TREND MICRO | Securing Your Web World

Stallion

Turvaliselt on hea!

Protecting Virtual Environments

Trend Micro Deep Security

Märt Erik, security engineer, Stallion

Simon Wikberg, senior pre- sales engineer, Trend Micro

Urmas Püss, sales consultant, Stallion

27.05.2011

Agenda

- Threats overview
- Smart Protection Network
- Deep Security
- Economic benefit - TCO & ROI


Threats overview

Threat Trends 2010

The Year of the Toolkit

- 2010 was distinguished by the full and proper emergence of toolkits as a means to perpetrate cybercrime
- Poisoning search engine results - Blackhat search engine optimization- BH SEO
  - XRumer or uMaxSoft Doorway Generator.
- Compromising sites
- Exploiting systems
  - Eleonore or Phoenix
- Malware itself
  - FakeAV or a banking trojan.
  - Zeus, SpyEye or Ares
- Social networks

Threat Trends 2010

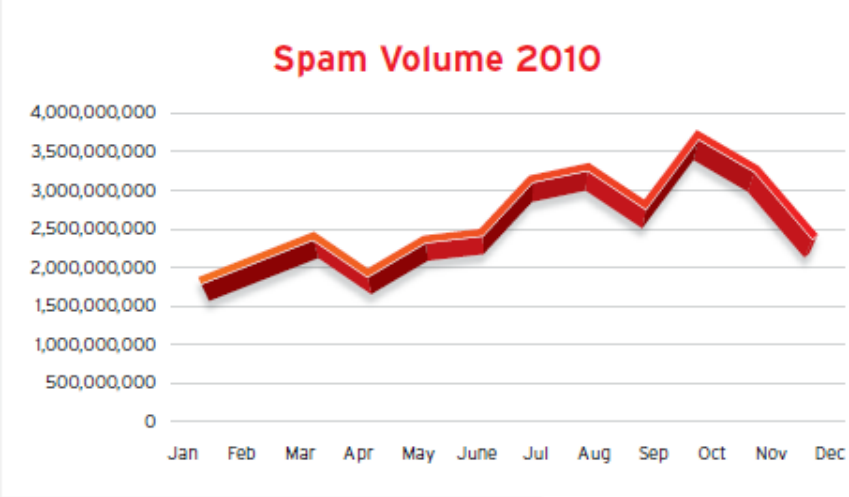
The Year of the Toolkit

„It's hard to underestimate the impact that toolkits have on online criminal activity. There used to be something of a barrier to entry, as technical knowledge and expertise were both necessary to enter the world of cybercrime. Today, with cybercrime toolkits in full production, very little, if any, technical knowhow is needed to profit“

Threat Trends 2010

Spam Trends

- Spam volume continued to rise when viewed on a year over year basis.
- Phishing email gradually started to target not only banks but also popular social networking sites like Facebook, Twitter, MySpace.
- Fewer global outbreaks, instead localized and targeted attacks.



TREND MICRO

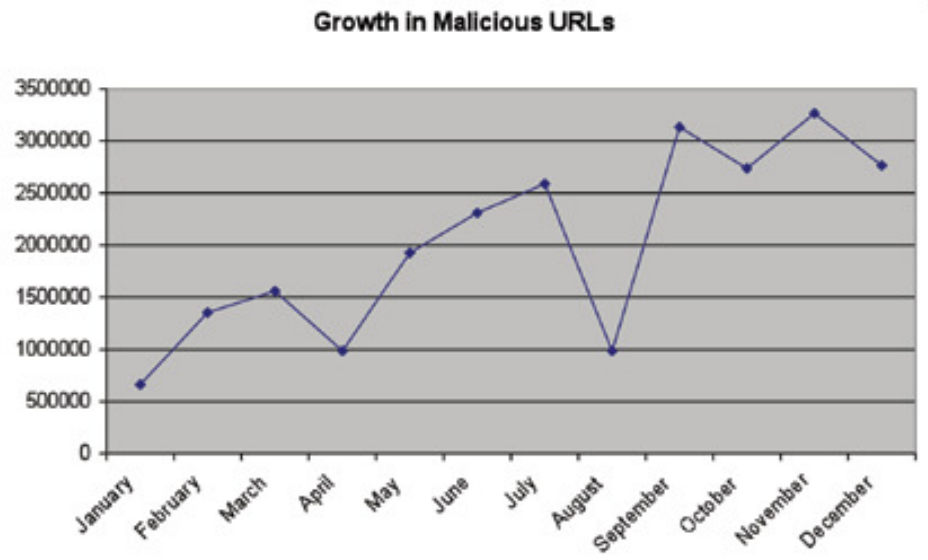
stallion

Threat Trends 2010

Web- Based Threats

- Web has become the preferred choice by which cybercriminals reach their victims

- Notable Site Compromises
  - Lenovo support page
  - Several Blogger pages
  - Several WordPress blogs
  - Social Networking sites



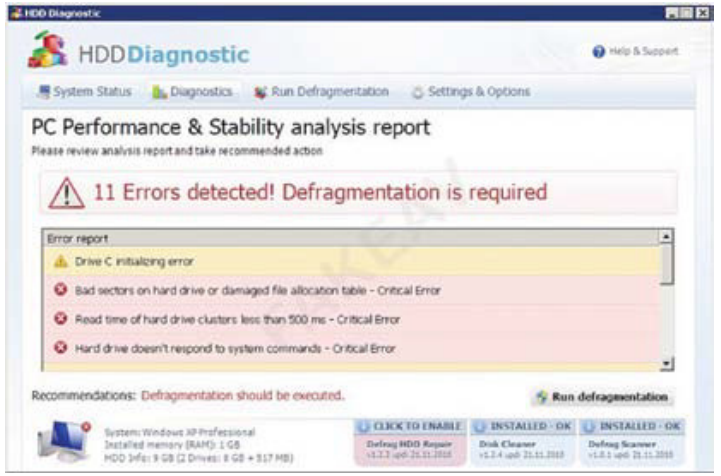
TREND MICRO

stallion

Threat Trends 2010

File- Based Threats

- DOWNAD (aka Conficker) continued to be the most prevalent malware.
- Most affected sectors were education and government.
- STUXNET attacks SCADA systems
- Zeus Development
- FakeAV and fake utility malware



TREND MICRO

Stallion

Threat Trends 2010

Vulnerability Landscape

- The number of vulnerabilities went down but popular applications and OSs were still affected.
- Windows, IE, Java, Adobe Acrobat, Adobe Reader, and Adobe Flash Player were all hit by new vulnerabilities throughout 2010.
- Total of 4651 vulnerabilities were assigned designations in the CVE database.

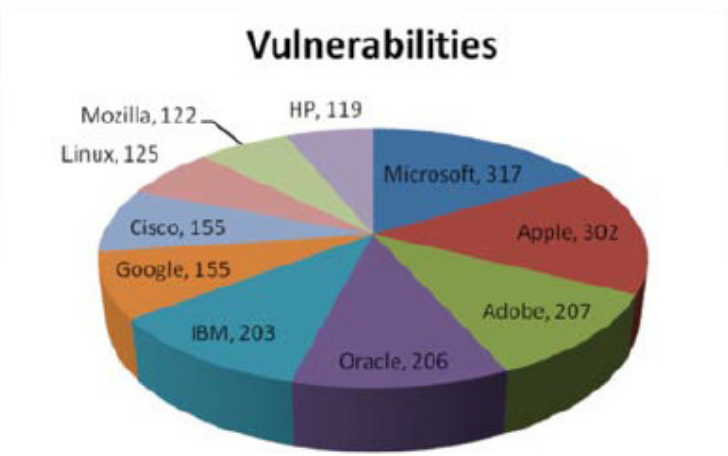
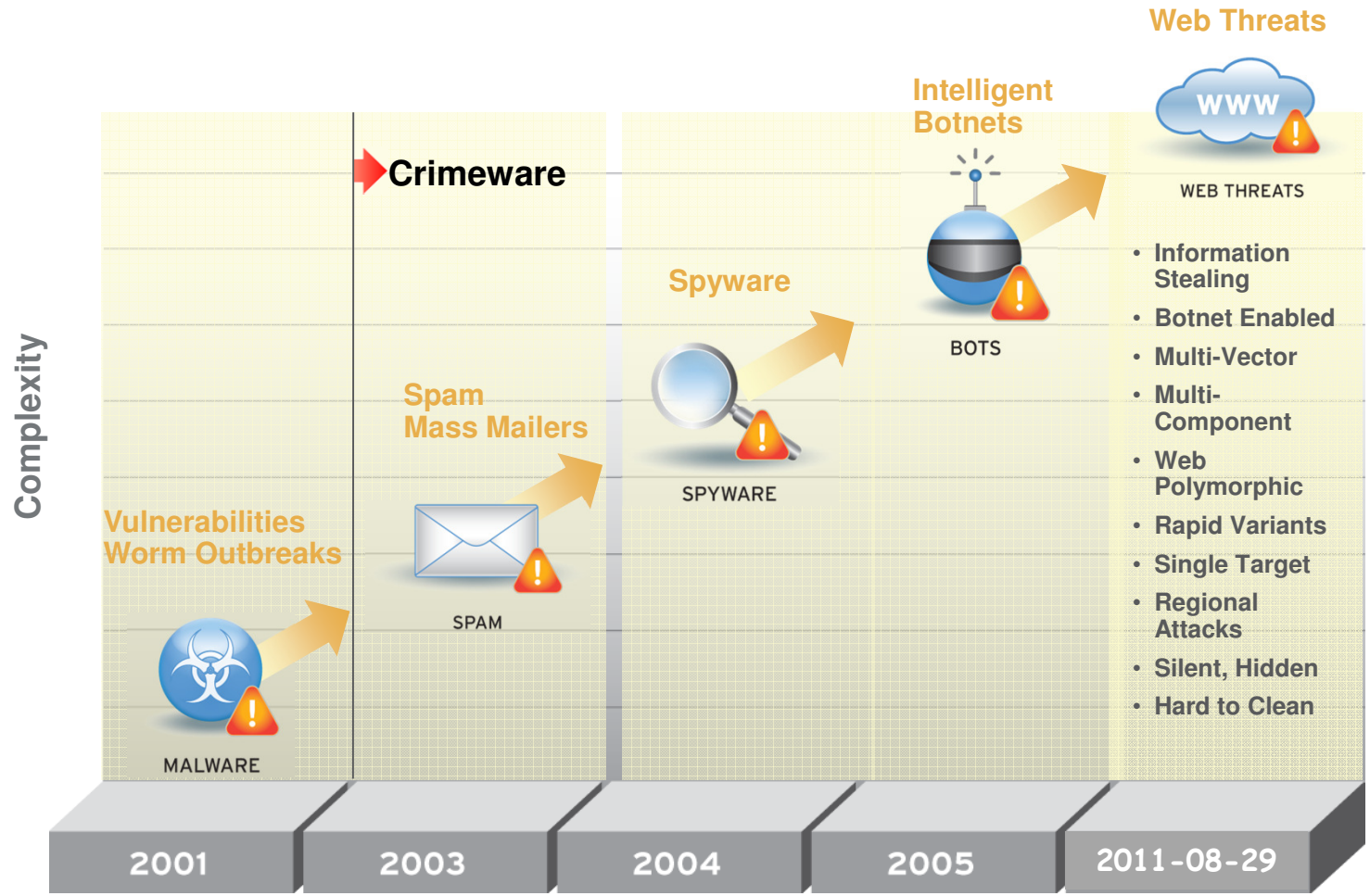


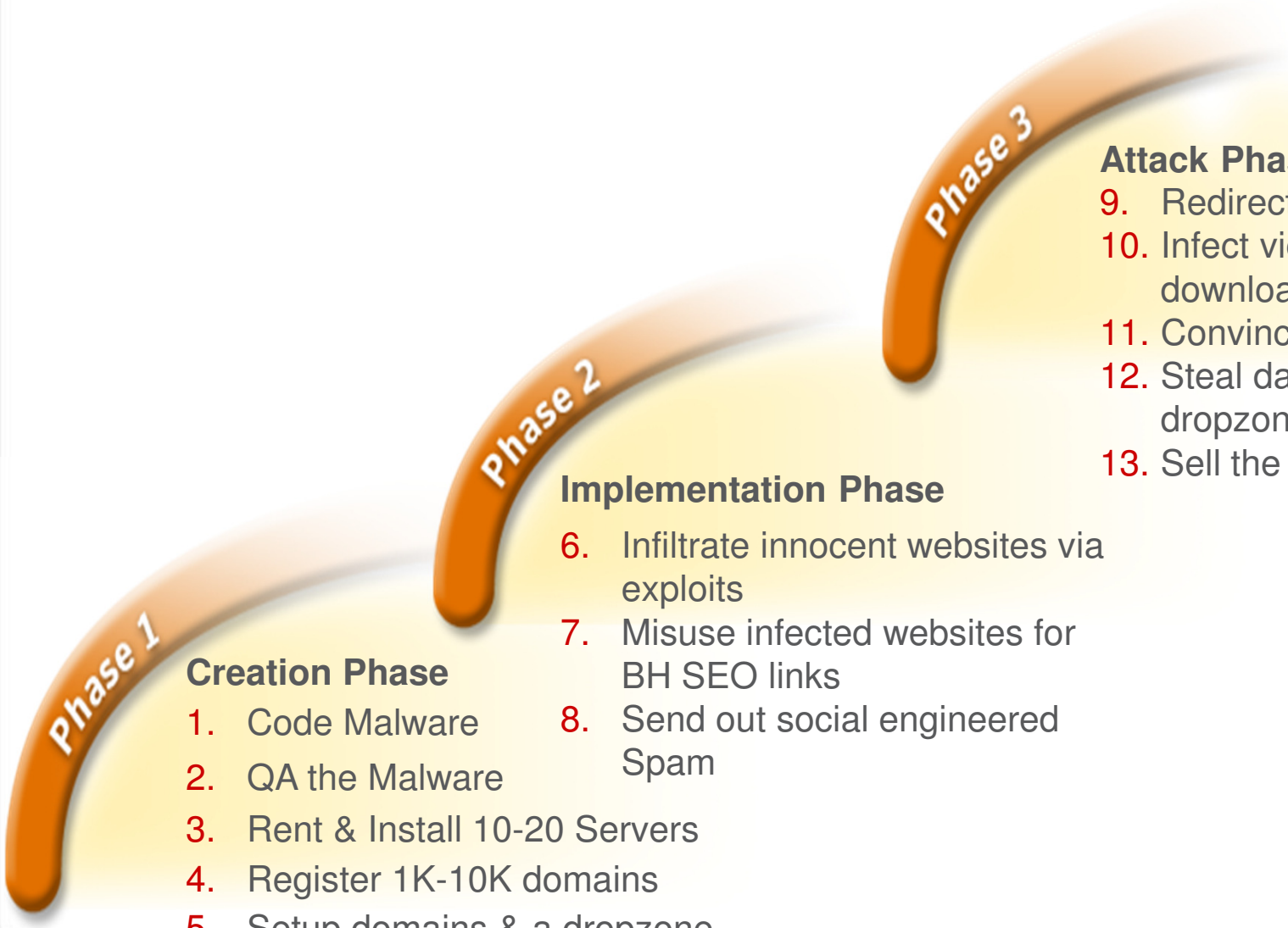
Figure 25. Top 10 vendors in terms of CVEs issued

Malware development



Enemy

A Typical Cyber Crime Process



Creation Phase

1. Code Malware
2. QA the Malware
3. Rent & Install 10-20 Servers
4. Register 1K-10K domains
5. Setup domains & a dropzone

Implementation Phase

6. Infiltrate innocent websites via exploits
7. Misuse infected websites for BH SEO links
8. Send out social engineered Spam

Attack Phase

9. Redirect Google victims
10. Infect victim via drive-by download
11. Convince users to click
12. Steal data & transfer to dropzone
13. Sell the data

In a Professional World

Creation Phase

1. Code Malware → **Toolkits, Encryption, Different per month**
2. QA the Malware → **VirusTotal like services**
3. Rent & Install 10-20 Servers → **Bulletproof Hosters, Images, preconfigured, lasts 5 min**
4. Register 1K-10K domains → **Free or extremely cheap hosters, many hundred domains on one server**
5. Setup domains & a dropzone → **Can be a hacked personal homepage**

In a Professional World

Phase 2

Implementation Phase

6. Infiltrate innocent websites → **Find servers that are vulnerable, execute script to exploit (can infect 1K's of sites simultaneously) with single keystroke**

7. Misuse infected websites → **Use obfuscated scripts to dynamically reference any site hacker wants to promote (BHSEO)**

8. Use Spam campaigns → **Clever social engineering convinces users to download a Video Codec or to read the latest news**

In a Professional World

Attack Phase

9. Redirect Google victims → **Compromised sites get promoted to top of search results**
10. Infect victim via drive-by download → **Up to 10k victims per day**
11. Victims download and executes → **Users are easy to convince**
12. Steal data & transfer to dropzone → **Undetected up to 3 years**
13. Sell the data → **Charge pennies to thousands for stolen data within underground communities**

Selling Stolen Data?

It‘s more than just bank & credit card data

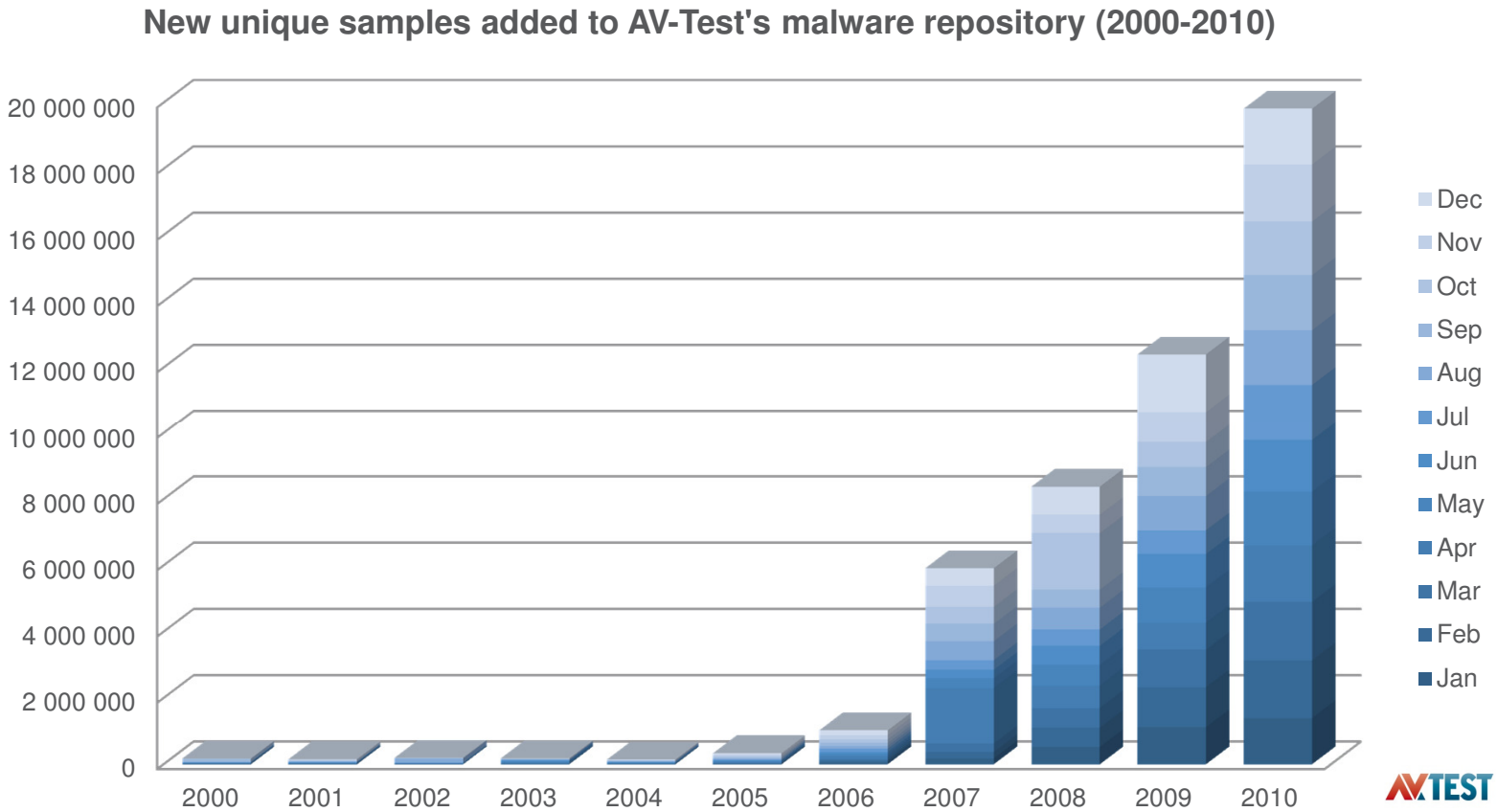
- Creditcard data
- Online Banking Accounts
- Email accounts
- Social network accounts (FB, Flickr, Twitter, …)
- Commercial accounts (Amazon, Ebay, …)
- Data found on your hard disk like copies of your passport
- Space on your hard disk (used to store child pornografic stuff)
- Your network bandwith (DDoS)

Underground Economy

ASSET	SELLS FOR
Passport/utility bill/statement (scanned document)	$20
Credit card (front and back) (as a scanned document)	$25 - $30
Drivers License (scanned document)	$20
Utility bill (scanned document)	$10
Various original docs (scanned document)	From $4
US credit cards: USA /Master Card / VISA	$1 each
Credit cards: Denmark, Greece, Ireland (Eire), Latvia, Netherlands, Norway, Sweden, Canada	$3 per card
Card information "input service"	$5
Hacked PayPal accounts	30% of the current balance on the PayPal Account


Smart Protection Network

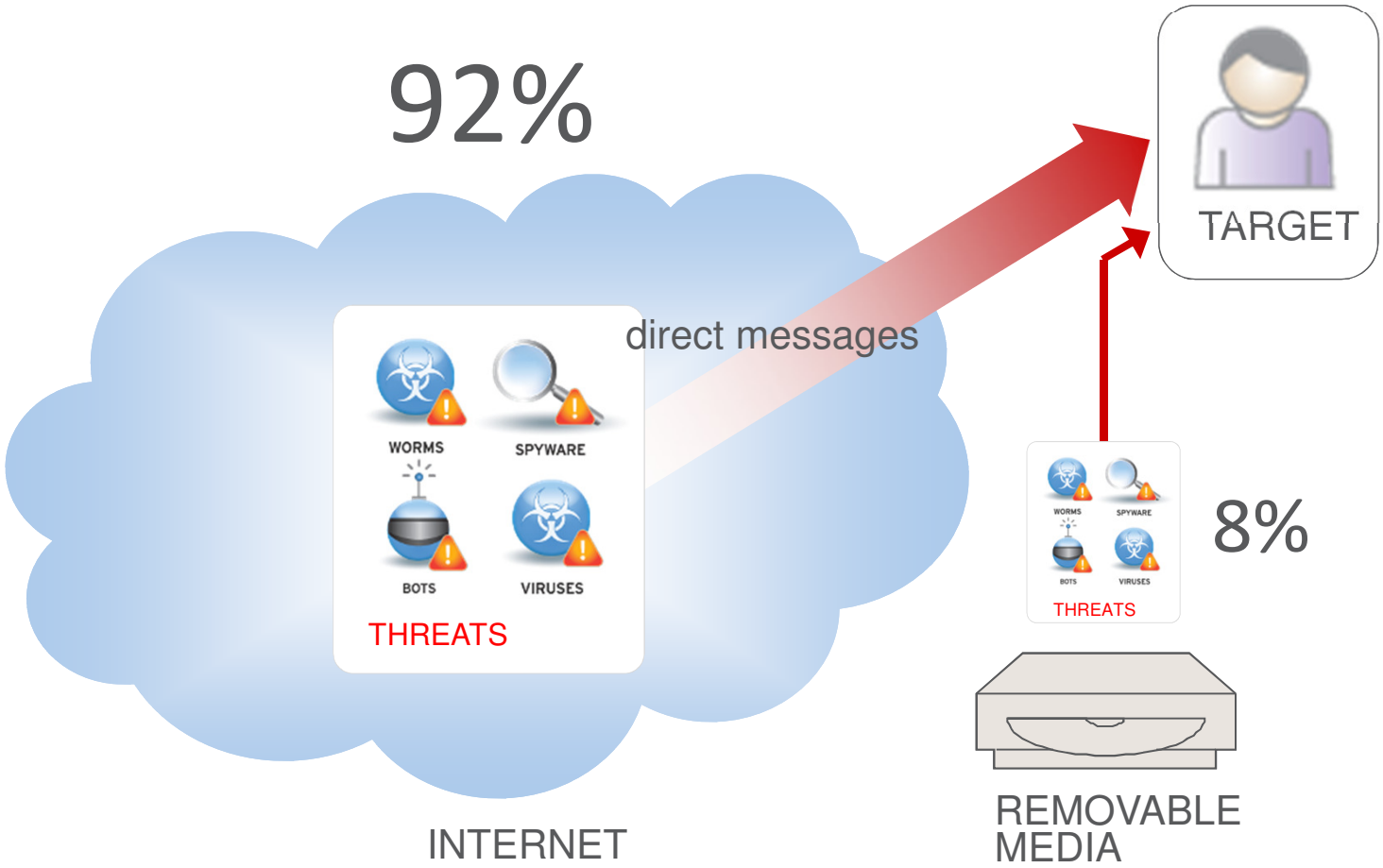
Malware is on a rise



TREND MICRO

stallion

The way in...


92%
TARGET
direct messages
WORMS
SPYWARE
BOTS
VIRUSES
THREATS
8%
THREATS
REMOVABLE MEDIA
INTERNET

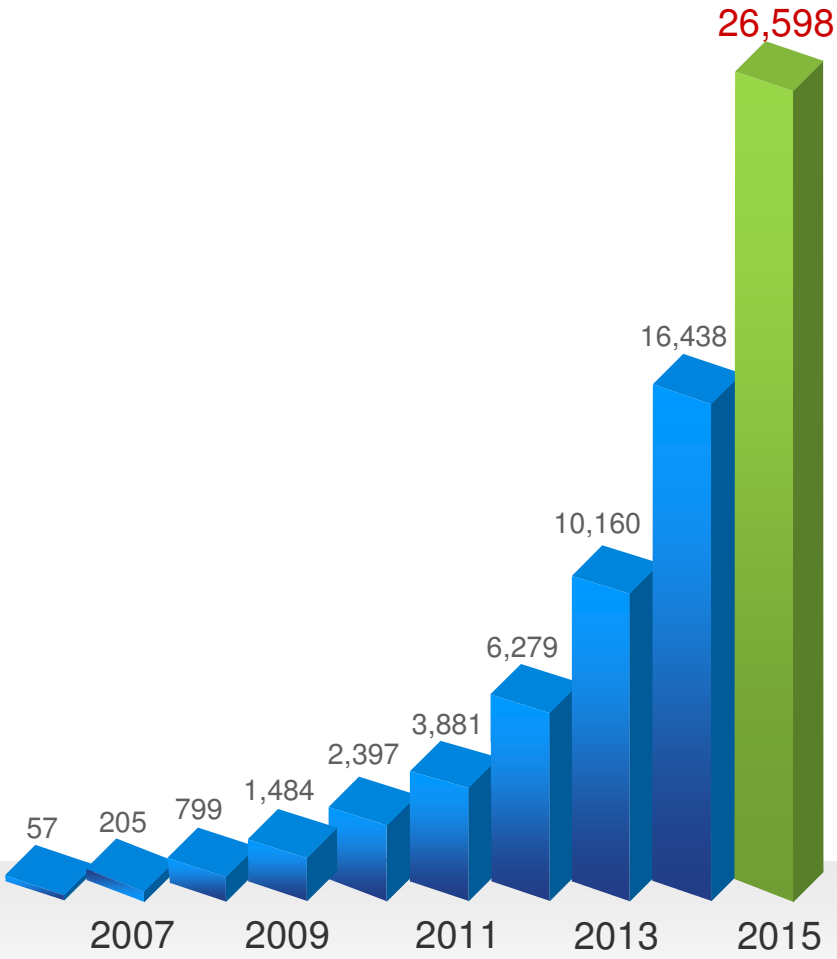
Traditional security

Signature file growing

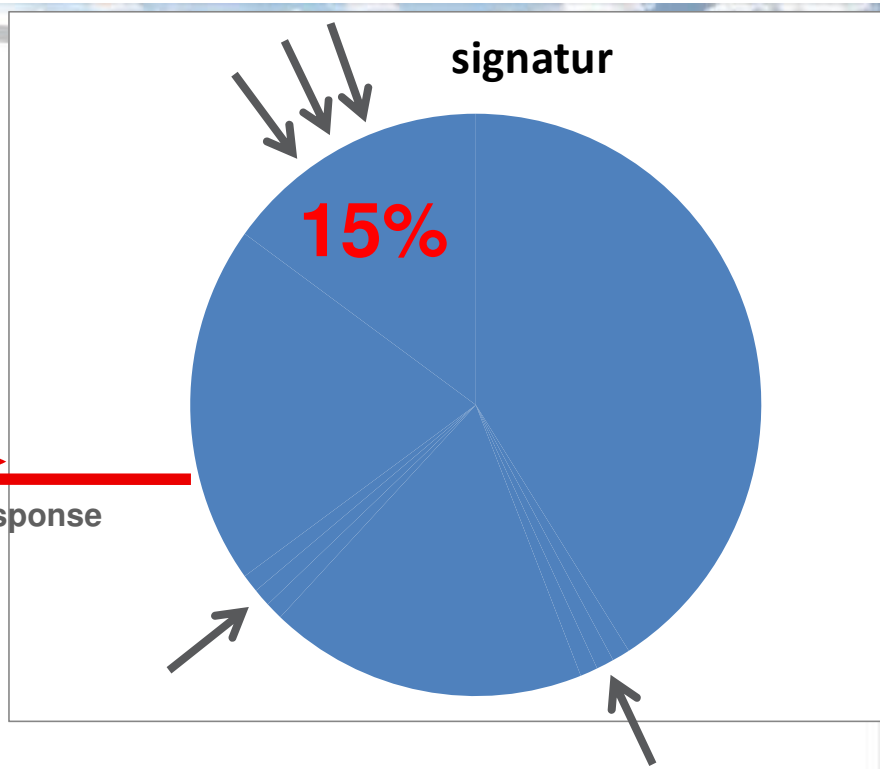
- Need for more memory
- Decreased performance
- More bandwidth
- Unpredictable growth

Signature updates too slow

- Critical vulnerabilities
- Long Time To Protect

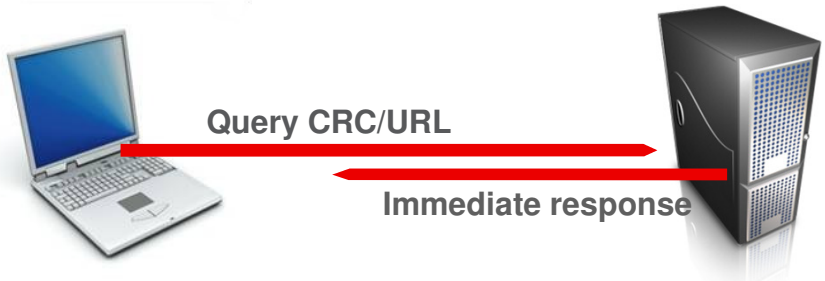


Smart Protection Network



mediate response

=



Local Smart Protection
Network Server

01100100001100100101101011010101
01100110000110010010110101101010

Smart Protection Network

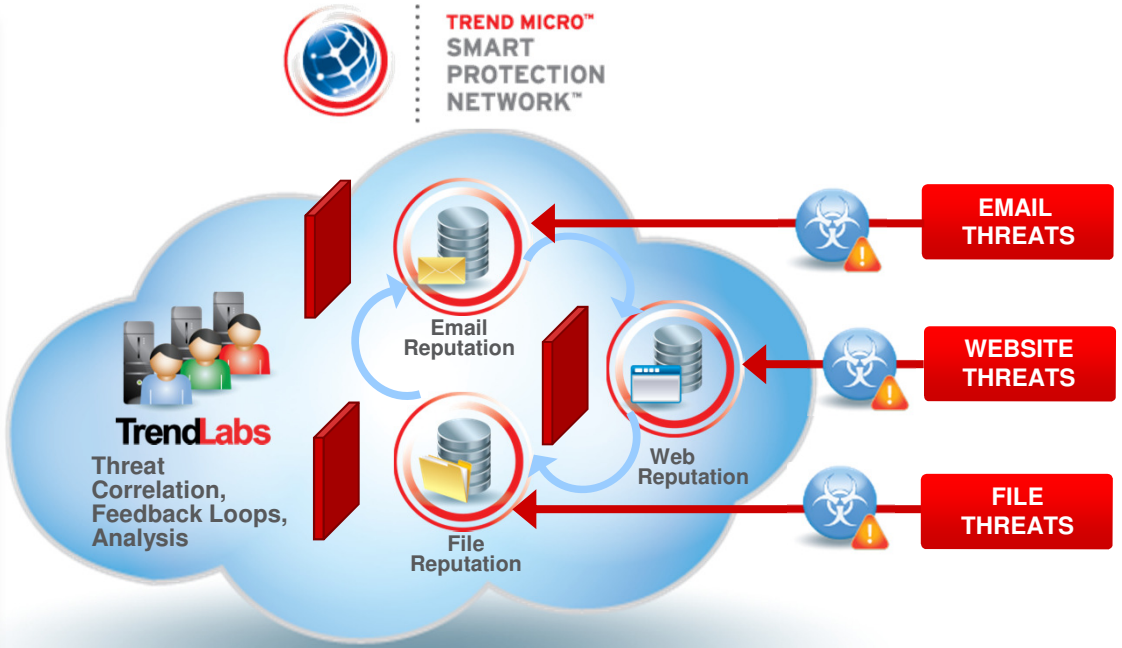
Innovative Cloud-Client Infrastructure

The Smart Protection Network Difference

- 4-year R&D investment
- Powers Trend Micro Enterprise Security
- Web, file, email reputation
- Enterprise, SMB, Consumer, Partner product integration
- 45 billion queries daily
- 5 billion threats blocked daily
- Automated Smart Feedback
- **#1** in **NSS Labs** Rankings
- All data collected, analyzed, *cross-correlated* to provide the best, real-time protection
- Most efficient signature mgt and endpoint footprint

" The Smart Protection Network demonstrates great vision and leadership"

— Jon Oltsik, Senior Analyst, ESG

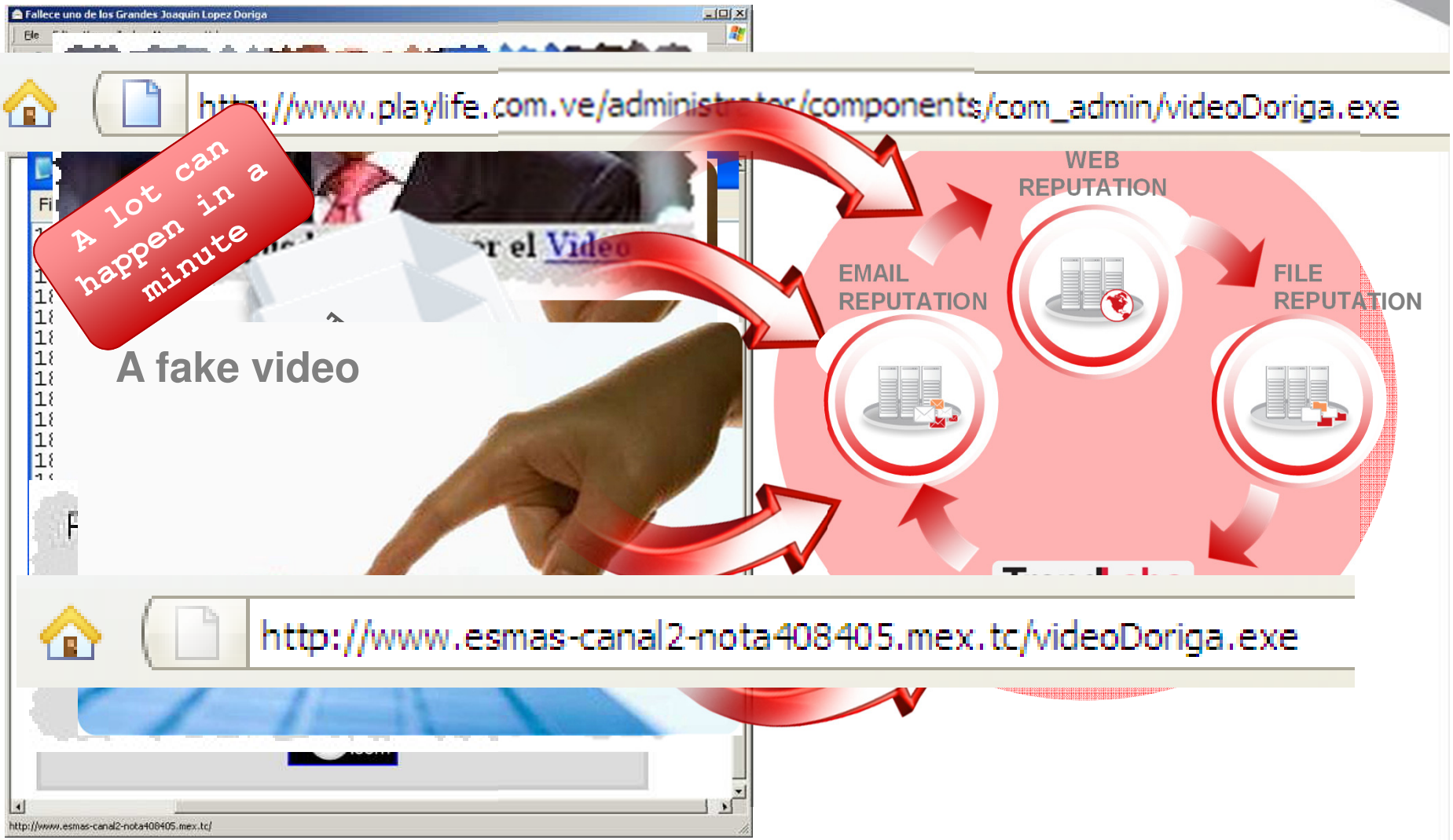


Real-time threat sourcing, analysis and protection deployment

TREND MICRO

stallion

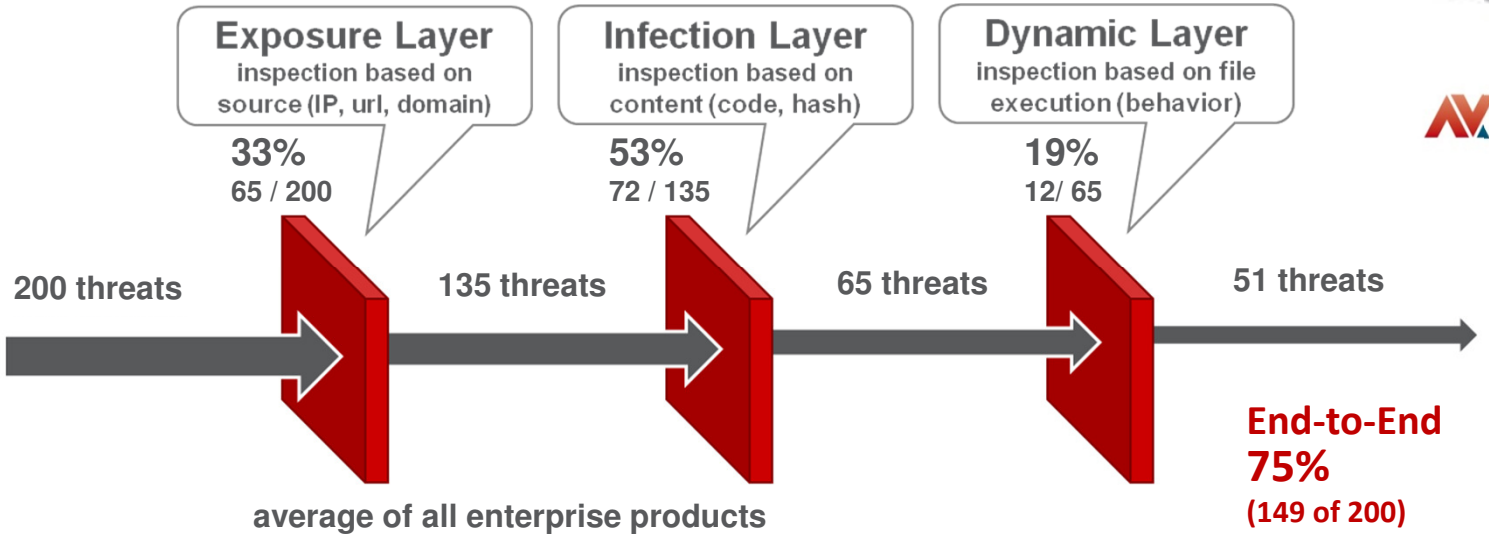
Smart Protection Network Correlation



TREND MICRO

stallion

Individual Layer Results

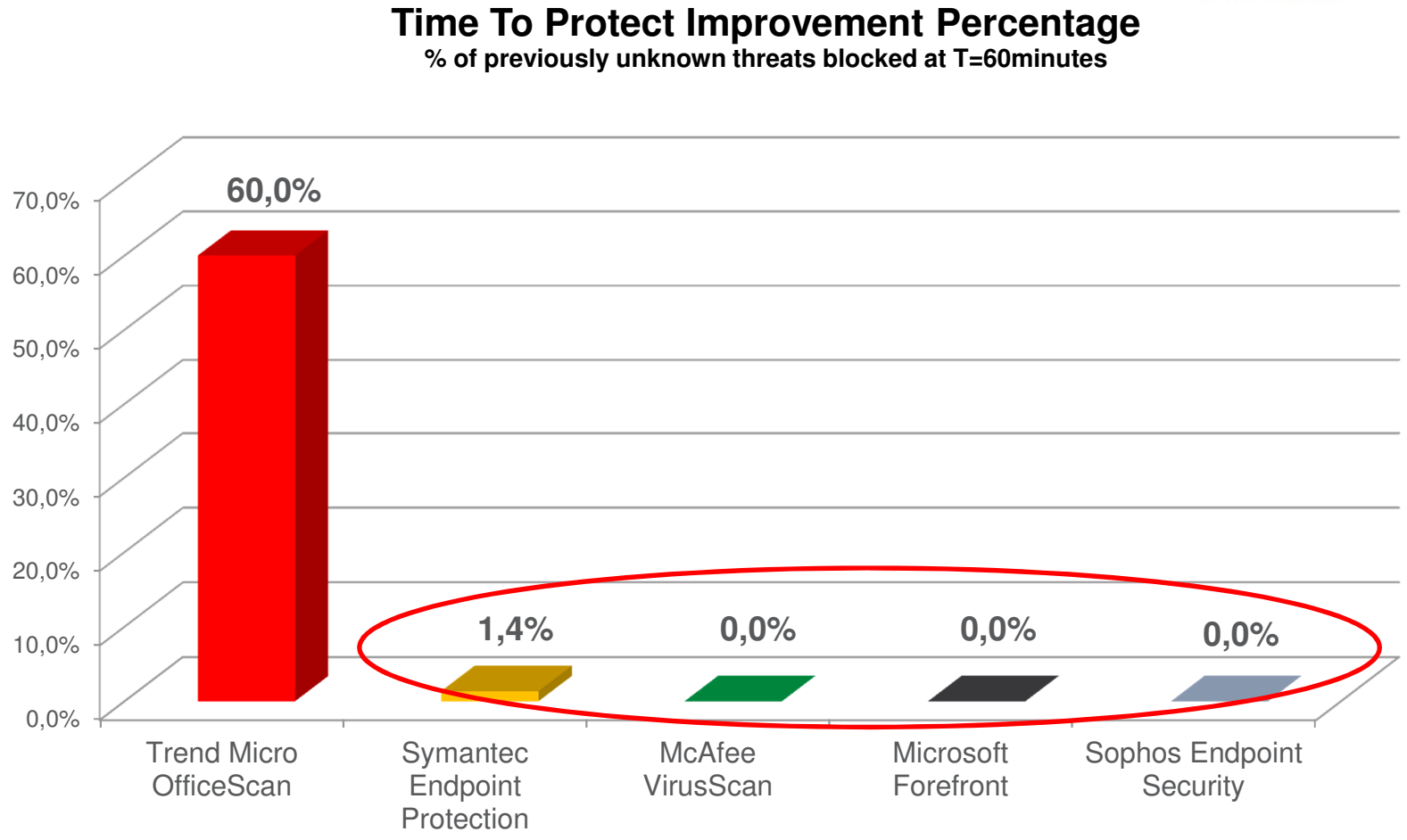


Threats prevented at each layer (of total threats that reached that layer)

	Trend Micro	Microsoft	Sophos	McAfee	Symantec
Exposure Layer	97% (194 of 200)	2% (3 of 200)	63% (126 of 200)	1% (2 of 200)	0% (0 of 200)
Infection Layer	67% (4 of 6)	68% (134 of 197)	19% (14 of 74)	50% (99 of 198)	54% (108 of 200)
Dynamic Layer	100% (2 of 2)	6% (4 of 63)	23% (14 of 60)	25% (25 of 99)	16% (15 of 92)
All Layers	100% (200 of 200)	71% (141 of 200)	77% (154 of 200)	63% (126 of 200)	62% (123 of 200)

Jan 2011 results of testing conducted by AV-Test.org (results from T+60 test)

AV-Test Oct 2010 Report – Time To Protect Results



Recent results of testing conducted by AV-Test.org (qualified for external use)

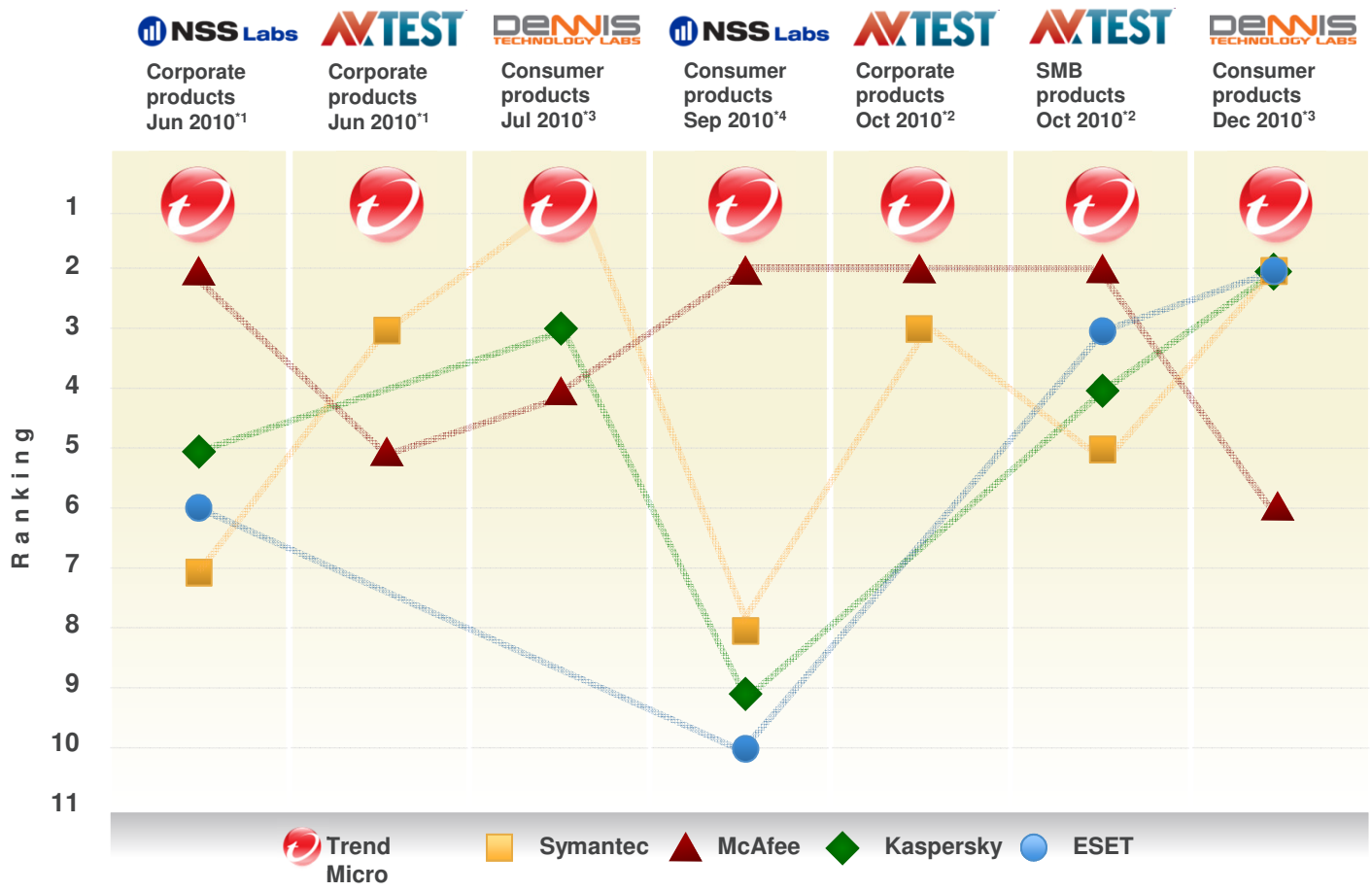
Security That Fits

Trend Micro's real-world protection validated by third-party test labs

3.5 NEW Threats Every Second

Blocking Billions of Threats Daily

#1 Real-world Online Testing



Note: If multiple products from one vendor were evaluated, then vendor's best performance is listed.

*1: http://www.trendmicro.co.jp/protection
*2: http://www.nsslabs.com/research/endpoint-security/anti-malware/q3-2009-endpoint-protection-group-test-report-socially-engineered-malware.html
*3: http://www.dennistechnologylabs.com/reports/s/a-m/trendmicro/PCVP2010-TM.pdf
*4: http://www.nsslabs.com/research/endpoint-security/anti-malware/consumer-anti-malware-products:-group-test-report-q3-2010.html

TREND MICRO

stallion

Threat Tracker

http://us.trendmicro.com/us/trendwatch/current-threat-activity/threat-tracker/index.html


Trend Micro Deep Security

Deep Security

Advanced security solution that provides protection for systems in the dynamic datacenter - from virtual desktops to physical, virtual or cloud servers.

Deep Security – 5 independent modules