IronPort®

Trends & Threats
June 08

Robin Sundin

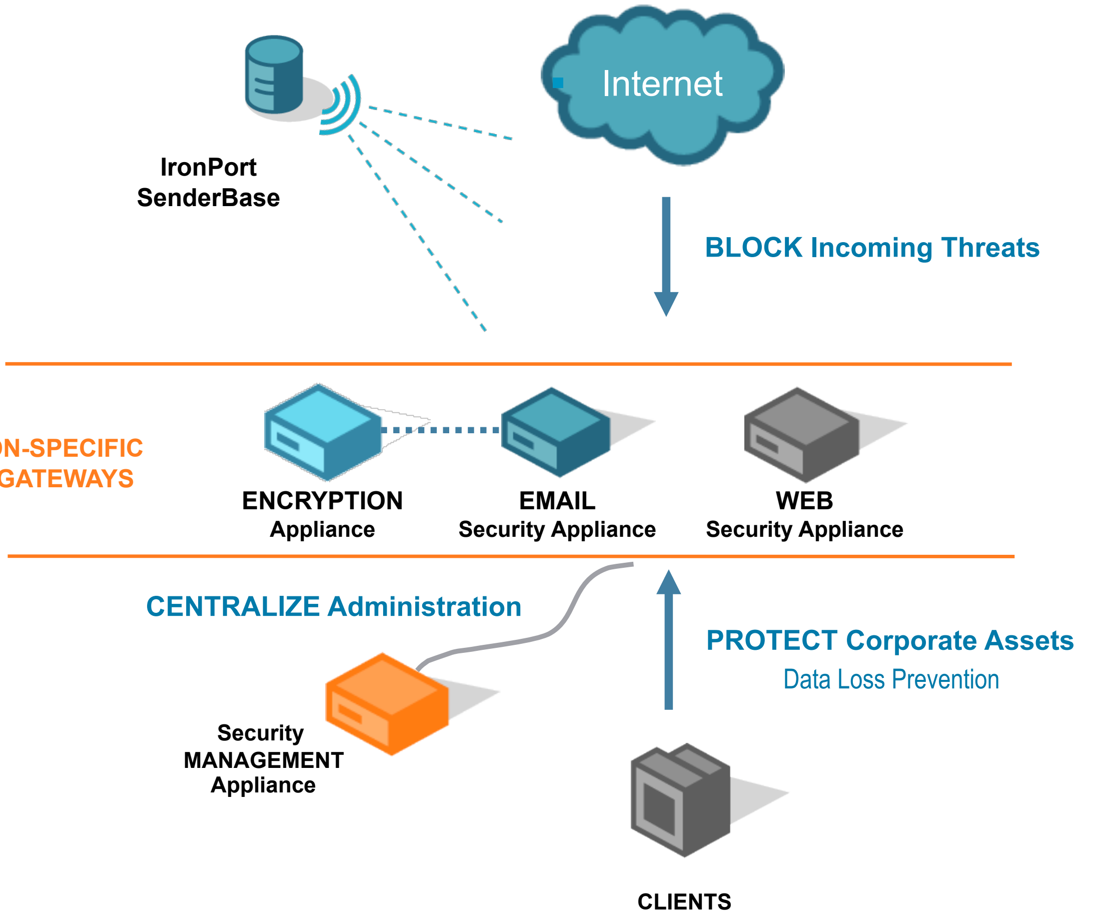
IronPort is now part of Cisco.

IronPort contacts

- Tomas Andberg
  - Territory Manager – Finland & Baltic Countries
  - tandberg@ironport.com
- Jari Salmi
  - Systems Engineer – Finland & Baltic Countries
  - jasalmi@ironport.com

IronPort® Gateway Security Products

APPLICATION-SPECIFIC SECURITY GATEWAYS



IronPort SenderBase

Internet

BLOCK Incoming Threats

ENCRYPTION Appliance

EMAIL Security Appliance

WEB Security Appliance

CENTRALIZE Administration

PROTECT Corporate Assets

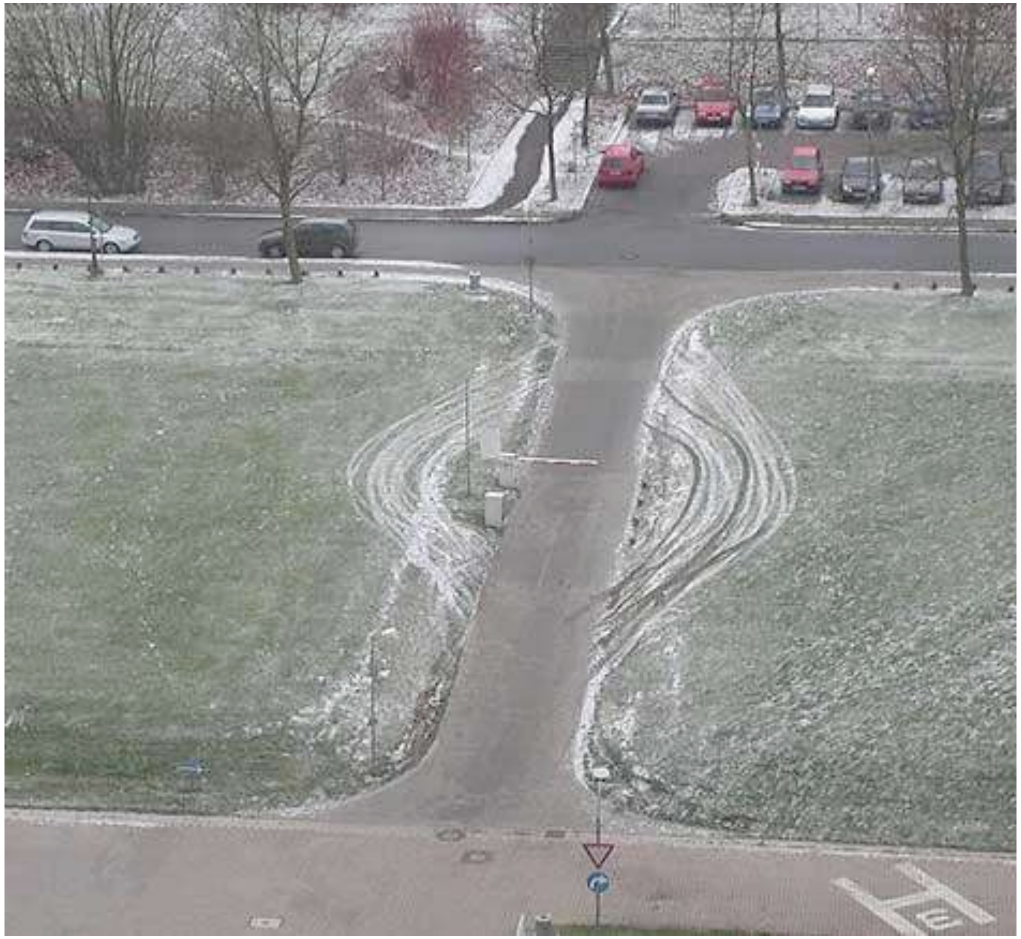
Data Loss Prevention

Security MANAGEMENT Appliance

CLIENTS

Web Security | Email Security | Security Management | Encryption

Reactive Security



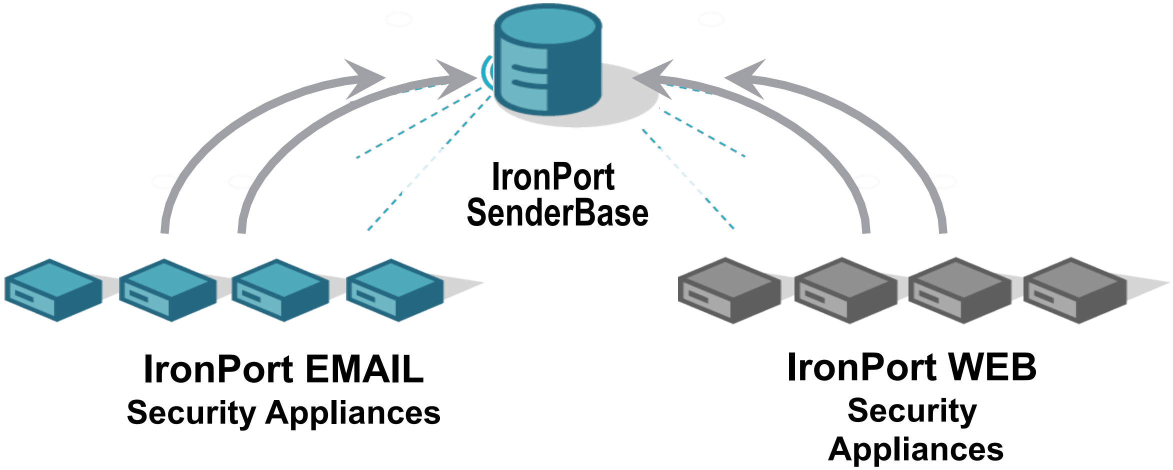
The IronPort SenderBase® Network

Global Reach Yields Benchmark Accuracy

- **30B+** queries daily
- **150+** Email and Web parameters
- **25%** of the World's Traffic
- Cisco Network Devices

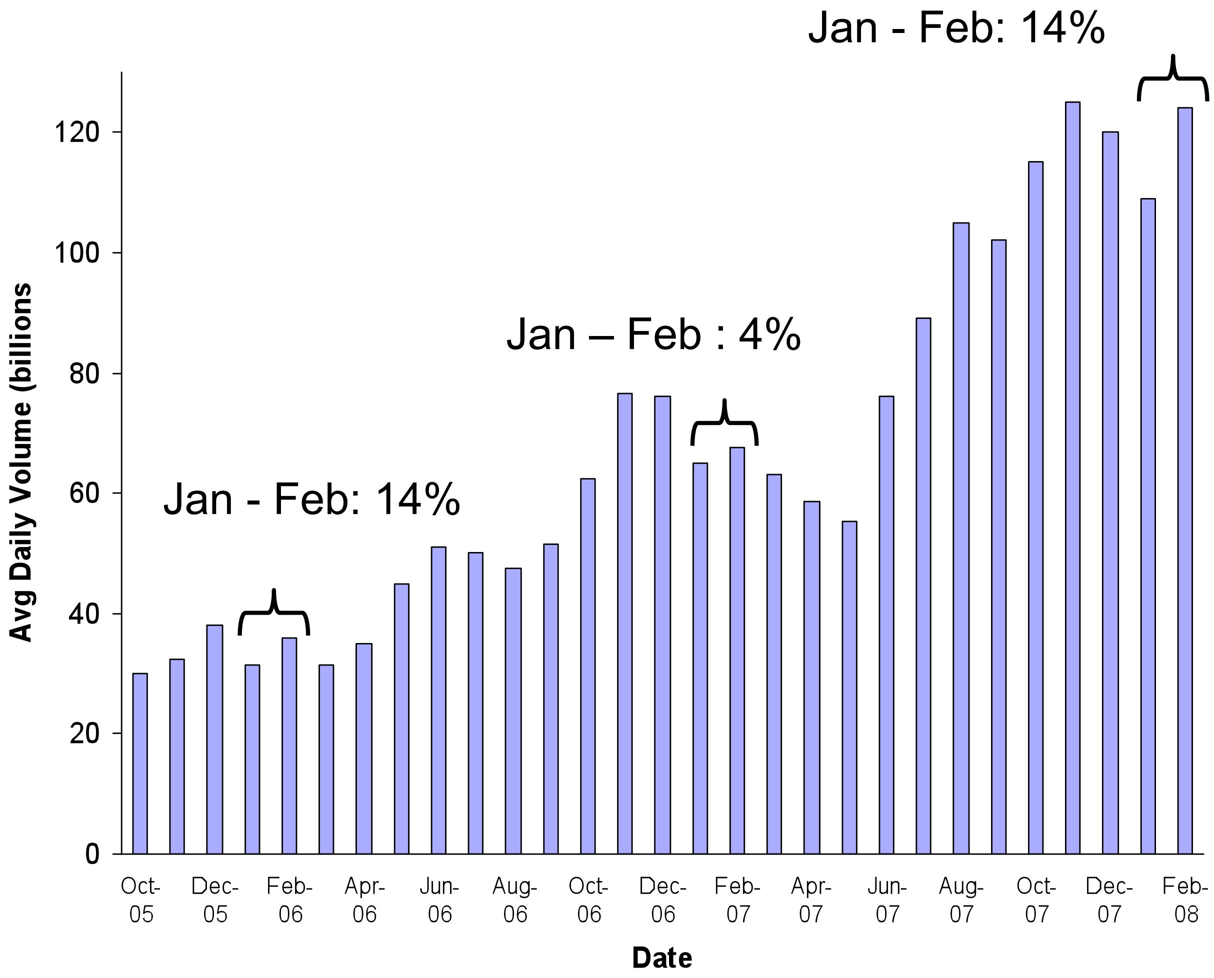
- View into **both** email & Web traffic dramatically improves detection
- 80% of spam contains URLs
- Email is a key distribution vector for Web-based malware
- Malware is a key distribution vector for Spam zombie infections

Combines Email & Web Traffic Analysis



Spam Volumes

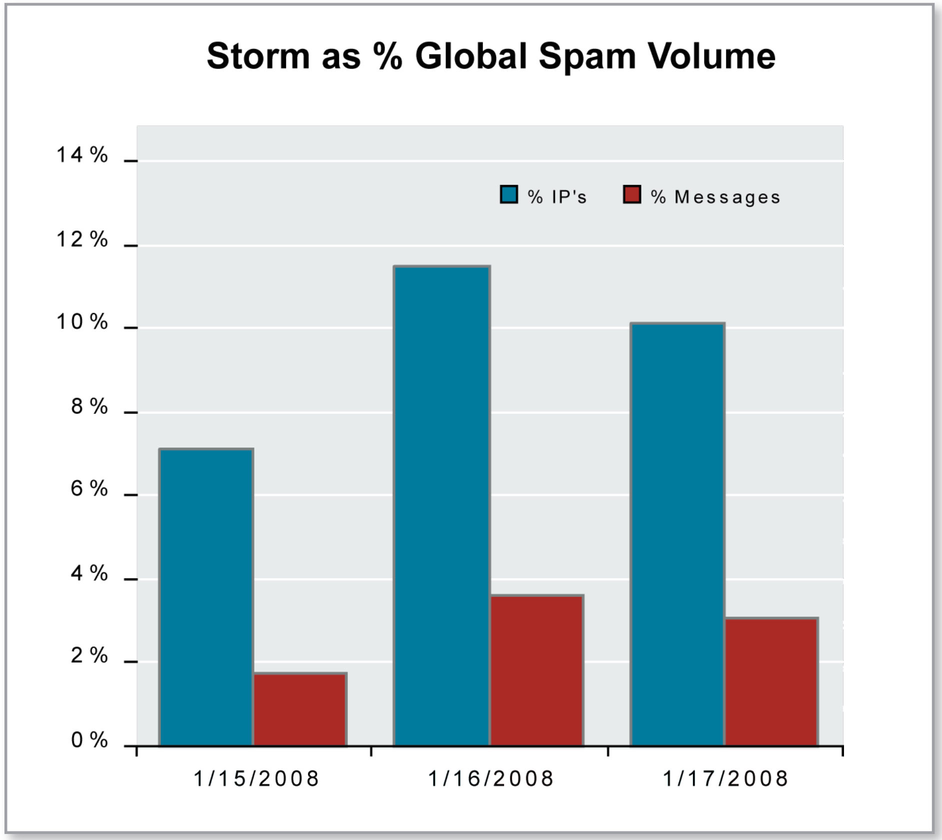
Through March 2008



- Volumes up, consistent w/ historic trends

Storm Spam Volumes

- Storm IPs were 9.6% of all corpus spam sources (ML 23%)
- Storm spam was 2.8% of all corpus spam
- Extrapolating to Internet:
  - Storm sent 3.1 billion msgs per day
  - Storm sent from 183,000 IP addresses per day
  - 16,940 Daily msgs per IP
- ML quoted in March 08 report 20% of all spam from Storm

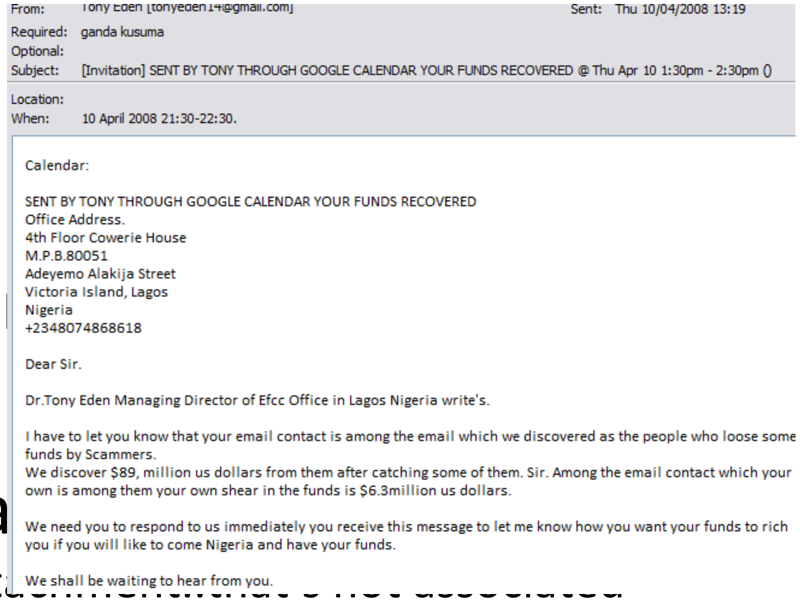

Storm as % Global Spam Volume

Storm Volumes are down 80% from their July, 2007 Peak

Interesting spam trends

- Google still >3% of all spam see

- Calendar/invite spam from gma
  - May not be scanned in same way as it's an attachment that's not associated with spam typically



From: Tony Eden [tonyeden14@gmail.com] Sent: Thu 10/04/2008 13:19
Required: ganda kusuma
Optional:
Subject: [Invitation] SENT BY TONY THROUGH GOOGLE CALENDAR YOUR FUNDS RECOVERED @ Thu Apr 10 1:30pm - 2:30pm ()

Location:
When: 10 April 2008 21:30-22:30.

Calendar:

SENT BY TONY THROUGH GOOGLE CALENDAR YOUR FUNDS RECOVERED
Office Address.
4th Floor Cowerie House
M.P.B.80051
Adeyemo Alakija Street
Victoria Island, Lagos
Nigeria
+2348074868618

Dear Sir.

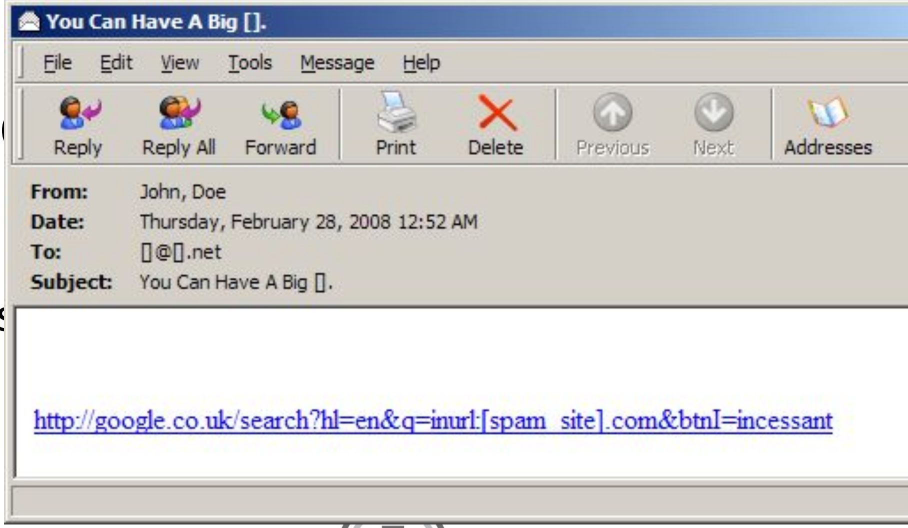
Dr.Tony Eden Managing Director of Efcc Office in Lagos Nigeria write's.

I have to let you know that your email contact is among the email which we discovered as the people who loose some funds by Scammers.
We discover $89, million us dollars from them after catching some of them. Sir. Among the email contact which your own is among them your own shear in the funds is $6.3million us dollars.

We need you to respond to us immediately you receive this message to let me know how you want your funds to rich you if you will like to come Nigeria and have your funds.

We shall be waiting to hear from you.

- Spam URL's back using Google r
  - SURBLS will fail as a result
  - http://www.google.com/search?q=3Dsite%3As e%2Ecom&btn

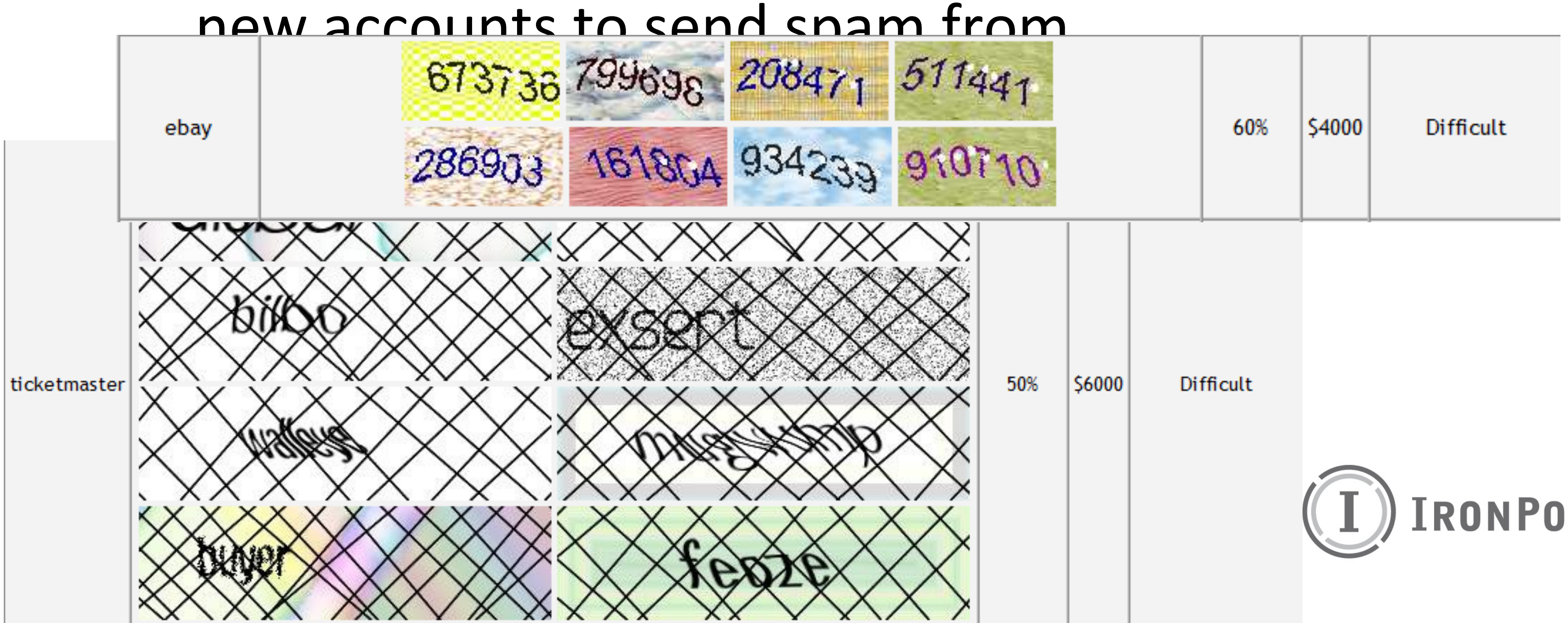


From: John, Doe
Date: Thursday, February 28, 2008 12:52 AM
To: []@[].net
Subject: You Can Have A Big [].

http://google.co.uk/search?hl=en&q=inurl:[spam site].com&btnI=incessant

CAPTCHAS

- **C**ompletely **A**utomated **P**ublic Turing test to tell **C**omputers and **H**umans **A**part
- Hotmail/Gmail/Yahoo CAPTCHAS have been broken / compromised driving spammers to sign up new accounts to send spam from

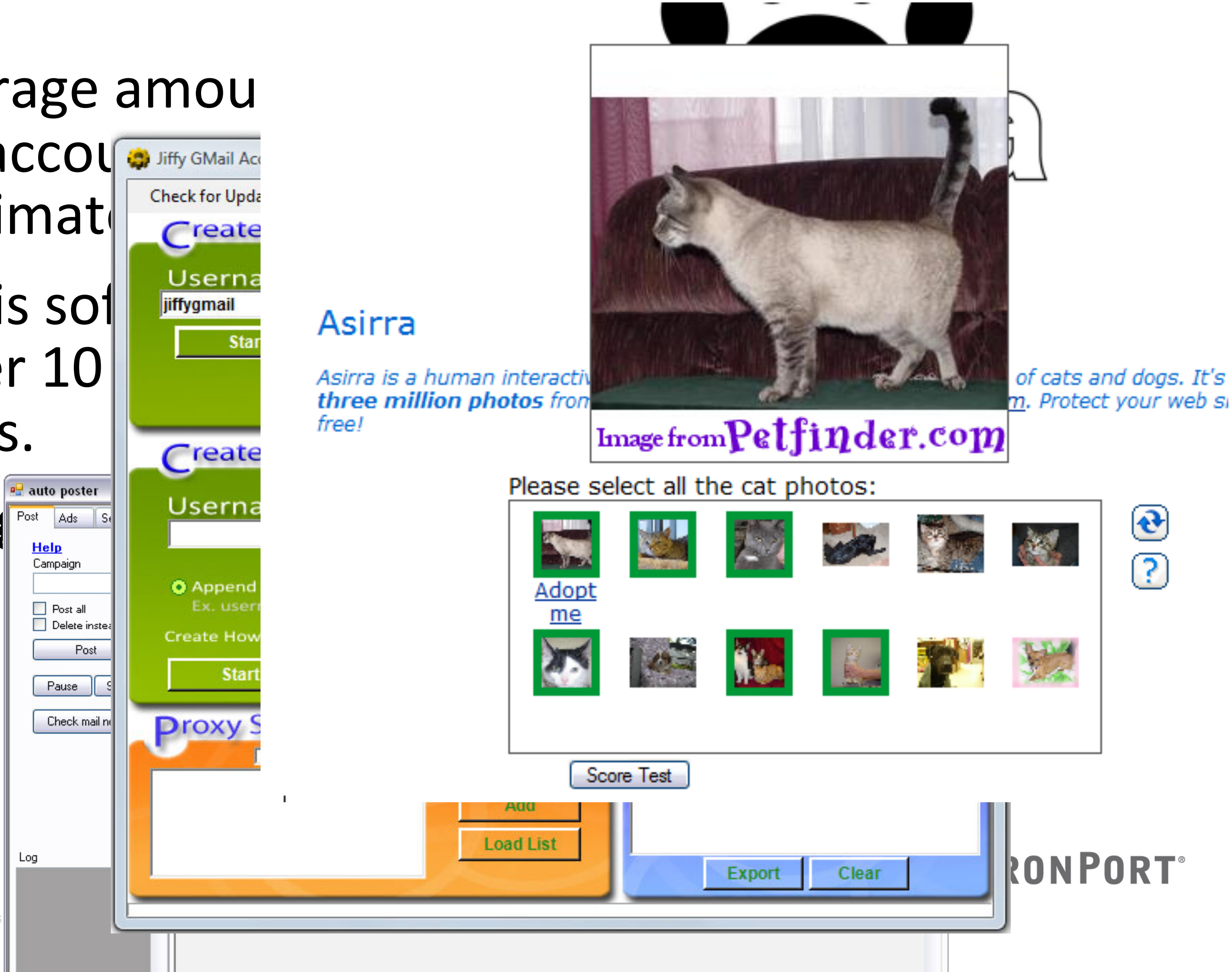


ebay		60%	$4000	Difficult

ticketmaster		50%	$6000	Difficult

Off the shelf software for spammers

- the average amou GMail accou approximat
- With this sof in under 10 minutes.
- The prog one.



Asirra

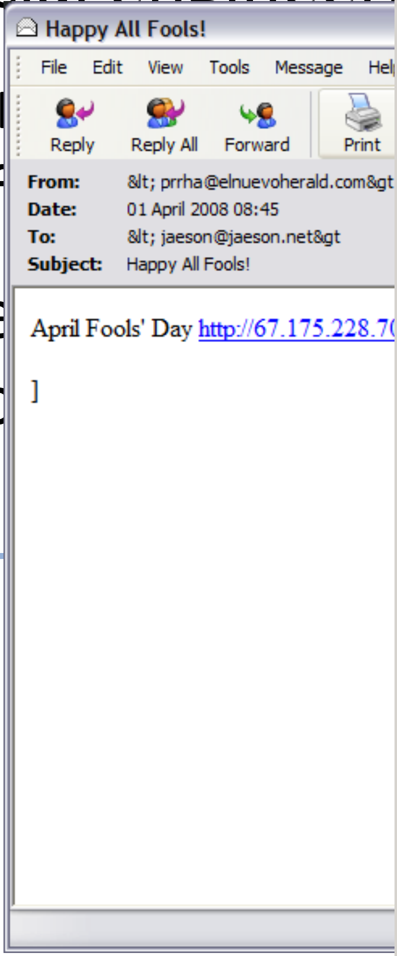
Asirra is a human interactiv of cats and dogs. It's three million photos fro m. Protect your web si free!

Image from Petfinder.com

Please select all the cat photos:

Storm update

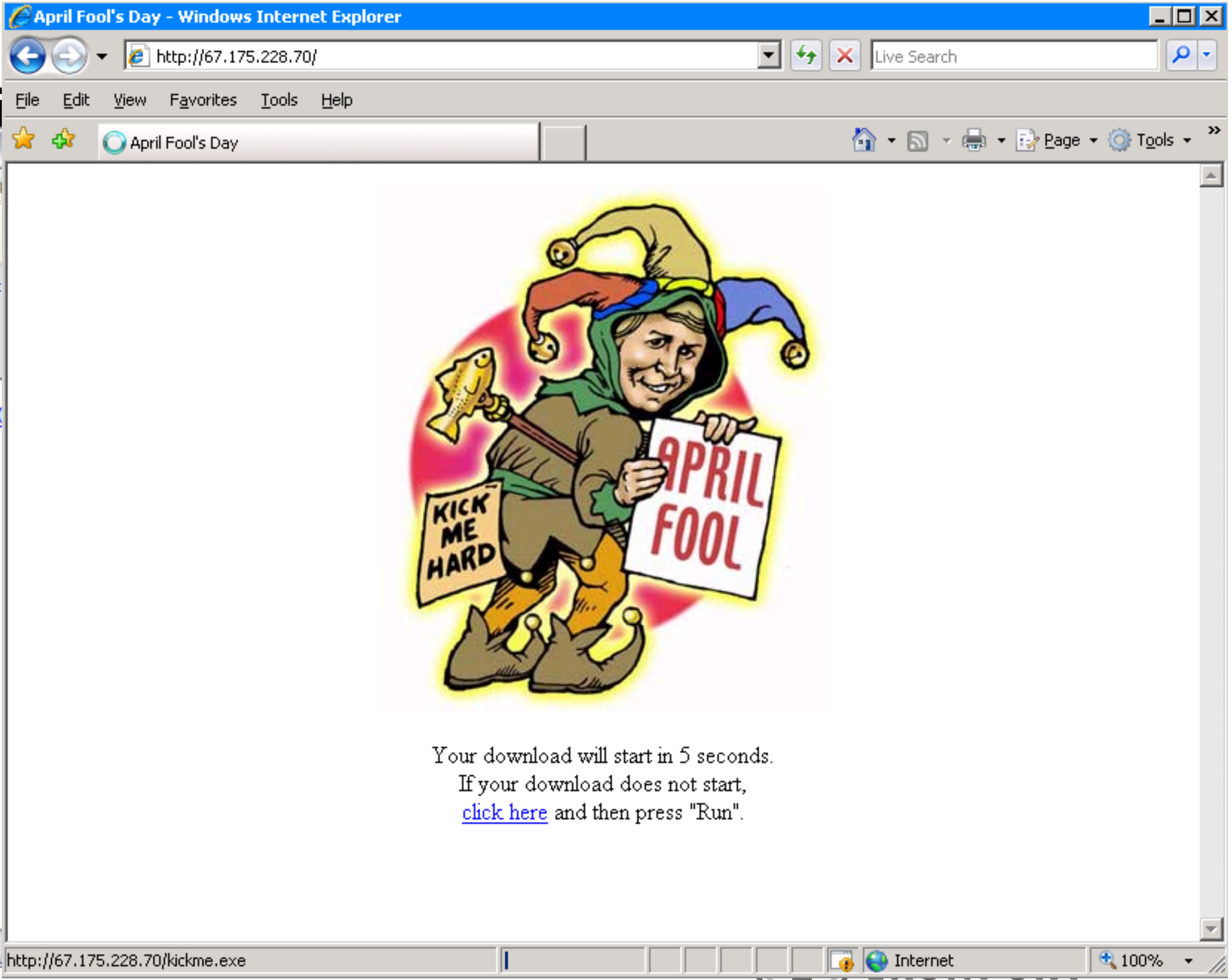
- Social engineeri
- Apr
  inf
- We
  fro
- htt



From: &lt; prrha@elnuevoherald.com&gt
Date: 01 April 2008 08:45
To: &lt; jaeson@jaeson.net&gt
Subject: Happy All Fools!

April Fools' Day http://67.175.228.7(

]



Your download will start in 5 seconds.
If your download does not start,
click here and then press "Run".

http://67.175.228.70/kickme.exe

Phishing trends

- Refresh – what is a Phish?
- $3.2 bn lost to phishing in 2007
  - Financial sector continues to be most targetted (92%)
  - Govt (5% - think tax dept scams etc..)
  - Retails & ISP's (1.5% each)

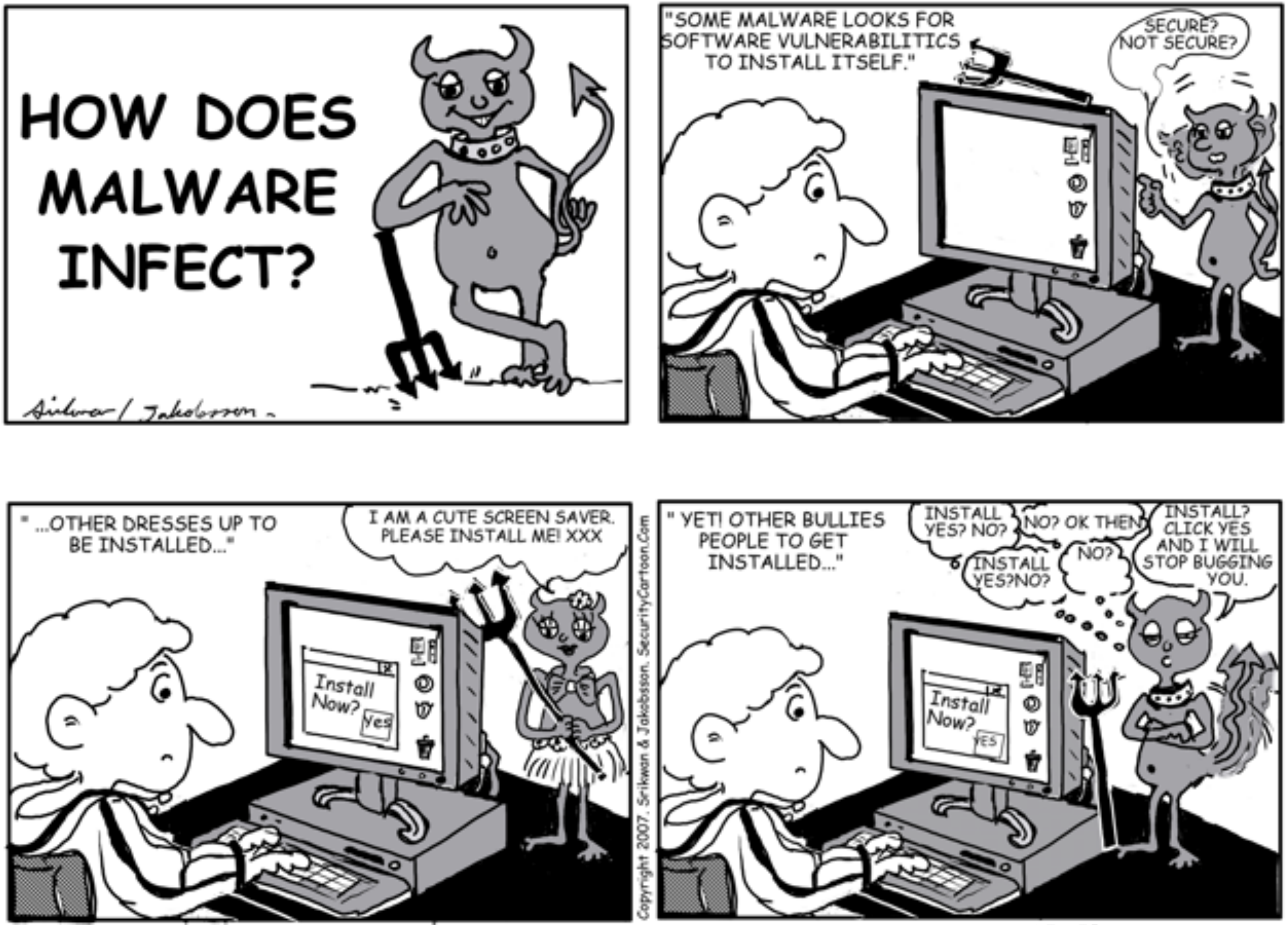
- 18 % of all verified phishing Web sites were hosted on just three IP addresses!!
- Paypal now blocking requests from weaker browsers (user-agent tag)
- Web sites ending in ".cn" - the Top Level Domain (TLD) assigned to China - account for 4 of the top 5 Web sites with the most valid phishes
- One unique phishing scam is launched every two minutes
- USA still hosts >66% of systems hosting phish sites

- Cost to buy a kit $1000 – writers scam the people whom host the site as well..

Portable Storage

- USB, Music, Video & DVD players targets
- Plug into PC at home & work….trusted
- ‘Expansion of network endpoint’
- 43% businesses have no security to address removable media
- Recent attacks
  - Digital Picture frames (San Fran Dec 2007)
  - Tom Toms (UK March 2007)
  - Media Players (infected & made in China)

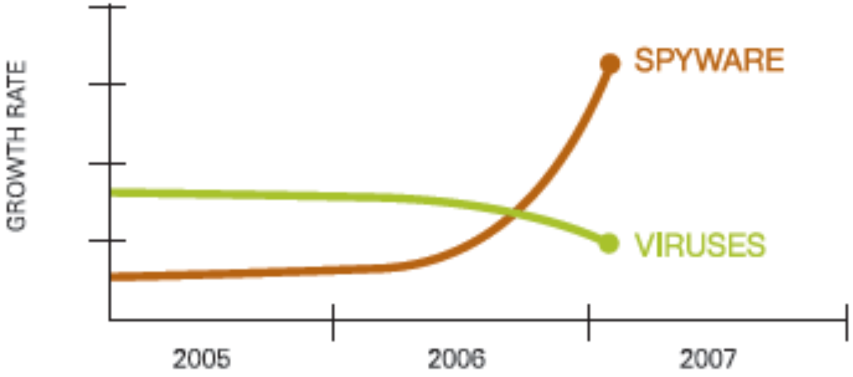
- Targetting manufacturing facilities

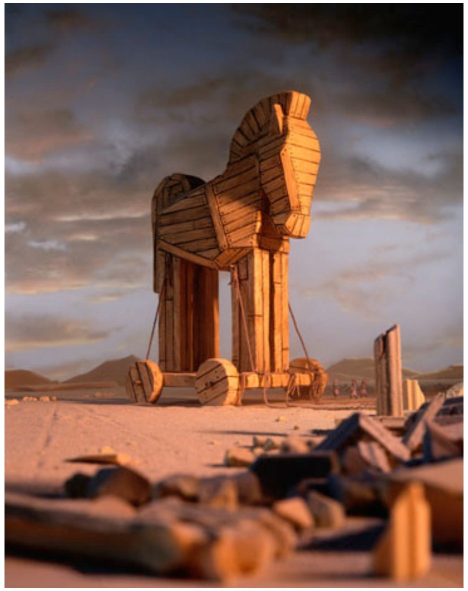

HOW DOES MALWARE INFECT?
Sirkwan / Jakobsson
"SOME MALWARE LOOKS FOR SOFTWARE VULNERABILITICS TO INSTALL ITSELF."
SECURE? NOT SECURE?
" ...OTHER DRESSES UP TO BE INSTALLED..."
I AM A CUTE SCREEN SAVER. PLEASE INSTALL ME! XXX
Install Now?
Yes
Copyright 2007. Srikwan & Jakobsson. SecurityCartoon.Com
" YET! OTHER BULLIES PEOPLE TO GET INSTALLED..."
INSTALL YES? NO?
NO? OK THEN
INSTALL YES?NO?
NO?
INSTALL? CLICK YES AND I WILL STOP BUGGING YOU.
Install Now?
YES

Spyware..

Malware is spreading

- AVtest: 5m different pieces of spyware in 2007
- Keyloggers : x20 in 5 years,
- High growth for rootkits (tools designed to hide other more malicious codes)

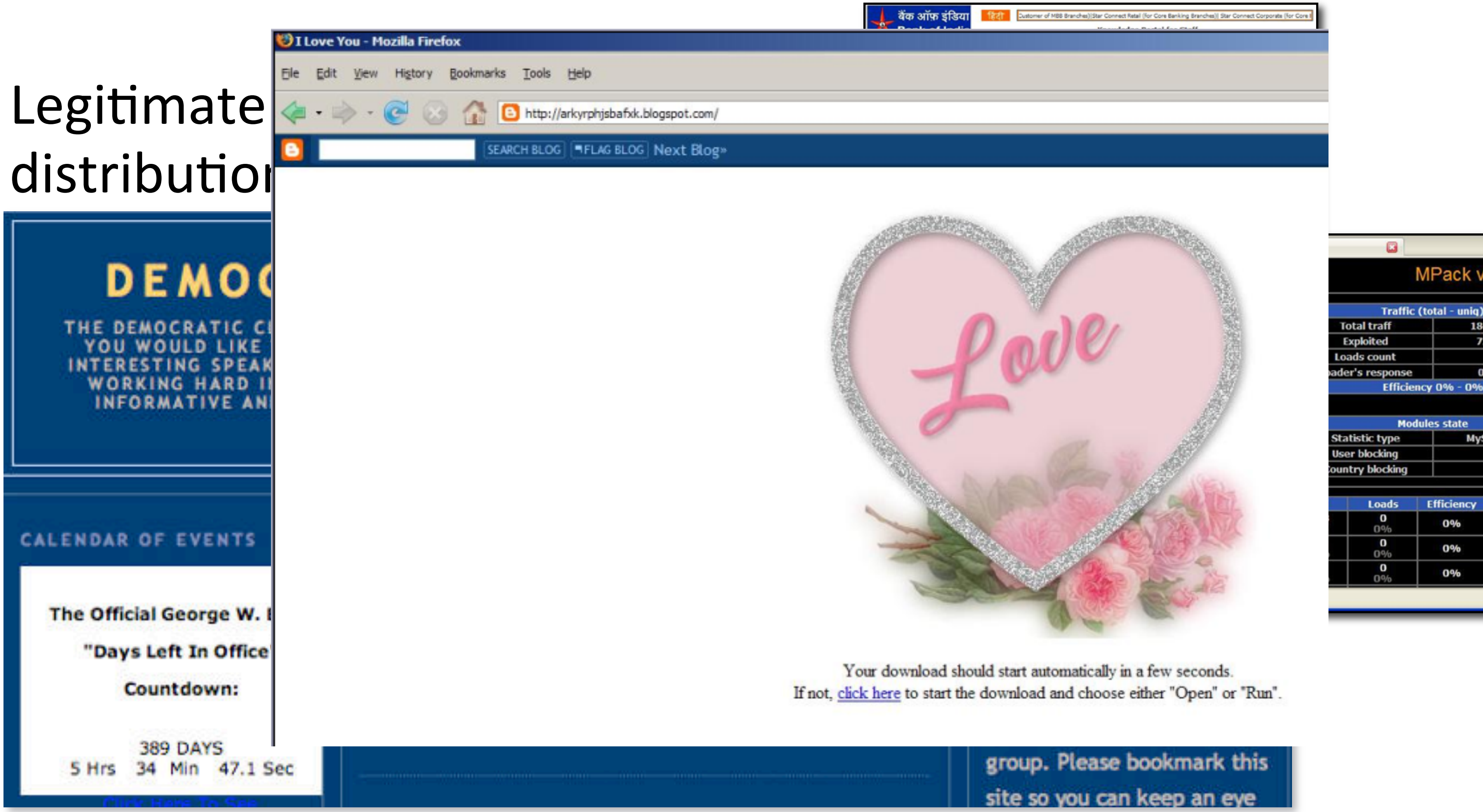




Legitimate Websites Getting Hacked

- Legitimate
distributio

-



बैंक ऑफ इंडिया

हिंदी

I Love You - Mozilla Firefox

http://arkyrphjsbafxk.blogspot.com/

Your download should start automatically in a few seconds.
If not, click here to start the download and choose either "Open" or "Run".

DEMOC

THE DEMOCRATIC CL
YOU WOULD LIKE
INTERESTING SPEAK
WORKING HARD I
INFORMATIVE AN

CALENDAR OF EVENTS

The Official George W.

"Days Left In Office

Countdown:

389 DAYS
5 Hrs 34 Min 47.1 Sec

group. Please bookmark this
site so you can keep an eye

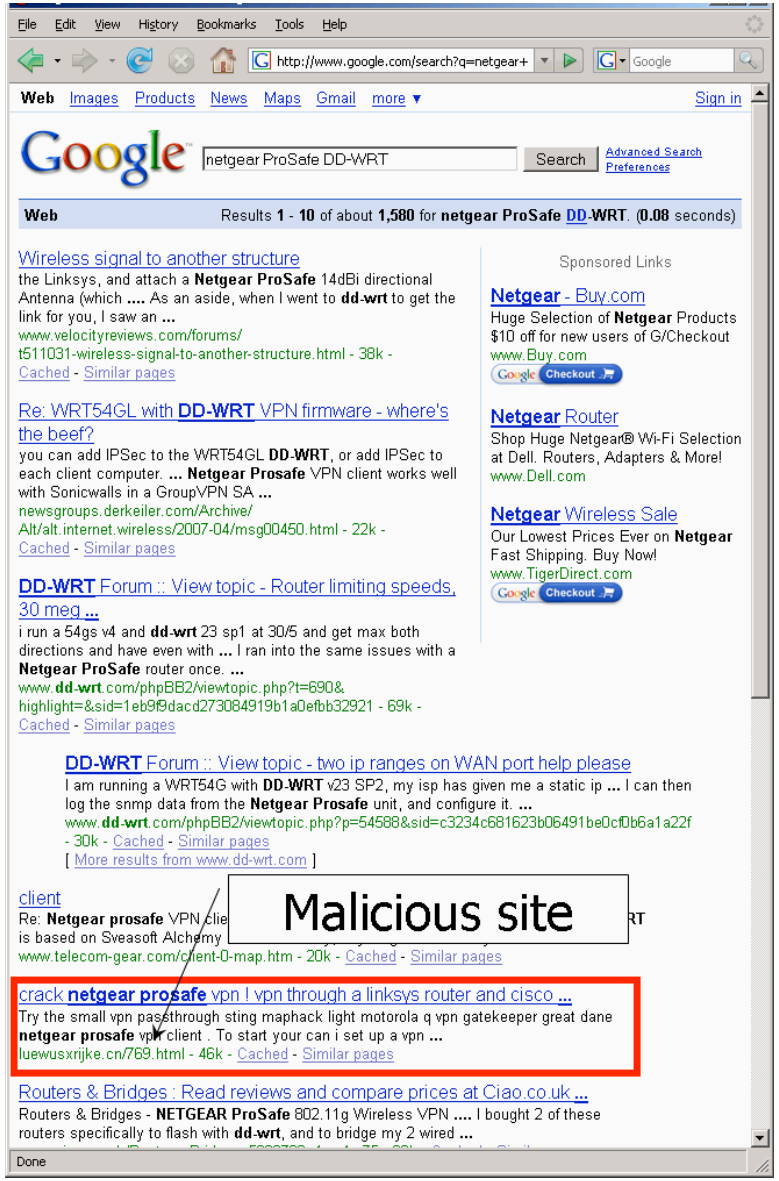
MPack v

Traffic (total - uniq)	
Total traff	18
Exploited	7
Loads count	
ader's response	0
Efficiency 0% - 0%	

Modules state	
Statistic type	My
User blocking	
ountry blocking	

Loads	Efficiency
0 0%	0%
0 0%	0%
0 0%	0%

Threat Spotlight – Search Engine Vector


File Edit View History Bookmarks Tools Help
http://www.google.com/search?q=netgear+
Google
Web Images Products News Maps Gmail more ▾
Sign in
Search
Advanced Search
Preferences
Done

netgear ProSafe DD-WRT

Web Results **1** - **10** of about **1,580** for **netgear ProSafe DD-WRT**. (**0.08** seconds)

Wireless signal to another structure
the Linksys, and attach a **Netgear ProSafe** 14dBi directional Antenna (which **....** As an aside, when I went to **dd-wrt** to get the link for you, I saw an **...**
www.velocityreviews.com/forums/t511031-wireless-signal-to-another-structure.html - 38k - Cached - Similar pages

Re: WRT54GL with **DD-WRT** VPN firmware - where's the beef?
you can add IPSec to the WRT54GL **DD-WRT**, or add IPSec to each client computer. **... Netgear Prosafe** VPN client works well with Sonicwalls in a GroupVPN SA **...**
newsgroups.derkeiler.com/Archive/Alt/alt.internet.wireless/2007-04/msg00450.html - 22k - Cached - Similar pages

DD-WRT Forum :: View topic - Router limiting speeds, 30 meg **...**
i run a 54gs v4 and **dd-wrt** 23 sp1 at 30/5 and get max both directions and have even with **...** I ran into the same issues with a **Netgear ProSafe** router once. **...**
www.**dd-wrt**.com/phpBB2/viewtopic.php?t=690&highlight=&sid=1eb9f9dacd273084919b1a0efbb32921 - 69k - Cached - Similar pages

DD-WRT Forum :: View topic - two ip ranges on WAN port help please
I am running a WRT54G with **DD-WRT** v23 SP2, my isp has given me a static ip **...** I can then log the snmp data from the **Netgear Prosafe** unit, and configure it. **...**
www.**dd-wrt**.com/phpBB2/viewtopic.php?p=54588&sid=c3234c681623b06491be0cf0b6a1a22f - 30k - Cached - Similar pages
[More results from www.dd-wrt.com]

client
Re: **Netgear prosafe** VPN clie RT
is based on Sveasoft Alchemy
www.telecom-gear.com/client-0-map.htm - 20k - Cached - Similar pages

crack **netgear prosafe** vpn ! vpn through a linksys router and cisco **...**
Try the small vpn passthrough sting maphack light motorola q vpn gatekeeper great dane **netgear prosafe** vpn client . To start your can i set up a vpn **...**
luewusxrijke.cn/769.html - 46k - Cached - Similar pages

Routers & Bridges : Read reviews and compare prices at Ciao.co.uk **...**
Routers & Bridges - **NETGEAR ProSafe** 802.11g Wireless VPN **....** I bought 2 of these routers specifically to flash with **dd-wrt**, and to bridge my 2 wired **...**

Sponsored Links

Netgear - Buy.com
Huge Selection of **Netgear** Products
$10 off for new users of G/Checkout
www.Buy.com
Google Checkout

Netgear Router
Shop Huge Netgear® Wi-Fi Selection at Dell. Routers, Adapters & More!
www.Dell.com

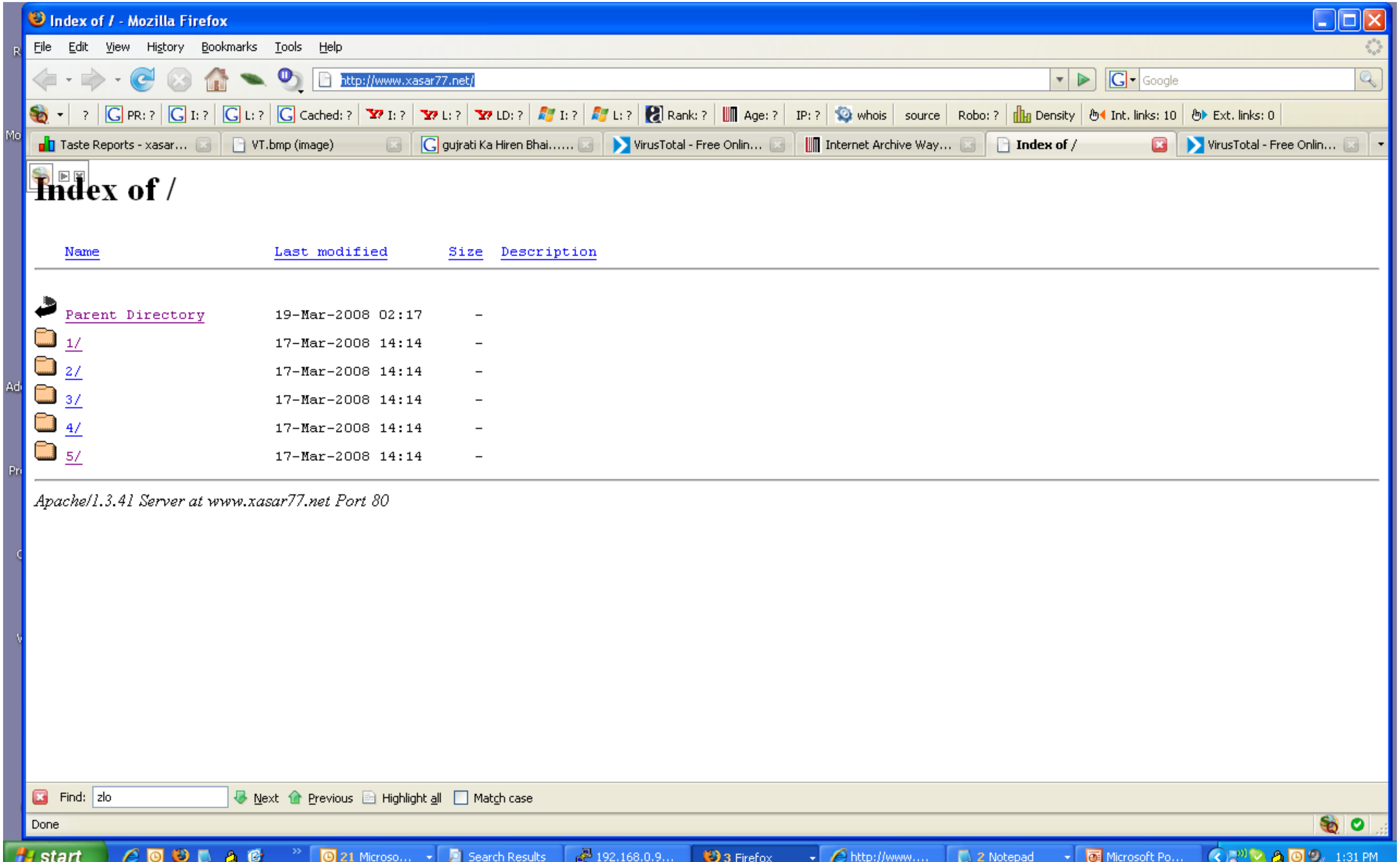
Netgear Wireless Sale
Our Lowest Prices Ever on **Netgear**
Fast Shipping. Buy Now!
www.TigerDirect.com
Google Checkout

Malicious site

- Google estimate 1.4% all searches 'dirty'
- Malicious sites boosted by "comment spam" & "blog spam"
- Users commonly select site due to high placement in search results
- Redirected to pages serving malware
  - Fake codec installation dialog or IFrame attack

One malware site – lets look

Xasar77.net registered on the 17th March by estdomains, hosted 10,000 malurls



Index of / - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.xasar77.net/
Google
PR: ? I: ? L: ? Cached: ? I: ? L: ? LD: ? I: ? L: ? Rank: ? Age: ? IP: ? whois source Robo: ? Density Int. links: 10 Ext. links: 0
Taste Reports - xasar... VT.bmp (image) gujrati Ka Hiren Bhai...... VirusTotal - Free Onlin... Internet Archive Way... Index of / VirusTotal - Free Onlin...
Find: zlo Next Previous Highlight all Match case
Done
start 21 Microso... Search Results 192.168.0.9... 3 Firefox http://www.... 2 Notepad Microsoft Po... 1:31 PM

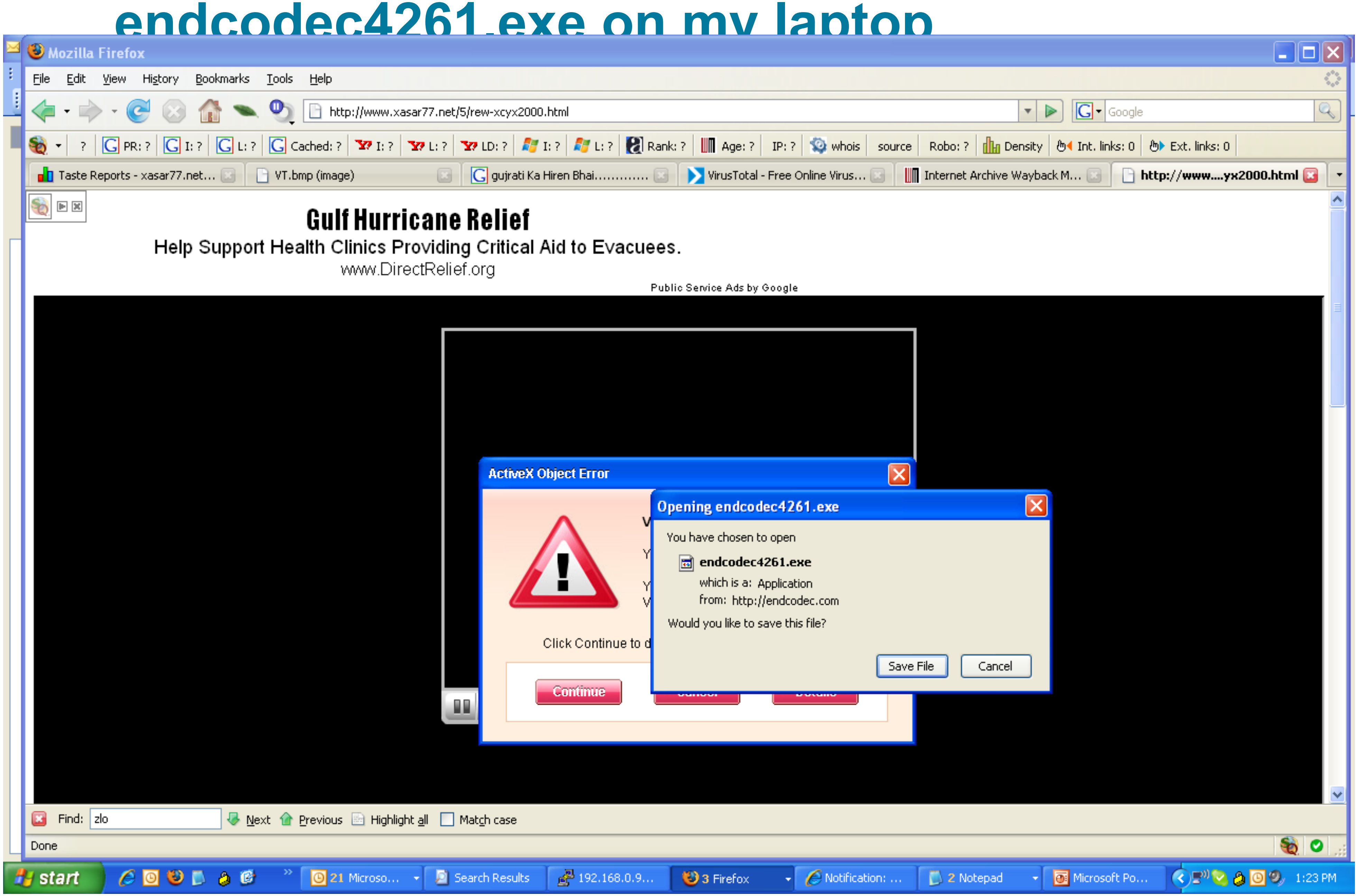
Index of /

```
Name                    Last modified       Size  Description

Parent Directory        19-Mar-2008 02:17     -
1/                      17-Mar-2008 14:14     -
2/                      17-Mar-2008 14:14     -
3/                      17-Mar-2008 14:14     -
4/                      17-Mar-2008 14:14     -
5/                      17-Mar-2008 14:14     -
```

Apache/1.3.41 Server at www.xasar77.net Port 80

The urls wants to install a codec endcodec4261.exe on my laptop



Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.xasar77.net/5/rew-xcyx2000.html
Google
PR: ? I: ? L: ? Cached: ? I: ? L: ? LD: ? I: ? L: ? Rank: ? Age: ? IP: ? whois source Robo: ? Density Int. links: 0 Ext. links: 0
Taste Reports - xasar77.net...
VT.bmp (image)
gujrati Ka Hiren Bhai............
VirusTotal - Free Online Virus...
Internet Archive Wayback M...
http://www....yx2000.html
Find: zlo
Next
Previous
Highlight all
Match case
Done
start
21 Microso...
Search Results
192.168.0.9...
3 Firefox
Notification: ...
2 Notepad
Microsoft Po...
1:23 PM

Gulf Hurricane Relief

Help Support Health Clinics Providing Critical Aid to Evacuees.

www.DirectRelief.org

Public Service Ads by Google

ActiveX Object Error

Click Continue to d

Opening endcodec4261.exe

You have chosen to open

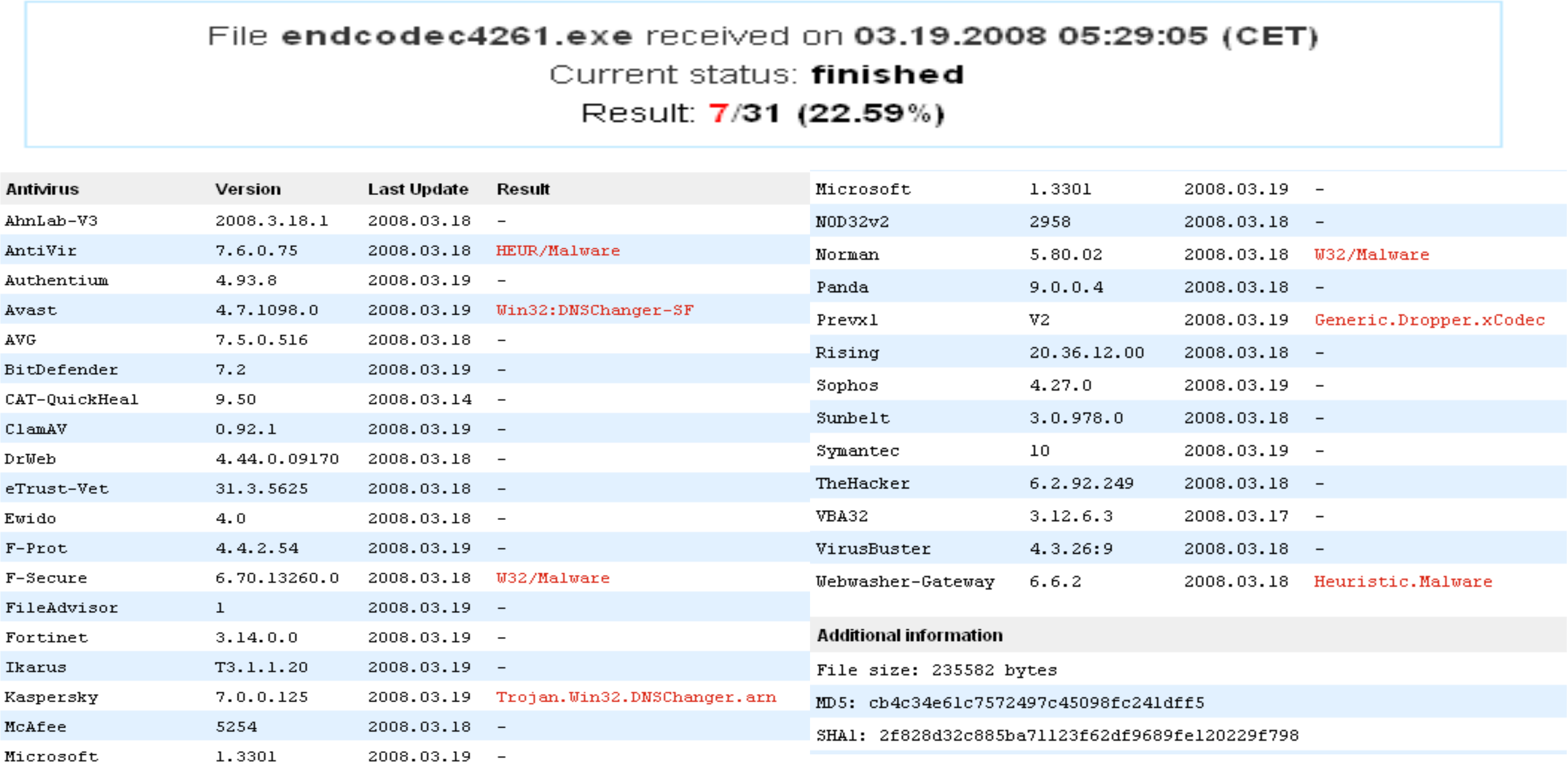
endcodec4261.exe

which is a: Application

from: http://endcodec.com

Would you like to save this file?

The result



File **endcodec4261.exe** received on **03.19.2008 05:29:05 (CET)**

Current status: **finished**

Result: **7/31 (22.59%)**

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.3.18.1	2008.03.18	-
AntiVir	7.6.0.75	2008.03.18	HEUR/Malware
Authentium	4.93.8	2008.03.19	-
Avast	4.7.1098.0	2008.03.19	Win32:DNSChanger-SF
AVG	7.5.0.516	2008.03.18	-
BitDefender	7.2	2008.03.19	-
CAT-QuickHeal	9.50	2008.03.14	-
ClamAV	0.92.1	2008.03.19	-
DrWeb	4.44.0.09170	2008.03.18	-
eTrust-Vet	31.3.5625	2008.03.18	-
Ewido	4.0	2008.03.18	-
F-Prot	4.4.2.54	2008.03.19	-
F-Secure	6.70.13260.0	2008.03.18	W32/Malware
FileAdvisor	1	2008.03.19	-
Fortinet	3.14.0.0	2008.03.19	-
Ikarus	T3.1.1.20	2008.03.19	-
Kaspersky	7.0.0.125	2008.03.19	Trojan.Win32.DNSChanger.arn
McAfee	5254	2008.03.18	-
Microsoft	1.3301	2008.03.19	-
Microsoft	1.3301	2008.03.19	-
NOD32v2	2958	2008.03.18	-
Norman	5.80.02	2008.03.18	W32/Malware
Panda	9.0.0.4	2008.03.18	-
Prevx1	V2	2008.03.19	Generic.Dropper.xCodec
Rising	20.36.12.00	2008.03.18	-
Sophos	4.27.0	2008.03.19	-
Sunbelt	3.0.978.0	2008.03.18	-
Symantec	10	2008.03.19	-
TheHacker	6.2.92.249	2008.03.18	-
VBA32	3.12.6.3	2008.03.17	-
VirusBuster	4.3.26:9	2008.03.18	-
Webwasher-Gateway	6.6.2	2008.03.18	Heuristic.Malware

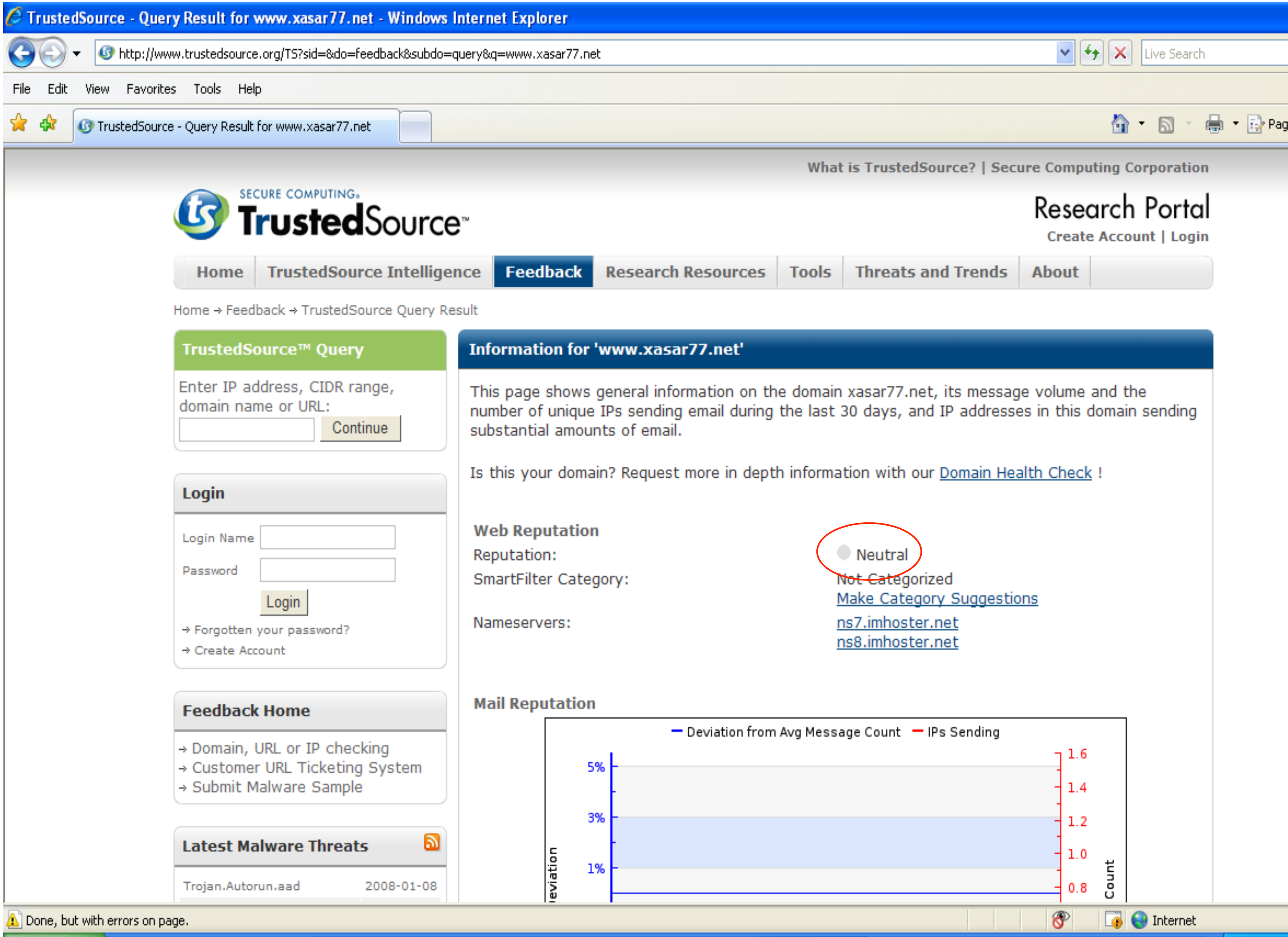
Additional information

File size: 235582 bytes

MD5: cb4c34e61c7572497c45098fc241dff5

SHA1: 2f828d32c885ba71123f62df9689fe120229f798

IRONPORT®



TrustedSource - Query Result for www.xasar77.net - Windows Internet Explorer
http://www.trustedsource.org/TS?sid=&do=feedback&subdo=query&q=www.xasar77.net
Live Search
File
Edit
View
Favorites
Tools
Help
TrustedSource - Query Result for www.xasar77.net
Pag

What is TrustedSource? | Secure Computing Corporation

SECURE COMPUTING. TrustedSource™

Research Portal

Create Account | Login

Home | TrustedSource Intelligence | Feedback | Research Resources | Tools | Threats and Trends | About

Home → Feedback → TrustedSource Query Result

TrustedSource™ Query

Enter IP address, CIDR range, domain name or URL:

Continue

Login

Login Name

Password

Login

→ Forgotten your password?

→ Create Account

Feedback Home

→ Domain, URL or IP checking
→ Customer URL Ticketing System
→ Submit Malware Sample

Latest Malware Threats

Trojan.Autorun.aad	2008-01-08

Information for 'www.xasar77.net'

This page shows general information on the domain xasar77.net, its message volume and the number of unique IPs sending email during the last 30 days, and IP addresses in this domain sending substantial amounts of email.

Is this your domain? Request more in depth information with our Domain Health Check !

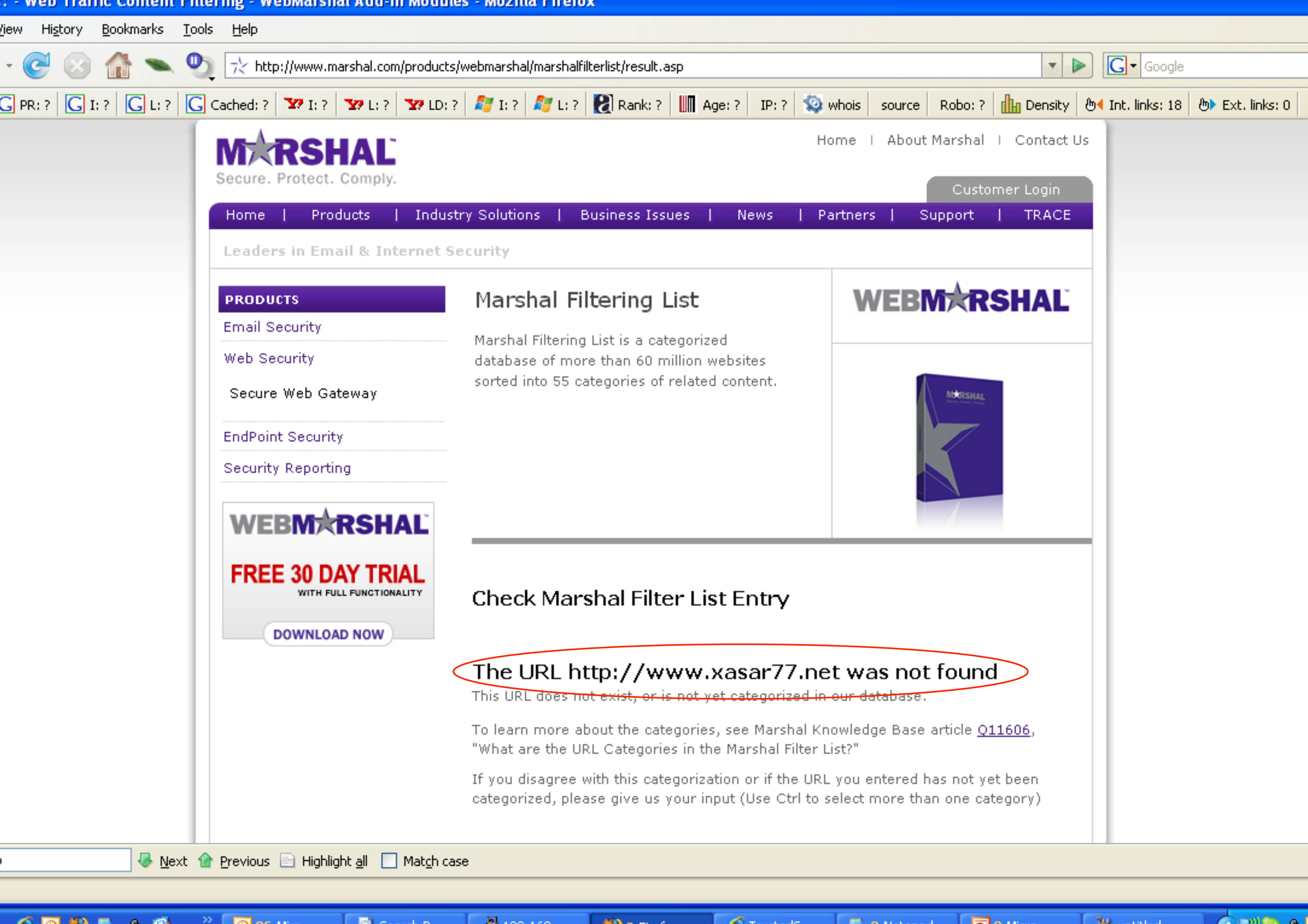
Web Reputation

Reputation:	○ Neutral
SmartFilter Category:	Not Categorized Make Category Suggestions
Nameservers:	ns7.imhoster.net ns8.imhoster.net

Mail Reputation

Done, but with errors on page.

Internet


: - Web Traffic Content Filtering - WebMarshal Add-in Modules - Mozilla Firefox
View History Bookmarks Tools Help
http://www.marshal.com/products/webmarshal/marshalfilterlist/result.asp
Google
PR: ? I: ? L: ? Cached: ? I: ? L: ? LD: ? I: ? L: ? Rank: ? Age: ? IP: ? whois source Robo: ? Density Int. links: 18 Ext. links: 0
MARSHAL
Secure. Protect. Comply.
Home | About Marshal | Contact Us
Customer Login
Home | Products | Industry Solutions | Business Issues | News | Partners | Support | TRACE
Leaders in Email & Internet Security
PRODUCTS
Email Security
Web Security
Secure Web Gateway
EndPoint Security
Security Reporting
WEBMARSHAL
FREE 30 DAY TRIAL
WITH FULL FUNCTIONALITY
DOWNLOAD NOW
WEBMARSHAL
Next Previous Highlight all Match case

Marshal Filtering List

Marshal Filtering List is a categorized database of more than 60 million websites sorted into 55 categories of related content.

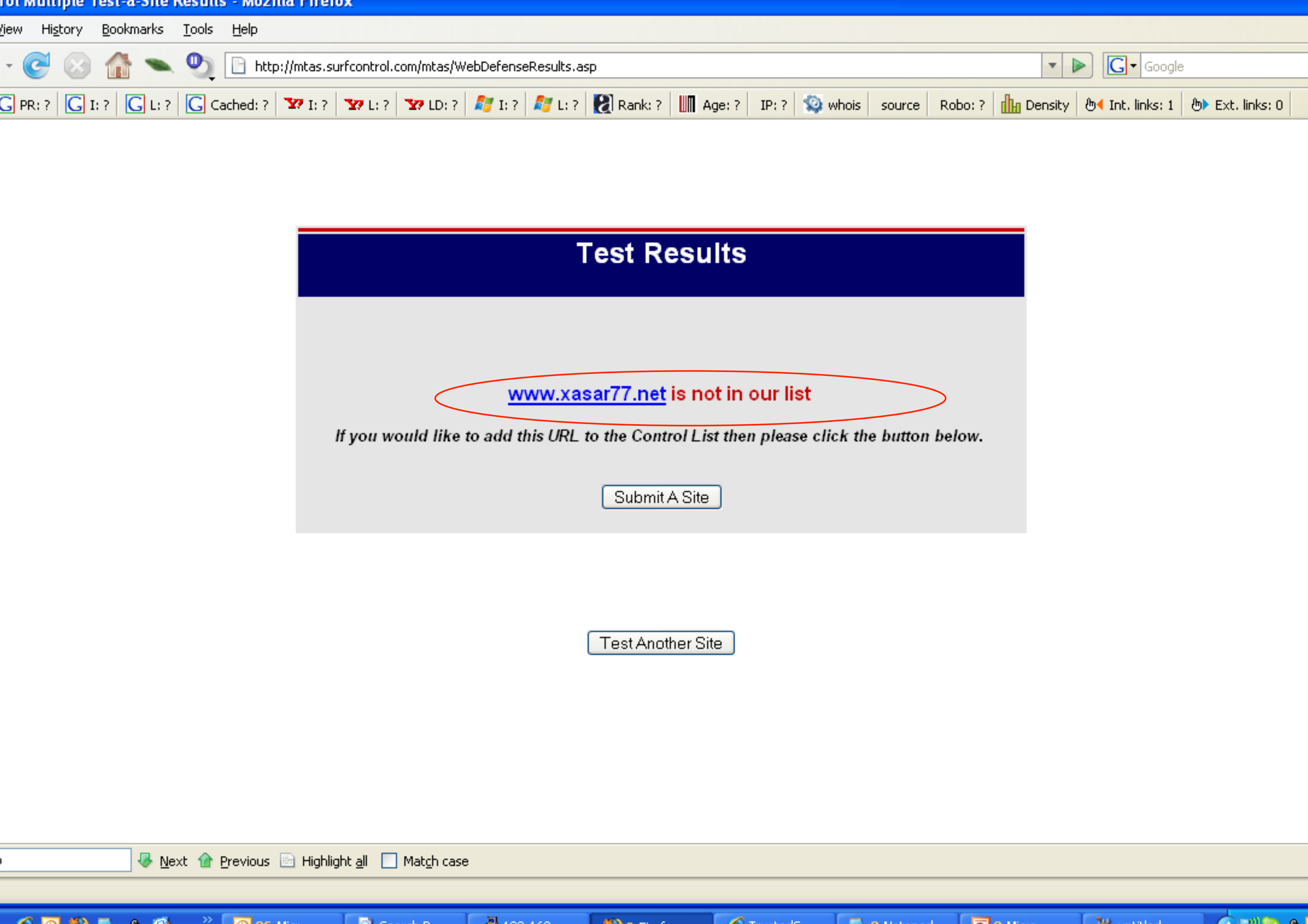
Check Marshal Filter List Entry

The URL http://www.xasar77.net was not found

This URL does not exist, or is not yet categorized in our database.

To learn more about the categories, see Marshal Knowledge Base article Q11606, "What are the URL Categories in the Marshal Filter List?"

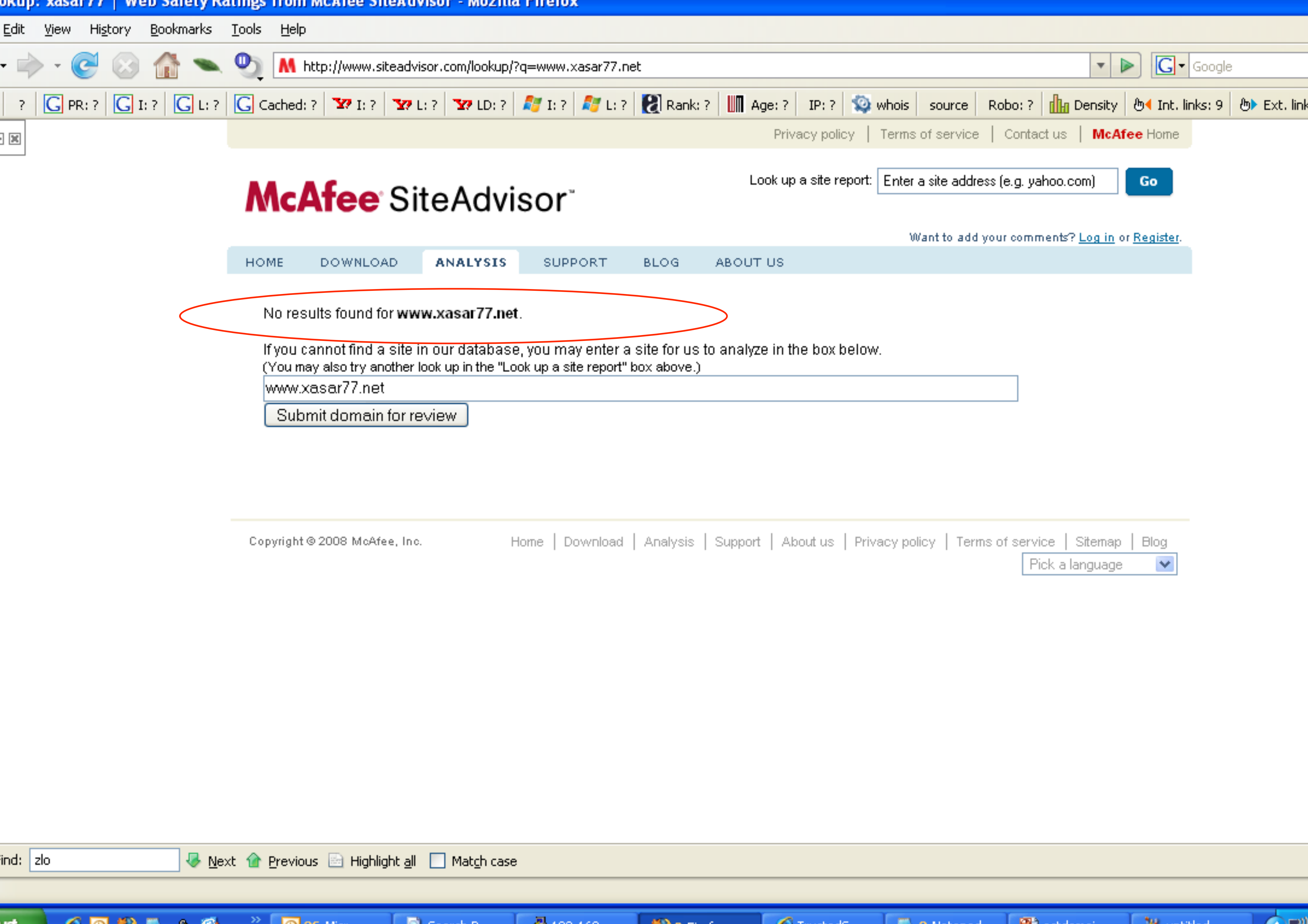
If you disagree with this categorization or if the URL you entered has not yet been categorized, please give us your input (Use Ctrl to select more than one category)



Test Results

www.xasar77.net is not in our list

If you would like to add this URL to the Control List then please click the button below.


okup: xasar77 | Web Safety Ratings from McAfee SiteAdvisor - Mozilla Firefox
Edit
View
History
Bookmarks
Tools
Help
Google
? PR: ? I: ? L: ? Cached: ? I: ? L: ? LD: ? I: ? L: ? Rank: ? Age: ? IP: ? whois source Robo: ? Density Int. links: 9 Ext. link
Privacy policy | Terms of service | Contact us | McAfee Home
McAfee SiteAdvisor
Look up a site report:
Enter a site address (e.g. yahoo.com)
Go
Want to add your comments? Log in or Register.
HOME
DOWNLOAD
ANALYSIS
SUPPORT
BLOG
ABOUT US
Home | Download | Analysis | Support | About us | Privacy policy | Terms of service | Sitemap | Blog
Pick a language
Find:
Next
Previous
Highlight all
Match case

http://www.siteadvisor.com/lookup/?q=www.xasar77.net

No results found for **www.xasar77.net**.

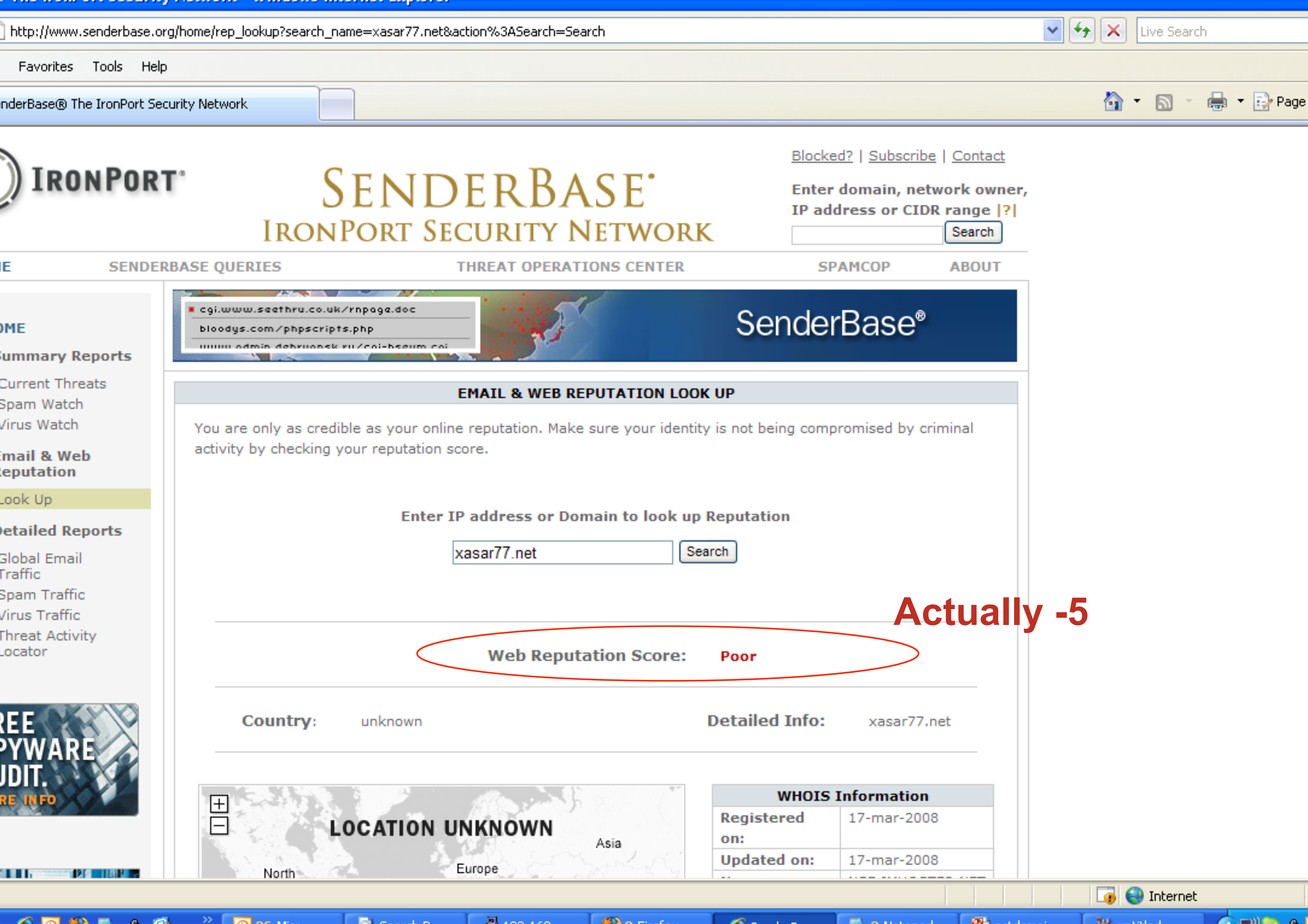
If you cannot find a site in our database, you may enter a site for us to analyze in the box below.
(You may also try another look up in the "Look up a site report" box above.)

www.xasar77.net

Submit domain for review

Copyright © 2008 McAfee, Inc.

Find: zlo



EMAIL & WEB REPUTATION LOOK UP

You are only as credible as your online reputation. Make sure your identity is not being compromised by criminal activity by checking your reputation score.

Enter IP address or Domain to look up Reputation

xasar77.net Search

Actually -5

Web Reputation Score: Poor

Country: unknown

Detailed Info: xasar77.net

WHOIS Information	
Registered on:	17-mar-2008
Updated on:	17-mar-2008

Future threats

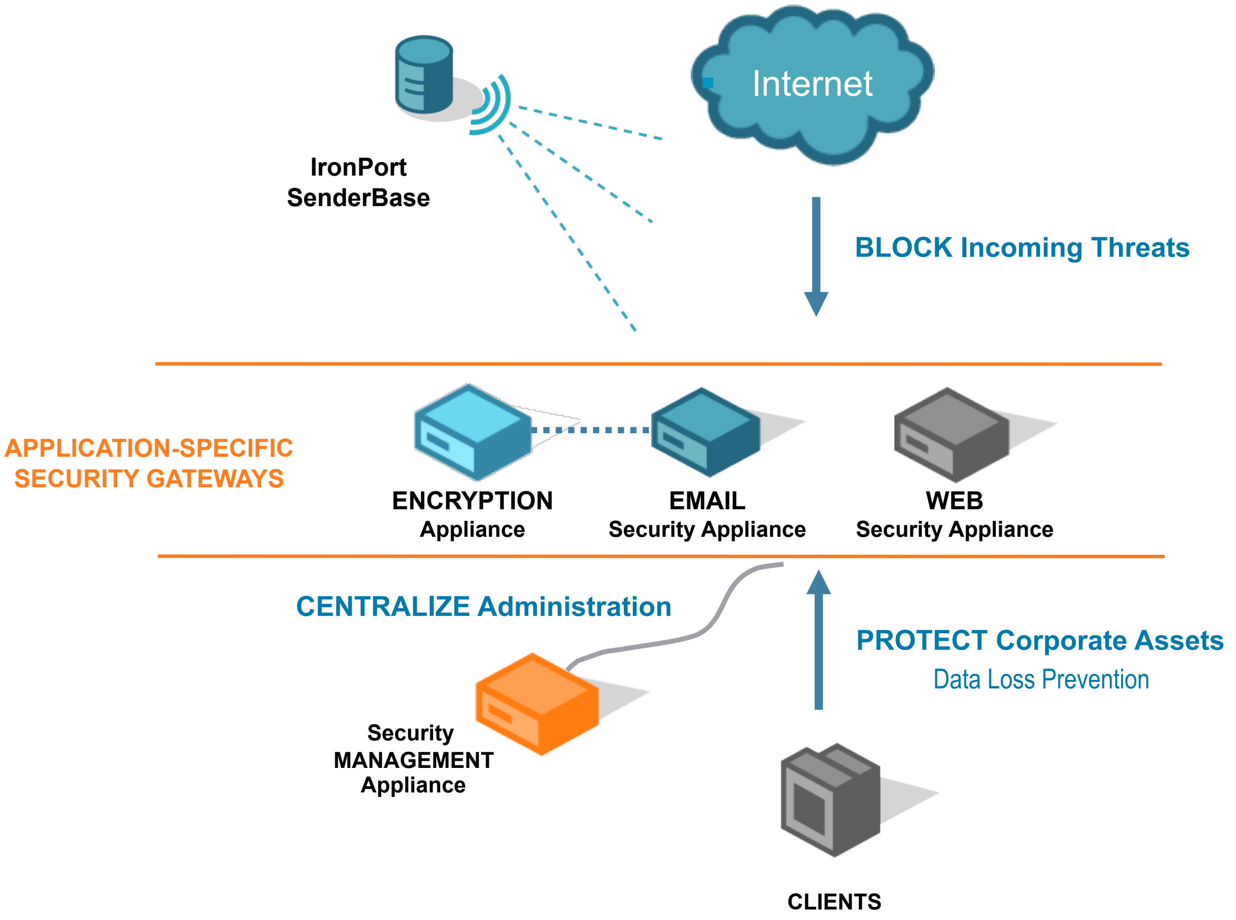
- Olympics
- European championships
- Earth day
- US Presidential election (November)

Solution???

Recommendations

- Understand the problem holistically
- New paradigm: attack in depth
- Measure infections on your network
- Protect the HTTP vector
  - #1 source of infections
- User education to combat social engineering
- NAC

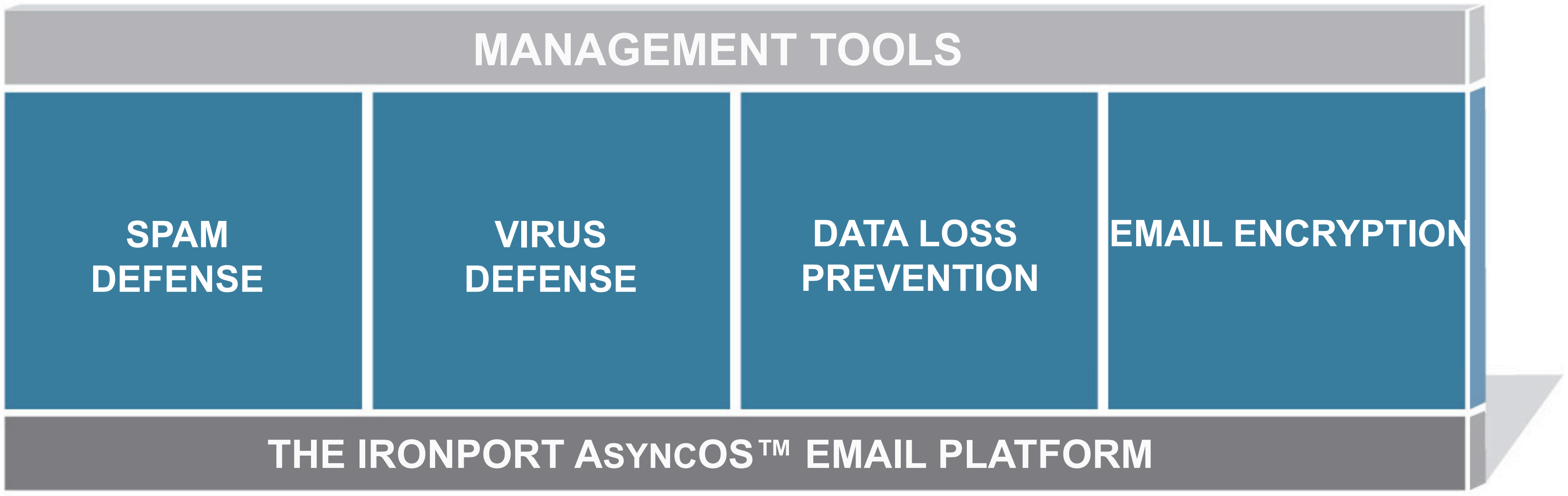
IronPort® Gateway Security Products



Web Security | Email Security | Security Management | Encryption

IRONPORT®

IronPort Architecture for Multi-Layered Email Security



MANAGEMENT TOOLS

SPAM DEFENSE

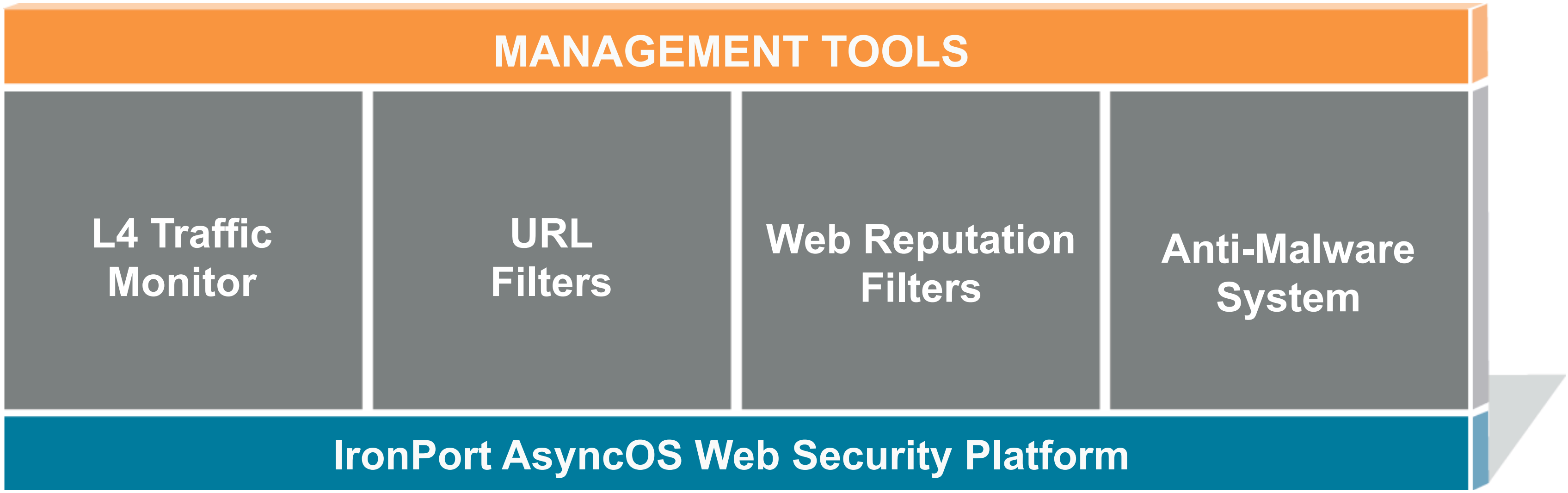
VIRUS DEFENSE

DATA LOSS PREVENTION

EMAIL ENCRYPTION

THE IRONPORT ASYNCOS™ EMAIL PLATFORM

IronPort Architecture for Multi-Layered Web Security



MANAGEMENT TOOLS

L4 Traffic Monitor

URL Filters

Web Reputation Filters

Anti-Malware System

IronPort AsyncOS Web Security Platform

Thank you!

IRONPORT®