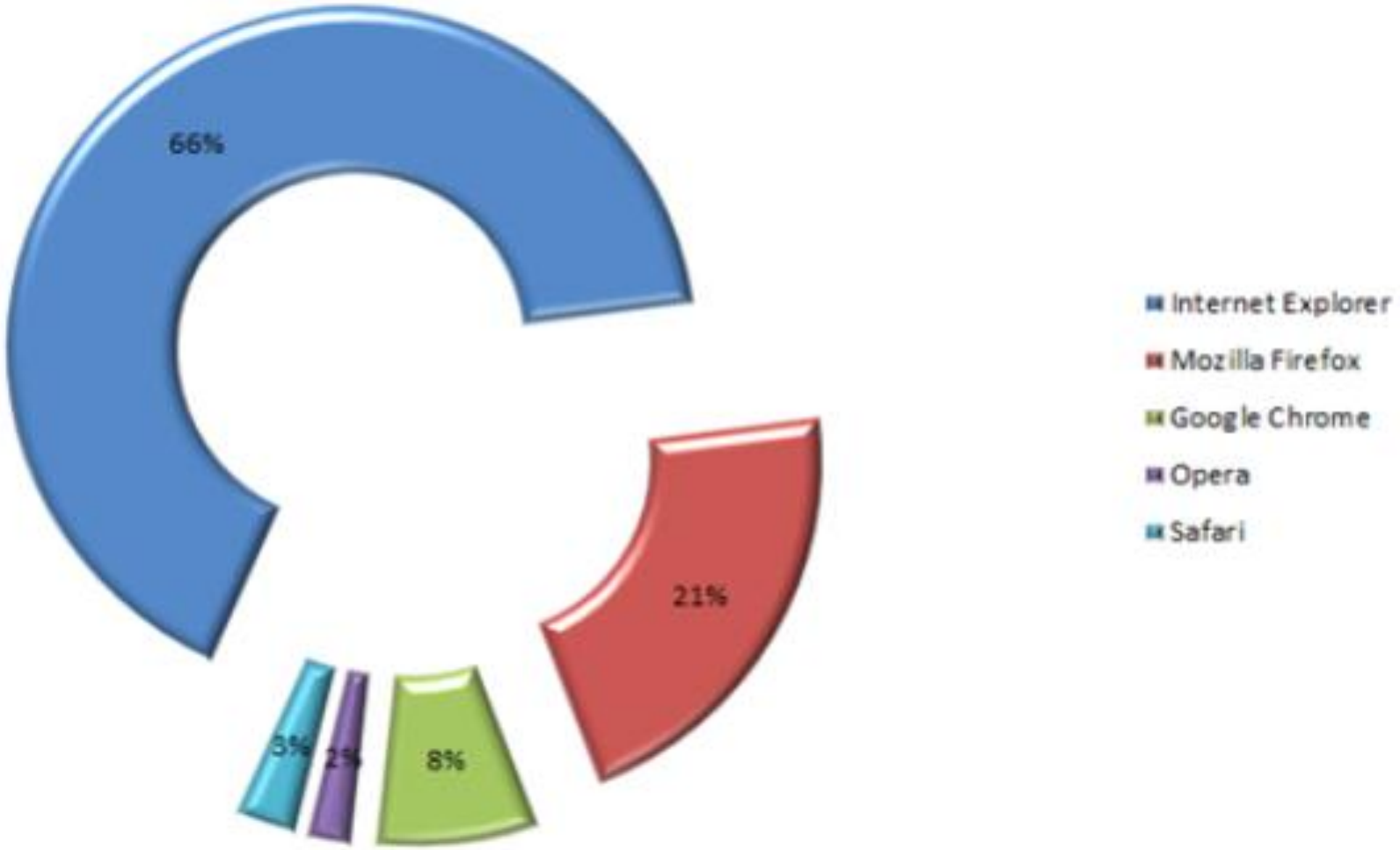
eEye Digital Security®

Which app is more vulnerable?

76 Vulnerabilities? OR 32 Vulnerabilities?

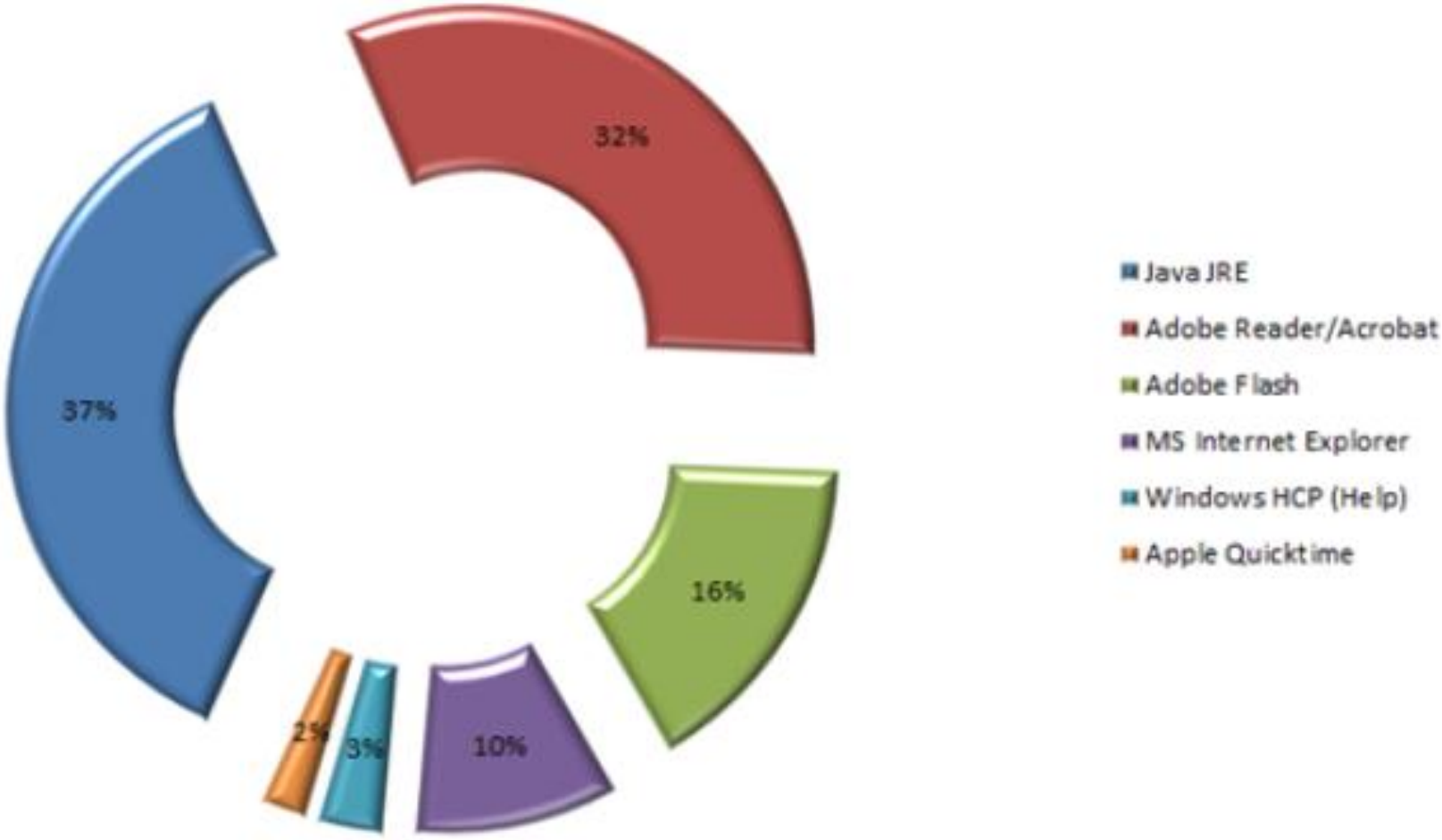
eEye Digital Security®

Most Exploited Web Browser



eEye Digital Security®

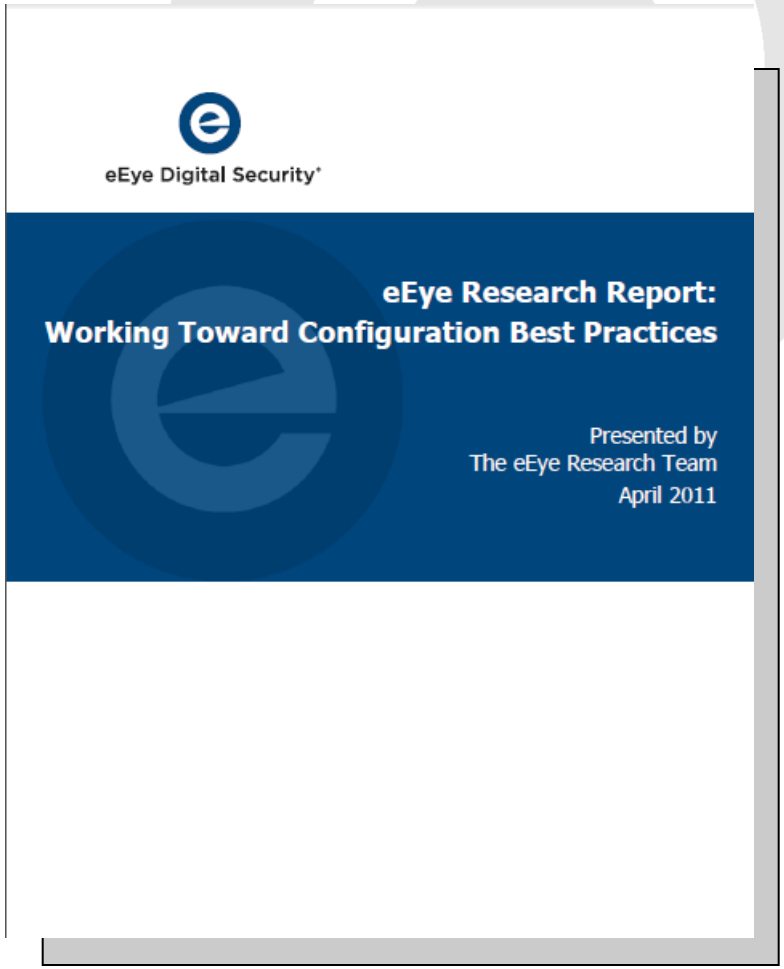
Most Exploited Software



eEye Digital Security®

eEye Research Report

- New report from the eEye Research Team:
  In Configuration We Trust
- Insights into straightforward changes you can make right away – for free – that will dramatically improve your security posture.
- http://pages.eeye.com/ConfigurationReport.html



eEye Digital Security

Free eEye Resources

A Tradition of Supporting the IT Security Community:

- Zero Day Tracker: www.eeye.com/zdt
- Vulnerability Experts Forum: www.eeye.com/vef
- eEye Blog and Social Networking: http://blog.eeye.com
- Retina Community: http://community.eeye.com

eEye Digital Security®