FireEye™

# Defending Against Advanced Targeted Attacks

Dirk Beste
Security System Engineer
FireEye, Inc. Germany
Dirk.Beste@FireEye.Com

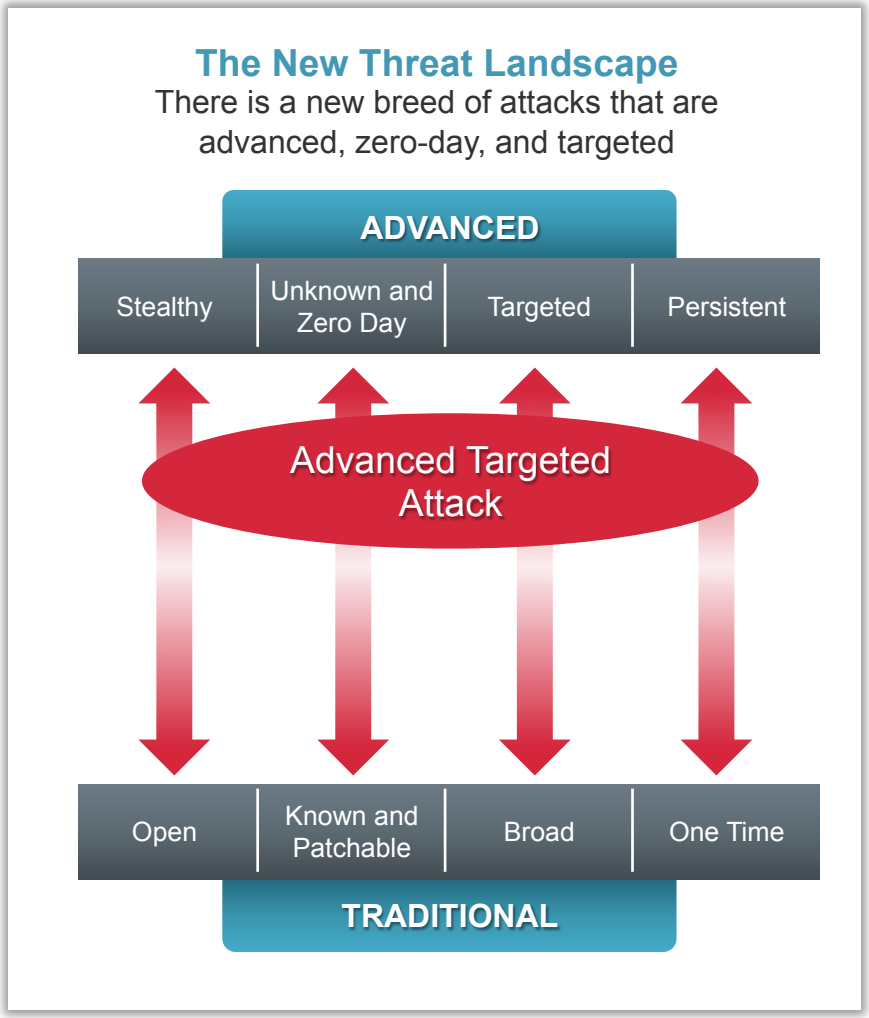
# Company Overview

- Founded 2004, based in California
- 5 years engineering development
- Multiple patents awarded
- The leader in stopping advanced targeted attacks
- One of the fastest growing enterprise technology companies in the world


FireEye

# Defining Advanced Targeted Attacks

- Utilizes advanced techniques and/or malware
  - Unknown
  - Targeted
  - Polymorphic
  - Dynamic
  - Personalized
- Uses zero-day exploits, commercial quality toolkits, and social engineering
- Often targets IP, credentials and often spreads laterally throughout network
- AKA—Advanced Persistent Threat (APT)




FireEye

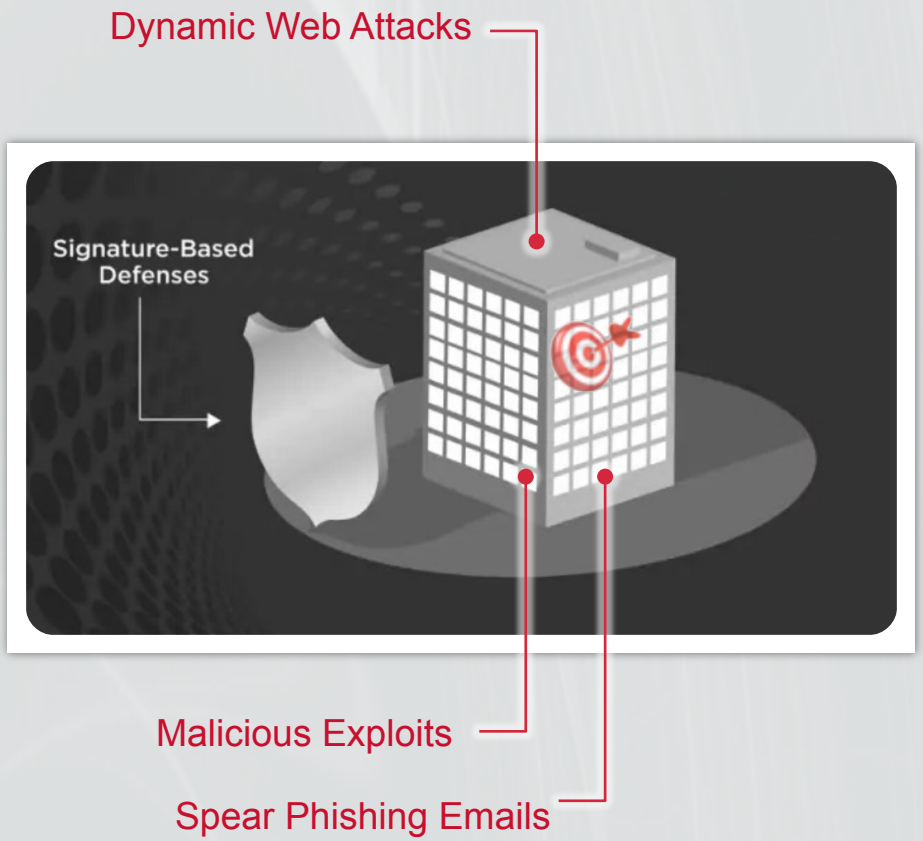
# Attacks Increasingly Sophisticated

## Multi-Vector

- Delivered via Web or email
- Blended attacks with email containing malicious URLs
- Uses application/OS exploits

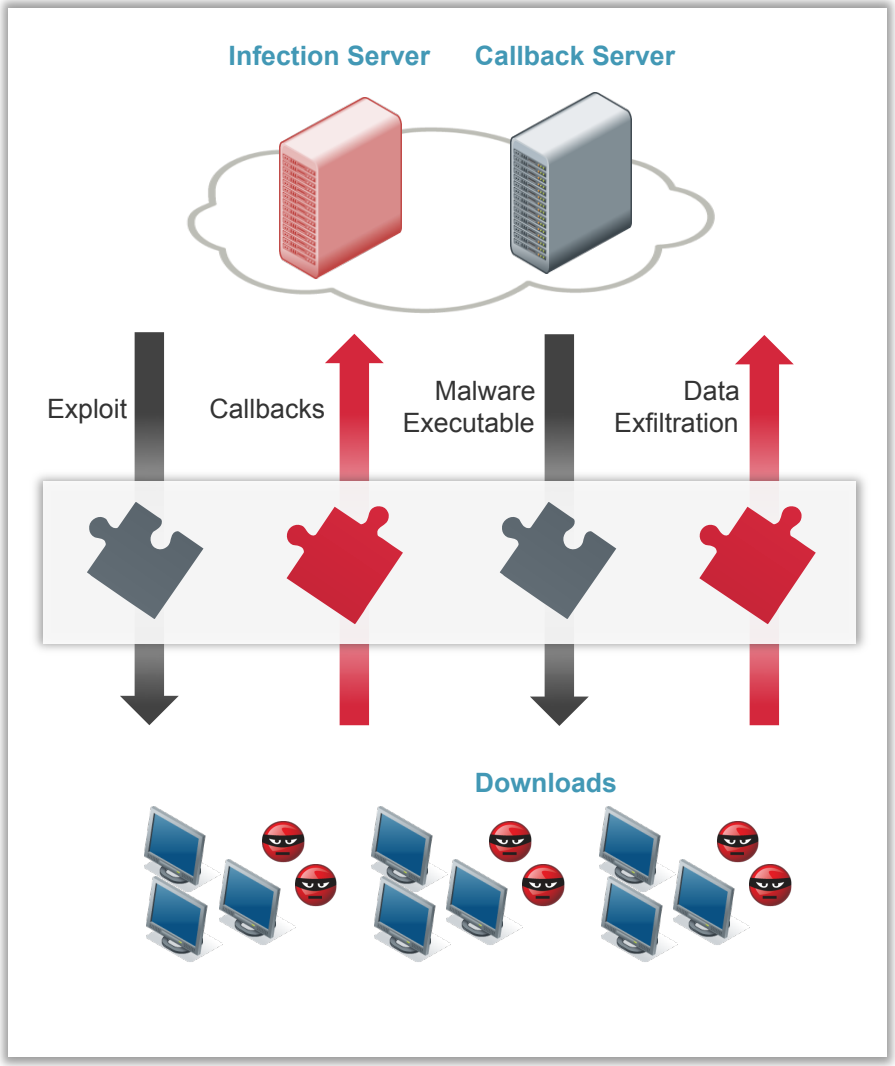
## Multi-Stage

- Initial exploit stage followed by malware executable download, callbacks and exfiltration
- Lateral movement to infect other network assets




FireEye

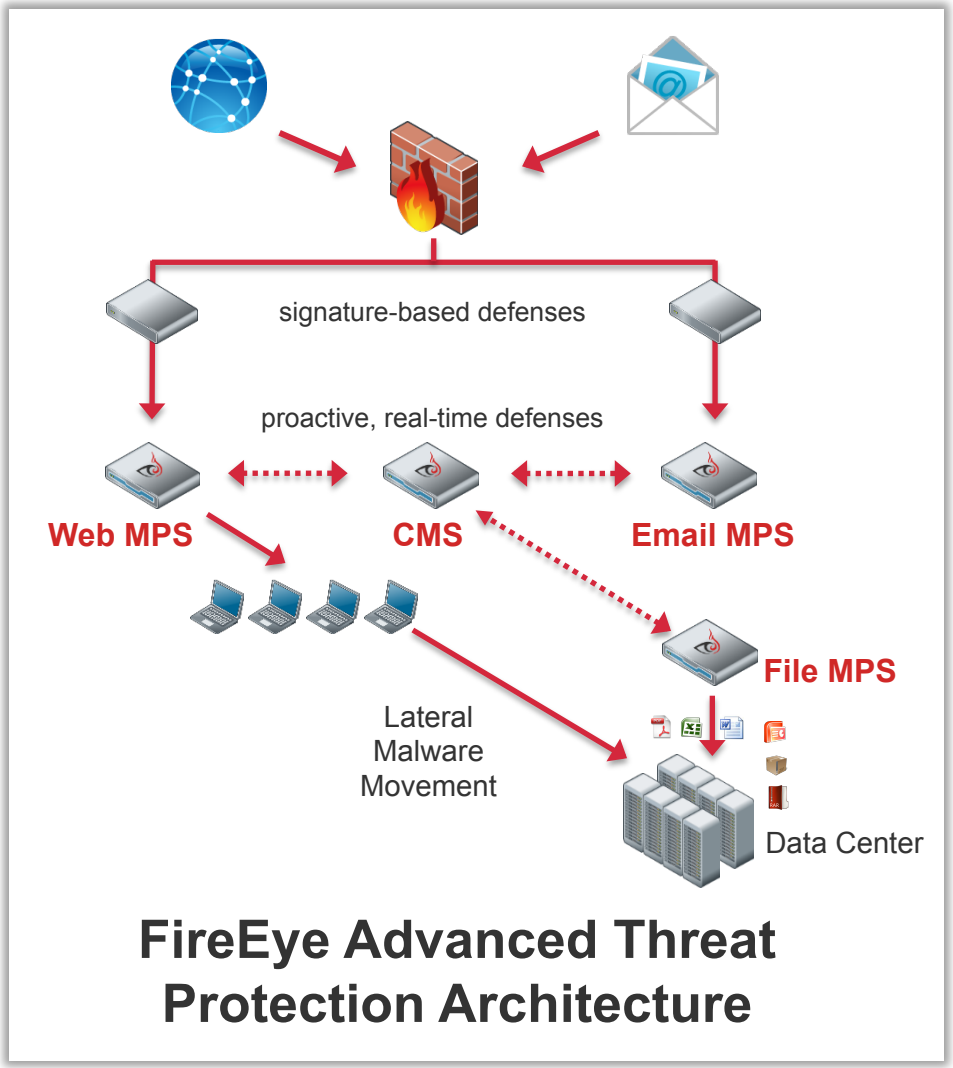
# Multi-Flow, Stateful Web Attack Analysis




- FireEye uses multi-flow analysis to understand the full context of an advanced attack
- Stateful attack analysis enables customers to see the entire attack lifecycle
- Point products only focus on a single attack object (e.g., malware executable), thereby missing the attack and full lifecycle view

FireEye

# Protecting Against Advanced Targeted Attacks




**FireEye Advanced Threat Protection Architecture**

- Inline blocking and quarantine available across MPS portfolio
  - Block inbound zero-day Web attacks
  - Multi-protocol blocking of callbacks
  - Quarantine of malicious zero-day emails
  - Quarantine of malicious zero-day files
- Mitigates risk of data exfiltration
- Provides highly actionable information for timely incident response

FireEye

# Multi-Protocol, Real-Time VX Engine

**PHASE 1**
Multi-Protocol Object Capture

**PHASE 2**
Virtual Execution Environments

**PHASE 1: WEB MPS**
- Aggressive Capture
- Web Object Filter

**PHASE 1: E-MAIL MPS**
- Email Attachments
- URL Analysis

**PHASE 1: FILE MPS**
- Network File Shares

**Map to Target OS and Applications**

**DYNAMIC, REAL-TIME ANALYSIS**
- Exploit detection
- Malware executable analysis
- Cross-matrix of OS/apps
- Originating URL
- Subsequent URLs
- OS modification report
- C&C protocol descriptors

FireEye

# Summary

- Pace of advanced targeted attacks is accelerating, affecting all verticals and all segments
- Traditional defenses (NGFW, IPS, AV, and gateways) no longer stop these attacks
- Real-time, integrated signature-less solution is required across Web, email and file attack vectors
- FireEye has engineered the most advanced threat protection to supplement traditional defenses and stop advanced targeted attacks

**For more information:**
[www.fireeye.com](http://www.fireeye.com)


FireEye