Trend Micro
Smart Protection Network

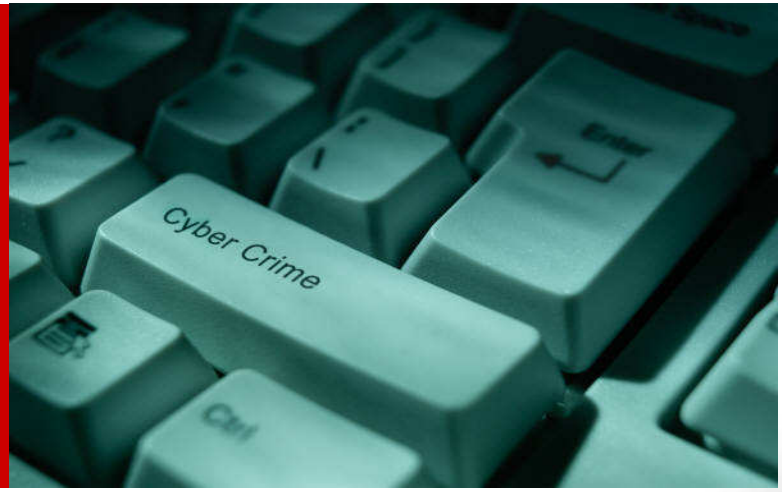
Veli-Pekka Kusmin
Pre-Sales Engineer
Trend Micro Baltics & Finland

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?

TREND MICRO 20 1988-2008 ANNIVERSARY

Collaboration in the Underground

Botnet Vendors and Hackers

Independent Businessman

Carders Spammers Blackmailers

Malware Vendors

Anti-Detection Vendors Toolkit Vendors

TREND MICRO 20 1988-2008 ANNIVERSARY

Increase in unique malware samples

1988: 1738 unique malware samples

1998: 177615 unique malware samples

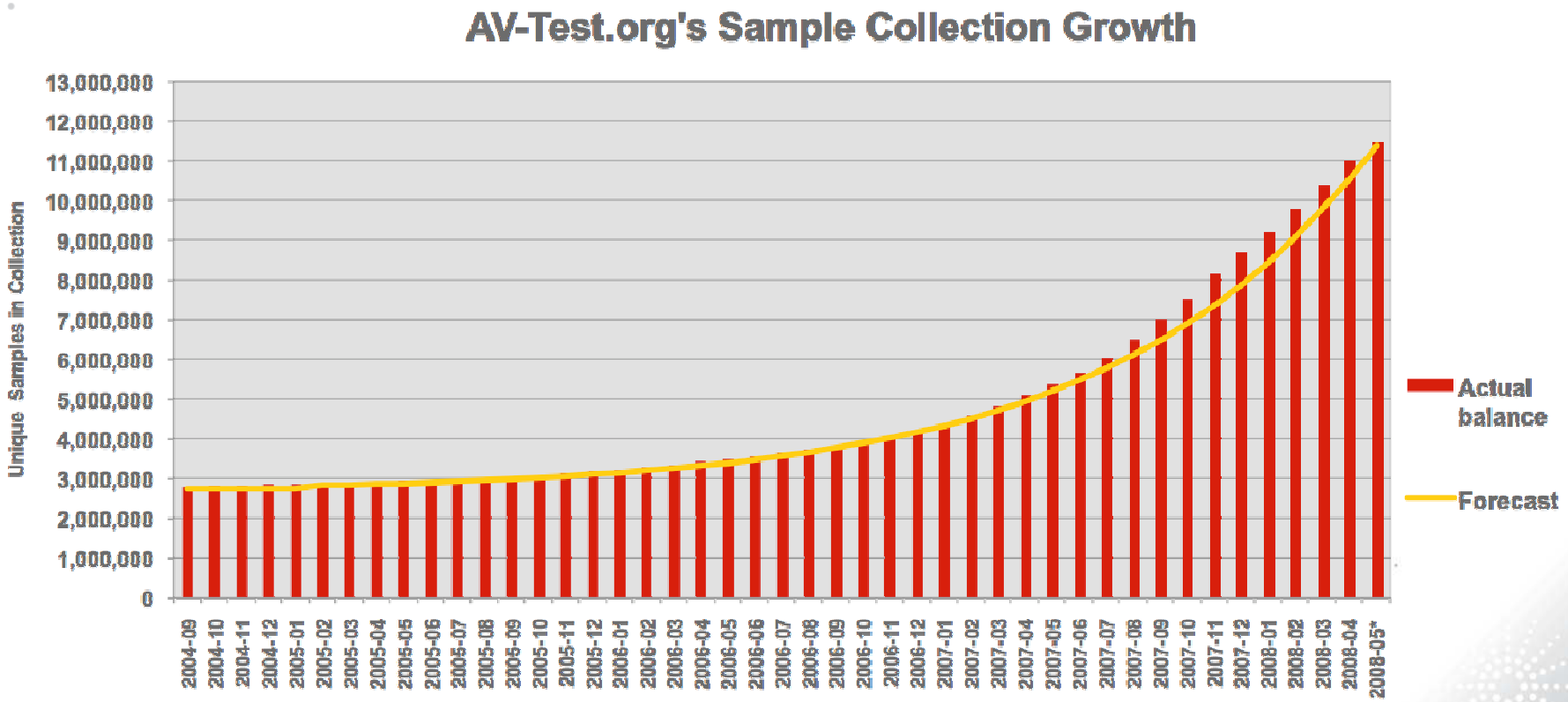
2008 Jan-May: 2753587 unique malware samples*

Data source: AV-Test.Org, June 2008

* = January - May 2008

TREND MICRO 1988-2008 20 ANNIVERSARY

Increase in unique malware samples

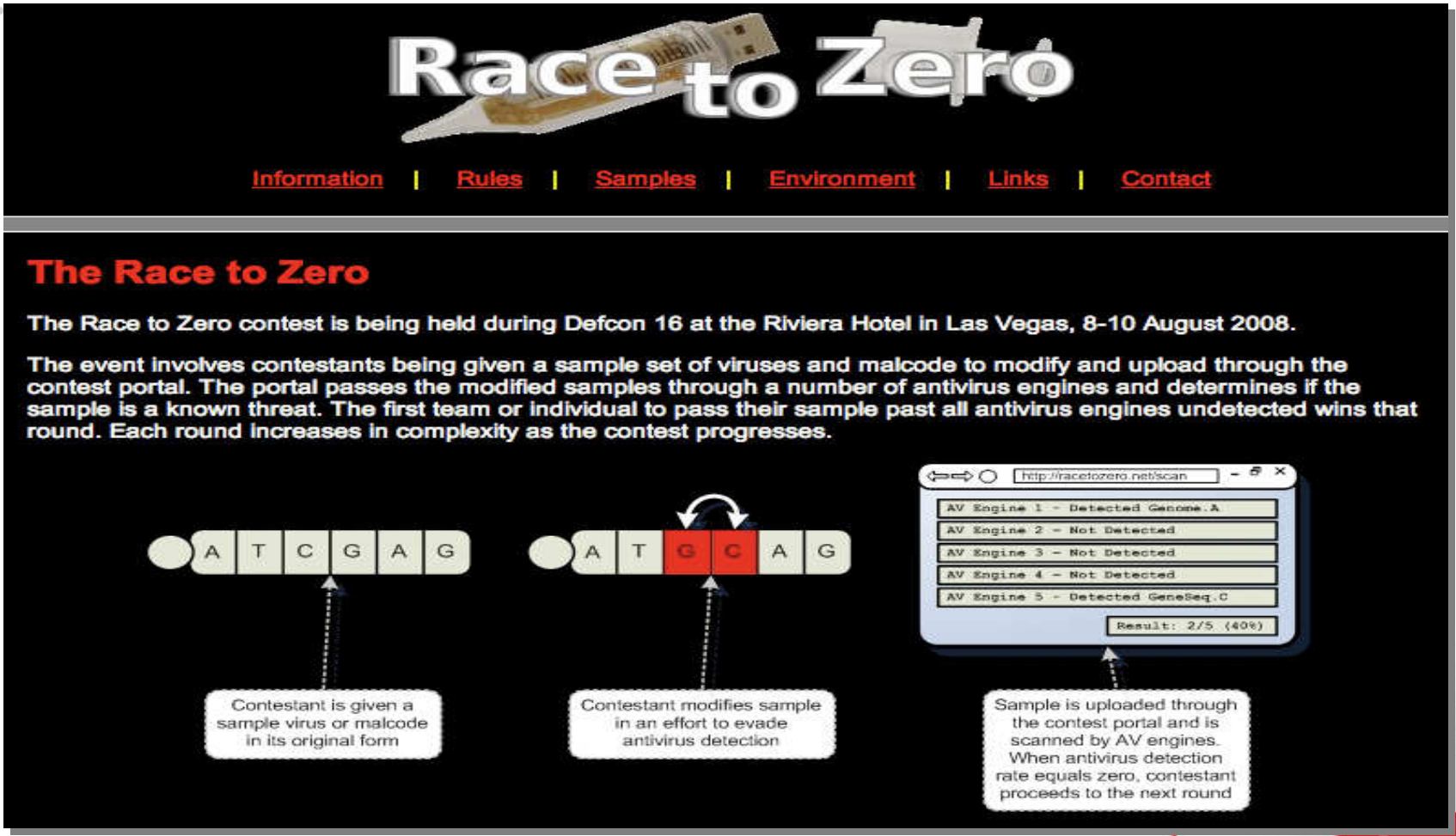


Data source: AV-Test.Org, June 2008

Note: Samples include malware variants

TREND MICRO 20 1988-2008 ANNIVERSARY

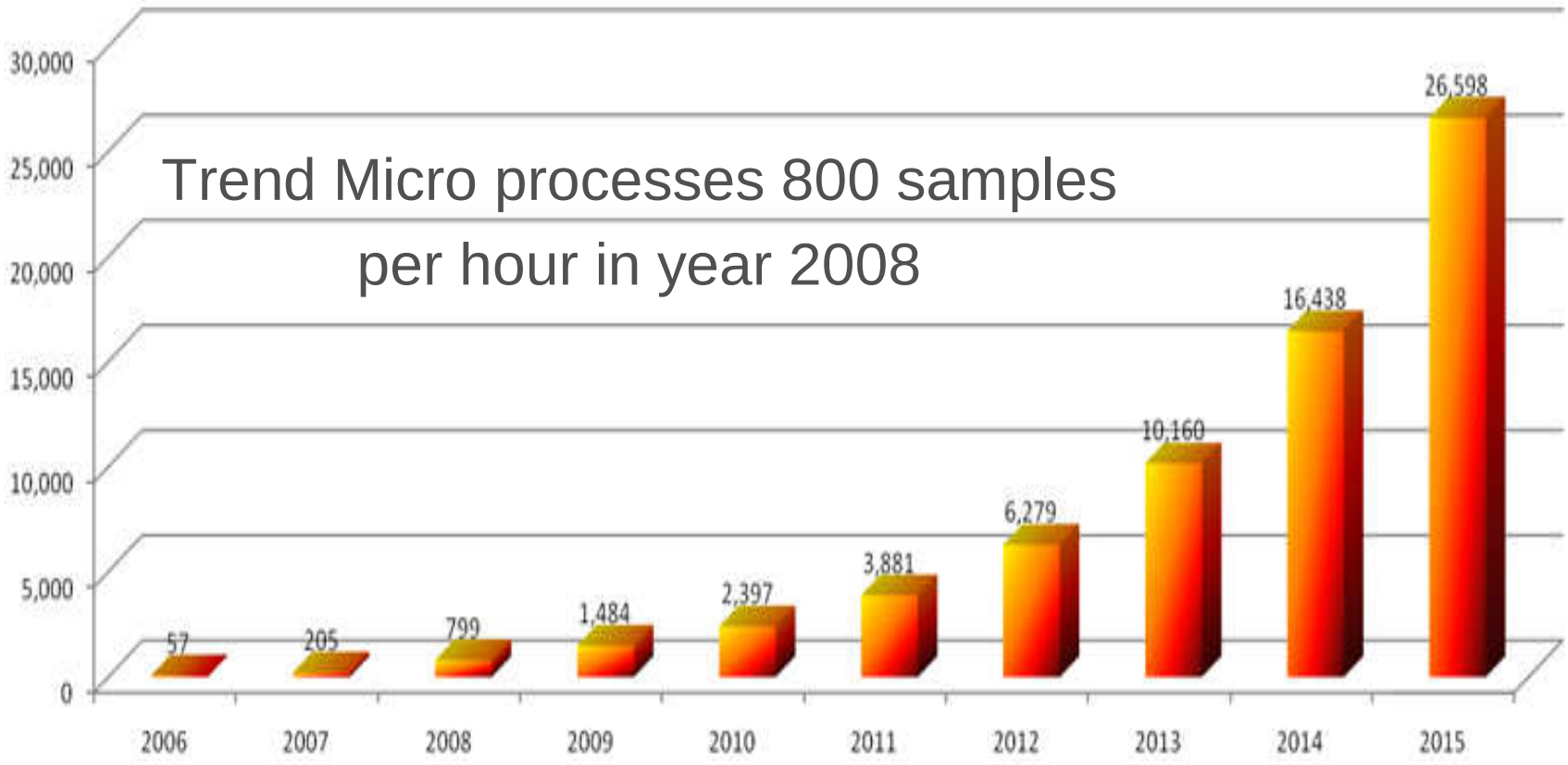
Could we rely on this Prognosis?



Source: www.defcon.org

TREND MICRO 20 1988-2008 ANNIVERSARY

Incoming Threat Samples Per Hour

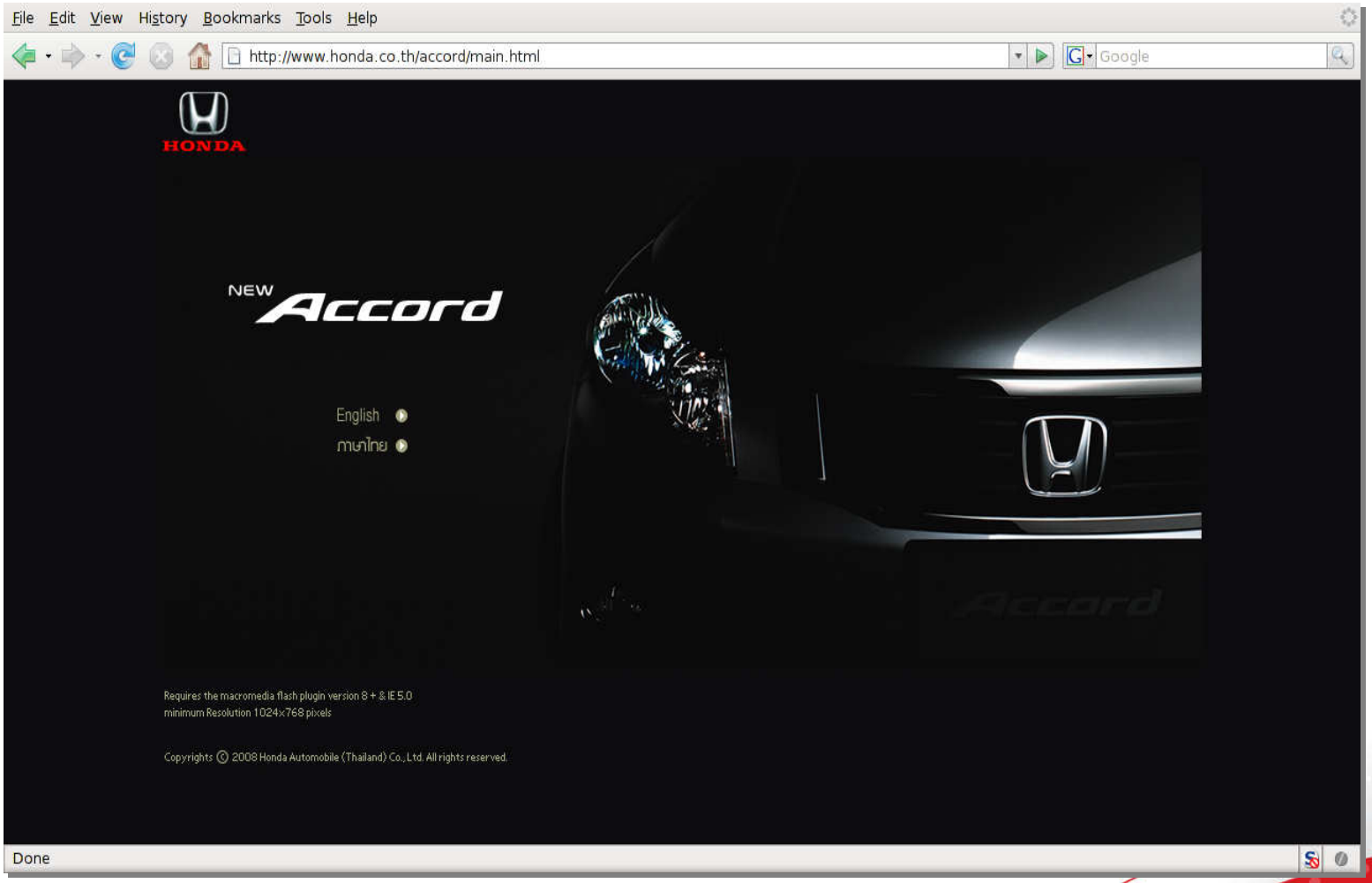


Trend Micro processes 800 samples per hour in year 2008

Problems in the pattern deployment in the future?

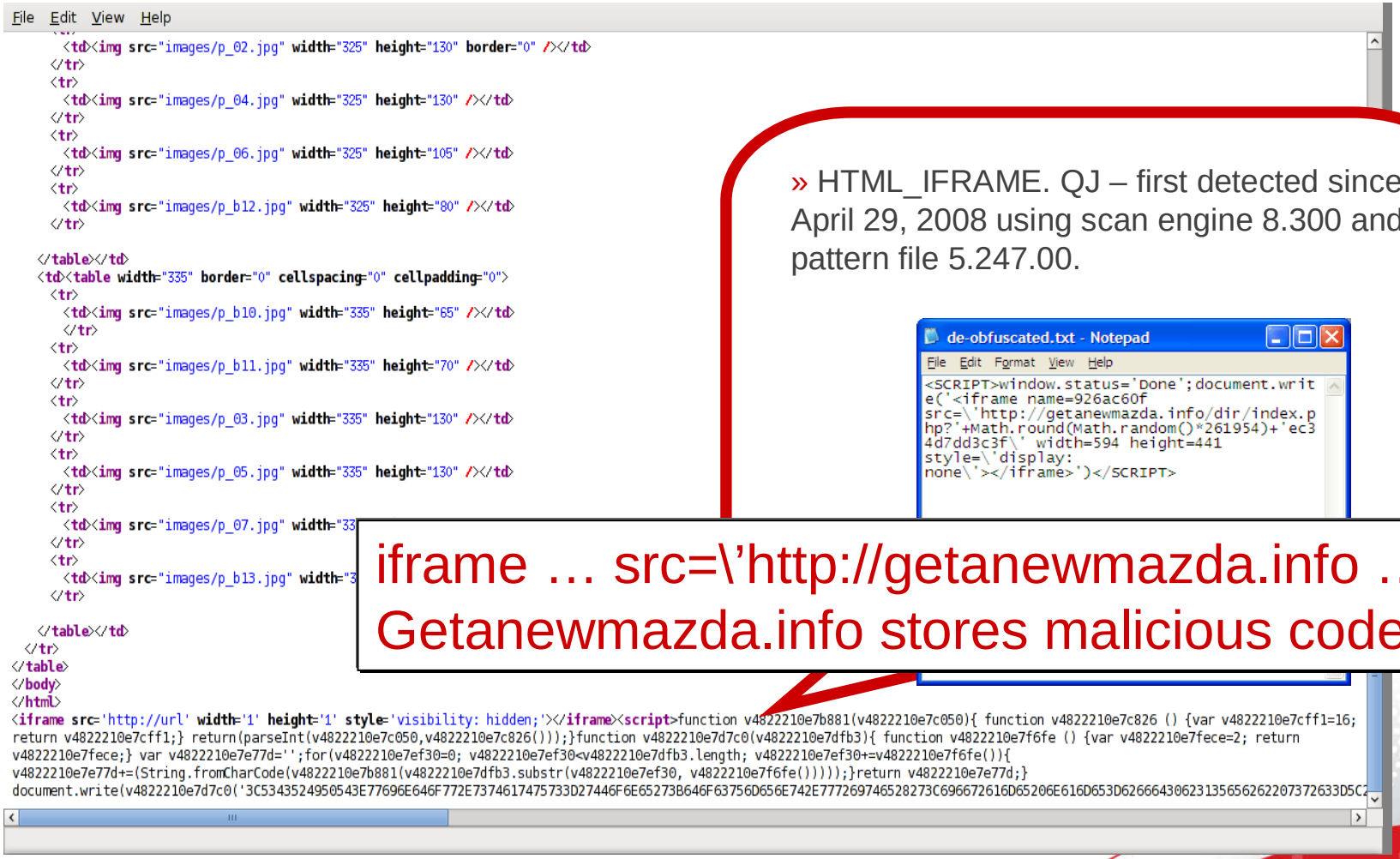
TREND MICRO 20 1988-2008 ANNIVERSARY

A Typical Web Threat – 9th of May 2008



TREND MICRO 20 ANNIVERSARY 1988-2008

What does the HTML Code look like?

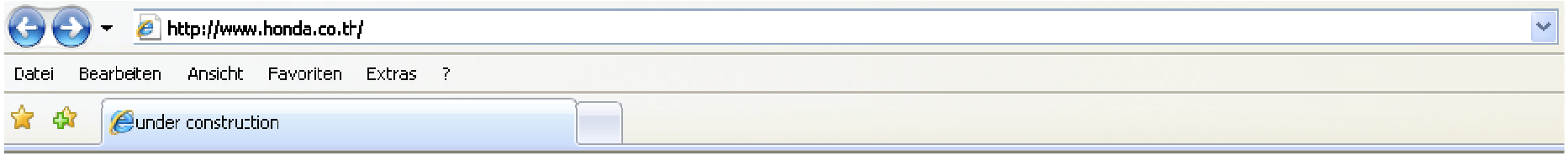


» HTML_IFRAME. QJ – first detected since April 29, 2008 using scan engine 8.300 and pattern file 5.247.00.

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

TREND MICRO 20 1988-2008 ANNIVERSARY

Fast Reaction from Honda!



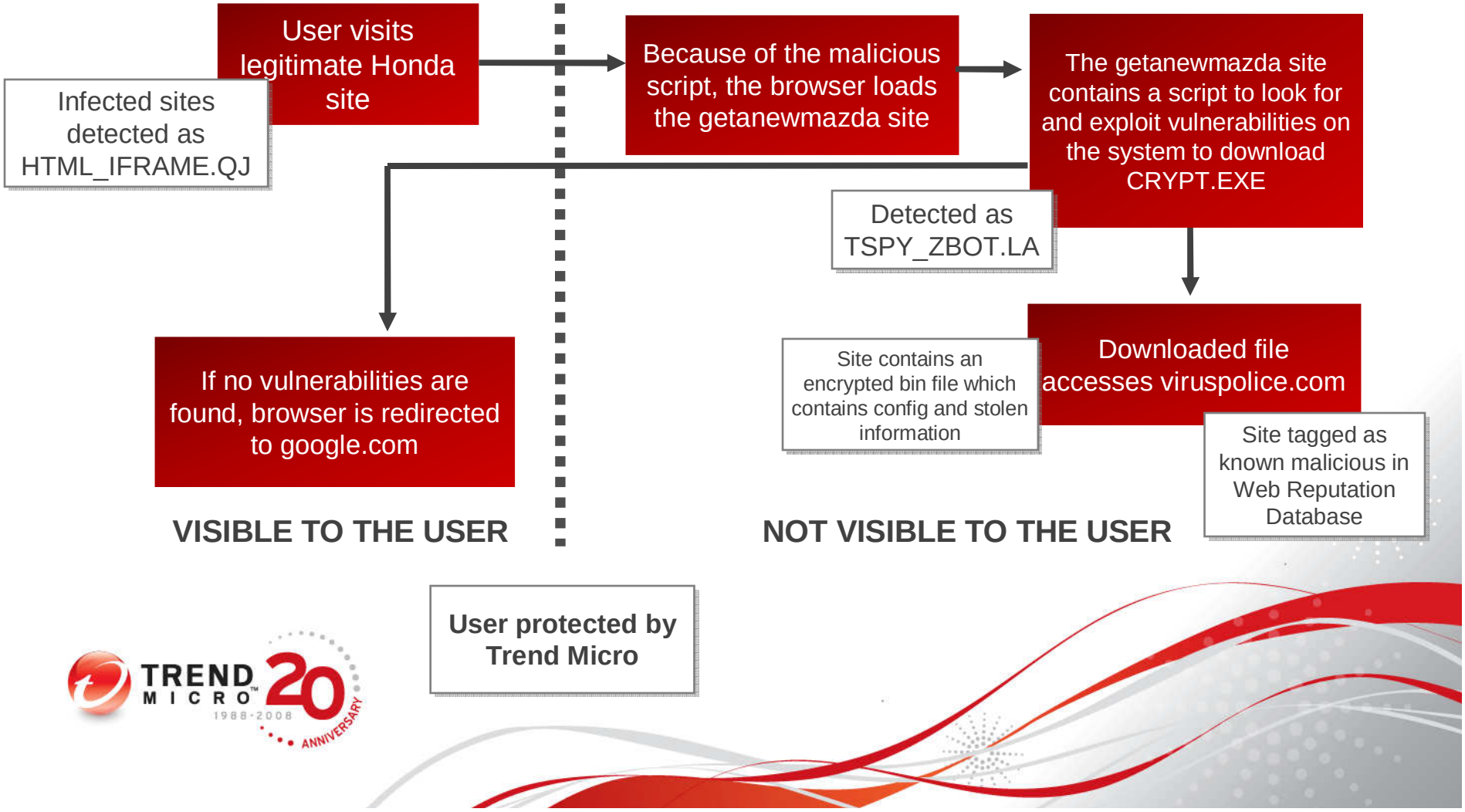
HONDA

Under Construction

TREND MICRO 20 1988-2008 ANNIVERSARY

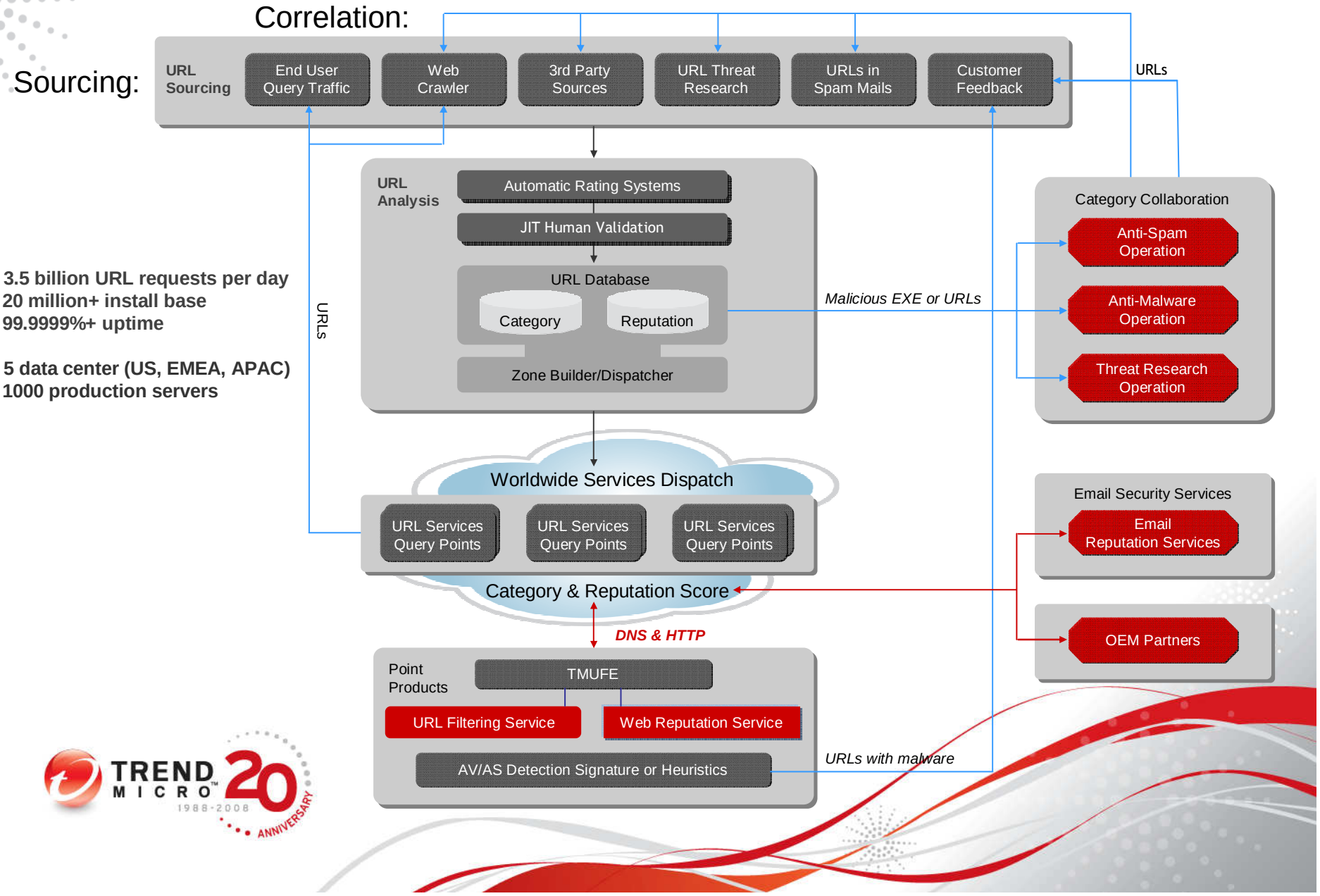
How does the infection chain work?

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



TREND MICRO 20 1988-2008 ANNIVERSARY

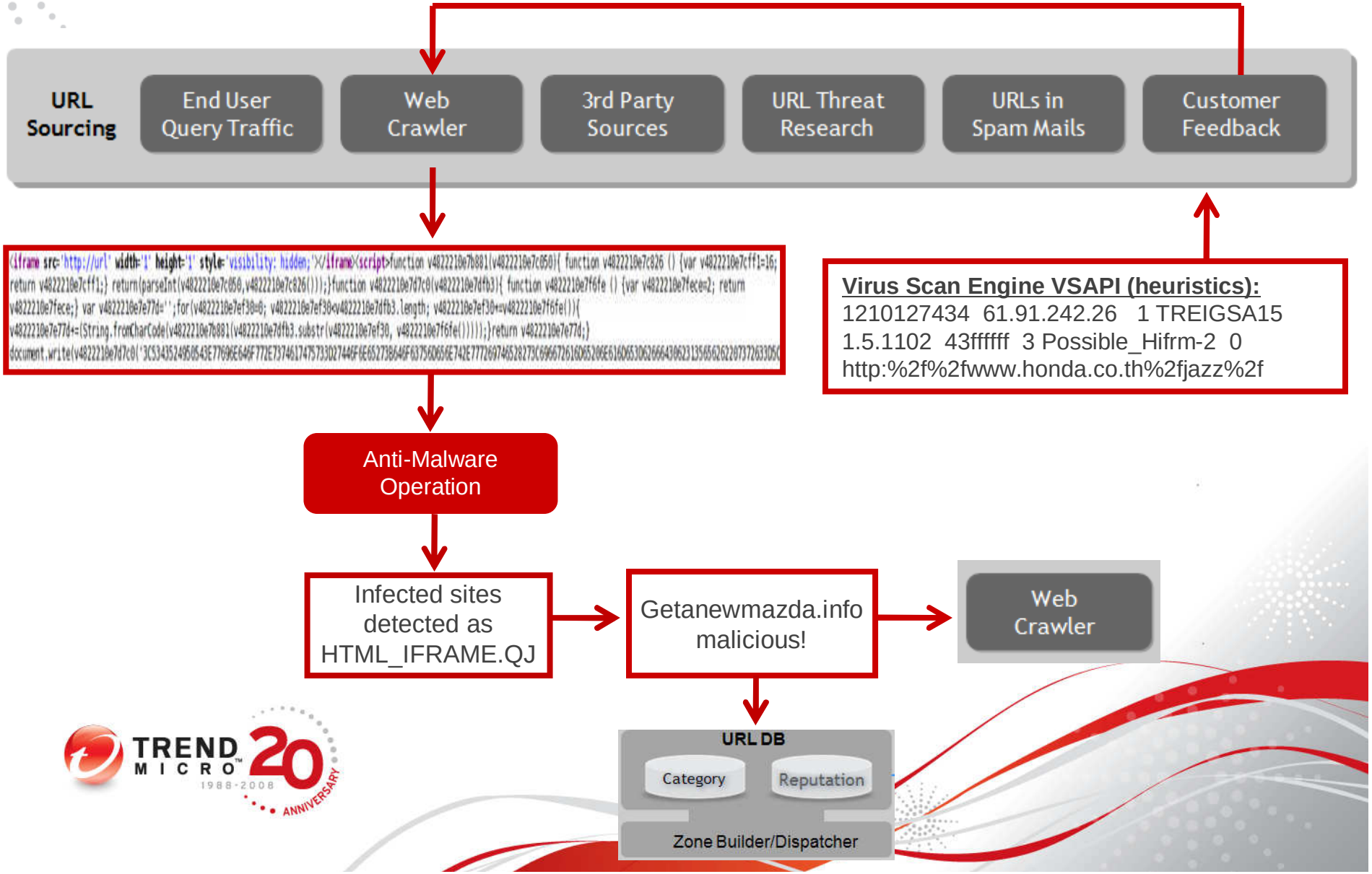
Trend Micro Smart Protection Network (Web)



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

TREND MICRO 20 1988-2008 ANNIVERSARY

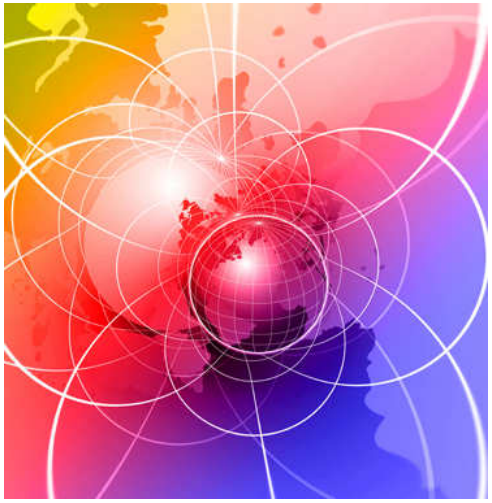
Processing of a Web Threat - Honda example



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)

TREND MICRO 20 1988-2008 ANNIVERSARY

Why File Reputation in the Cloud?

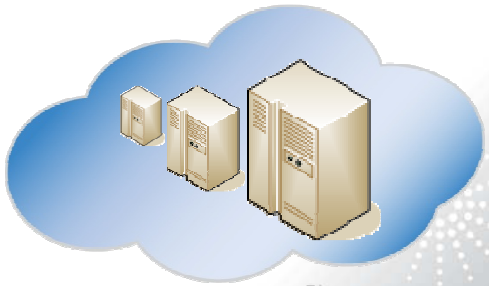
The traditional approach to Malware protection places the burden of storage and detection intelligence on the customer.

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

TREND MICRO 20 1988-2008 ANNIVERSARY

Why File Reputation in the Cloud?

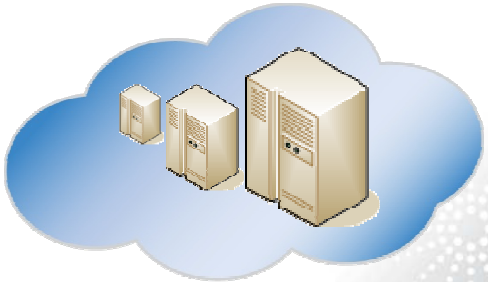
The future approach to Malware protection places the burden of storage and detection intelligence in the cloud.

Burden of Storage

Endpoint

Advantages

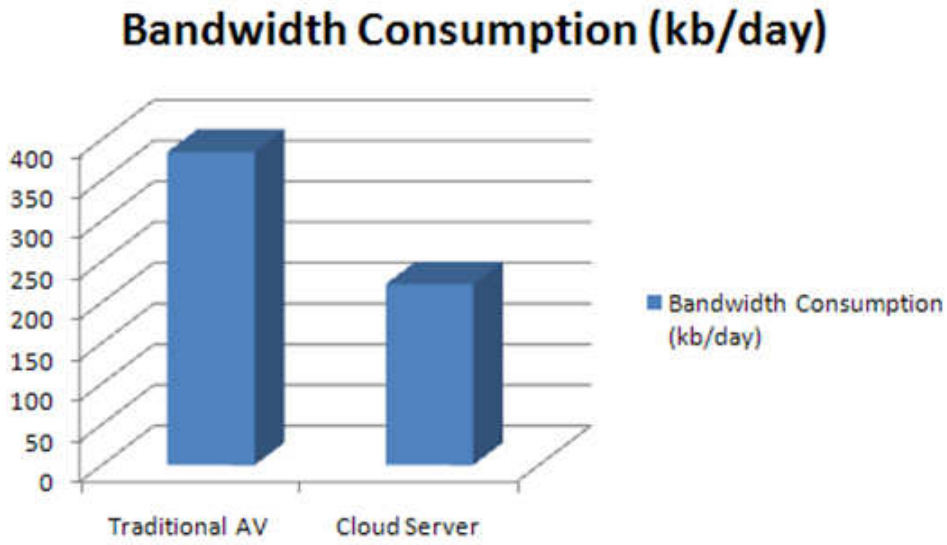
- minimal endpoint resource usage
- consistent network bandwidth usage
- immediate handling of new threats
- increased awareness of localized threats

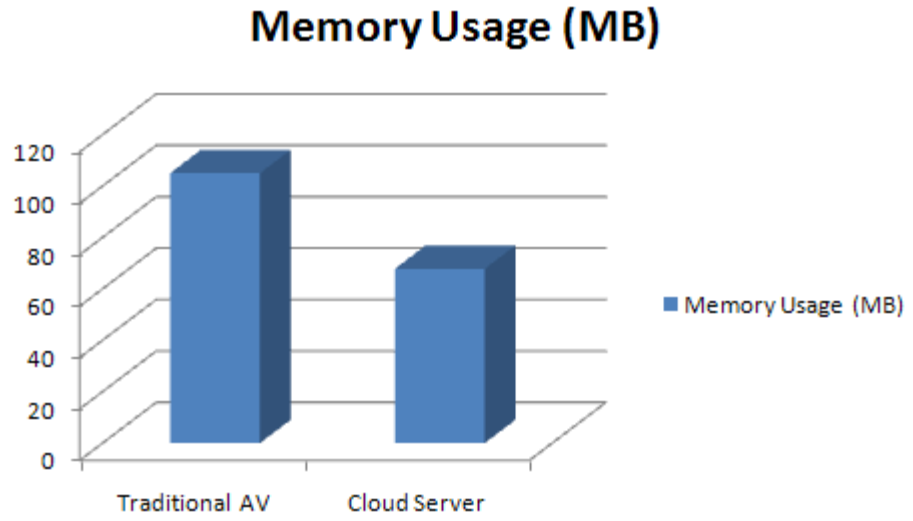


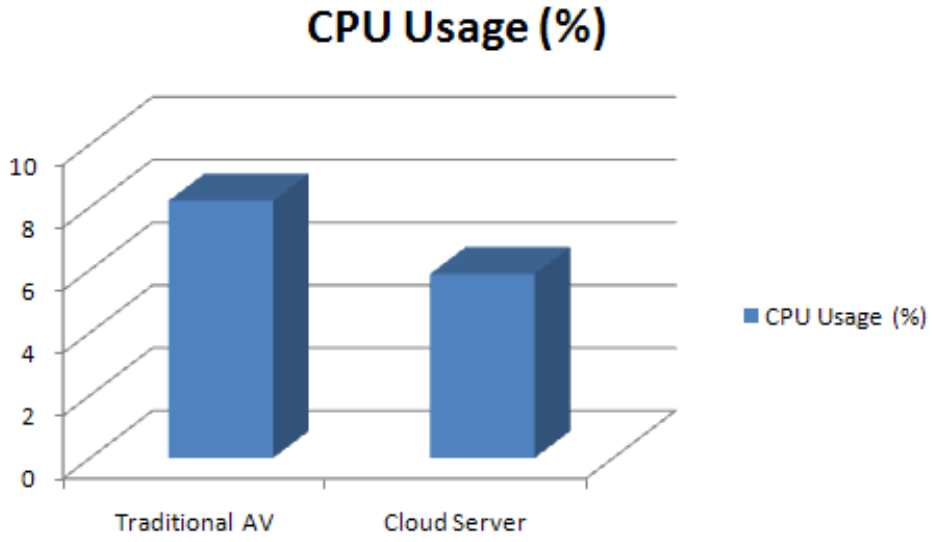
Cloud

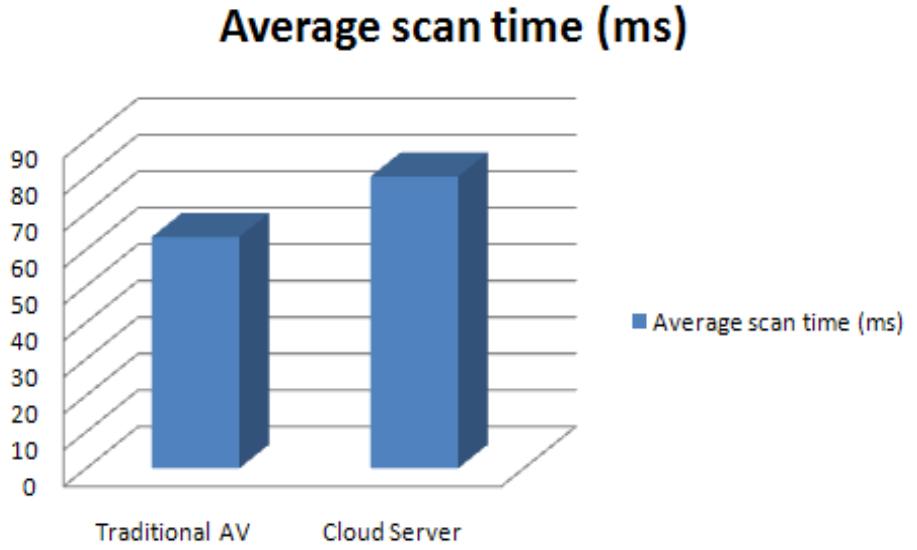
TREND MICRO 20 1988-2008 ANNIVERSARY

Pros and Cons for File Reputation In The Cloud









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

TREND MICRO 20 1988-2008 ANNIVERSARY

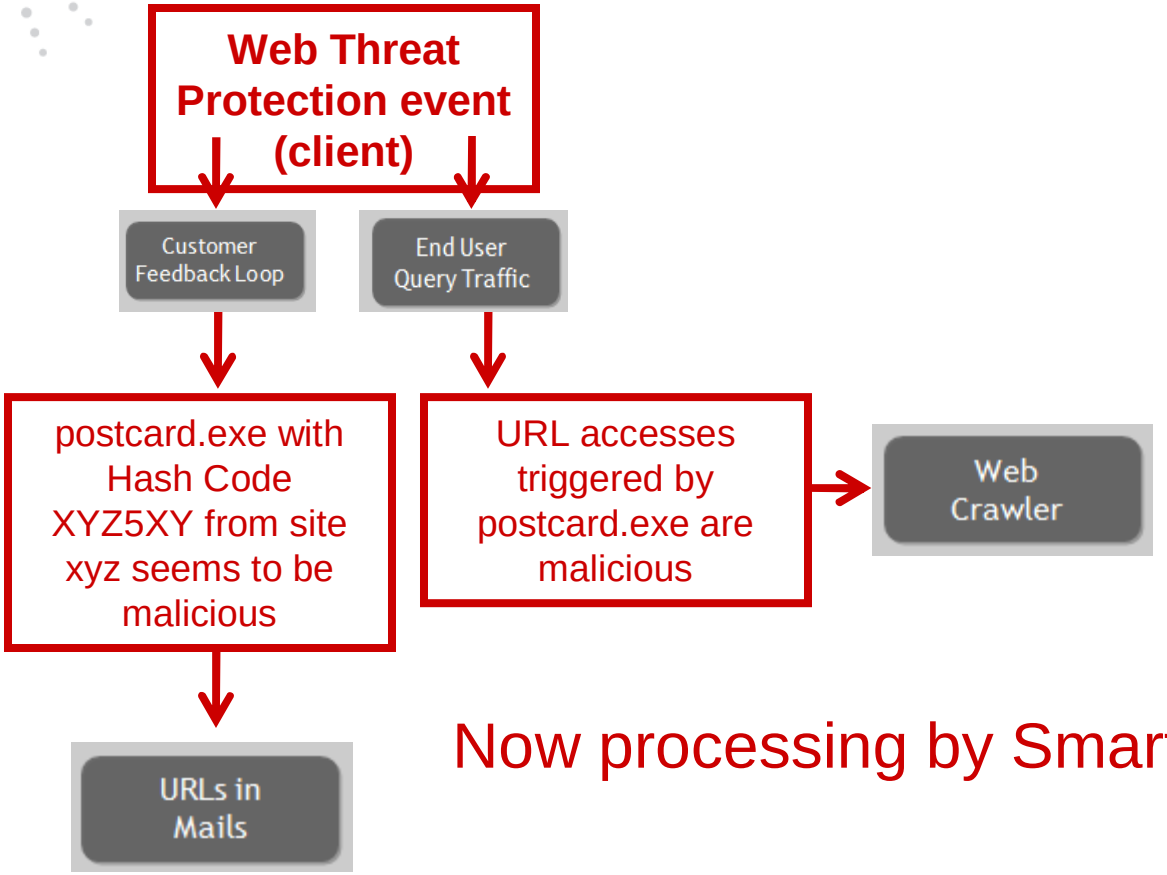

My Computer
Recycle Bin
Adobe Reader 8
InterVideo WinDVD 7
Mozilla Firefox
Nero StartSmart
NXPowerLite 3
Skype
VMware Player
Unused Desktop Shortcuts
NXPowerLite2.5
Ultralingua
license to
l.o.v.e.
LEGAL ORGANIZED VIRUS ELIMINATION
start
DE
Inbox - Microsoft Out...
Search Desktop
96%
14:48

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:



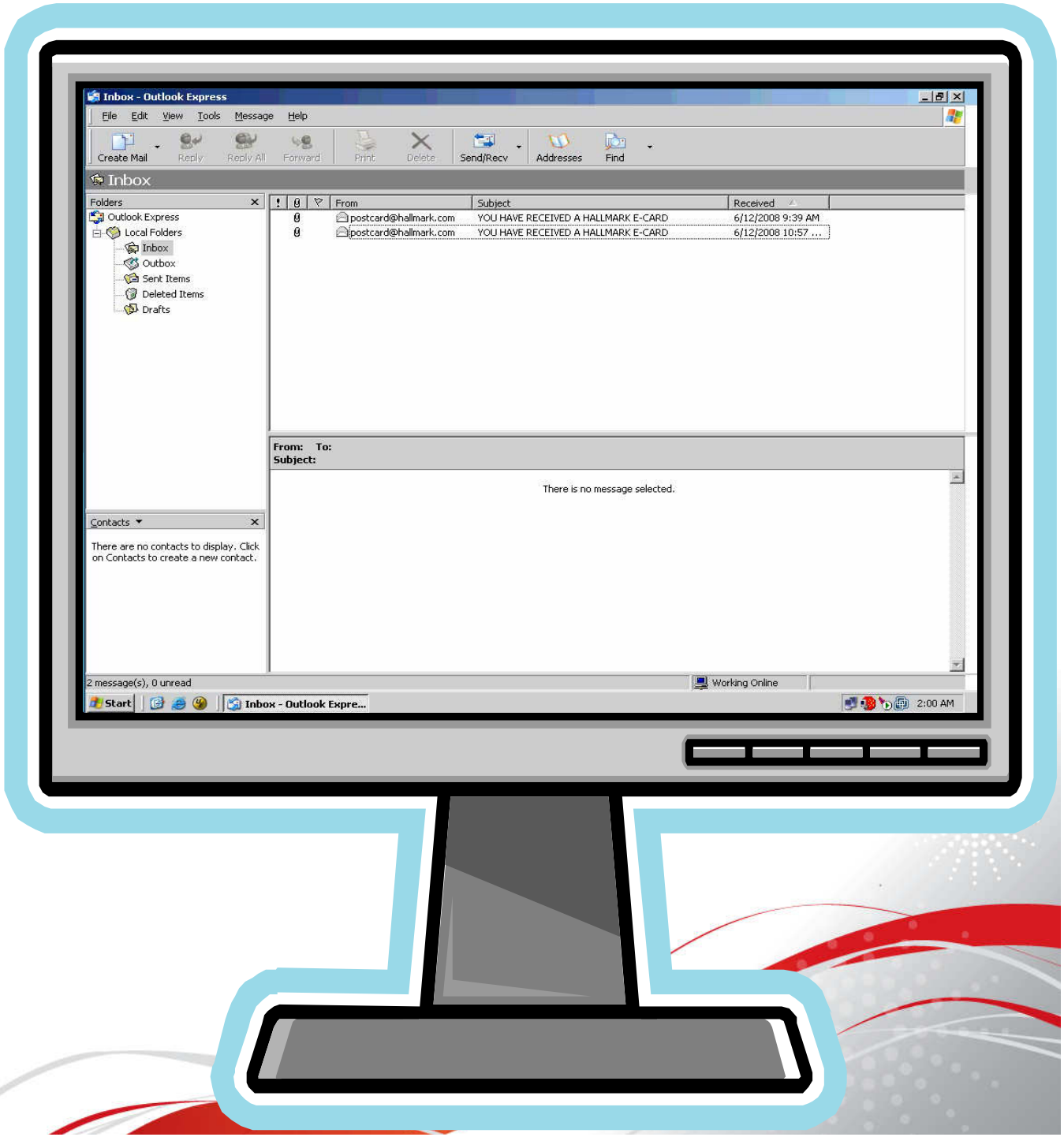
Now processing by Smart Protection Network …

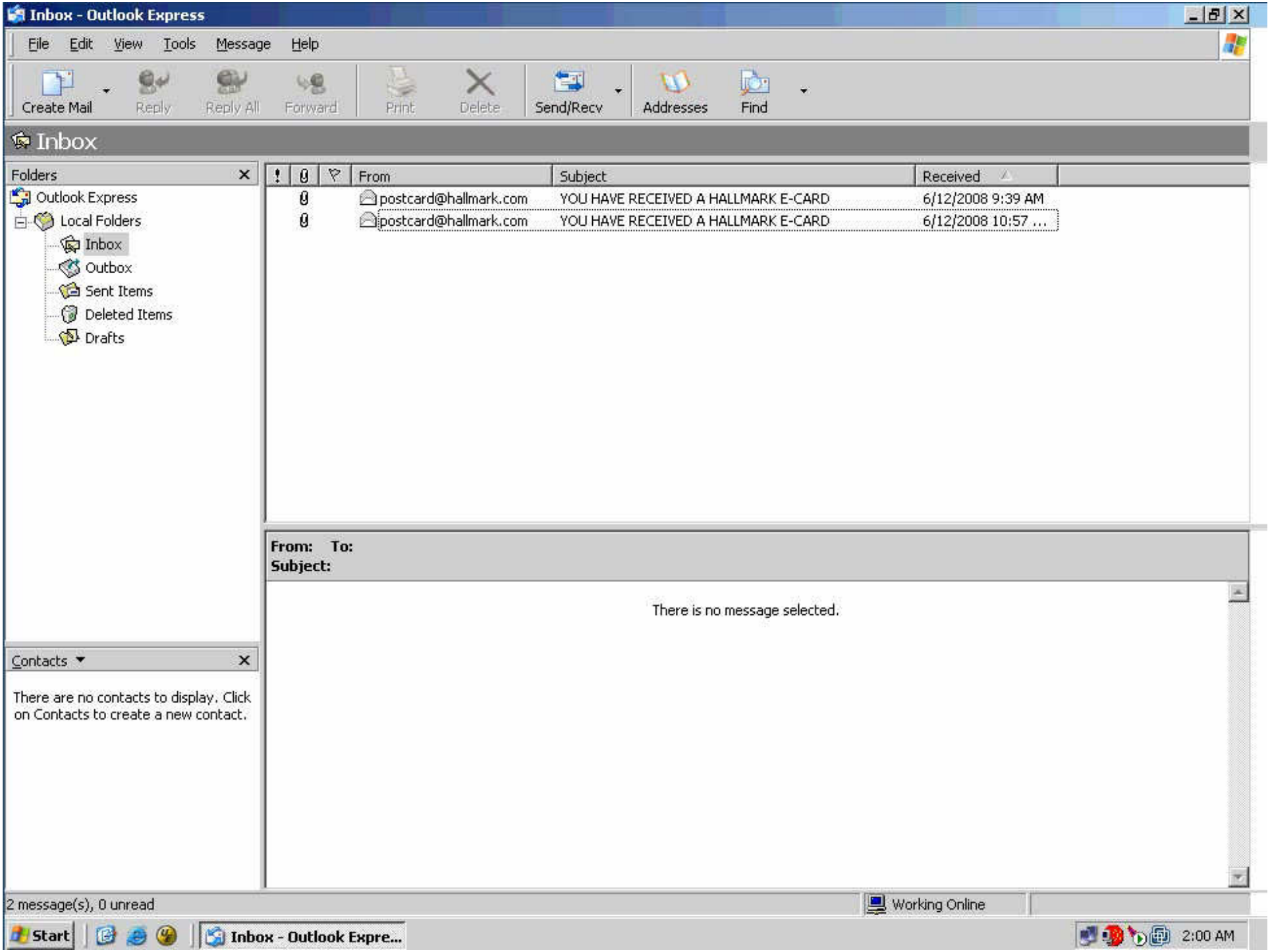
TREND MICRO 20 1988-2008 ANNIVERSARY

While the systems are busy in the data centers:

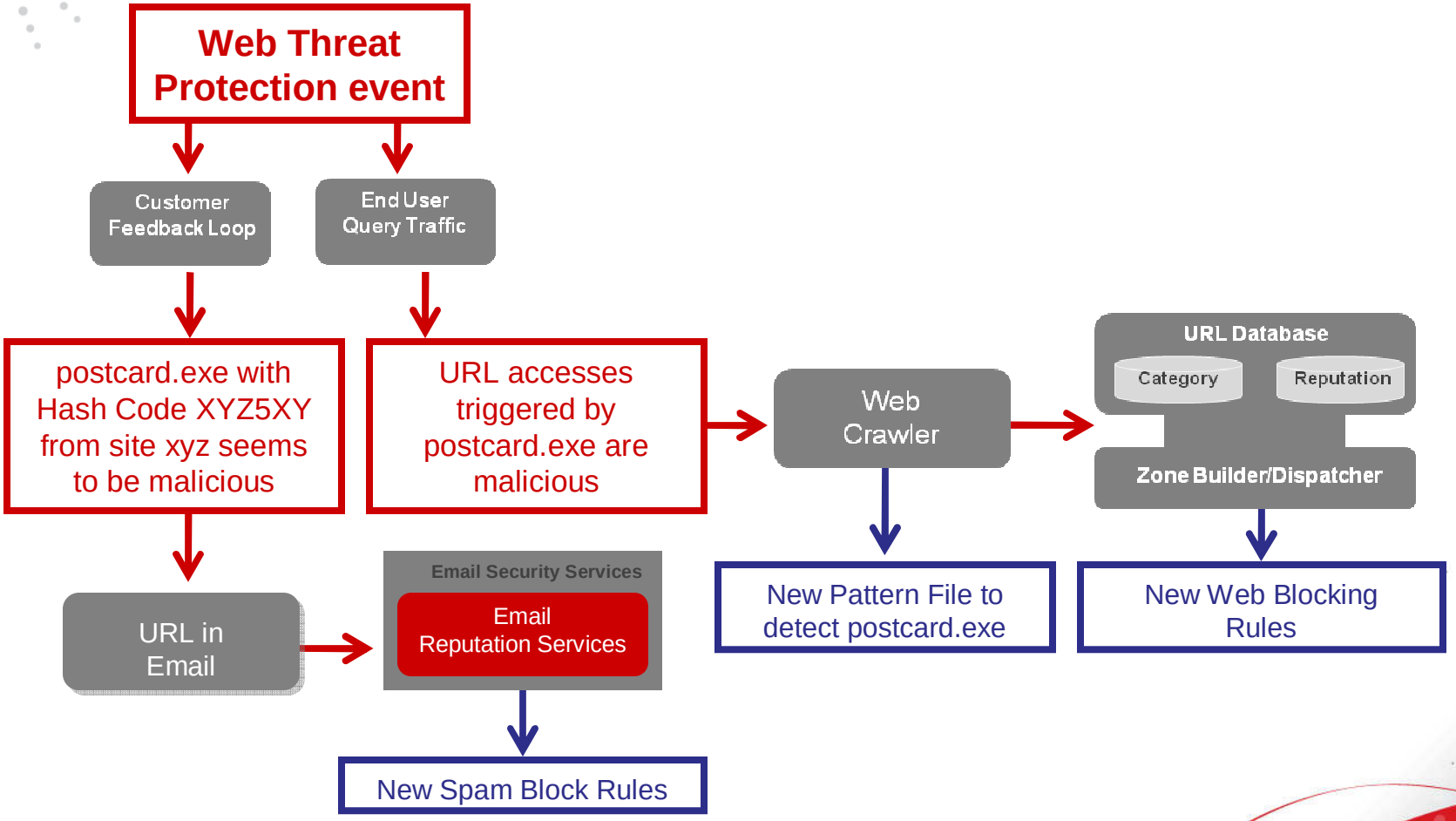
Another user receives the greeting card as well.

But he saves the attachment on the harddrive.




Inbox - Outlook Express
File Edit View Tools Message Help
Create Mail
Reply
Reply All
Forward
Print
Delete
Send/Recv
Addresses
Find
Inbox
Folders
Outlook Express
Local Folders
Inbox
Outbox
Sent Items
Deleted Items
Drafts
From
Subject
Received
postcard@hallmark.com
YOU HAVE RECEIVED A HALLMARK E-CARD
6/12/2008 9:39 AM
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.
2 message(s), 0 unread
Working Online
Start
Inbox - Outlook Expre...
2:00 AM

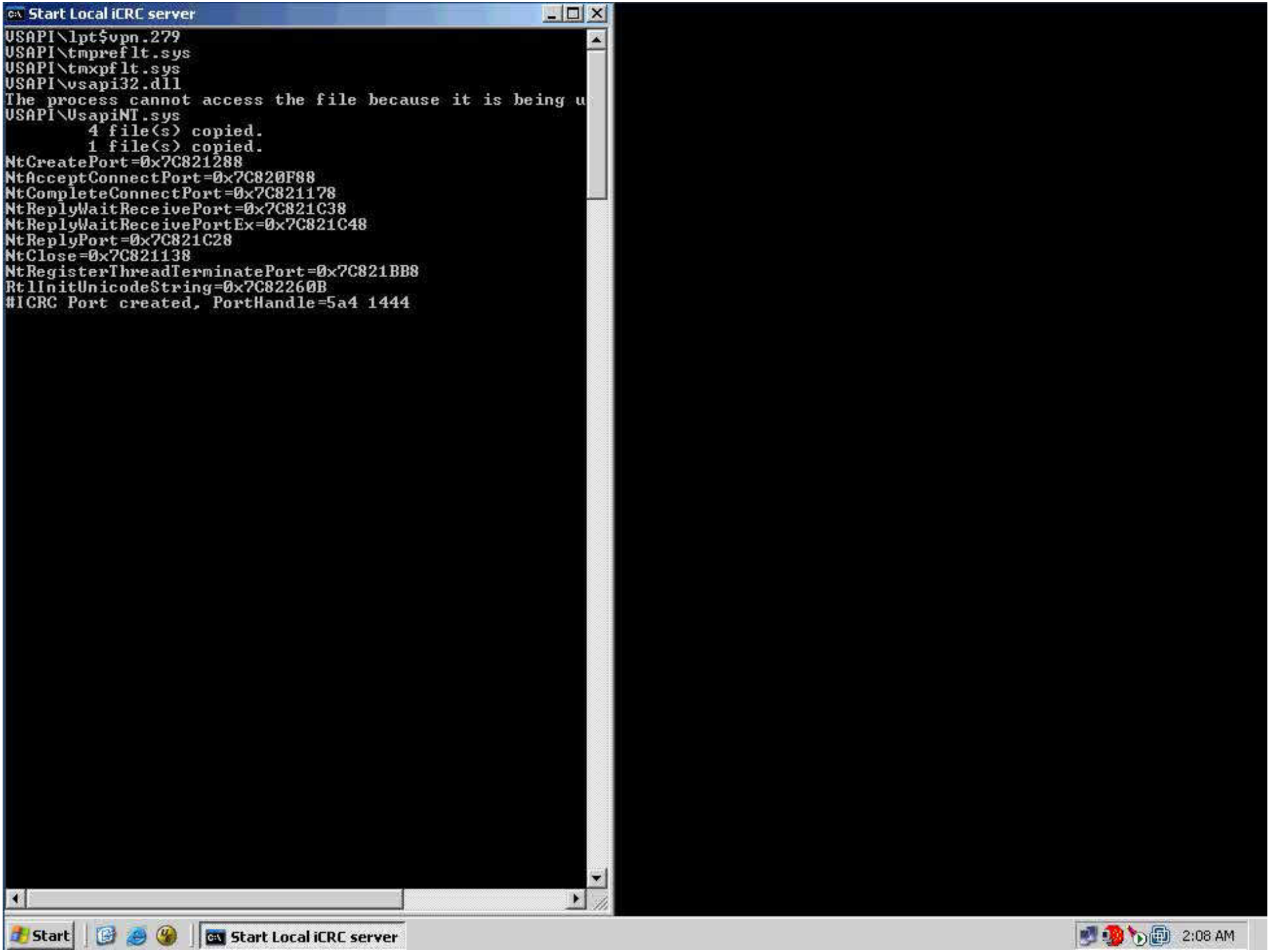
Processing is done!!!



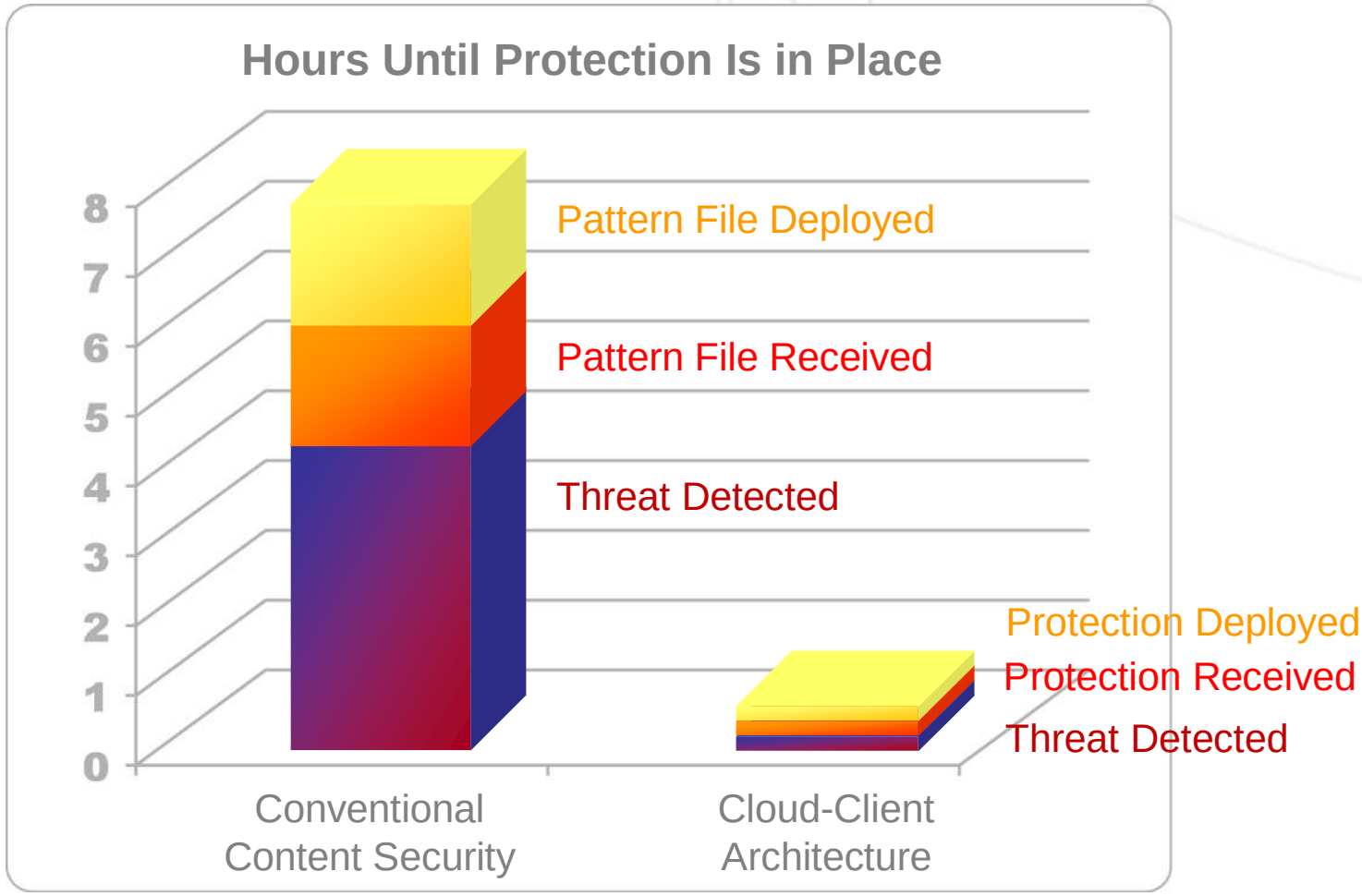
The previous was scanning using OfficeScan with the local Pattern File

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
VSAPI\lpt$vpn.279
VSAPI\tmpreflt.sys
VSAPI\tmxpflt.sys
VSAPI\vsapi32.dll
The process cannot access the file because it is being u
VSAPI\VsapiNT.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
Start
Start Local iCRC server
2:08 AM

Benefits of Cloud-Client Architecture



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

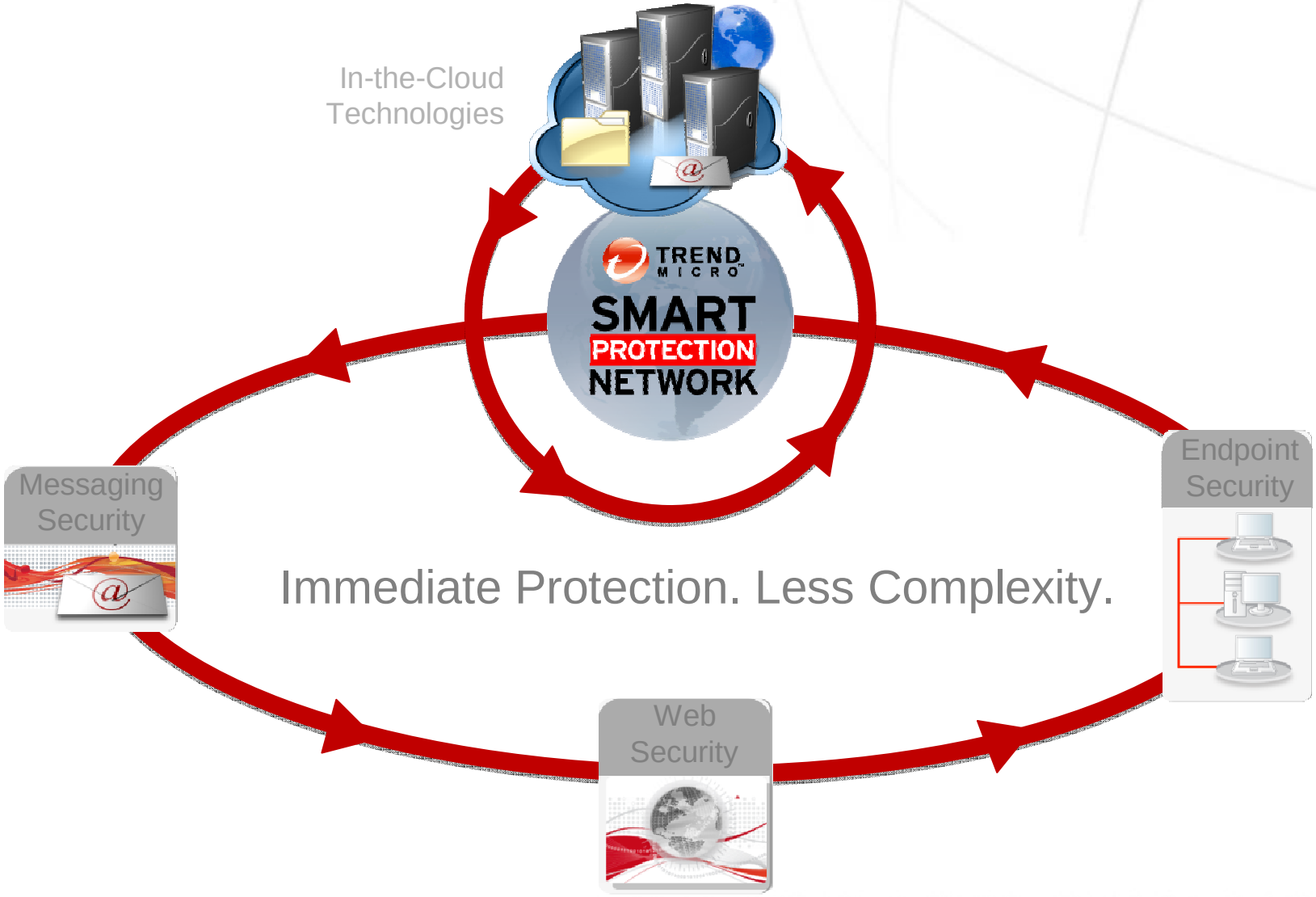
250 Million
Malware Samples Processed Each Year

TREND MICRO SMART PROTECTION NETWORK

Trend Micro Enterprise Security

Securing Your Web World

Powered by Smart Protection Network



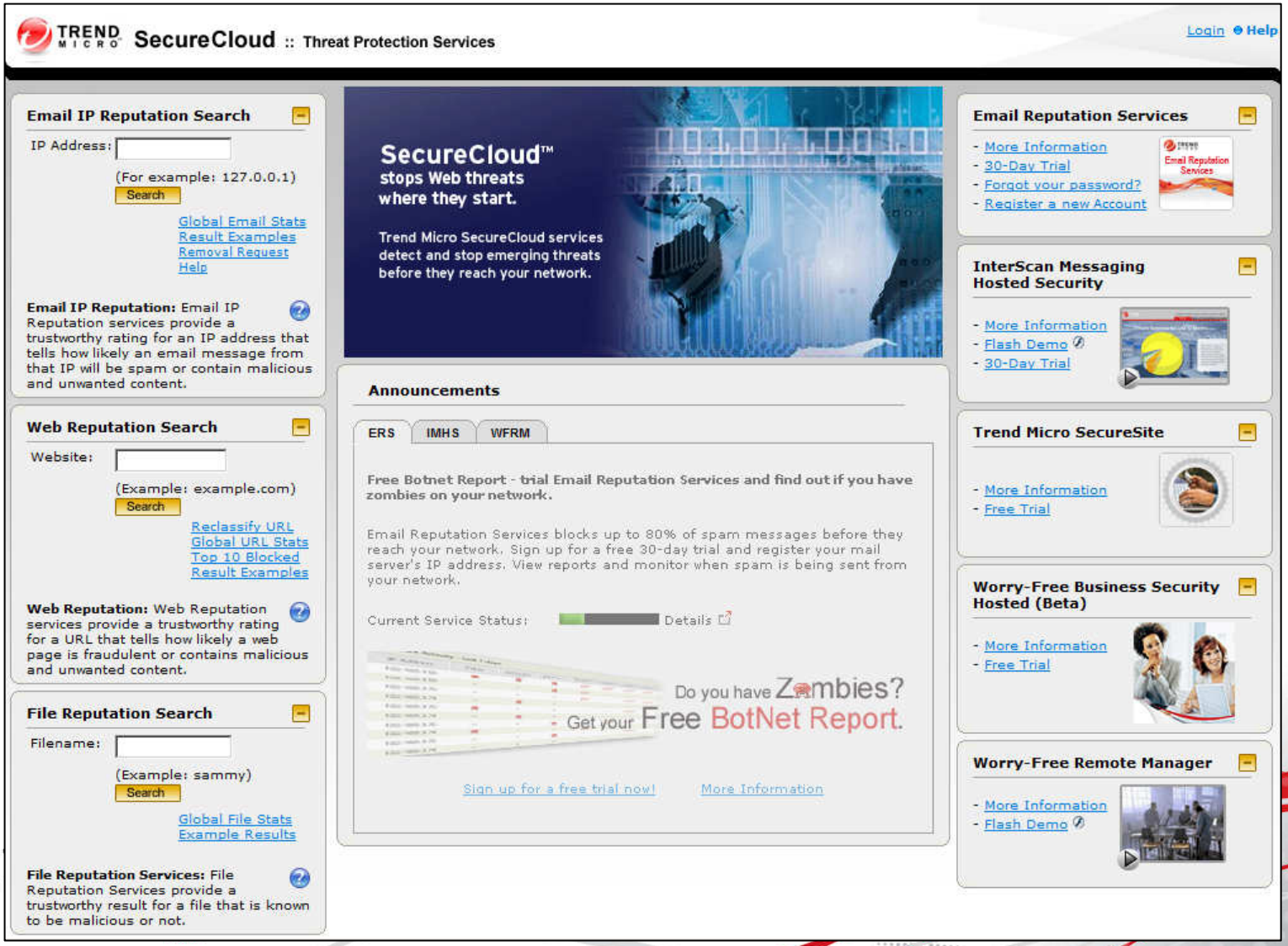
Trend Micro Enterprise Security powered by Smart Protection Network

Minimize your

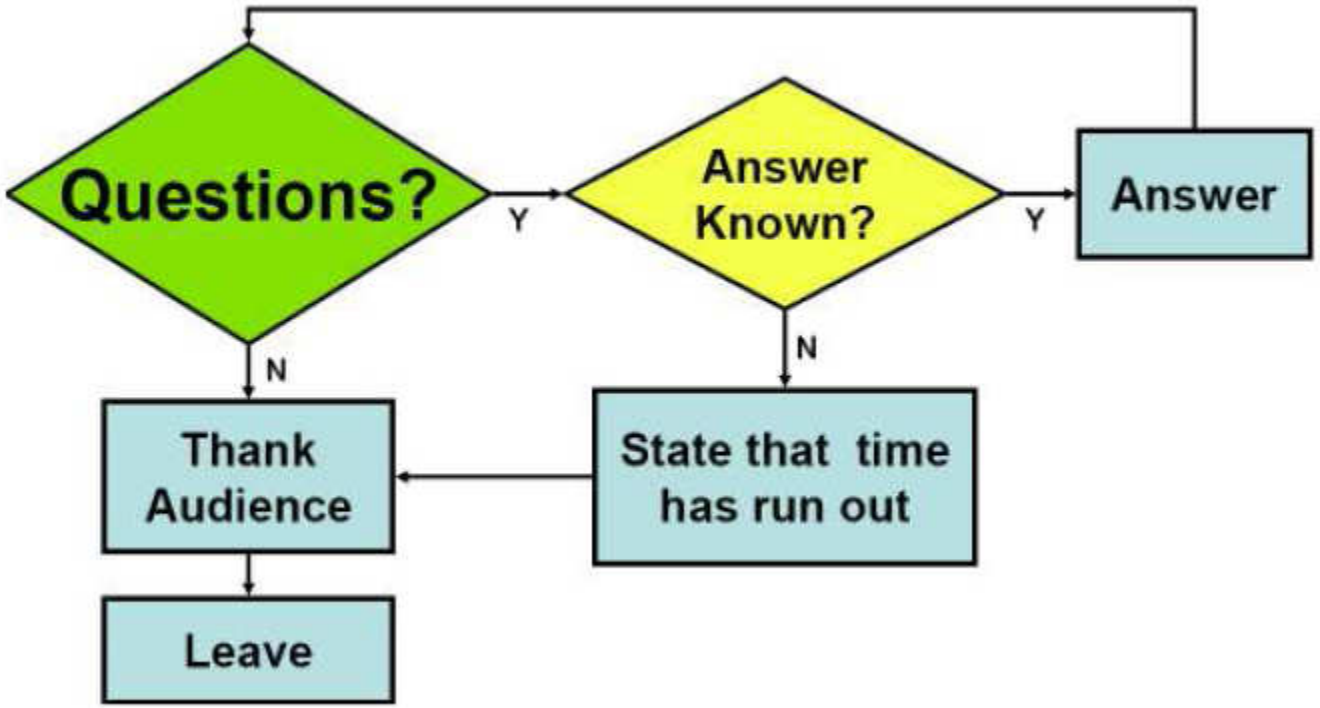
Time to Protection

TREND MICRO 20 1988-2008 ANNIVERSARY

SecureCloud Portal – securecloud.com



Questions?


Questions?
Y
Answer Known?
Y
Answer
N
N
Thank Audience
State that time has run out
Leave

Trend Micro | Securing Your Web World



Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Baltics & Finland
Pakkalakuja 7, 3rd 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
http://fi.trendmicro-europe.com