Evolving email threats and counter technology

James Todd IronPort Systems

IRONPORT™

Agenda

- The State of SPAM
- New Spamming Techniques
- Predicative Security
- Rebuilding Trust in Email

IronPort

“Zombies” Execute Email Attacks

SEARCH

Microsoft sees botnets as top '07 Net threat

Undead PC armies 'where it's at for serious cybercriminals'

Robert McMillan Today's Top Stories ▸ or Other Security Stories ▸

December 27, 2006 (IDG News Service) -- If there's one thing that Aaron Kornblum would like to quash, it's the botnet armies.

These are the remote-controlled PCs that have been taken over without their users' knowledge. Symantec Corp. counted more than 4.5 million of them during the first six months of the year, and according to Kornblum, they are the backbone of today's cybercrime.

"Botnets are really where it's at for serious cybercriminals, because of their concentrated power," said Kornblum, a senior attorney with Microsoft Corp.'s Internet Safety Enforcement team. "That power can be used for all sorts of malicious conduct on the Internet."

powered by YAHOO! GO

Tech Products

Products home

Edward C. Baig

Gaming

By Byron Acohido and Jon Swartz, USA TODAY

In the calculus of Internet crime, two of the most sought-after commodities are zombie PCs and valid e-mail addresses.

Viruses are Becoming More and More Dangerous . . .

- 70% of all spam comes from virus infected PC zombies
- 75% of all viruses contain spam delivery engines
- 200% increase in spyware delivered by email in the past 6 months
- 65% increase in keystroke loggers in 2005
- 200% increase in rootkits

IRONPORT

What's changed

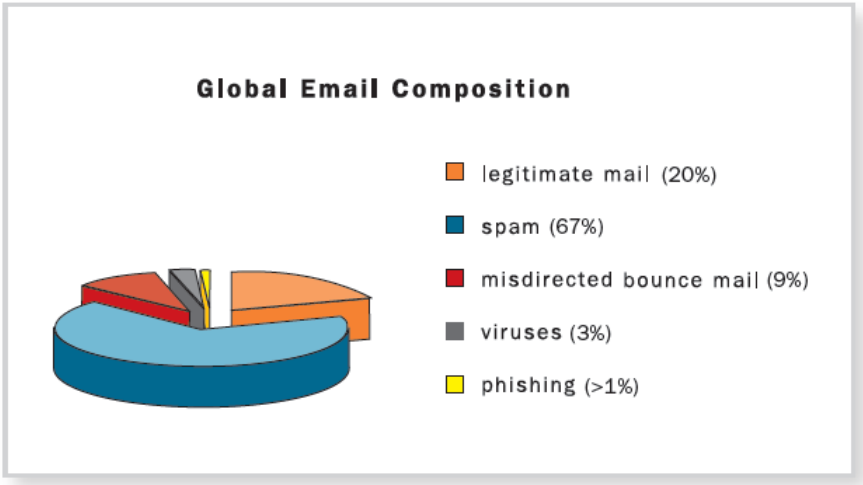
- Old Days
  - Hacking for fame, fun or profit
  - Script Kiddies
  - Hackivists ,Black Hats, VX'ers
- Today
  - Hacking for Profit
  - Disorganized crime
  - Web mobs
  - Organized crime

The dark side of the Internet involves not only fraud and theft, pervasive pornography, and pedophile rings, but also drug trafficking and criminal organizations that are more intent upon exploitation than the disruption that is the focus of the hacking community.
Phil Williams
Professor of International Security Studies
University of Pittsburgh

IRONPORT

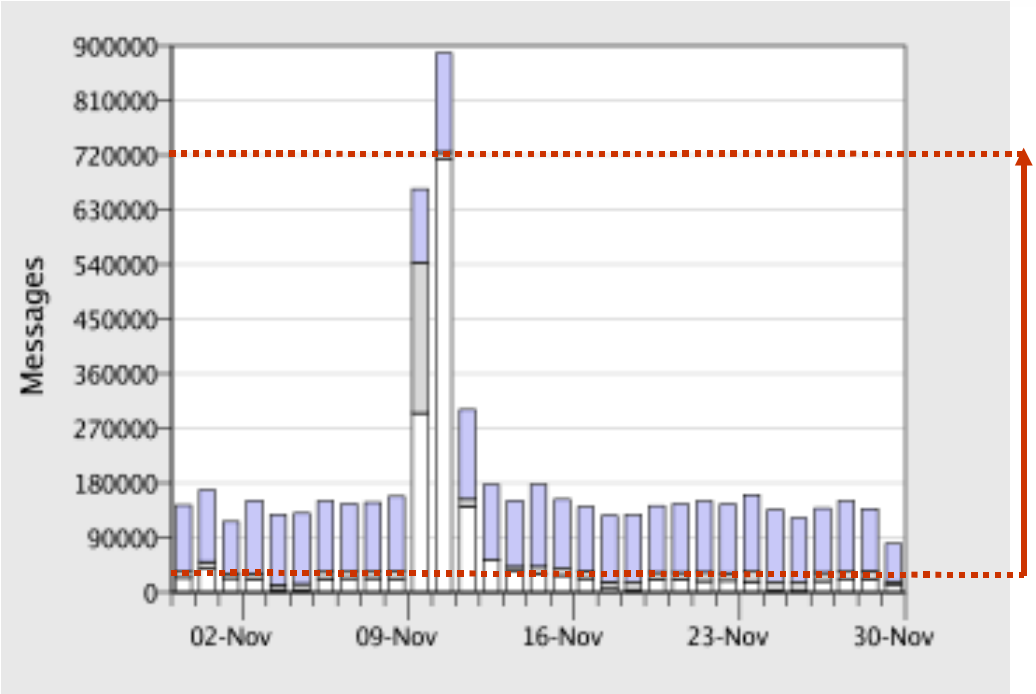
The Email Bounce Problem BDOS

- **Email's Other Billion Dollar Problem**
  - *Bounces are 9% of email*
- **Anti-Spam Scanners Are Not Effective**
  - *Misdirected bounces look legitimate*
  - *Do not trigger Anti-Spam scores*
  - *Originate from good reputation senders*



IRONPORT

Bounce DOS



20 fold increase in the number of mails accepted

IronPort

New Trends

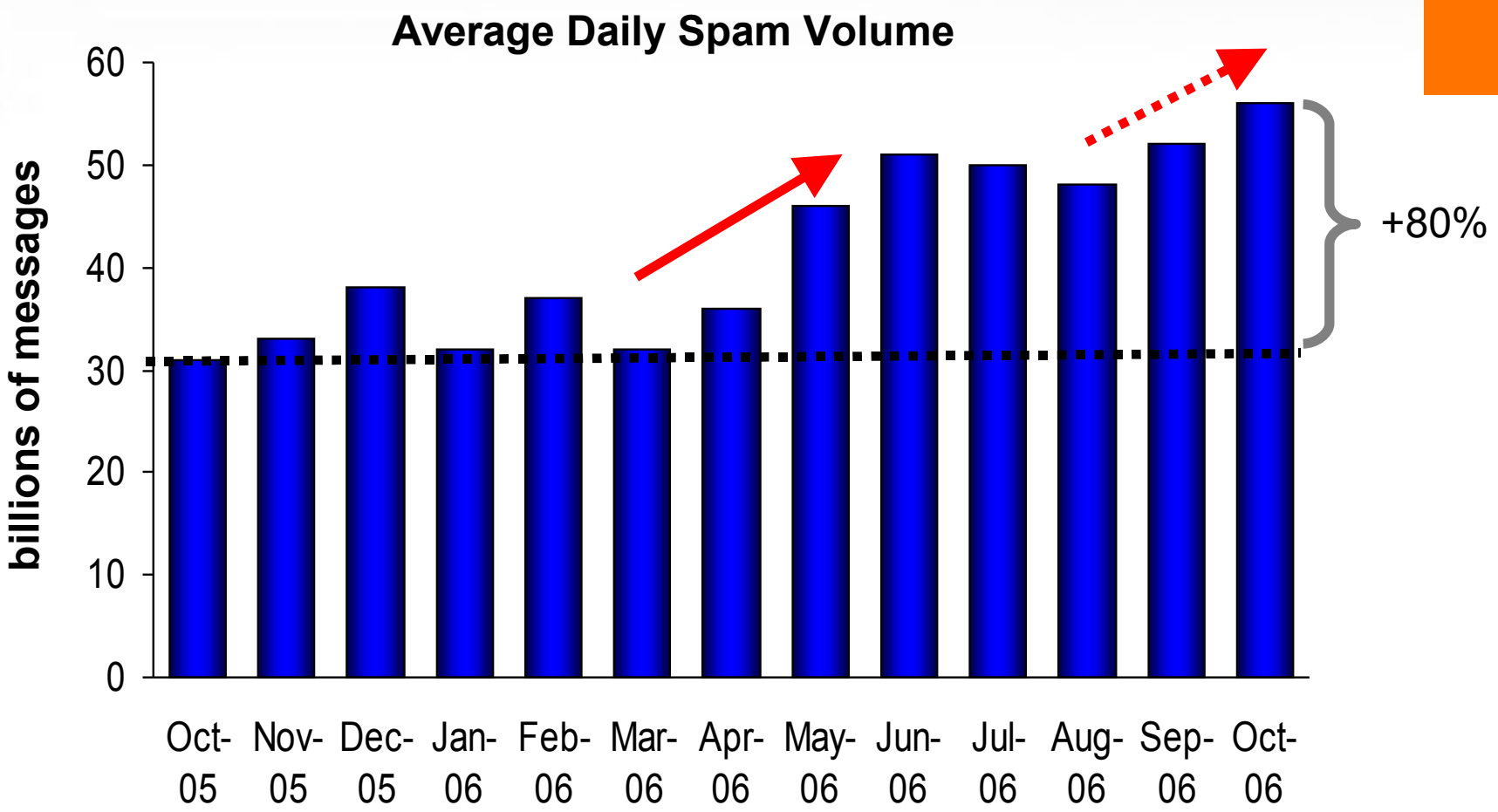
- Come along way since Sobig A
- Viruses becoming very sophisticated & devastating
  - Warezov virus stub sent via email…viral payload downloaded via http
  - Rustock goal is to be a spam proxy & send spam but evade detection & analysis
  - Both reside in memory & use alternate data streams for evasion
- Viral message volume dropping
  - keeps end user paranoia low and effectiveness high
- Spam, phishing & spyware interwoven

IRONPORT

The State of SPAM

IronPort™

Spam Increases to 60 Billion per Day



Total Volume by Data Size Jumps

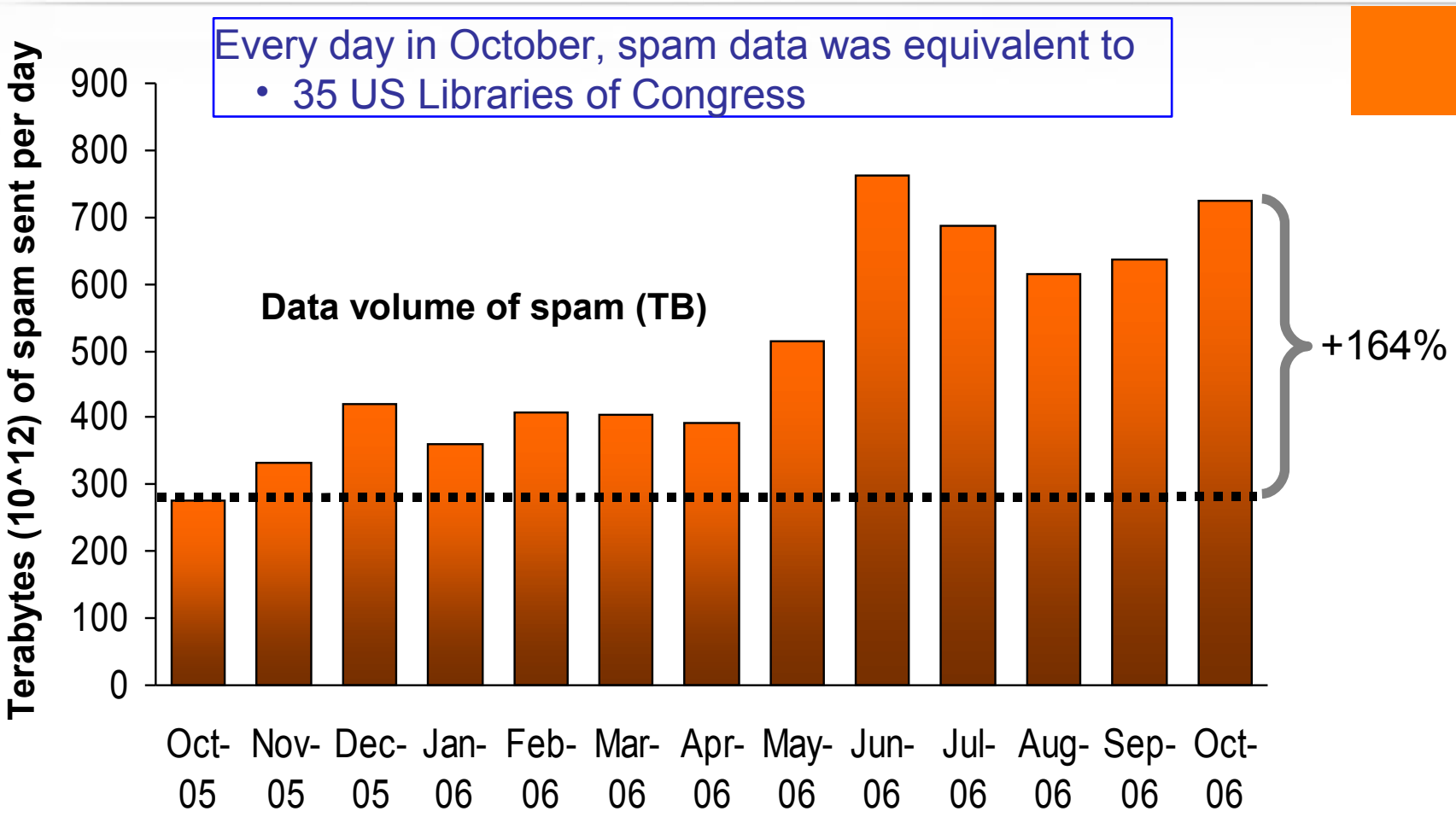
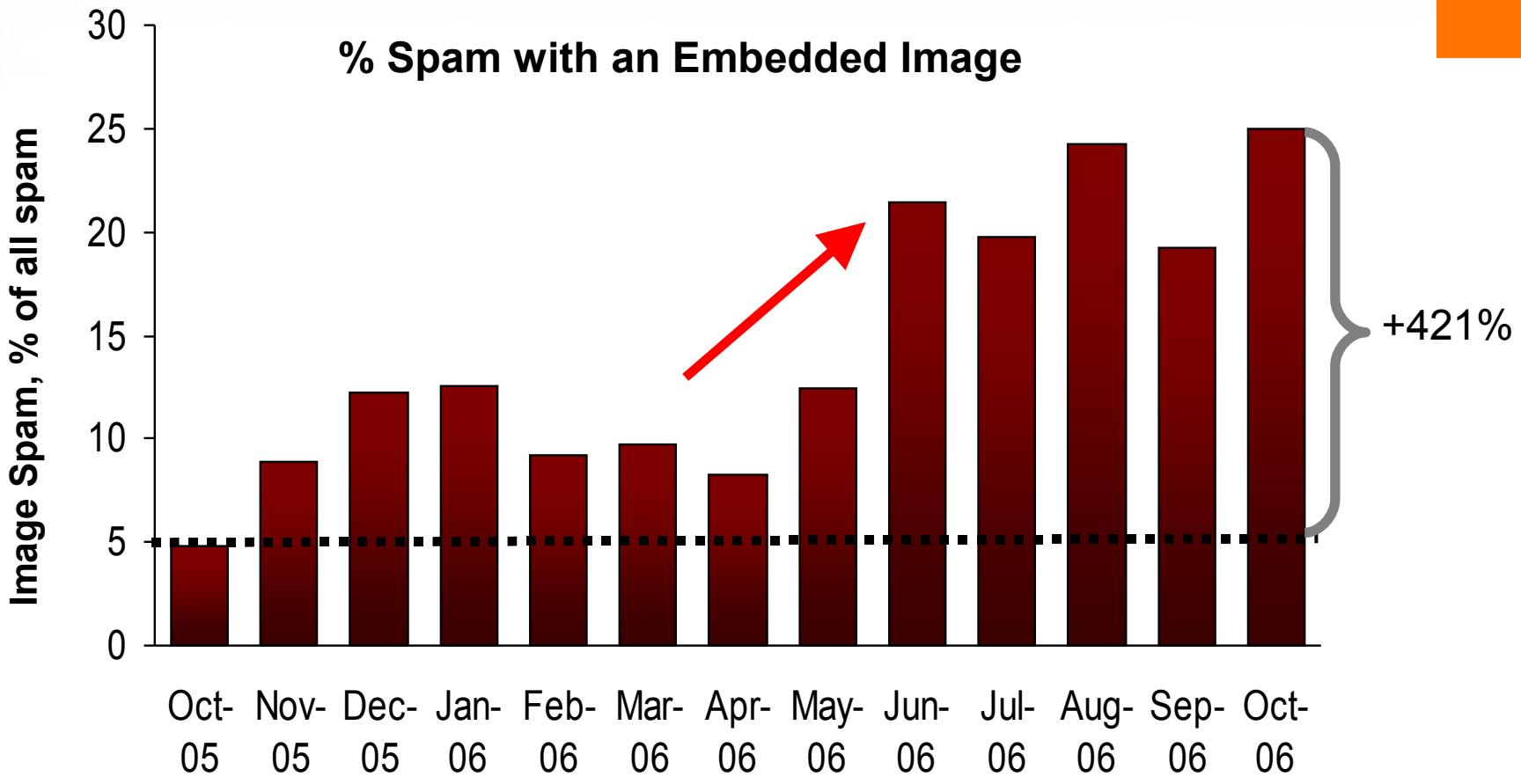
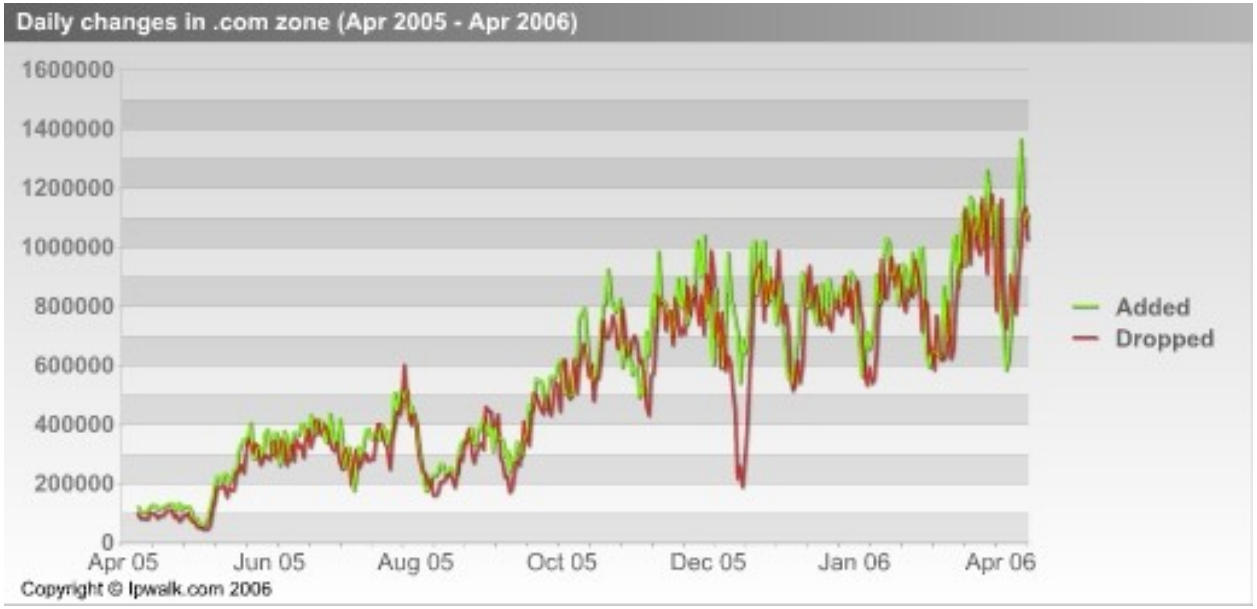


Image Spam Explodes – 5 to 25%



URL Attacks Mutate More Rapidly

- A Trend Called Domain “Kiting” Is on the Rise
  - Brings the cost of registering a domain to *zero*
  - Domains are now advertised in spam for < **4hrs**
  - Makes URL Blacklists/whitelists ineffective



** Source: IPWalk.com*

New Spamming Techniques

IronPort™

Image Spam

IronPort

Why?

Jonathan Lebed made $850,000 from **Pump & Dump**

Subj: THE MOST UNDERVALUED STOCK EVER
Date: 2/03/00 3:43pm Pacific Standard Time
From: LebedTG1
FTEC is starting to break out! Next week, this thing will EXPLODE...
Currently FTEC is trading for just $2 1/2! I am expecting to see FTEC at $20 VERY SOON.

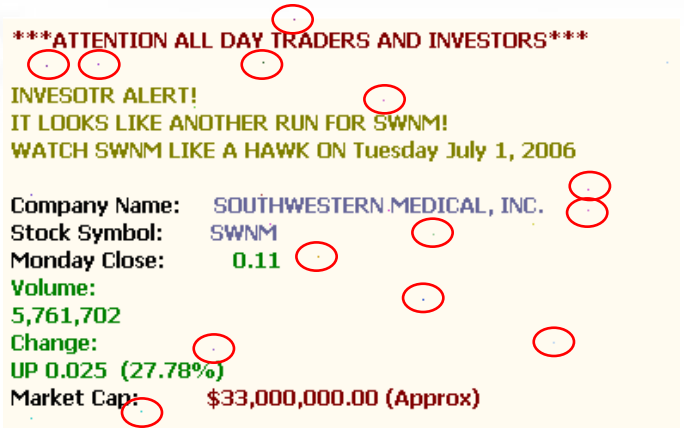
"Meyers Pollock Robbins" brokerage firm defrauded $176 million from investors using Pump & Dump

- CEO Michael Ploshnick served 3 years prison

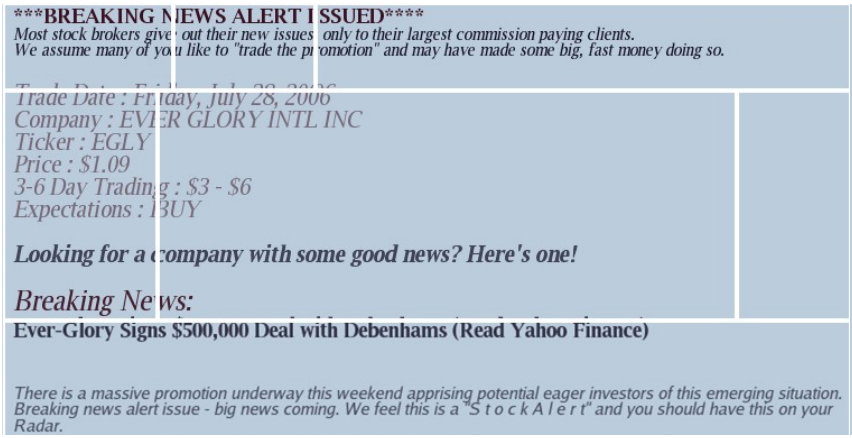
IRONPORT

Image Spam Gets Sneakier

1. “Polka dots”



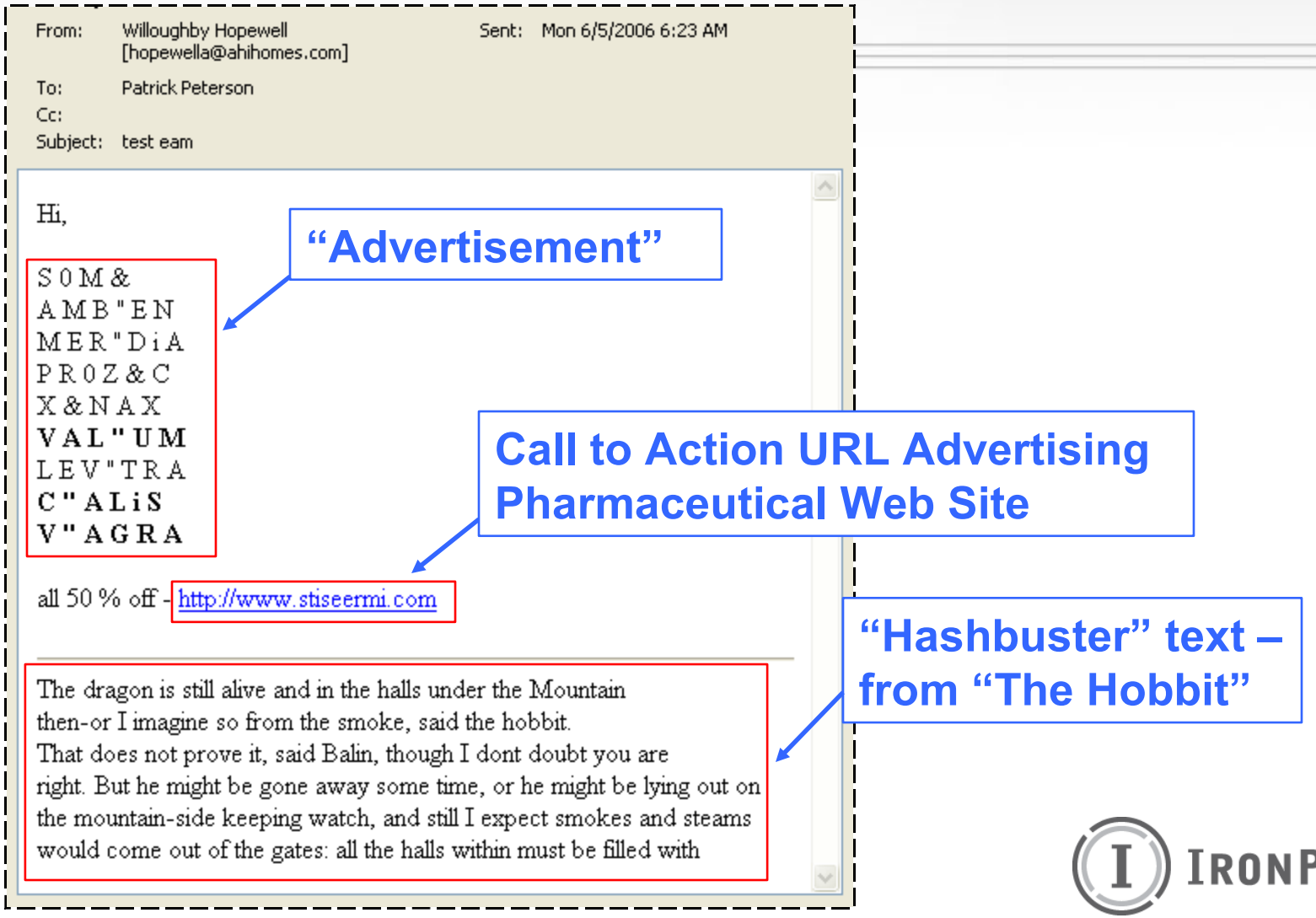
2. “Slice & Dice”



URL Spam

IronPort

One Spam



IRONPORT

Six Spam

From: Ajeet Tatham [mailto:tatajeet@bbok.com]
Sent: Tuesday, May 30, 2006 12:30 AM
To: Goldschmidt, Ron
Subject: [Ironport SPAM Positive] Re: 91 petersha

Hi,
AMB/EN
X^NAX
C?ALiS
VAL/UM
V?AGRA
LEV?TRA
PROZ^C
SOM^
MER?DiA
http://www.mithireda.com

Call to Action URL

longer making for the main forest-road to the south of his land. Had they followed the pass, their path would have led them down the stream from the mountains that joined the great river miles south of the Carrock. At that point there was a deep ford which they might have passed, if they had still had their ponies, and beyond that a track led to the skirts of the wood and to the entrance of the old forest road.

"Hashbuster" text

From: Njord Parrish [mailto:njorde@dimensionshealth.or]
Sent: Tuesday, May 30, 2006 1:01 AM
To: Miccio, John
Subject: [Ironport SPAM Positive] Re: 39 baron

Hi,
C?ALiS
V?AGRA
MER?DiA
LEV?TRA
SOM^
AMB/EN
X^NAX
PROZ^C
VAL/UM
http://www.mithireda.com

its yours after all and not mine-you had better slap your arms and rub your legs and try and help me get the others out while there is a chance!
Thorin of course saw the sense of this, so after a few more groans he got up and helped the hobbit as well as he could. In the darkness floundering in the cold water they had a difficult and very nasty job finding which were the right barrels. Knocking outside and calling only

From: Irina Pavlick [mailto:pavlieirina@]
Sent: Monday, May 29, 2006 4:11 AM
To: Zipperstein, Steve
Subject: robi 3649

Hi,

LeV/TRA
CiAL/S
X&nax
V/aGRA
Amox/cill/n
PROz&C
Tr&madol
SOm&
AmB/EN
VAL/uM
MeR/D/A

http://www.hisheron.com

on the stone, and shaking their prisoners as well.
Clap! Snap! the black crack!
Grip, grab! Pinch, nab!
And down down to Goblin-town
You go, my lad!
Clash, crash! Crush, smash!

From: Poncio Wedel [mailto:poncio@ca-sunshine.com]
Sent: Monday, May 29, 2006 10:57 PM
To: Tanouye, Duane
Subject: [Ironport SPAM Positive] Re: 695 swun

Hi,
X^NAX
C?ALiS
LEV?TRA
VAL/UM
MER?DiA
AMB/EN
V?AGRA
PROZ^C
SOM^
http://www.carogethi.com

again at last in spite of his fears.
It was full morning when he awoke. One of the dwarves had fallen over him in the shadows where he lay, and had rolled down with a bump from the platform on to the floor. It was Bofur, and he was grumbling about it, when Bilbo opened his eyes.
Get up lazybones, he said, or there will be no breakfast left for

From: Nicolina Krug [mailto:nicolinakrug@aolcom.com]
Sent: Monday, May 29, 2006 9:52 PM
To: Maddox, Roderick
Subject: [Ironport SUSPECT SPAM] Re: 240 unshake

Hi,
X^NAX
MER?DiA
AMB/EN
VAL/UM
PROZ^C
C?ALiS
LEV?TRA
SOM^
V?AGRA
http://www.romadaque.com

Somehow it struck all of them as not at all a nice place, although there was nothing wrong to see.
All of a sudden they heard a howl away down hill, a long shuddering howl. It was answered by another away to the right and a good deal nearer to them, then by another not far away to the left. It was wolves howling at the moon,wolves gathering together!

From: Sukie Lawhon [mailto:sukielaw@blaineschools.org]
Sent: Monday, May 29, 2006 9:41 PM
To: Young, Tina
Subject: [Ironport SPAM Positive] Re: 644 Cupi

Hi,
SOM^
PROZ^C
V?AGRA
LEV?TRA
C?ALiS
AMB/EN
VAL/UM
MER?DiA
X^NAX
http://www.romadaque.com

this Bilbo ought to have done something at once. Either he should have gone back quietly and warned his friends that there were three fair-sized trolls at hand in a nasty mood, quite likely to try toasted dwarf, or even pony, for a change; or else he should have done a bit of good quick burgling. A really first-class and legendary burglar would at this point have picked the trolls pockets-it is nearly always

The Spam Attack

Spam Content

- 1.5 billion messages over 2 weeks
- ~2000 unique content mutations – changed every 12 minutes
- 1500 unique domains used – changed every 15 minutes

Spam Source

- 100,000 infected PCs (zombies) in 119 countries

Command and Control (C&C) infrastructure

- Web sites
- Web servers
- DNS servers
- Payment processing and customer service systems

IRONPORT

http://infected.xit.dp.ua/en/

Google

CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Index of /marcom/docs/2006... | Itinerary | Сообщение Форума | ZloY TEaM - ICQ RQ QIP &RQ... | iNFECTE

INFECTED

uCT | SoCKS | DDoS SerVICE | ABoUT

|- WEB-ToolS -|- Rusian Version -|

SALE: Cryptor, Mail'SYSTEM, DownLoader, and other soft from iNFECTED.

We Give the facilities DDoS and Spam.
Also, there is in presence anonymous SockS5 server in good supply!
The Development script's and program's under order!

Contact: ICQ: 337614 or 741873

FreND

Pinc
AK-
The
XHa
MIN
Ano
Loc
[::F
[:: D
bla
WW
Sell
Ces
Age
Онл
San
Priv
RIC
COM

CoUN

123 Hidden Sender (Free DEMO Version)

File Send Email Help

Start Pause Stop | Download Proxy Server | Preview | Test Send | Settings | Diagnose | Register | Homepage

Message | Status | Logging

Recipients: Import Mailing List From Text File... | Input Recipients Directly

From Alias or File: Browse #ShortRandom#

Email From or File: Browse #ToEmail#

To Alias or Files: Browse #LongRandom#

Subject or File: Browse This is a subject #RandomDateTime#

Priority: Normal

Rotating message file: (for use with #RotatingText# in body message) (Optional) Browse

HTML File: Import HTML File | Clear HTML File

Body | HTML Preview | Dynamic Message

Dynamic From Name
- Disable Dynamic From Name
- As same as recipients' email
- Randomize From Name

Dynamic Email From
- Disable Dynamic Email From
- As same as recipients' email
- Randomize Email From

Dynamic To Alias
- Disable Dynamic To Alias
- As same as sender's alias
- Randomize To Alias

Dynamic Subject
- Append Date & Time
- Append Receiptor's Name
- Append Random Words
- Append Random Date & Time

Dynamic Body at TOP
- Insert Date & Time at the start
- Insert Receiptor's Name at the start
- Insert Random Words at the start
- Insert Date & Time at the start

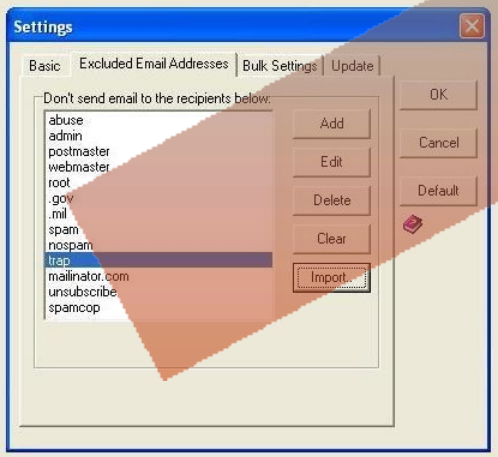
Dynamic Body at BOTTOM
- Append Date & Time at the end
- Append Receiptor's Name
- Append Random Words
- Append Date & Time

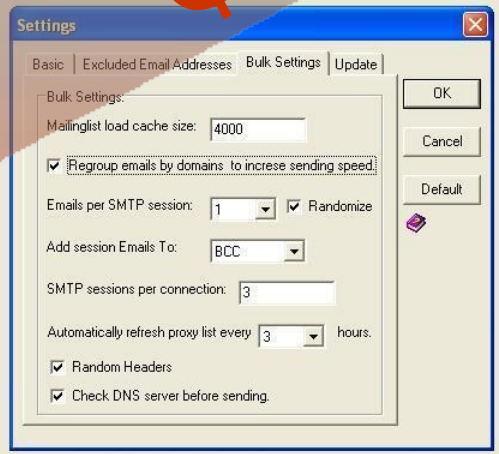
Attachment | Add | Delete

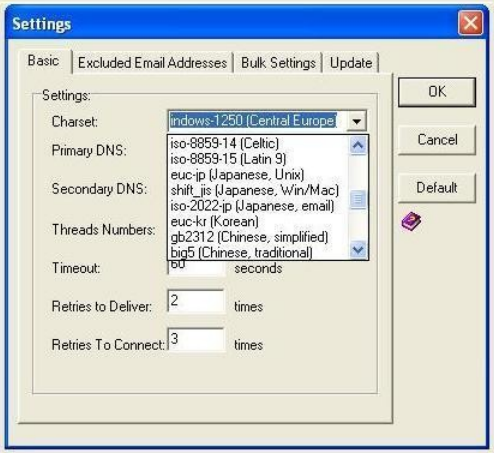
splash_hidd...

Total:1

$99







Time Elapsed: | Total Recipients: | Processed: | Successful:

start | eTrust Spyware Ency... | 123 Hidden Sender s... | http://www.123hidde... | 123 Hidden Sender (F... | 1232 - Paint | 1:21 PM

Atomic Email Hunter - UNREGISTERED VERSION

File Plugins Results Settings Tools Help

Hunt: australian government GO Advanced...

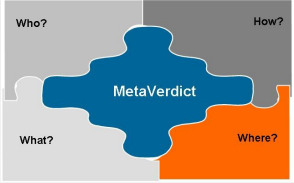
E-mail address	Owner	Location
senator.coonan@aph.gov.au	senator.coonan@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DCommunications%5C%2C%20Information%20Technology%20and%20the%20Arts%2Co%3DPortfolios%2Co%3DCommc
julie.bishop.mp@aph.gov.au	Julie.Bishop.mp@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DEducation%5C%2C%20Science%20and%20Training%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2
greg.hunt.mp@aph.gov.au	Greg.Hunt.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DEnvironment%20and%20Heritage%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&elevat
senator.ian.campbell@aph.gov.au	senator.ian.campbell@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DEnvironment%20and%20Heritage%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&elevat
minister.brough@facsia.gov.au	minister.brough@facsia.gov.au	http://www.directory.gov.au/osearch.php?o%3DFamilies%5C%2C%20Community%20Services%20And%20Indigenous%20Affairs%2Co%3DPortfolios%2Co%3DCommor
julie.bishop@dest.gov.au	julie.bishop@dest.gov.au	http://www.directory.gov.au/osearch.php?o%3DFamilies%5C%2C%20Community%20Services%20And%20Indigenous%20Affairs%2Co%3DPortfolios%2Co%3DCommor
john.cobb@mfacsia.gov.au	john.cobb@mfacsia.gov.au	http://www.directory.gov.au/osearch.php?o%3DFamilies%5C%2C%20Community%20Services%20And%20Indigenous%20Affairs%2Co%3DPortfolios%2Co%3DCommor
warren.truss.mp@aph.gov.au	Warren.Truss.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DForeign%20Affairs%20and%20Trade%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&ele
minister.downer@dfat.gov.au	minister.downer@dfat.gov.au	http://www.directory.gov.au/osearch.php?o%3DForeign%20Affairs%20and%20Trade%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&ele
ian.macfarlane.mp@aph.gov.au	Ian.Macfarlane.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DIndustry%5C%2C%20Tourism%20and%20Resources%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%
fran.bailey.mp@aph.gov.au	Fran.Bailey.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DIndustry%5C%2C%20Tourism%20and%20Resources%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%
bob.baldwin.mp@aph.gov.au	Bob.Baldwin.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DIndustry%5C%2C%20Tourism%20and%20Resources%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%
m.vaile.mp@aph.gov.au	M.Vaile.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DTransport%20and%20Regional%20Services%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3D
de-anne.kelly.mp@aph.gov.au	De-Anne.Kelly.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DTransport%20and%20Regional%20Services%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3D
j.lloyd.mp@aph.gov.au	J.Lloyd.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?o%3DTransport%20and%20Regional%20Services%2Co%3DPortfolios%2Co%3DCommonwealth%20of%20Australia%2Cc%3D
mal.brough.mp@aph.gov.au	Mal.Brough.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
ministerial@treasury.gov.au	ministerial@treasury.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
peter.mcgauran.mp@aph.gov.au	Peter.McGauran.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
mark.vaile.mp@aph.gov.au	Mark.Vaile.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
tony.abbott.mp@aph.gov.au	Tony.Abbott.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
b.nelson.mp@aph.gov.au	B.Nelson.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
senator.minchin@aph.gov.au	senator.minchin@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
w.truss.mp@aph.gov.au	W.Truss.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
kevin.andrews.mp@aph.gov.au	kevin.andrews.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DCabinet%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&changeba
ian.harris.reps@aph.gov.au	Ian.Harris.Reps@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DDepartment%20of%20the%20House%20of%20Representatives%2Co%3DCommonwealth%20Parliament%2Co%3DCon
b.wright.reps@aph.gov.au	B.Wright.Reps@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DDepartment%20of%20the%20House%20of%20Representatives%2Co%3DCommonwealth%20Parliament%2Co%3DCon
query@fedcourt.gov.au	query@fedcourt.gov.au	http://www.directory.gov.au/osearch.php?ou%3DFederal%20Court%20of%20Australia%2Co%3DCourts%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU&char
customer.service@fmc.gov.au	customer.service@fmc.gov.au	http://www.directory.gov.au/osearch.php?ou%3DFederal%20Magistrates%20Court%20of%20Australia%2Co%3DCourts%2Co%3DCommonwealth%20of%20Australia%2
tony.abbott@aph.gov.au	Tony.Abbott@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Office%20Holders%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwe
ian.causley.mp@aph.gov.au	Ian.Causley.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Office%20Holders%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwe
peter.mcgauran@aph.gov.au	Peter.McGauran@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Office%20Holders%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwe
harry.jenkins.mp@aph.gov.au	Harry.Jenkins.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Office%20Holders%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwe
jill.hall.mp@aph.gov.au	Jill.Hall.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
michael.danby.mp@aph.gov.au	Michael.Danby.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
j.forrest.mp@aph.gov.au	J.Forrest.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
p.neville.mp@aph.gov.au	P.Neville.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
stewart.mcarthur.mp@aph.gov.au	stewart.mcarthur.mp@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
kerry.bartlett.mp@aph.gov.au	kerry.bartlett.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
joanna.gash.mp@aph.gov.au	Joanna.Gash.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
kim.beazley.mp@aph.gov.au	kim.beazley.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
rogerpricemp@aph.gov.au	rogerpricemp@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DHouse%20of%20Representatives%20Party%20Leaders%20and%20Whips%2Co%3DCommonwealth%20Parliament%2C
j.hockey.mp@aph.gov.au	j.hockey.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
gary.hardgrave.mp@aph.gov.au	Gary.Hardgrave.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
b.billson.mp@aph.gov.au	B.Billson.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
g.nairn.mp@aph.gov.au	G.Nairn.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
peter.dutton.mp@aph.gov.au	Peter.Dutton.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
s.stone.mp@aph.gov.au	S.Stone.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
senator.santoro@aph.gov.au	senator.santoro@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
john.cobb.mp@aph.gov.au	John.Cobb.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
ministerforjustice.customs@ag.gov.au	ministerforjustice.customs@ag.gov.au	http://www.directory.gov.au/osearch.php?ou%3DOuter%20Ministry%2Co%3DCommonwealth%20Parliament%2Co%3DCommonwealth%20of%20Australia%2Cc%3DAU8
bernie.ripoll.mp@aph.gov.au	Bernie.Ripoll.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
ann.corcoran.mp@aph.gov.au	Ann.Corcoran.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
john.murphy.mp@aph.gov.au	John.Murphy.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
warren.snowdon.mp@aph.gov.au	Warren.Snowdon.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
jennie.george.mp@aph.gov.au	Jennie.George.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
kirsten.livermore.mp@aph.gov.au	Kirsten.Livermore.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
peter.garrett.mp@aph.gov.au	Peter.Garrett.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3
catherine.king.mp@aph.gov.au	Catherine.King.MP@aph.gov.au	http://www.directory.gov.au/osearch.php?ou%3DParliamentary%20Secretaries%20to%20the%20Shadow%20Ministers%2Co%3DCommonwealth%20Parliament%2Co%3

Searching the sites by keyword "australian government" at MSN... Smart search 562 e-mails 1455 pages

start Atomic Email Hunter 3:52 PM

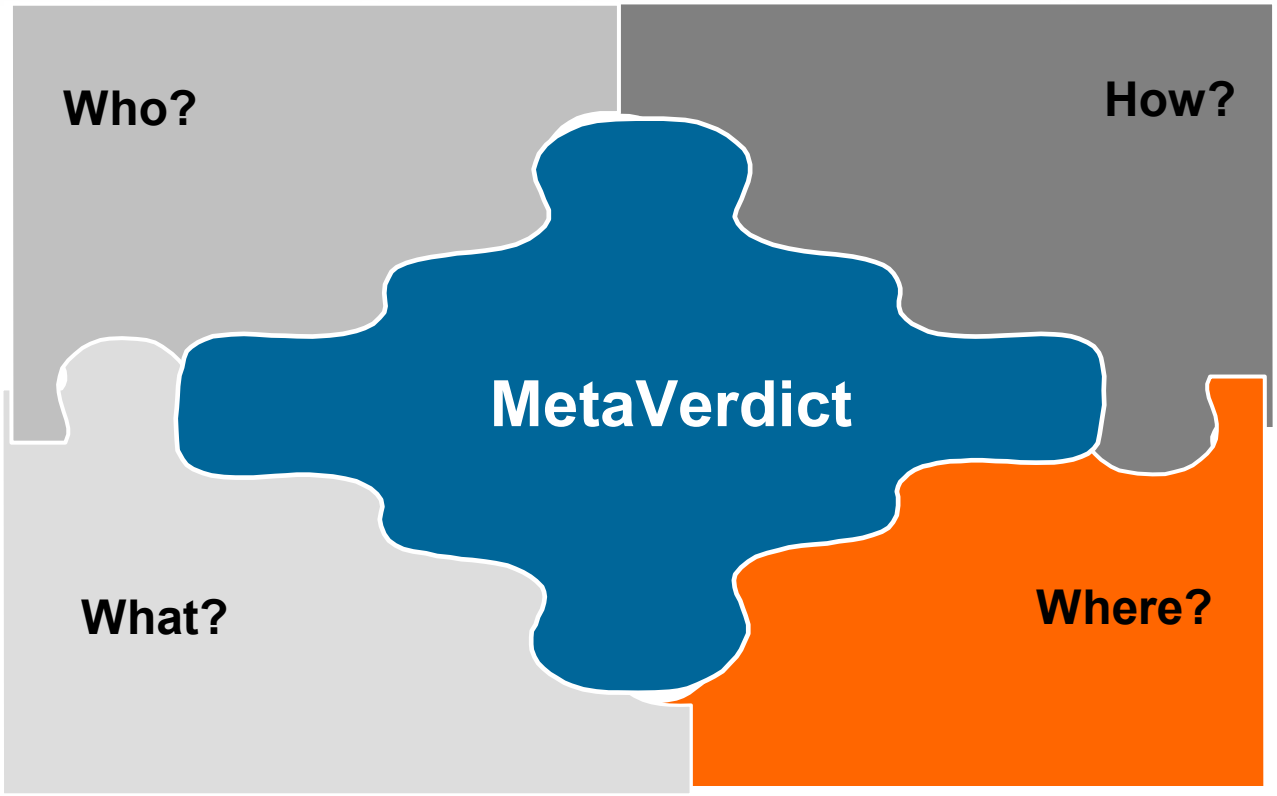
Predicative Security

IronPort™



Predicative Security

Predicate what is good - Predicate what is bad



IRONPORT

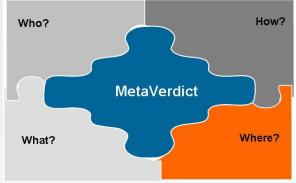


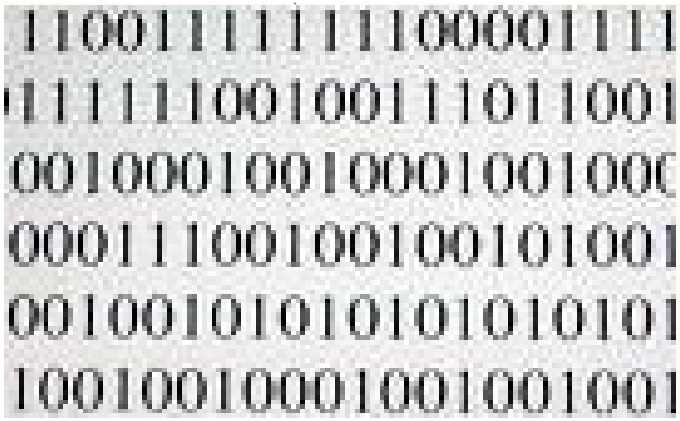
Image Spam Example

Traditional Content Filters

HOW?

WHAT?

- *No spam content found in message*
- *Doesn't match known signatures*



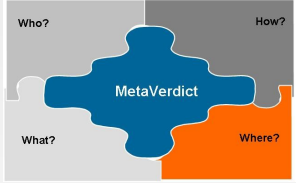
WHO?

- *IP address not on any blacklists*

WHERE?

Verdict

UNKNOWN



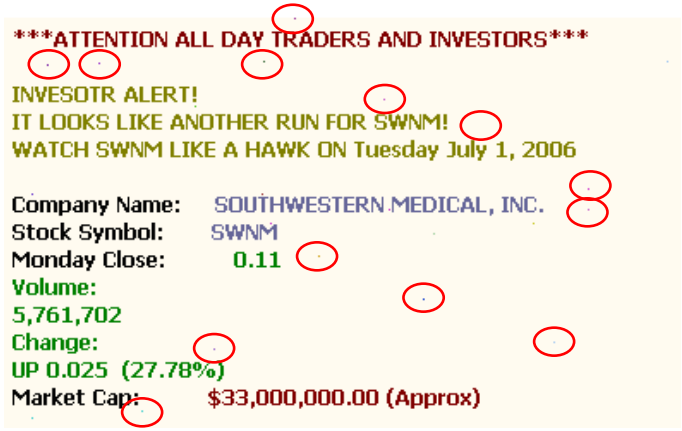
Predicative Security for Image Spam

HOW?

- *Message leaves trace of spamware tool*

WHAT?

- *All text inside an image*
- *Random dots appear within the message*
- *Nearly identical color scheme in 100,000's spamtrap msgs*



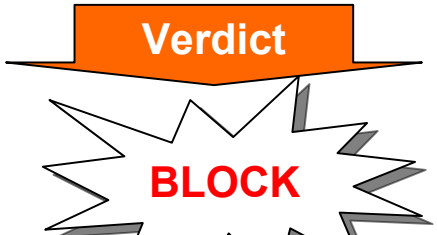
WHO?

- *IP address recently started sending email*
- *Message originated from dial-up IP address*
- *Sending IP address located in Russia*

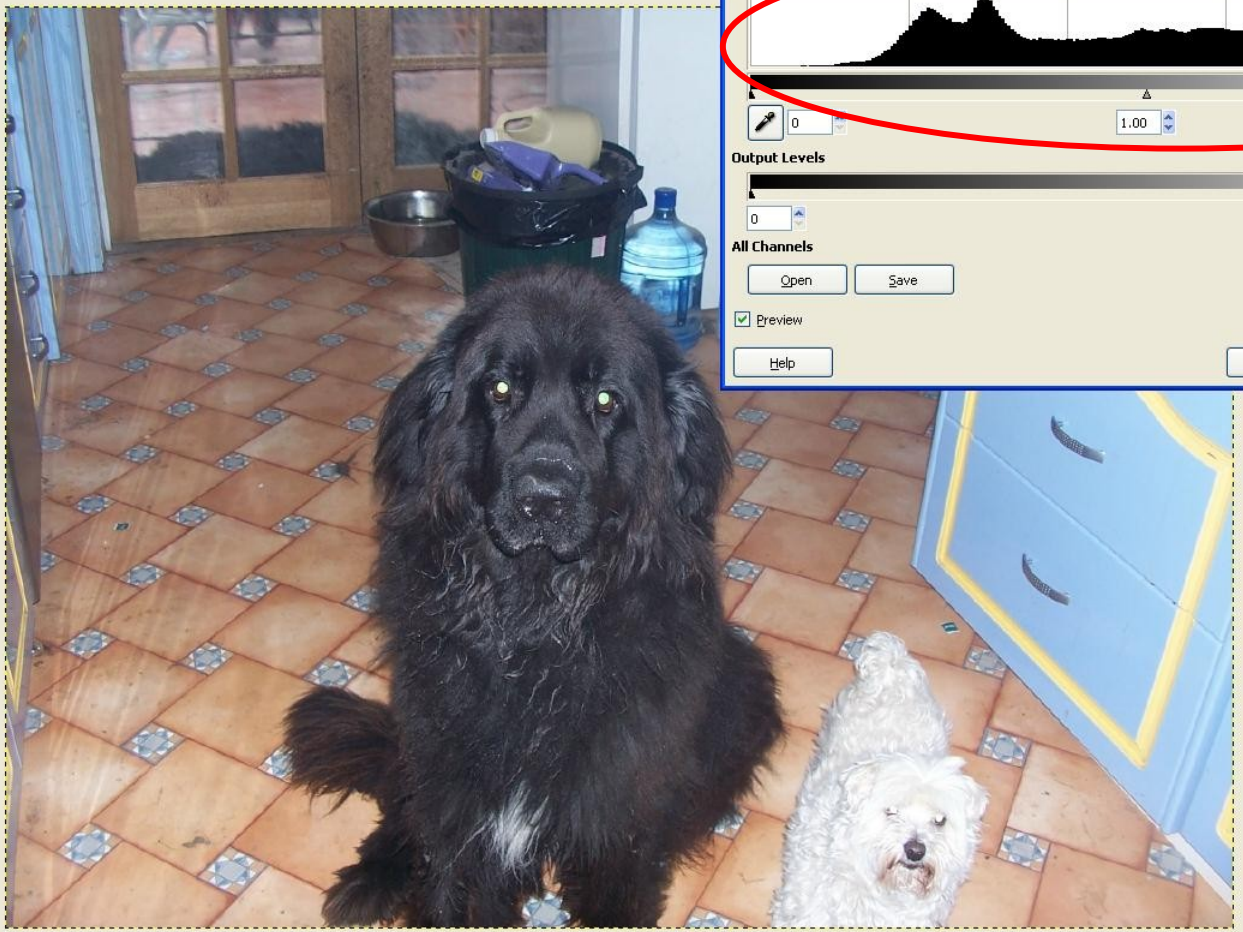
WHERE?

http://urllink.call.to.action.ipaddressisinrussia.com

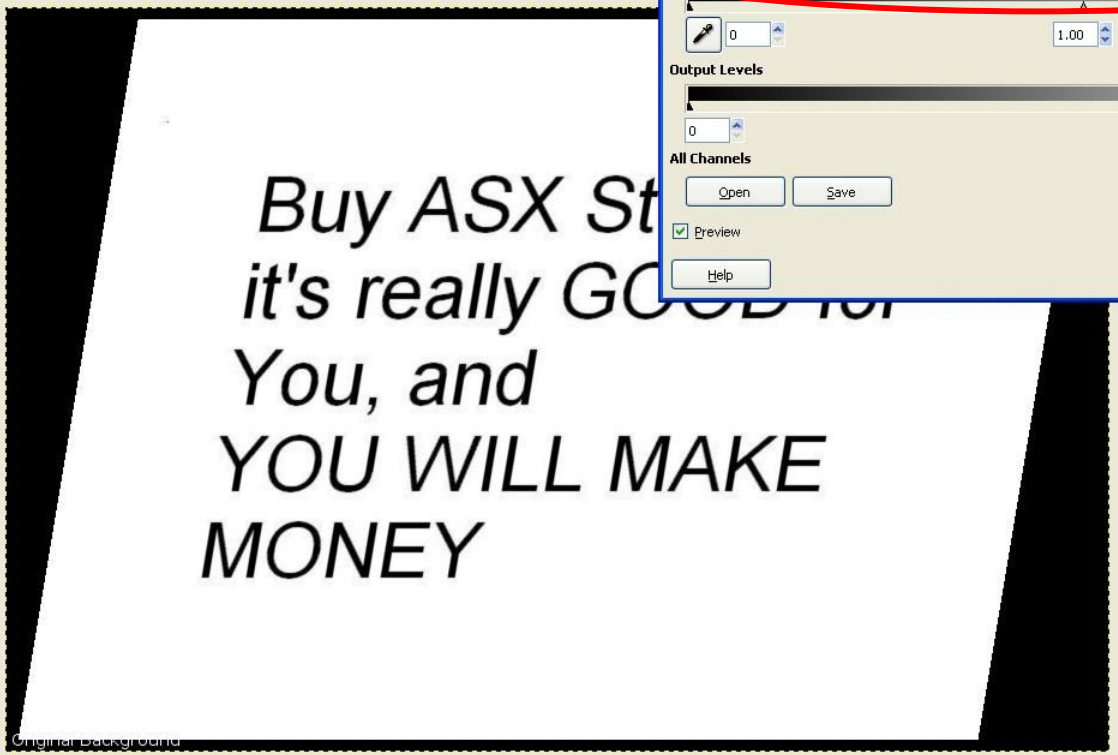
Network Owner	DataNet
Domain	dnet.pl
Date of first message seen from this address	2006-06-18
CIDR range	unknown
# of domains controlled by this network owner	500
Geography data	
Country	RU
State	48
City	Moscow

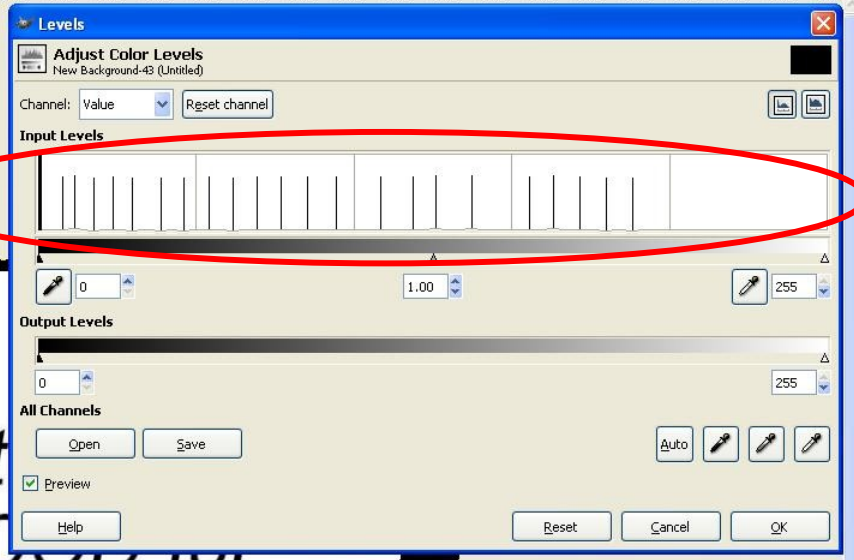


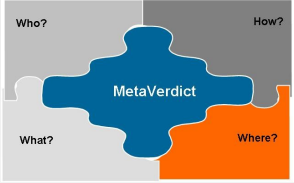
Spectrum of colour spread throughout the entire image



Limited spectrum of Colours, drastic colour change, produces ECG like pattern

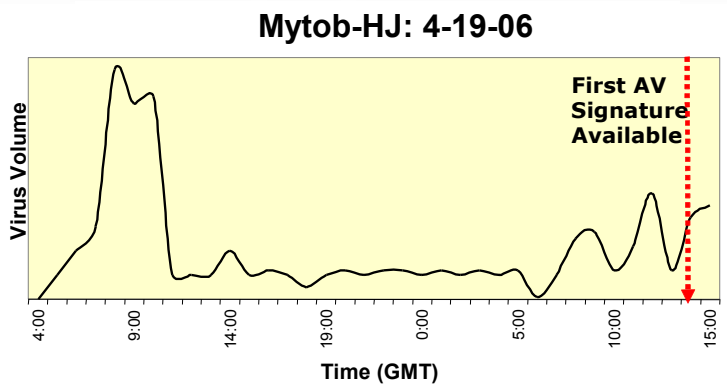


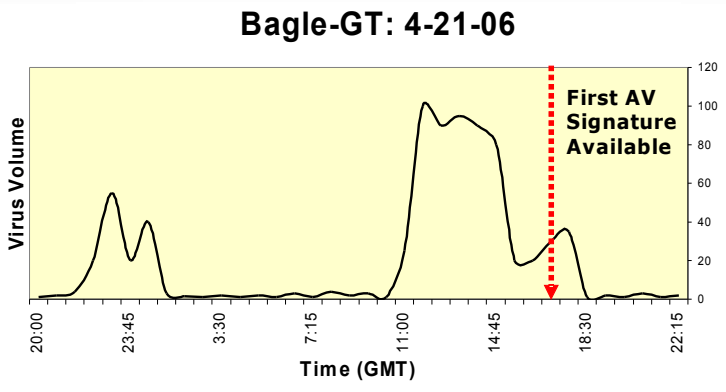


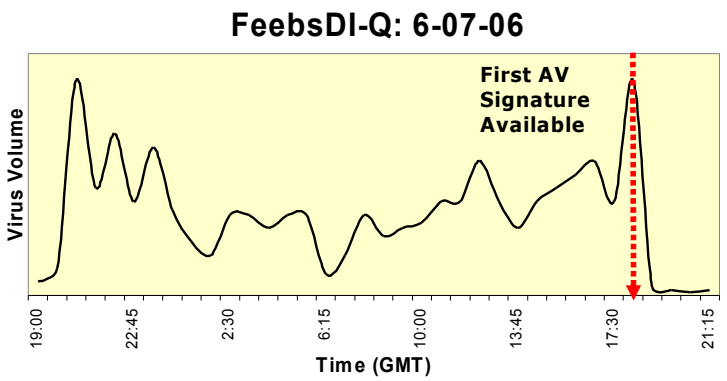


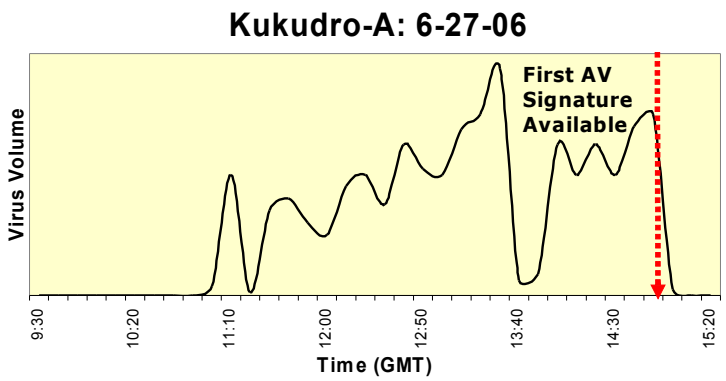
Virus Outbreak Example

Traditional AV Signature Update



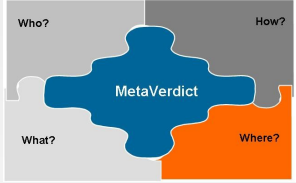






TRONPORT

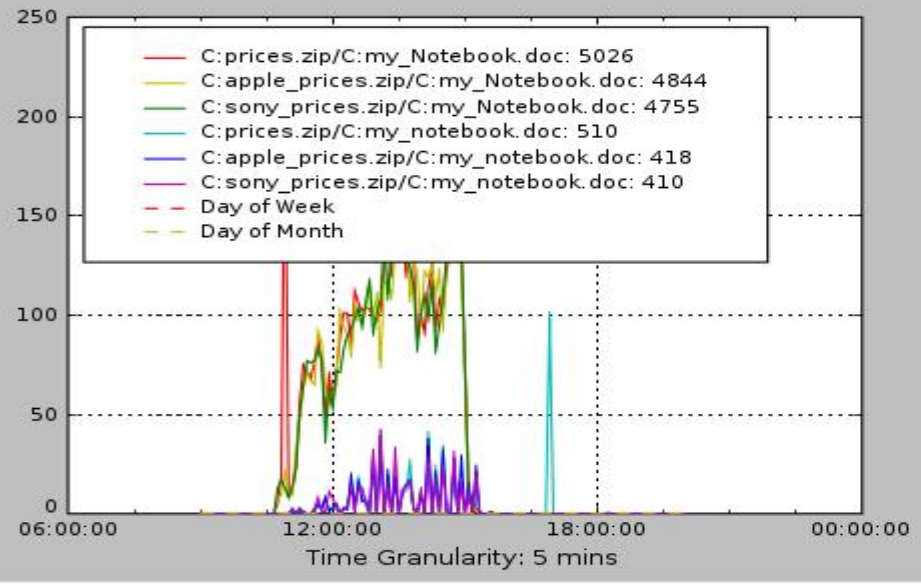
Calculated as publicly published signatures from the following vendors: Sophos, Trend Micro, Computer Associates, F-Secure, Symantec and McAfee. If signature time is not available, first publicly published alert time is used.



Virus Outbreak Predicates

Extensions Broken Down By Filenames

Extensions Broken Down By Filenames



Showing: C:prices.zip/C:my_Notebook.doc, C:prices.zip/C:my_notebook.doc

No.	Filenames	# Files
1	C:prices.zip/C:my_Notebook.doc	5026
2	C:prices.zip/C:my_notebook.doc	510

Filenames List

Download

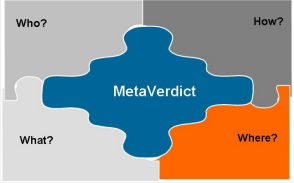
--ALL--: 24113
C:prices.zip/C:my_Notebook.doc: 5026
C:apple_prices.zip/C:my_Not...doc: 4844
C:sony_prices.zip/C:my_Note...doc: 4755
C:Test.zip/C:Test.doc: 2773
C:prices.zip/C:my_notebook.doc: 510
C:apple_prices.zip/C:my_not...doc: 418
C:sony_prices.zip/C:my_note...doc: 410
C:Golden.zip/C:Golden.doc: 32
H:AAAAAAAAAA AAAAAAAAA 0 AA...doc: 28
H:AAAAAAAAAA AAAAAAAAA 0 AA...doc: 28
H:AAA Aaaaaaaaa 00-00-00.zi...doc: 27
H:Aaaaaaaaaaa000000.zip/H:A...doc: 25
H:AA-AA AAA AAA-AAA 00.zip/...doc: 16
C:0076307.zip/C:0076307.doc: 11
C:0076308.zip/C:0076308.doc: 11
C:0076309.zip/C:0076309.doc: 11
C:0076310.zip/C:0076310.doc: 11
C:0076316.zip/C:0076316.doc: 11
C:0076317.zip/C:0076317.doc: 11
C:0076318.zip/C:0076318.doc: 11
C:0076319.zip/C:0076319.doc: 11
C:0076320.zip/C:0076320.doc: 11
C:0076321.zip/C:0076321.doc: 11
H:000_AA_Aaaaaaaaaaaa Aaaaa...doc: 9
H:AaaaaaaaA0000.zip/H:Aaa A...doc: 8
H:AaaaaaaaA0000.zip/H:Aaa A...doc: 8
H:aaaaaaaaaaaaaaaa.zip/H:Aa...doc: 8
H:AA AAAAAAAAAA AAAAAA.zip/...doc: 7
H:Aaaaaaaa 00000000.zip/H:A...doc: 7
C:0076311.zip/C:0076311.doc: 6

Sort List By: Name Volume

Update

Go to Filenames Report

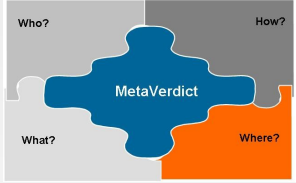
IRONPORT



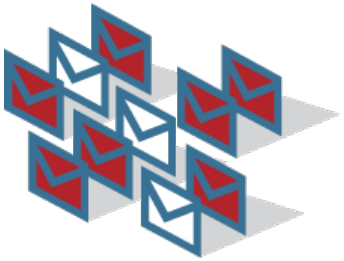
Outbreak Predicates

Attachment Size Report

	# Messages			
Attachment Size Bucket	Absolute Volume	Change(%)	% vs Moving Avg	% Total Seen
0k	10		-68.75	0.00305652430395
4k	1		-66.6666666667	0.000305652430395
10k	3	-100.0	-25.0	0.000916957291186
15k	34	-33.3333333333	21.4285714286	0.0103921826334
20k	45	200.0	-29.6875	0.0137543593678
25k	75		74.4186046512	0.0229239322796
30k	89	800.0	97.7777777778	0.0272030663052
35k	52	800.0	79.3103448276	0.0158939263806
40k	36	200.0	24.1379310345	0.0110034874942
45k	40	-100.0	-25.9259259259	0.0122260972158
50k	37		19.3548387097	0.0113091399246
55k	23		-50.0	0.00703000589909
60k	23		-8.0	0.00703000589909
65k	19	-100.0	18.75	0.00580739617751
70k	13		8.33333333333	0.00397348159514
75k	11		-67.6470588235	0.00336217673435
80k	11		-21.4285714286	0.00336217673435
85k	4984	1064.0	1433.53846154	1.52337171309
90k	5		-58.3333333333	0.00152826215198

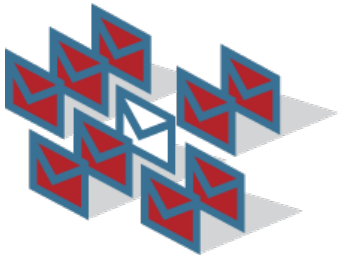


Predicates build context to take Action



T1 = 0

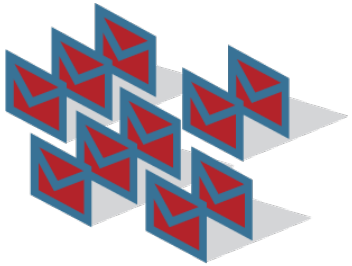
–zip (exe) files



T2 = 5 mins

-zip (exe) files

-Size 50 to 55 KB.



T3 = 15 mins

–zip (exe) files

–Size 50 to 55KB

–"Price" in the name file

Messages Scanned & Deleted

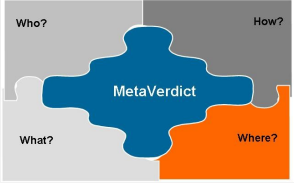
T4 = 8 hours

–Release messages if signature update is in place

Fine-grained Rules, Multiple Parameters:

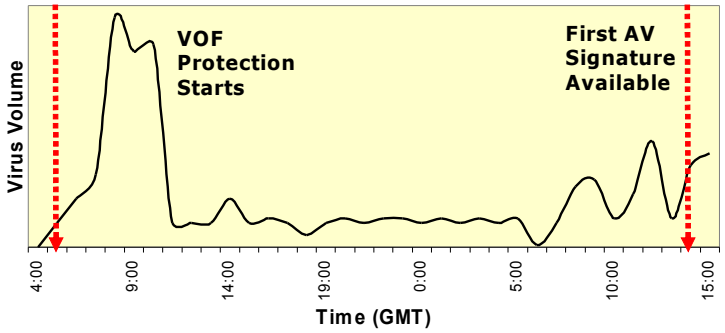
Attachment Type, Attachment Size, URLs, Filenames & More

IRONPORT

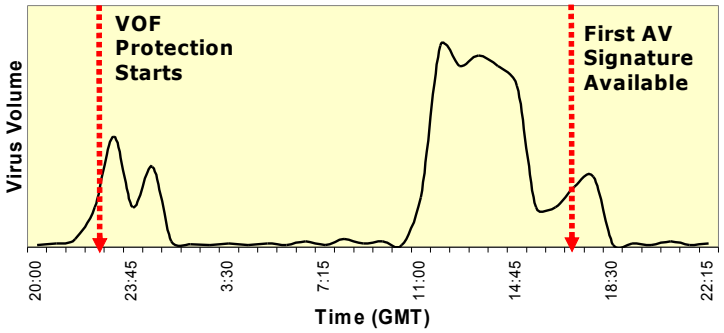


Outbreak Predicate Results

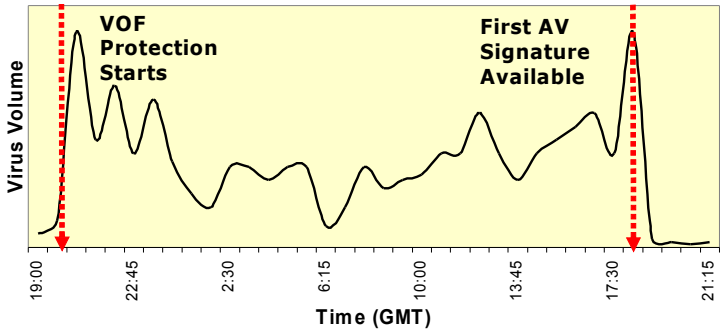
Mytob-HJ: *32 hrs 57 mins Lead Time!*



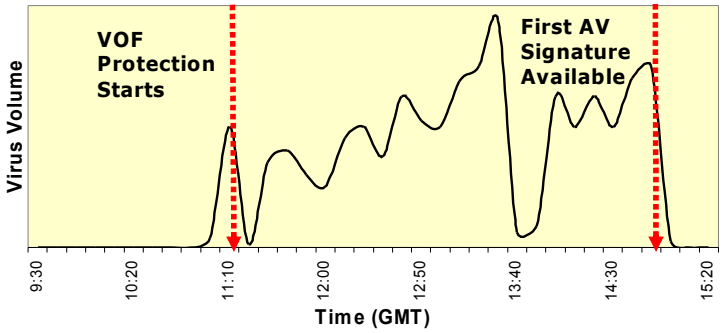
Bagle-GT: *18 hrs 28 mins Lead Time!*



FeebsDl-Q: *21 hrs 59 mins Lead Time!*

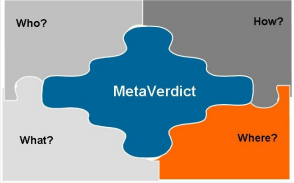


Kukudro-A: *3 hrs 38 mins Lead Time!*



TRONPORT

Calculated as publicly published signatures from the following vendors: Sophos, Trend Micro, Computer Associates, F-Secure, Symantec and McAfee. If signature time is not available, first publicly published alert time is used.



URL Spam Example traditional content filter

From: Willoughby Hopewell [hopewella@ahihomes.com] Sent: Mon 6/5/2006 6:23 AM

To: Patrick Peterson

Cc:

Subject: test eam

Hi,

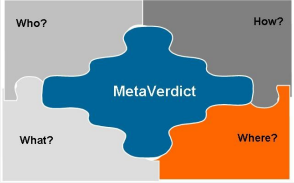
S0M&
AMB"EN
MER"DiA
PR0Z&C
X&NAX
VAL"UM
LEV"TRA
C"ALiS
V"AGRA

all 50 % off - http://www.stiseermi.com

The dragon is still alive and in the halls under the Mountain then-or I imagine so from the smoke, said the hobbit. That does not prove it, said Balin, though I dont doubt you are right. But he might be gone away some time, or he might be lying out on the mountain-side keeping watch, and still I expect smokes and steams would come out of the gates: all the halls within must be filled with

Check URL blacklists

IRONPORT



Web Predicates for URL spam

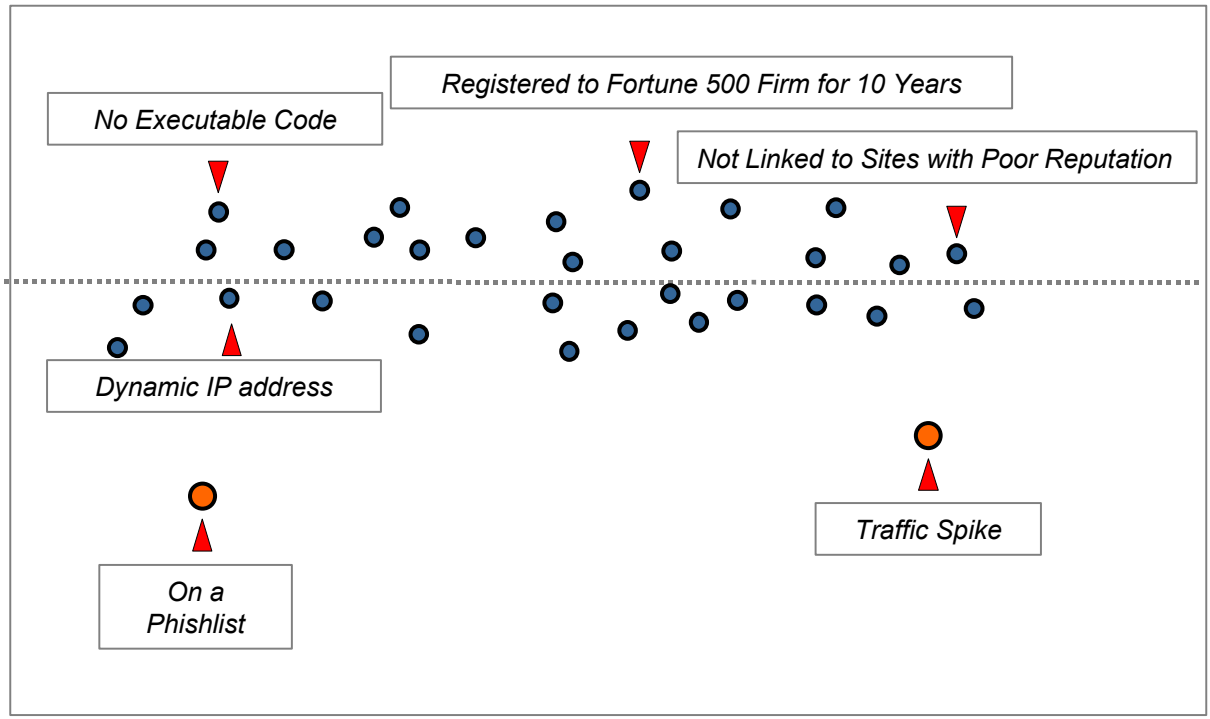
Predicates

- Web Server Blacklist & Whitelists
- Domain Blacklists & Safelists
- Website Composition Data
- Global Volume Data
- Domain Registrar Information
- Dynamic IP Addresses
- Name Server Data

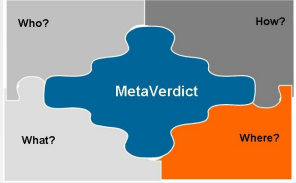
EMAIL DATA

Email Server Blacklists & Whitelists

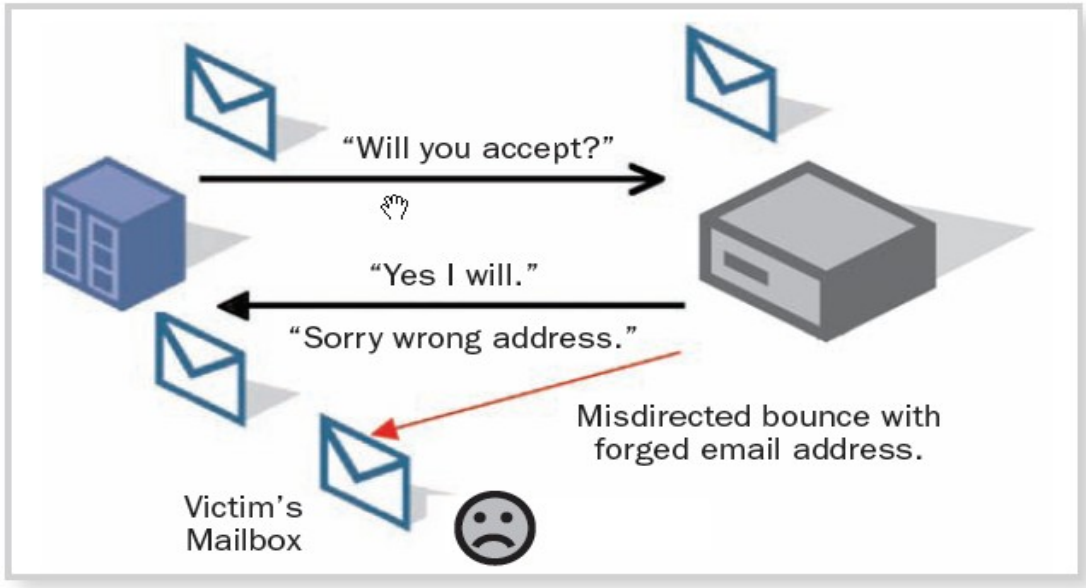
Spikes in URLS found in Emails



IRONPORT



Bounce DOS



- Based on Bounce Address Tag Validation
- Proposed RFC

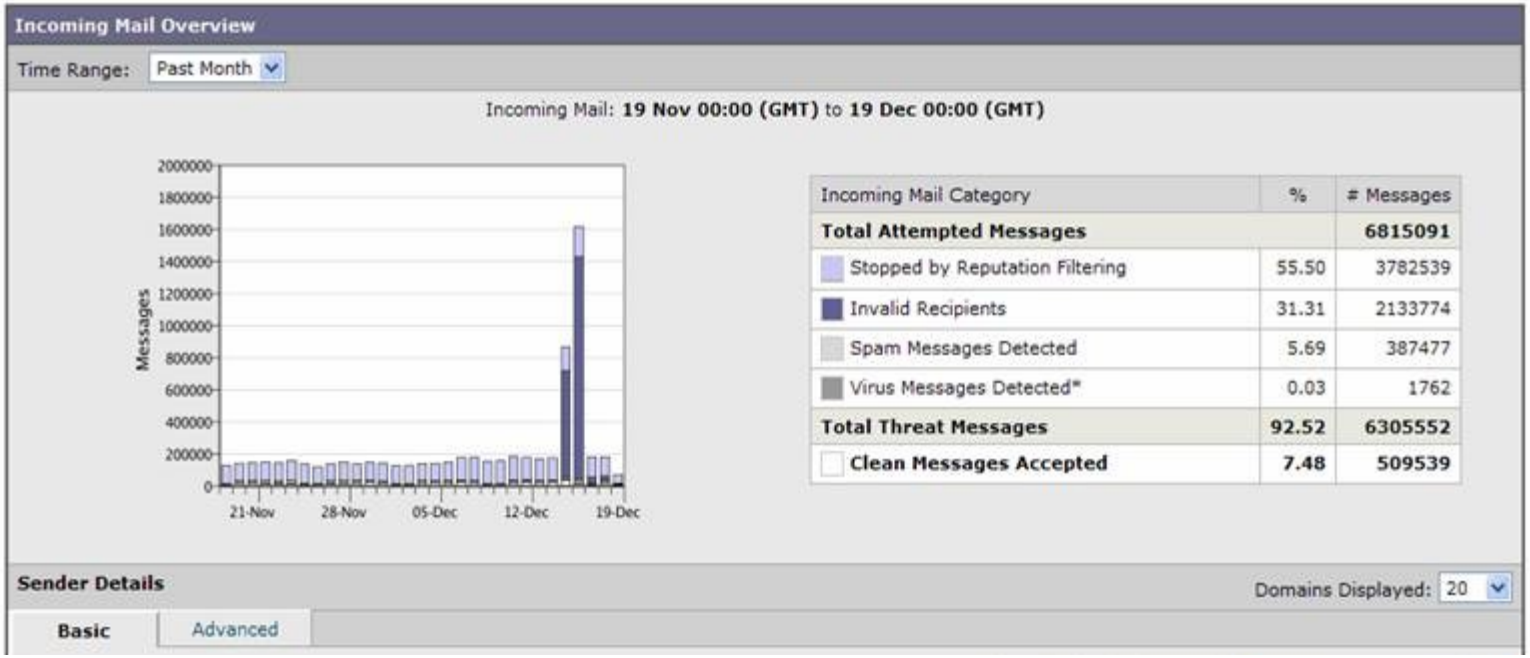
Envelope MAIL-FROM address changes so

'bob@from.com' becomes 'prvs=bob=385c70f2a@from.com'

IRONPORT

Bounce Address Tag Validation

Bounce DOS Protection

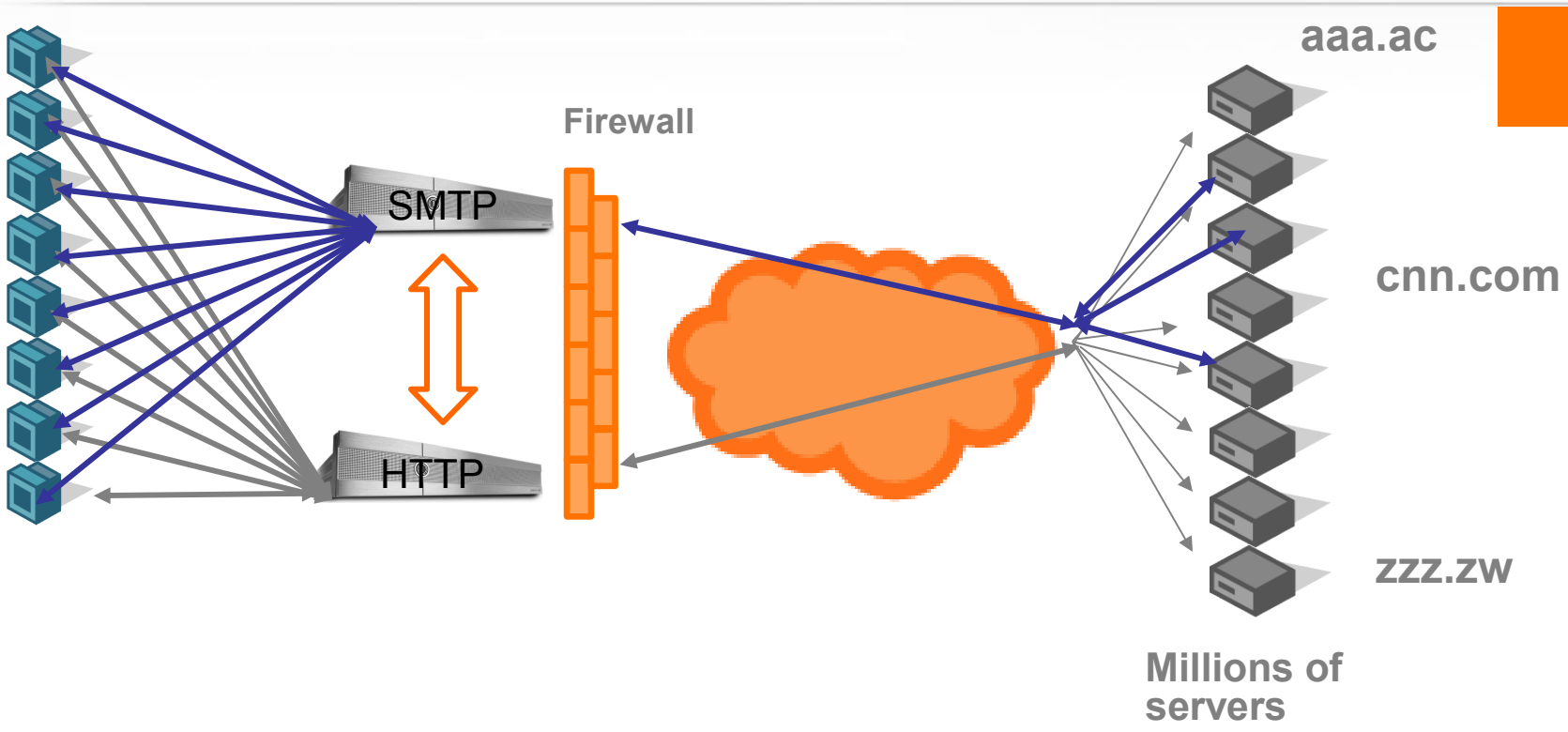


IRONPORT

Rebuilding Trust in Email

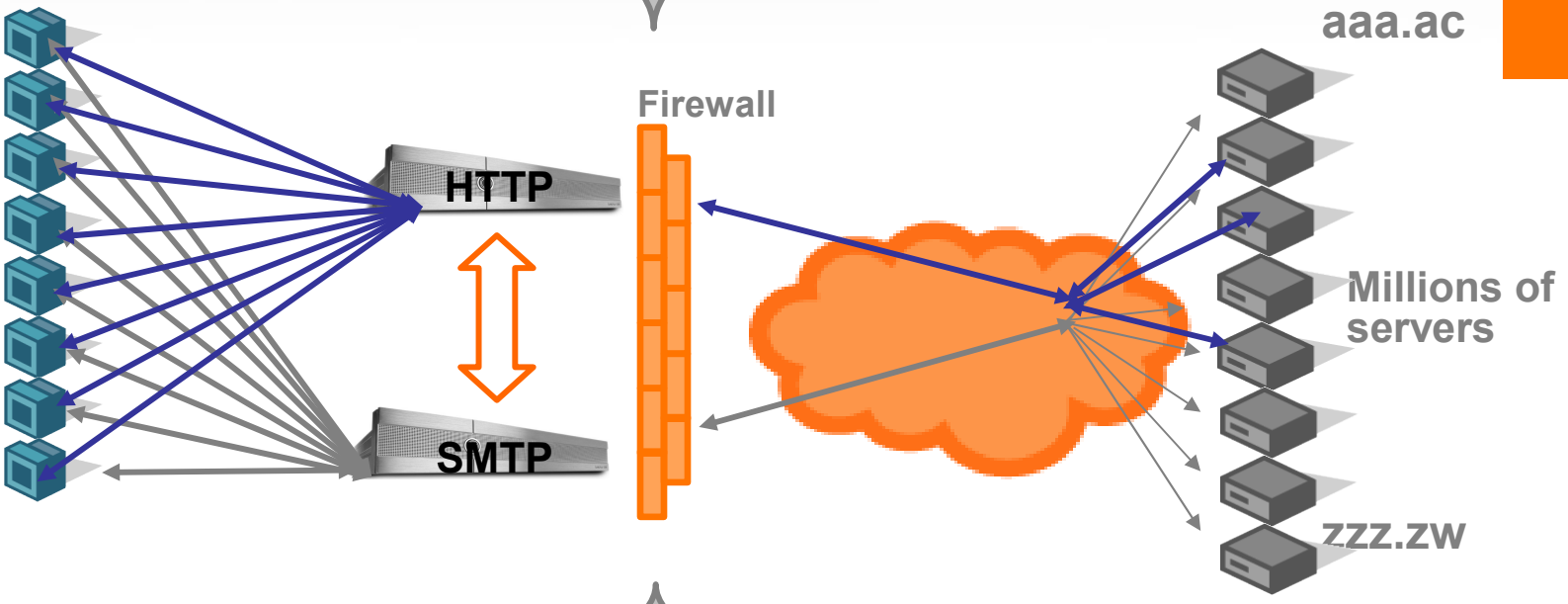
IronPort™

Step1# Email and Web internet gateways must share predicates to secure against evolving threats



Phishing URLs & Domains	Malware URLs & Domains	Malware CLSIDs	Malware Binaries, Short checksums	Malware User Agents

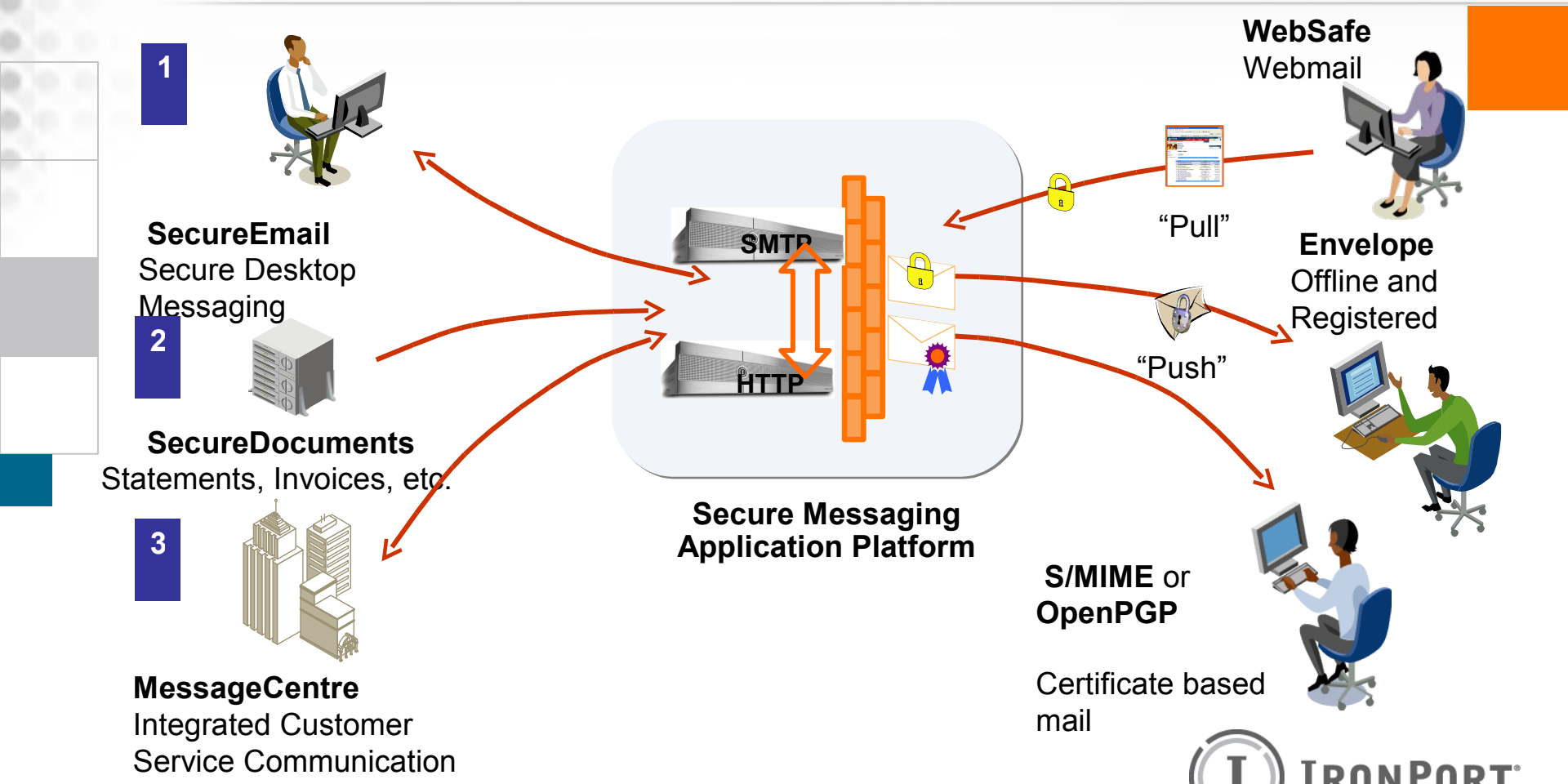
Broad Set of Anti-Malware Predicates



Broad set of AntiSpam Predicates

SpamTraps	Complaint Reports	Message Composition	White/Blacklists	Volume

Step2# Establish encrypted email applications



Without the need for Client software for any mail platfrom

IRONPORT

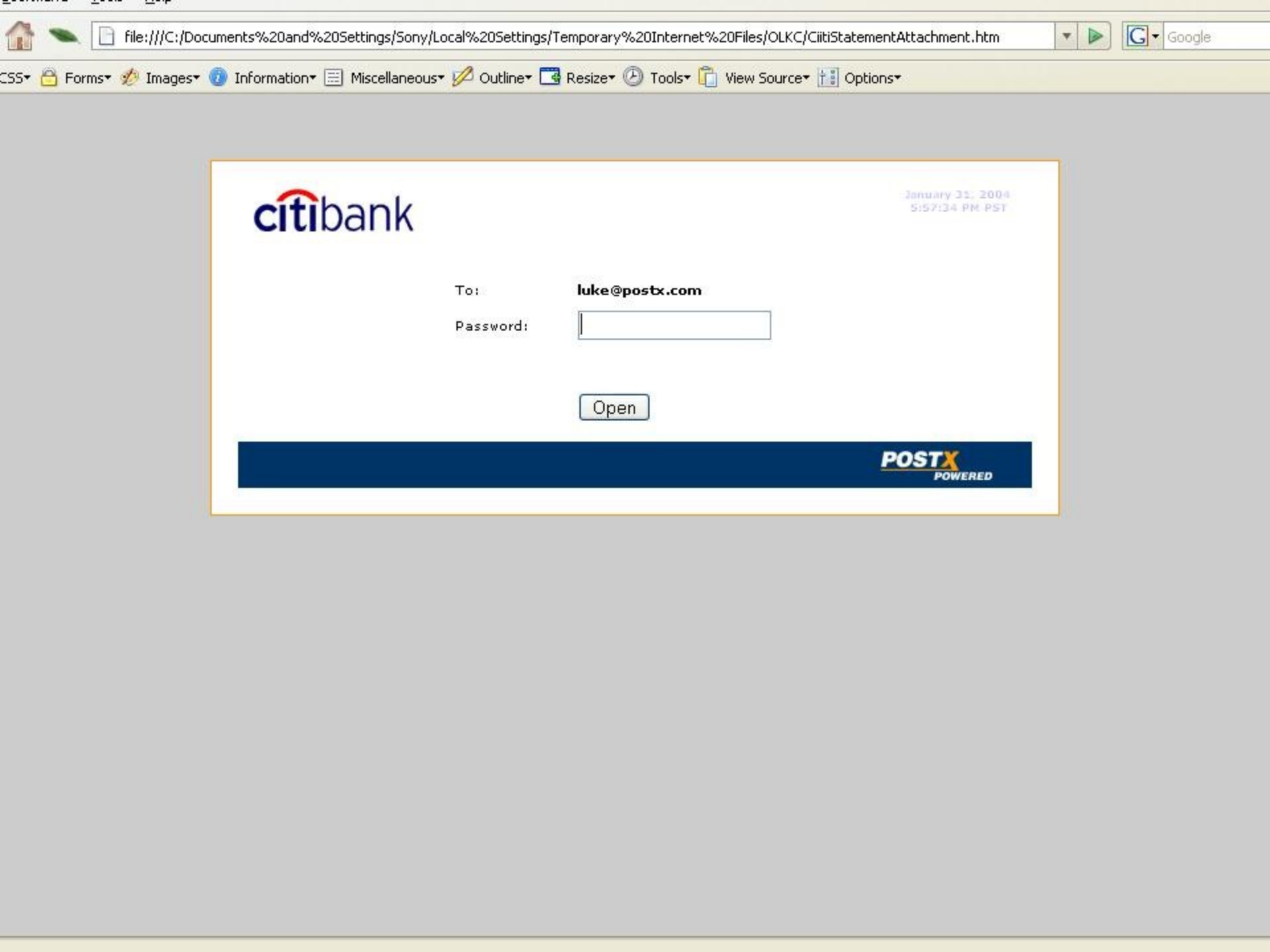
Steps1&2 address Business needs and concerns

- Businesses rely on electronic communications for many of their business processes, however…
  - Concerns about security, especially B→C and B→B

- Legislation and regulations impose tighter regimes for information security and governance
  - Data Protection Act, ISO17799, Sarbanes-Oxley, …

- Businesses can see efficiency savings and new business and revenue opportunities
  - Statements – 60p (paper) vs. 5p (electronic)
  - Customer service - £2.60 (call centre) vs. 6p (email)

IRONPORT


file:///C:/Documents%20and%20Settings/Sony/Local%20Settings/Temporary%20Internet%20Files/OLKC/CitiStatementAttachment.htm
Google
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
citibank
January 31, 2004
5:57:34 PM PST
To:
luke@postx.com
Password:
Open
POSTX
POWERED

citibank 花旗信用卡月結單

- Payment mode/Information
- Marketing Message/ Link
- Term and Condition linkage
- Customer Service
- Your statement

Your statement

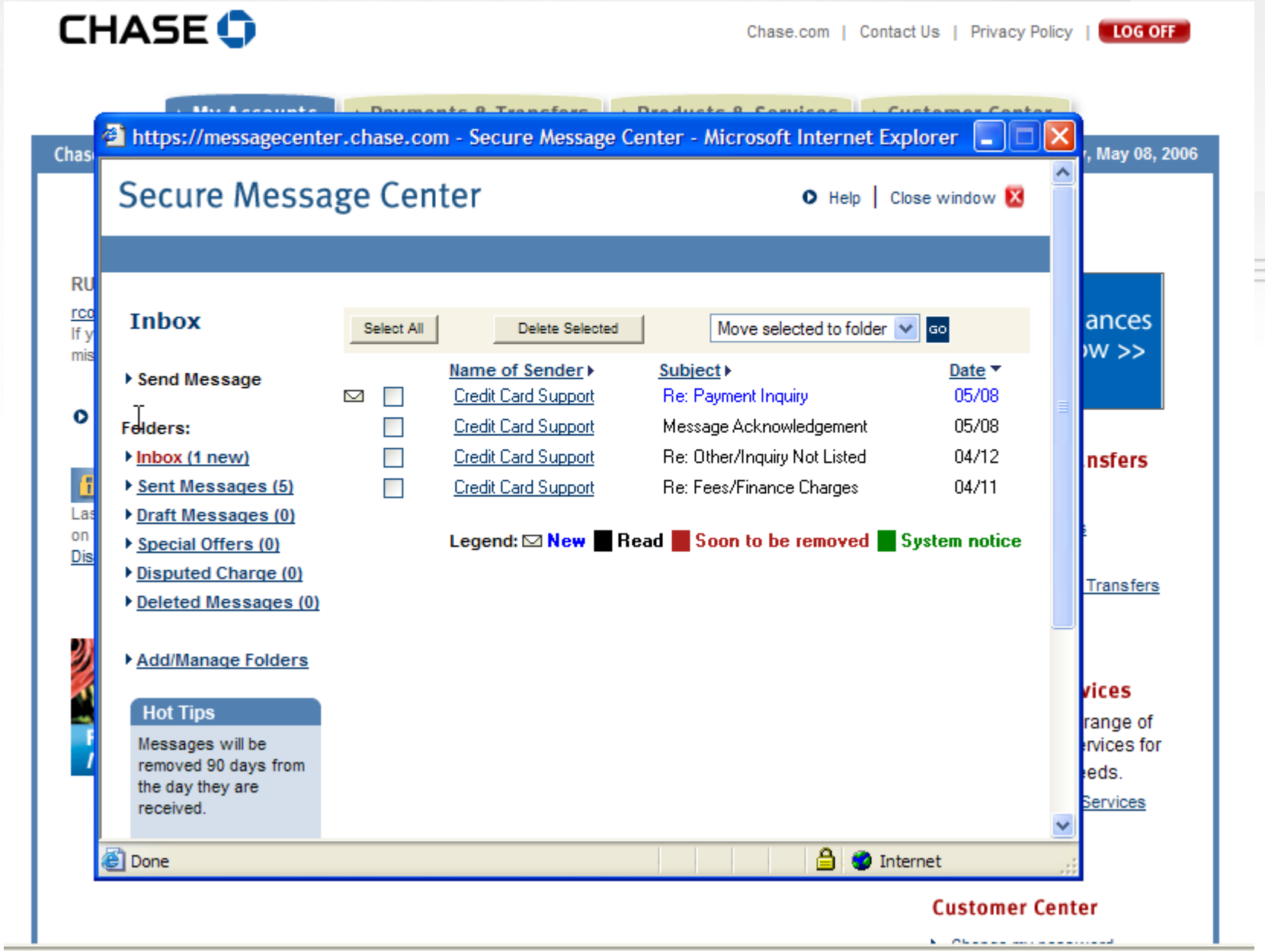
119
台北市信義區基隆路1段159號5樓之1
李建夫 先生/小姐
0287871315
0000062256620220
花旗VISA透明卡
4563188400187203

本期應付總帳單	25,300
最低應繳金額	5,000
繳款截止日	12/25/03

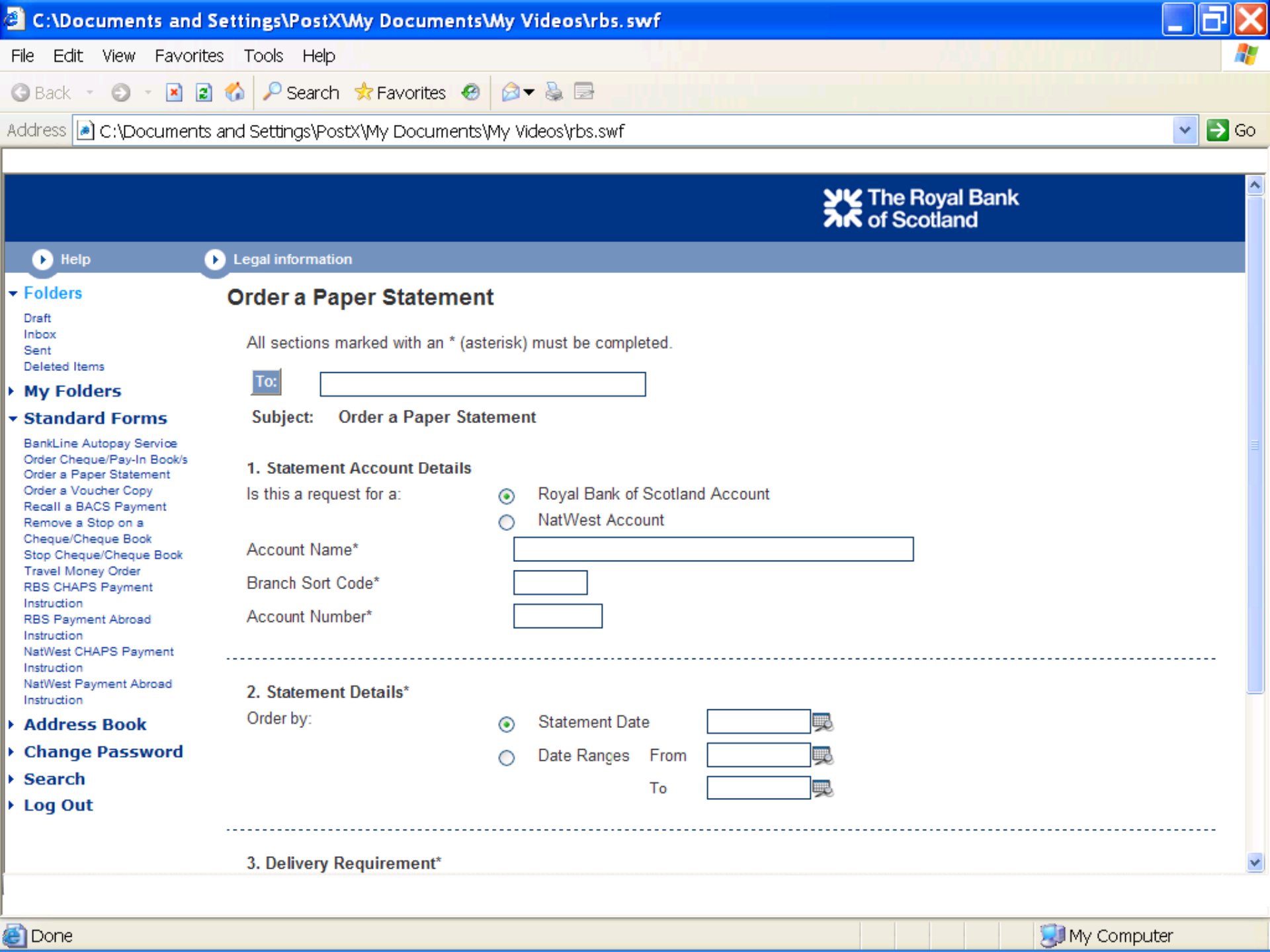
信用額度: 80,000
結帳日: 2003/12/8

Account activity

簽帳日	入帳日	消費類型	說明	金額
			上期應付帳款	94,568
11/15	11/16		謝謝您！提款機付款(郵局繳款)已入帳	- xxxx
11/22	11/23		主卡會員年費	xxxx
11/22	11/26		自動轉帳付款-花旗銀行	xxxx
11/25	11/29		利息費用	xxxx
			小計	xxxx
11/15	11/16	郵購直銷	代繳電話費	xxxx
11/22	11/23	郵購直銷	代繳電費	xxxx
11/22	11/26	郵購直銷	代繳水費	xxxx
11/25	11/29	一般商品	東森得易購股份-分期本金第1期/共12期	xxxx
			這是您的主卡xxxx-xxxx-xxxx-xxxx新增消費	xxxx


CHASE
Chase.com | Contact Us | Privacy Policy | LOG OFF
https://messagecenter.chase.com - Secure Message Center - Microsoft Internet Explorer
Secure Message Center
Help | Close window
Inbox
Select All
Delete Selected
Move selected to folder
go
Send Message
Folders:
Inbox (1 new)
Sent Messages (5)
Draft Messages (0)
Special Offers (0)
Disputed Charge (0)
Deleted Messages (0)
Add/Manage Folders
Name of Sender
Subject
Date
Credit Card Support
Re: Payment Inquiry
05/08
Credit Card Support
Message Acknowledgement
05/08
Credit Card Support
Re: Other/Inquiry Not Listed
04/12
Credit Card Support
Re: Fees/Finance Charges
04/11
Legend: New Read Soon to be removed System notice
Hot Tips
Messages will be removed 90 days from the day they are received.
Done
Internet
Customer Center

IRONPORT


C:\Documents and Settings\PostX\My Documents\My Videos\rbs.swf
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\PostX\My Documents\My Videos\rbs.swf
Go
The Royal Bank of Scotland
Help
Legal information
Folders
Draft
Inbox
Sent
Deleted Items
My Folders
Standard Forms
BankLine Autopay Service
Order Cheque/Pay-In Book/s
Order a Paper Statement
Order a Voucher Copy
Recall a BACS Payment
Remove a Stop on a Cheque/Cheque Book
Stop Cheque/Cheque Book
Travel Money Order
RBS CHAPS Payment Instruction
RBS Payment Abroad Instruction
NatWest CHAPS Payment Instruction
NatWest Payment Abroad Instruction
Address Book
Change Password
Search
Log Out
Order a Paper Statement
All sections marked with an * (asterisk) must be completed.
To:
Subject: Order a Paper Statement
1. Statement Account Details
Is this a request for a:
Royal Bank of Scotland Account
NatWest Account
Account Name*
Branch Sort Code*
Account Number*
2. Statement Details*
Order by:
Statement Date
Date Ranges From
To
3. Delivery Requirement*
Done
My Computer

Private Practice

From: dr.heart@privatepractice.postx.com
To: patient@postx.com
Date: Wed, 16 Mar 2005 14:01:13 -0800
Subject: Appointment Reminder

Secure Reply

Dear Judith Smith --

You are currently scheduled to see Dr. Jones on Friday, May 14, 2004 at 2:00pm.

If you need to reschedule this appointment, please call 123-4567, or you may respond securely to this email using the 'Secure Reply' button at the top of this page.

Regards,

Jane Allen
Administrator

PostX Secured Email

IronPort

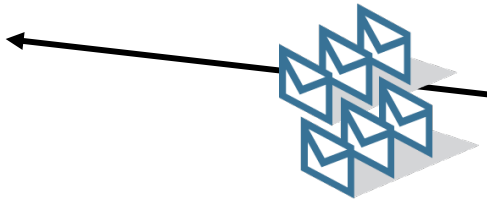
A New Class Of Email Emerges

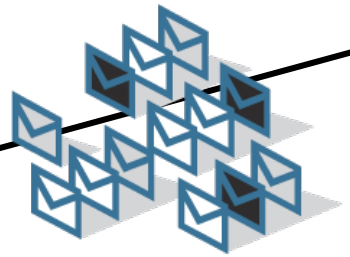
Secure, Authenticated, Business Class Mail

+ DK Authentication
+ Encrpytion
+ Positive Reputation

Reliable, unrestricted service

Trusted Sender





Unknown Sender

- Unwilling to authenticate or encrypt

Service restrictions and filtering

IRONPORT

Questions

Thank You

James Todd
Technical Manager
IronPort Systems
james@ironport.com

IRONPORT