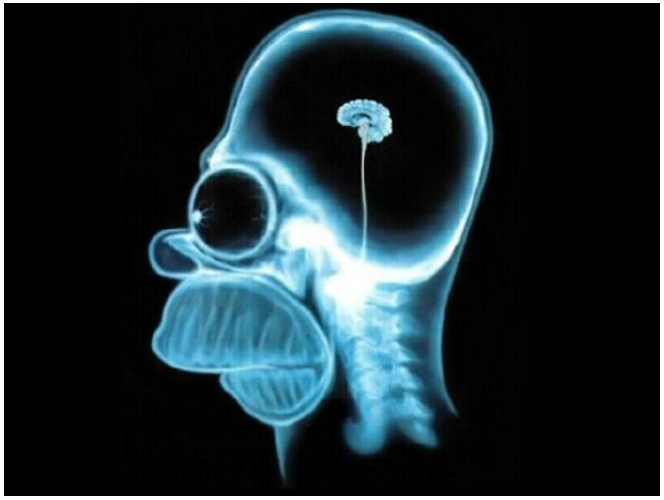
Pete Nieminen
Key Accounts
Baltics and Finland

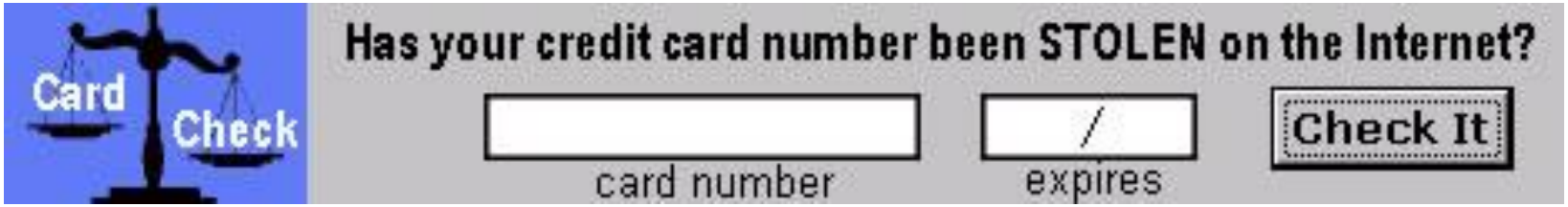
Evolution from Internet threats to Cybercrime

What cybercrime? Isn't the problem about the stoopid end-users?

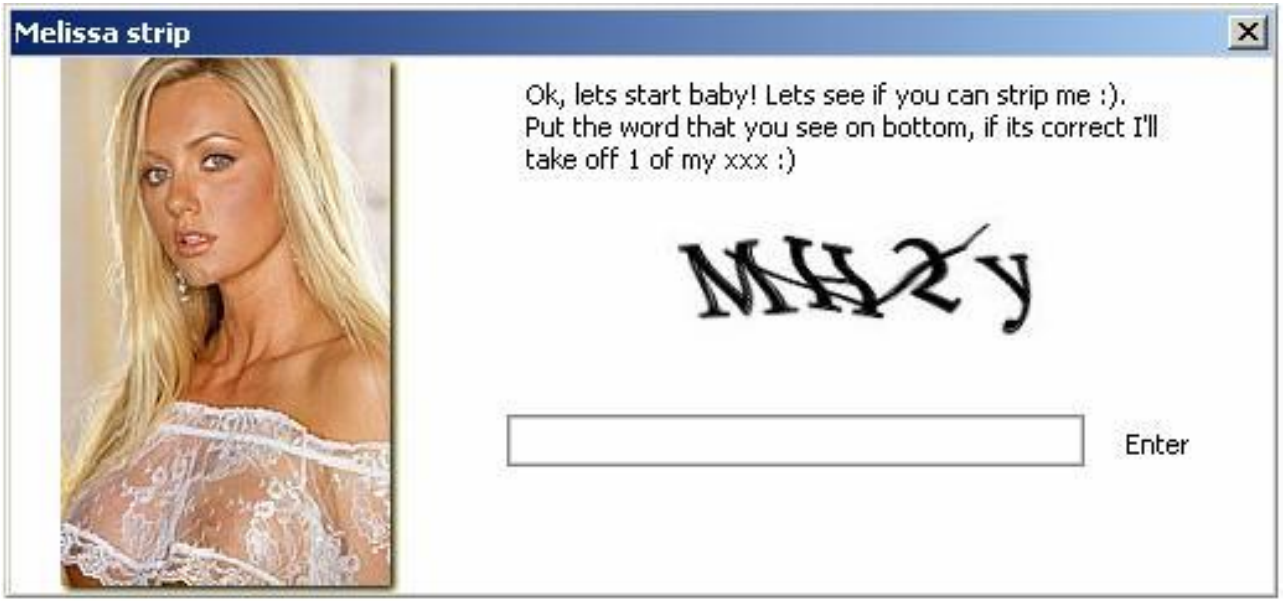


TREND MICRO™ 20 1988-2008 ANNIVERSARY

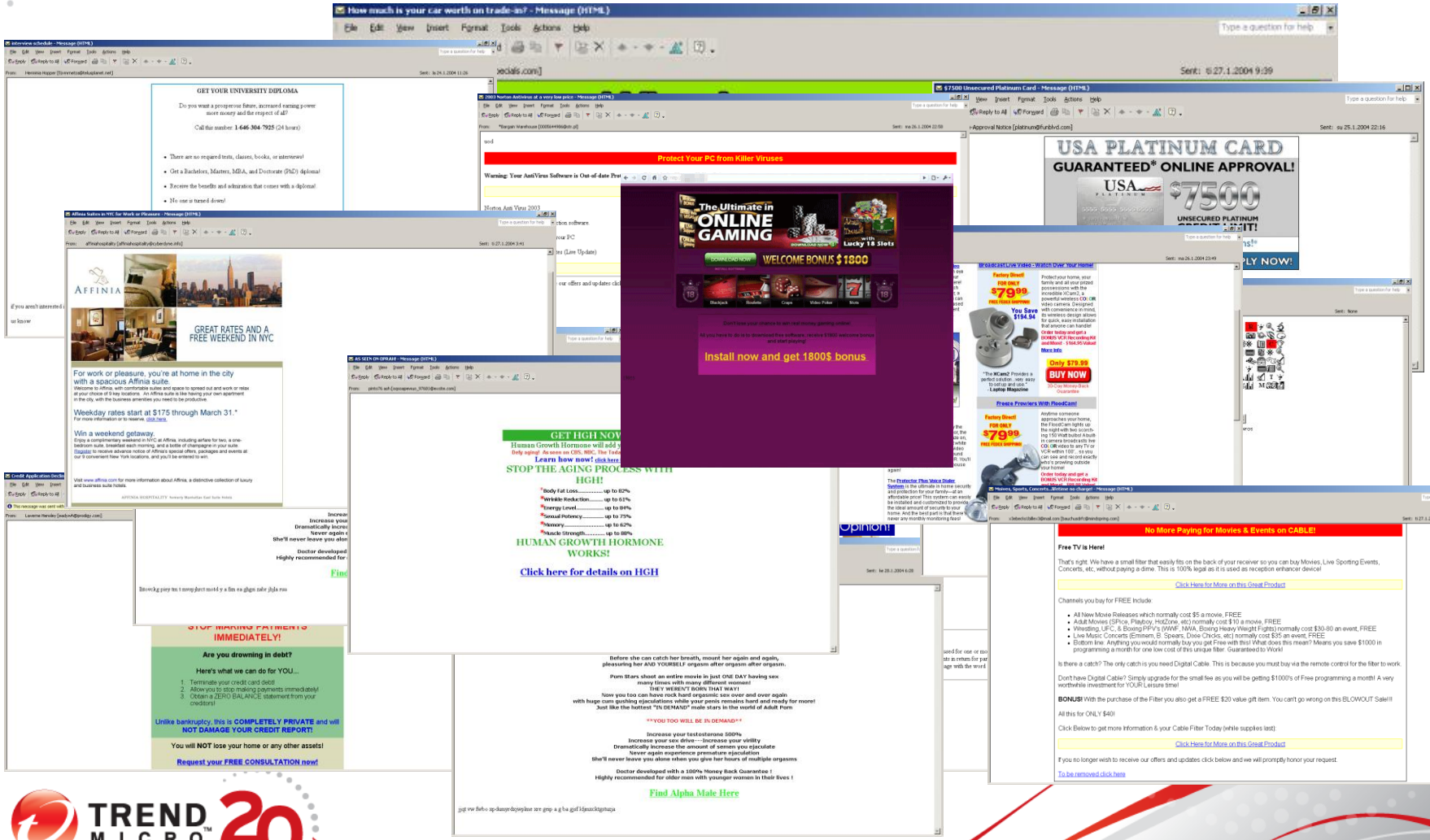
Handy Internet tool?



Type the CAPTCHA and strip the lady...

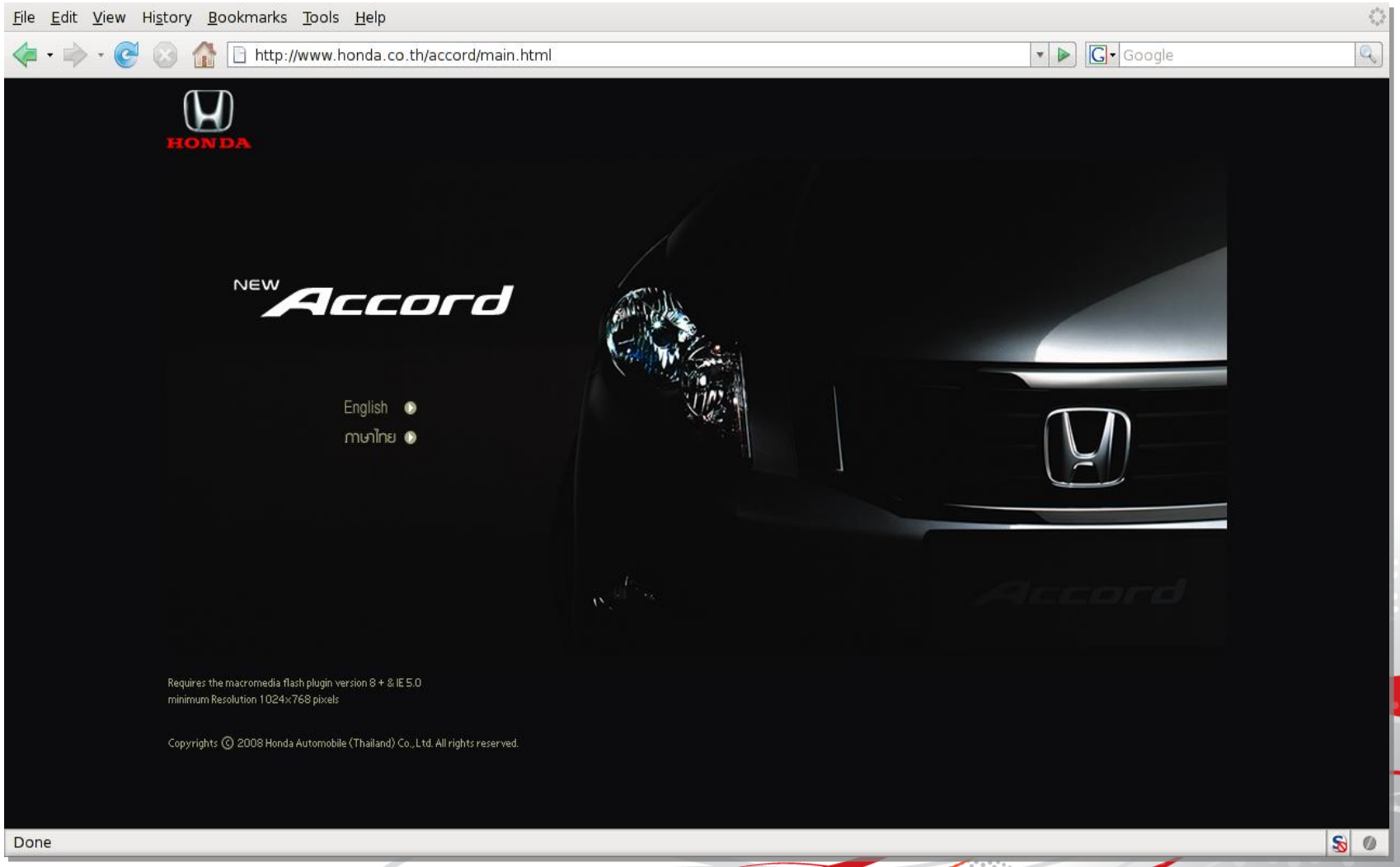


...and tons of more



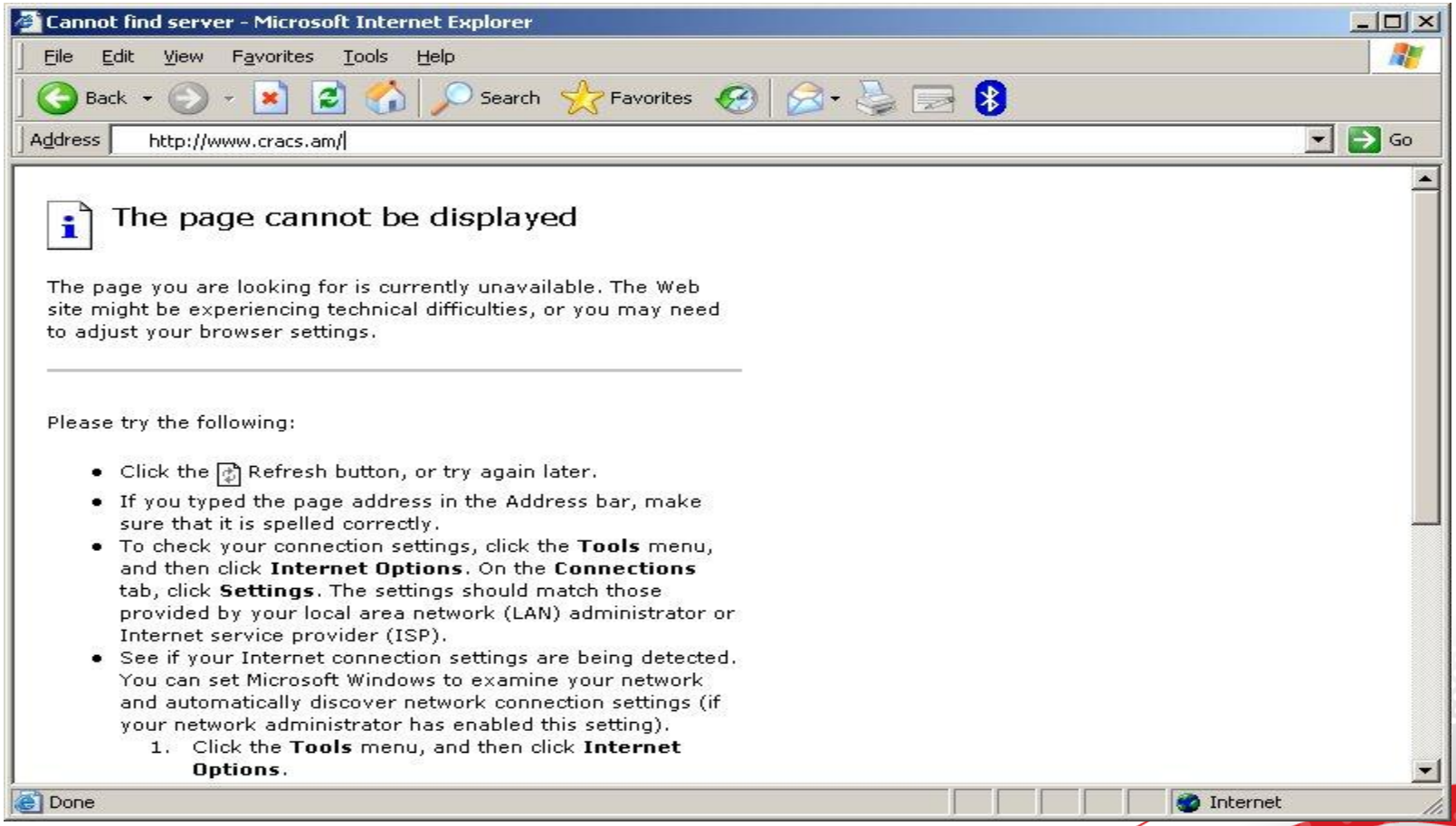
TREND MICRO™ 20 1988-2008 ANNIVERSARY

So what is wrong with this one?



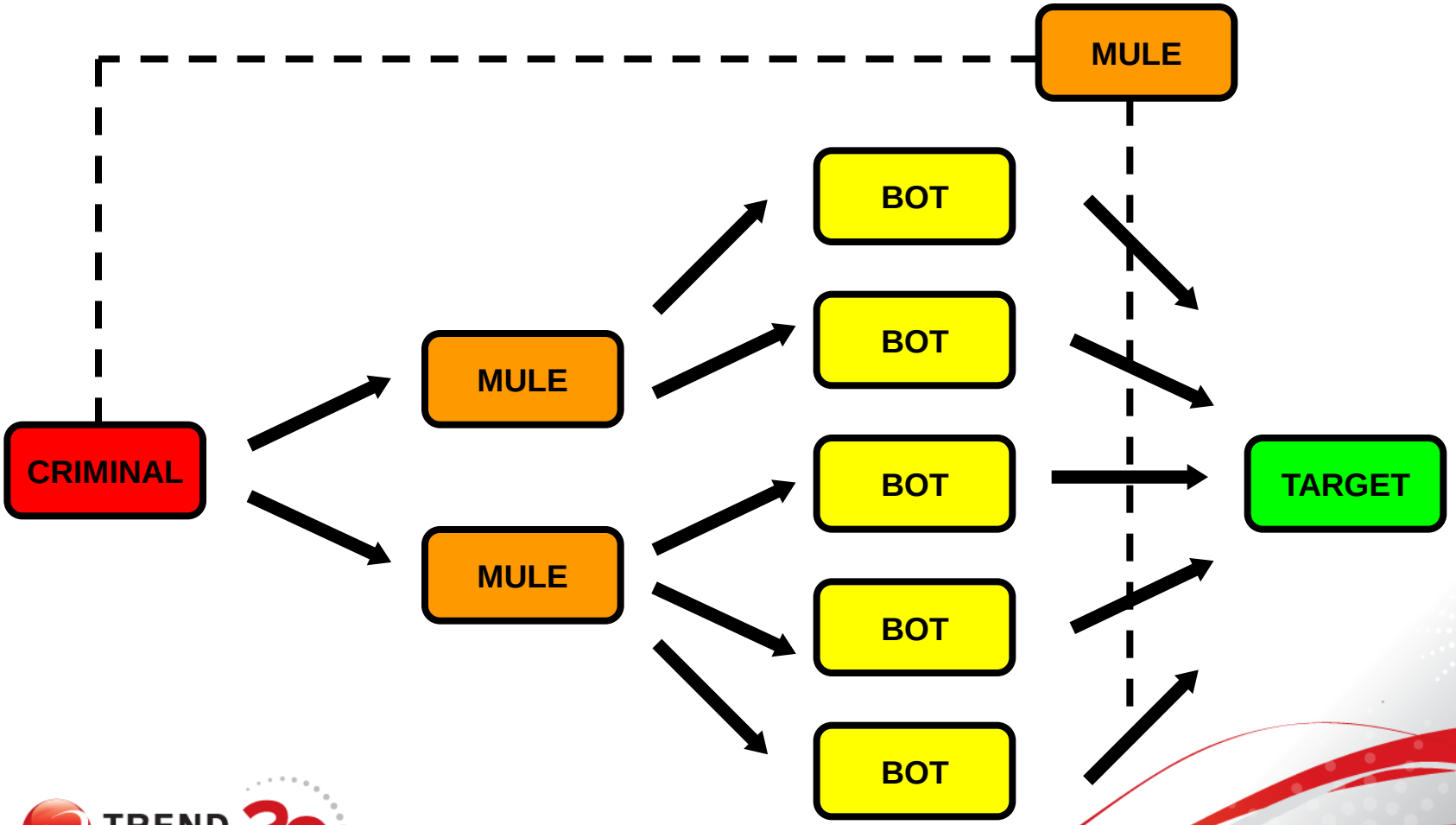
Web infiltration

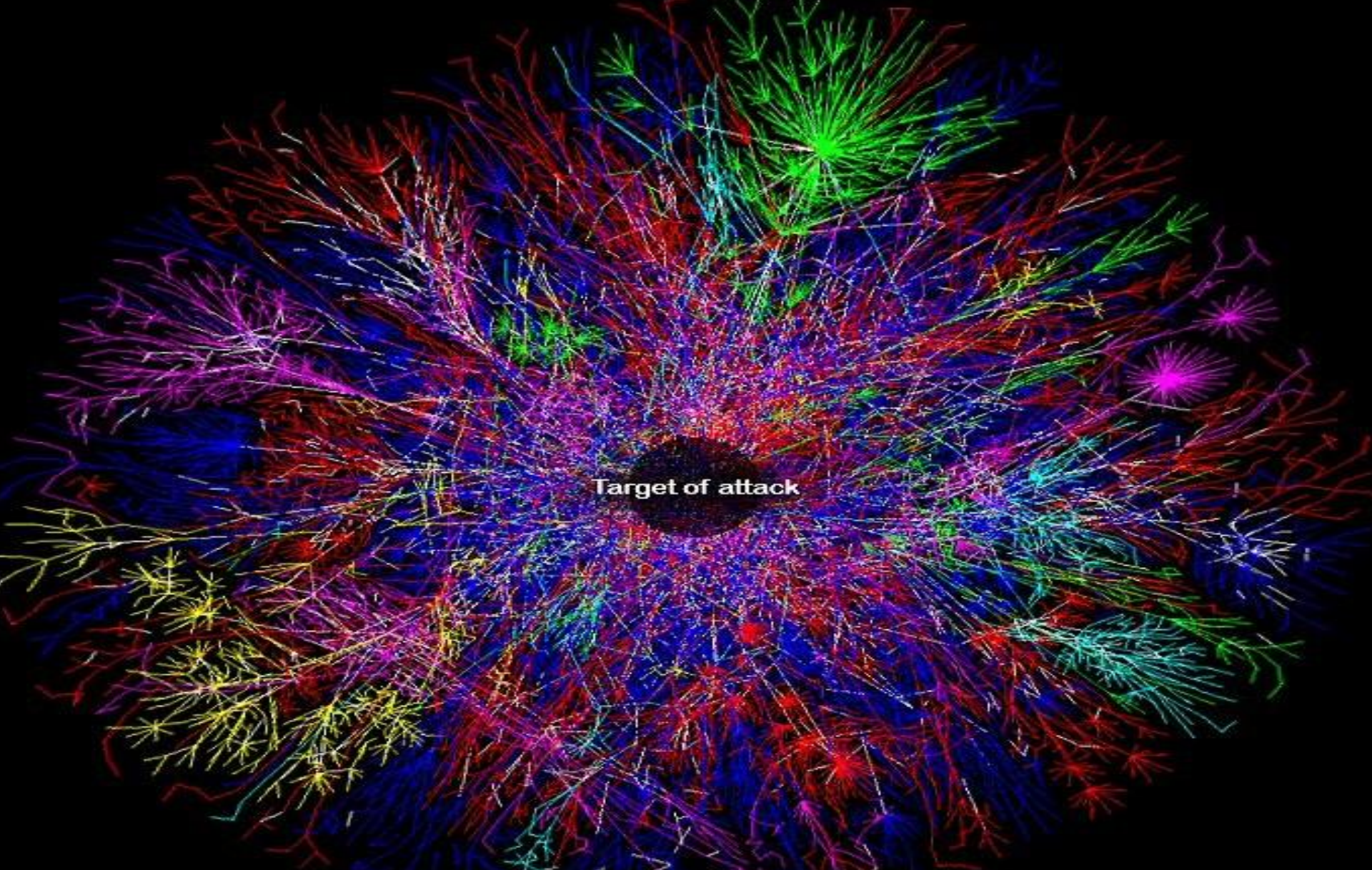
How about this?



TREND MICRO 1988-2008 20 ANNIVERSARY

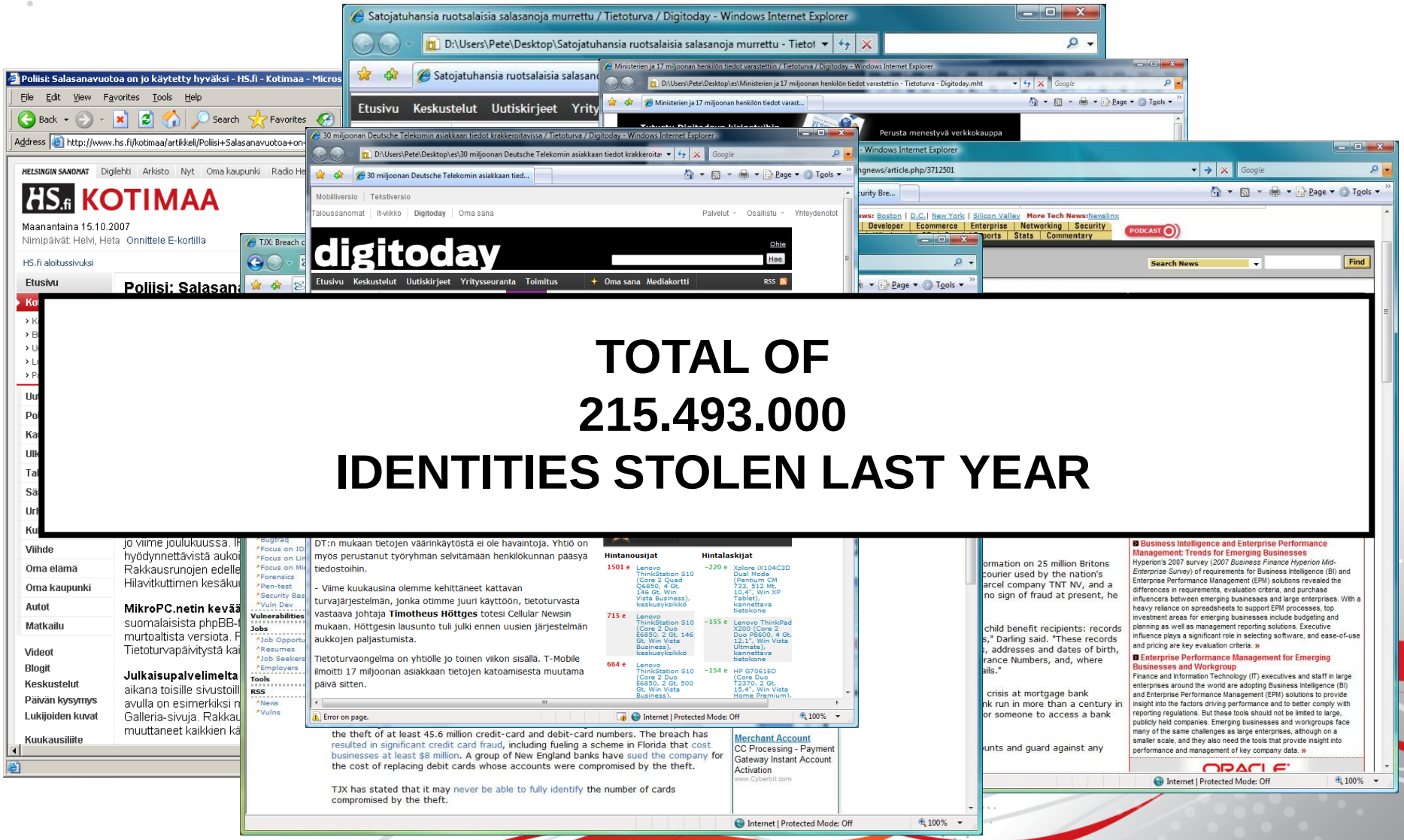
Growing amount of botnets





Today's botnets are attacking with the power of over 1.5 million nodes

Identity thefts



***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)

A spyware application has been detected and Windows has been shut down to prevent damage to your computer

SPYWARE.MONSTER.FX_WILD_0x00000000

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure your antivirus software is properly installed. If this is a new installation, ask your software manufacturer for any antivirus updates you might need.

Windows detected unregistered version of Antivirus 2009 protection on your computer
If problems continue, please activate your antivirus software to prevent computer damage and data loss.

*** SRV.SYS - Address F73120AE base at C00000000, DateStamp 36b072a3

Beginning dump of physical memory...

Physical memory dump complete. Restarting...

Microsoft®
Windows®xp

Your Antivirus 2009 copy is unregistered. Microsoft Security Center recommends you to activate your antivirus protection software.

Microsoft

Customized 0-day attack

- Rogue AV infections and 0-day attacks continue:
  - Displays fake BSOD that mentions the fake AV product
  - Displays fake reboot screen that has text
  - Both are actually screensavers
- Detected as TROJ_FAKEAV.SV

TREND MICRO 20 1988-2008 ANNIVERSARY

So let’s talk about the real criminals

TREND MICRO™ 20 1988-2008 ANNIVERSARY

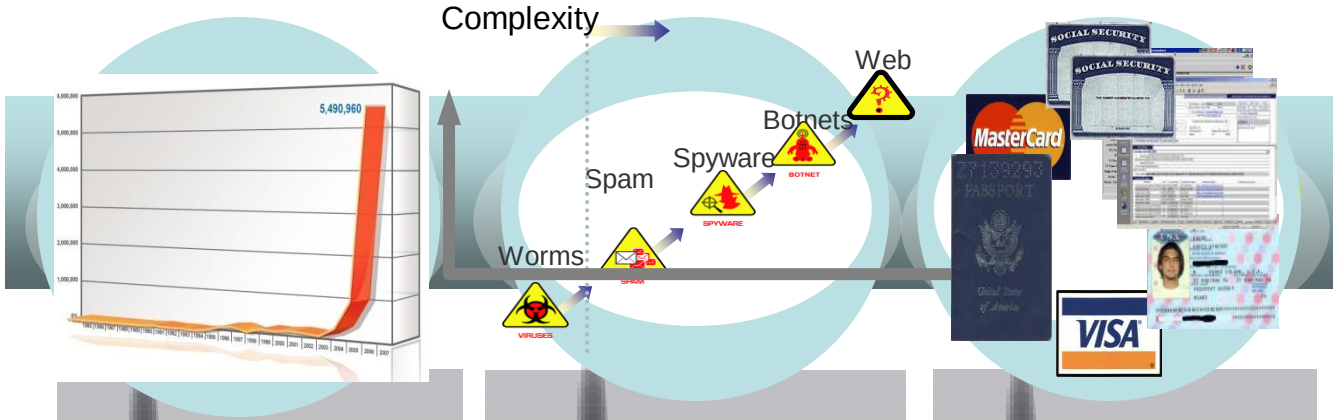
Bad Times are Good for Cybercrime

Other security companies, even the FBI, are one in saying that as global markets go down, cybercrime goes up:

- *McAfee, Inc. announced findings from its annual cyber security study in which experts warned that the recession is proving a hotbed for fraudulent activity as cybercriminals capitalize on a climate of consumer fear and anxiety.*
- *The underground economy is booming even as the rest of the economy lurches towards recession, according to a new study by Symantec.*
- *PandaLabs reported a direct correlation between the recent stock market declines and increases in targeted cyberattacks.*
- *"One thing we've seen is financially based cybercrime is recession-proof," says Darren Mott, supervisory special agent for the FBI's Cyber Division.*

The Evolving Threat Landscape

Malware is multiplying	Malware is sophisticated	Malware is profit-driven



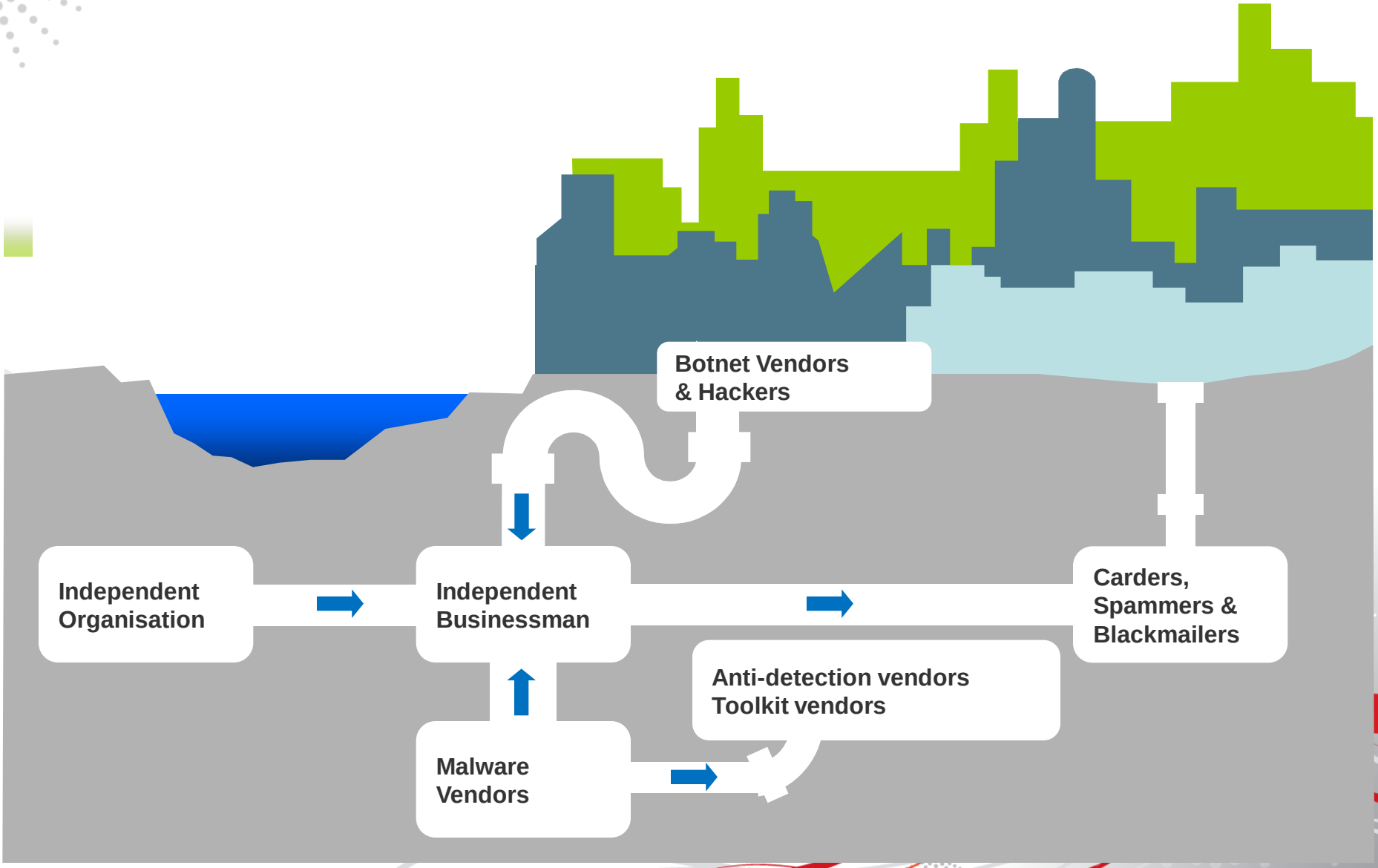
Malware samples
- 1988: 1738
- 1998: 177615
- 2008: 2,750,000 and up
- Pattern files can't keep up.

Malware variants
- Multi-vector
- Polymorphic
- Rapid variants
- Very hard to detect

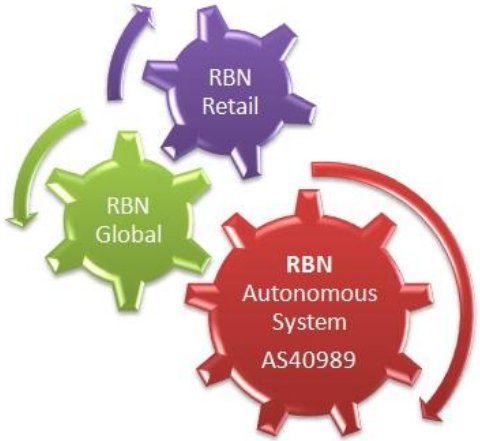
Malware actions
- Stealthy
- Targeted
- Crime & Espionage
- Increased liability costs

Malware is getting increasingly dangerous and harder to detect.

Economic structure of Cybercriminals

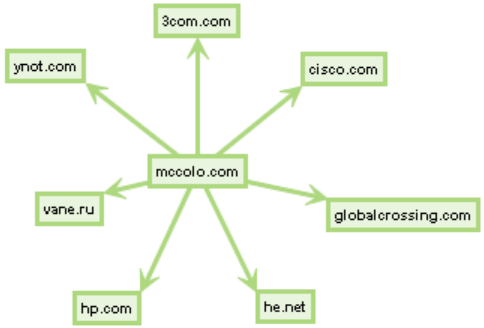


Criminal ISP's providing services for cybercriminals
Russian Business Network & McColo



"Unlike many ISPs that host predominately legitimate items, RBN is entirely illegal.

VeriSign iDefense research identified phishing, malicious code, botnet command-and-control (C&C), and denial of service (DoS) attacks on **every single server** owned and operated by RBN."



McColo was an Internet service provider providing service to malware and botnet operators.

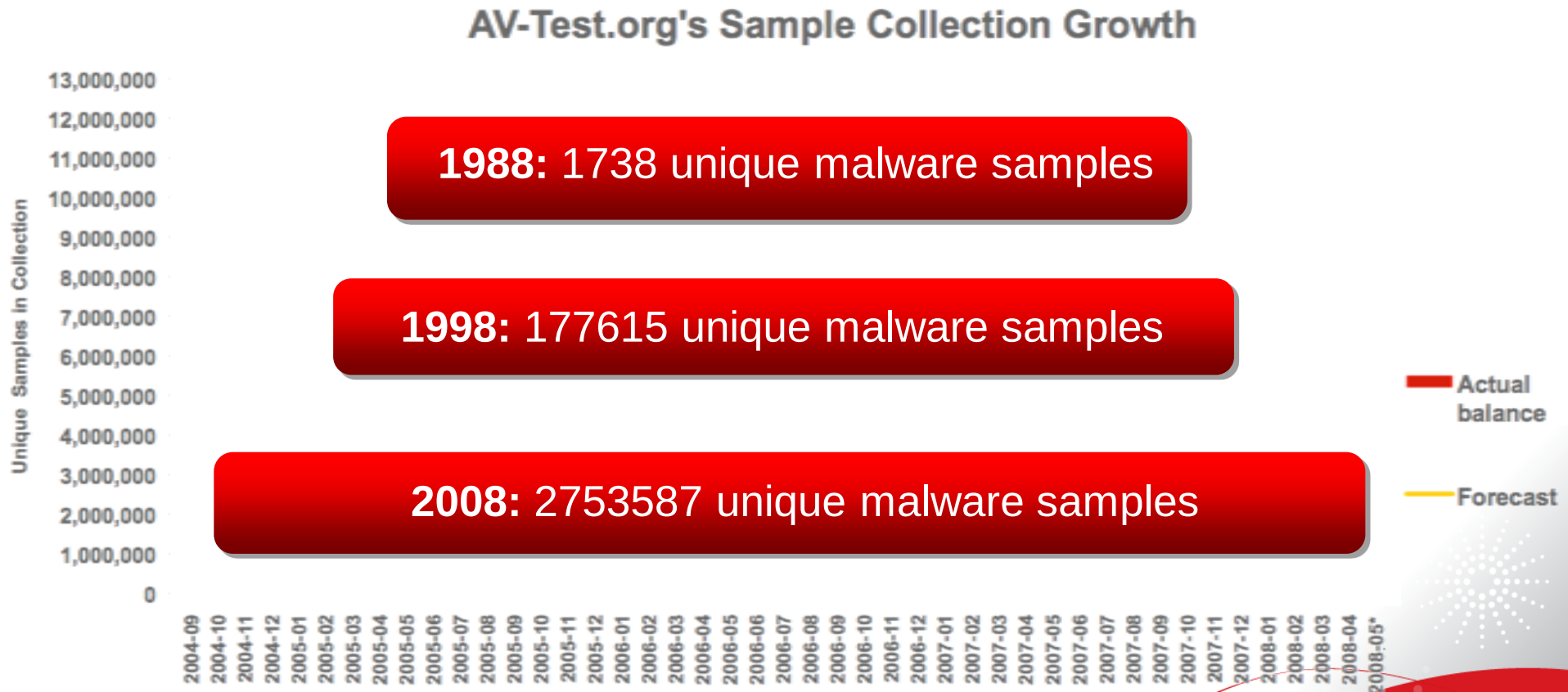
McColo customers were responsible for a substantial proportion of all email spam then flowing and subsequent reports claim a **two-thirds** or greater reduction in **global spam volume**

TREND MICRO 1988-2008 20 ANNIVERSARY

Customized malware is cheap

Pay-out for each unique adware installation	30 cents in the United States, 20 cents in Canada, 10 cents in the UK, 2 cents elsewhere
Malware package, basic version	$1,000 – $2,000
Malware package with add-on services	Varying prices starting at $20
Exploit kit rental – 1 hour	$0.99 to $1
Exploit kit rental – 2.5 hours	$1.60 to $2
Exploit kit rental – 5 hours	$4, may vary
Undetected copy of a certain information-stealing Trojan	$80, may vary
Distributed Denial of Service attack	$100 per day
10,000 compromised PCs	$1,000
Stolen bank account credentials	Varying prices starting at $50
1 million freshly-harvested emails (unverified)	$8 up, depending on quality

Increase in unique malware samples



1988: 1738 unique malware samples

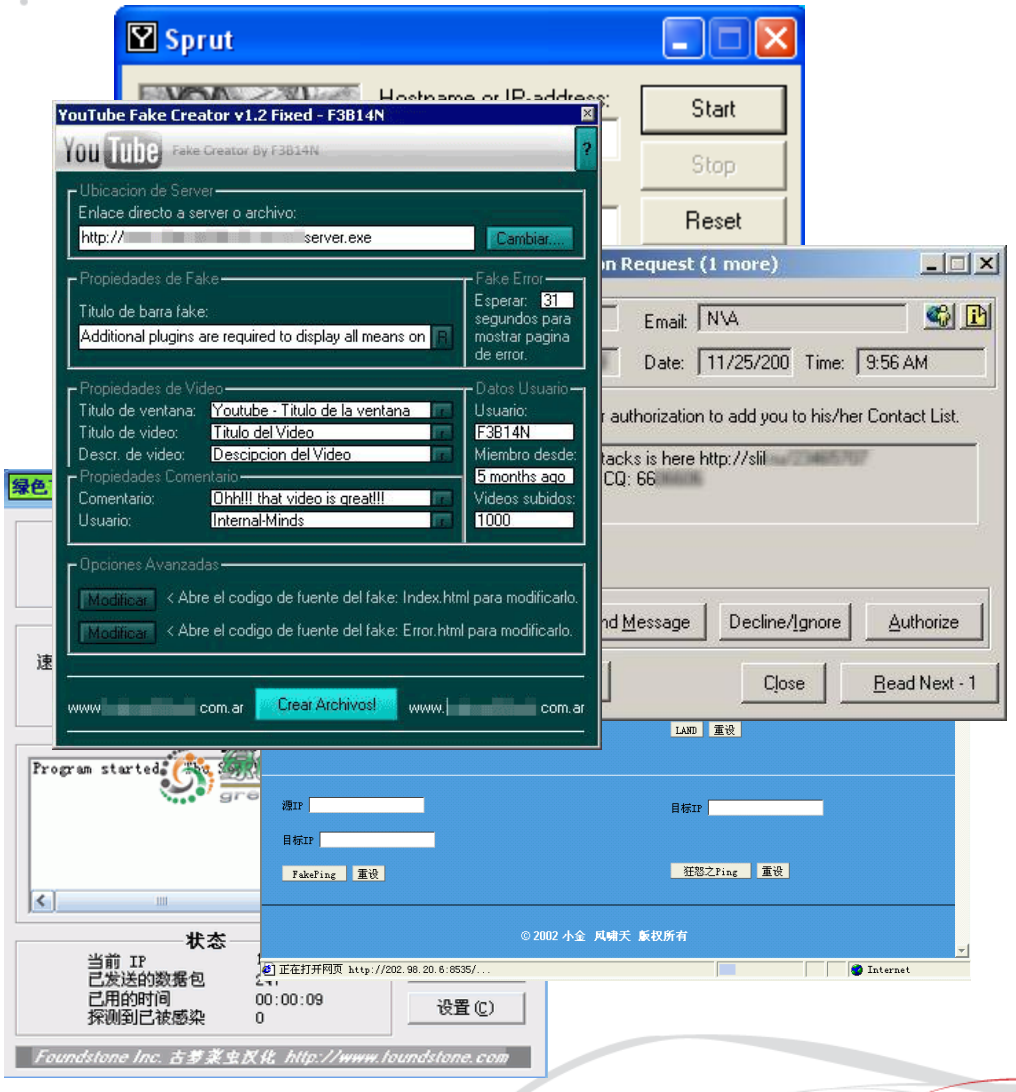
1998: 177615 unique malware samples

2008: 2753587 unique malware samples

Data source: AV-Test.Org, June 2008

TREND MICRO 1988-2008 20 ANNIVERSARY

Simple tools are crashing huge organizations

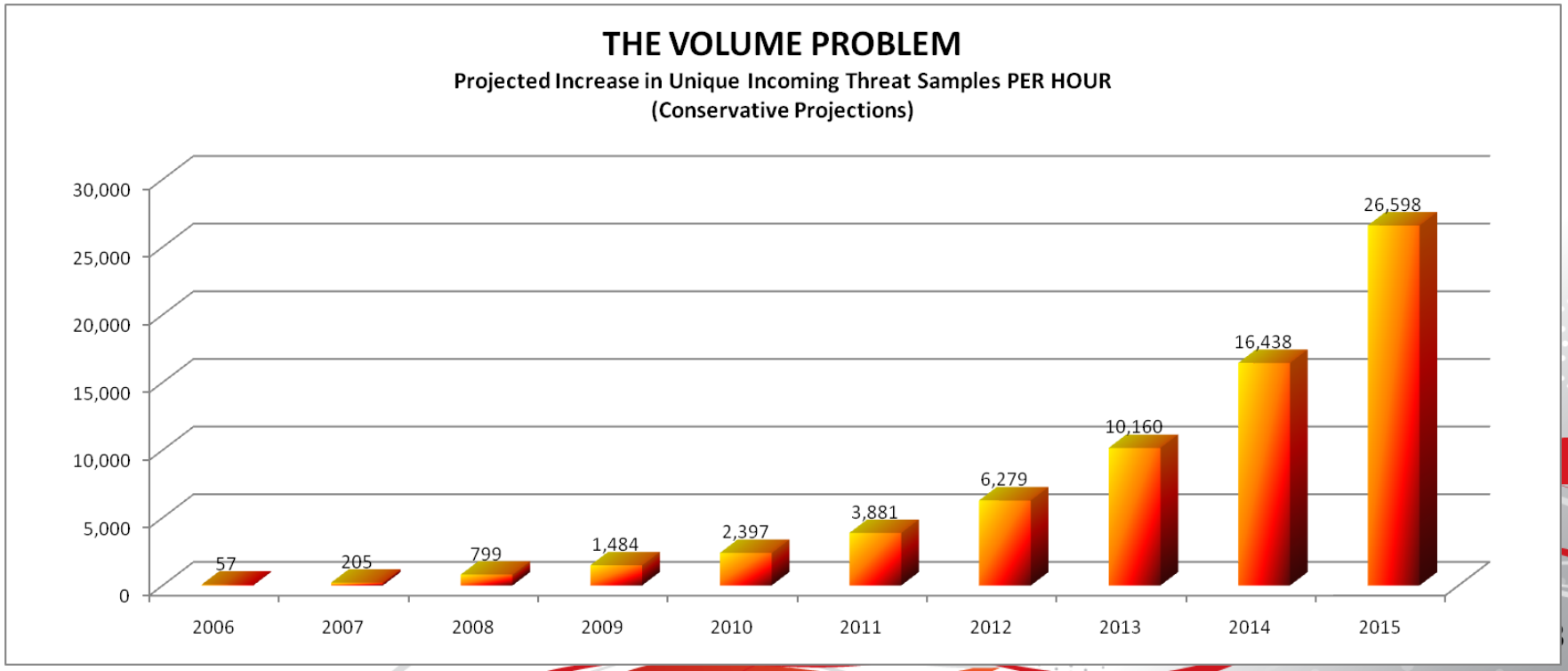


- eBay, 1999
- Yahoo, 2000
- CNN, 2000
- Microsoft, 2002
- Alabama Power Plant, 2006
- DNS root servers, 2002, 2007
- Swedish Police, 2007
- Estonian Government, 2007
- Finnish National Radio, 2007
- Eniro Finland and Sweden, 2007
- CERT-FI, 2007
- Google, YouTube, 2008

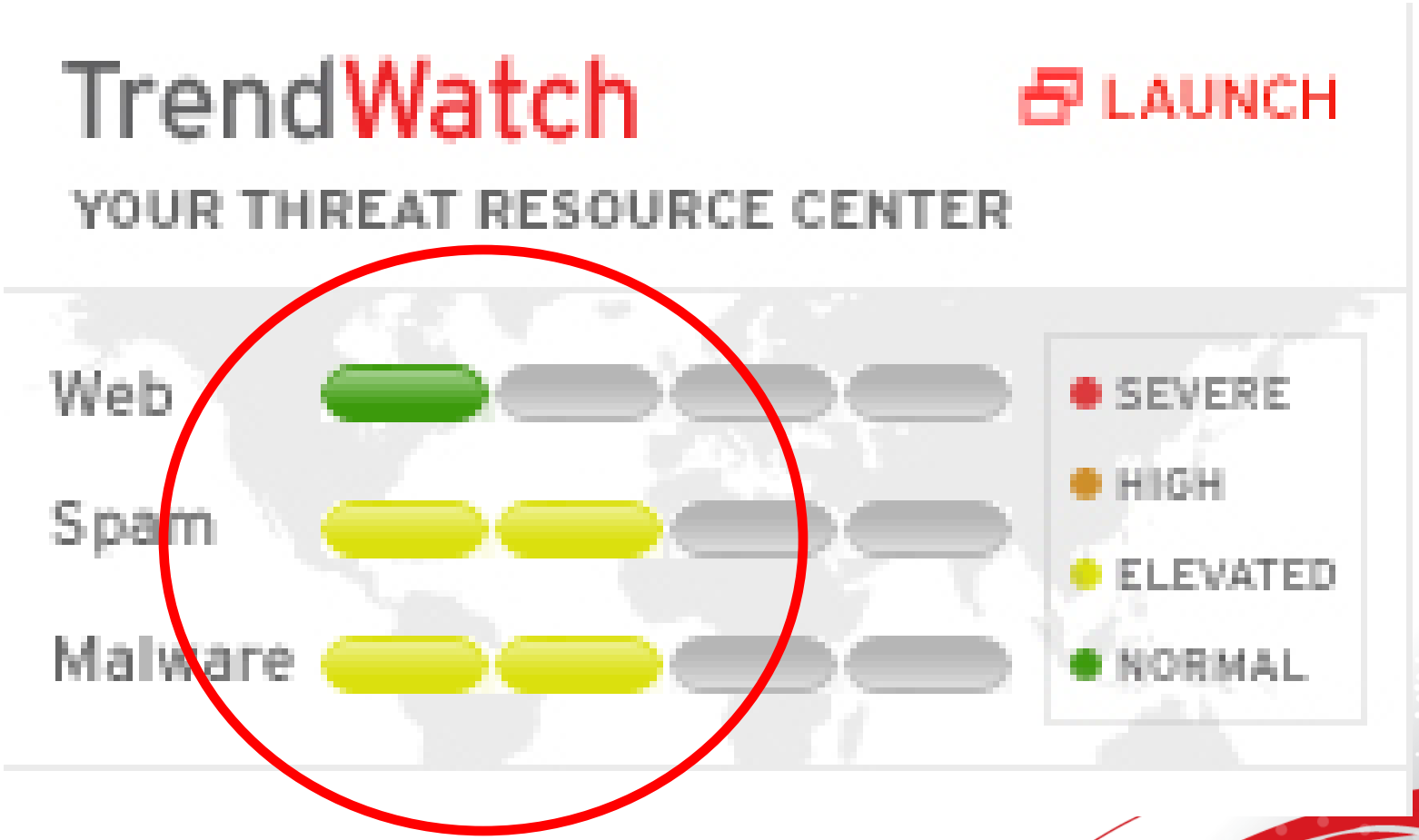
Security Challenge: Dramatic Increase in Number of customized Malware Samples

- If the volume of threats continues to increase at the current rate, 233,000,000 will be the number of unique threats that emerge in 2015 alone. Endpoint systems will need to be aware of over 26,598 new threats per hour in order to be effectively protected.

A CHANGE OF OUR THREAT HANDLING INFRASTRUCTURE IS REQUIRED!



Crimeware ...last 3 days



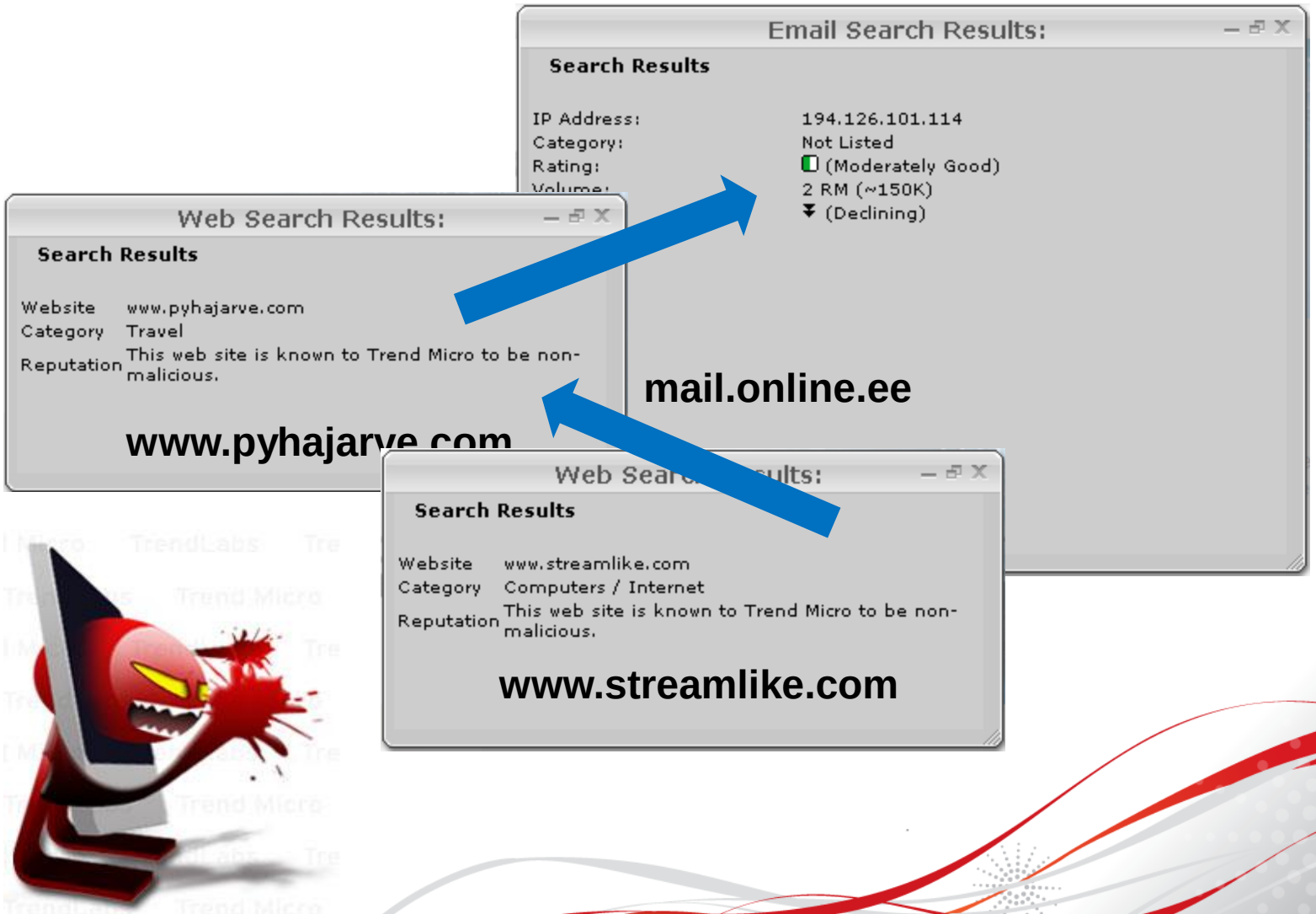
Forget the heavy fingerprints and inaccurate heuristics

…it's the reputation: Powered by Smart Protection Network

- **Processes over 50 million URL's per day**
- **Over 1.2 terabytes of new data per day**
- **More than 1500 security researchers**
- **Receives over 5 billion requests per day**
- **Operates 24/7 in 10 datacenters**

Web and E-mail Reputation sample

Provided by Trend Micro Smart Protection Network



In real time!

Provided by Trend Micro Smart Protection Network

- What's the current cybercrime situation
- Wich ISP's are hosting the most amount of spam and botnets
- What are the TOP 10 threats?
- Which countries are sending the most of spam?

Plan a your requirements well

...and remeber that the cheapest is not necessarily the best!