The Open Proxy Problem: Should I Worry About Half a Million Trivially Exploitable Hosts?

Internet2/NLANR Joint Techs
University of Kansas, Lawrence
August 4th, 2003

Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu)
Director, User Services and Network Applications
University of Oregon Computing Center

http://darkwing.uoregon.edu/~joe/jt-proxies/

I. Introduction

My interest in proxy servers

- My interest in proxy servers goes back many years now.
- For example, I brought up the first Squid box at the University of Oregon (then a Sparc 5, wow! :-)), and I also encouraged deployment of caching web proxies at other Oregon University System schools and K12 sites statewide served by Oregon's OWEN/NERO network.
- I've also done beta testing of commercial cache boxes. My interest in proxy server security (or lack thereof) really dates from that testing work.
- While testing one particular commercial cache appliance, I noted it had *no* access controls at all; my feedback on that point to the vendor was blown off, and I was told "don't worry, our caches will always be deployed behind a firewall." No, in fact they weren't.

What was old became new again

- My interest in open proxy security issues was rekindled this last year when it became clear that spammers were exploiting insecure proxy servers to inject unsolicited commercial email.
- Examples of bulk email software products which have touted their use of proxies for sending bulk email include: G-Lock's EasyMail, List Sorcerer, Send-Safe, and many others.
- Clearly abuse of open proxies for sending spam had become a systematic/structural phenomenon. I became intrigued, and decided I should study the open proxies that were being abused.

Questions I had...

- -- Where were all these open proxies located? (Put another way, what ISPs seemed least competent when it came to dealing with abused boxes?)

  -- How many open proxies were out there? (I'd assumed that there were at most a few hundred, or maybe a couple of thousand, but I was off by several orders of magnitude)

  -- Which proxy blacklists worked best?

  -- I also wanted to test a theory I had that when publicly identified, insecure proxies tended to get fixed, or crushed into unusability by massive worldwide demand.
- This talk is the result of my investigation into open proxies and those topics.

"Is this talk relevant to me?"

- Because this talk introduces a security topic which hasn't been talked about at previous Joint Tech meetings, you may wonder, "Is this talk relevant to me?"
- I suppose that depends…
  -- If you’ve ever wondered how spammers anonymously shovel unsolicited commercial email at you, yes, it will be relevant.
  -- If you're attempting to develop a strategy to cope with spam, attempting to understand an attack vector you may be confronting, or attempting to understand why it is important to secure your own proxy, it's definitely relevant.
  -- If you’re an engineer responsible for your network's security, it definitely will be relevant.

"Is this talk relevant to me?" (2)

- -- If you’re concerned with acceptable use issues, privacy and anonymity issues, bandwidth management policies, maintaining Internet2/non-Internet-2 network traffic separation, etc., it will be relevant.

  -- The rest of you can hit the bar early. :-)

Talk format

- Just as we've done for other Joint Tech talks, this presentation has sufficient detail to allow for *post hoc* use as a tutorial, so that folks who may not be here can still work through what was covered.
- We've attempted to include “something for everyone” in this talk. Some may find it to be more technical than they might like, others may find it rehashes what they already know in spots -- sorry about that. [In particular, I wanted to insure that we all started with a common foundation of information about proxy servers.]
- I should also mention that this talk is an updated version of the presentation I did at the Internet2 Member Meeting in Arlington, Virginia, earlier this year.

What this talk is NOT about...

- This talk is NOT about eliminating open proxies as a way of facilitating censorship.
- Nor is this a primer on “how to be a cracker/hacker” or “how to be a spammer”; all the security issues mentioned are already publicly known and well documented.
- Lastly, this talk is not meant to dictate how you should run your network or how to configure your servers -- that's a decision for you to make after considering the totality of all applicable circumstances (but I do have some suggestions)

II. A Brief Tutorial on Caching Proxy Servers

What's a caching web proxy server? Why would anyone run one?

- Caching proxy servers are **NOT** intrinsically evil (*malum in se*).
- For instance, consider a computer lab being used by a class. The instructor may say, “Okay class, let's all look at the Smithsonian's web site. Please go to http://www.si.edu/”
- The thirty or forty students in that class then (all more-or-less simultaneously) retrieve a copy of the Smithsonian's home page (and its associated images) over the Internet.
- Think about what just happened -- why should *each* person in that class retrieve their *own* copy of the Smithsonian's web page via the Internet? Why not just let the *first* person to ask for that page retrieve a copy over the Internet, saving and (locally) sharing that recent copy with other local users who are also interested in that same page? It turns out that that's precisely what caching web proxy servers actually do….

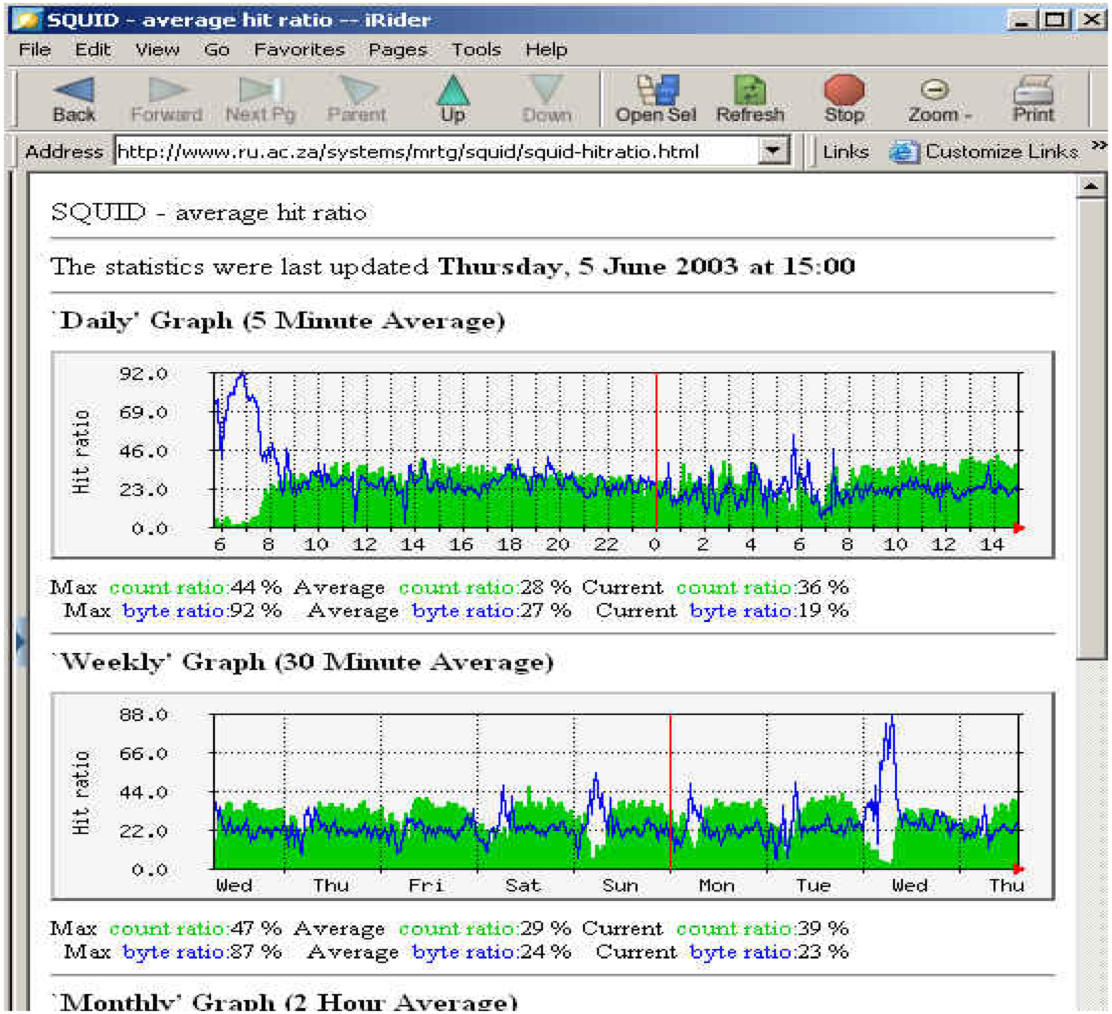
Quantifying bandwidth savings associated with doing web proxy caching...

- It is common to see cache vendors claim that a properly deployed web proxy cache box can typically serve 1/3 to 1/2 of all end user page requests locally, thereby reducing bandwidth usage by up to 25% or more.
- You can see some publicly available proxy cache stat reports by searching google for

  calamaris "Proxy Report“

  (Calamaris is one of the more popular web proxy cache log parsers).

Some folks even use MRTG to track web proxy cache hit ratios...



SQUID - average hit ratio

The statistics were last updated **Thursday, 5 June 2003 at 15:00**

'Daily' Graph (5 Minute Average)

Max count ratio:44 % Average count ratio:28 % Current count ratio:36 %
Max byte ratio:92 % Average byte ratio:27 % Current byte ratio:19 %

'Weekly' Graph (30 Minute Average)

Max count ratio:47 % Average count ratio:29 % Current count ratio:39 %
Max byte ratio:87 % Average byte ratio:24 % Current byte ratio:23 %

'Monthly' Graph (2 Hour Average)

Web proxy caching and improving the user’s "Internet experience"

- Caching can also improve the user's "Internet experience," since document retrievals "feels faster" (and large documents are delivered faster, considering bandwidth-delay product issues) when served from a local, lightly loaded, properly engineered cache box connected via gigabit ethernet.

There are <u>many</u> web caching proxy server products which one could use...

- Squid (free): http://www.squid-cache.org/
- Blue Coat (formerly CacheFlow): http://www.bluecoat.com/
- NetApp: http://www.netapp.com/products/netcache/
- Volera: http://www.volera.com/
- … and many others (including "big names" like Cisco, IBM, Microsoft, Sun, etc.)

Do ISPs actually use web proxy caching?

- You betcha. Not withstanding arguments for network transparency (e.g., RFC 2775), and not withstanding the ready availability of cheap commodity transit bandwidth (and the importance of non-proxy-enabled P2P applications in determining ISP bandwidth usage), caching is still common at many large ISPs such as AOL, Comcast, Cox, Road Runner, etc., as well as at large universities (e.g., http://www.cites.uiuc.edu/webcache/)

Both ends of the spectrum...

- One of the (many) ironies of web proxy caching is that web proxy caches tend to be deployed by two completely dissimilar types of sites: a) at huge ISPs (such as RBOCs, cable modem providers, and large universities) offering broadband connectivity to 10’s or 100’s of thousands of users, and b) at small sites that are thinly connected to the Internet (such as foreign sites paying outrageous fees for connectivity).
- Proxies also tend to pop up deployed both at the very center of large networks, as well as all the way out at the edge of the network, e.g., on customer workstations.
- Because of the diversity of deployment scenarios seen, it isn’t surprising that a wide variety of proxy products exist, and a wide variety of proxy-related problems arise.

For example: are all web pages cacheable?

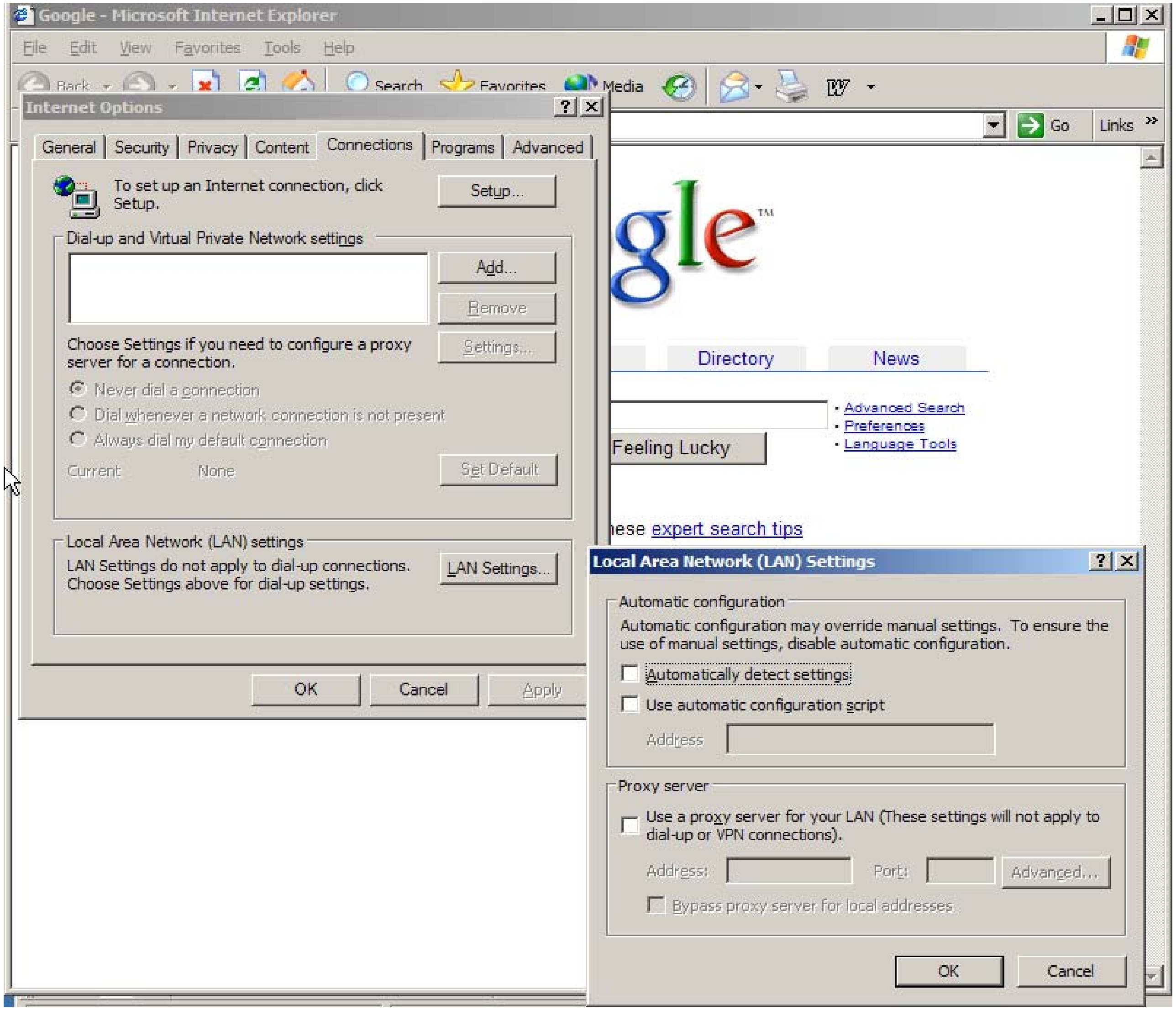
- It is comparatively easy to intentionally (or accidentally) create non-cacheable web pages, including:
  -- https (secure web pages), or pages protected with HTTP authentication
  -- pages with dynamic content (e.g., URLs including .cgi, .asp, a ? or a ; are often not cached), or pages using cookies
  -- pages explicitly marked as non-cacheable
- To check the cacheability of a given page, see http://www.ircache.net/cgi-bin/cacheability.py
- One of the most influential pages encouraging both cache deployment and cache-friendly web page design is the CacheNow! web site at http://vancouver-webpages.com/CacheNow/

Then there’s the issue of getting users to use a caching web proxy…

- Assuming an ISP wanted to deploy a web proxy cache, how might they do it? There are basically three different ways:

  One way is for a provider to offer a caching web proxy and allow users to manually configure their browser to use it (or not use it) as they personally see fit. This approach assumes that users will be willing and able to manually configure their web browser's settings/options/preferences to use the proxy server. [Doing that configuration isn't all that hard, but it isn't particularly intuitive, either, and it requires the user to enter a host name and port number, which is often site specific/poorly standardized]

Manually configuring IE



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

To set up an Internet connection, click Setup. [Setup...]

Dial-up and Virtual Private Network settings

[Add...] [Remove] [Settings...]

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None [Set Default]

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings. [LAN Settings...]

[OK] [Cancel] [Apply]

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

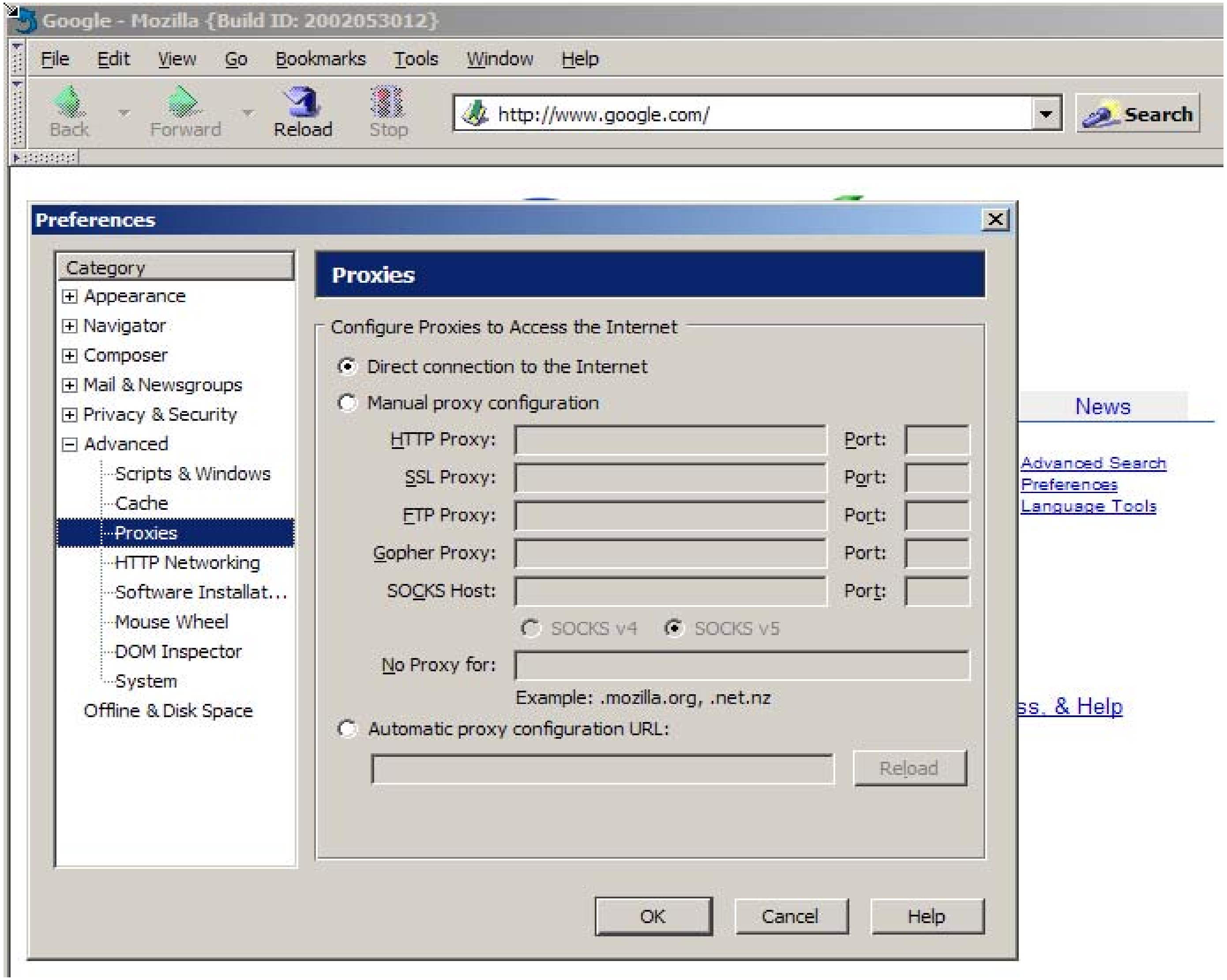
□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: [Advanced...]

□ Bypass proxy server for local addresses

[OK] [Cancel]

Manually configuring Mozilla



Proxies

Configure Proxies to Access the Internet

● Direct connection to the Internet

○ Manual proxy configuration

HTTP Proxy: Port:

SSL Proxy: Port:

FTP Proxy: Port:

Gopher Proxy: Port:

SOCKS Host: Port:

○ SOCKS v4 ● SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz

○ Automatic proxy configuration URL:

Reload

Another approach: ISPs "incenting" voluntary use of a web cache

- Why anyone would bother to use a non-mandatory web cache? At least some sites may offer "incentives" to encourage web cache use, such as exempting traffic flowing through the site's web cache from per-byte traffic charges, or excluding traffic flowing through the site's web cache from per-user traffic quotas, or excluding traffic flowing through the site's web cache from traffic shaping rulesets (thus usually making page downloads faster):

  -- http://rcn.oregonstate.edu/bandwidth_faq
  "Any traffic you use through the proxy server does not count against your inbound traffic limits."

  -- www.ucs.uwa.edu/web/info/access/netusage_faqs/traffic
  "If the item is already in the cache there is no charge."

Yet another approach: WPAD

- A site could also exploit WPAD (Web Proxy Auto-Discovery Protocol) to auto-direct most browsers (including IE) to a suitable local web cache.

- This assumes:
  -- users have left "Automatically detect settings" checked in their Internet Explorer Preferences (see the "Manually configuring IE" slide earlier in this talk)
  -- your web proxy cache box has a suitable name (e.g., wpad.<domain> (or WPAD info is being passed via DHCP at address assignment time)

Some WPAD references

- -- http://www.wrec.org/Drafts/draft-ietf-wrec-wpad-01.txt (expired draft)
  -- http://www.wrec.org/Drafts/draft-cooper-webi-wpad-00.txt (expired draft)
  -- http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/ proxy-live.html (03/1996)
  -- http://www.microsoft.com/windows2000/en/datacenter/help/ autodis.htm (see also the MS IE 5.X Resource Kit, Chapter 21)
- Don’t you love it when fundamentally important behaviors are largely documented in expired draft RFCs? :-;

Important security sidebar: wpad.<domain> is a magic/important hostname

- Because many web browsers automatically look for wpad.<domain>, uh, some security conscious folks might want to insure that that address is pointed at an, uh, "trustworthy" host. **This is a subtle but important point**.
- Empirically checking 211 Internet2 members to see if wpad.<domain> was in fact defined, I found that only six domains (bradley.edu, brandeis.edu, orst.edu, swmed.edu, ucsd.edu, uoregon.edu) bother to define wpad.<domain>.
- **Note: this statistic is 100% unchanged from the Spring I2 Member Meeting, when I first raised this issue.**
- Extra credit for the recursively aware: if your site uses subdomains, you might want to also check for wpad.<subdomain>.<domain>, etc. (See also wpad.<tld>)

Another approach: transparent web proxy caching

- A site can transparently ("passively") route all web traffic through a cache box, either by using Web Cache Communication Protocol (WCCP) on a router or layer 4 ethernet switch, or by physically forcing all traffic through an inline network gateway device which includes proxy server functionality.
- A few useful WCCP-related web pages are:
  www.cisco.com/warp/public/732/Tech/switching/wccp/
  www.cacheflow.com/support/config/transparent/wccp.cfm
  http://squid.visolve.com/developments/wccpv2.htm
- **Before considering ANY use of WCCP, see also: http://www.ciac.org/ciac/bulletins/i-054.shtml**

III. Inline Proxy Servers Aren't Just Web Proxy Cache Boxes Anymore

… they also include a corkscrew, a screwdriver, a nail file, a can opener, a magnifying glass, a tiny pair of little scissors, a toothpick….

Transparent caching using an inline gateway device

- The primary alternative to steering traffic via WCCP for inline transparent caching is forcing web traffic through a network "choke point" -- an inline gateway device functioning as a proxy (the gateway device may also act as a web content filter/traffic monitor, a firewall, anti-virus scanner, etc.)
- Customary downsides to single points of failure, and problems going really fast through an appliance, are hereby stipulated.

Despite single points of failure issues and capacity issues...

- … inline transparent cache boxes are still quite popular because of all the additional stuff that can be done in addition to the proxy server's basic caching functionality.
- Put another way, the availability of a single centralized possible point of control is just "too sweet" for many admins to forgo, which is why web content filtering software is perhaps the most common add-on....

Content filtering via an inline web proxy

- Some examples of web proxy filtering ("censorware") products deployed via inline transparent proxy boxes include:
  -- Bess (http://www.n2h2.com/)
  -- BlueCoat (http://www.bluecoat.com/solutions/content_filtering.html)
  -- SquidGuard (http://www.squidguard.org/)
  -- Websense (http://www.websense.com/)

- A critique of the merits of "censorware" is available at http://censorware.net/ see also http://www.sethf.com/anticensorware/

Advertising content filters deployed via an inline proxy

- It is worth mentioning that besides the semi-controversial "censorware" products targeting "objectionable"/ "recreational" web content, there are proxy filtering products which target cruft such as ads, popups, and a host of other obnoxious advertising-related stuff.
- http://internet.junkbuster.com/ and many others are listed at http://dmoz.org/Computers/Software/ Internet/Servers/ Proxy/Filtering/Ad_Filters/

Anti-viral filtering via an inline web proxy server

- Sites may also combine web proxies with anti-viral filtering at a gateway box.

- Examples of products doing this sort of thing include:
  -- Trend Micro's InterScan VirusWall
  -- McAfee WebShield
  -- Symantec AntiVirus Gateway

- **But hey, you’ve site licensed a desktop antivirus product and you’re doing SMTP executable attachment defanging for most virus mail with a simple dozen line procmail script already, right?**

Proxy servers for privacy enhancement

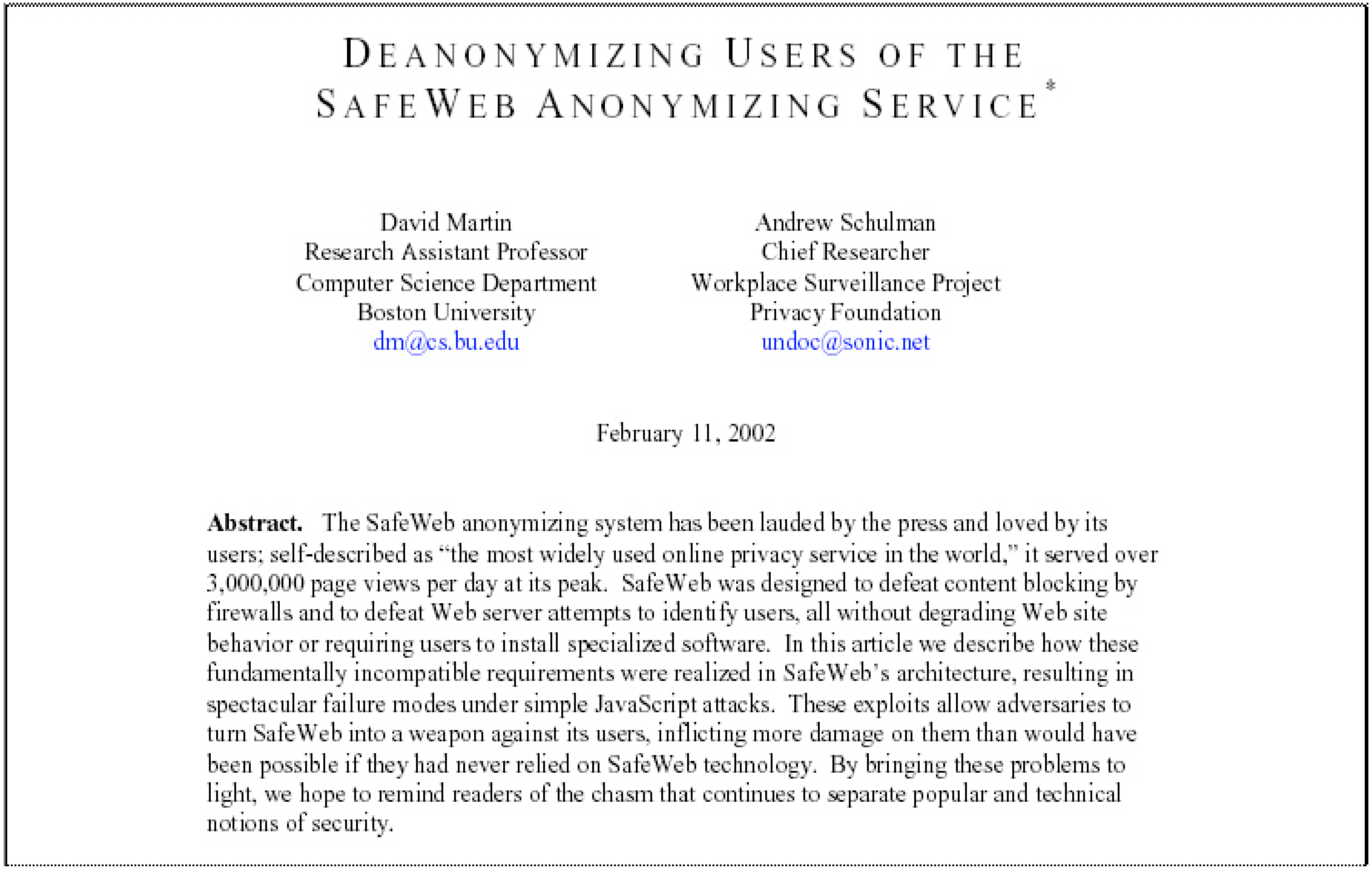
- Some people believe that proxy servers will give them "enhanced privacy;" maybe... but don't forget about X-Forwarded-For: headers![*]
- Various browser anonymity checking web sites will let you see what your browser is actually revealing when you connect via a proxy, including:
  http://www.all-nettools.com/pr.htm
  http://www.gemal.dk/browserspy/
  http://privacy.net/analyze/
  http://www.samair.ru/proxy/proxychecker/

[*] An example of enabling use of X-Forwarded-For header data: http://squid.sourceforge.net/follow_xff/

If you <u>really</u> need privacy...

- There are some companies that offer privacy enhancement services via proxy servers such as allconfidential.com, primedius.com, anonymizer.com, freedom.net, guardster.com, etc.
- Curious? You can test drive an anonymizer: http://anon.free.anonymizer.com/http://cnn.com/
- *Note:* I'm not qualified to assess the quality of the privacy delivered by these or any other service, but there are analyses out there you <u>should</u> see. For example...

http://cs.bu.edu/techreports/pdf/2002-003-deanonymizing-safeweb.pdf



DEANONYMIZING USERS OF THE SAFEWEB ANONYMIZING SERVICE*

David Martin
Research Assistant Professor
Computer Science Department
Boston University
dm@cs.bu.edu

Andrew Schulman
Chief Researcher
Workplace Surveillance Project
Privacy Foundation
undoc@sonic.net

February 11, 2002

Abstract. The SafeWeb anonymizing system has been lauded by the press and loved by its users; self-described as "the most widely used online privacy service in the world," it served over 3,000,000 page views per day at its peak. SafeWeb was designed to defeat content blocking by firewalls and to defeat Web server attempts to identify users, all without degrading Web site behavior or requiring users to install specialized software. In this article we describe how these fundamentally incompatible requirements were realized in SafeWeb's architecture, resulting in spectacular failure modes under simple JavaScript attacks. These exploits allow adversaries to turn SafeWeb into a weapon against its users, inflicting more damage on them than would have been possible if they had never relied on SafeWeb technology. By bringing these problems to light, we hope to remind readers of the chasm that continues to separate popular and technical notions of security.

Windows connection sharing

- Some entities run Windows host-based proxy servers as a way of sharing a single Internet connection.

  Examples include:

  -- ICS (integrated in Windows itself…)
  -- AnalogX Proxy
  -- Avirt Spaghetti
  -- Deerfield WinGate
  -- Grok Developments NetProxy
  -- Ingetic Proxy+
  -- Kerio WinRoute Pro
  -- Youngzsoft CCProxy, etc., etc., etc.

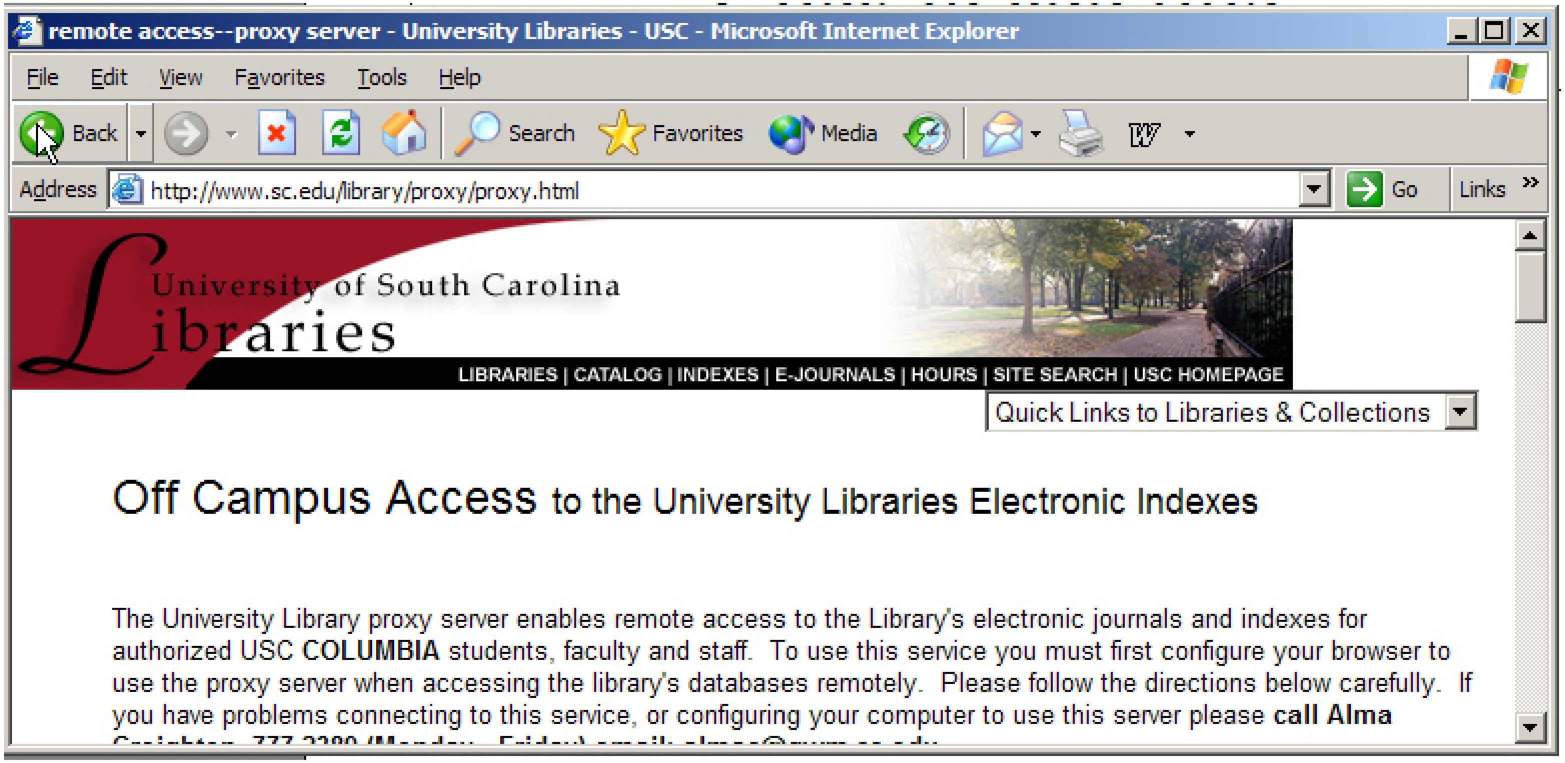
Windows connection sharing insecurity

- While some of those connection sharing products go to great pains to do that sharing securely, other Windows connection sharing products are quite "casual" about security.
- Moreover, **many of the open proxies we'll talk about later are actually associated with Windows connection sharing software installed by technically unsophisticated users** who have no idea what they've done when they install a proxy server without thoroughly locking it down.

Reverse proxies

- Another category of proxy server is the reverse proxy server. Reverse proxy servers are commonly deployed to allow remote users to do username and password authentication and gain access to domain-name- or ip-address-range-limited resources such as proprietary online databases. Reverse proxies are commonly deployed by academic libraries; a better alternative is to deploy a VPN offering authentication and encryption.

A typical academic library reverse proxy server



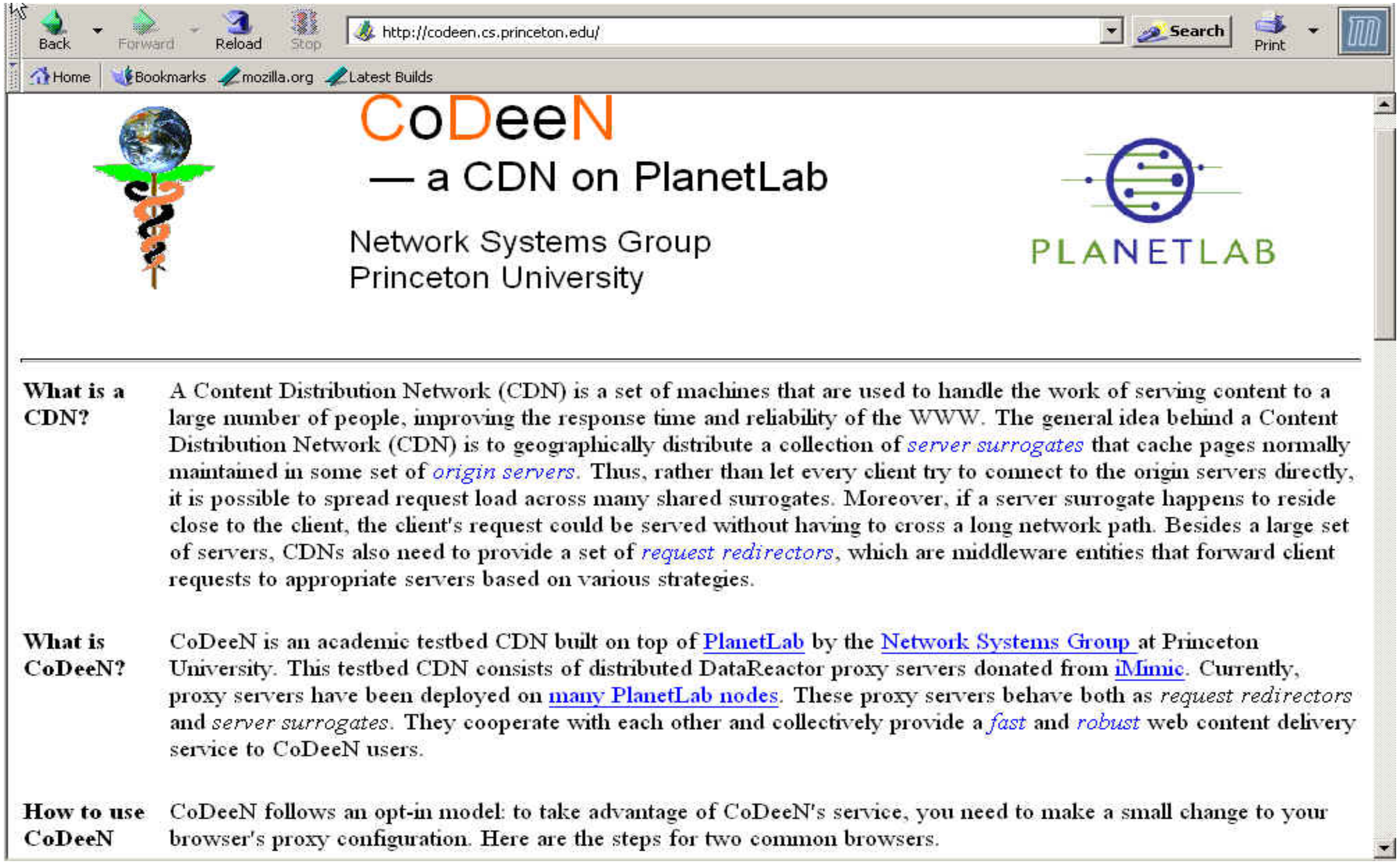
remote access--proxy server - University Libraries - USC - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.sc.edu/library/proxy/proxy.html
Go
Links
University of South Carolina
Libraries
LIBRARIES | CATALOG | INDEXES | E-JOURNALS | HOURS | SITE SEARCH | USC HOMEPAGE
Quick Links to Libraries & Collections

Off Campus Access to the University Libraries Electronic Indexes

The University Library proxy server enables remote access to the Library's electronic journals and indexes for authorized USC **COLUMBIA** students, faculty and staff. To use this service you must first configure your browser to use the proxy server when accessing the library's databases remotely. Please follow the directions below carefully. If you have problems connecting to this service, or configuring your computer to use this server please **call Alma** Creighton, 777-2280 (Monday - Friday) email: almac@gwm.sc.edu

Codeen

- And just this summer, Codeen, a DARPA-funded proxy server-based content distribution network running on top of PlanetLab, was deployed at a number of I2-connected schools:



CoDeeN

— a CDN on PlanetLab

Network Systems Group
Princeton University

What is a CDN? A Content Distribution Network (CDN) is a set of machines that are used to handle the work of serving content to a large number of people, improving the response time and reliability of the WWW. The general idea behind a Content Distribution Network (CDN) is to geographically distribute a collection of *server surrogates* that cache pages normally maintained in some set of *origin servers*. Thus, rather than let every client try to connect to the origin servers directly, it is possible to spread request load across many shared surrogates. Moreover, if a server surrogate happens to reside close to the client, the client's request could be served without having to cross a long network path. Besides a large set of servers, CDNs also need to provide a set of *request redirectors*, which are middleware entities that forward client requests to appropriate servers based on various strategies.

What is CoDeeN? CoDeeN is an academic testbed CDN built on top of PlanetLab by the Network Systems Group at Princeton University. This testbed CDN consists of distributed DataReactor proxy servers donated from iMimic. Currently, proxy servers have been deployed on many PlanetLab nodes. These proxy servers behave both as *request redirectors* and *server surrogates*. They cooperate with each other and collectively provide a *fast* and *robust* web content delivery service to CoDeeN users.

How to use CoDeeN CoDeeN follows an opt-in model: to take advantage of CoDeeN's service, you need to make a small change to your browser's proxy configuration. Here are the steps for two common browsers.

IV. Open Proxies

From benign to...

- Now that you understand a little about how proxy servers are supposed to work, let's buckle down and talk about the true subject of this talk: open proxies.

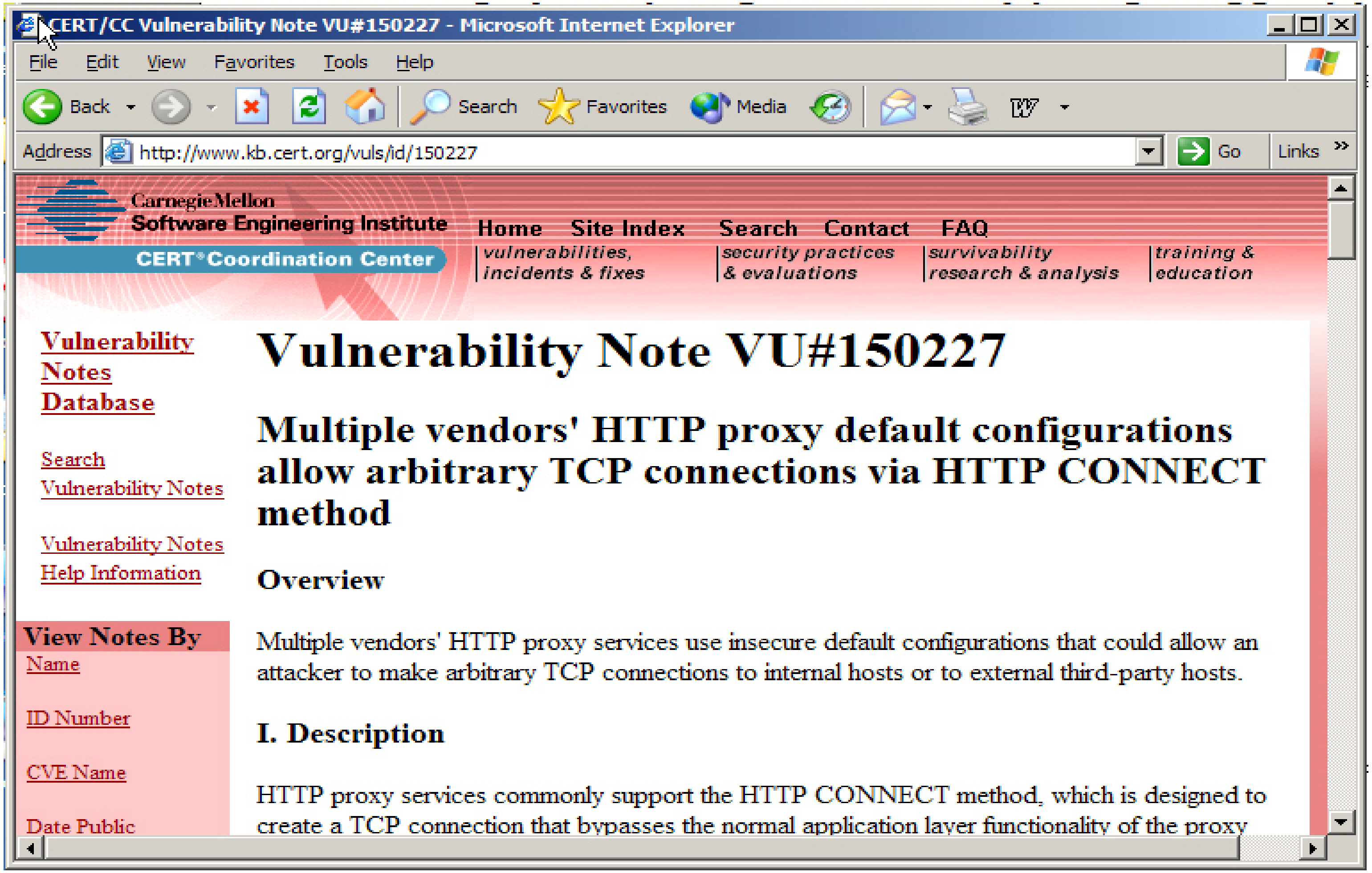
What is an "open proxy?"

- An open proxy is a computer that accepts connections from anyone, anywhere, and forwards the traffic from those connections as if it had originated locally from that host.
- In some cases, the proxied connection may only allow access to the world wide web, but in many cases the open proxy may also be used to ftp files, read and post Usenet news, send email (including spam), do IRC or instant messaging, launch a DOS attack, etc.

Open proxies are NOT the same as open SMTP relays

- Folks sometimes confuse open SMTP relays (which most folks now have pretty well under control) with open proxy servers.
- Open proxies are NOT the same as open SMTP relays -- open proxies are a far, far more serious problem, since they allow traffic for virtually ANY network service to be "bounced through" that host (although open proxies can and do also act as spam conduits).

Open proxies have been the subject of security bulletins...



CERT/CC Vulnerability Note VU#150227 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.kb.cert.org/vuls/id/150227
Go
Links
CarnegieMellon
Software Engineering Institute
CERT® Coordination Center
Home
Site Index
Search
Contact
FAQ
vulnerabilities, incidents & fixes
security practices & evaluations
survivability research & analysis
training & education
Vulnerability Notes Database
Search Vulnerability Notes
Vulnerability Notes Help Information
View Notes By
Name
ID Number
CVE Name
Date Public

Vulnerability Note VU#150227

Multiple vendors' HTTP proxy default configurations allow arbitrary TCP connections via HTTP CONNECT method

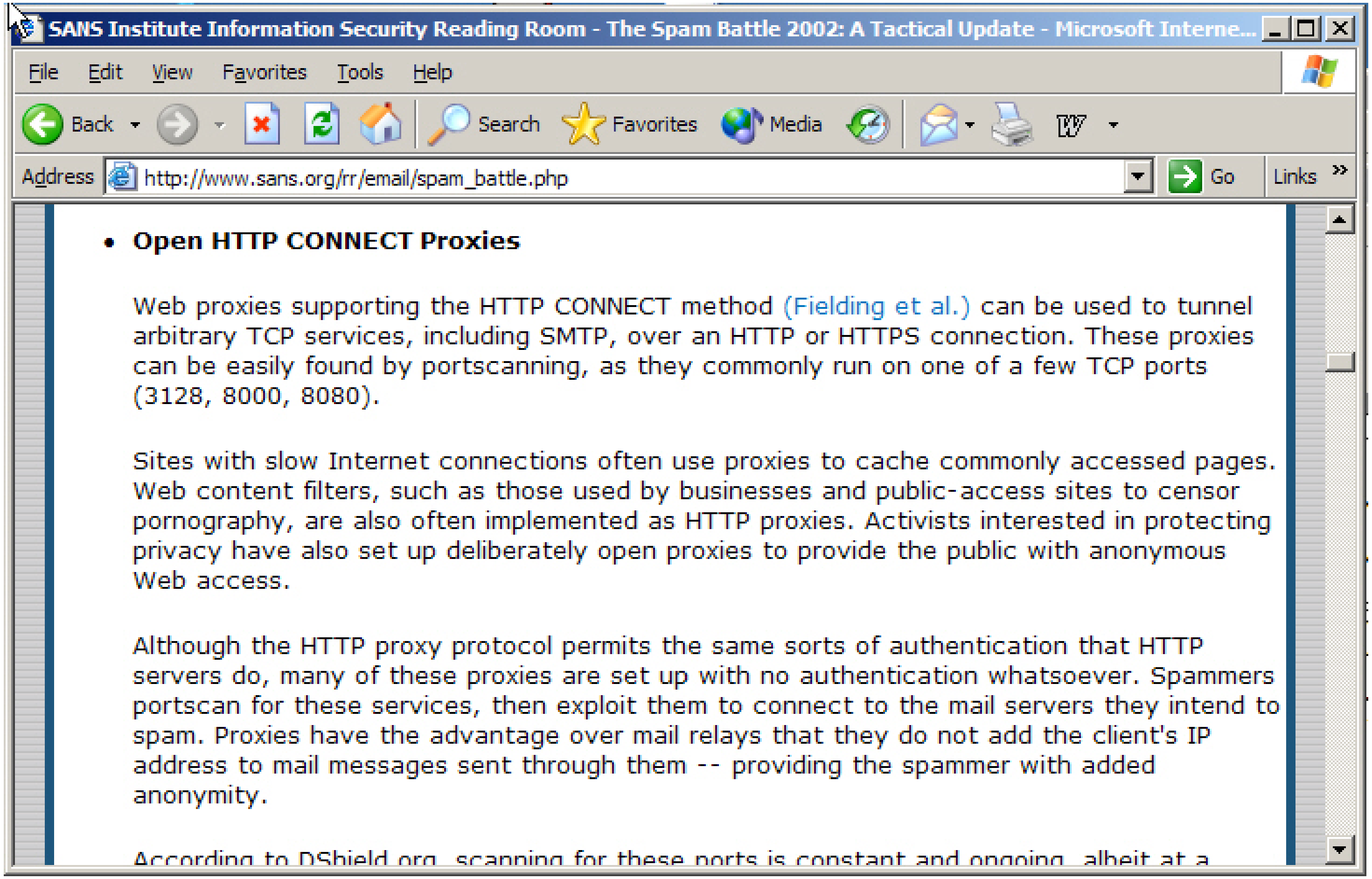
Overview

Multiple vendors' HTTP proxy services use insecure default configurations that could allow an attacker to make arbitrary TCP connections to internal hosts or to external third-party hosts.

I. Description

HTTP proxy services commonly support the HTTP CONNECT method, which is designed to create a TCP connection that bypasses the normal application layer functionality of the proxy

And excellent narrative discussions...


SANS Institute Information Security Reading Room - The Spam Battle 2002: A Tactical Update - Microsoft Interne...
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.sans.org/rr/email/spam_battle.php
Go
Links

- **Open HTTP CONNECT Proxies**

  Web proxies supporting the HTTP CONNECT method (Fielding et al.) can be used to tunnel arbitrary TCP services, including SMTP, over an HTTP or HTTPS connection. These proxies can be easily found by portscanning, as they commonly run on one of a few TCP ports (3128, 8000, 8080).

  Sites with slow Internet connections often use proxies to cache commonly accessed pages. Web content filters, such as those used by businesses and public-access sites to censor pornography, are also often implemented as HTTP proxies. Activists interested in protecting privacy have also set up deliberately open proxies to provide the public with anonymous Web access.

  Although the HTTP proxy protocol permits the same sorts of authentication that HTTP servers do, many of these proxies are set up with no authentication whatsoever. Spammers portscan for these services, then exploit them to connect to the mail servers they intend to spam. Proxies have the advantage over mail relays that they do not add the client's IP address to mail messages sent through them -- providing the spammer with added anonymity.

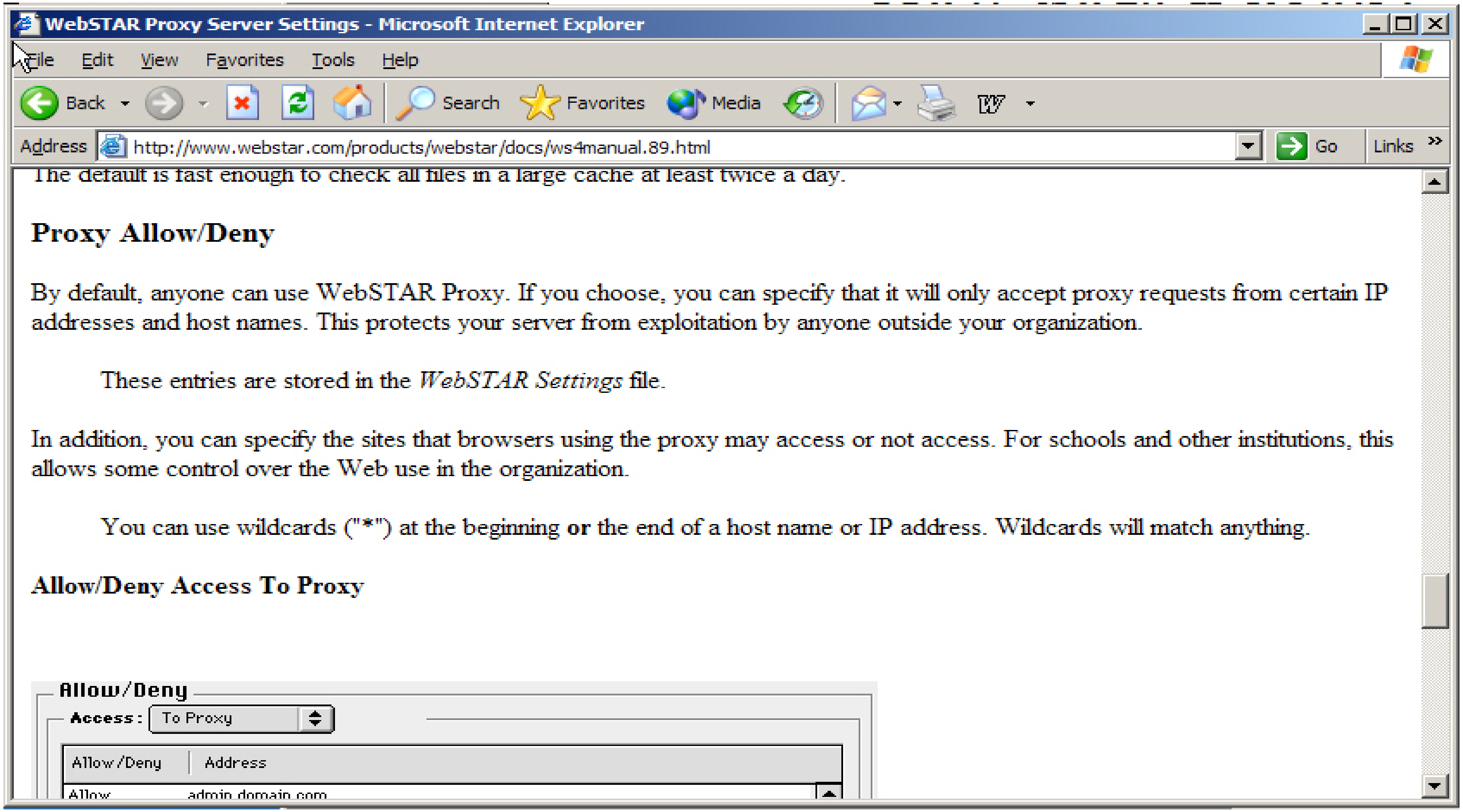
  According to DShield.org, scanning for these ports is constant and ongoing, albeit at a

So how does a proxy server become open and abusable?

- A proxy server becomes open due to:

  -- misconfiguration/lack of configuration by the administrator (e.g., a proxy server may ship "open by default," and access control lists may never have been installed, or if ACLs were installed, they may have been mis-specified)
  -- inherent protocol/application deficiencies (e.g., authentication in SOCKS4)
  -- a conscious decision on the part of the party installing the proxy to run it wide open (proxying software installed by hacker/crackers on 0wn3d boxes, proxying software intentionally run wide open for philosophical reasons, etc.)

Example of a proxy server shipping "open by default"


WebSTAR Proxy Server Settings - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.webstar.com/products/webstar/docs/ws4manual.89.html
Go
Links

The default is fast enough to check all files in a large cache at least twice a day.

Proxy Allow/Deny

By default, anyone can use WebSTAR Proxy. If you choose, you can specify that it will only accept proxy requests from certain IP addresses and host names. This protects your server from exploitation by anyone outside your organization.

These entries are stored in the *WebSTAR Settings* file.

In addition, you can specify the sites that browsers using the proxy may access or not access. For schools and other institutions, this allows some control over the Web use in the organization.

You can use wildcards ("*") at the beginning **or** the end of a host name or IP address. Wildcards will match anything.

Allow/Deny Access To Proxy

Allow/Deny

Access: To Proxy

Allow/Deny	Address
Allow	admin.domain.com

Trojan'd proxy servers

- Other users may be running a proxy server which was installed by a hacker/cracker via a virus/trojan horse
- Canonical example: jeem.mail.pv
  Jeem creates an open SMTP relay plus two open proxy ports on odd high numbered ports. See, for example:
  http://securityresponse.symantec.com/avcenter/venc/data/backdoor.jeem.html
- See also: http://www.lurhq.com/sobig.html
  http://www.lurhq.com/sobig-e.html
- As the pool of “normal" open proxies diminishes, we will probably see more virus-related activity to create proxies
- I mentioned the importance of site licensing a desktop antivirus product, and defanging attachments already, right?

V. Why Are Open Proxies of Interest to "Bad Guys"?

Are **bad guys** **really** **interested in open proxies?**

- Yes -- I believe open proxies are of exceptional interest to various and sundry "bad guys" for many reasons.
- To get an idea of some of those reasons, see the excellent day-in-the-life-of-an-abusable-proxy-server piece available at http://www.lurhq.com/proxies.html (“Exposing the Underground: Adventures of an Open Proxy Server”)
- Or it may help to just walk through things from their point of view for a bit...

(a) "I don't want folks to know where I'm *really* coming from"

- Connections made via an open proxy are often non-accountable, since the proxy may be doing no logging, or if logging is being done, logs may be unavailable to those investigating network incidents.
- In the case of bad guys who are exploiting proxy servers with the goal of trying to "cover their tracks," proxy server logs files *might* sometimes be obtainable. The accepted "bad guy solution" to that problem is to simply chain multiple proxy servers together, either manually or using a product such as http://proxychains.sourceforge.net/
- Doing explicit traffic routing via multiple indirect hops is not really a brand new idea...

Remember "blueboxes"?

- In 1971, (a long, ***long*** time ago by Internet standards), a popular activity with some "telephone hobbyists" was something called "tandem stacking." Someone engaged in tandem stacking might use a special device to chain a phone call from one central office switch to another, with the most audacious striving to build a path which would route a simple intra-city call thru switches spanning the globe. (*Esquire,* 10/1971)
- Thirty two years later, people are ***still*** routing traffic in unexpected ways -- but now the oddly routed traffic is network data traffic, not voice telephony traffic.
- For example, any technically inclined person will have wondered, "Why am I getting spammed (or why is my firewall getting probed) from odd places in Asia, Africa, and South America?"
- Concise answers: open proxies (of course).

(b) "I want to attack you from many odd locations at once!"

- Open proxies allow a single entity to launch attacks/send traffic from multiple provider-diverse sources at the same time, thereby complicating the problem of blocking spam or firewalling an attack. Dealing with multiple parallel (potentially changing) attack sources is one of several reasons why distributed denial of service network attacks are potentially so tough to deal with.

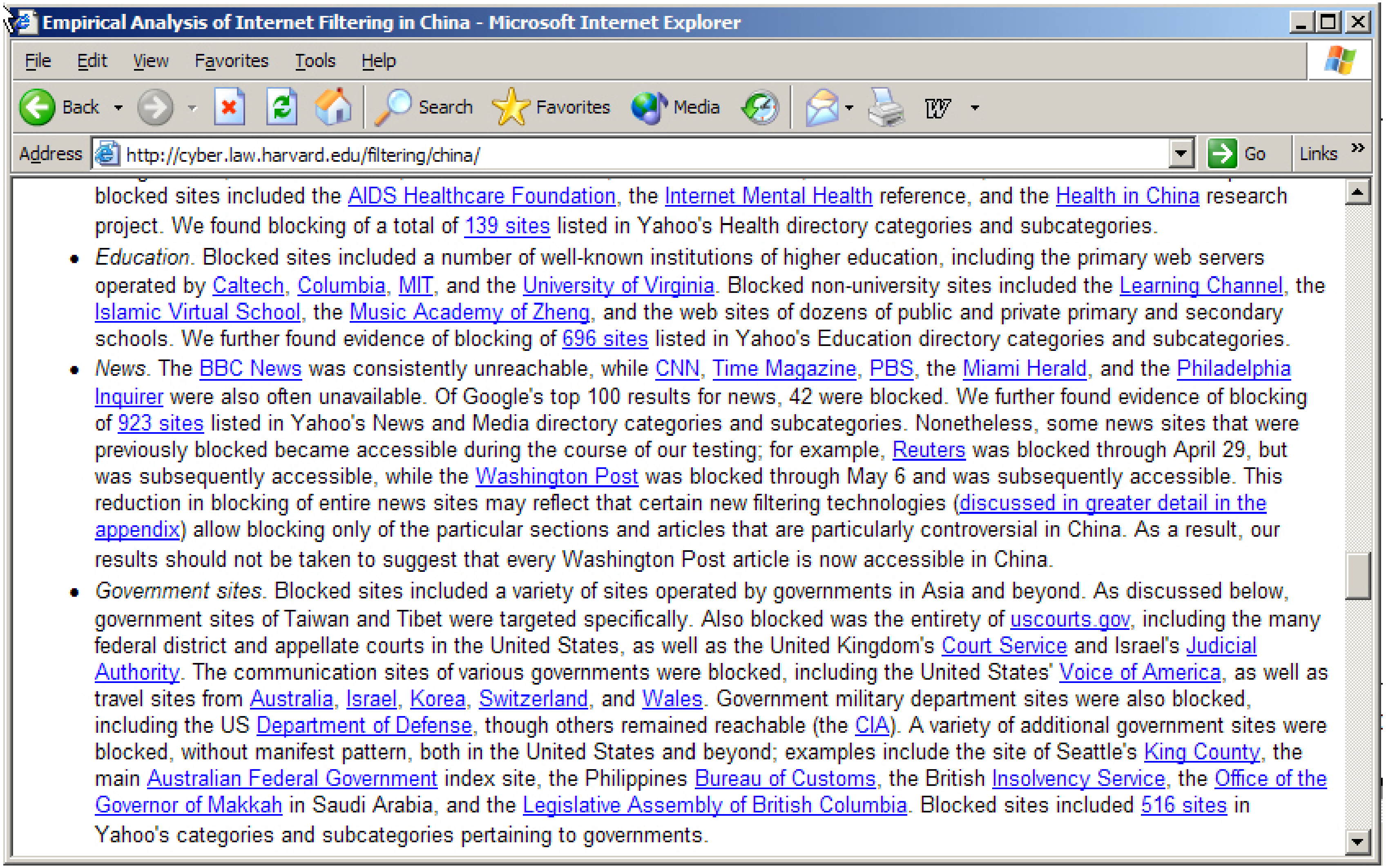
(c) "I want to try misleading naïve users by forging garbage into mail headers!"

- Unlike spam sent via an open SMTP relay, spam sent via an open proxy server can be constructed so as to have arbitrary Received: message headers, thereby inhibiting efforts at backtracking spam to its source.
- It is interesting that many of the latest generation of state anti-spam laws (see http://spamlaws.com/) prohibit spammer "falsification of message routing data"
- Use of open proxies is pretty much the best/only "message routing falsification" trick spammers have available once you get users to the "could you please turn on full headers?" level of spam analysis and reporting (http://micro.uoregon.edu/fullheaders/)

(d) "How dare you try to censor me!"

- By using an open proxy server, a user may be able to overcome local connection filtering.
- For example, if your local network disallows connections to recreational web sites, but intentionally or accidentally allows you to connect to an open proxy, you can access a recreational web site of interest by connecting to it indirectly, via the open proxy.
- Open proxy servers are thus particularly popular with subjects of totalitarian regimes, and K12 students.

For example: filtering in CN...

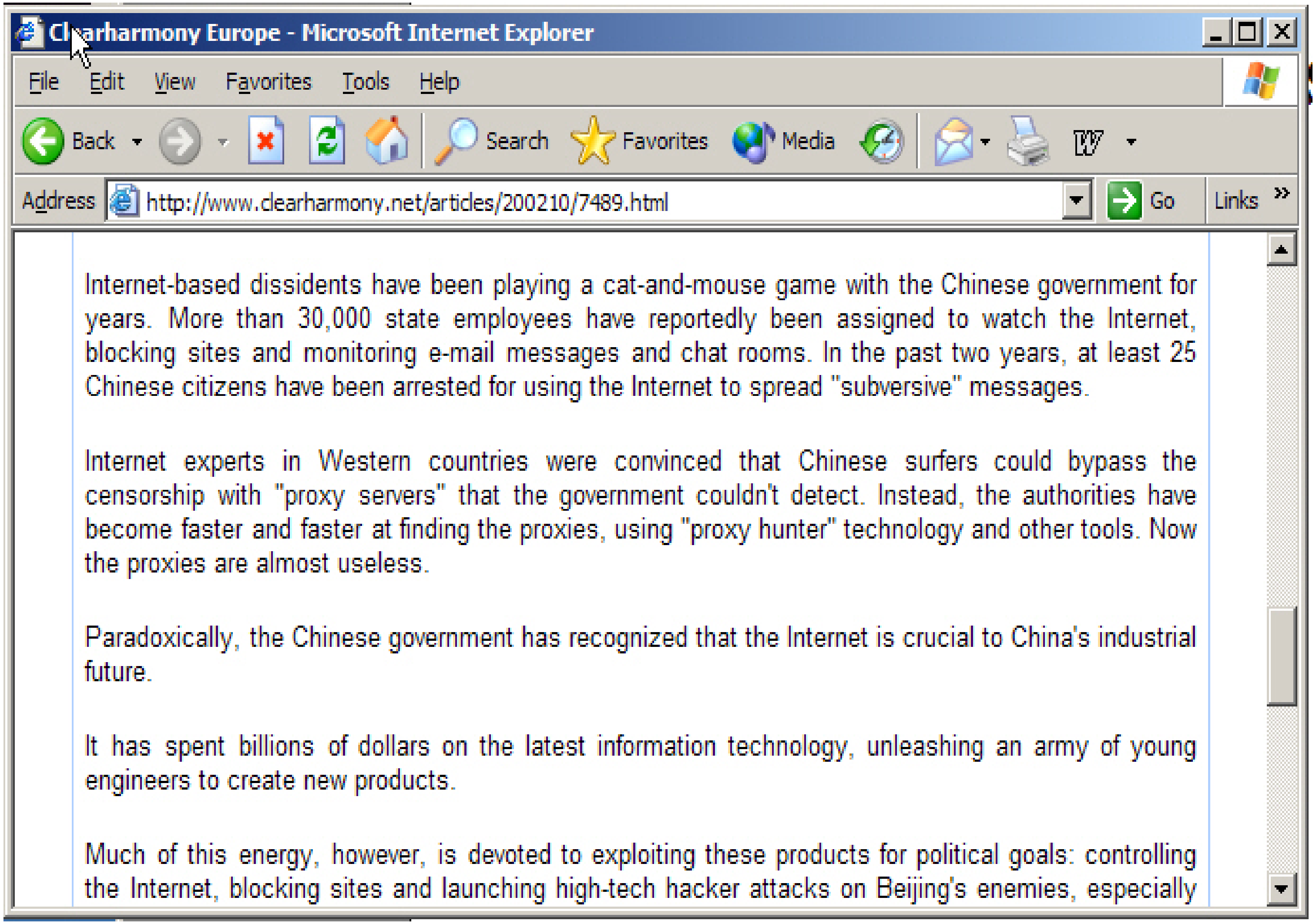


Empirical Analysis of Internet Filtering in China - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://cyber.law.harvard.edu/filtering/china/
Go
Links »

blocked sites included the AIDS Healthcare Foundation, the Internet Mental Health reference, and the Health in China research project. We found blocking of a total of 139 sites listed in Yahoo's Health directory categories and subcategories.

- *Education*. Blocked sites included a number of well-known institutions of higher education, including the primary web servers operated by Caltech, Columbia, MIT, and the University of Virginia. Blocked non-university sites included the Learning Channel, the Islamic Virtual School, the Music Academy of Zheng, and the web sites of dozens of public and private primary and secondary schools. We further found evidence of blocking of 696 sites listed in Yahoo's Education directory categories and subcategories.
- *News*. The BBC News was consistently unreachable, while CNN, Time Magazine, PBS, the Miami Herald, and the Philadelphia Inquirer were also often unavailable. Of Google's top 100 results for news, 42 were blocked. We further found evidence of blocking of 923 sites listed in Yahoo's News and Media directory categories and subcategories. Nonetheless, some news sites that were previously blocked became accessible during the course of our testing; for example, Reuters was blocked through April 29, but was subsequently accessible, while the Washington Post was blocked through May 6 and was subsequently accessible. This reduction in blocking of entire news sites may reflect that certain new filtering technologies (discussed in greater detail in the appendix) allow blocking only of the particular sections and articles that are particularly controversial in China. As a result, our results should not be taken to suggest that every Washington Post article is now accessible in China.
- *Government sites*. Blocked sites included a variety of sites operated by governments in Asia and beyond. As discussed below, government sites of Taiwan and Tibet were targeted specifically. Also blocked was the entirety of uscourts.gov, including the many federal district and appellate courts in the United States, as well as the United Kingdom's Court Service and Israel's Judicial Authority. The communication sites of various governments were blocked, including the United States' Voice of America, as well as travel sites from Australia, Israel, Korea, Switzerland, and Wales. Government military department sites were also blocked, including the US Department of Defense, though others remained reachable (the CIA). A variety of additional government sites were blocked, without manifest pattern, both in the United States and beyond; examples include the site of Seattle's King County, the main Australian Federal Government index site, the Philippines Bureau of Customs, the British Insolvency Service, the Office of the Governor of Makkah in Saudi Arabia, and the Legislative Assembly of British Columbia. Blocked sites included 516 sites in Yahoo's categories and subcategories pertaining to governments.

And it is clear the Chinese are aware of open proxy servers


Clearharmony Europe - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.clearharmony.net/articles/200210/7489.html
Go Links

Internet-based dissidents have been playing a cat-and-mouse game with the Chinese government for years. More than 30,000 state employees have reportedly been assigned to watch the Internet, blocking sites and monitoring e-mail messages and chat rooms. In the past two years, at least 25 Chinese citizens have been arrested for using the Internet to spread "subversive" messages.

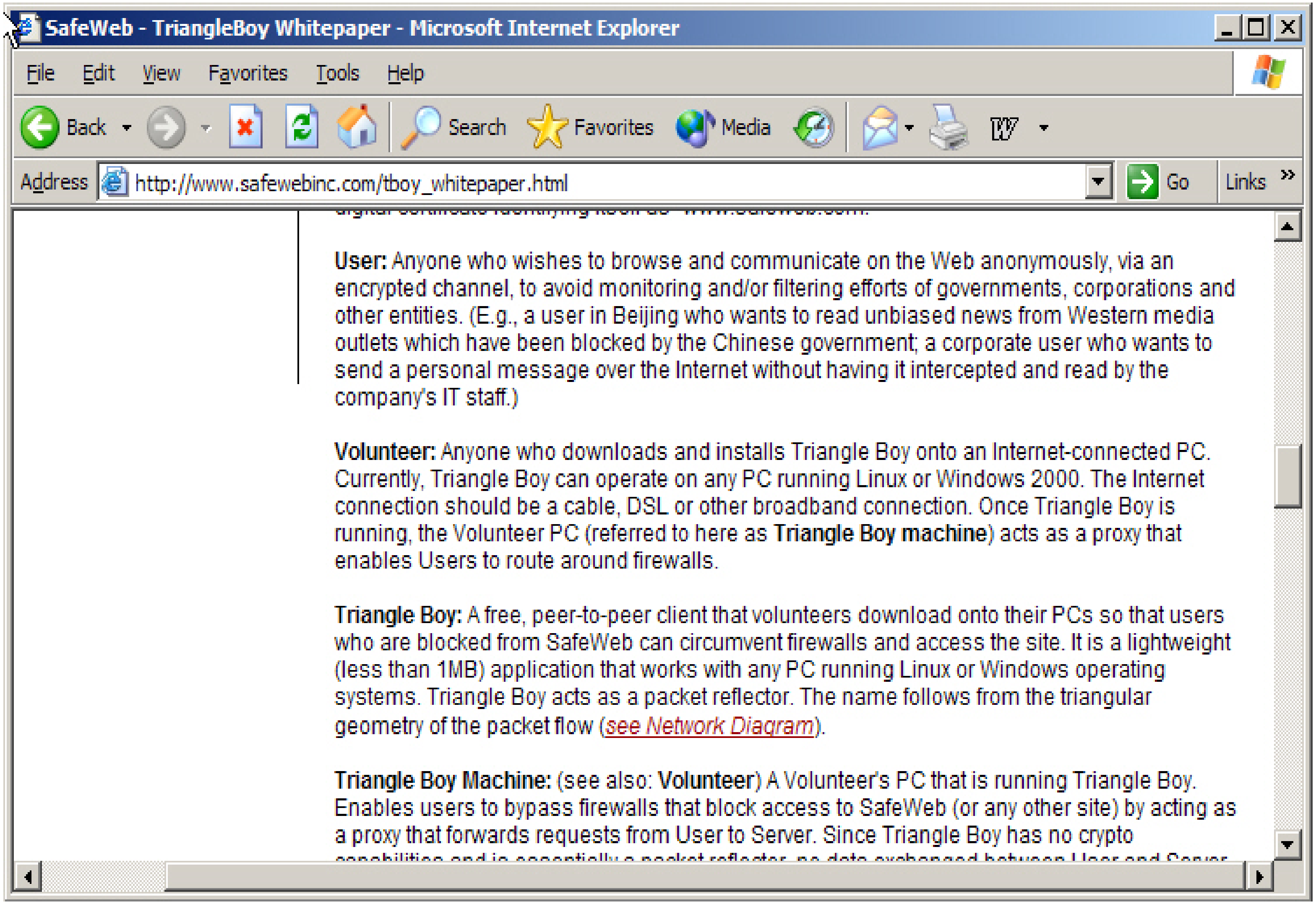
Internet experts in Western countries were convinced that Chinese surfers could bypass the censorship with "proxy servers" that the government couldn't detect. Instead, the authorities have become faster and faster at finding the proxies, using "proxy hunter" technology and other tools. Now the proxies are almost useless.

Paradoxically, the Chinese government has recognized that the Internet is crucial to China's industrial future.

It has spent billions of dollars on the latest information technology, unleashing an army of young engineers to create new products.

Much of this energy, however, is devoted to exploiting these products for political goals: controlling the Internet, blocking sites and launching high-tech hacker attacks on Beijing's enemies, especially

"Triangleboy"


SafeWeb - TriangleBoy Whitepaper - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.safewebinc.com/tboy_whitepaper.html
Go
Links

digital certificate identifying itself as "www.safeweb.com".

User: Anyone who wishes to browse and communicate on the Web anonymously, via an encrypted channel, to avoid monitoring and/or filtering efforts of governments, corporations and other entities. (E.g., a user in Beijing who wants to read unbiased news from Western media outlets which have been blocked by the Chinese government; a corporate user who wants to send a personal message over the Internet without having it intercepted and read by the company's IT staff.)

Volunteer: Anyone who downloads and installs Triangle Boy onto an Internet-connected PC. Currently, Triangle Boy can operate on any PC running Linux or Windows 2000. The Internet connection should be a cable, DSL or other broadband connection. Once Triangle Boy is running, the Volunteer PC (referred to here as **Triangle Boy machine**) acts as a proxy that enables Users to route around firewalls.

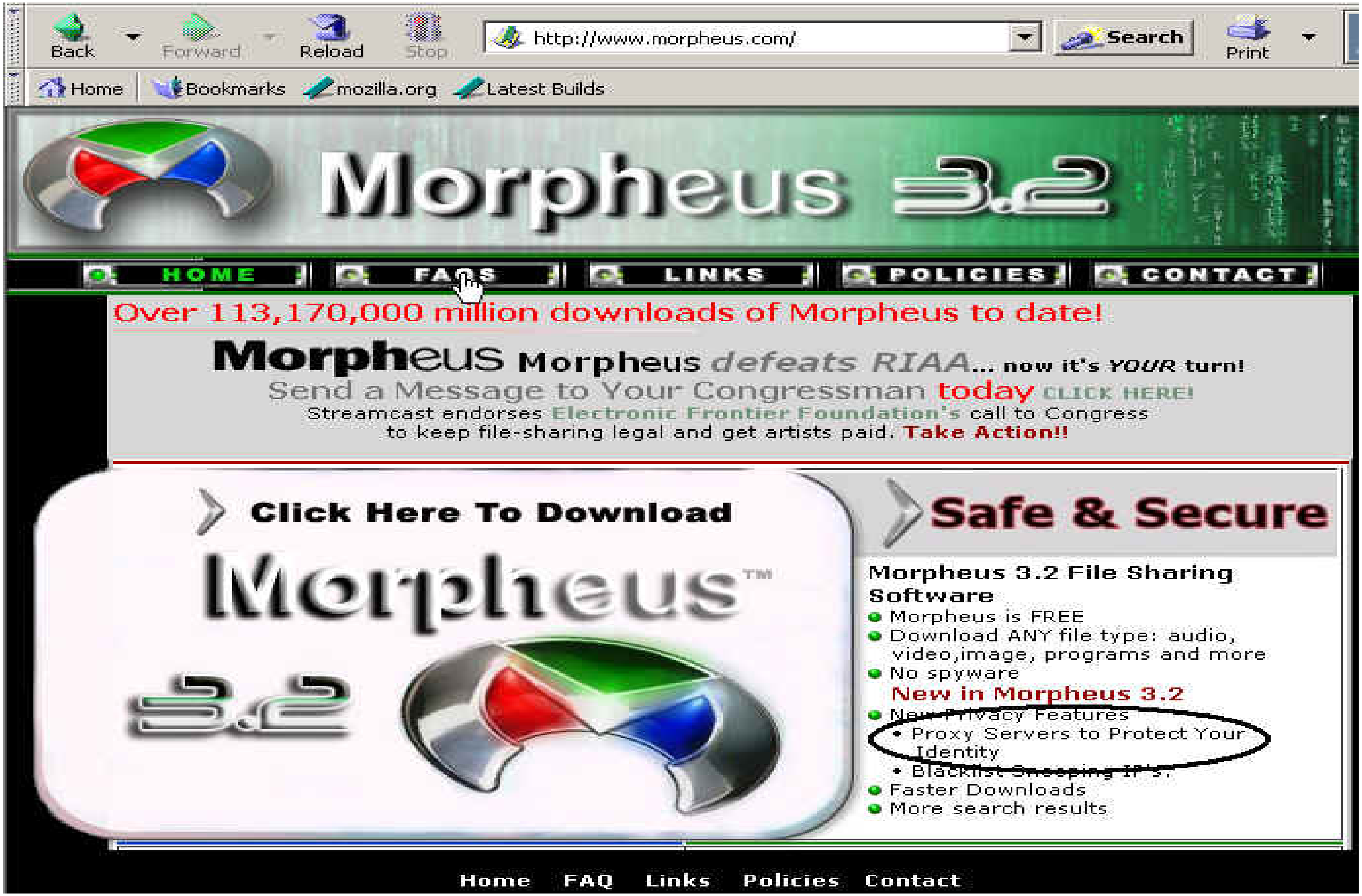
Triangle Boy: A free, peer-to-peer client that volunteers download onto their PCs so that users who are blocked from SafeWeb can circumvent firewalls and access the site. It is a lightweight (less than 1MB) application that works with any PC running Linux or Windows operating systems. Triangle Boy acts as a packet reflector. The name follows from the triangular geometry of the packet flow (*see Network Diagram*).

Triangle Boy Machine: (see also: **Volunteer**) A Volunteer's PC that is running Triangle Boy. Enables users to bypass firewalls that block access to SafeWeb (or any other site) by acting as a proxy that forwards requests from User to Server. Since Triangle Boy has no crypto capabilities and is essentially a packet reflector, no data exchanged between User and Server

(e) "Ack! They're blocking common P2P ports…"

- While there is substantial interest among users in accessing web content via proxies, and spammers certainly like to use proxies to send email, administrators may not recognize that even non-proxified peer-to-peer applications such as Kazaa, Edonkey, Grokster, etc. can **also** use proxy servers via 3rd party proxy tunnelling applications such as ProxyCap (http://proxylabs.netwu.com/proxycap/)
- Now that Morpheus 3.2 includes explicit integrated proxy server support, one should expect other P2P products to follow suit…

P2P applications -- with proxy support…



Over 113,170,000 million downloads of Morpheus to date!

Morpheus Morpheus *defeats RIAA*... now it's *YOUR* turn!

Send a Message to Your Congressman today CLICK HERE!

Streamcast endorses Electronic Frontier Foundation's call to Congress to keep file-sharing legal and get artists paid. Take Action!!

Click Here To Download

Morpheus™ 3.2

Safe & Secure

Morpheus 3.2 File Sharing Software

- Morpheus is FREE
- Download ANY file type: audio, video,image, programs and more
- No spyware

New in Morpheus 3.2

- New Privacy Features
  - Proxy Servers to Protect Your Identity
  - Blacklist Snooping IP's.
- Faster Downloads
- More search results

"My ISP is blocking outbound traffic sent directly to port 25…"

- Some bad guys may also be interested in open proxy servers as a way of getting past provider-installed filters on any outbound SMTP traffic (these sort of filters typically exempt only email that’s sent via the provider's designated SMTP server(s))..
- Providers who filter outbound port 25 traffic should also be smart enough to filter at least the common proxy server ports, but in some cases, maybe not.

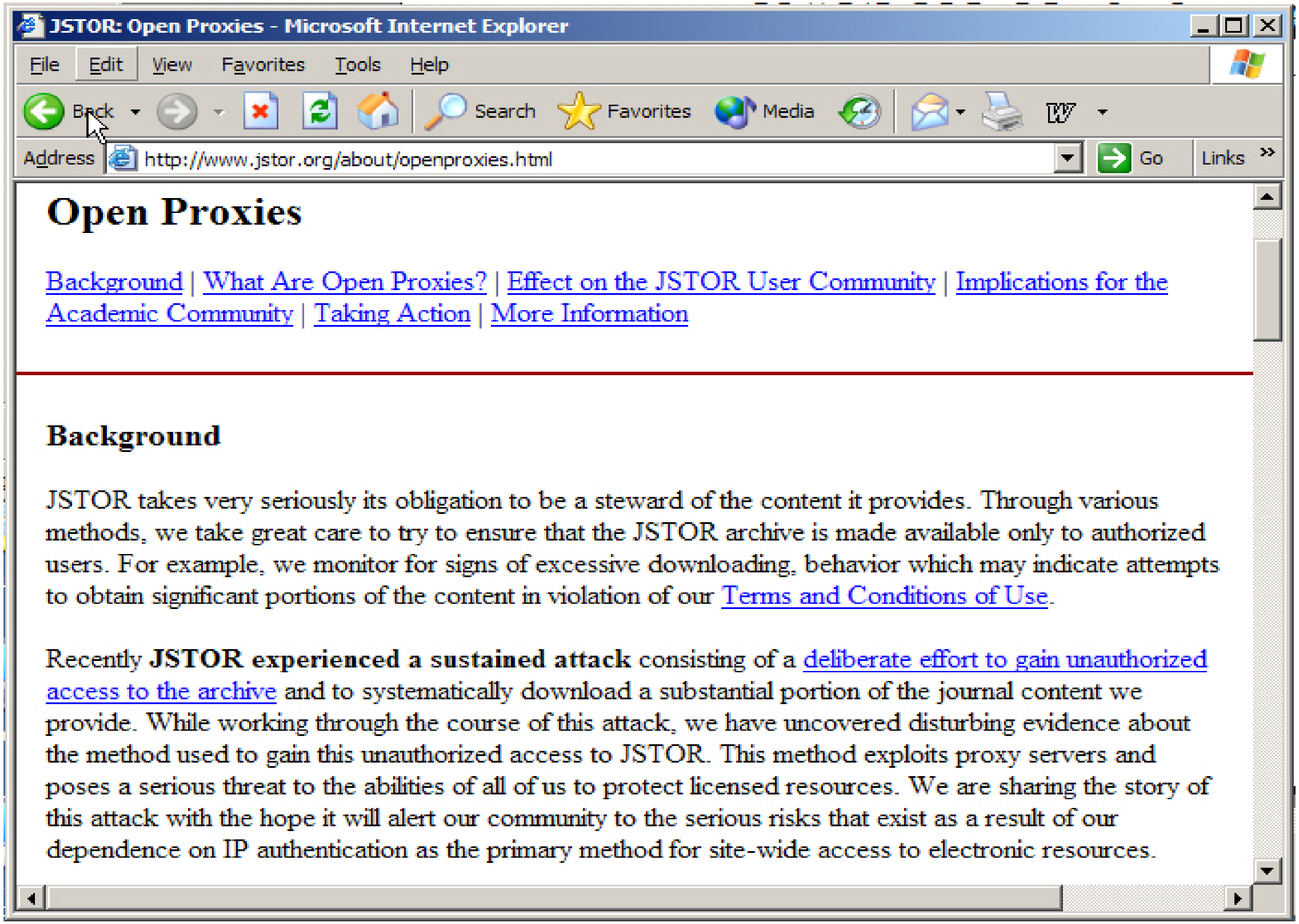
(f) "Hey, *I know* how we can get access to Internet2…"

- Particularly relevant to this audience, you should note that open proxy servers running at Internet2-connected sites may grant access to resources which might otherwise not be available, such as network access to Abilene, or network access to a federal government high performance mission network such as DREN, ESNet, NISN, etc.

(g) "Limited just to their site? Nah, it's open to the world…"

- More than just access to high performance networks is at risk from open proxies. Other assets which are vulnerable to the existence of local open proxies include:
  -- Usenet News servers
  -- site-licensed software distribution servers, and
  -- online proprietary databases, and
  -- any resource that does domain name or IP address-based access control
- For example...

JSTOR and open proxies



JSTOR: Open Proxies - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.jstor.org/about/openproxies.html Go Links

Open Proxies

Background | What Are Open Proxies? | Effect on the JSTOR User Community | Implications for the Academic Community | Taking Action | More Information

Background

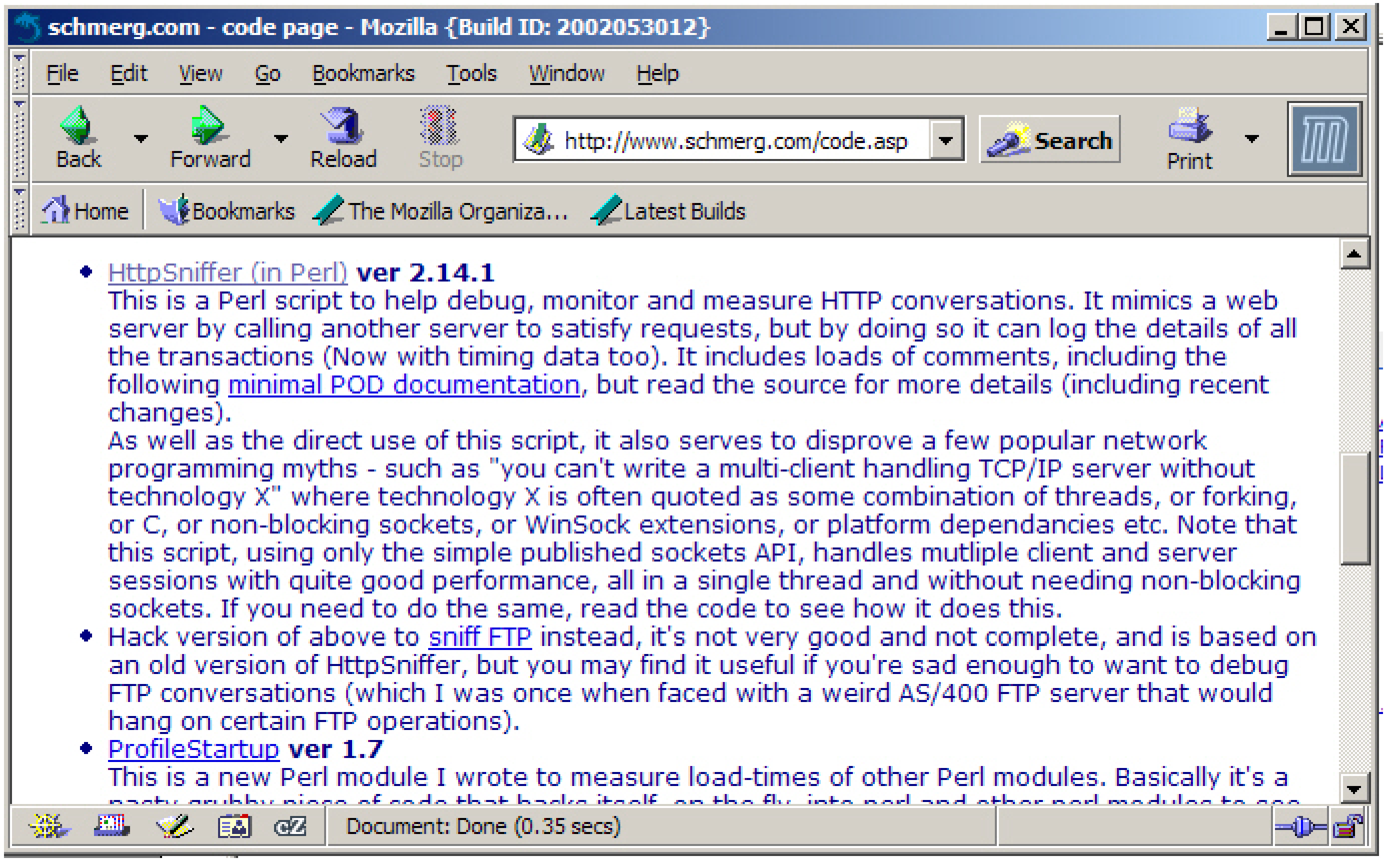
JSTOR takes very seriously its obligation to be a steward of the content it provides. Through various methods, we take great care to try to ensure that the JSTOR archive is made available only to authorized users. For example, we monitor for signs of excessive downloading, behavior which may indicate attempts to obtain significant portions of the content in violation of our Terms and Conditions of Use.

Recently **JSTOR experienced a sustained attack** consisting of a deliberate effort to gain unauthorized access to the archive and to systematically download a substantial portion of the journal content we provide. While working through the course of this attack, we have uncovered disturbing evidence about the method used to gain this unauthorized access to JSTOR. This method exploits proxy servers and poses a serious threat to the abilities of all of us to protect licensed resources. We are sharing the story of this attack with the hope it will alert our community to the serious risks that exist as a result of our dependence on IP authentication as the primary method for site-wide access to electronic resources.

(h) "I know a way we can get <u>all sorts</u> of traffic to sniff…"

- Open proxy servers may (or may not) offer you some level of privacy -- a proxy server may be logging nothing about a transaction that occurs via it, or, on the other hand, the proxy server may be undetectably sniffing every character that passes through it (and the origin of those transmissions), snagging unencrypted usernames and passwords, or other confidential info....
- Open proxy (ab)users should also be aware that apparently open proxy servers may actually be honeypots – see, for example:
  http://world.std.com/~pacman/proxypot.html

HttpSniffer


schmerg.com - code page - Mozilla {Build ID: 2002053012}
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://www.schmerg.com/code.asp
Search
Print
Home
Bookmarks
The Mozilla Organiza...
Latest Builds
Document: Done (0.35 secs)

- HttpSniffer (in Perl) **ver 2.14.1**
  This is a Perl script to help debug, monitor and measure HTTP conversations. It mimics a web server by calling another server to satisfy requests, but by doing so it can log the details of all the transactions (Now with timing data too). It includes loads of comments, including the following minimal POD documentation, but read the source for more details (including recent changes).
  As well as the direct use of this script, it also serves to disprove a few popular network programming myths - such as "you can't write a multi-client handling TCP/IP server without technology X" where technology X is often quoted as some combination of threads, or forking, or C, or non-blocking sockets, or WinSock extensions, or platform dependancies etc. Note that this script, using only the simple published sockets API, handles mutliple client and server sessions with quite good performance, all in a single thread and without needing non-blocking sockets. If you need to do the same, read the code to see how it does this.
- Hack version of above to sniff FTP instead, it's not very good and not complete, and is based on an old version of HttpSniffer, but you may find it useful if you're sad enough to want to debug FTP conversations (which I was once when faced with a weird AS/400 FTP server that would hang on certain FTP operations).
- ProfileStartup **ver 1.7**
  This is a new Perl module I wrote to measure load-times of other Perl modules. Basically it's a nasty grubby piece of code that hacks itself, on the fly, into perl and other perl modules to see

(i) "I'm ***not*** making enough on clickthroughs right now…"

- Open proxies may also be exploited by those who are trying to artificially generate inflated "hits" on revenue-generating web site links.

  Pay-per-hit revenue programs typically limit payments made on a per- unique-address basis, so to artificially inflate pay-per-hit revenues, you need lots of addresses from which to generate "hits"
  http://www.securiteam.com/securitynews/
  6M00B2A0KQ.html

(j) "Do you really suppose we could…"

- And of course, open proxy servers allow bored people to try random network experiments such as routing web traffic from a local workstation to a local server via a chain of proxies spanning the world, just like blueboxers from the early 1970's.

- And I'm just waiting for network researchers to start exploiting open proxies as “volunteer” endpoints for distributed network measurement projects. :-; Nah, that would never happen. :-)

VI. Open Proxies (From the Point of View of the Intended Users of That Proxy)

"I don't like this place at all
Makes me wonder what I'm here for
Someone take this pain away…"

Yet Another Day (Riva Remix),
from *Touched* (George Acosta)

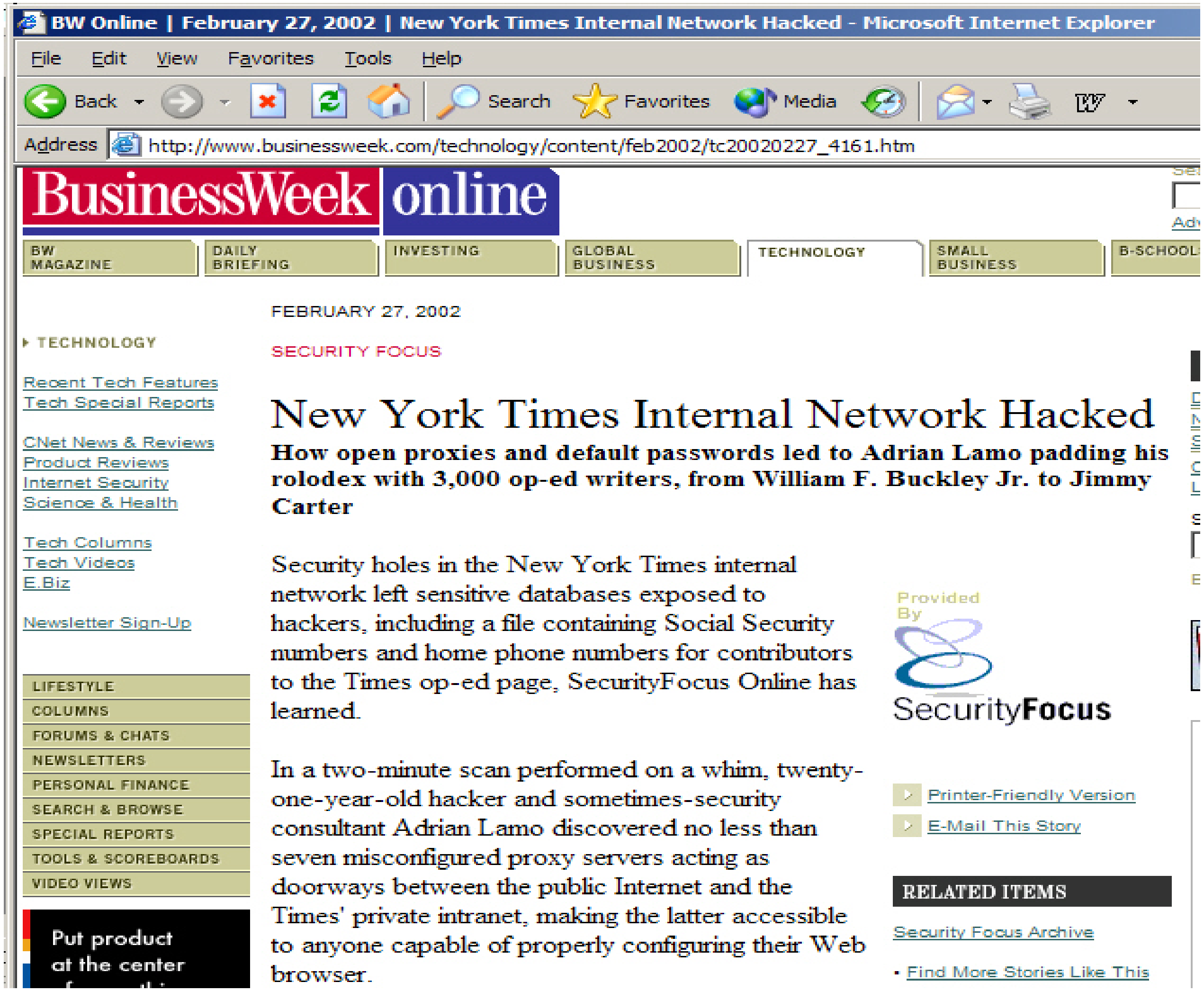
Problems associated with hosting an open proxy

- In addition to being a "public nuisance" or a security risk to the Internet at large for all the reasons outlined above, open proxy servers really do a disservice to "innocent parties" who sit behind them, too.

(a) Firewall? What firewall?

- Open proxy servers may serve as a conduit for inbound attacks, completely bypassing a site's firewall architecture.

This has happened to some prominent sites….



FEBRUARY 27, 2002

SECURITY FOCUS

New York Times Internal Network Hacked

How open proxies and default passwords led to Adrian Lamo padding his rolodex with 3,000 op-ed writers, from William F. Buckley Jr. to Jimmy Carter

Security holes in the New York Times internal network left sensitive databases exposed to hackers, including a file containing Social Security numbers and home phone numbers for contributors to the Times op-ed page, SecurityFocus Online has learned.

In a two-minute scan performed on a whim, twenty-one-year-old hacker and sometimes-security consultant Adrian Lamo discovered no less than seven misconfigured proxy servers acting as doorways between the public Internet and the Times' private intranet, making the latter accessible to anyone capable of properly configuring their Web browser.

(b) Sharing your pipe with a 100,000 of your closest friends

- Because anyone, anywhere, can freely access the Internet from an open proxy server, unauthorized users will often completely saturate the bandwidth available to that server.
- This typically results in extremely poor performance for the proxy server's intended users (often folks located in remote parts of the world where bandwidth is scarce or expensive).
- Oh yes: if your billing is usage sensitive, the end of the month can contain some nasty surprises, too.

(c) Warrants, subpoenas, and writs, oh my!

- If you host open proxy servers, you should not be surprised if you see a steady stream of warrants, subpoenas and writs seeking customer information, copies of server contents (or the servers themselves).
- I would assert that it is better to buy network engineers and/or security staff to deal with open proxies rather than lawyers to deal with warrants, but each to their own.

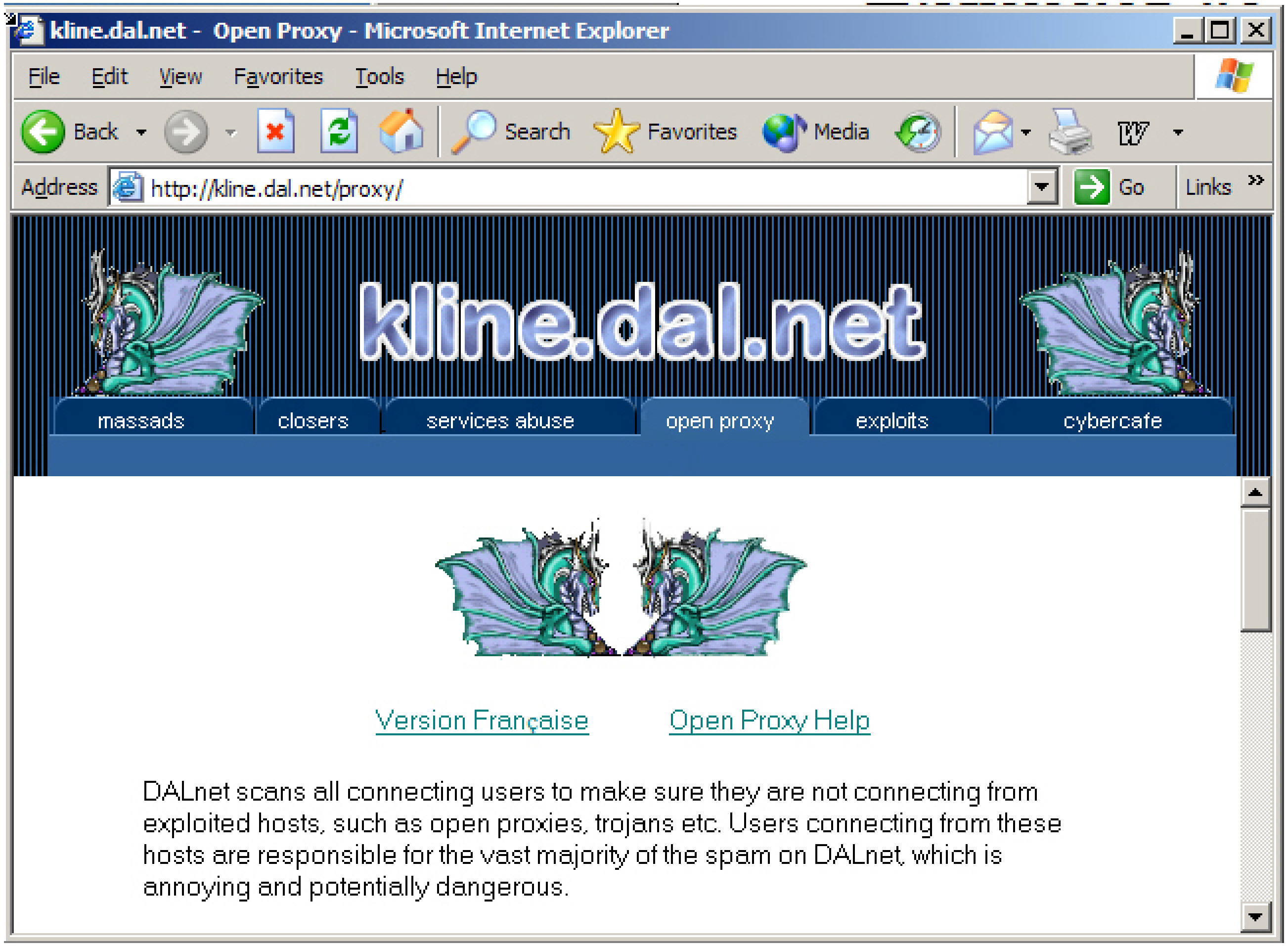
(d) Open proxies may attract probes for other vulnerabilities

- Hosting persistently open proxies may result in an increased risk of that host (and its network) getting scanned for other vulnerabilities, presumably because persistent open proxies serves as an indicator that no one cares/no one is paying attention. This is much like the association between graffiti and crime rates in decaying urban areas. [Customers of some RBOCs must be seeing *incredible* levels of scans…]

(e) Anti-open proxy DNSBLs may block legitimate users

- As open proxy servers become identified and added to open proxy blacklists, legitimate users of those proxy servers may suddenly find that they are blocked by DNSBLs from accessing Internet resources (such as IRC servers) because they are connecting from an open proxy server.

Example of an IRC network blocking open proxies



kline.dal.net - Open Proxy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://kline.dal.net/proxy/ Go Links
kline.dal.net
massads
closers
services abuse
open proxy
exploits
cybercafe

Version Française Open Proxy Help

DALnet scans all connecting users to make sure they are not connecting from exploited hosts, such as open proxies, trojans etc. Users connecting from these hosts are responsible for the vast majority of the spam on DALnet, which is annoying and potentially dangerous.

"Compared to the locusts, the frogs weren't really that bad"

- While having an open proxy DNSBL list a particular /32 can be admittedly inconvenient if you are a user of that open proxy server, it is far LESS inconvenient than having your entire country blocked!
- Yes, there ARE country-wide blacklists in use by people who are completely fed up with spam from some parts of the world that just don't seem to care about network abuse. (I discourage use of country-wide DNSBLs)

Some examples of <u>country-wide</u> blacklists

- http://www.blackholes.us/ (DNSBLs for network blocks assigned to ISPs in AR, BR, CN, HK, JP, KR, MY, NG, RU, SG, TW, TH; also has blackhole DNSBLs for selected large US/international ISPs)
- http://www.okean.com/asianspamblocks.html
- See also: "Not All Asian E-Mail is Spam" http://www.wired.com/news/politics/0,1283,50455,00.html
- Per-ASN blacklists are probably a better solution; see http://cc.uoregon.edu/cnews/summer2003/perasn.html

(f) "Semi-innocent" local users may get targeted by inept local bandwidth witch hunts

- When connections get saturated and local performance becomes awful, rather than suspecting that users from all over the world are connecting to an open proxy and gobbling up bandwidth, many folks will just say "AHAH! Someone is <fill in relatively trivial unacceptable local network behavior here>…" with predictable results: a local inquisition and bandwidth crackdown.
- Hint: your horrible network bandwidth usage problem is probably NOT the result of some kid playing a network game.

(g) More joy of open proxies: getting LOTS of complaints

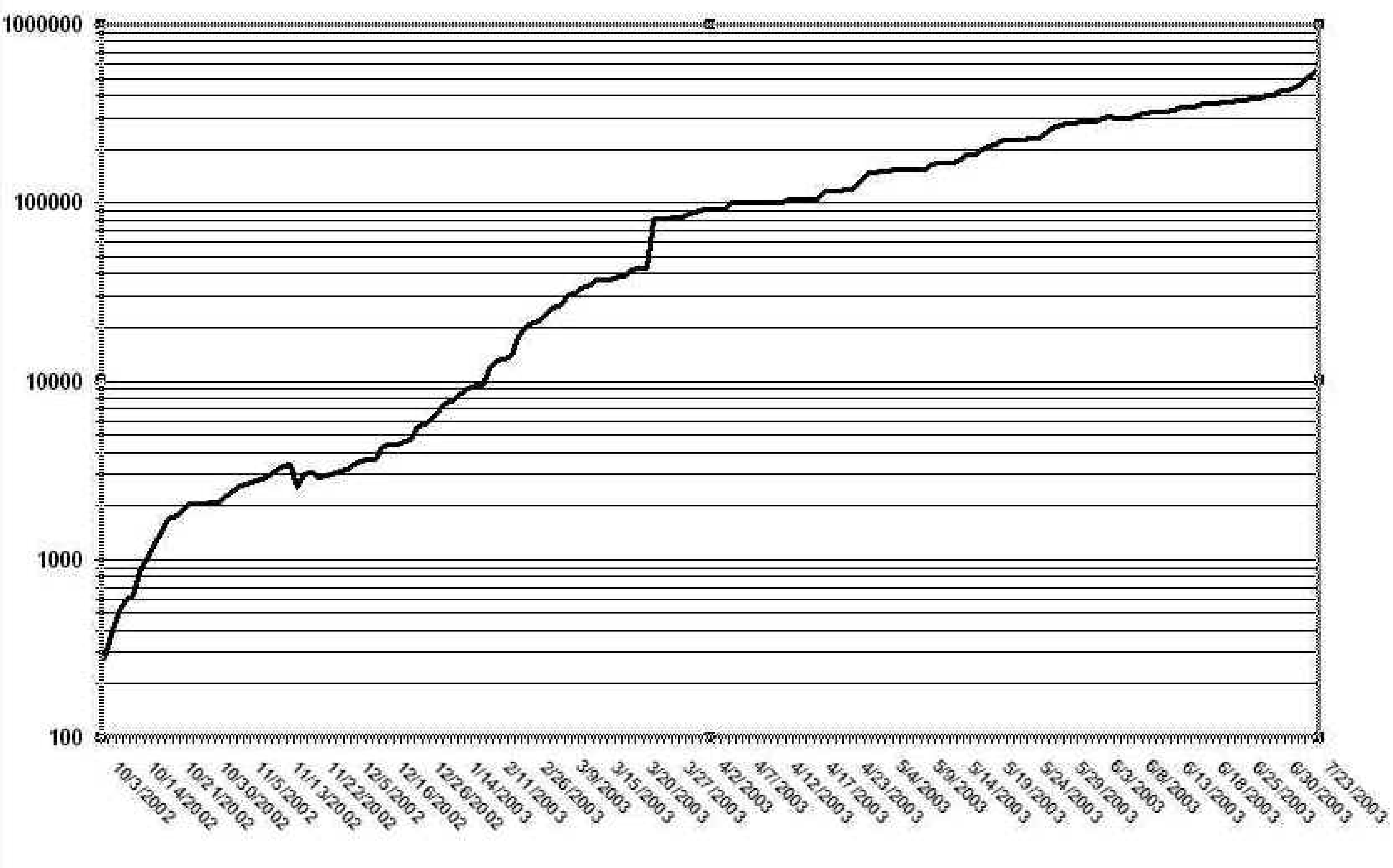
- The parties of record responsible for your network will get LOTS of complaints from angry users who've gotten spammed or otherwise abused via a local open proxy.
- Parties who will get complaints include whois-listed contacts for your domain, network address block, and ASN; your postmaster and security staff; your DMCA contact of record; random senior management; etc.
- If left undealt-with, complaint volume can cause an abuse response "death spiral:“ too many complaints come in to handle, so abuse addresses are /dev/null’d, so abuse problems increase, real customers flee, spammer business is thought to be critical to avoid financial collapse, etc.)
- Oh yes: don’t get listed on http://www.rfc-ignorant.org/

Okay, so having an open proxy really isn't that much fun...

- 100% correct. Having an open proxy server on your network can be really can be miserable.

  Given that, what’s really amazing is that despite the substantial pain associated with hosting an open proxy server, and the fact that an open proxy server can exist only if BOTH the system owner/sysadmin AND their ISP or local network administrator don't take steps to deal with the problem, there are LOTS of open proxies out there.

VII. How Many Open Proxies Are Out There?



A serious epidemic, or one person with sniffles?

- The severity of the open proxy problem, like many other problems, is largely a function of its size.
- Obviously, if there are only a few hundred open proxies, the problem is a different one than if there are thousands or tens of thousands or hundreds of thousands of open proxies.

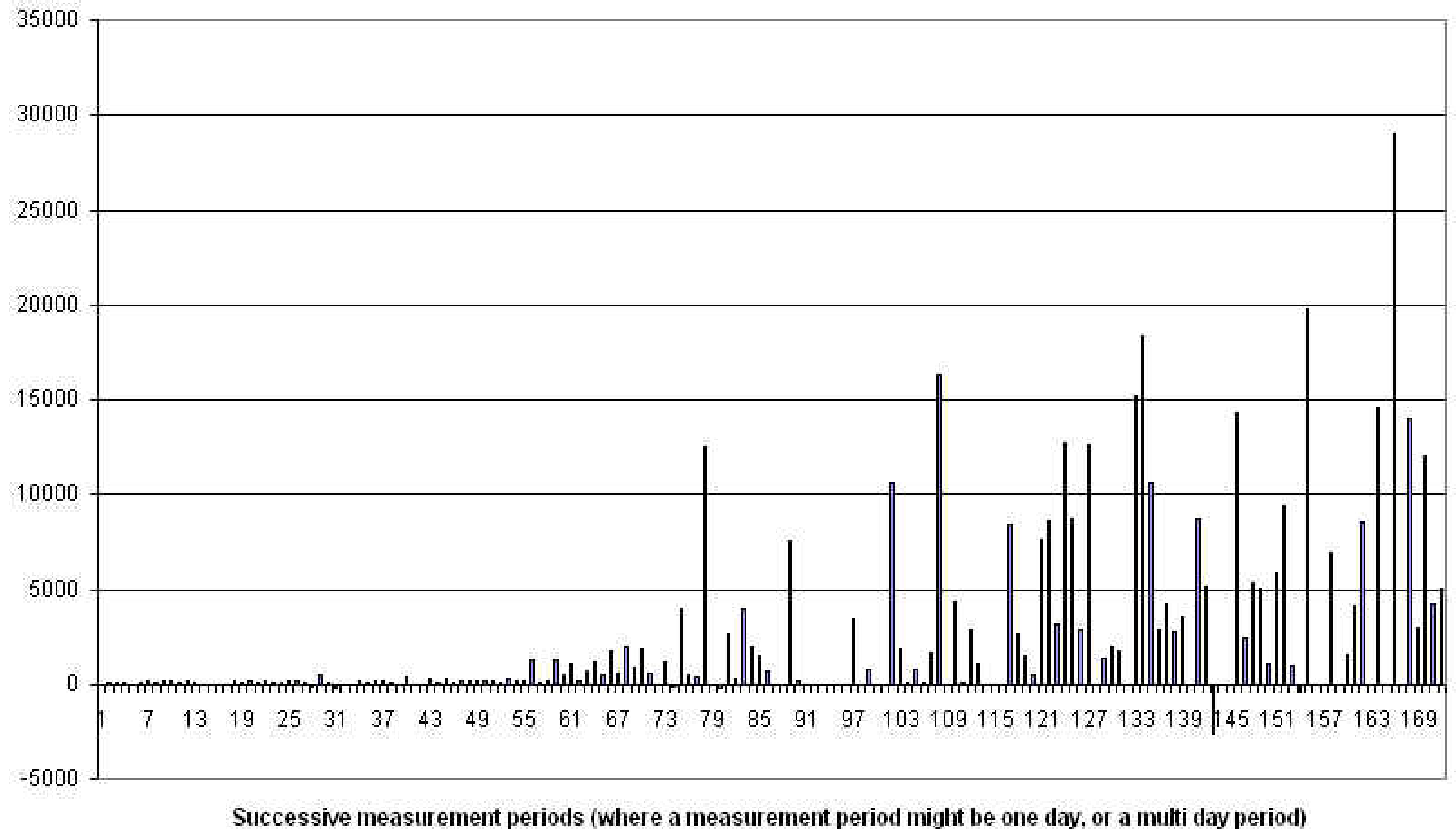
Bounding the immeasurable

- No one can authoritatively tell you the total number of open proxies in existence on the Internet today -- that number is constantly changing, and is fundamentally unknowable without systematically probing all possible proxy server ports on all possible addresses.
- Put another way, while we may know how many we've seen so far, we don't know (yet) how many more open proxies are still out there undetected, ripe for abuse.
- There are, however, some ways we can work towards an estimate of the number of open proxies. For example, some publicly available open proxy lists already run to the hundreds of thousands of unique addresses. Obviously, just from that indicator alone, we know we're talking about an epidemic, not one person with a head cold.

Or we could look at the rate of discovery of new open proxies

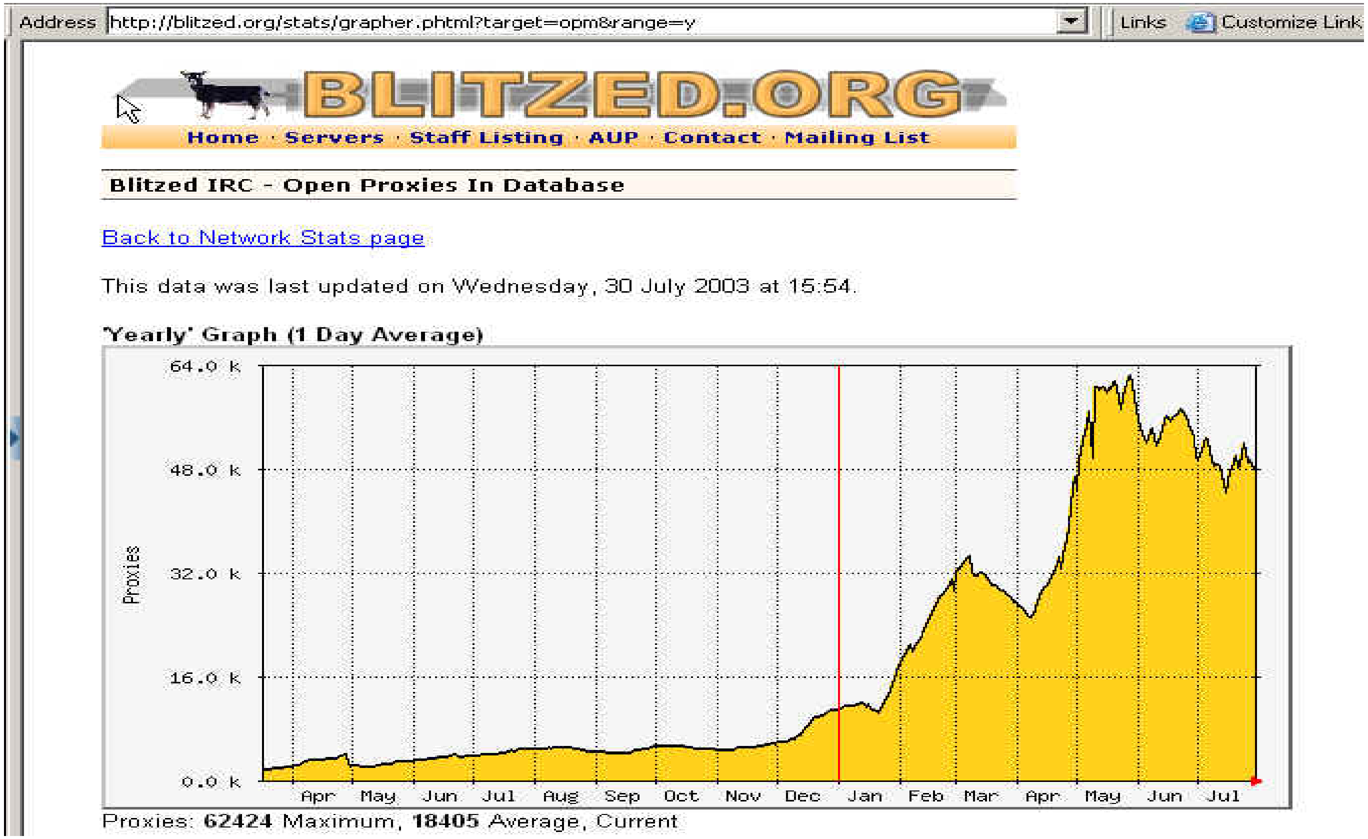
- Let's assume spammers are aggressively looking for new open proxies, and the number of open proxies is constant.
- As spammers begin to have problems finding new one, the number of newly abused open proxies we see per day should decrease, and our estimate of the true number of open proxies should begin to asymptotically approach the true number of open proxies.
- Unfortunately, we're nowhere near asymptotic yet (and the problem may be that spammers are systematically creating new open proxies, rather than working from a limited stable pool of open proxies).

Average new open proxy hosts/day
(total new proxies in this measurement period/number of days in the measurement period)
for each measurement period from March 2002 through July 2003



One (possible) positive sign...

- We have noted one positive sign: the number of open proxy hosts listed by one entity, Blitzed, has actually begun to decline. (This may simply represent a shift from Blitzed to other open proxy DNSBLs, however)



Address http://blitzed.org/stats/grapher.phtml?target=opm&range=y

Links
Customize Link
BLITZED.ORG
Home · Servers · Staff Listing · AUP · Contact · Mailing List

Blitzed IRC - Open Proxies In Database

Back to Network Stats page

This data was last updated on Wednesday, 30 July 2003 at 15:54.

'Yearly' Graph (1 Day Average)

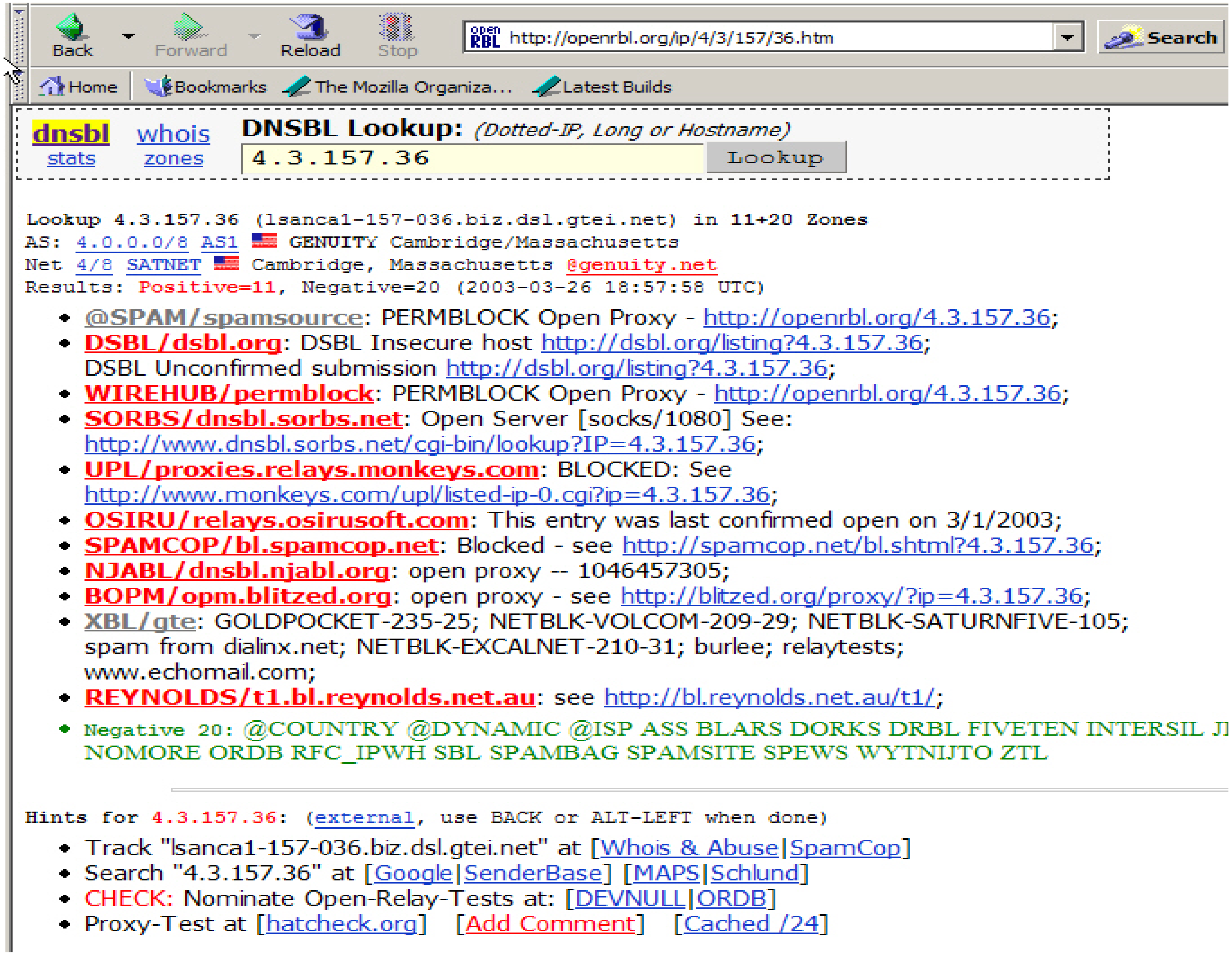
Proxies: **62424** Maximum, **18405** Average, Current

VIII. Sorting the Sheep from the Goats

How do we know if a host is an open proxy server?

- There are five main ways whereby you can determine if a particular IP address is now or has formerly been an open proxy server:
  -- you can check http://openrbl.org/
  -- you can query open proxy DNS blacklists
  -- you can use a fully functional open proxy tester
  -- you can scan the dotted quad in question for common open proxy ports, or
  -- we may be able to watch MRTG graphs and spot characteristic bandwidth usage patterns.

[This is my OpenRBL slide from 3/26/03]



DNSBL Lookup: *(Dotted-IP, Long or Hostname)*

4.3.157.36 Lookup

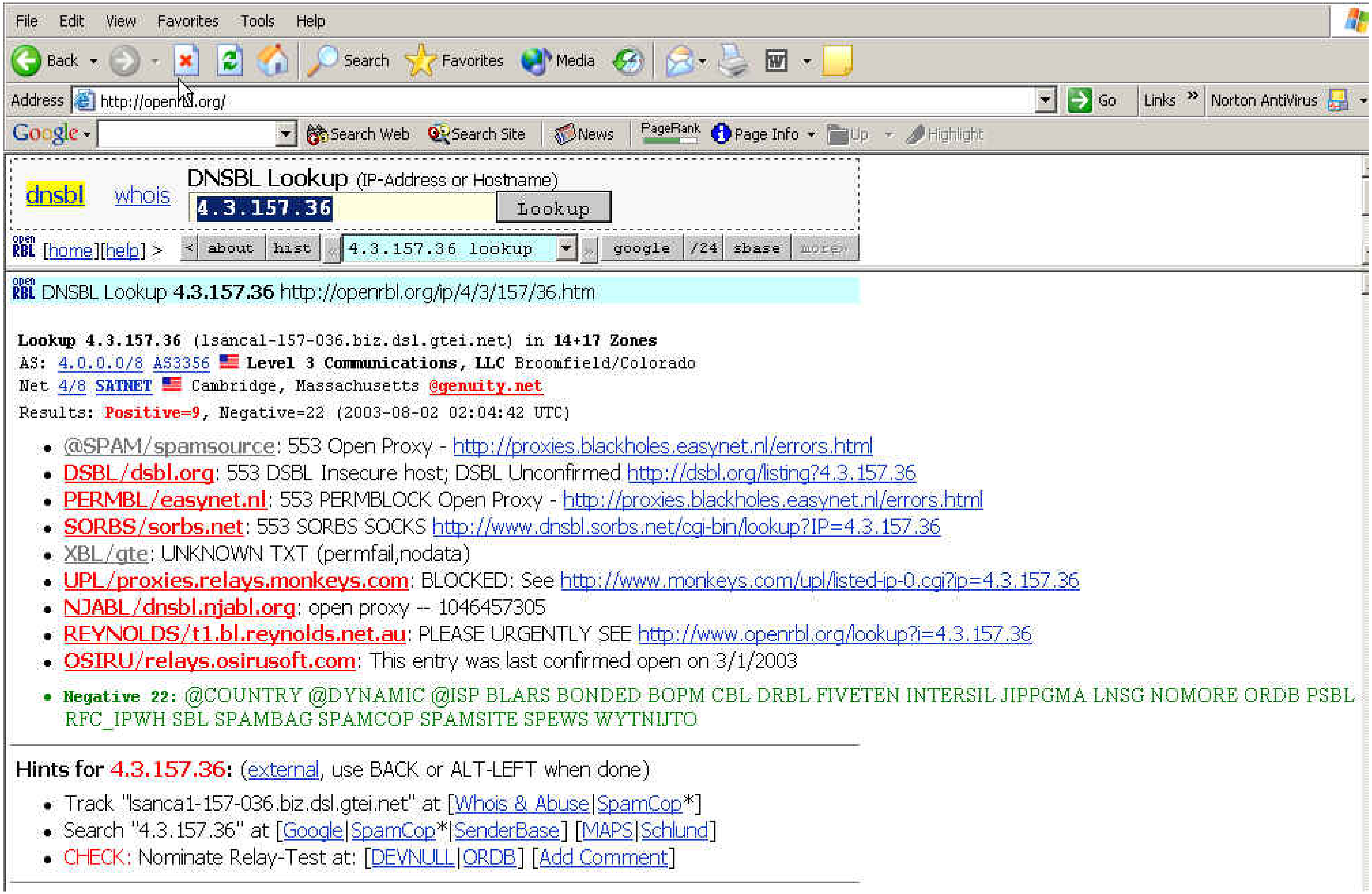
```
Lookup 4.3.157.36 (lsanca1-157-036.biz.dsl.gtei.net) in 11+20 Zones
AS: 4.0.0.0/8 AS1 GENUITY Cambridge/Massachusetts
Net 4/8 SATNET Cambridge, Massachusetts @genuity.net
Results: Positive=11, Negative=20 (2003-03-26 18:57:58 UTC)
```

- @SPAM/spamsource: PERMBLOCK Open Proxy - http://openrbl.org/4.3.157.36;
- DSBL/dsbl.org: DSBL Insecure host http://dsbl.org/listing?4.3.157.36;
  DSBL Unconfirmed submission http://dsbl.org/listing?4.3.157.36;
- WIREHUB/permblock: PERMBLOCK Open Proxy - http://openrbl.org/4.3.157.36;
- SORBS/dnsbl.sorbs.net: Open Server [socks/1080] See: http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=4.3.157.36;
- UPL/proxies.relays.monkeys.com: BLOCKED: See http://www.monkeys.com/upl/listed-ip-0.cgi?ip=4.3.157.36;
- OSIRU/relays.osirusoft.com: This entry was last confirmed open on 3/1/2003;
- SPAMCOP/bl.spamcop.net: Blocked - see http://spamcop.net/bl.shtml?4.3.157.36;
- NJABL/dnsbl.njabl.org: open proxy -- 1046457305;
- BOPM/opm.blitzed.org: open proxy - see http://blitzed.org/proxy/?ip=4.3.157.36;
- XBL/gte: GOLDPOCKET-235-25; NETBLK-VOLCOM-209-29; NETBLK-SATURNFIVE-105; spam from dialinx.net; NETBLK-EXCALNET-210-31; burlee; relaytests; www.echomail.com;
- REYNOLDS/t1.bl.reynolds.net.au: see http://bl.reynolds.net.au/t1/;
- Negative 20: @COUNTRY @DYNAMIC @ISP ASS BLARS DORKS DRBL FIVETEN INTERSIL JI NOMORE ORDB RFC_IPWH SBL SPAMBAG SPAMSITE SPEWS WYTNIJTO ZTL

Hints for 4.3.157.36: (external, use BACK or ALT-LEFT when done)

- Track "lsanca1-157-036.biz.dsl.gtei.net" at [Whois & Abuse|SpamCop]
- Search "4.3.157.36" at [Google|SenderBase] [MAPS|Schlund]
- CHECK: Nominate Open-Relay-Tests at: [DEVNULL|ORDB]
- Proxy-Test at [hatcheck.org] [Add Comment] [Cached /24]

[Same host 4 months later, on 8/1/03…]



DNSBL Lookup (IP-Address or Hostname)

4.3.157.36

open RBL DNSBL Lookup **4.3.157.36** http://openrbl.org/ip/4/3/157/36.htm

Lookup 4.3.157.36 (lsancal-157-036.biz.dsl.gtei.net) **in 14+17 Zones**
AS: 4.0.0.0/8 AS3356 🇺🇸 **Level 3 Communications, LLC** Broomfield/Colorado
Net 4/8 **SATNET** 🇺🇸 Cambridge, Massachusetts **@genuity.net**
Results: **Positive=9**, Negative=22 (2003-08-02 02:04:42 UTC)

- @SPAM/spamsource: 553 Open Proxy - http://proxies.blackholes.easynet.nl/errors.html
- DSBL/dsbl.org: 553 DSBL Insecure host; DSBL Unconfirmed http://dsbl.org/listing?4.3.157.36
- PERMBL/easynet.nl: 553 PERMBLOCK Open Proxy - http://proxies.blackholes.easynet.nl/errors.html
- SORBS/sorbs.net: 553 SORBS SOCKS http://www.dnsbl.sorbs.net/cgi-bin/lookup?IP=4.3.157.36
- XBL/gte: UNKNOWN TXT (permfail,nodata)
- UPL/proxies.relays.monkeys.com: BLOCKED: See http://www.monkeys.com/upl/listed-ip-0.cgi?ip=4.3.157.36
- NJABL/dnsbl.njabl.org: open proxy -- 1046457305
- REYNOLDS/t1.bl.reynolds.net.au: PLEASE URGENTLY SEE http://www.openrbl.org/lookup?i=4.3.157.36
- OSIRU/relays.osirusoft.com: This entry was last confirmed open on 3/1/2003
- **Negative 22:** @COUNTRY @DYNAMIC @ISP BLARS BONDED BOPM CBL DRBL FIVETEN INTERSIL JIPPGMA LNSG NOMORE ORDB PSBL RFC_IPWH SBL SPAMBAG SPAMCOP SPAMSITE SPEWS WYTNIJTO

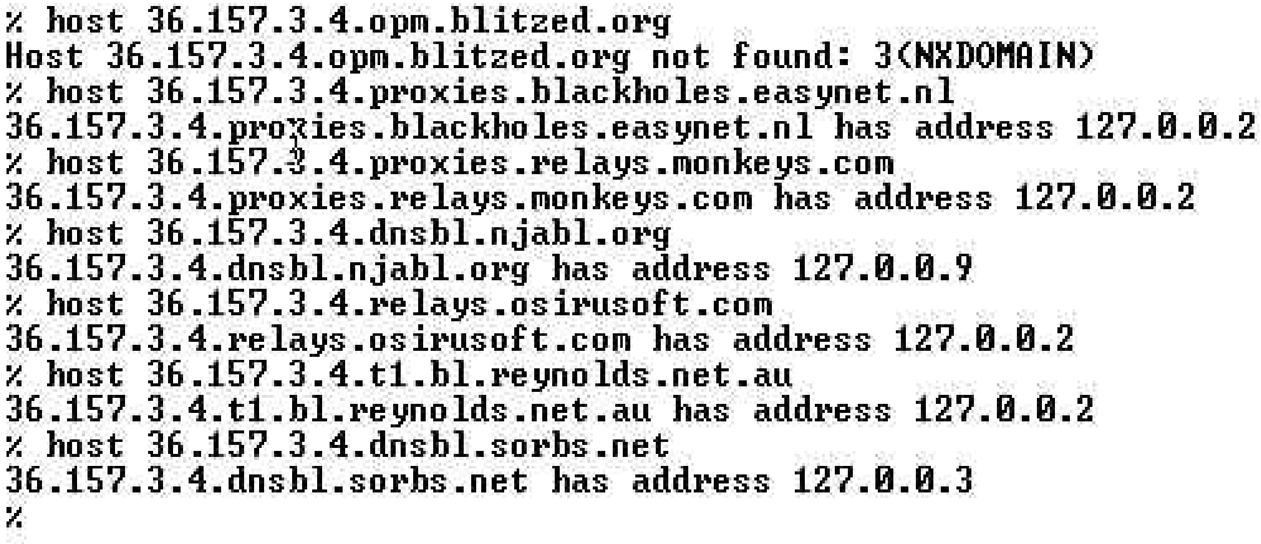
Hints for 4.3.157.36: (external, use BACK or ALT-LEFT when done)

- Track "lsanca1-157-036.biz.dsl.gtei.net" at [Whois & Abuse|SpamCop*]
- Search "4.3.157.36" at [Google|SpamCop*|SenderBase] [MAPS|Schlund]
- CHECK: Nominate Relay-Test at: [DEVNULL|ORDB] [Add Comment]

About OpenRBL

- OpenRBL is a very convenient way for a user to query a comparatively small number of hosts, but it really isn't designed for bulk queries:
  -- it is relatively slow (at least if you need to do tens of thousands of queries)
  -- it only permits a limited number of queries/day
  -- it has anti-scripting functionality built-in
- If you're doing many queries, you'll probably want to do those queries directly.

Querying DNS blacklists



```
% host 36.157.3.4.opm.blitzed.org
Host 36.157.3.4.opm.blitzed.org not found: 3(NXDOMAIN)
% host 36.157.3.4.proxies.blackholes.easynet.nl
36.157.3.4.proxies.blackholes.easynet.nl has address 127.0.0.2
% host 36.157.3.4.proxies.relays.monkeys.com
36.157.3.4.proxies.relays.monkeys.com has address 127.0.0.2
% host 36.157.3.4.dnsbl.njabl.org
36.157.3.4.dnsbl.njabl.org has address 127.0.0.9
% host 36.157.3.4.relays.osirusoft.com
36.157.3.4.relays.osirusoft.com has address 127.0.0.2
% host 36.157.3.4.t1.bl.reynolds.net.au
36.157.3.4.t1.bl.reynolds.net.au has address 127.0.0.2
% host 36.157.3.4.dnsbl.sorbs.net
36.157.3.4.dnsbl.sorbs.net has address 127.0.0.3
%
```

Understanding DNSBLs

- DNS servers are normally just used to translate domain names to numeric IP addresses and vice versa but DNS servers can also be used as an efficient way to convey other info (usually in the form of a "coded" network address from the 127.0.0.0 block), such as whether a network address is known to be an open proxy server.
- For reasons relating to maintenance of the DNSBL listings, DNSBLs usually use reversed IPs.
- Example, to see if the fictitious DNSBL zone badhost.foo.bar has 123.45.6.78 listed, you'd use host (or dig, etc.) to see if 78.6.45.123.badhost.foo.bar was defined.
- DNSBL's are "opaque" -- unless the operator chooses to make a copy of that zone publicly available, one can only tell if an entry is defined by testing checking that address.

Some notes on DNS blacklists

- (1) Open proxies exist which aren't in any blacklists (duh); conversely some listed dotted quads may no longer be open proxies
(2) Some DNSBLs list open proxies AND open relays AND spam-tolerant hosts AND virus-infested hosts AND… pay close attention to the addresses each DNSBL returns if you only care about open proxies.
(3) Some DNSBLs may have restrictive terms and conditions that are trivial to accidentally violate. I would urge you to respect those terms and conditions, and simply avoid DNSBLs with restrictive T&C's -- there are others w/o tight T&C's.
(4) Because DNSBLs are remote databases delivered via DNS, recognize that DNS queries *may* sometimes fail (e.g., if all servers delivering DNSBL 'foo' are offline).

Some notes on DNS blacklists (2)

- (5) If you do lots of DNSBL queries, your local name server infrastructure may suddenly become even more important than normal to you, and may need watching to avoid performance issues.
  [Note to self: *time for DNS server benchmarking work?*]
  [Second note to self: *after looking at open proxies problem, is it time to look at open recursive DNS servers?*]
  (6) It is (sort of) trivial to locally automate DNS queries of open proxy DNSBLs using shell scripts or small utility programs. Forget about trying to manually check DNSBLs for open proxy listings -- you really MUST automate this process due to the transaction volume. Also note that you are (potentially) talking about a LOT of DNS queries, so be sure to automate <u>intelligently</u>.

And of course...

- If you decide to automatically block email traffic from open proxies, you WILL end up using a DNSBL since that's basically the only scalable approach. :-)
- A nice introduction to using DNSBL's with sendmail is available at http://mail-abuse.org/rbl/usage.html

Active open proxy testers

- Note: actively checking dotted quads for open proxy servers may not be appreciated, and depending on your jurisdiction may (or may not) be legal, particularly if those systems or the network they are on isn’t yours.
- Assuming you did want to test some systems on your own network, some sites offering either proxy testing software or a proxy testing service include:
  -- http://www.corpit.ru/mjt/proxycheck.html
  -- http://www.unicom.com/sw/pxytest/
  -- http://www.helllabs.com.ua/labs.php?group=products&
  page=1&lang=en_
  -- http://www.send-safe.com/scanner.php
- Caution: some active open proxy testing software/sites reserve the right to use any information about any proxies found for their own purposes.

Sometimes black is white (or grey, or red, or …)

- DNSBL tests may not be consistent with the results of fully functional active open proxy tests.
- It can be disturbing to find that doing a fully functional test of a dotted quad listed in a DNSBL sometimes doesn't result in consistent results... After all, they should agree.
- Some possible sources of inconsistency between DNSBL's and active open proxy testers include
  1) a formerly open proxy may truly no longer be open, but no one has bothered to delist that dotted quad from all the various DNSBLs that are out there.
  2) the open proxy may still be open, but may only be intermittently available (e.g., an open proxy running on a desktop that is only powered up 8-5 local time).

More sources of inconsistency

- 3) The fully functional open proxy tester may be getting firewalled by the open proxy operator or their, even though the open proxy itself may still accessible from other locations on the Internet.
  4) The open proxy may be running on an uncommon port, or may be periodically changing the port(s) it is using to hinder detection (or to evade upstream filtering of common open proxy ports by the ISP).
  5) The open proxy may only be open for a limited range of services (e.g., web browsing, but not SMTP traffic transmission, for example), and the proxy tester might be checking the proxy only for some service it doesn't offer (like SMTP).

More sources of inconsistency (2)

- 6) The open proxy server may have been running on a dynamically allocated address, and its lease may have expired (allowing that address to be recycled for use by some other innocent/secure host).
  7) The network connecting an actively abused open proxy server may be completely saturated, resulting in TCP timeouts or other odd errors.
  8) Proxy servers may accept incoming connections on one address and create outgoing connections on a completely different address. Testing an output ("apparent source") interface rather than an input interface may result in incorrect inferences being made.

More sources of inconsistency (3)

- 9) The putative open proxy may NEVER have been truly open, although it may have exhibited suspicious behaviors (e.g., it may have open ports on numbers strongly associated with open proxies, e.g., 1080 or 6588, etc.).
  10) A host may have been maliciously nominated as an act of retribution (a so-called "Joe-job"), etc.
  [Most DNSBL's require evidence and validate user submissions, but there are exceptions; know your BL's listing criteria!]

Scanning via NMAP or specialized proxy discovery tools

- Administrators may use a general purpose scanning tool such as NMAP (http://www.insecure.org/nmap/) to identify potential open proxies; there are also specialized proxy detection and analysis tools in widespread circulation such as Proxy Hunter, Proxy Sniper, etc. (see: http://www.proxys4all.com/tools.shtml)
- If using NMAP to scan for proxies, you should know that some proxies may be running on well known ports such as 80 (http) or 443 (https). Common proxy ports are typically:
  -- SOCKS 4/5: 1080
  -- HTTP: 3128, 8080, 6588, 80, 81, 4480
  -- Wingate: 23
  -- Peekabooty/Triangleboy/etc.: 443
- But of course, a proxy server can potentially be bound to any random TCP port.

And speaking of scanning...

- Let me reiterate that scanning someone else's host(s) or someone else's network(s) without their permission may be/is unlawful (at least in some jurisdictions) and is not recommended (although we empirically know it is a common practice).
- This leads to the open proxy delisting paradox: "If one believes a host to be an open proxy, how is one to learn that that host is no longer an open proxy if the owner doesn't know of your belief (and thus can’t set you straight) and active scans to check the status of that host are unlawful?"

Manually testing a connect mode open proxy

- Telnet to the open proxy port then enter:

```
CONNECT foo.bar.baz:25 HTTP/1.0
<return>
<return>
```

If you see `200 Connected` you know that you've found an open proxy that's willing to channel SMTP traffic to server `foo.bar.baz`

MRTG as an open proxy spotting tool

- Yet another way of spotting a *possible* open proxy server is by watching traffic graphs for individual switch ports where outgoing traffic closely mirrors incoming traffic.
- This technique is mentioned (and nicely illustrated) at: http://www.rsc-london.ac.uk/technical/network/monitoring/ (see the “spotting open proxy servers” section)

Or you can just wait for the complaints to pour in...

- The final way to identify open proxies on your own network is to do nothing, and simply wait for the complaints to come pouring in.
- **At a minimum EVERY DOMAIN should have a monitored abuse@<domain> address!** See RFC 2142 at section 4!
- http://www.abuse.net/
  http://www.rfc-ignorant.org/

IX. Our Open Proxy List

The use-it-and-lose-it paradox

- One of the most delightful things about spammers using open proxies is that when a spammer sends spam through an open proxy, that act advertises the existence of that open proxy, thereby facilitating its closure.
- Thus, whenever we'd see a logged "hit" on one or more of the open proxy DNS blacklists, or receive email from what was obviously a new open proxy spamming us directly, we'd add an entry for that host to:
  http://darkwing.uoregon.edu/~joe/
  open-proxies-used-to-send-spam.html

  Caution: this is now a large file (41+MB, >600K lines). wget is your friend. Compressed versions are available.

Tracking open proxies

- We began building that list in September 2002, systematically looking at all IP addresses associated with spam which slipped through our filters and which were reported to us, as well as at the IP addresses of all mail which had been rejected by filtering rulesets running on our shared systems. [You *could* just scrutinize ALL SMTP relay addresses seen in your SMTP server logs, but you'll waste a lot of time and do a lot of pointless queries.]
- More recently, we've also begun listing open proxies brought to our attention from public sources (provided that at least one of the open proxy DNSBLs we use lists that dotted quad).

You won't notice open proxies if you're drowning in other spam...

- Key point: if you're interested in identifying open proxies via their appearance in spam, as we were, the first step is to carve off all the *other* sources of spam, e.g., direct-from-dialup spam, spam sent via open SMTP relays, spam sent via vulnerable formmail cgi's, spam sent from so-called "bulletproof“ dedicated spam houses, etc.
- While there are many ways of blocking spam with DNSBLs, one combination that works fairly well is the mail-abuse.org RBL+ (not free, but quite affordable in zone transfer mode for universities, and now it even includes a open proxy servers via the mail-abuse.org OPS), plus the free SBL from spamhaus.org. That combo will kill most spam (although you may still want to add some local blocks, or augment those DNSBLs with additional ones).

Pointers to some popular open proxy DNSBLs also worth consideration

- Blitzed: http://www.blitzed.org/bopm/
- Easynet (formerly Wirehub):
  http://abuse.easynet.nl/proxies.html
  I’m a particularly big fan of the Easynet open proxy list…
- Mail-abuse.org OPS:
  http://www3.mail-abuse.org/ops/index.html
- NJABL: http://njabl.org/
- Osirusoft: http://relays.osirusoft.com/faq.html
- SORBS: http://www.dnsbl.sorbs.net/using.html
- … and there are others.

The format of my open proxy listing

- Anyhow… the entries that make up the core of my open-proxies-used-to-send-spam file look like:

```
[snip]
63.206.136.141 (06/02/2003) [adsl-63-206-136-141.dsl.lsan03.pacbell.net] ----WN
63.206.136.195 (04/27/2003) [adsl-63-206-136-195.dsl.lsan03.pacbell.net] ----W-
63.206.136.221 (06/12/2003) [adsl-63-206-136-221.dsl.lsan03.pacbell.net] --OSWN
63.206.137.79 (06/13/2003) [adsl-63-206-137-79.dsl.lsan03.pacbell.net] ---SWN
63.206.137.116 (05/26/2003) [adsl-63-206-137-116.dsl.lsan03.pacbell.net] -----N
63.206.137.154 (06/02/2003) [adsl-63-206-137-154.dsl.lsan03.pacbell.net] ----WN
63.206.137.155 (06/29/2003) [adsl-63-206-137-155.dsl.lsan03.pacbell.net] ---SWN
63.206.137.196 (04/18/2003) [adsl-63-206-137-196.dsl.lsan03.pacbell.net] B--SWN
63.206.137.211 (05/15/2003) [adsl-63-206-137-211.dsl.lsan03.pacbell.net] -----N
63.206.137.222 (05/27/2003) [adsl-63-206-137-222.dsl.lsan03.pacbell.net] ----WN
63.206.137.229 (02/25/2003) [adsl-63-206-137-229.dsl.lsan03.pacbell.net] –OSW
[snip]
```

Format of the open proxy list (2)

- Entries are maintained in numeric order by dotted quad, one entry per line.
- Each line shows the dotted quad in question, the date the various DNSBLs were checked for that address, the hostname associated with the dotted quad (or "no reverse DNS" if applicable), and a mask showing which open proxy DNSBLs listed the address at the time it was checked/listed (and possibly information about the ports the proxy used)

Coding of DNSBL proxy entries

- The three to six character mask at the end of each entry is encoded using the scheme:

B	opm.**b**litzed.org
-	[used to show a now-omitted DNSBL]
O	relays.**o**sirusoft.com (127.0.0.9)
S	dnsbl.**s**orbs.net (127.0.0.2, 127.0.0.3, and 127.0.0.4)
W	Easynet.nl (the W stands for this DNSBL’s old domain, Wirehub)
N	dnsbl.**n**jabl.org (127.0.0.9)

- When a host isn't listed on a given DNSBL, a dash is entered as a placeholder

"Wait a minute! By publishing that kind of list, you're just making the problem worse!"

- No. There are already plenty of open proxy lists in existence, and those lists routinely include information (such as port numbers) that amateur/bulk proxy abusers want. My list *only* includes port numbers in limited circumstances (for example, when I'm documenting a proxy that isn't otherwise listed on a DNSBL we use, or I've personally received spam via that proxy).
- Moreover, hardcore proxy abusers don't use hosts from public lists... Known open proxies tend to be blocked/saturated/slow, so professional open proxy abusers scan for their own "fresh" proxies, buy private lists of open proxies from scanning specialists, or trade open proxies among themselves. (For some sense of that activity, search for proxies in groups.yahoo.com or groups.msn.com)

Don't shoot the messenger

- The first step to fixing any problem is dragging it out from the shadows into the light of day. If you refuse to talk about a problem, it will never get fixed. The open proxy problem NEEDS to get fixed.
- Unless you can document and detail a problem, many ISPs are unwilling to take action to fix that problem.
- People need to see the full extent of the problem to appreciate the need for large scale corrective action.
- Besides, *anyone* who gets spammed and has access to sendmail logs, web server logs, firewall logs, etc. could build a similar list; I'm not doing something magic here…
- On the other hand, we do know that our list gets retrieved LOTS of times every day, sometimes via open proxies (which we often dutifully add to the list). :-)

What domains are seen most often on the open proxy list as of 8/2003?

```
• 191158 32.9% non-resolvable-IP-addr
   25536  4.4% telesp.net.br
   22962  4.0% prodigy.net.mx
   20604  3.6% veloxzone.com.br
   12840  2.2% wanadoo.fr
   11927  2.1% rr.com
   10487  1.8% telecom.net.ar
   10140  1.7% swbell.net
    9667  1.7% pacbell.net
    8696  1.5% interbusiness.it
    8427  1.5% brasiltelecom.net.br
    7971  1.4% hinet.net
    7959  1.4% dsl-verizon.net
```

What domains are seen most often on the open proxy list as of 8/2003? (2)

-
  ```
  7572 1.3% attbi.com
  7129 1.2% ameritech.net
  6526 1.1% speedy.com.ar
  5919 1.0% rima-tde.net
  5697 1.0% comcast.net
  4731 0.8% bellsouth.net
  4432 0.8% btopenworld.com
  3874 0.7% ntl.com
  3650 0.6% prima.net.ar
  3354 0.6% skynet.be
  3194 0.6% vtr.net
  3005 0.5% adelphia.net
  ```

What domains are seen most often on the open proxy list as of 8/2003? (3)

```
• 2970 0.5% carter.com
  2536 0.4% bezeqint.net
  2487 0.4% videotron.ca
  2472 0.4% terra.cl
  2285 0.4% rogers.com
  2259 0.4% speedyterra.com.br
  2256 0.4% sympatico.ca
  2191 0.4% tpnet.pl
  2112 0.4% telepar.net.br
  2046 0.4% bigpond.net.au
  1976 0.3% telekom.at
  1864 0.3% blueyonder.co.uk
```

What domains are seen most often on the open proxy list as of 8/2003? (4)

-
  ```
  1817 0.3% tele.dk
  1810 0.3% 012.net.il
  1760 0.3% club-internet.fr
  1742 0.3% ono.com
  1720 0.3% virtua.com.br
  1672 0.3% t-dialin.net
  1657 0.3% t-net.net.ve
  1639 0.3% hispeed.ch
  1595 0.3% seed.net.tw
  1584 0.3% shawcable.net
  1539 0.3% cox.net
  1460 0.3% proxad.net
  ```

What domains are seen most often on the open proxy list as of 8/2003? (5)

```
• 1459 0.3% netvision.net.il
  1417 0.2% menta.net
  1415 0.2% ethome.net.tw
  1374 0.2% bbtec.net
  1343 0.2% noos.fr
  1331 0.2% wanadoo.nl
  1247 0.2% hansenet.de
  1169 0.2% hkcable.com.hk
  1127 0.2% papalegua.com.br
  1106 0.2% telia.com
  1102 0.2% verizon.net
  1049 0.2% metropolis-inter.com
```

What domains are seen most often on the open proxy list as of 8/2003? (6)

```
• 1048 0.2% fibertel.com.ar
  1025 0.2% mindspring.com
   988 0.2% anteldata.net.uy
   983 0.2% optonline.net
   971 0.2% brdterra.com.br
   923 0.2% chello.nl
   892 0.2% arcor-ip.net

  [all others contributed less than 0.2%]
```

The no reverse DNS folks

- The same people who can't securely configure their proxies obviously also don't give a damn about PTR records. :-)
- In some cases, the lack of reverse DNS may be due to domain names not being "relevant" (e.g., at sites that use non-roman languages), but some other ISPs may *intentionally* not provide a reverse address in an effort to reduce the number of complaints they receive... That's okay, we 'll soon be mapping those dotted quads to ASNs.
- We also are beginning to look at doing timing of reverse DNS lookups; we believe some ISPs are exhibiting anomalous delays when returning results for DNS queries, and those delays should be identified and documented.

Too big to block?

- If you meditate on the country code distribution shown in that list, you can see why some use country-wide blocks, even if they do inflict lots of collateral damage.
- There are some folks on that list who should (and do) know better than to ignore open proxies on their network. They may have apparently come to believe "we're too big to get blocked," or "we don't want to cut off *any* paying customer, even if they are insecure -- we'll just ignore the complaints.“ I wouldn’t count on it.

Fast connections (except from higher education) are beloved

- Clearly, there is an association between connection speed and open proxy presence; fast connections are more likely to be trying to do connection sharing, and because those connections are fast, they tend to be attractive to abusers.
- For the most part, higher education sites do NOT tend to show up much, which is excellent news (and contrary to some commonly articulated popular perceptions).

And yes, some open proxies <u>have</u> been listed "forever"

- It is absolutely true that there are some proxies on the list that have been listed for a REALLY long time, e.g., since Autumn 2002 in some cases.
- What can I say? Some people simply may not care if they have an open proxy; in other cases, the proxies may be secured, but the system owner may not know how to get off a DNSBL we use, or may not care to bother.

Taking entries <u>off</u> the list

- Periodically we recheck the blacklists for all the entries on our list and remove the dotted quads that are no longer listed on any of the five used.
- Retesting can become, um, tricky, when you're talking about doing millions of queries (>600K hosts X n DNSBLs).
- It currently takes roughly half a day to do half a million retests… yes, we could make the rechecks faster/more aggressive, but we need to be careful of our impact on DNS servers...

X. "What Can I Do?"

Chip in...

- The most important step, if you see spam from an open proxy that isn't already listed at sites such as OpenRBL, is to report it. Open proxy DNSBL's develop better coverage and work better for all of us as more people use and contribute to them.
- One of the best ways to report spam you may receive is via http://spamcop.net/
- If you use the mail-abuse.org RBL+, you should consider submitting open proxies to the mail-abuse.org OPS (see http://www3.mail-abuse.org/ops/submit.html)
- Be sure to also train your end users how to report spam which they may receive!

Make sure you aren't part of the problem...

- If you run a proxy server, review your config and your log files for problems.
- If you are responsible for your campus' network, make sure it isn't infested with open proxy servers.
- Review your acceptable use policy to insure that you've disallowed open proxy servers, either by name, or via general prohibitions on "unauthorized resource sharing"
- Make sure you've got an abuse@ address, and mail to it gets read and acted on.

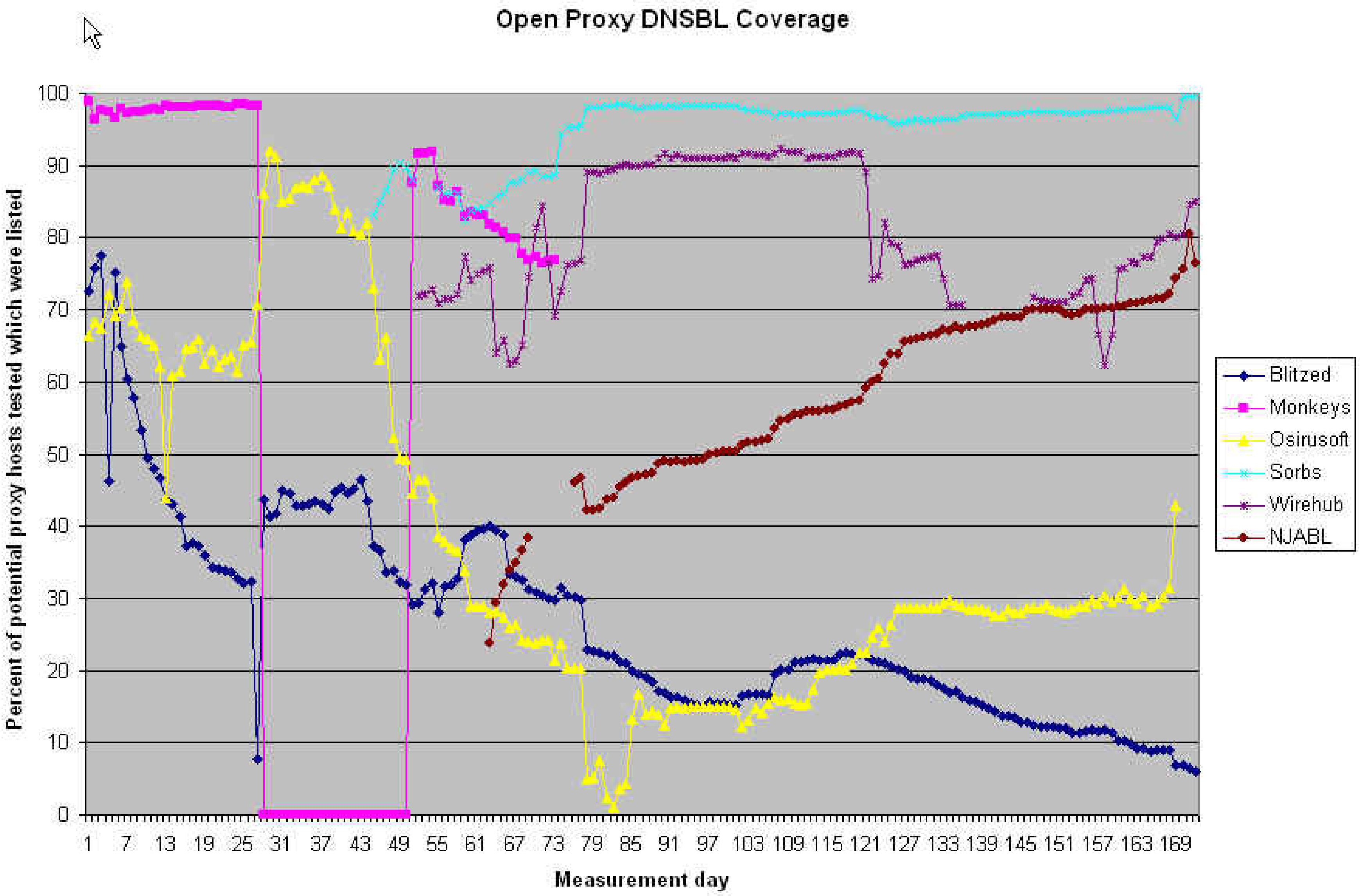
Protect your own mail servers

- Use an open proxy DNSBL to protect your own mail servers, just as you may already reject mail from open SMTP relays. Blocking traffic from open proxies is a basic step that a growing number of major ISPs are already doing. For example:

  -- http://postmaster.info.aol.com/ops.html
  -- http://security.rr.com/mail_blocks.htm
  -- http://help.yahoo.com/help/us/mail/defer/defer-02.html

Which of the open proxy DNSBLS is "best?"

- There are many factors to consider when evaluating an open proxy DNSBL:
  -- you're trusting the operator of the DNSBL with ability to "break" delivery of mail to users of your system; does the DNSBL operator appear to deserve that trust?
  -- does the DNSBL appear to be good at listing all or most open proxies, or do they only list a small number of IPs?
  -- can the DNSBL be downloaded to a local nameserver? (this can greatly improve performance and reliability)
  -- do cleaned up hosts get delisted
  -- is there a fee for use of the DNSBL?
  -- are there terms and conditions associated with use of the DNSBL?


Open Proxy DNSBL Coverage
Percent of potential proxy hosts tested which were listed
Measurement day
100
90
80
70
60
50
40
30
20
10
0
1
7
13
19
25
31
37
43
49
55
61
67
73
79
85
91
97
103
109
115
121
127
133
139
145
151
157
163
169
Blitzed
Monkeys
Osirusoft
Sorbs
Wirehub
NJABL

Educate downstream partners, the carriers you work with, and even the media…

- Some I2 sites/state networks are already aware of the open proxy issue, and are doing a good job getting the word out to their downstream partners. For example, see: http://www.more.net/security/advisories/2002/020304.html
- If you buy transit bandwidth, don't miss that opportunity to beat the drum about the problem of open proxies. Carriers are NEVER more receptive to your feedback than when they're trying to make a sale. Insist that they describe the steps they take to deal with open proxy abuse (and spam in general), before you sign that P.O.
- Even the media has become interested in open proxies; see: www.nytimes.com/2003/05/20/technology/20SPAM.html Be polite if a reporter calls with network questions. :-)

And get involved with your state legislature…

- You may also want to become involved at the state level in promoting anti-spam laws which address open proxy server abuse.
- Thirty five states have some sort of anti-spam law at this point -- how about yours? (see http://spamlaws.com/)
- If you don't have one, work with your state Attorney General's office to get one passed, or volunteer to provide technical assistance.

Acknowledgments

- While I am solely responsible for the content and opinions expressed in this document, I would like to thank a number of people who have provided invaluable support and/or technical assistance on this project, including Joanne Hugi, my boss and the Associate VP for Information Service; Steve VanDevender and Bob Jones of the Computing Center Systems group; Jon Miyake, Computing Center Acceptable Use Officer (and Perl expert); the whole Computing Center Network Services DNS crew (particularly John Kemp and Jason Edmiston); all the people who offer DNSBLs or other antispam tools to the net; and my family, which has patiently put up with my latest obsession.

And thank you!

- Thanks for your patience with this long talk so late in the day.
- Questions?