Spam and Crimeware

Christian Heinel
Systems Engineer
Cisco

cheinel@cisco.com

IronPort

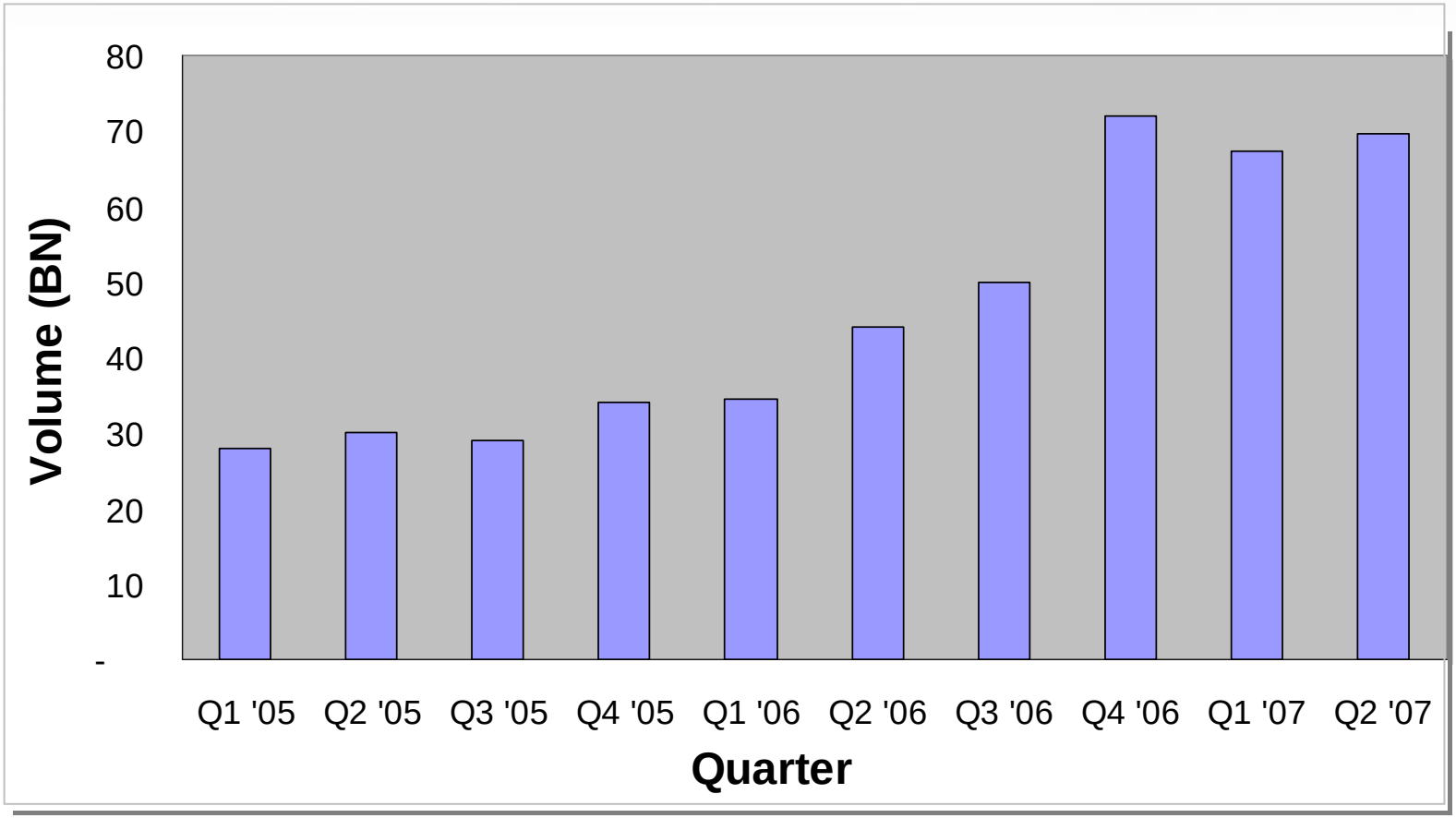
Evolution of hackers & attacks

BEFORE	NOW
Hacking for Glory	Hacking for money
Isolated Hacker	Organized Crime
Visible attacks	Discreet & limited-in-time attacks
Massive attacks	Targeted attacks
From the outside	The user : unwillingly helping the hacker

IRONPORT

Spam Volumes Explode

Average Daily Spam Volumes, By Quarter

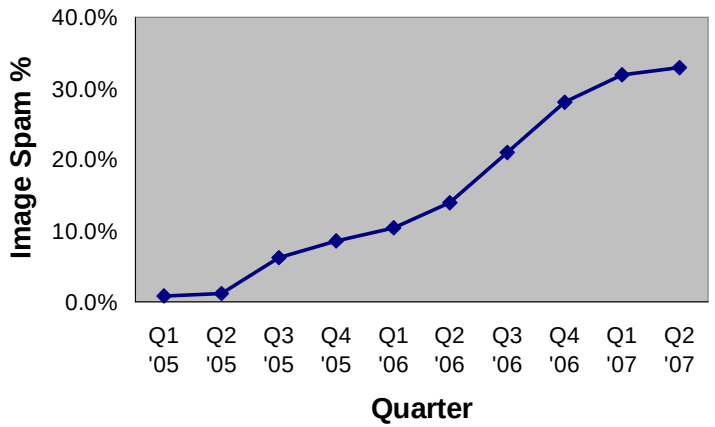


Spam Becomes More Difficult to Catch

Increasingly Sophisticated

- Image spam as a % of overall spam up 7x in last 2 years
- *Accurate spam detection technology is critical*

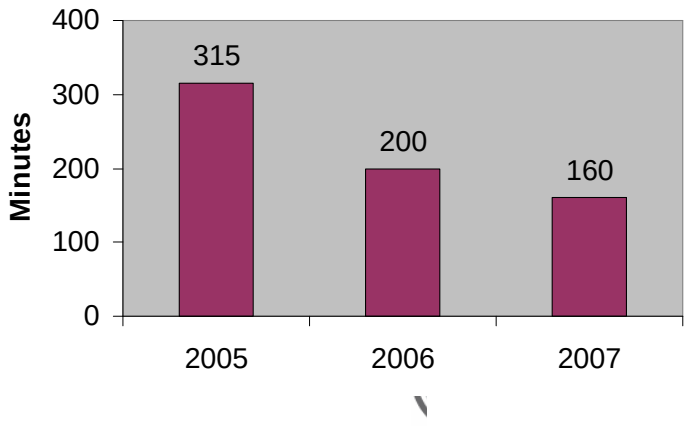
IMAGE SPAM AS % OF TOTAL SPAM



Spreading Quickly

- Emergence of bot networks means that spammers can send twice as fast as two years ago
- *Reaction time to spam outbreaks is critical*

MEDIAN OUTBREAK DURATION



Source: IronPort Systems

Image Spam Gets Sneakier

1. “

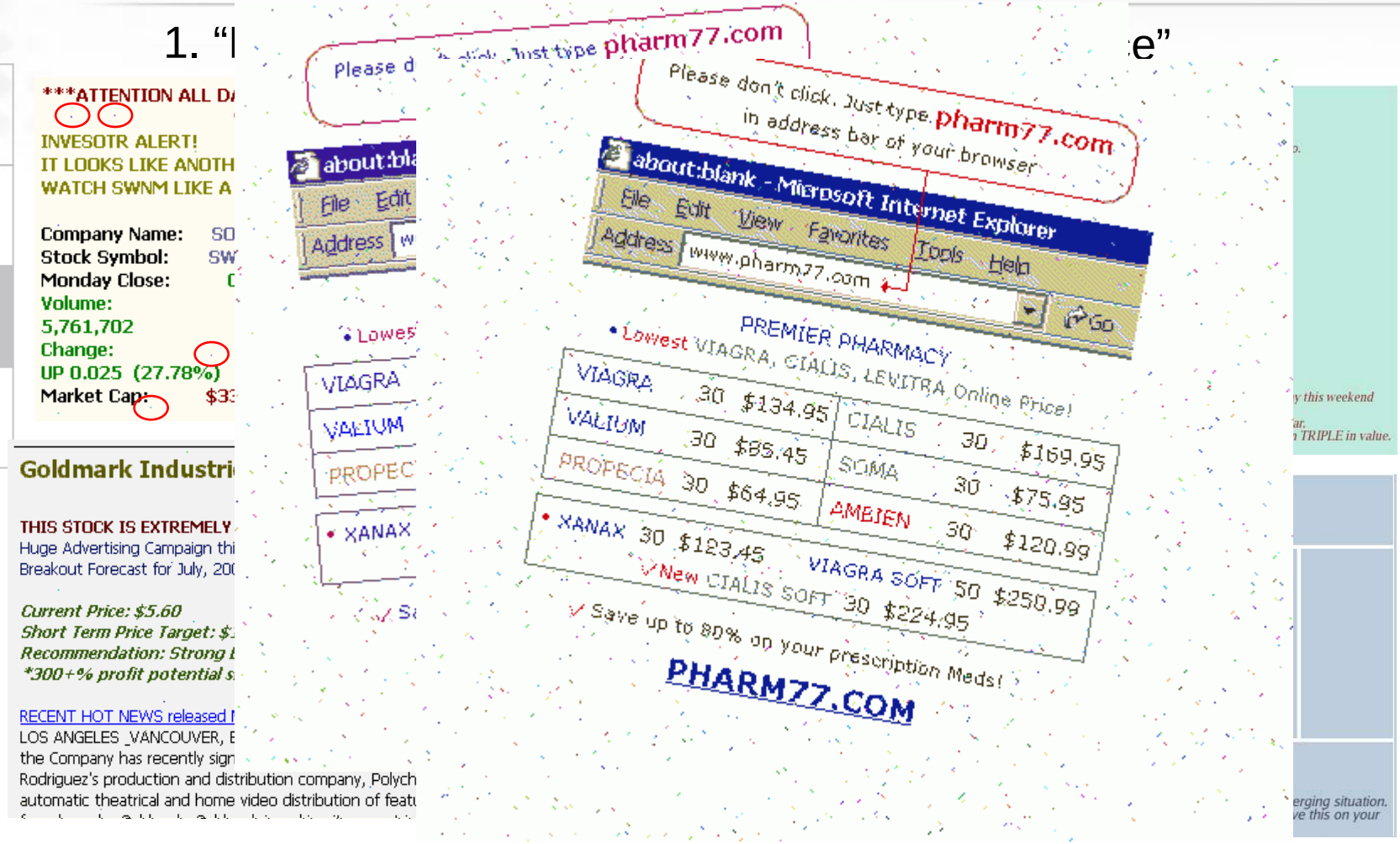
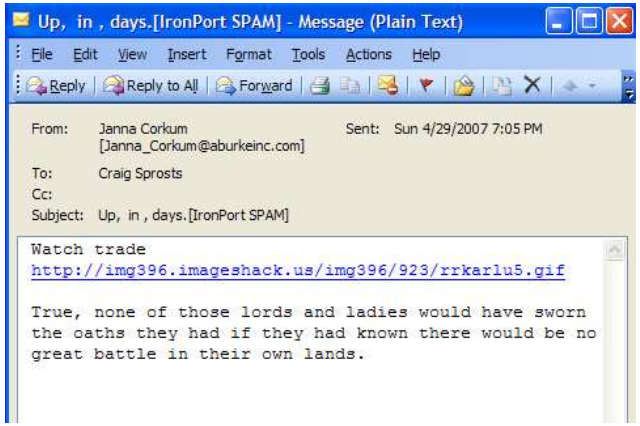
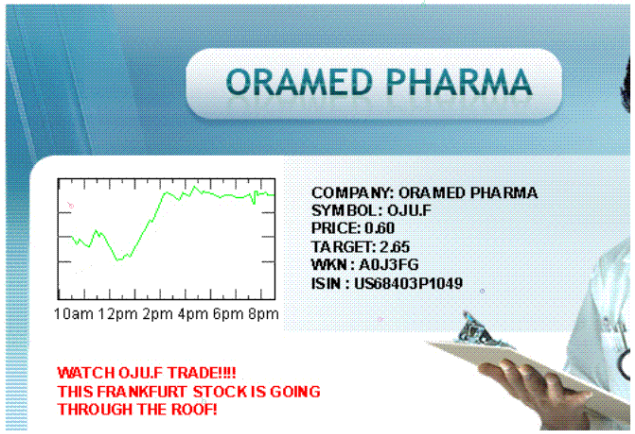


Image-Link Stock Spam Outbreak

Late April - May 2007

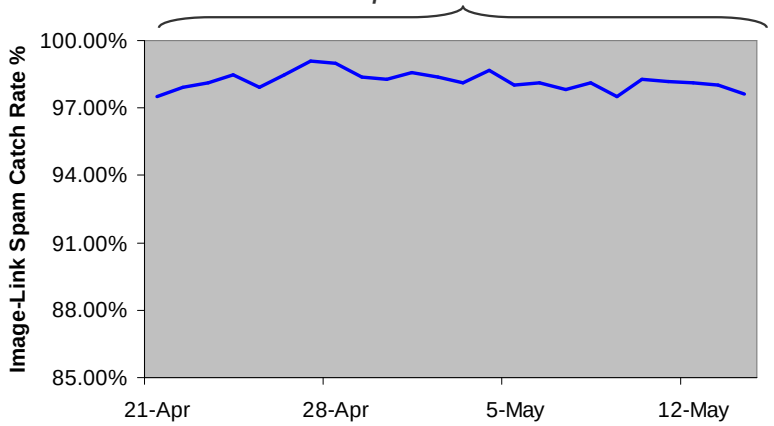


after link is clicked



- URL link references image spam
- 4% of total spam volumes in May
- Very difficult to detect:
  - Legitimate domains are used – domain blacklisting not adequate
  - Web Reputation is essential
  - **IronPort maintains ~98% catch rate against Image-Link spam**

IronPort protects against outbreak in real-time; no drop in catch-rate



Latest Techniques

Started in November ’06

“ASCII Art” Based Spam

- uses a series of numbers to spell out a stock symbol
- numbers randomized in different order for each email to evade signatures
- similar to image spam in that there are no actual words in the email for anti-spam engines to key on

```
> ----- Original Message -----
> From: "Evan Platt" <evan <at> espphotography.com>
> To: <users <at> spamassassin.apache.org>
> Sent: Friday, November 17, 2006 10:48 AM
> Subject: Re: I've got TORA.08 spelled with numbers?
>
>
> > At 07:44 AM 11/17/2006, you wrote:
> >>I'm getting a bunch of spams this morning that have
> >>TORA.08 spelled out with numbers like this.
> >>
> >>4216775   0611576   215556        7            3308011   3258576
> >>    6      7     5   1    5       3 8           5     2   7     3
> >>    8      3     6   5    0      4   1          2     7   0     5
> >>    7      2     2   257873     5     7         4     1   3387715
> >>    6      2     5   7  1      111500075       8     6   2     2
> >>    8      2     2   7   7      3       2   656   0     3   0     8
> >>    0      6430533   4    4     8       6   207   5412501   7637213
> >>
```

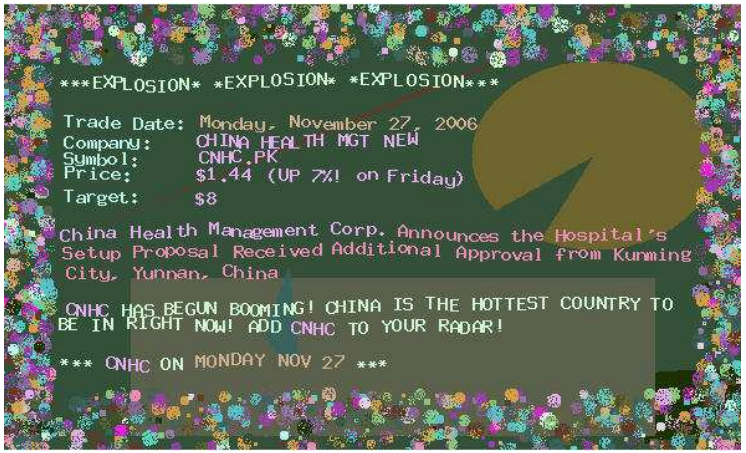


Image Spam 2.0

- Attempts to mask itself as a legitimate picture by adding “greeting card” like border”
- Inserts shapes such as rectangles and pies to spoof powerpoint / excel charts
- Wavy text more difficult for OCR technologies to decipher

PDF spam

IRONPORT

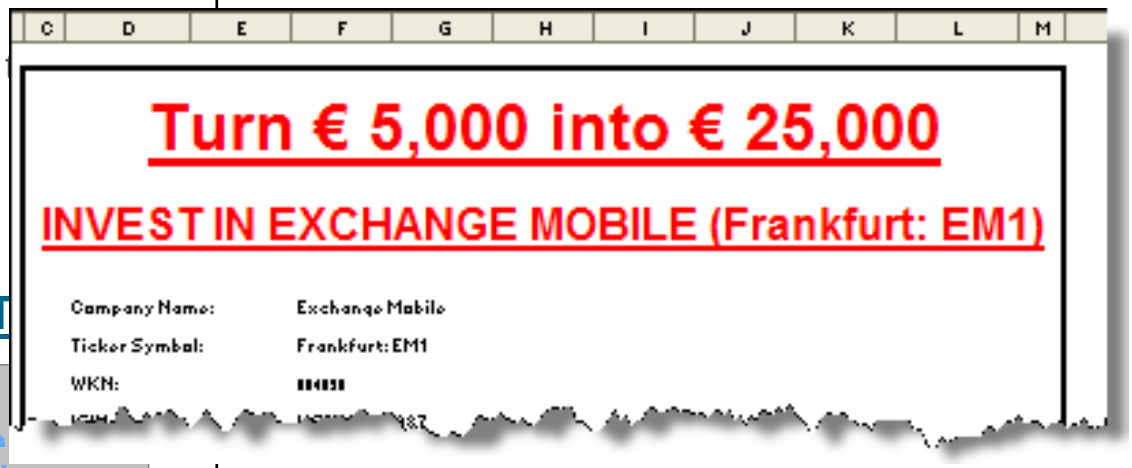
Excel Spam

July 21st, 2007

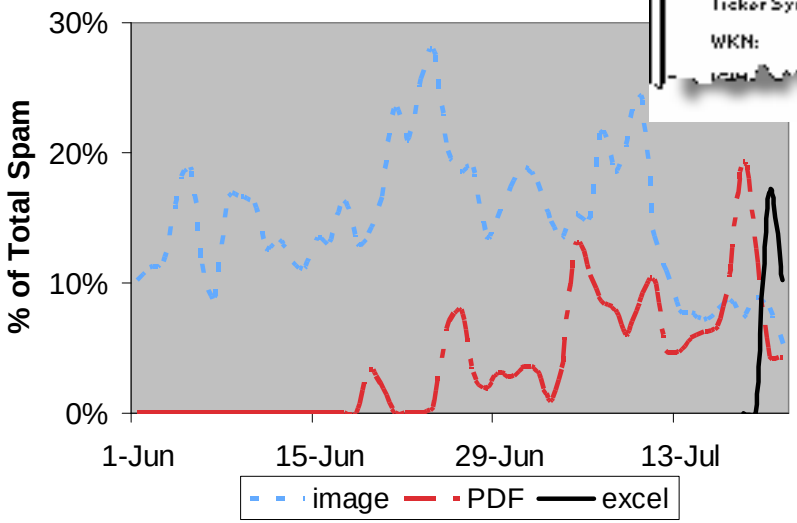
OUTBREAK DESCRIPTION

- Spam sent as text inside excel file
- First appeared July 21st, 2007
- Within hours, represented 17% of
spam volumes

EXCEL SPAM EXAMPLE



SPAM VOLUMES BY T



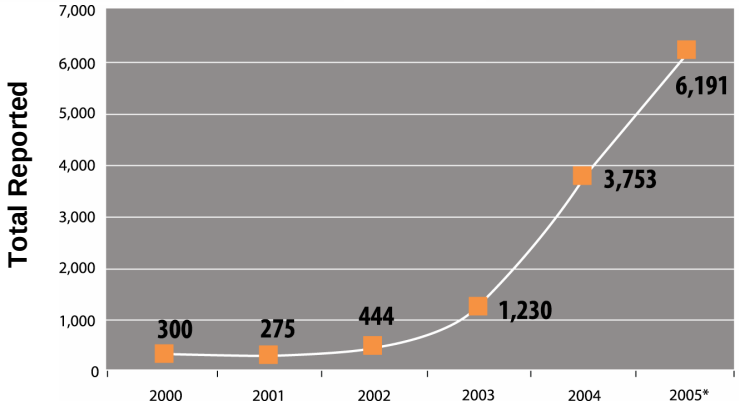
Spyware & Keyloggers are spreading

Number of pieces of spyware (in thousands)

Source : State Of Spyware Report/Web Security Report 2006/ Internet Security Trends 2007

- 144 000 different pieces of spyware (end of Q2 2006)
- More than 1 corporate desktop out of 10 is contaminated on a worldwide basis

Evolution of keyloggers 2000-2005



Source: iDefense Labs, November 2005

- High Growth
- Recording of key strokes and sending to external servers
- Current evolution : screen scrapers

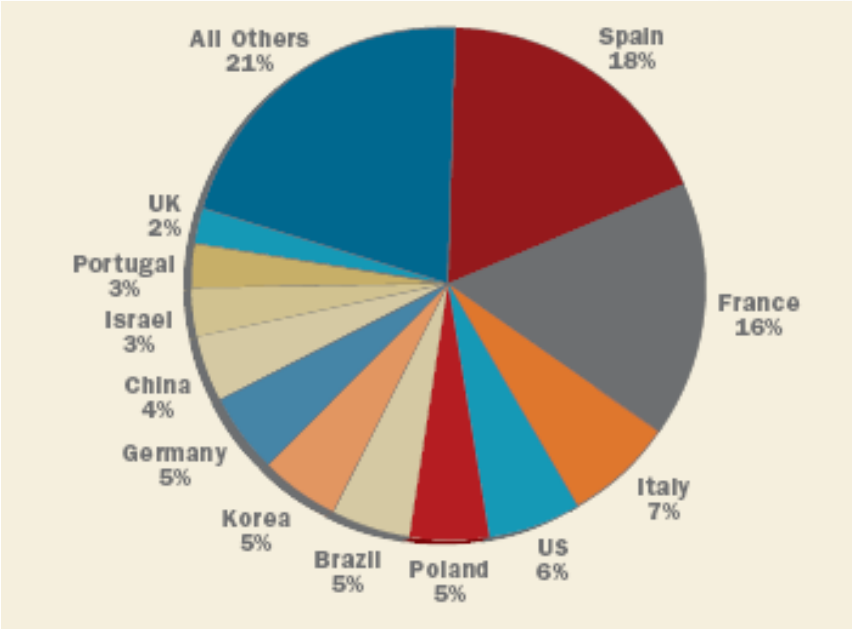
IRONPORT

Zombie networks are multiplying

- « Bot » (or robot) : « sleeping code » installed on a desktop without the user knowing it, doing nothing at that time. The hacker can remotely start an attack thanks to that code.
- The contaminated PC becomes a real zombie, following the hacker's orders.
- Iberia: ranked 5th on a worldwide basis (5% of global zombies)
- Uses : Denial of service, cyber-extorsion, phishing, spam, etc.

IRONPORT

Example of a large-scale spam attack using zombies

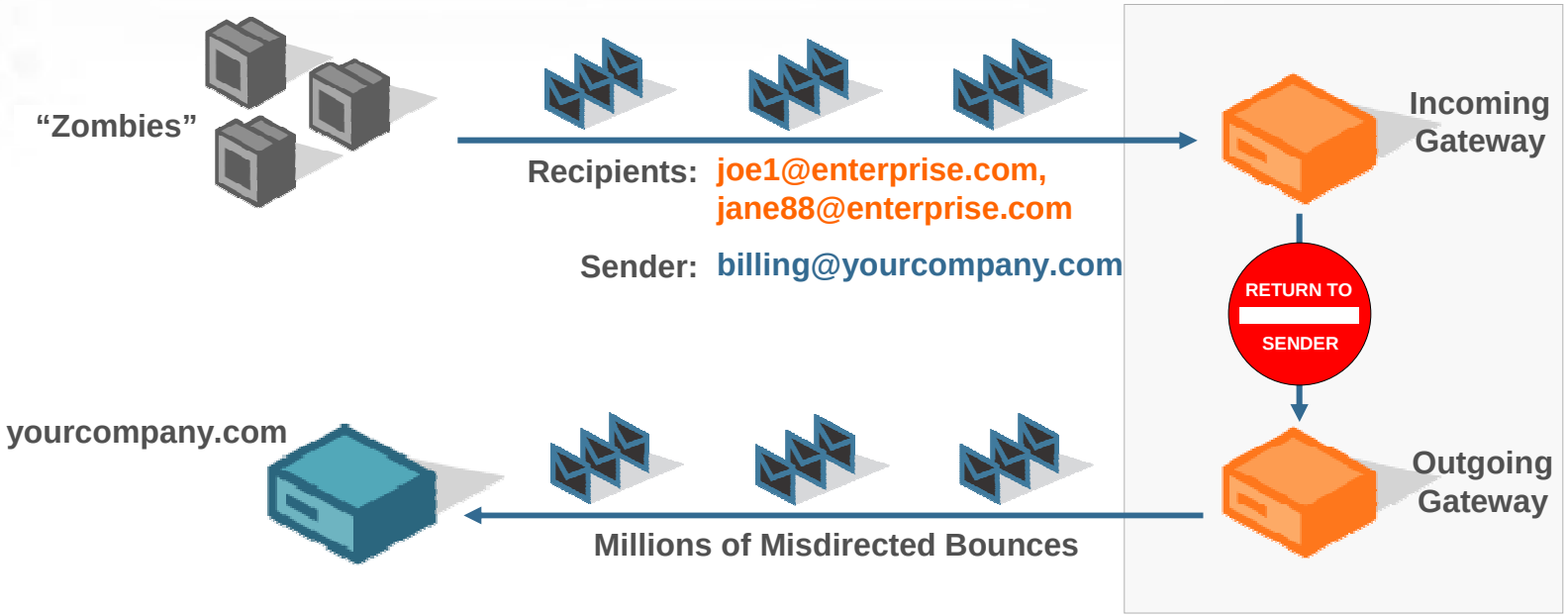


- More than 80% of spam is sent through zombies
- EXAMPLE : A single spam attack uses zombies from more than 100 different countries

IRONPORT

The Misdirected Bounce Threat

*Makes Up 9% of all Internet Email**



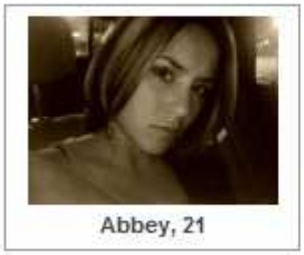
More than 55% of F500s have experienced disruption of service or a total denial of service due to misdirected bounces

IRONPORT

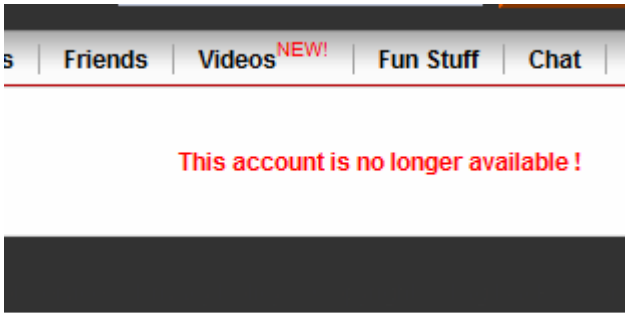
**Source: IronPort Threat Operations Center,*
INTERNET EMAIL TRAFFIC EMERGENCY: SPAM "BOUNCE" MESSAGES ARE COMPROMISING NETWORKS, April 2006.

Social networking sites

- Profiles attract requests

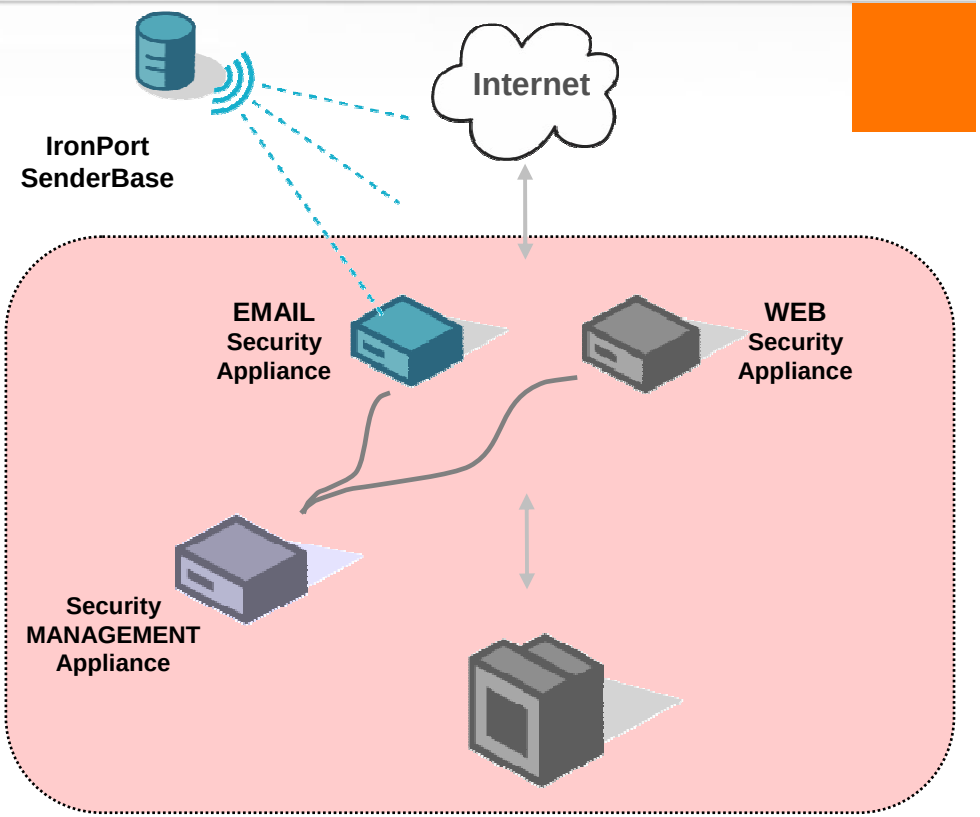


- Social engineering - got to my site to contact me
  - Page shows personal details to contact
  - Site contains malware
- 2 weeks later



IRONPORT

The IronPort Vision



Web Security | Email Security | Security management

IRONPORT

Reactive Security

IRONPORT

SenderBase® / Threat Operations Center

SenderBase

TOC

- **Expert** team of skilled analysts
- Staffed **24 x 7 x 365**
- **32 languages** spoken
- **Documented & verified** processes

+ than 90 parameters

- *Data Volume*
- *Message Structure*
- *Complaints*
- *Blacklists, whitelists*
- *Off-line data*

E-Mail Reputation Filters → **Reputation Score**

+than 45 parameters

- *URL blacklists & whitelists*
- *HTML Content*
- *Domain Info*
- *Known "bad" URLs*
- *Website history…*

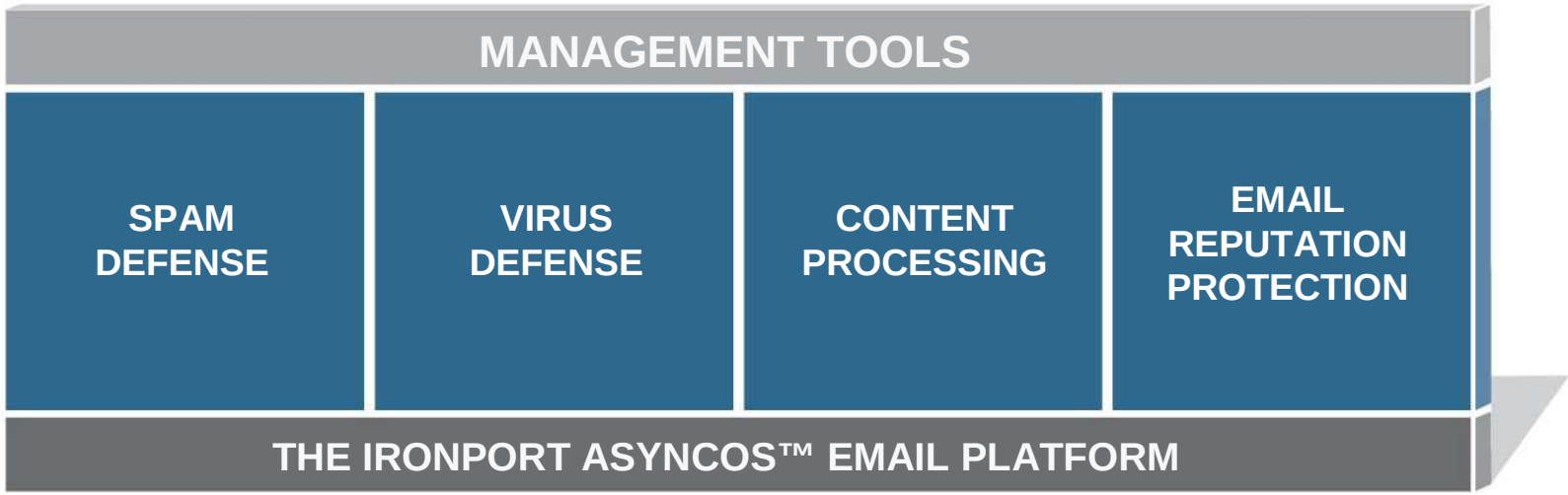
Web Reputation Filters → **Reputation Score**

E-Mail Security

IronPort C-Series

IRONPORT

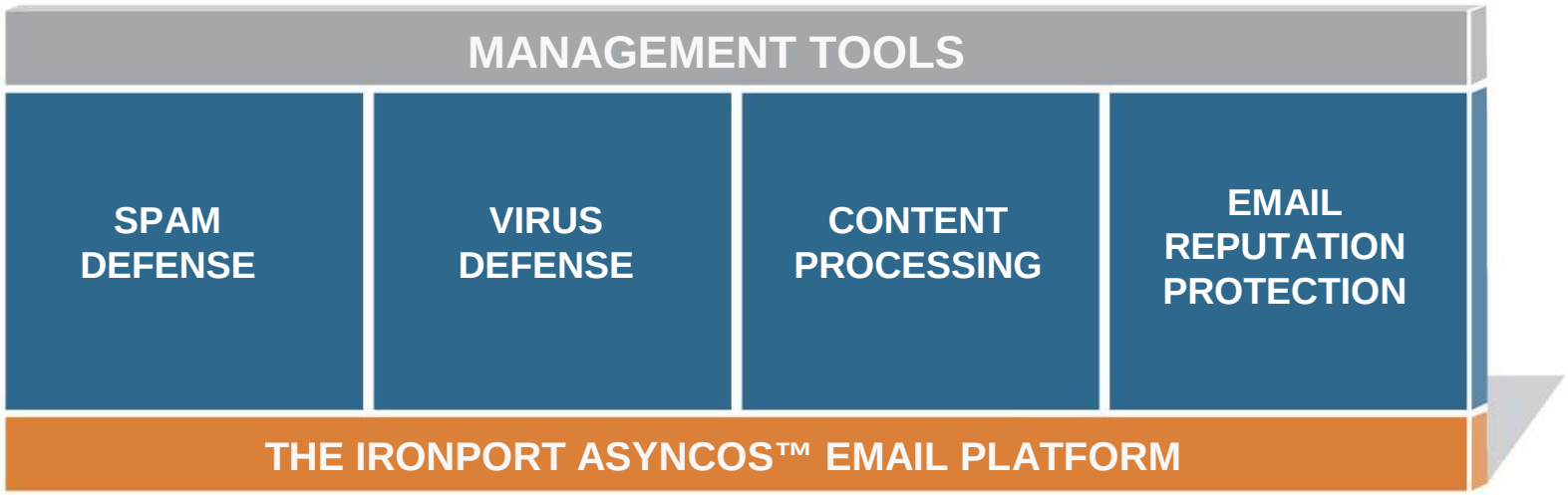
C-Series Architecture



IRONPORT

The MTA is your first protection

AsynOS : new generation MTA

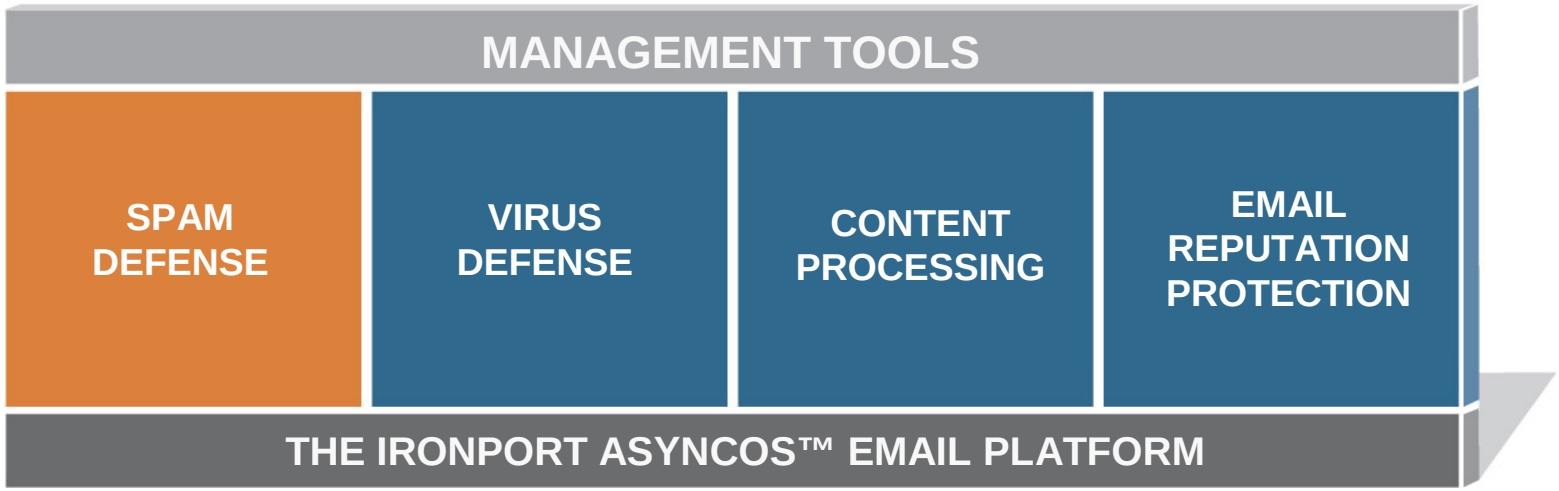


- **AsyncOS** – dedicated & optimized OS for the e-mail, allowing 10.000 simultaneous SMTP connections
- **Advanced Queue Management** - queues per domain, retry schedule on a per-domain basis, etc.
- **Virtual Gateway™** – Protects the reputation of your messaging server
- **Directory Harvest Attack Prevention** – Protection against Directory Harvest Attacks

IRONPORT

Multi-layer Spam Defense

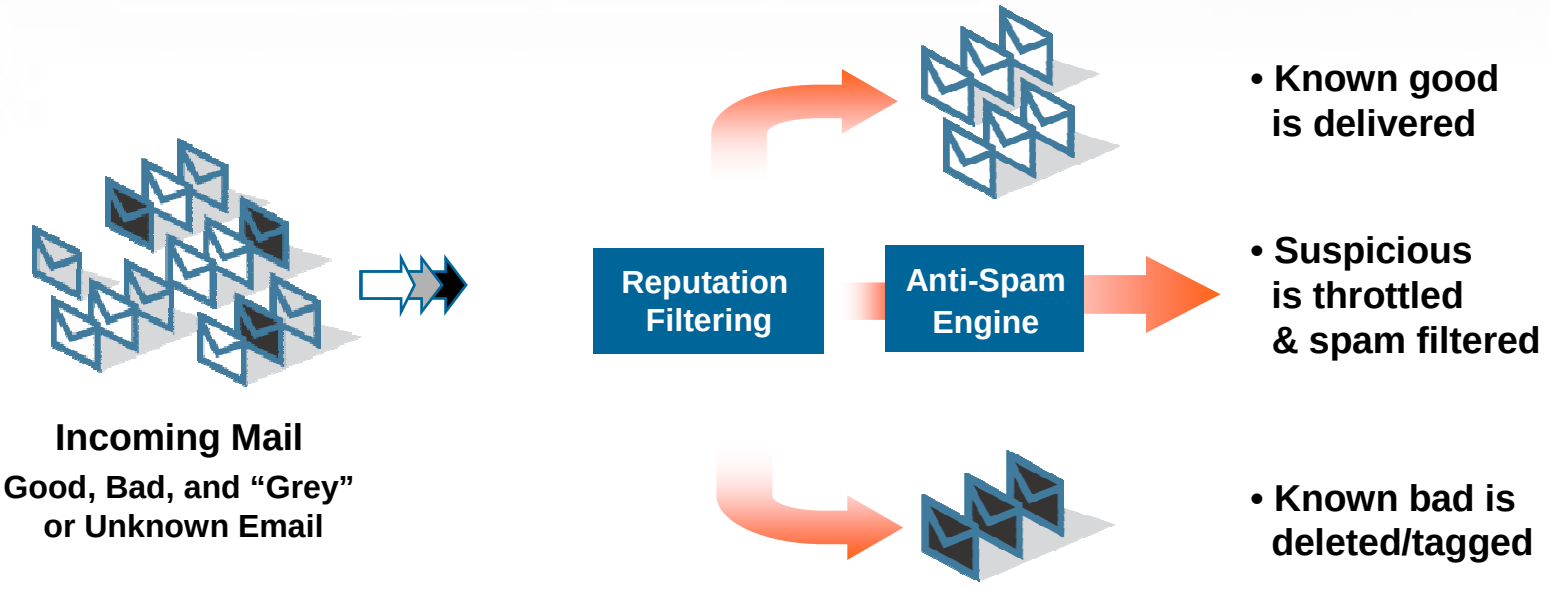
Best of Breed



- **Preventive : IronPort Reputation Filters** – the first layer of defense, at the connection level
- **Reactive : IronPort Anti-Spam** – at the content level

IRONPORT

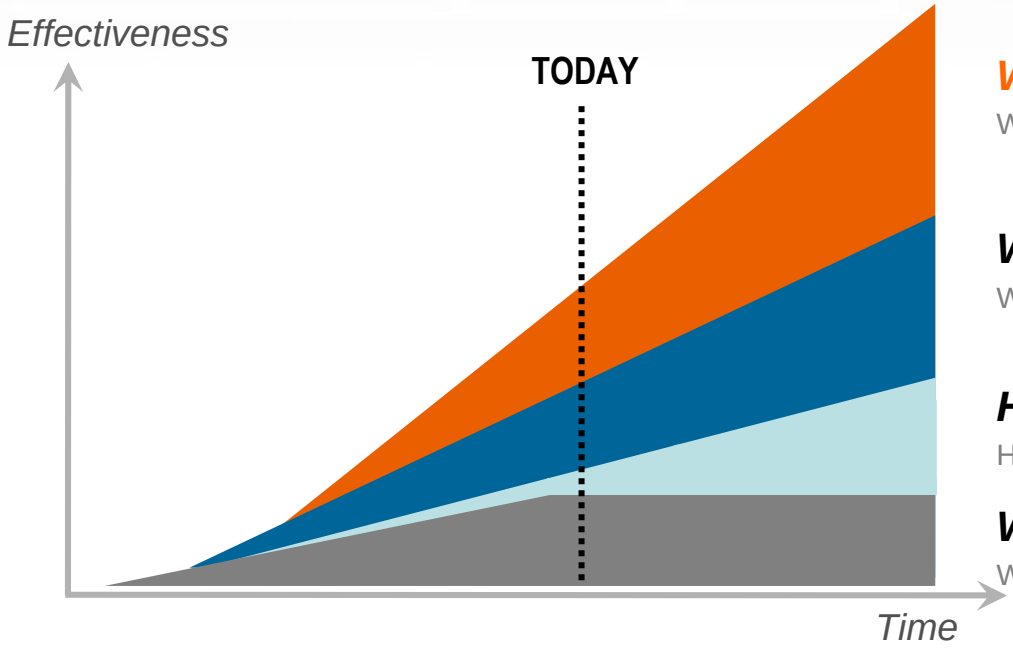
IronPort Reputation Filters Stop 80% of Hostile Mail at the Door….



- IronPort uses identity & reputation to apply policy
- Sophisticated response to sophisticated threats

IRONPORT

IronPort Anti-Spam (IPAS)
4 questions for a 97% capture rate



Where? **Web Reputation**
Where does the call to action take you?

Who? **Email Reputation**
Who is sending you this message?

How? **Message Structure**
How was this message constructed?

What? **Message Content**
What content is included in this message?

- Content filtering techniques alone are inadequate
- Email & Web reputation systems improved protection
- Capture rate >97% with false positives fewer than 1 on a million

IRONPORT

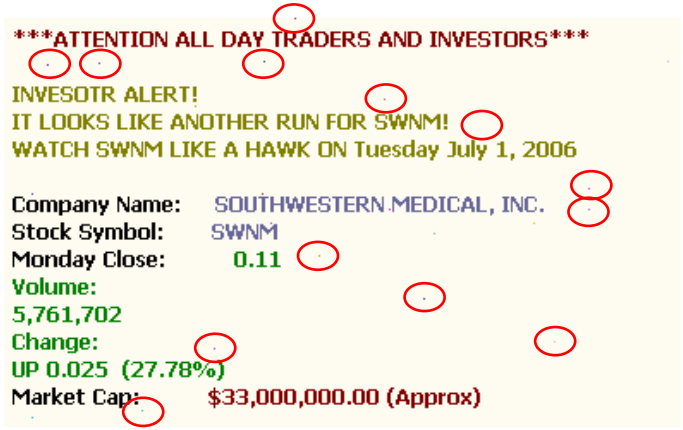
Image Spam Example

HOW?

- *Message leaves trace of spamware tool*

WHAT?

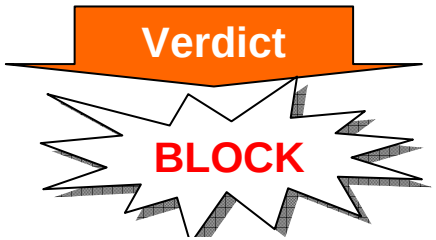
- *All text inside an image*
- *Random dots appear within the message*
- *Nearly identical color scheme in 100,000's spamtrap messages*



WHO?

- *IP address recently started sending email*
- *Sending IP address located in Russia*

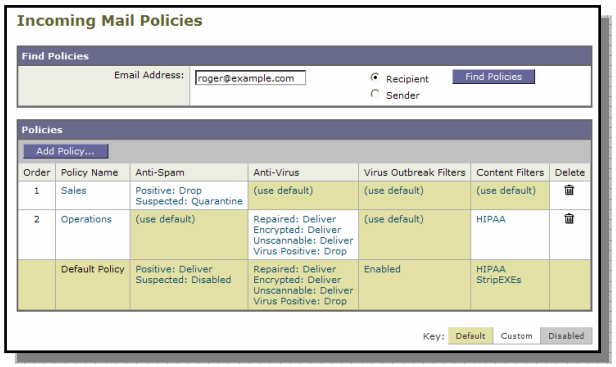
WHERE?



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

Management Capabilities

Comprehensive Administrator Controls



Intuitive User Interface

- **Drop spam positive, quarantine suspect**
- **Drop spam positive for all others**

Group 1

- **Quarantine spam positive**
- **Conservative spam thresholds**

Group 2

- **Drop spam positive & suspect**
- **Aggressive spam thresholds**

Group 3

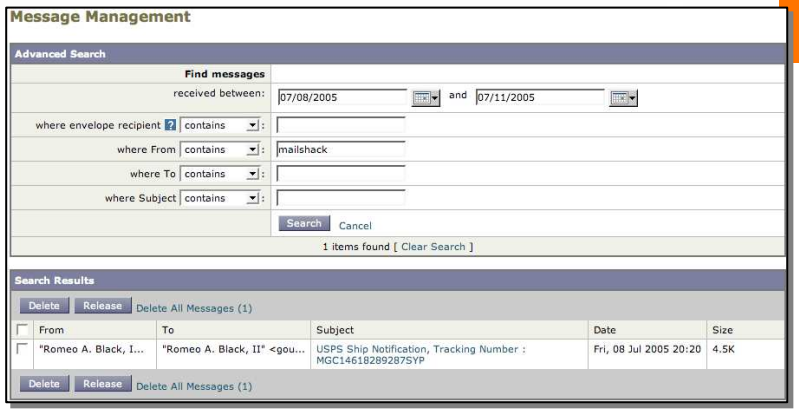
Domain, Email Address, or LDAP Group

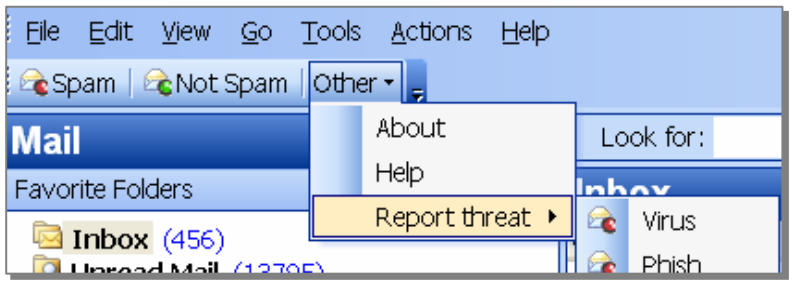
- Manage global configurations
- Set user and group policies with Email Security Manager
- Configure IronPort Spam Quarantine, Email “Digest”

IRONPORT

Management Capabilities
End User Controls

- Spam Quarantine
  - Fully featured quarantine for admins & end users
  - On-box or consolidated quarantine (M-Series)
  - Authenticate users against LDAP, AD, or IMAP/POP
- Outlook Plug-in
  - One-click reporting of spam, viruses & phishing attacks
  - Block & Allow lists supported natively in Outlook

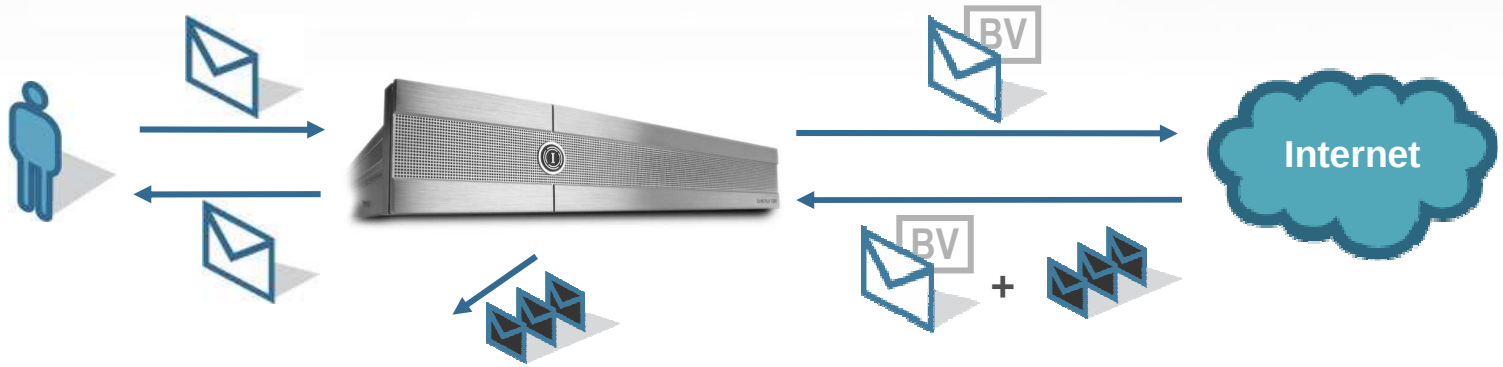




IRONPORT

IronPort Bounce Verification™

Protects Against Misdirected Bounce Attacks

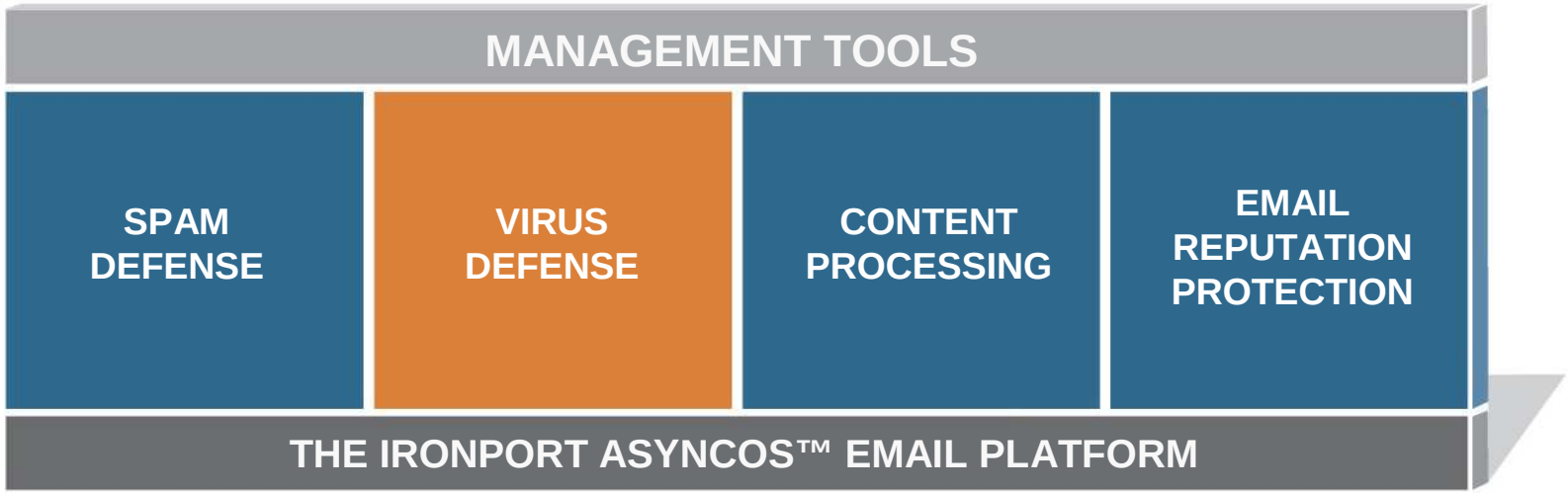


- All Outgoing Mail Stamped Allowing **Legitimate Bounces to be Identified on Return**
- Transparent to End Users, No Industry Adoption Required
- **Eliminates Help Desk Calls and End User Confusion**
- Another IronPort Technical “First"

IRONPORT INNOVATION

IRONPORT

2. Multi-layer Virus Defense



- **Preventive : IronPort Virus Outbreak Filters** stop outbreaks 13 hours ahead of signatures
- **Reactive : Sophos Anti-Virus** & **McAfee Anti-Virus** signature-based solutions

IRONPORT

Virus Outbreak Filters

A few figures…

Virus Name	IronPort	Sophos	McAfee	Trend Micro	Symantec
Troj/SpamToo-AG	04/18/2007 20:50	+0d 15h 34m	+0d 21h 48m	+1d 8h 19m	+0d 22h 8m
Trojan Peacomm!zip	04/12/2007 18:44	Not Published	Not Published	+0d 7h 37m	+0d 1h 55m
W32.Virut!dr	04/12/2007 05:57	+1d 6h 58m	+1d 10h 44m	Not Published	+1d 10h 28m
W32/Dref-AG	04/11/2007 21:03	+0d 3h 55m	+0d 22h 25m	+0d 11h 13m	Not Published
Troj_Virut.WX	04/11/2007 07:26	Not Published	+2d 9h 15m	+2d 6h 33m	+2d 8h 59m
Troj/DwnLdr-GTK	04/10/2007 16:13	+2d 20h 42m	+3d 1h 18m	+3d 1h 5m	+3d 1h 59m
W32/Dref-AF	04/08/2007 18:16	+0d 2h 23m	+0d 20h 54m	+0d 17h 45m	+1d 0h 20m
W32/Grum-A	03/29/2007 18:30	+0d 6h 22m	+0d 22h 50m	Not Published	+0d 20h 51m
Troj/DwnLdr-GFN	03/03/2007 14:25	+1d 17h 29m	+2d 3h 20m	+1d 19h 46m	+2d 4h 15m
W32/WowPWS-AU	03/03/2007 19:59	+0d 6h 49m	+1d 21h 46m	+2d 4h 13m	+1d 5h 11m
W32/Stration.DR	02/23/2007 13:10	Not Published	+0d 5h 19m	+2d 14h 53m	+0d 5h 12m
Troj/Clagger-AZ	02/19/2007 18:21	+0d 3h 30m	+0d 22h 8m	+0d 20h 11m	+0d 14h 24m
Troj/Dloader-ATK	02/19/2007 05:12	+0d 9h 42m	+0d 11h 29m	+0d 22h 46m	+0d 13h 33m
Troj/Clagger-AX	02/14/2007 06:27	+0d 3h 28m	Not Published	+1d 0h 11m	+0d 15h 16m
Troj/StraDl-D	02/14/2007 02:35	+0d 1h 48m	+0d 14h 0m	Not Published	+0d 19h 8m
W32/Dref-AB	02/13/2007 20:10	+0d 4h 3m	Not Published	Not Published	+1d 1h 33m
Troj/Dloadr-ATD	02/12/2007 09:56	+0d 4h 8m	Not Published	+0d 18h 59m	+0d 11h 12m
Troj_Cimuz.BF	02/11/2007 12:41	Not Published	Not Published	+0d 16h 3m	+1d 8h 27m
Troj/DwnLdr-GAI	02/10/2007 11:32	+0d 0h 56m	Not Published	+1d 17h 12m	+2d 9h 36m
Troj/DwnLdr-GAG	02/08/2007 06:34	+0d 7h 3m	Not Published	+0d 23h 1m	+0d 11h 11m

Average lead time*……over 13 hours

Outbreaks blocked * ……175 outbreaks

Total incremental protection*……over 94 days

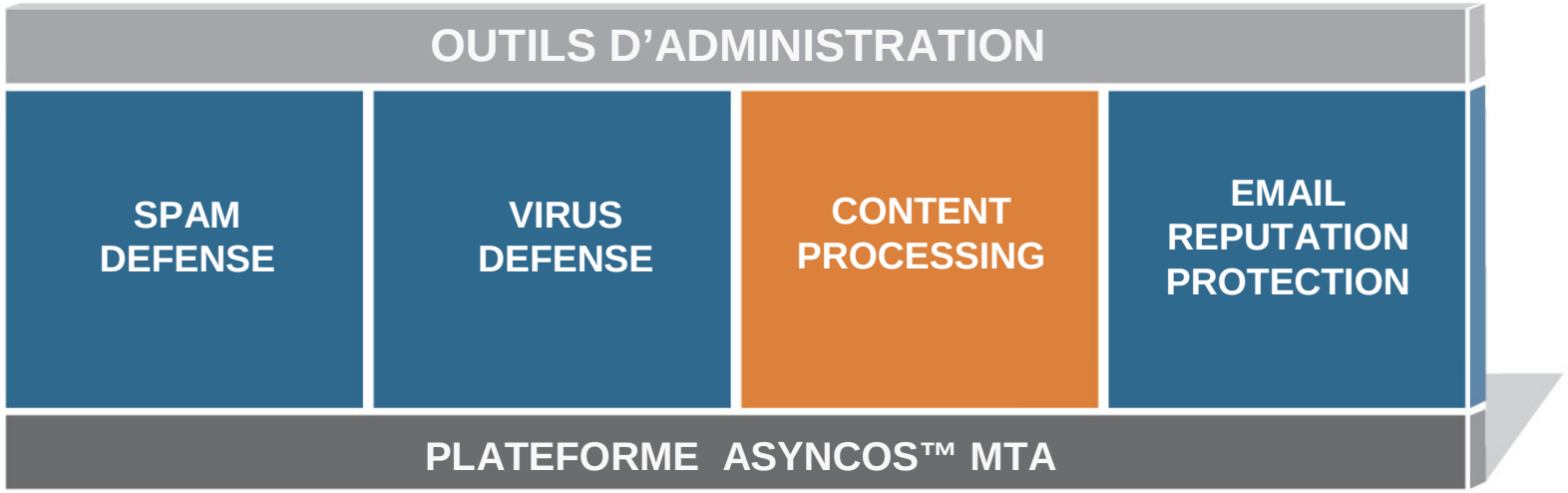
IRONPORT

** Between Nov. 2005 et Dec. 2006.*

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..

3. Content Processing

Filters & Encrypts contents

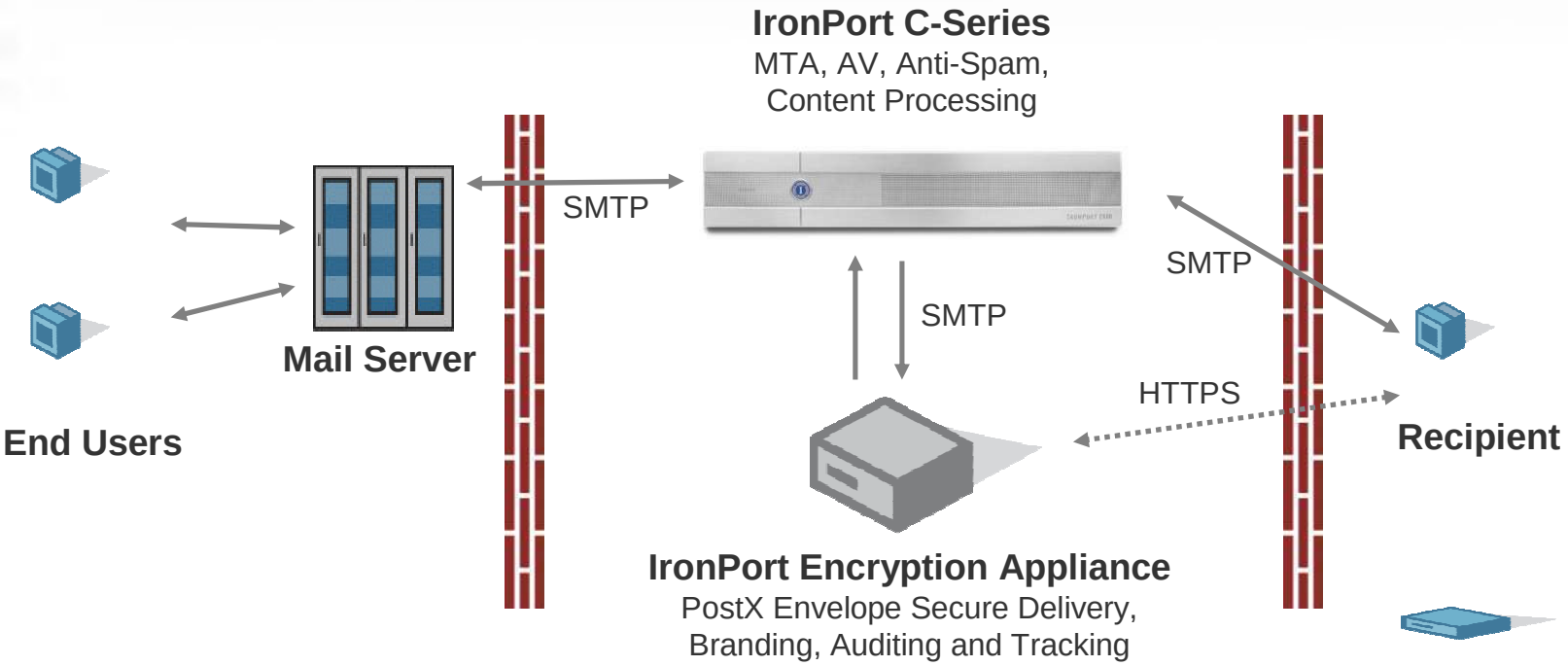


- **Content Analysis Rules** defined according to source or destination IP, domain or address, headers, keywords in message body or attachments, attachment size or type, reputation of a sender or data available in an LDAP query.
- **Actions** taken include quarantine, redirect, notify, tag, archive, bounce, encryption.

IRONPORT

IronPort E-Mail Encryption

PostX E-Mail Delivery Solution

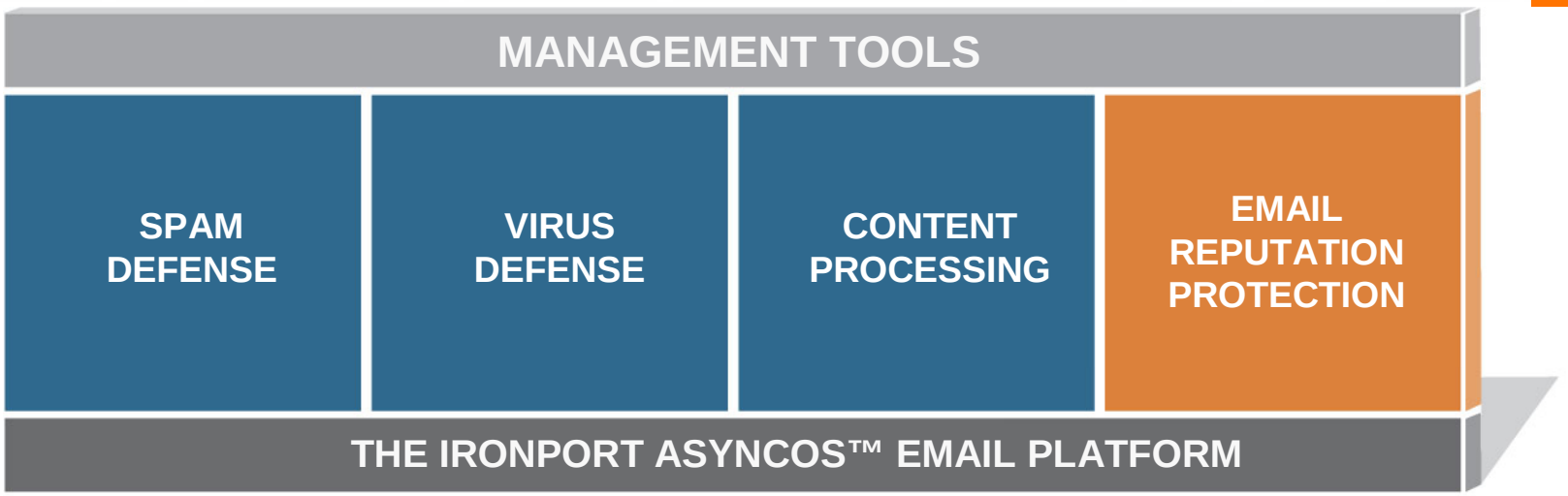


Flexible & easy-to-use solutions:

- No need of a client software on the recipient's desktop
- All messaging platforms supported
- Various delivery methods : push, pull, certificates

IRONPORT

4. Protection of your E-Mail reputation on the Internet



DomainKeys – Makes sure that the sender of an e-mail is really the one written.

300M+ Email Accounts Use DomainKeys to Authenticate the Email Sender

IRONPORT