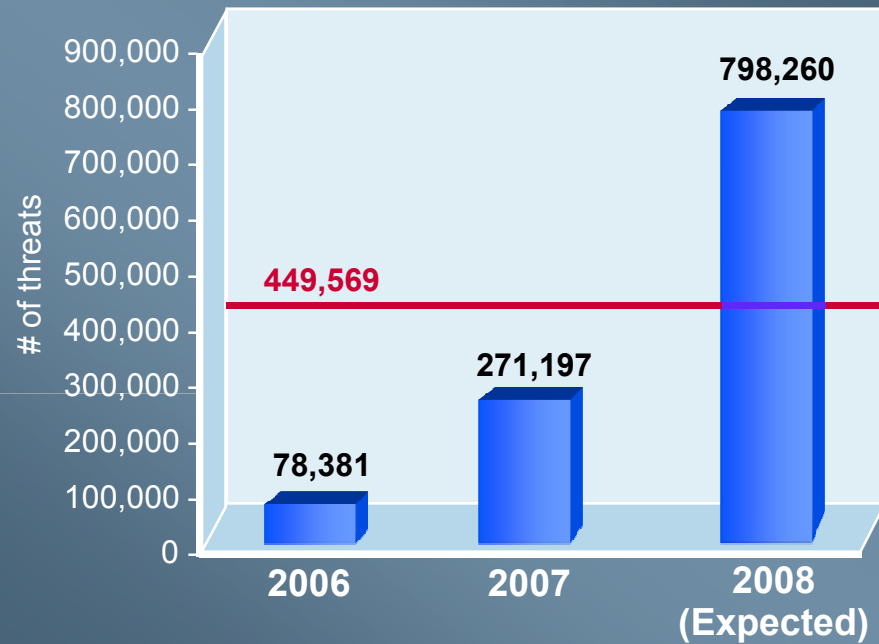




# Cyber Crime Altering Threat Landscape



- 246% growth from '06 to '07
- 300% growth projected from '07 to '08
- YTD greater than '06 and '07 combined
- Over 3500 updates added to DAT file per day

Source: McAfee Avert Labs

**McAfee**

23 MAY 2008



Protect what you value.

## The Last Two Years in Anti-Malware:

- **357820 unique pieces of malware identified by Avert Labs by the end of 2007**
- Over **135885+** malware identified during 2007 which WAS 38% of all malware created up to that point in time
- **Over 711000 identified by Avert Labs in 2008 alone**
- **137528** in June 2008
- **231715** in July 2008
- **95%** or more are static (nor replicating)
  - If it ain't a trojan it's a trojan
- **90%** or more are obfuscated
  - Runtime packers and/or encryption

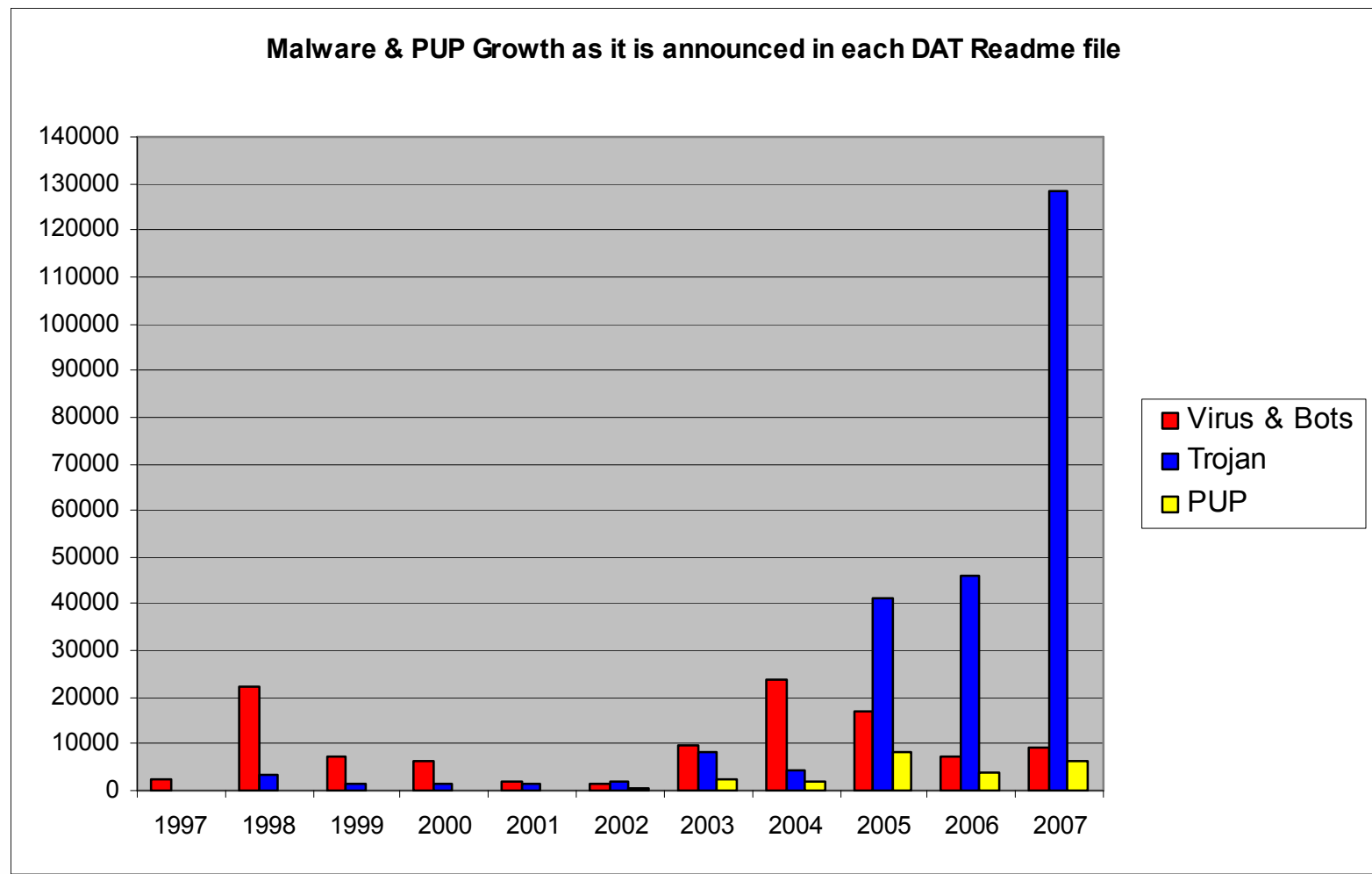
The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

23 MAY 2008



Protect what you value.

# Malware today is very different from days of old

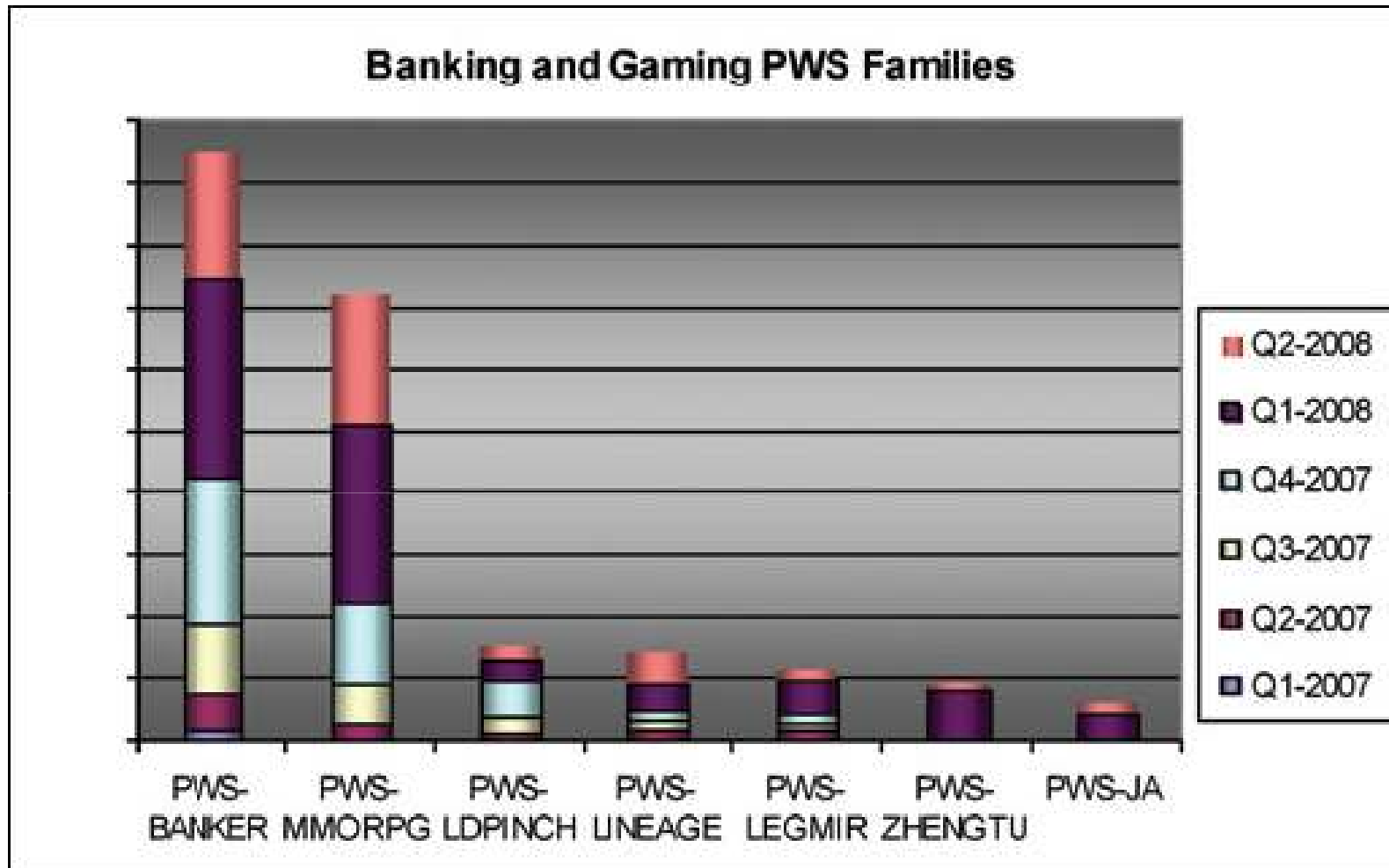


**McAfee**

23 MAY 2008

Protect what you value.

# The Malware of Choice: Password Stealers



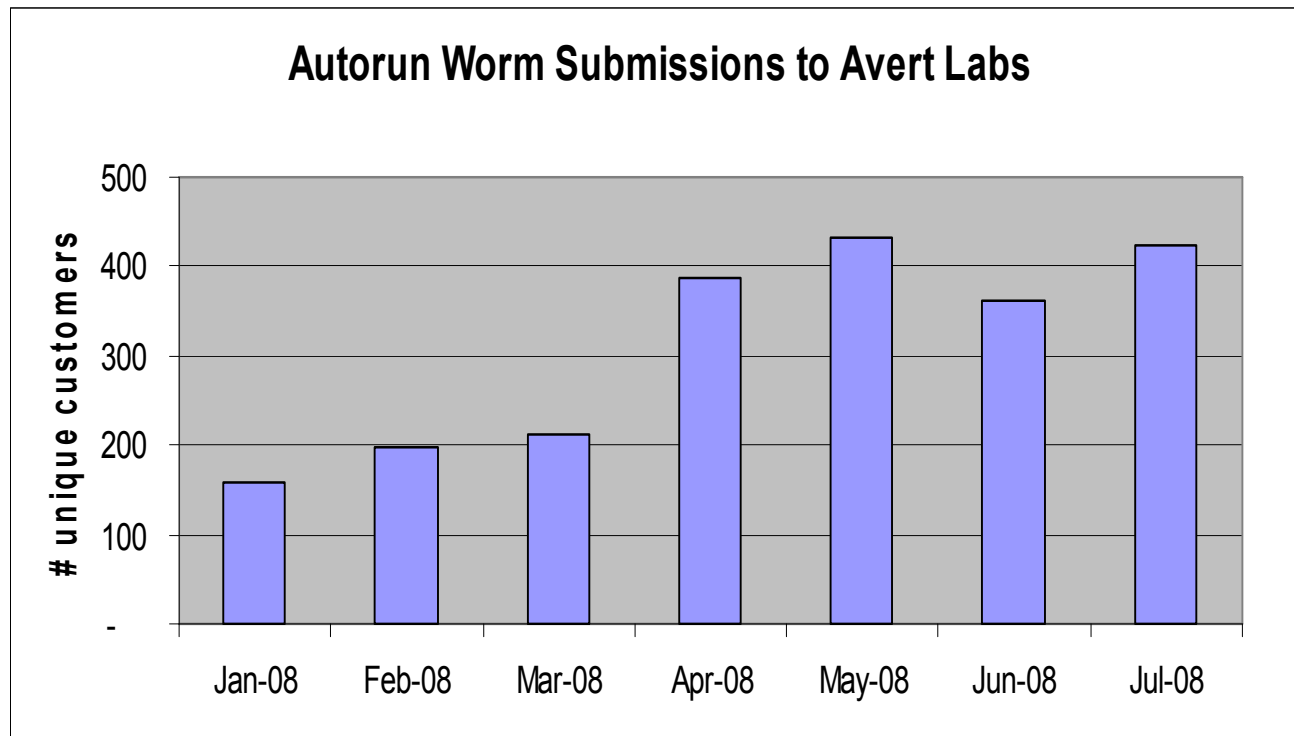
**McAfee**

23 MAY 2008



Protect what you value.

# Valuable data is everywhere



- Flash Ram

- Cameras
- MP3 players
- Cell phones
- Digital picture frames
- ???

**McAfee**

23 MAY 2008



Protect what you value.



**symantec**<sup>™</sup>

Confidence in a connected world.

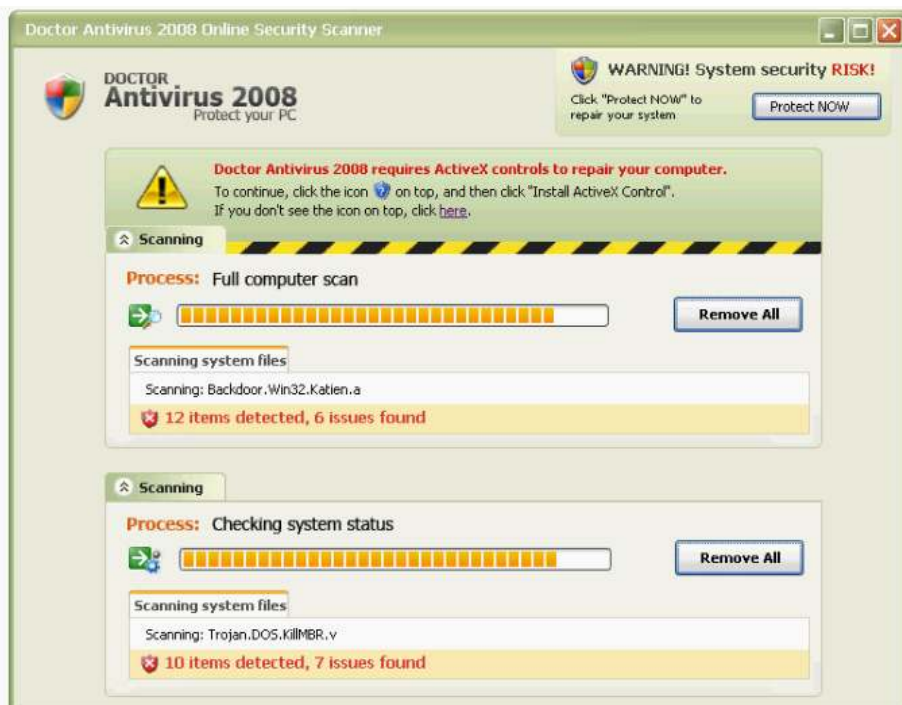
# Leveraging IPS technology for better protection

Jim Waggoner, CISSP

Sr. Principal Product Manager

September 16, 2008

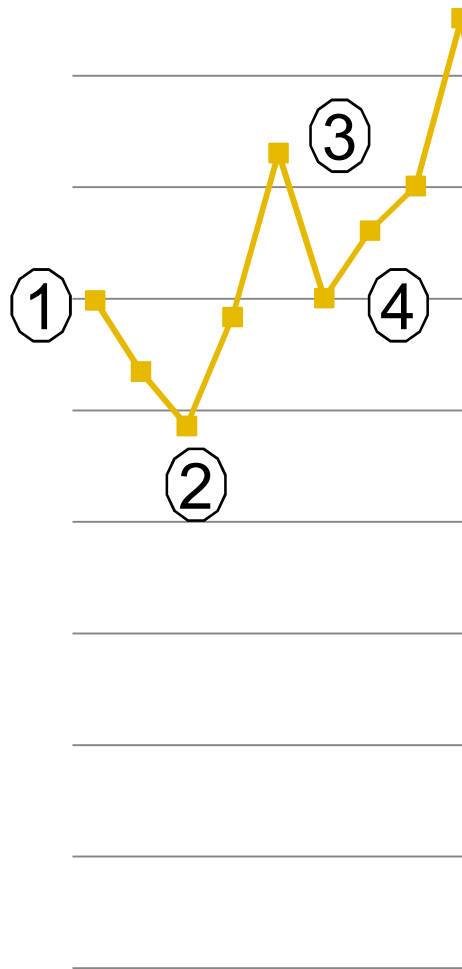
# Misleading Application



This won't protect your system, it will infect your system

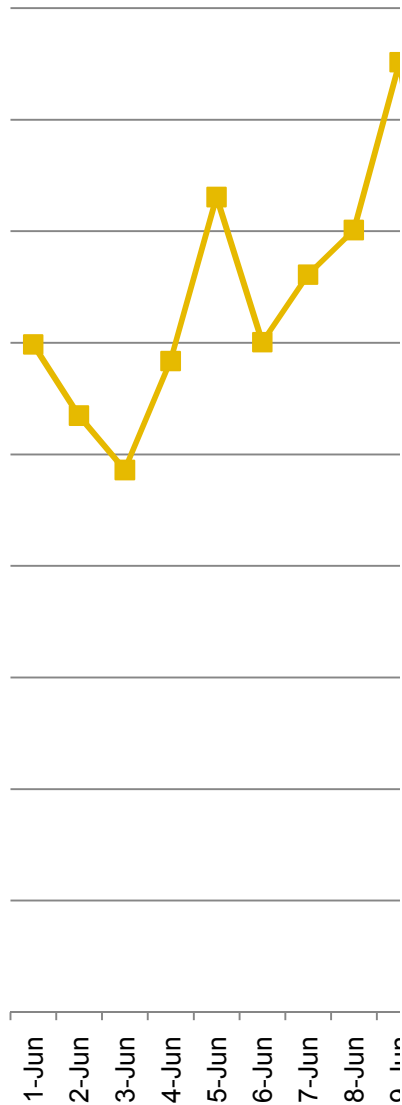
- Misleading application (or rogue antispyware) is a large source of malware for customers
- Zlob and Vundo are consistently among top reported malicious files
  - Users fooled into download through social engineering
  - Variants weekly, sometime daily to avoid AV detection
- Monitoring detections in the field gives us insight into when variants are released

# Cat and Mouse



1. New variant released, SEP detections go down
2. Symantec updates signature to catch new variant, detections go up
3. Miscreants release new variant, SEP detections goes down
4. New signature released, SEP detections go up

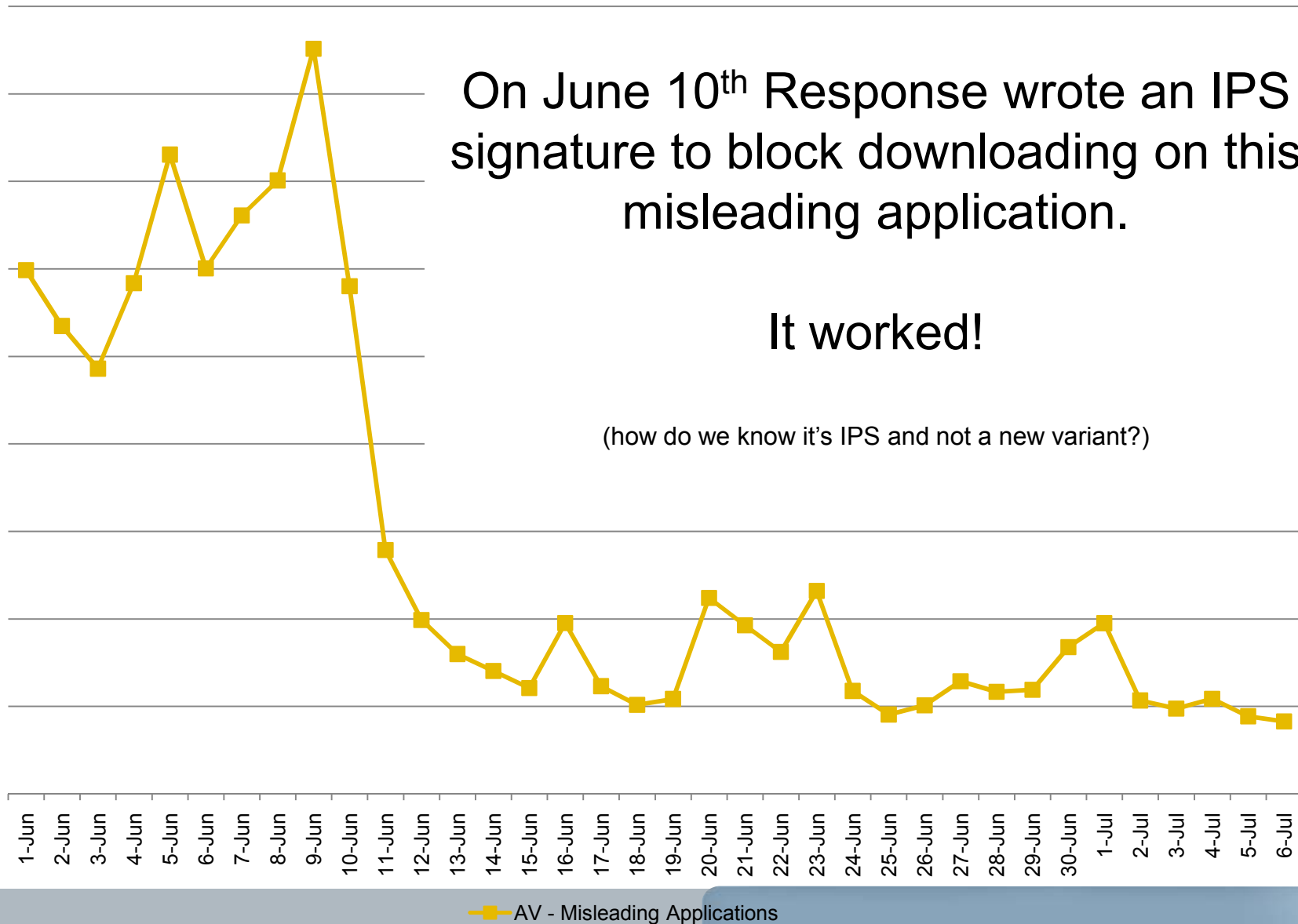
And on and on

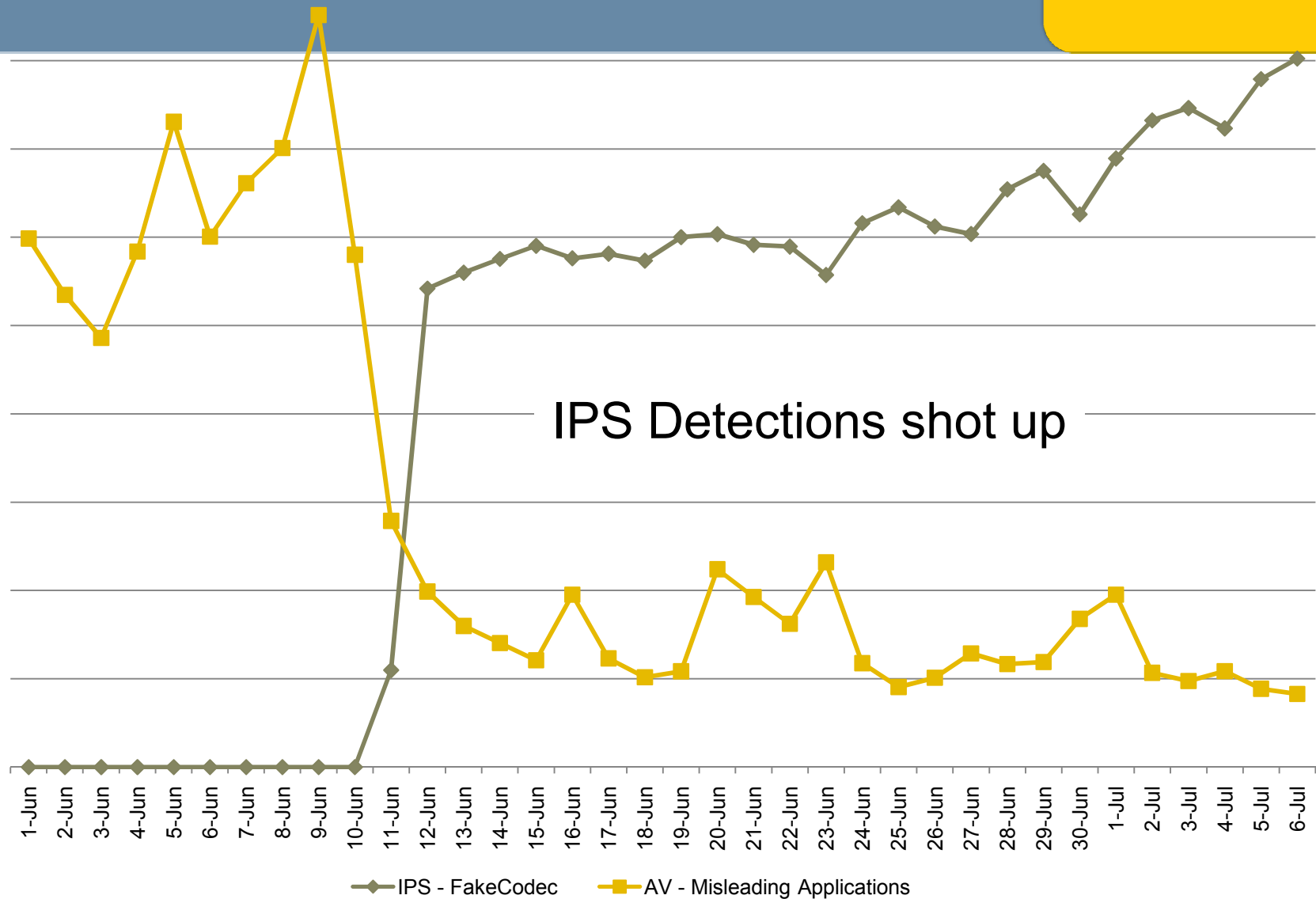


This happened within a 10 day period in June

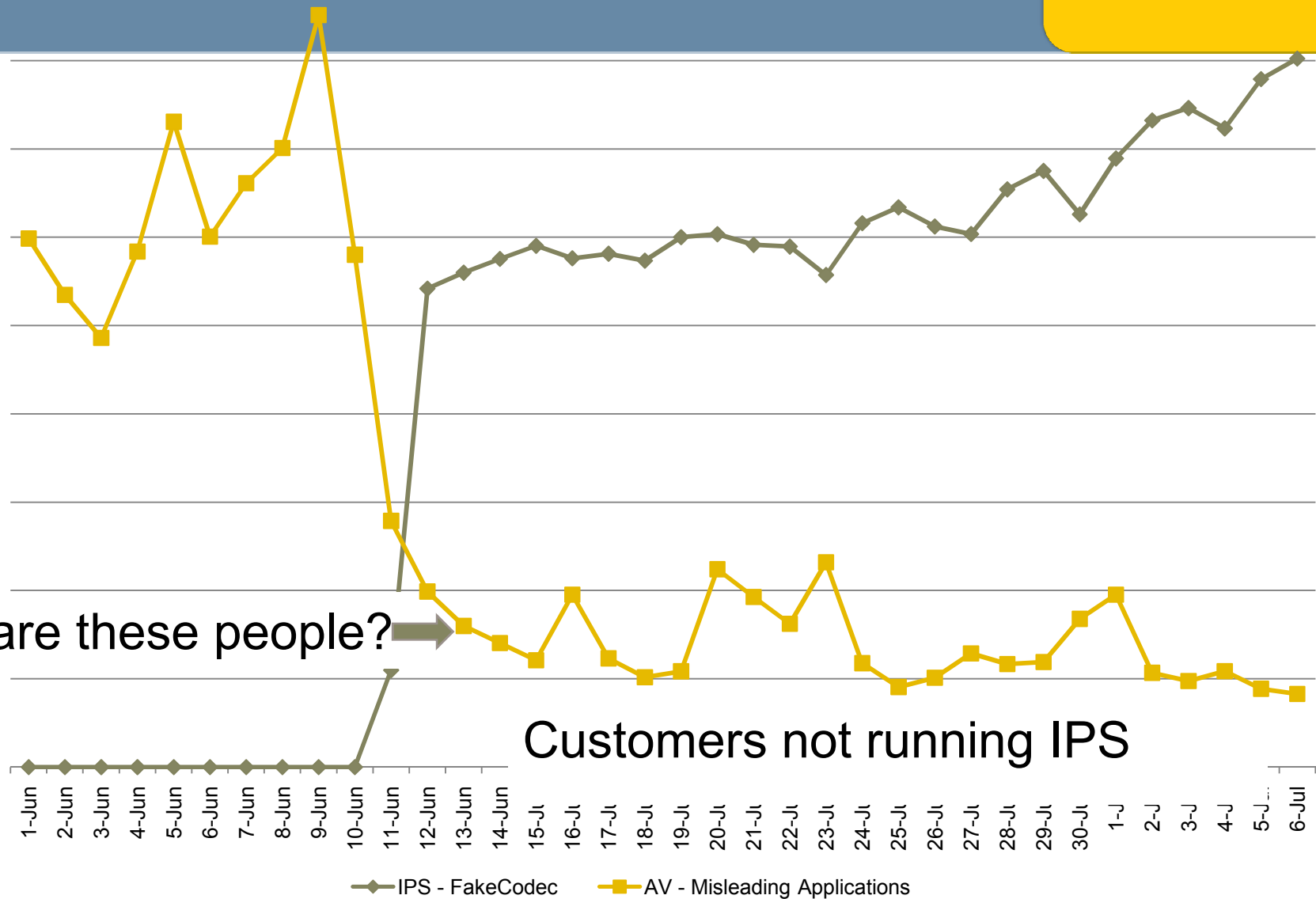
3 variants, 3 signatures

So we tried something different





Who are these people? →



Customers not running IPS



## **What About the Endpoint?**

**Mark Harris – Global Director SophosLabs**

## Endpoint is Under Attack!

- Huge growth in threats
- 20,000 new samples per day
- Thousands of vulnerabilities
- In Hundreds of applications  
(Not just Windows)



## Reduce Attack Surface - Gateway

- 90% of email is spam
- 1 in 900 web requests are to spam web sites
- 12% of people 'admit' to purchasing goods via spam
- 1 in 2000 emails have infected attachments
- Move towards links to email (Storm / Dorf etc)



## Reduce Attack Surface - Web

- 1 new infected webpage every 5 seconds
- 1 in every 1600 page requests are to infected website
- 90% of websites are compromised
- Not just about 'Productivity Filtering'



## Application Control & Potentially Unwanted Apps

- Over 86% of administrators want to be able to block
  - Instant Messaging
  - P2P Apps
  - VOIP
- Ability to manage and control
  - Hacking tools
  - BHO's
  - Remote admin tools, etc



## Network Access Control

Recent Sophos Endpoint Assessment Test

- 63% missing at least one Microsoft security patch
- 5% Had no Anti Virus active
- 50% No firewall enabled
- 81% Non-compliant



## Device Control & Data Leakage Prevention

- Growing trend of 'usb key' malware
- Growth in mobile data devices
- Concern over data leakage and compliance
- Need to manage devices
- And what can be copied to them
- Protect data with encryption



## Run Time Behavior Analysis

- Monitoring 'Suspicious' behaviour
  - Install apps
  - Copying itself
  - Hooking processes etc



## “Traditional” Anti Virus

- Pre emptive behaviour analysis
  - Content – Packed \ Encrypted
  - Behavior – Registry access
  - Reputation – compare with known ‘good’ applications
- Generic Detection
- Fast response time
- High Quality detection



## The Sophos vision



•Better security through control

•Integrated, simplified and automated

•Unified security and PC management

**McAfee**



Protect what you value.