TREND MICRO™ Securing Your Web World

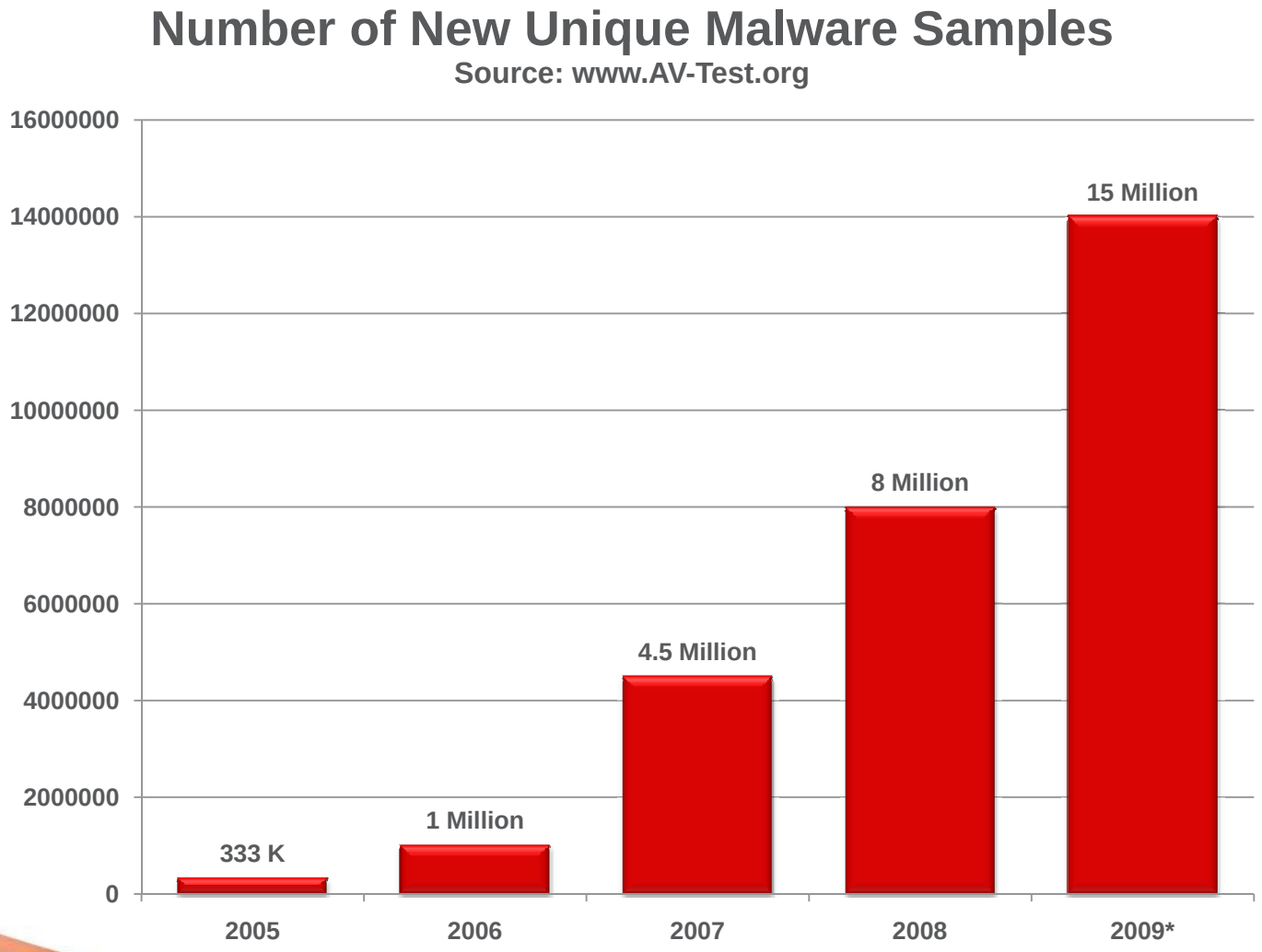
Volume of Threat:
The AV Update Deployment Bottleneck

Wei Yan • Anthony Arrott • Robert McArdle

vb 2009 GENEVA

 Copyright 2009 Trend Micro Inc.

Malware Volume Increase



Copyright 2009 Trend Micro Inc.

More Samples -> More Patterns

Increase in Malware Samples

Copyright 2009 Trend Micro Inc.

More Samples -> More Patterns

Increase in Malware Samples

Increase in Patterns

Copyright 2009 Trend Micro Inc.

More Samples -> More Patterns

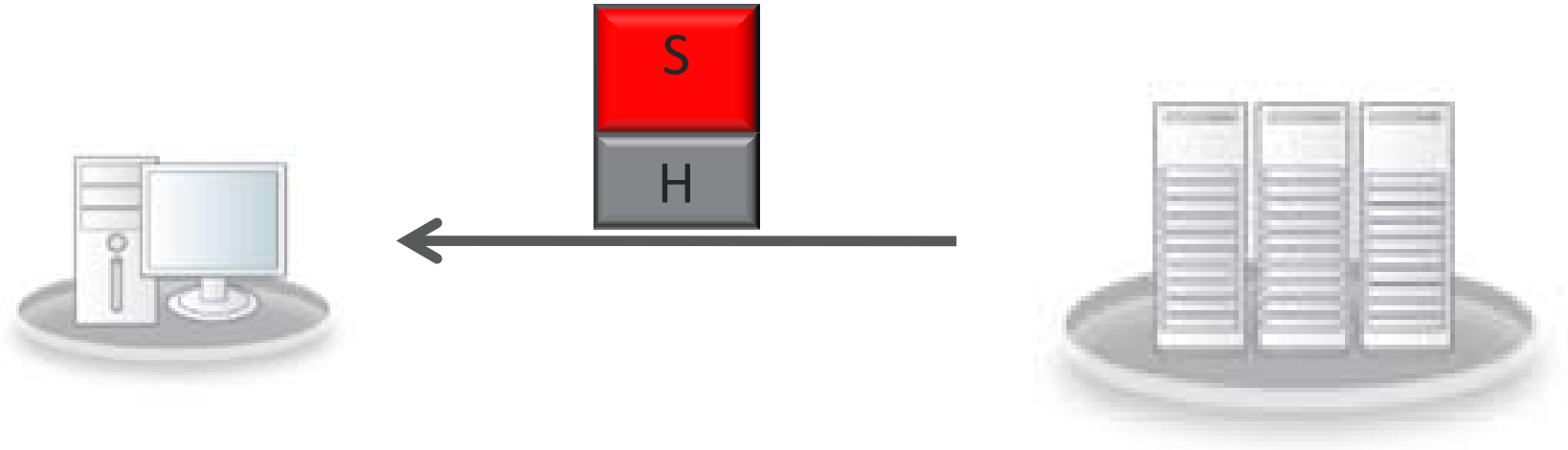
Increase in Malware Samples

Increase in Patterns

 Copyright 2009 Trend Micro Inc.

TREND MICRO

AV Updates (Now)

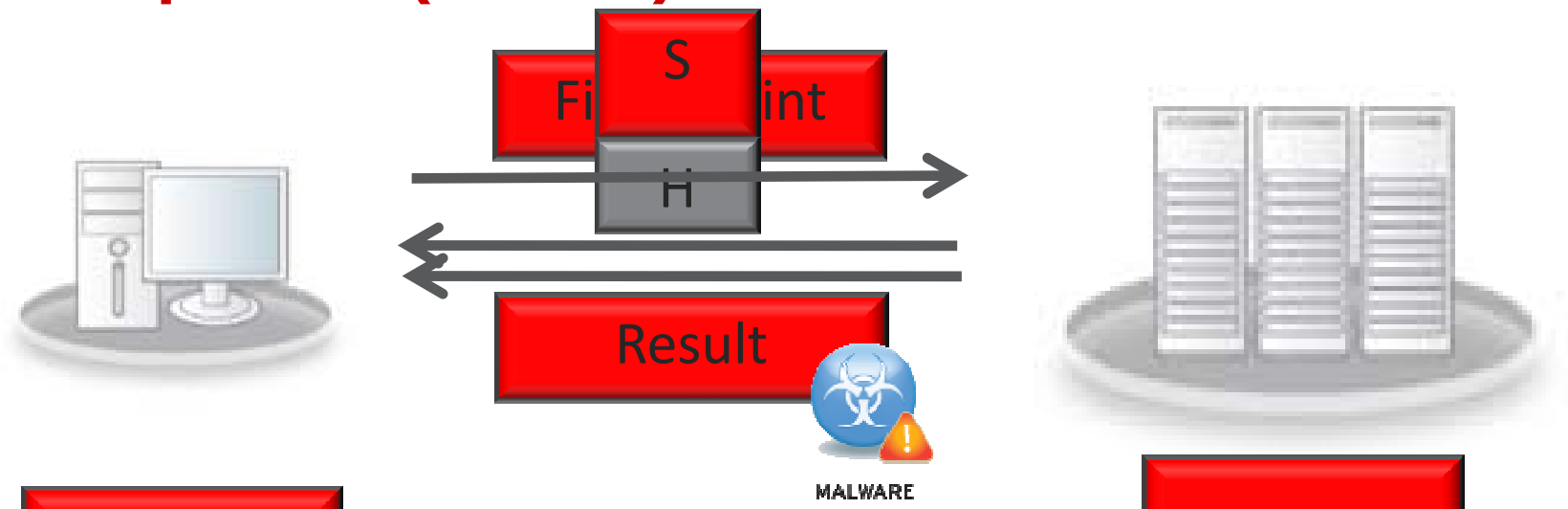


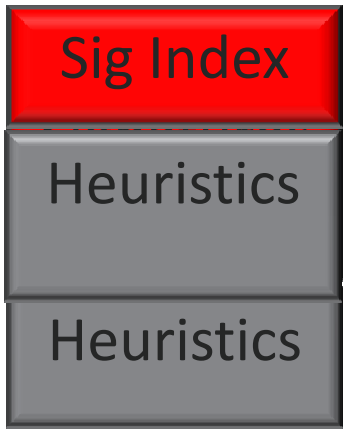
Static Signatures

Heuristics

Copyright 2009 Trend Micro Inc.

AV Updates (Future)





Copyright 2009 Trend Micro Inc.

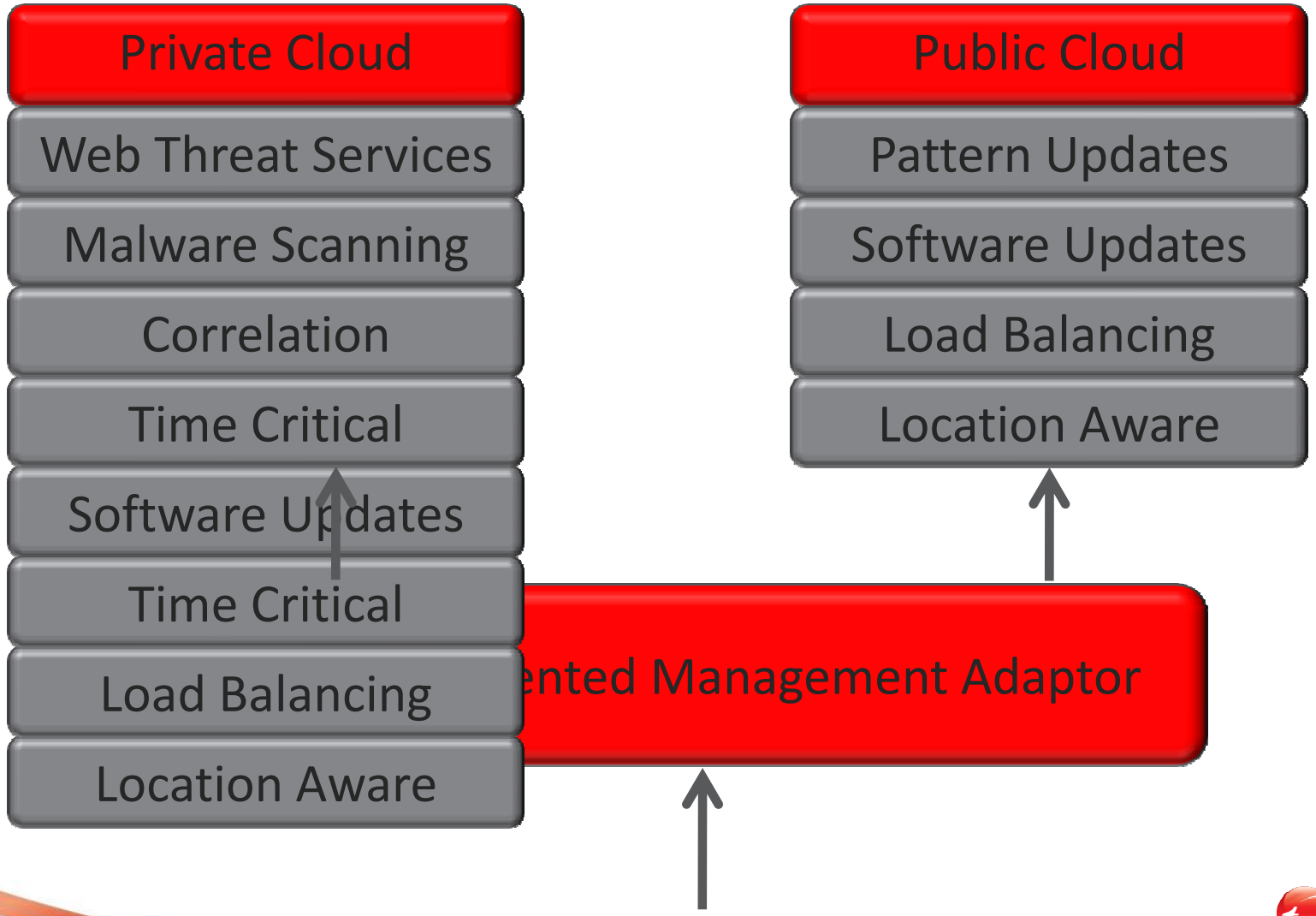
TREND MICRO

Cloud Architecture

Private Cloud	Public Cloud
• Complete Control • Clear control of QoS • Control Security Settings	• Limited API Access • Limited QoS based on SLA • Unclear Security Standards • Excellent Load Balancing & Location Awareness
• Time Critical Systems **• Continuous Communications**	**• Non-Time Critical Systems** **• Unpredictable Communications**

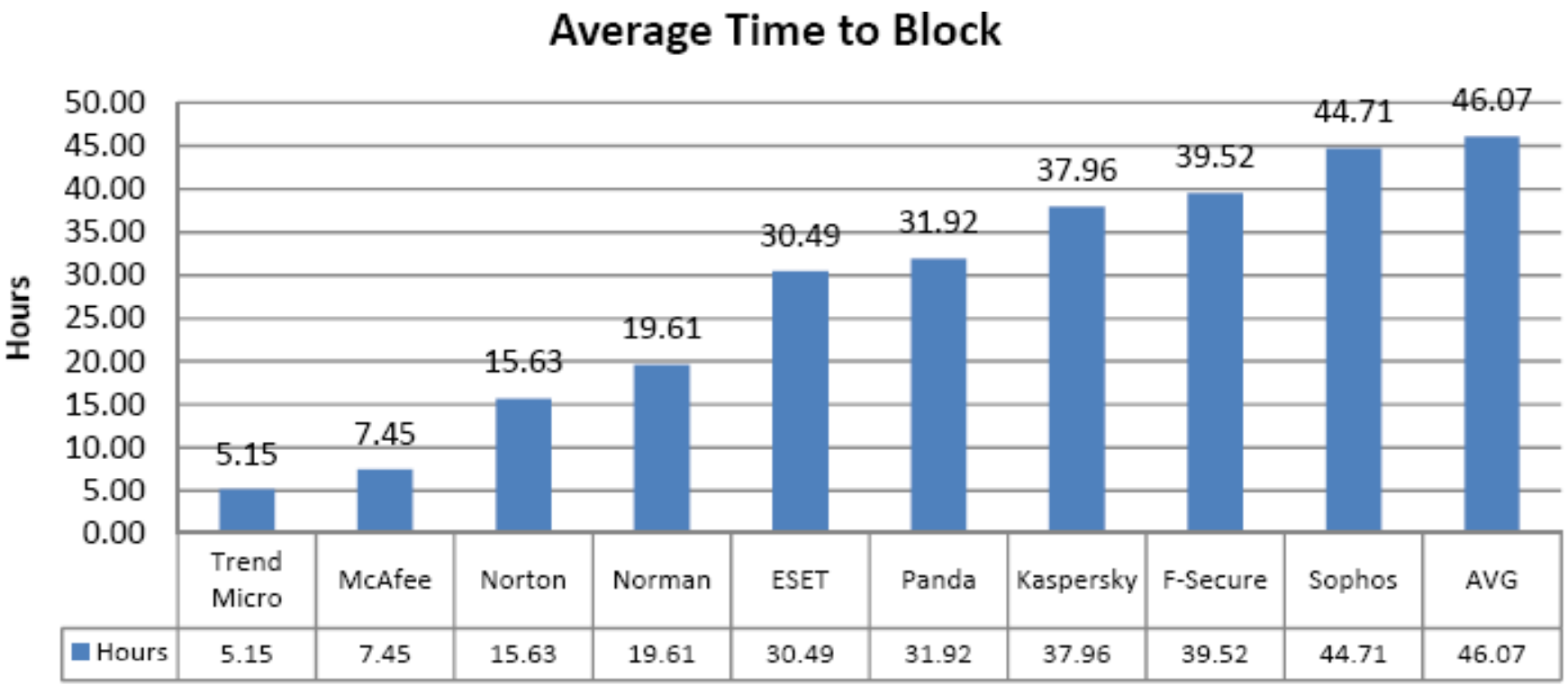
Copyright 2009 Trend Micro Inc.

Putting it all together



Copyright 2009 Trend Micro Inc.

Does all this work?



Source: NSS Labs – based on 231,351 tests on 3,243 unique malicious URLS - http://nsslabs.com/

Copyright 2009 Trend Micro Inc.

Conclusions

- Increase in Malware -> AV Update Bottleneck

Copyright 2009 Trend Micro Inc.

Conclusions

Increase in Malware -> AV Update Bottleneck

Current Pattern Deployment on it's last legs

Copyright 2009 Trend Micro Inc.

Conclusions

Increase in Malware -> AV Update Bottleneck

Current Pattern Deployment on it's last legs

Cloud system is a powerful new layer of defense

Copyright 2009 Trend Micro Inc.

TREND MICRO

TREND MICRO™

 Copyright 2009 Trend Micro Inc.

TREND MICRO™ Securing Your Web World

Backup Slides

Copyright 2009 Trend Micro Inc.

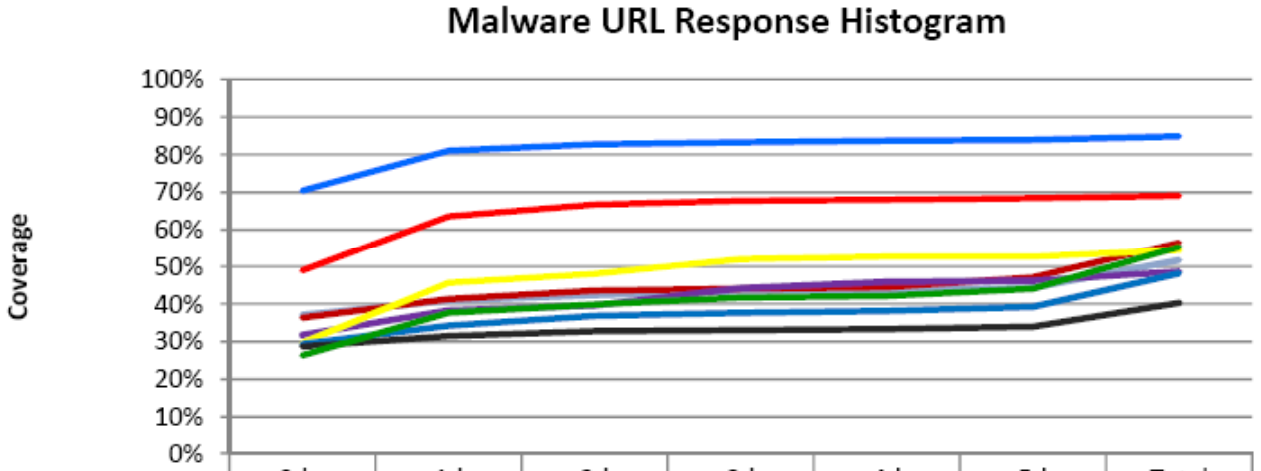
NSS Labs Report

Product	Caught Initially on Download	Caught Subsequently on Execution	Total
Trend Micro	91.0%	5.5%	96.4%
Kaspersky	78.5%	9.3%	87.8%
Norton	50.5%	31.3%	81.8%
McAfee	79.8%	1.9%	81.6%
Norman	66.3%	14.9%	81.2%
F-Secure	63.7%	16.4%	80.0%
AVG	65.0%	8.3%	73.3%
Panda	64.4%	7.6%	72.0%
ESET	65.4%	2.5%	67.9%

Source: NSS Labs – based on 231,351 tests on 3,243 unique malicious URLS - http://nsslabs.com/

Copyright 2009 Trend Micro Inc.

NSS Labs Report



	0-hr	1d	2d	3d	4d	5d	Total
Trend Micro	70%	81%	83%	83%	84%	84%	85%
McAfee	49%	64%	67%	68%	68%	68%	69%
ESET	37%	41%	42%	43%	44%	44%	52%
Kaspersky	36%	41%	44%	44%	44%	47%	56%
Norman	32%	38%	40%	44%	46%	46%	49%
Norton	30%	46%	48%	52%	53%	53%	54%
F-Secure	29%	34%	37%	38%	38%	39%	48%
Panda	29%	31%	33%	33%	33%	34%	40%
AVG	26%	38%	40%	42%	42%	44%	55%

Source: NSS Labs – based on 231,351 tests on 3,243 unique malicious URLS - http://nsslabs.com/

Copyright 2009 Trend Micro Inc.

TREND MICRO