commtouch®
Real Security. In Real Time.

Spam and the Anti-Spam Technological Environment

Oren Drori – Director of Product Marketing

Spam – Who Needs It?

1970: Monty Python's Flying Circus

'Spam' sketch

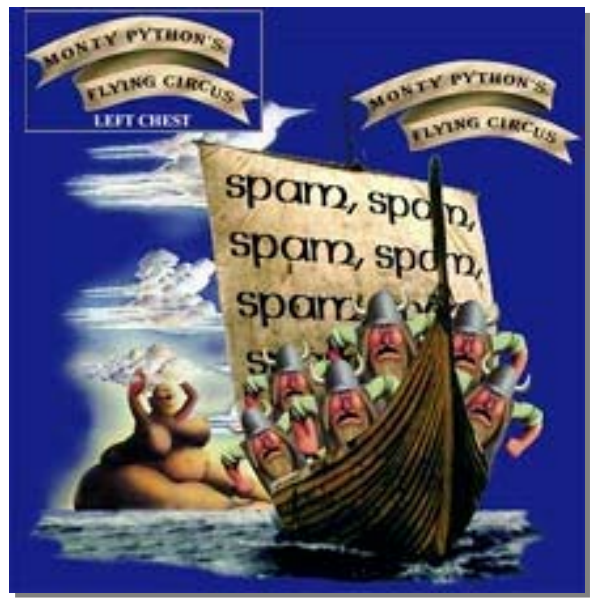
1978: First mass e-mailing

(Everyone with an e-mail got it!)

1994 First Unsolicited Commercial E-mails (UCE)

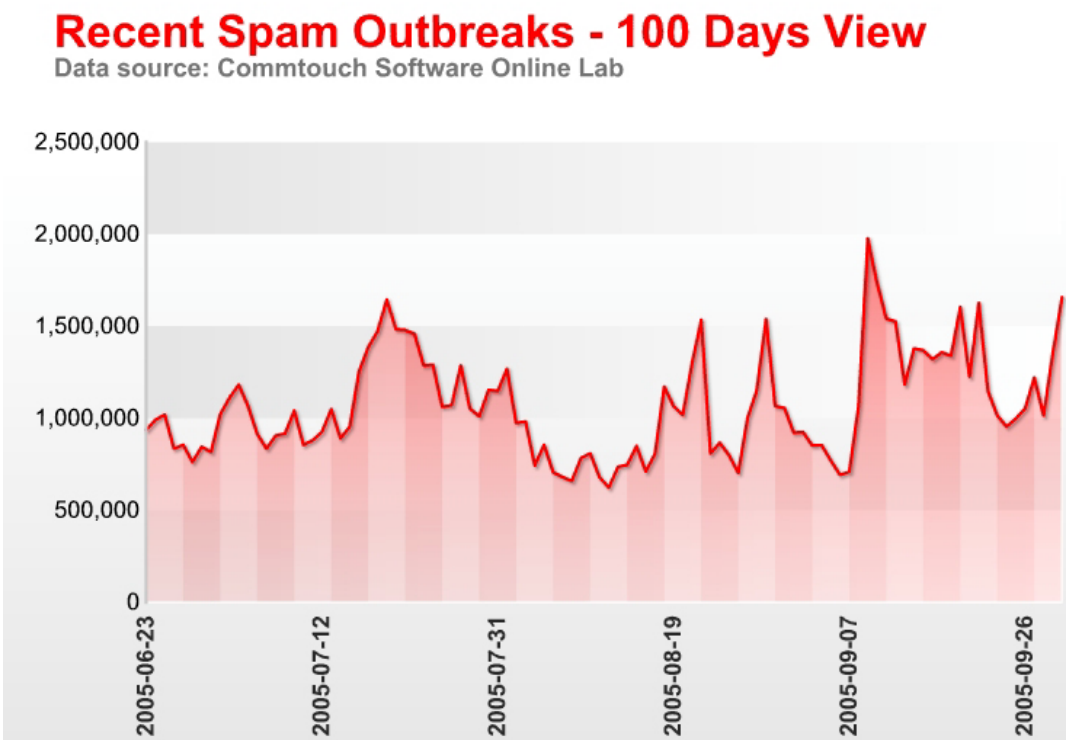
1st - Green card lottery applications

2nd - "Global Alert for All: Jesus is Coming Soon"



… 10 Years Later

- **25 Billion** spam messages distributed daily
- **60%** of global email is spam
- **80%** for some corporations …
- **600K - 2 Million** outbreaks a day



commtouch®
Real Security. In Real Time.

- **Who are these people?**

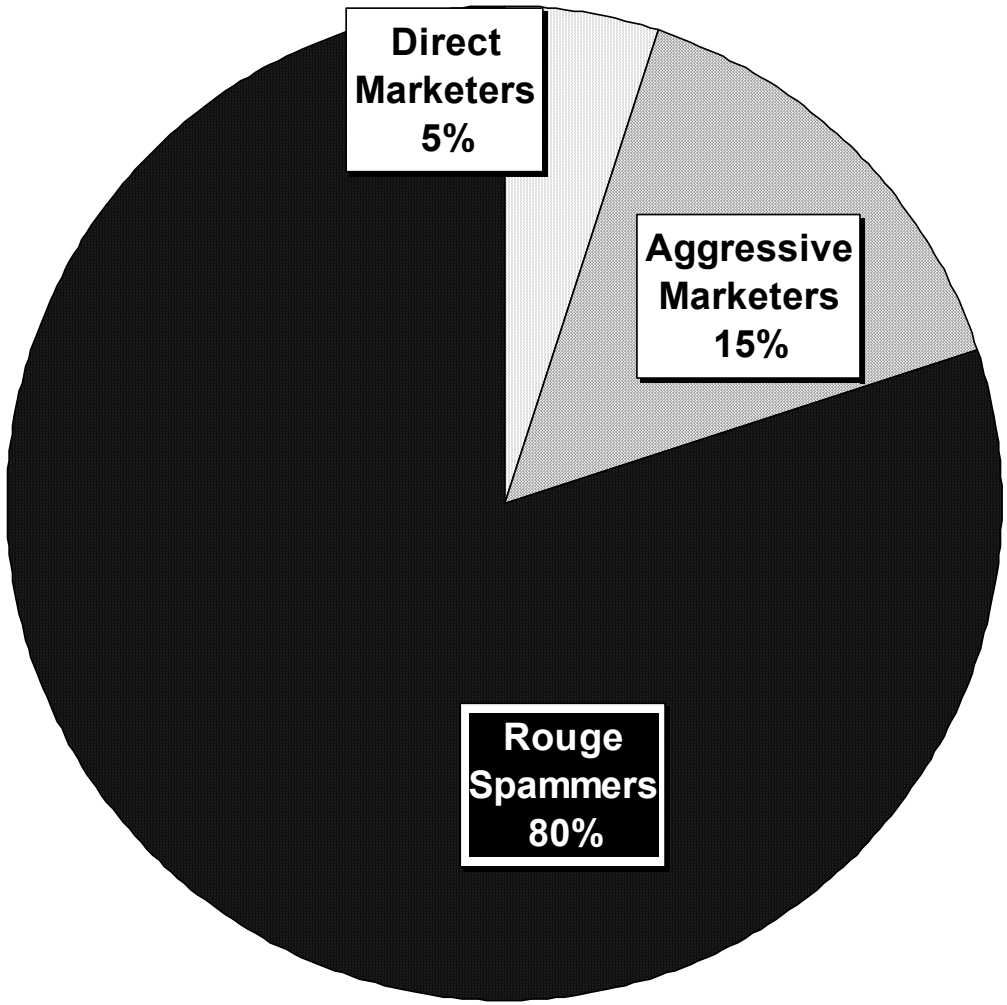
"In a perfect world... Spammers would get caught, go to jail, and share a cell with heavy men who have enlarged their penises, taken Viagra and are looking for a new relationship."

Friendly wishes, posted at Bash.org

Who Are The Spammers?

'Pure' DLs	Direct Marketers	Aggressive Marketers	Rogue Spammers	Organized Crime
Informative content	**Main stream products**	**Borderline legit Products**	**Anything goes…**	**Tendency to criminal action**
Opt-in Opt-out	**Opt-in Opt-out (-)**	**No opt-out Address-trading**	**• Addresses harvesting • Trojans**	**• Financing hackers**
"Victims" of Anti-Spam Efforts	**Legislation: Limited relevancy**		**Spam legislation - irrelevant**	

The Criminalization of Spam



commtouch®
Real Security. In Real Time.

- **Spam-Malware Convergence**

Spam Technology Becomes Vehicle For Viruses

Figure 1-A: Typical viral propagation

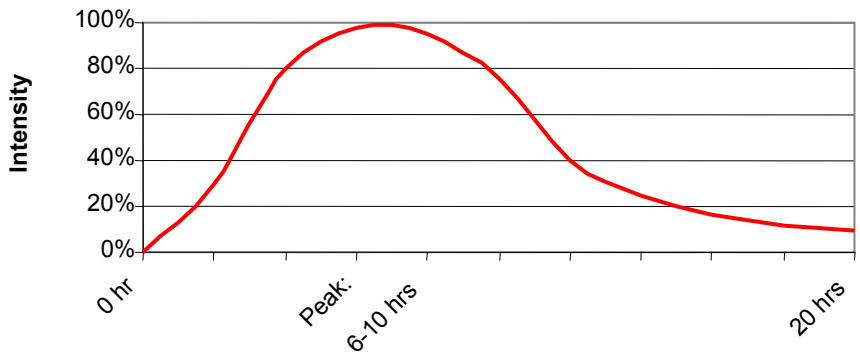
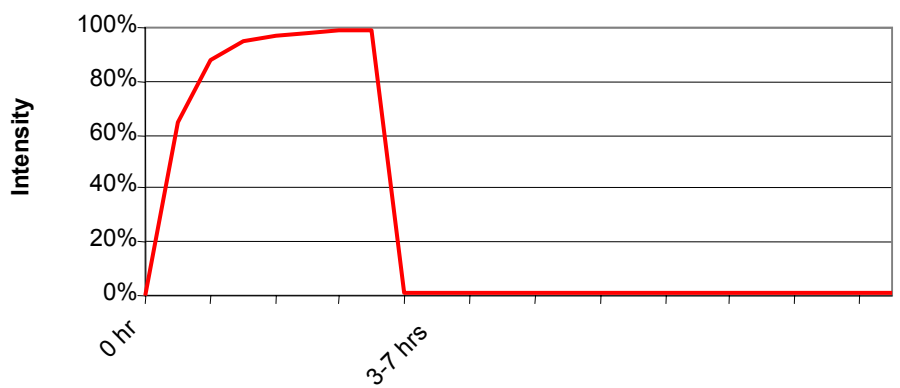


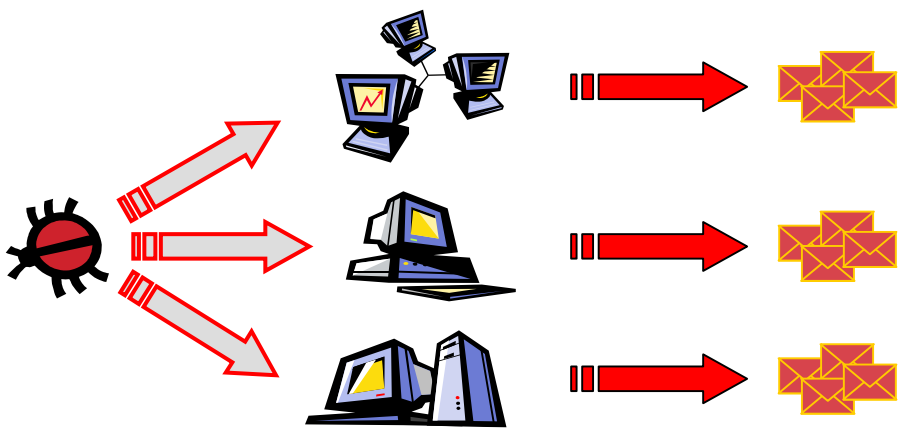
Figure 1-B: Short Span attack



Malware Techniques Used By Spammers

Step 1: planting multiple Trojans ('zombies')

Step 2: Dormant Trojans activated at once



Distribution Sources	1000s
Volume	+100M messages
Duration	1-3 Hours
1 Hour Detection Lag	30-100% miss

commtouch®
Real Security. In Real Time.

- **Inside The Spam-Can**

commtouch®
Real Security. In Real Time.

50 ways to spam Viagra

V I @ G R A , V--1.@--G.R.a, \./iagra, Viiagra, Vìagrä, V--i--a--g--r—a, V!agra, V1agra, VI.A.G.R.A, vi@gra, vIagr.a, via-gra, Via.gra, Vriagra, Viag*ra, vi-agra, Vi-ag.ra, v-iagra, Viagr-a, V^I^A^G^G^A, V'i'a'g'r'a', V*I*A,G,R.A, VI.A.G.R.A..., Viag\ra!, Vj@GRA, V-i:ag:ra, V'i'a'g'r'a, V/i;a:g:r:a, V i a g r @, V+i\a\g\r\a, Viag[ra, Víagra, V;I;A*G-R-A, V-i-a-g-r-a, V*I*A*G*R*A , V-i-@-g-r-a, VI@AGRA, , V\i\a.g.r.a, V1@GRA, v_r_i_a_g_r_a, V\i\a:g:r:a, V^i^a^g^r^a, V-i-@-g-r-@, Viag(ra……..

Handling Multiple Anti-Spam Filters

From: Nell Gomez [mailto:jjfwfasjcjsu@earthlink.net]
Sent: Wednesday, December 20, 2004 2:56 PM
To: !@#$%%$;
Subject: mammal coalition hugo antithetic postpone

Hi,

Genierc Viagrand Sepur Viarga (Caiils) available onlnie!
Most trsuted onilne source!

Vagira & Cilais
takes afefct right away & lasts 24-36 huors!

FOR SUEPR VAIRGA TOCUH HERE

Not itnreseted
cobweb deck nude cowherd contiguous execrable cretinous melange moldboard notice acapulco deject hydronium advisee malfunction diamagnetism iodate cremate holiday headstrong bluish flange bhoy shown antic alumnae galvanic
ethyl
aim g
nume
planc
pack

Fake Address

Take a close look: SUEPR VAIRGA subject

Positive Bayesian Values

'Typoglycemia' (Social Engineering):

Words identification regardless of letters order

commtouch®
Real Security. In Real Time.

‘Chinese Menu’

From: charmainea.richardsdl@no.org
Date: Sunday, September 18, 2005 11:42 AM
To:
Subject: hello John-J two girls waiting to meet you

It's ${quick|fast}, ${easy|simple} and ${anonymous|very private}.
Our ${dat.ing|matchin.g} ${system|portal} has taken live ${dating|matching}
to a ${whole new|much higher} level.

Now you can {meet|get to know} someone in ${seconds|nanoseconds},
${conversate|talk} to them and ${ensure|make sure} it's all ${that you like|by your taste}!

${Send|Give} them virtual kisses now and ${meet up|get together} the next day.
Why ${spend|be} another minute alone?
${Check|Visit} us here, join the real fun!

http://www.hockeyhicks.com/extra/gettingitgood/

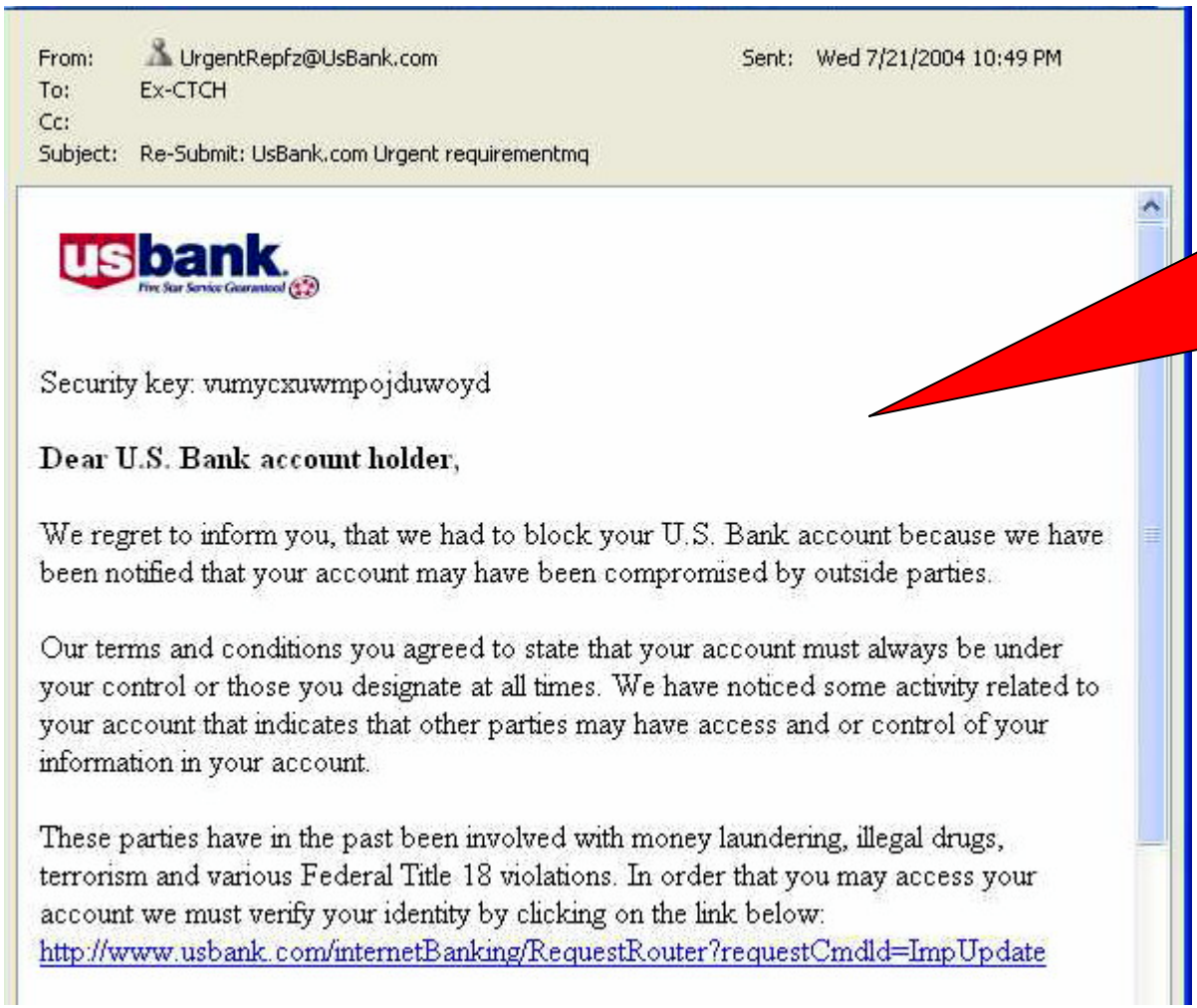
- **2^16 = 65,536 permutations**

… for simple message

… using legit vocabulary only

… and proper grammar

Phishing



From: UrgentRepfz@UsBank.com Sent: Wed 7/21/2004 10:49 PM
To: Ex-CTCH
Cc:
Subject: Re-Submit: UsBank.com Urgent requirementmq

usbank
Five Star Service Guaranteed

Security key: vumycxuwmpojduwoyd

Dear U.S. Bank account holder,

We regret to inform you, that we had to block your U.S. Bank account because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

These parties have in the past been involved with money laundering, illegal drugs, terrorism and various Federal Title 18 violations. In order that you may access your account we must verify your identity by clicking on the link below:
http://www.usbank.com/internetBanking/RequestRouter?requestCmdId=ImpUpdate

If you cannot tell the difference …

… your content filter can't either

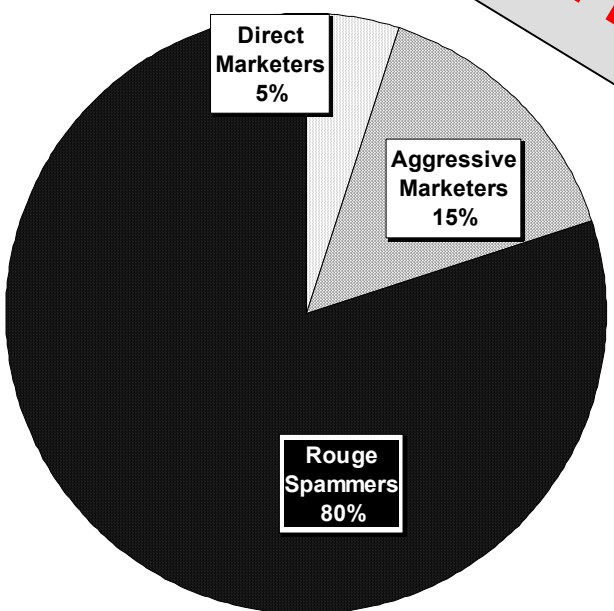
commtouch®
Real Security. In Real Time.

- Non- Commercial Attempts
  Limited Success

92 Laws And Acts In US and Europe

- D…challenge
- Inter…allenge
- Enforceme…e

Irrelevant



US Federal Laws	**4 Proposals 1 Enacted**
US State Laws	**Over 40**

European union	10
Austria	3
Belgium	1
Czech Republic	3
Denmark	4
Finland	4
France	2
Germany	3
Greece	1
Ireland	1
Italy	3
Luxemburg	1
Netherlands	1
Norway	3
Portugal	1
Spain	1
Sweden	3
UK	3
Total European Anti-spam Laws	**48**

Public Blacklists – "Let's Block Spammers"

- **Impact:**
  - **Wide adoption**: all email servers, most ISPs
  - **Effective for**: fighting open-proxies ('killed' them)

- **Didn't work against spam:**
  - Complaints based - not real time
  - Ineffective against dynamic sources
  - Most spam is sent by zombies (via ISPs)

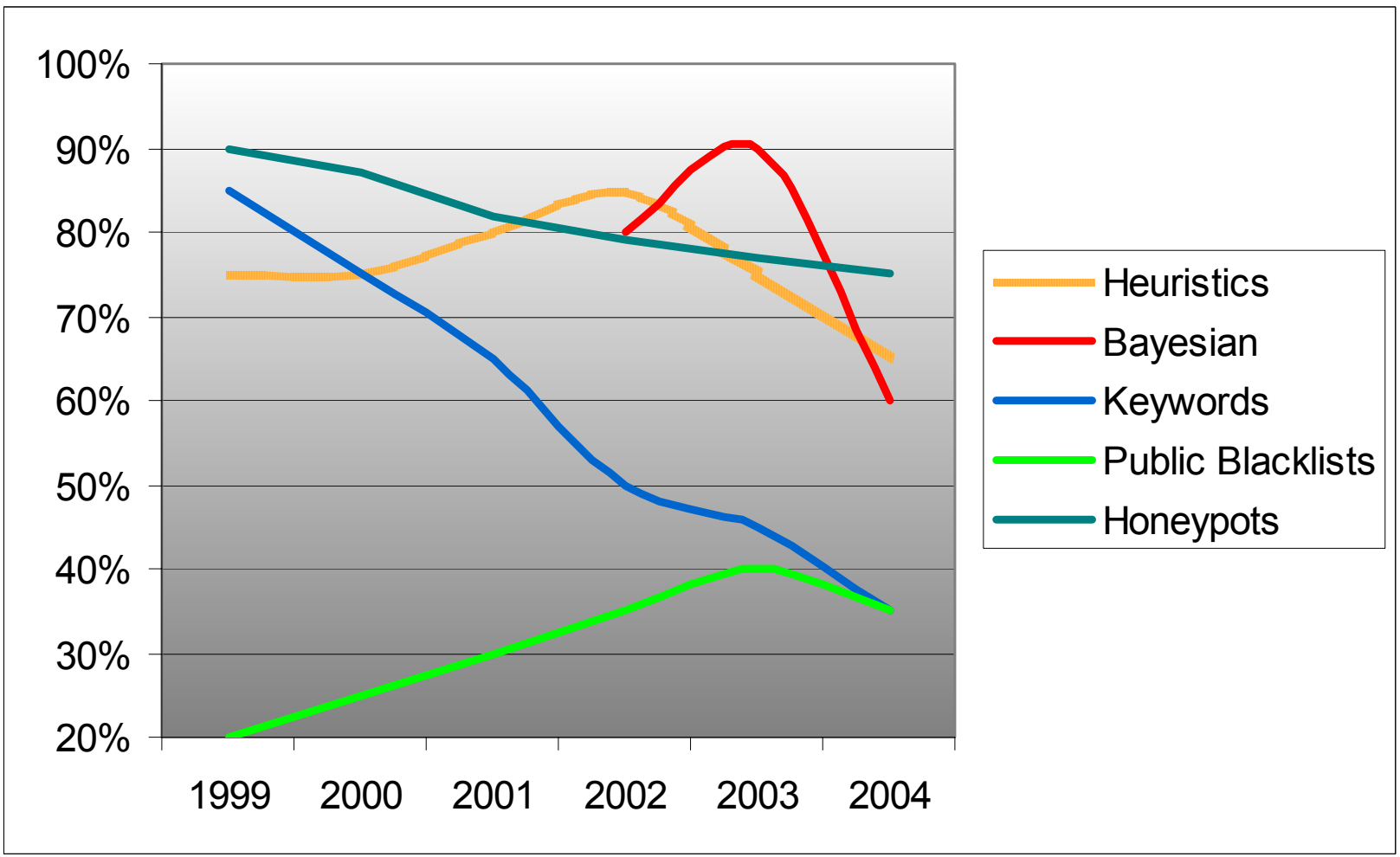
Internet Standardization

- **Bill Gate's "Penny Black" Initiative**
  - "We'll make spammers pay" – 1c/Email
  - Drawbacks: lots of 1c's …
  - Impact so far: Some media coverage…
- **SPF/Sender-ID, DKIM Initiatives:**
  - Goal: improving sender identification & authentication
  - Will enforce spammers to change tactics

commtouch®
Real Security. In Real Time.

- **Commercial Solutions**

Research-based / Reactive Solutions



commtouch®
Real Security. In Real Time.

"Cocktail Solutions"

- **Pro**
  - Manage to achieve results
  - Harder for spammers to manipulate
- **Cons**
  - False positives challenge
  - Expensive maintenance to the vendor
  - Always need more layers

Barracuda Spam Firewall … ten defense layers:

- IP block list
- Rate control
- User-specified rules
- Spam fingerprint check
- Intention analysis
- Bayesian analysis
- Rule-based scoring

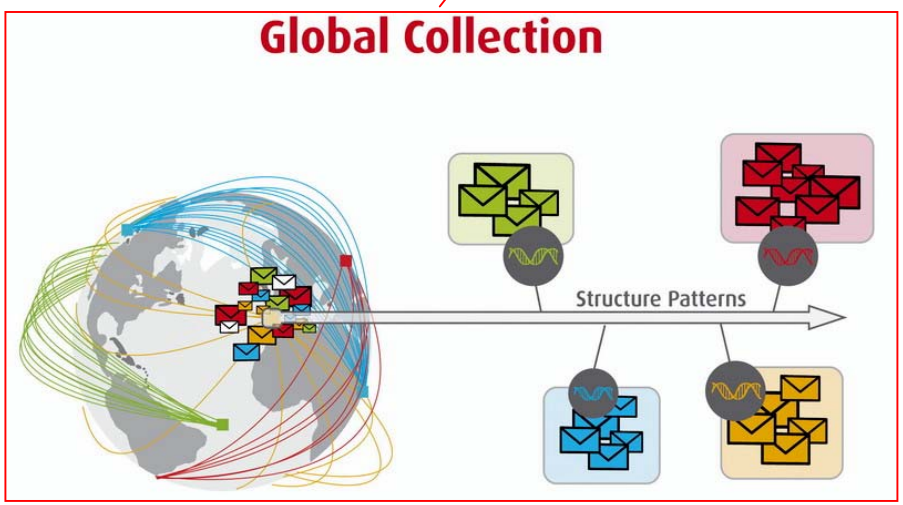
"… over **17 different technologies** … heuristics, reputation, language ID …" – **Symantec Brightmail**

Network Based Approach

- **Security vendors:**
  Microsoft-Sybari, Mirapoint, Tumbleweed, Ironport, Proofpoint, Commtouch …
- **Large MSPs:** Messagelabs, Frontbridge…
- **Open source:**
  DCC – Distributed Checksum Clearinghouse

Outbreak Detection

Patent #6-330-590



Additional Benefits

- **Effective against all outbreak-type threats – Spam, Phishing, Mass-mailing Malware**

- **Zero-Hour Virus Protection**
  - **Signature Independent**
  - **Heuristic-less**

commtouch®
Real Security. In Real Time.

Thank You

Oren Drori
orend@commtouch.com

First Spam (1978, To All Arpanet Users)

Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT
Date: 1 May 1978 1233-EDT
From: THUERK at DEC-MARLBORO
Subject: ADRIAN@SRI-KL

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS. WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH.

THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

commtouch®
Real Security. In Real Time.

Spam & Organized Crime

Organized crime may be behind phishing; Fraudulent e-mail scams show more sophistication
Saul Hansell, New York Times,
Monday, March 29, 2004

Organized crime invades cyberspace
Dan Verton — Computerworld
Monday August 30, 2004

Is Organized Crime Controlling Your PC?
Symantec report says Internet attacks for financial gain on the rise
Samantha Perry, PC-World
Monday, September 27, 2004

Online organized crime
Internet criminals want your money and their tactics are becoming increasingly refined and organized.
CNN, Monday, September 26, 2005