

CS 161: Computer Security

Prof. Vern Paxson

**TAs: Devdatta Akhawe, Mobin Javed
& Matthias Vallentin**

<http://inst.eecs.berkeley.edu/~cs161/>

January 18, 2011

How Expensive is the Learning?

- Absorb material presented in lectures and section
- ~3 course projects (30% total)
 - Done individually or in small groups
- ~4 homeworks (20% total)
 - Done individually
- One midterm (20%)
 - 80 minutes long: Tue Mar 8, location TBD
- A comprehensive final exam (30%)
 - Thu May 12 8AM-11AM

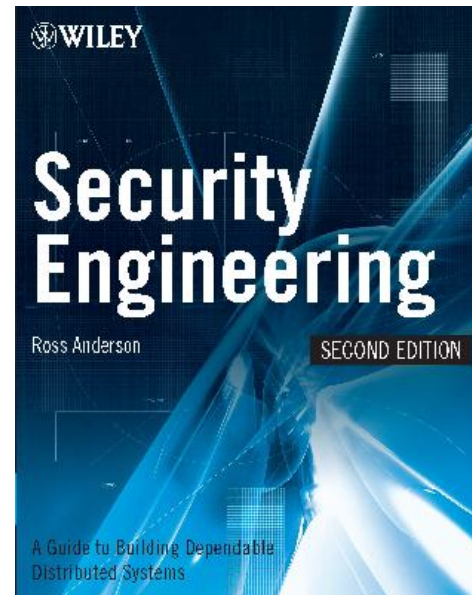
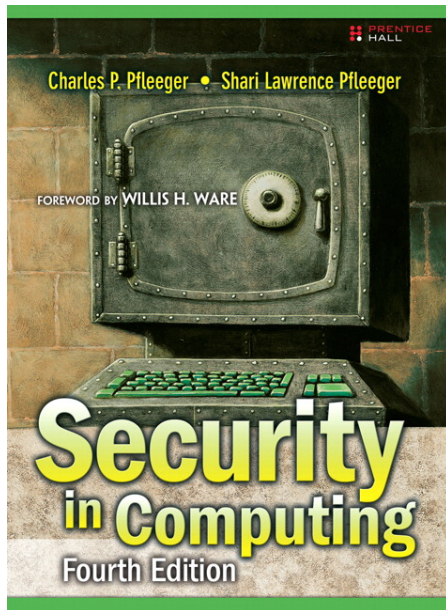
What's Required?

- Prerequisites:
 - Math 55 or CS 70, CS 61B and 61C (= Java + C)
 - Concurrent CS 70 only if ok w/ math & some extra work
 - Familiarity with Unix
- Engage!
 - In lectures, in section
 - Note: I'm **hearing-impaired**, so be prepared to repeat questions!
 - Feedback to us is highly valuable; anonymous is fine
- Class accounts - pick up in section **tomorrow**
- Participate in *Piazza*
 - Send course-related questions/comments there, or ask in Prof/TA office hours
 - For private matters, contact Prof or TA via email

What's Not Required?

- *Optional* book #1: *Security in Computing*, Pfleeger & Pfleeger, 4th ed.
- *Optional* book #2: *Security Engineering*, Anderson, 1st or 2nd ed.

<http://www.cl.cam.ac.uk/~rja14/book.html>



Class Policies

- Late homework: **no credit**
- Late project: **-10%** if < 24 hrs, **-20%** < 48 hrs, **-40%** < 72 hrs, **no credit** ≥ 72 hrs
- Original work, citing sources: **mandatory**
- Working in teams: **only as assignment states**
- If lecture materials are made available prior to lecture, *don't use them to answer questions* asked during class
- Will the class size increase?
 - Unfortunately, no. We're at the limit that our resources can effectively support.

Ethics & Legality

- We will be discussing (and launching!) **attacks** - many quite nasty - and powerful eavesdropping technology
- None of this is in *any way* an invitation to undertake these in any fashion **other than with informed consent** of **all** involved parties
 - The existence of a security hole is no excuse
- These concerns regard not only ethics but UCB policy and California/United States law
- If in some context there's any question in your mind, **talk with instructors first**

Some Broad Perspectives

- A vital, easily overlooked facet of security is *policy* (and accompanying it: operating within *constraints*)
- High-level goal is *risk management*, not bulletproof protection.
 - Much of the effort concerns *raising the bar* and *trading off resources*
 - How to prudently spend your time & money?
- Key notion of *threat model*: what you are defending against
 - This can differ from what you'd expect
 - Consider the Department of Energy ...

Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...

New Unique Samples Added to AV-Test.org's Malware Collection

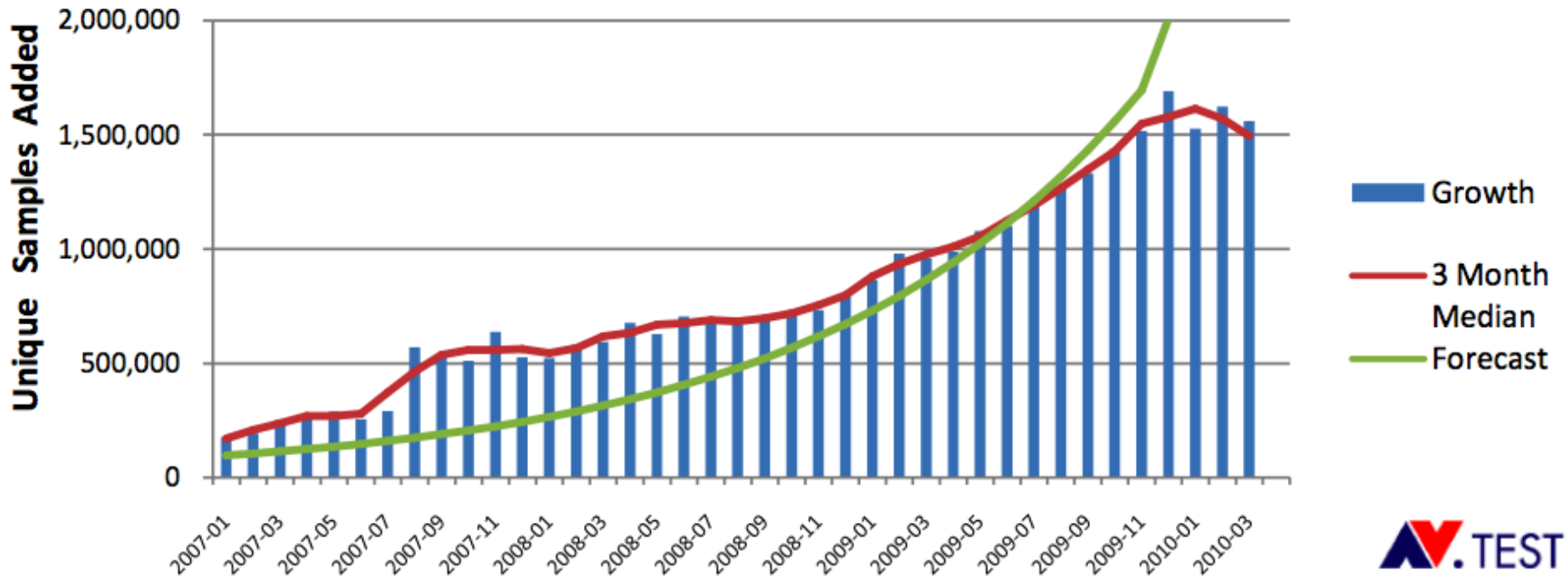
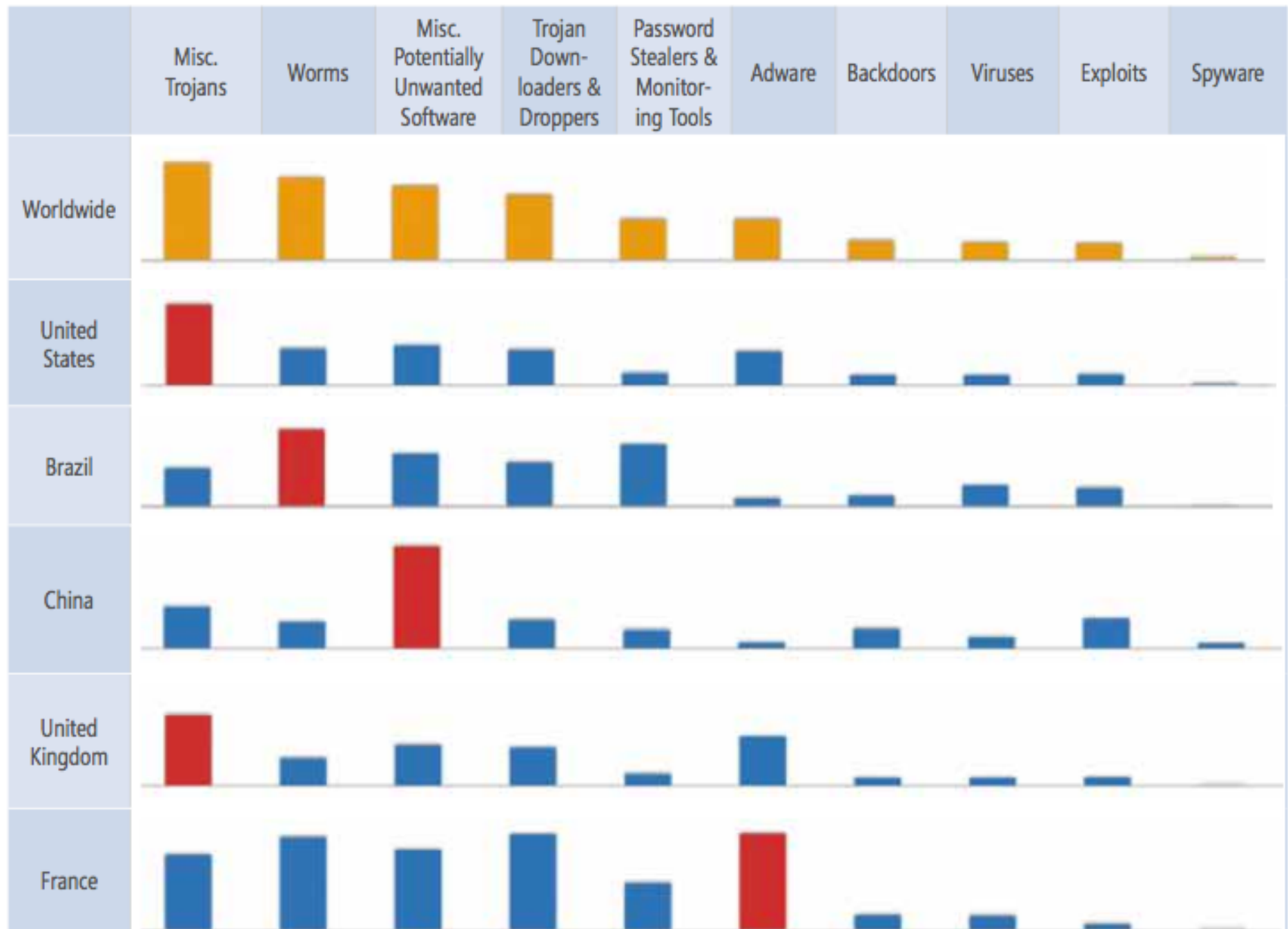


FIGURE 37. The locations with the most computers cleaned by Microsoft desktop anti-malware products in 1Q10 and 2Q10

Rank	Country/Region	Computers Cleaned (1Q10)	Computers Cleaned (2Q10)	Change
1	United States	11,025,811	9,609,215	-12.8% ▼
2	Brazil	2,026,578	2,354,709	16.2% ▲
3	China	2,168,810	1,943,154	-10.4% ▼
4	France	1,943,841	1,510,857	-22.3% ▼
5	Spain	1,358,584	1,348,683	-0.7% ▼
6	United Kingdom	1,490,594	1,285,570	-13.8% ▼
7	Korea	962,624	1,015,173	5.5% ▲
8	Germany	949,625	925,332	-2.6% ▼
9	Italy	836,593	794,099	-5.1% ▼
10	Russia	700,685	783,210	11.8% ▲
11	Mexico	768,646	764,060	-0.6% ▼

FIGURE 42. The top five countries/regions and their relative infection rates in 2Q10, by category



Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ... (not just MS)

iPhone, Safari, IE8, Firefox all fall on day one of Pwn2Own

'Technically impressive' exploit of IE8 bypasses DEP, ASLR on Windows 7 at hacking contest

By Gregg Keizer

March 24, 2010 08:42 PM ET

 Comments (28)  Recommended (8)  Digg  Twitter  Share/Email

Computerworld - Hackers took down [Apple's](#) iPhone and Safari browser, [Microsoft's](#) Internet Explore 8 (IE8) and Mozilla's Firefox within minutes at today's Pwn2Own contest, as expected.

The two-man team of Vincenzo Iozzo and Ralf-Philipp Weinmann exploited the iPhone in under five minutes, said a spokeswoman for 3Com TippingPoint, the [security](#) company that sponsored the contest. The pair also walked away with \$15,000 in cash, a record prize for the challenge, which is in its fourth year.

Iozzo, an Italian college student, works for Zynamics GmbH, the company headed by noted researcher Thomas Dullien, better known as Halvar Flake, while Weinmann is a post-doctoral researcher at the

Laboratory of Algorithms, Cryptology and Security at the University of Luxembourg.

Weinmann is probably best known for being part of a three-man team that in 2007 demonstrated how to [crack the Wi-Fi security protocol WEP](#) much faster than previously thought possible.

Charlie Miller, an analyst at Baltimore-based Independent Security Evaluators, brought down Safari on a MacBook Pro running [Snow Leopard](#) for a three-peat at Pwn2Own.

Miller won prizes in both 2008 and 2009 by hacking a Mac; last year, Miller cracked Safari in [just 10 seconds](#). For his work today, Miller walked off with the notebook and \$10,000 in cash.

No one else has won at Pwn2Own three

times.

When his turn came, Pwn2Own newcomer Peter Vreugdenhil successfully exploited a [vulnerability](#) in IE8 running on [Windows 7](#) with attack code called "technically impressive" by TippingPoint because it bypassed the operating system's Data Execution Prevention, or DEP,

More

Pwn2Own 2010

[Pwn2Own winner tells Apple, Microsoft to find their own bugs](#)

[Hacker busts IE8 on Windows 7 in 2 minutes](#)

[iPhone, Safari, IE8, Firefox all fall on day one of Pwn2Own](#)

[iPhone falls in Pwn2Own hacking contest](#)

[Former winners defend titles at Pwn2Own hacking contest](#)

[Hackers at Pwn2Own to compete for \\$100K in prizes](#)


[More in Security](#) ▶

White Papers & Webcasts

LIVE WEBCAST: Is Virtualization Compromising Your Data Protection?

LIVE Mar 30, 2010 02:00 PM ET

DDoS Mitigation: Best Practices for a Rapidly Changing Threat Landscape

This white paper identifies a set of best practices identify VeriSign that enables organizations to keep pace with C attacks while minimizing... 

Best Practices for Log Monitoring

Watch Now!


The Tangled Web: Silent Threats & Invisible Enemies

Download Now 

Hosted Security Services: Why it make budget and security sense in today's economy

Watch Now

Can Heuristic Technology Help Your Company Fight Viruses?

What is Heuristic Technology and how can it help safeguard your business against viruses? Learn more. 

Stacking Up Against the Competition - Actuate BIRT \ Business Objects, Cognos, Microstrategy, Jaspersoft Pentaho

Energizer Battery Charger Software Included Backdoor

Digg



Hello there! If you are new here, you might want to [subscribe to the RSS feed](#) for updates on this topic. You may also subscribe by email in the sidebar ➔

submit

Security experts at **Symantec** have discovered a software application made for a USB-based battery charger sold by **Energizer** actually included a hidden backdoor that allowed unauthorized remote access to the user's system. The backdoor Trojan is easily removed, but Symantec believes the tainted software may have been in circulation since May 2007.

The product is the **Energizer Duo** USB battery charger, a device that charges batteries by drawing power from a USB port. The downloadable software that goes with the product — designed to monitor the charger's performance and status — was available for both **Mac** and **Windows**, but according to the **U.S. Computer Emergency Response Team** (US-CERT) only the Windows version was affected.



Symantec **said** it found the backdoor after analyzing a component of the USB charger software sent to it by US-CERT. The backdoor is designed to run every time the computer starts, and then listen for commands from anyone who connects. Among the actions an attacker can take after connecting include downloading a file; running a file; sending a list of files on the system; and offloading the files to the remote attacker.

Rogue PDFs Account for 80% of All Exploits, Says Researcher

Just hours before Adobe plans to deliver the latest patches for its popular PDF viewer, a security firm said malicious Reader documents made up 80% of all exploits at the end of 2009.

By Gregg Keizer

 [Comments](#)

TUE, FEBRUARY 16, 2010 — **Computerworld** — Just hours before Adobe is slated to deliver the latest patches for its popular PDF viewer, a security firm announced that by its counting, malicious Reader documents made up 80% of all exploits at the end of 2009.

Slideshow: 11 Security Companies to Watch

According to ScanSafe of San Bruno, Calif., vulnerabilities in Adobe's Reader and Acrobat applications were the most frequently targeted of any software during 2009, with hackers' PDF exploits growing throughout the year.

In the first quarter of 2009, malicious PDF files made up 56% of all exploits tracked by ScanSafe. That figure climbed above 60% in the second quarter, over 70% in the third and finished at 80% in the fourth quarter.

"PDF exploits are usually the first ones attempted by attackers," said Mary Landesman, a ScanSafe senior security researcher, referring to the multi-exploit hammering that hackers typically give visitors to malicious Web sites. "Attackers are choosing PDFs for a reason. It's not random. They're establishing a preference for Reader exploits."

Landesman, the author of ScanSafe's just-published **annual threat report**, said that attackers' preferences for PDF exploits were clearly demonstrated by the data. Exactly why hackers choose Adobe as their prime target is tougher to divine, however.

Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...
- ... including powerful automated tools ...

September 6th, 2007

Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

Categories: [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

Tags: [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



150 TalkBacks

ADD YOUR OPINION



SHARE



PRINT



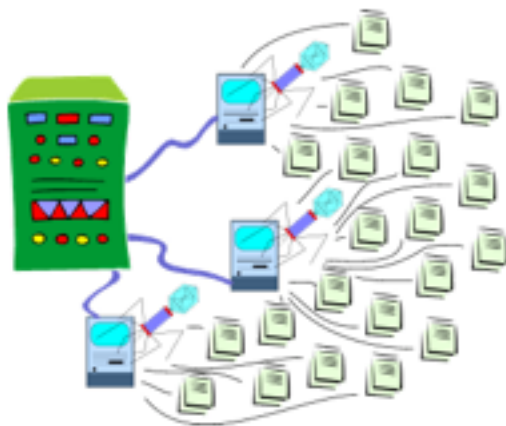
E-MAIL



+97

WORTHWHILE?

115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

botnet	% of spam	new spam/day	new spam/min	spam / bot/min	estimated botnet size	Country of Infection
Rustock	19%	20,191,511,739	14,021,883	91	540k to 810k	Brazil (21%), USA (9%), Poland (7%)
Cutwail	17%	18,417,396,993	12,789,859	59	1100k to 1600k	Vietnam (17%), RepKorea(12%), Brazil (10%)
Bagle	16%	17,334,321,383	12,037,723	37	520k to 780k	Brazil (12%), Spain (9%), USA (9%)
Bobax	14%	14,589,066,047	10,131,296	49	100k to 160k	Spain (12%), Italy (7%), India (7%)
Grum	9%	9,687,625,087	6,727,517	307	580k to 860k	Vietnam (18%), Russia (17%), Ukraine (8%)
Maazben	2%	2,161,829,037	1,501,270	93	240k to 360k	Romania (17%), Brazil (11%), Saudi Arabia (7%)
Festi	1%	1,353,086,645	939,644	53	140k to 220k	Vietnam (31%), India (11%), China (5%)
Mega-D	1%	996,079,588	691,722	46	50k to 70k	Vietnam (14%), Brazil (11%), India (6%)
Xarvester	1%	885,682,360	615,057	155	20k to 36k	Brazil (15%), Poland (11%), USA (10%)
Gheg	0%	436,044,470	302,809	22	50k to 70k	Brazil (15%), Poland (8%), Vietnam (8%)
Unclassified Botnets	3%	2,994,054,378	2,079,204	65	120k to 180k	
Other, smaller botnets	0%	439,986,486	305,546	47	130k to 190k	
Total BotnetSpam	83%	89,486,684,212	62,143,531	85	3600k to 5400k	Brazil (13%), Vietnam (7%), USA (6%)
Non-botnet spam	17%	17,827,092,771	12,379,926			
Grand Total	100%	107,313,776,983	74,523,456			

MessageLabs

SYMANTEC HOSTED SERVICES

™

Modern Threats

- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” ...
- ... including powerful automated tools ...
- ... and defenders likewise devise novel tactics ...



Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

SEARCH THIS BLOG

Go

RECENT POSTS

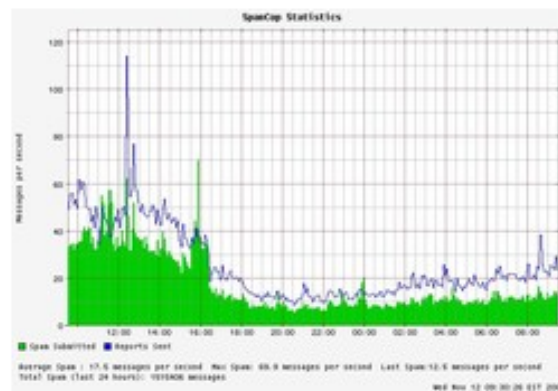
- [E-Banking on a Locked Down PC, Part II](#)
- [ChoicePoint Breach Exposed 13,750 Consumer Records](#)
- [President Obama on Cyber Security Awareness](#)
- [Mozilla Disables Microsoft's Insecure Firefox Add-on](#)
- [PayChoice Suffers Another Data Breach](#)

Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnings](#)

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note:** A link to the full story on McColo's demise is available [here](#).)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major

Modern Threats, con't

- Most cyber attacks aim for **profit** and are facilitated by a well-developed “underground economy ...



My Documents

ProAgent V2.0 Public Edition

Send Menu

- Send Passwords
- Send CD-Keys
- Send KeyLog
- Send System Information
- Send Address Book
- Send URL History
- Send Processes Log

Options

- Give a fake error message
- Melt server on install
- Disable AntiVirus Programs
- Clear Windows XP Restore Points
- Protection for removing Local Server

Server Icon

You can choose any icon for server



Choose Icon

Bind with File

Bind with File

You can bind server with any files you want



Select File To Bind

Notification

Your e-mail address which you will to receive information from ProAgent.

E-Mail:

Test

Decryptor

Remove Server

About

Buy Undetectable

Help

Create Server

ProAgent - Professional Agent Copyright © 2005 SIS-Team



Recycle Bin



ProAgent



9:56 AM

ProAgent v2.1



- ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.
- It is an ultimate solution for monitoring spouses, children, employees, or anyone else!
- ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!
- ProAgent can work in all kind of networks, it doesn't matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase **ProAgent v2.1** Special Edition...

Click here to download **ProAgent v2.1** Public Edition

SIS - Products

Purchase Program

Customer Support Department



Commercial Programs

Freeware Programs

Custom Special Programs

New Generation Software Solutions...

New Products

SIS-IExploiter v2.0

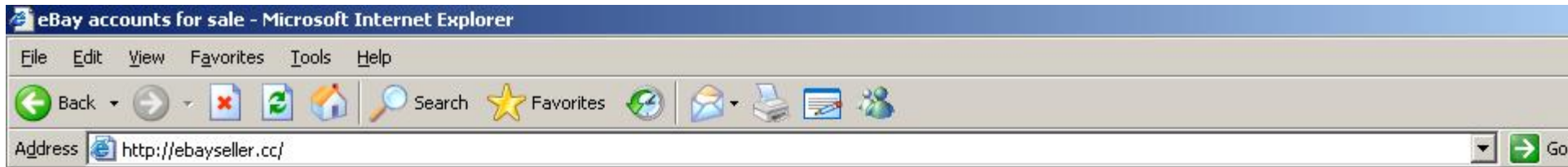
ProAgent v2.1



AntiDote v1.2

SIS-Downloader

Virtual Keyboard



Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.

Перед покупкой следует обязательно ознакомиться с FAQ.

По работе с товаром не консультирую.

Работа через гарант сервис приветствуется.

Мои цены:

seller/баер акк до 10 фидов = 5\$

seller/баер акк 10-25 фидов = 10\$

seller/баер акк 25-50 фидов = 15\$

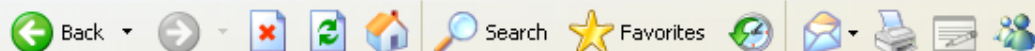
seller/баер акк более 50 фидов = 25\$



Recycle Bin

MyiFrame.com — Тарифы на продажу трафика - Microsoft Internet Explorer

File Edit View Favorites Tools Help



Address http://www.myiframe.com/support/?path=/30-client/20-tariffs/

Go

Links >>

Первая биржа iframe-трафика

Авторизация

Забыли пароль?

MyiFrame.com

НАВИГАЦИЯ

- Авторизация
- Забыли пароль?
- Регистрация
- Поддержка

принимает **WebMoney** Аттестованный участник системы **WM**

Рекомендуем использовать



ТАРИФЫ НА ПРОДАЖУ ТРАФИКА

Страна	«Чистый»	«Грязный»
RU	\$ 1,40 за 1000	\$ 5,46 за 1000
UA	\$ 0,60 за 1000	\$ 2,34 за 1000
BY	\$ 0,40 за 1000	\$ 1,56 за 1000
US	\$ 1,00 за 1000	\$ 3,90 за 1000
CA	\$ 0,80 за 1000	\$ 3,12 за 1000
other	\$ 0,20 за 1000	\$ 0,78 за 1000

PAY PER INSTALL AFFILIATE PROGRAMS

Today is: Tuesday 16. November 2010



CLICK HERE TO VISIT OUR BEST SPONSOR.

WE WORK Even when you sleep!

One of the best PPI programs. Up to \$180 per 1000 Installs.

Affiliate Program NewsLetter Get new programs via email

Insert your Email Address:

JOIN MAKE MONEY FORUM

Learn **How to make money with PPN Gateway**
Free guide to teach you **how to make \$7000 per day**

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates.

BOOKMARK US

MAKE MONEY CATEGORIES

- Pay Per Click
- Pay Per Impression
- Bid Search Engines
- Pay Per Lead
- Pay Per Install

OTHERS

- CONTACT

GET PAID from each toolbar install

Best Pay-per-install affiliate programs on the net. Earn money with any traffic, these ActiveX affiliates will convert anything and make you rich. Payments are up to \$1.50 per install. You usually distribute installation of toolbar and making cash. You can also make loads of money with content sites such are movies, games, mp3 and protect your content with Content Gateways which are paying most, to unlock the content user needs to install simple adware application and than he can get content for free.



All

Pages: [0] | 1 | 2 | 3 | 4

Make money with these BEST AFFILIATE PROGRAMS

BOOKMARK US

Last 10 Reviews

- CPALeAd - November/13/2010
- SexSearch - October/31/2010
- LoudMo - October/28/2010
- SexSearch - October/18/2010
- SexSearch - October/18/2010
- ioXes - October/12/2010
- Earning4u - September/09/2010
- Earning4u - August/30/2010

CONVERT INSTALLS TO CASH WITH HIGH RATES

GoldInstall

[Main](#)[Sign up](#)[Login](#)[Rates](#)[Contacts](#)[Terms of service](#)[FAQ](#)

Prices

Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13\$
US	150\$
GB	110\$
CA	110\$
DE	30\$
BE	20\$
IT	65\$
CH	20\$
CZ	20\$
DK	20\$
ES	30\$
AU	55\$
FR	30\$
NL	20\$
NO	20\$
PT	30\$
LB	6\$



CASH PARADISE UNIVERSITY

ТВОЙ КЛЮЧ К БОГАТСТВУ
YOUR KEY TO WEALTH



ICQ 24-77777777

JABBER: [REDACTED]



[MAIN](#)

[STUDY PROGRAMS](#)

[RULES](#)

[CONTACT US](#)

Study programs:

Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy

Google Buzz bug exposes user geo location

'Pretty nasty vulnerability'

By [Dan Goodin in San Francisco](#) • [Get more from this author](#)

Posted in [Security](#), 16th February 2010 21:13 GMT

[Hitachi IT Operations Analyzer: 30-day free trial](#)

Updated Already besieged by complaints of shoddy user privacy, Google Buzz is susceptible to exploits that allow an attacker to commandeer accounts and even learn where victims are located, a security researcher said Tuesday.

The XSS, or cross-site scripting, vulnerability is unusual because it affects google.com, the domain that sets authentication cookies for a variety of popular Google services, including Mail, Calendar and Documents. That means an attacker might be able to tamper with victims' accounts simply by tricking them into visiting a booby-trapped link, although the researcher said only cookies for Buzz appeared to be at risk in this case.

What's more, the vulnerability ties into to the much-vaunted [Google Location Services](#), making it possible for the attacker to learn the geographical location of users who have already opted in.

"It's a pretty nasty vulnerability, actually," Robert "RSnake" Hansen, CEO of [secTheory.com](#), told *The Register*. "If you've already agreed to that before being exploited, which most people will do, then the attacker also gets to know your location."

A Google spokesman on late Tuesday said the bug could affect users of Google Buzz for mobile. Company security personnel are in the process of fixing it, and there are no indications the flaw has been exploited, he said.

"We understand the importance of our users' security, and we are committed to further

Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*



Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

[Home](#) [Why Privacy](#) [About Us](#) [Fact Sheets](#) [Latest Issues](#) [Speeches & Testimony](#)

Chronology of Data Breaches

Go to Breaches for [2005](#), [2006](#), [2007](#), [2008](#), [2009](#) or [2010](#).

DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego	A hacker breached the security of two	3,500
Jan. 1, 2010	collective2.com	Users of the do-it-yourself trading site collective2.com received an "urgent" e-mail notifying them that the company's	25,000
Jan. 1, 2010	Netflix (Los Gatos, CA)	A class action suit was filed against Netflix, Inc., in the United States District Court for the Northern District of	100 million Not Added to Total
Jan. 12, 2010	Suffolk County National Bank (Long Island, NY)	Hackers have stolen the login credentials for more than 8,300 customers of small New York bank after breaching its security	8,373
TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005.			343,485,708 What does the total number indicate?

[Home](#) > [News](#) > [Security](#)

Security



May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by [Michelle Meyers](#)



Font size



Print



E-mail



Share



20 comments

0

tweet



Share

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday afternoon.

Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... and recent times have seen the rise of nation-state issues, including:
 - Censorship / network control

China Cracks Down on Tor Anonymity Network

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

THURSDAY, OCTOBER 15, 2009

[E-mail](#) [Audio](#) [Print](#) [Favorite](#) [Share](#) [T](#) [T](#) [T](#)

For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called [Tor](#), came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.



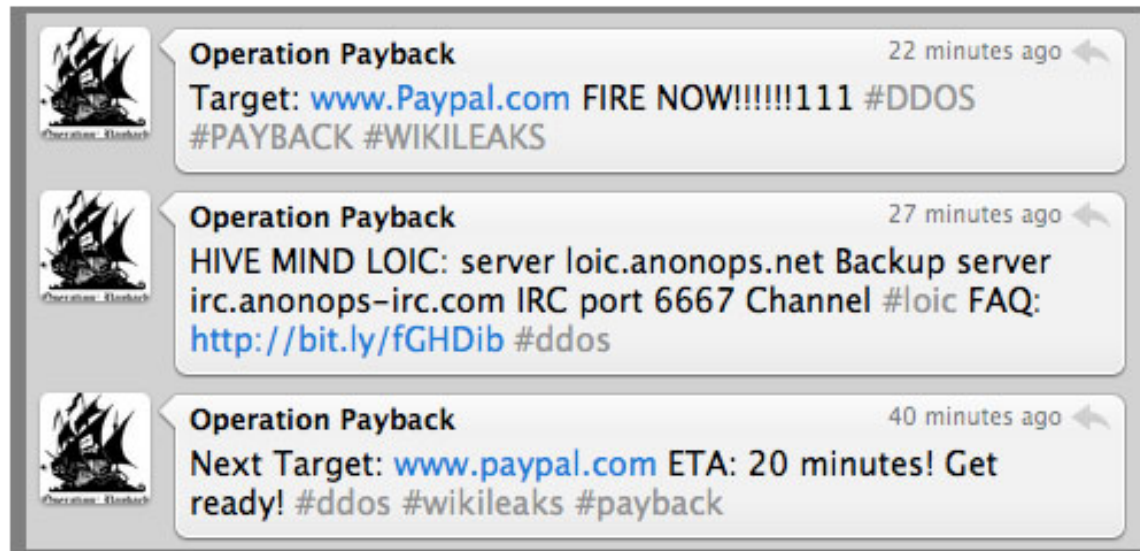
"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

[Tor is one of several systems](#) that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching



Continuing pro-Wikileaks DDOS actions, Anonymous takes down PayPal.com

Xeni Jardin at 7:10 PM Wednesday, Dec 8, 2010



Third finance-related Anonymous "Operation Payback" takedown in a single day: PayPal.com is effectively offline, moments after the command was tweeted. At the time of this blog post, the PayPal *service* is still functioning, but the site's dead. Earlier today, Visa.com and Mastercard.com were taken offline by Anonymous DDOS attacks, along with other targets perceived as enemies of Wikileaks and of online free speech... including Twitter.com, for a while.

Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... and recent times have seen the rise of nation-state issues, including:
 - Censorship / network control
 - Espionage

Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

THIS STORY

- » [Google attack part of vast campaign](#)
- [Google hands China an Internet dilemma](#)
- [Statement from Google: A new approach to China](#)

[+ View All Items in This Story](#)

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and [Dow Chemical](#) -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail



People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

[+ Enlarge Photo](#)

What Google might miss out on

Google said it may exit China,

Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

This article is by William J. Broad, John Markoff and David E. Sanger.

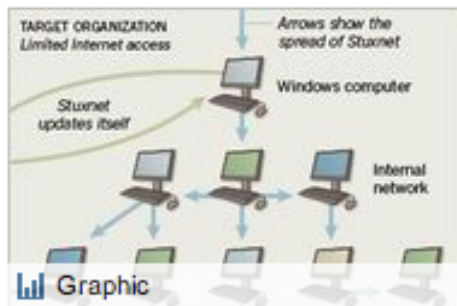
[Enlarge This Image](#)



Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

Multimedia



Graphic
How Stuxnet Spreads

The Dimona complex in the Negev desert is famous as the heavily guarded heart of [Israel's](#) never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine [Iran's](#) efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the [Stuxnet](#) computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear



Modern Threats, con't

- Most cyber attacks aim for profit and are facilitated by a well-developed “underground economy ...
- ... there are also extensive threats to privacy including *identity theft*
- ... but recent times have seen the rise of nation-state issues, including:
 - Censorship / network control
 - Espionage
 - ... and war

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels
 The Guardian, Thursday 17 May 2007
[Article history](#)



Bronze Soldier, the Soviet war memorial removed from Tallinn. Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

Categories: [Black Hat](#), [Botnets](#), [Denial of Service \(DoS\)](#), [Governments](#), [Hackers...](#)

Tags: [Security](#), [Cyber Warfare](#), [DDoS](#), [Georgia](#), [South Osetia...](#)

62 TalkBacks ADD YOUR OPINION
SHARE
PRINT
E-MAIL
+18 WORTHWHILE? **24** VOTES

In the wake of the [Russian-Georgian conflict](#), a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with [Georgia's Ministry of Foreign Affairs](#) undertaking a desperate step in order to disseminate real-time information by moving to a Blogger account.

Country	IPs	Count	Count	Count	Count
Finland, U.S.A.	Okay	19.4	19.9	40.1	
Netherlands, Netherlands	Okay	149.3	146.6	276.4	
Malaysia, Australia	Okay	179.9	174.5	178.9	
Singapore, Singapore	Okay	209.5	214.0	239.8	
San Jose, U.S.A.	Feedback Loop (1000)				
Amsterdam, Netherlands	Feedback Loop (1000)				
Atlanta, U.S.A.	Feedback Loop (1000)				
London, United Kingdom	Feedback Loop (1000)				
Stockholm, Sweden	Feedback Loop (1000)				
Oslo, Norway	Feedback Loop (1000)				
Chicago, U.S.A.	Feedback Loop (1000)				
Atlanta, U.S.A.	Feedback Loop (1000)				
Amsterdam, Netherlands	Feedback Loop (1000)				
Frankfurt, Germany	Feedback Loop (1000)				
Paris, France	Feedback Loop (1000)				
Copenhagen, Denmark	Feedback Loop (1000)				
San Francisco, U.S.A.	Feedback Loop (1000)				
Toronto, Canada	Feedback Loop (1000)				
Madrid, Spain	Feedback Loop (1000)				
Shanghai, China	Feedback Loop (1000)				
Lille, France	Feedback Loop (1000)				
Zurich, Switzerland	Feedback Loop (1000)				
Munich, Germany	Feedback Loop (1000)				
Capitani, Italy	Feedback Loop (1000)				
Shanghai, China	Feedback Loop (1000)				
Frankfurt, Germany	Feedback Loop (1000)				
Porto Alegre, Brazil	Feedback Loop (1000)				
Spokane, Washington	Feedback Loop (1000)				
Mumbai, India	Feedback Loop (1000)				
San Jose, U.S.A.	Feedback Loop (1000)				

U.S. cyber counterattack: Bomb 'em one way or the other

National Cyber Response Coordination Group establishing proper response to cyberattacks

By [Ellen Messmer](#), *Network World*, 02/08/07

San Francisco — If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source.

Coming Up ...

- Section meets tomorrow
- Thursday's lecture: *Buffer Overflow Attacks*
- Check out Piazza
- Due **next week:**
 - Get your class account set up
 - Use it to submit a writeup that you have read the class web page, including (especially) policies on collaboration, Academic Dishonesty, and ethics/legality