CS 161: Computer Security

Prof. Raluca Ada Popa

Prof. David Wagner

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

January 20, 2016

First off

- Can I have a volunteer, please?

THE CS161 EPIC LIP SYNC BATTLE

Injection attacks

- What does this have to do with computer security?

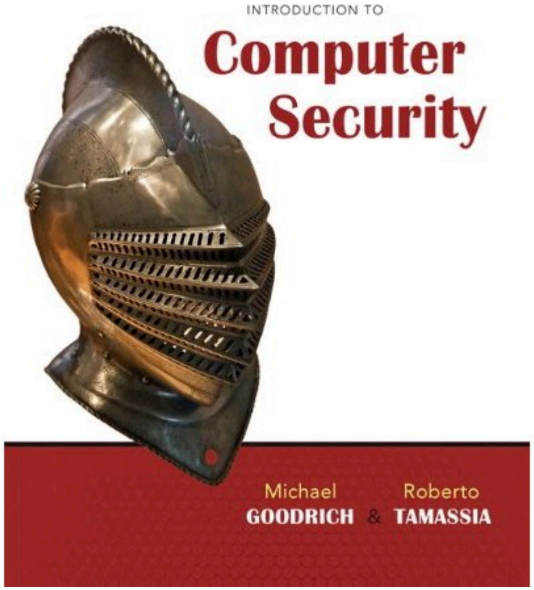
LOGISTICS

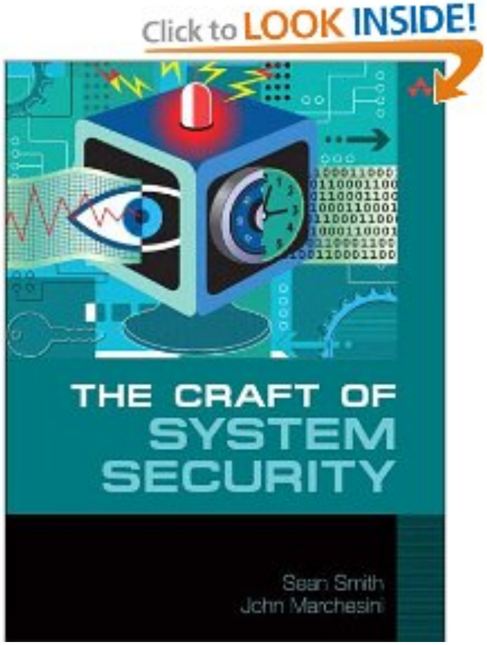
Course Structure

- Absorb material presented in lectures and section
- 3 course projects (24% total)
  - Done individually or in small groups
- ~4 homeworks (16% total)
  - Done individually
- Two midterms (30%)
  - Mon Feb 22 and Mon Mar 28, 8-9:30pm
- A comprehensive final exam (30%)
  - Tue May 10, 7-10pm

Textbooks

- No required textbook. If you want extra reading:
- *Optional*: *Introduction to Computer Security*, Goodrich & Tamassia
- *Optional*: The Craft of System Security, Smith & Marchesini





Class Policies

- Late homework: no credit
- Late project: -10% if < 24 hrs, -20% < 48 hrs, -40% < 72 hrs, **no credit** ≥ 72 hrs
- Never share solutions, code, etc., or let any other student see them. Work on your own (unless assignment states otherwise).
- If lecture materials available prior to lecture, *don't use to answer questions* during class
- Participate in Piazza
  - Send course-related questions/comments, or ask in office hours. No email please: it doesn't scale.

OVERVIEW OF THIS COURSE

What is Computer Security?

- Allow intended use of computer systems
- Prevent unwanted use that may cause harm

Why should you care?

- Impacts everyone’s day-to-day life
  - Millions of compromised computers, millions of stolen passwords

Learn About Security

Make a Difference

THREAT MODELS

Threat models

- 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
  - Determines which defenses are worthwhile

MANUAL

DOE M 470.4-1

Approved: 8-26-05
Review: 8-26-07
Chg 1: 3-7-06

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

U.S. DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

Vertical line denotes change.

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

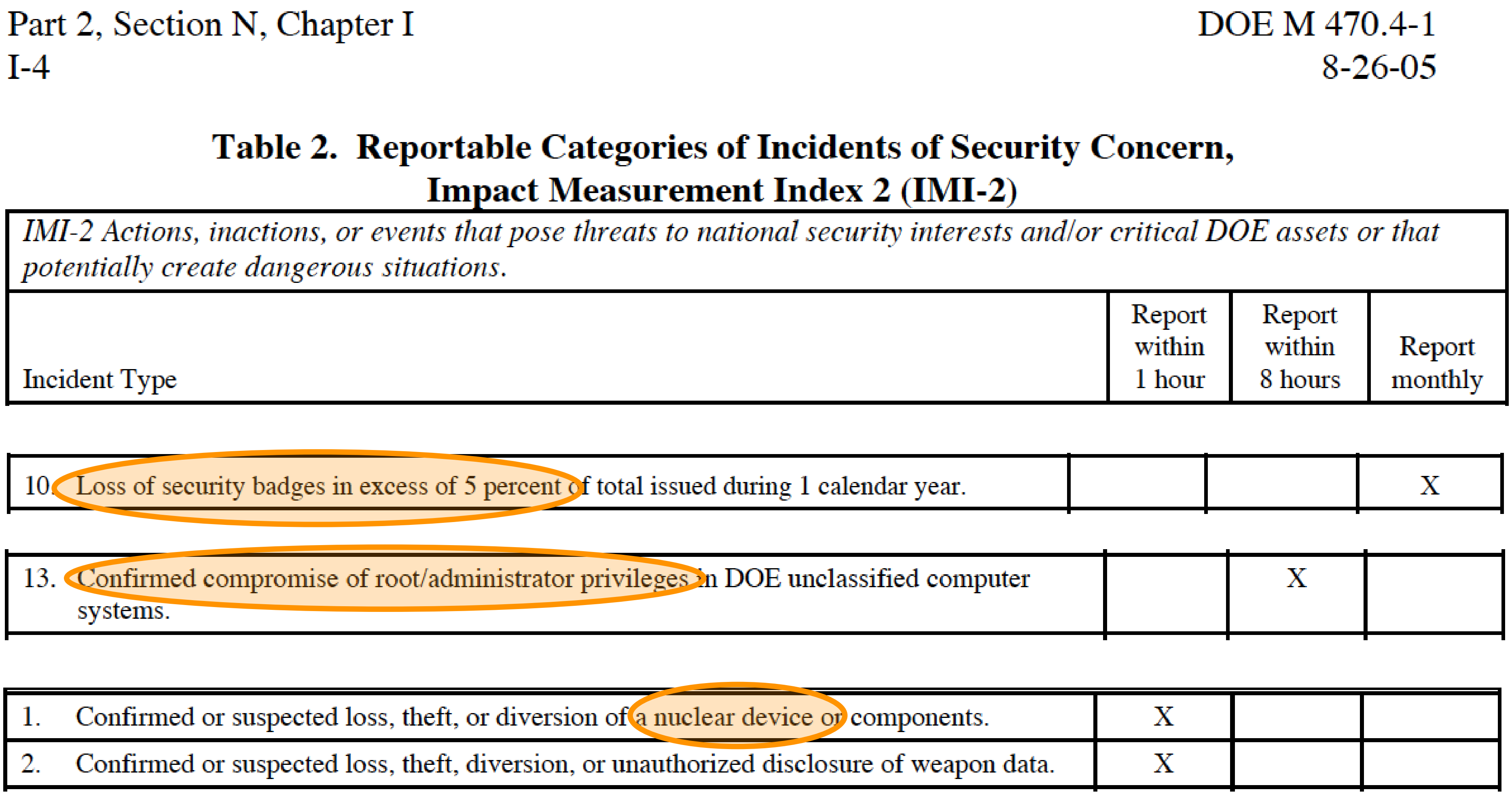
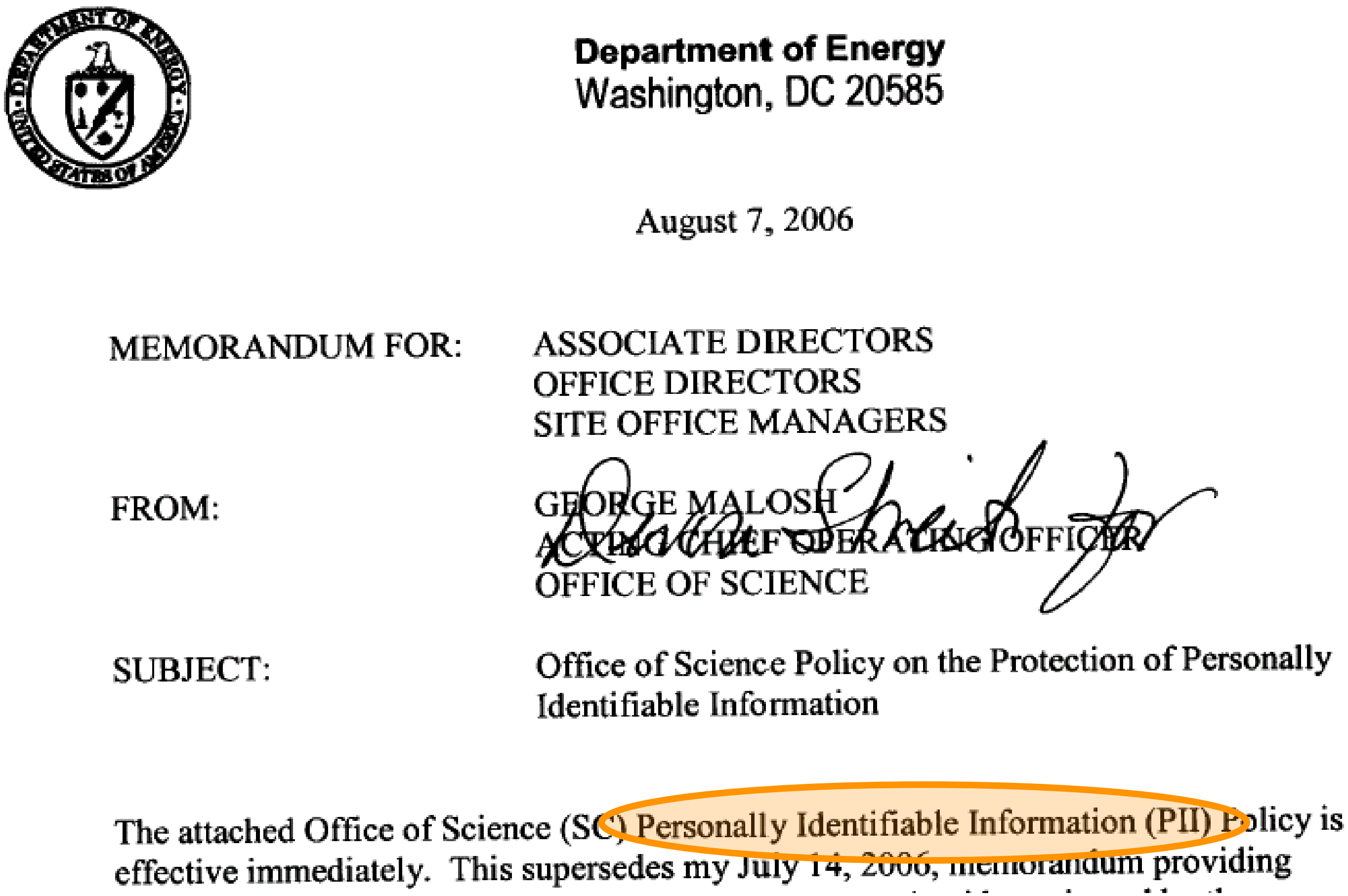


Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		



Department of Energy
Washington, DC 20585

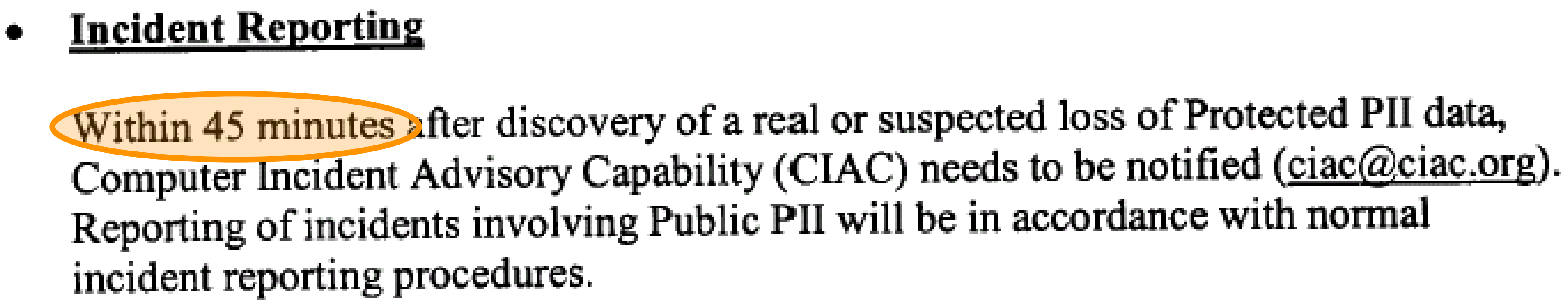
August 7, 2006

MEMORANDUM FOR: ASSOCIATE DIRECTORS
OFFICE DIRECTORS
SITE OFFICE MANAGERS

FROM: GEORGE MALOSH
ACTING CHIEF OPERATING OFFICER
OFFICE OF SCIENCE

SUBJECT: Office of Science Policy on the Protection of Personally Identifiable Information

The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing



- **Incident Reporting**

Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org). Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

Vast Data Cache About Veterans Is Stolen

By DAVID STOUT and TOM ZELLER Jr.
Published: May 23, 2006

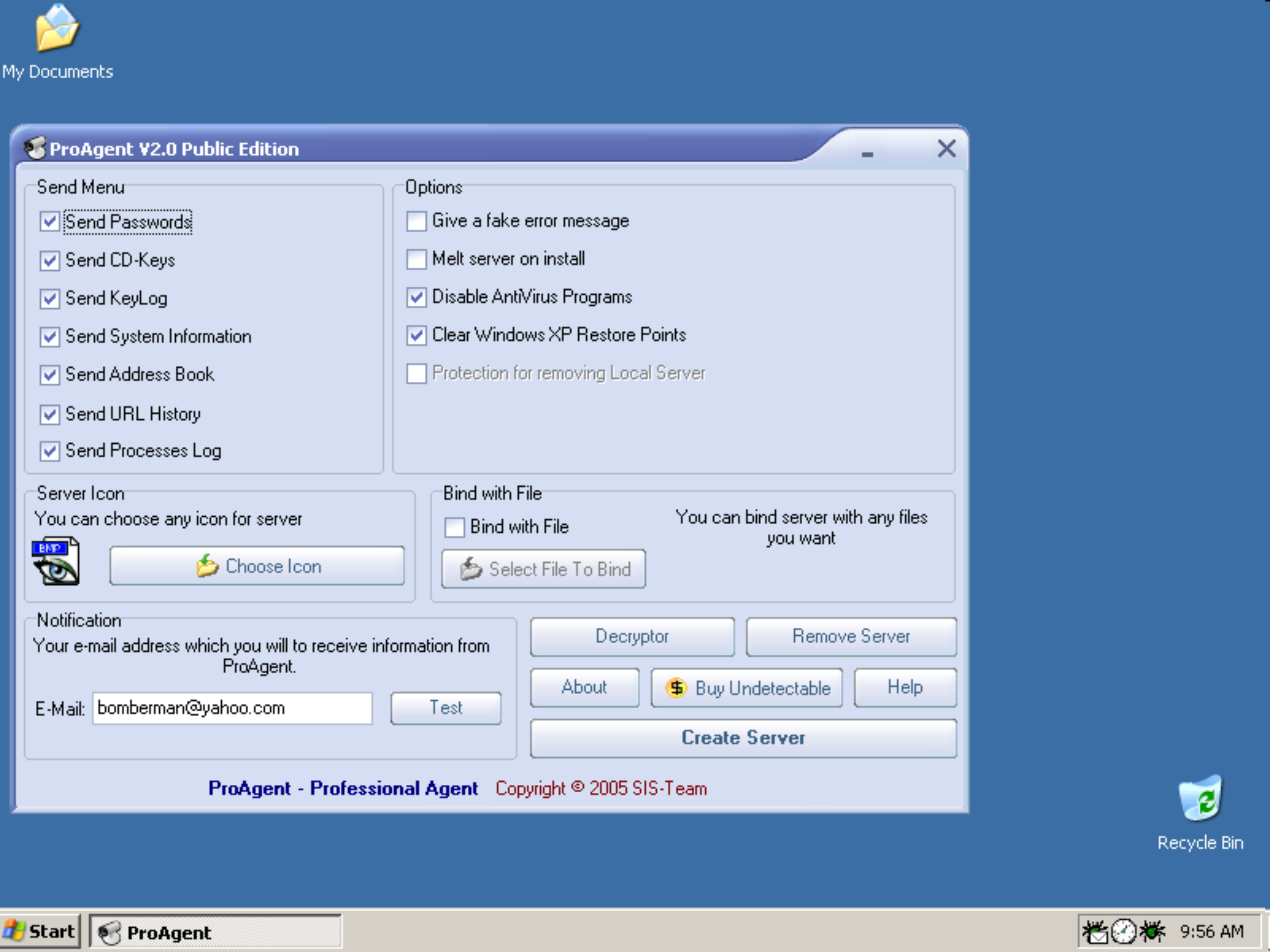
WASHINGTON, May 22 — Personal electronic information on up to 26.5 million military veterans, including their Social Security numbers and birth dates, was stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization, the agency said Monday.

Called to account at Capitol Hill hearings, Nicholson said he was angry that he hadn't been told about the burglary until nearly two weeks after it happened.

The theft exposed lax data-security procedures at the agency and led to congressional hearings and the departures of five senior VA officials. It also appears to have ended Johnson's career:

Threats have evolved…

- 1990’s: bragging rights
- late 2000’s: financially motivated
  - Spam, pharmaceuticals, credit card theft, identity theft



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

Bind with File

□ Bind with File

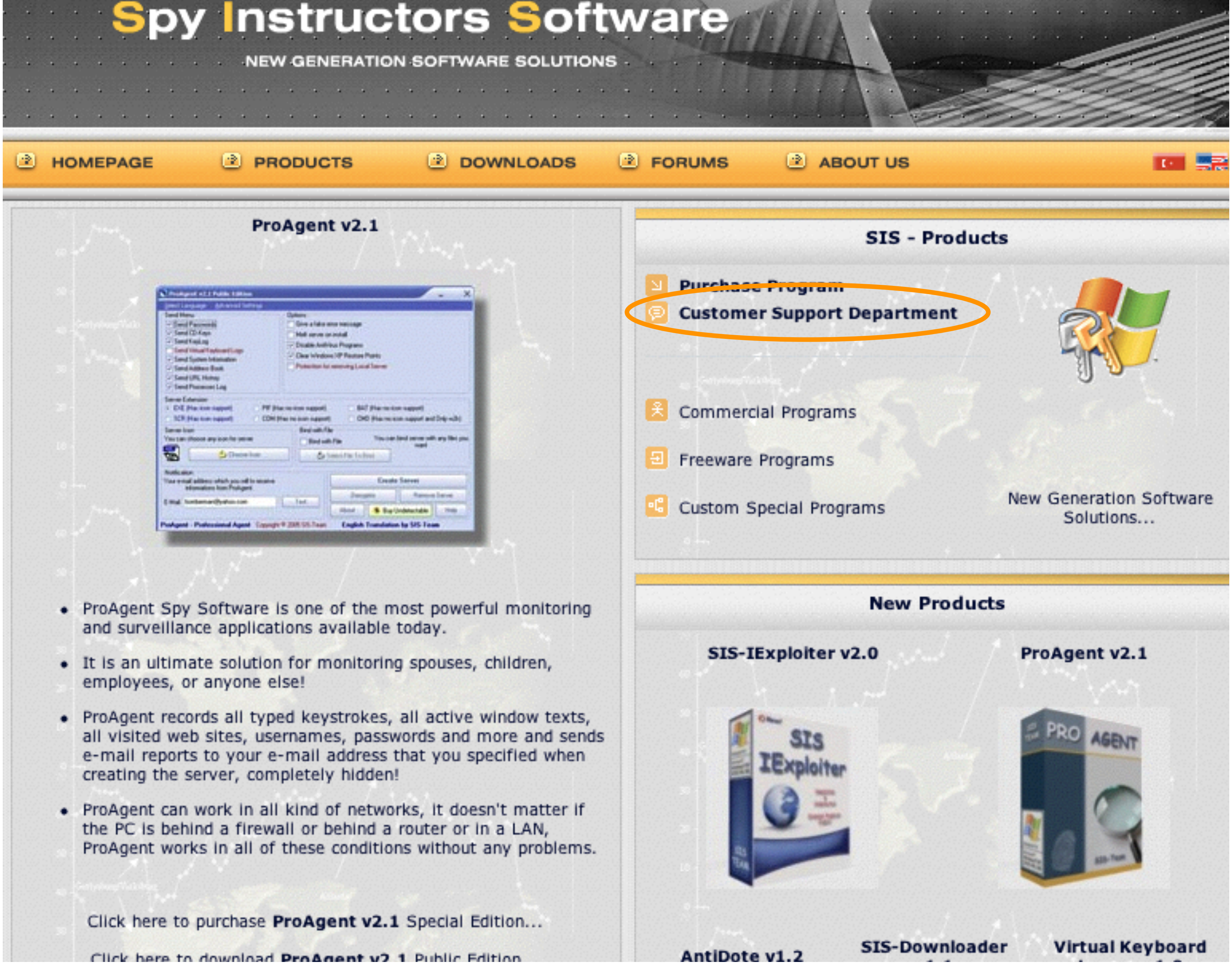
You can bind server with any files you want

Notification

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

E-Mail: bomberman@yahoo.com

ProAgent - Professional Agent Copyright © 2005 SIS-Team



Spy Instructors Software

NEW GENERATION SOFTWARE SOLUTIONS

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

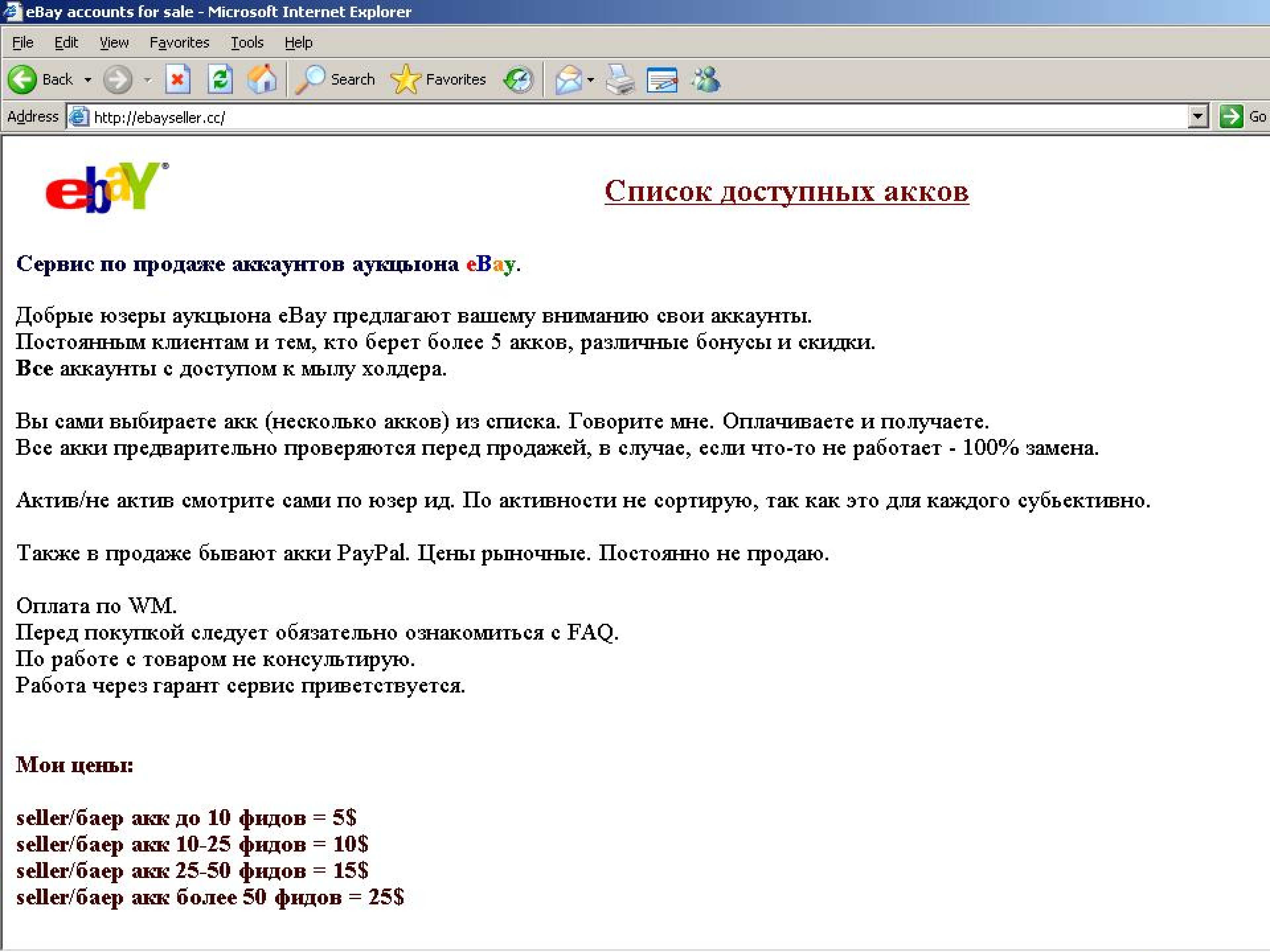
SIS-IExploiter v2.0

ProAgent v2.1

AntiDote v1.2

SIS-Downloader

Virtual Keyboard


eBay accounts for sale - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://ebayseller.cc/
Go
ebY

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.

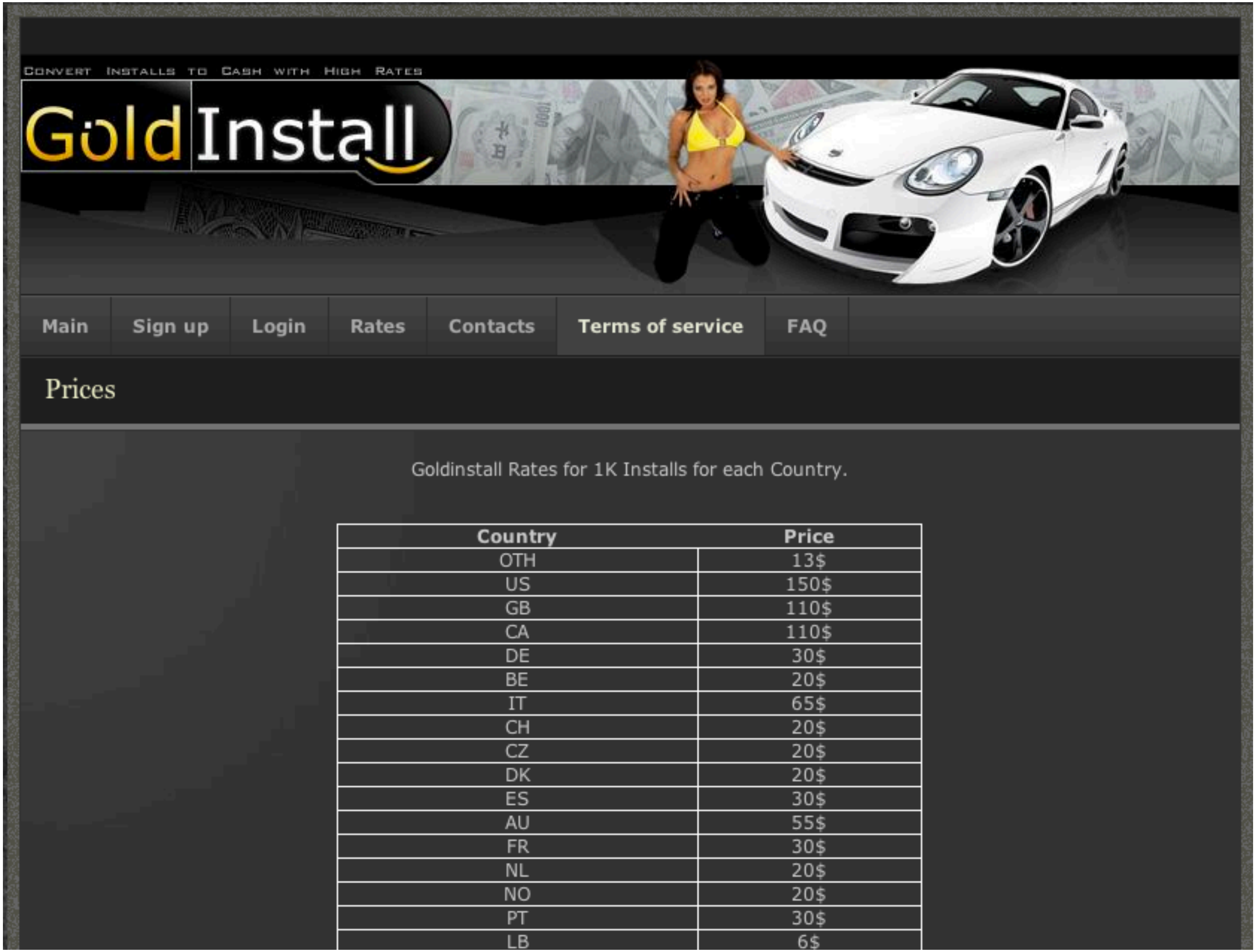
Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.

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:

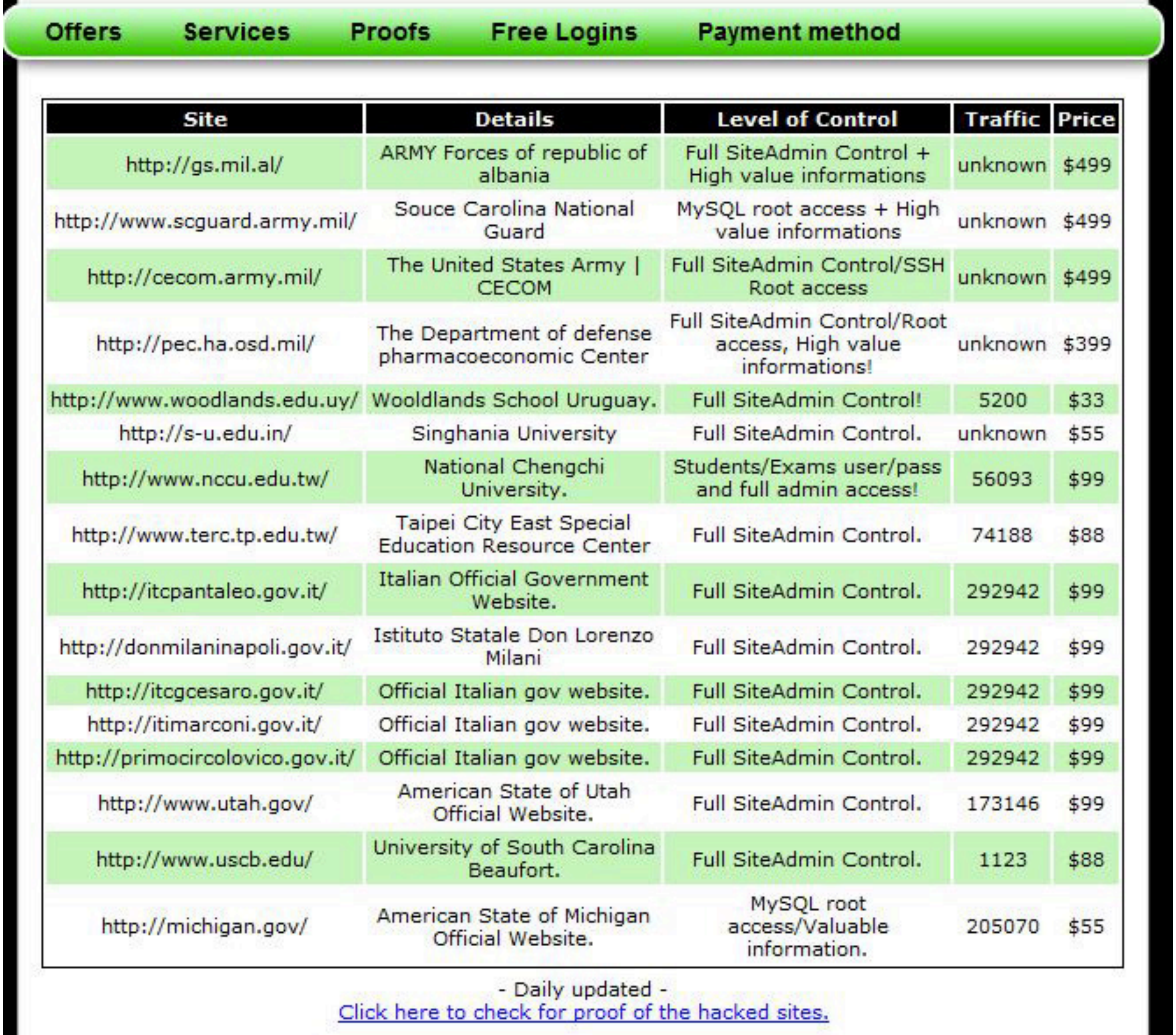
seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$



Prices

Goldinstall Rates for 1K Installs for each Country.

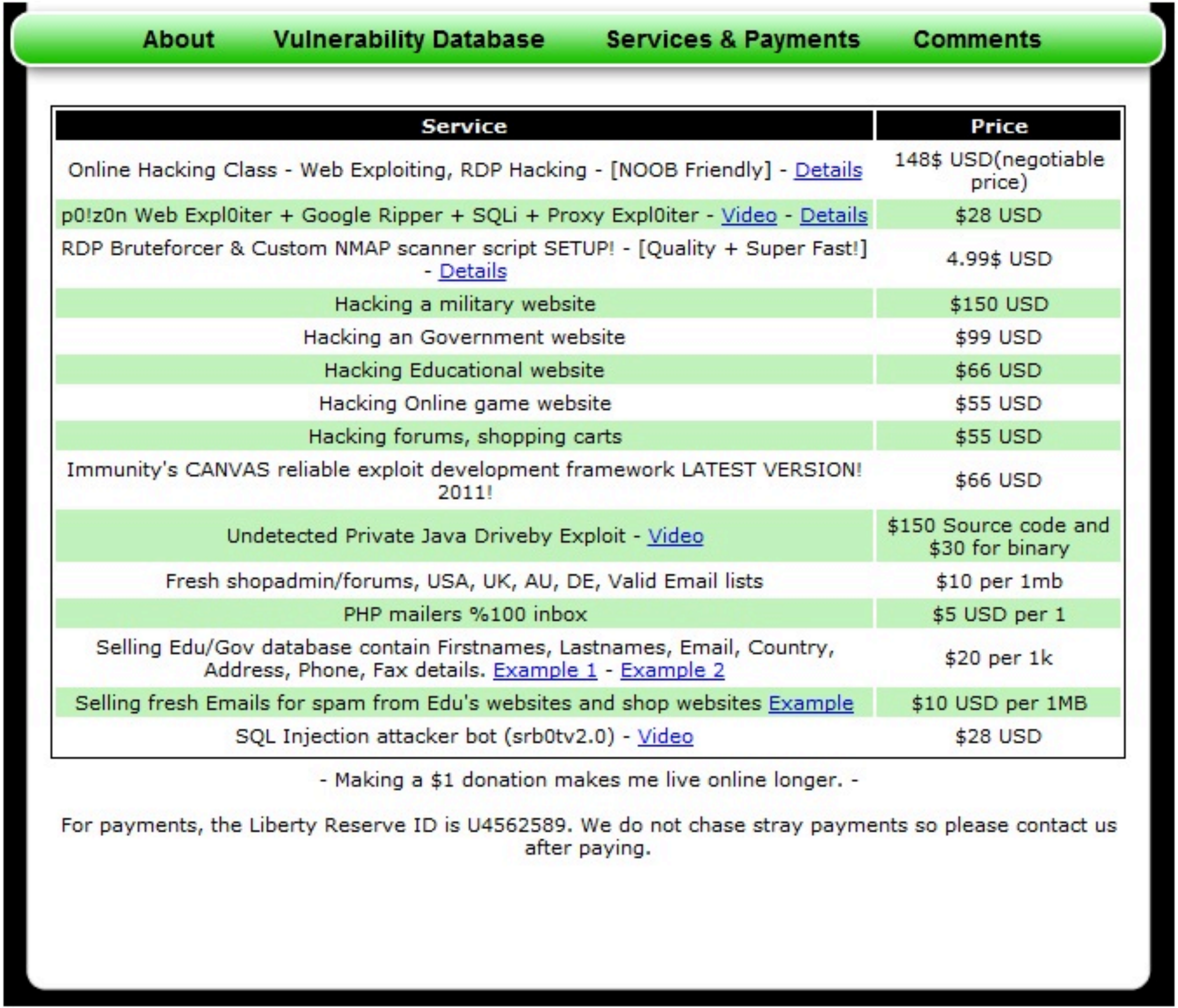
Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$
DK	20$
ES	30$
AU	55$
FR	30$
NL	20$
NO	20$
PT	30$
LB	6$



Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	$499
http://cecom.army.mil/	The United States Army | CECOM	Full SiteAdmin Control/SSH Root access	unknown	$499
http://pec.ha.osd.mil/	The Department of defense pharmacoeconomic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	$399
http://www.woodlands.edu.uy/	Wooldlands School Uruguay.	Full SiteAdmin Control!	5200	$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://itimarconi.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://primocircolovico.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99
http://www.utah.gov/	American State of Utah Official Website.	Full SiteAdmin Control.	173146	$99
http://www.uscb.edu/	University of South Carolina Beaufort.	Full SiteAdmin Control.	1123	$88
http://michigan.gov/	American State of Michigan Official Website.	MySQL root access/Valuable information.	205070	$55

- Daily updated -

Click here to check for proof of the hacked sites.



Service	Price
Online Hacking Class - Web Exploiting, RDP Hacking - [NOOB Friendly] - Details	148$ USD(negotiable price)
p0!z0n Web Expl0iter + Google Ripper + SQLi + Proxy Expl0iter - Video - Details	$28 USD
RDP Bruteforcer & Custom NMAP scanner script SETUP! - [Quality + Super Fast!] - Details	4.99$ USD
Hacking a military website	$150 USD
Hacking an Government website	$99 USD
Hacking Educational website	$66 USD
Hacking Online game website	$55 USD
Hacking forums, shopping carts	$55 USD
Immunity's CANVAS reliable exploit development framework LATEST VERSION! 2011!	$66 USD
Undetected Private Java Driveby Exploit - Video	$150 Source code and $30 for binary
Fresh shopadmin/forums, USA, UK, AU, DE, Valid Email lists	$10 per 1mb
PHP mailers %100 inbox	$5 USD per 1
Selling Edu/Gov database contain Firstnames, Lastnames, Email, Country, Address, Phone, Fax details. Example 1 - Example 2	$20 per 1k
Selling fresh Emails for spam from Edu's websites and shop websites Example	$10 USD per 1MB
SQL Injection attacker bot (srb0tv2.0) - Video	$28 USD

- Making a $1 donation makes me live online longer. -

For payments, the Liberty Reserve ID is U4562589. We do not chase stray payments so please contact us after paying.

Threats have evolved…

- Attackers have become more sophisticated; arms race between attackers and defenders fuels rapid innovation in malware

- Many attacks aim for profit and are facilitated by a well-developed “underground economy”

Threats have evolved…

- 1990’s: bragging rights
- late 2000’s: financially motivated
  - Spam, pharmaceuticals, credit card theft, click fraud
- 2010’s: politically motivated
  - Government actors: Stuxnet, Flame, Aurora
  - Private activism: Anonymous, Wikileaks

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 »

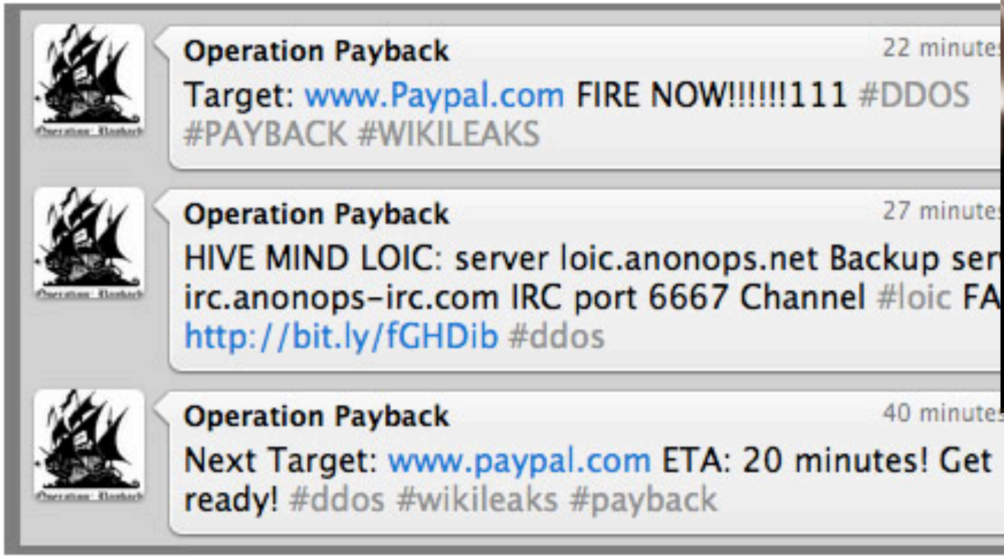
For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor, came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which 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

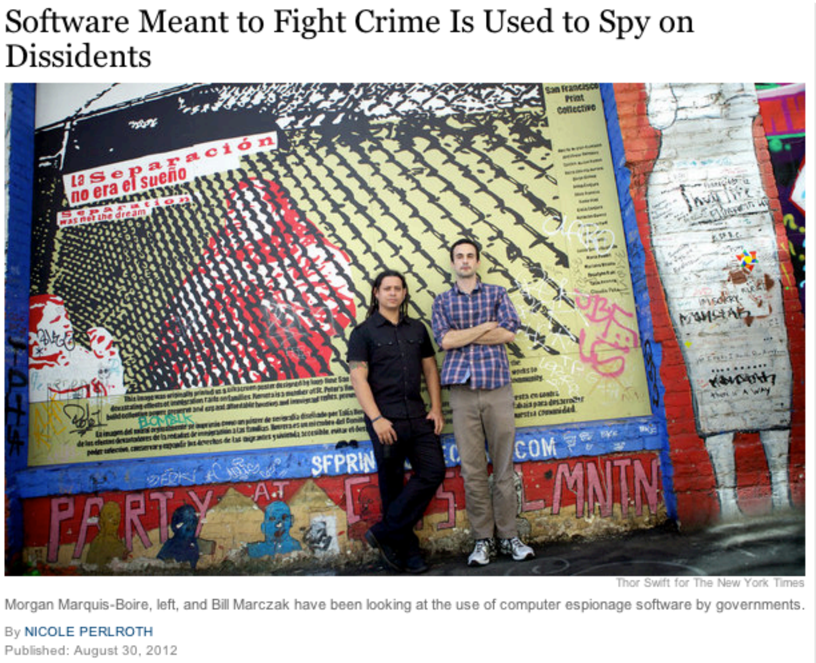


Operation Payback 22 minute
Target: www.Paypal.com FIRE NOW!!!!!!111 #DDOS #PAYBACK #WIKILEAKS

Operation Payback 27 minute
HIVE MIND LOIC: server loic.anonops.net Backup ser
irc.anonops-irc.com IRC port 6667 Channel #loic FA
http://bit.ly/fGHDib #ddos

Operation Payback 40 minutes ago
Next Target: www.paypal.com ETA: 20 minutes! Get ready! #ddos #wikileaks #payback

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.



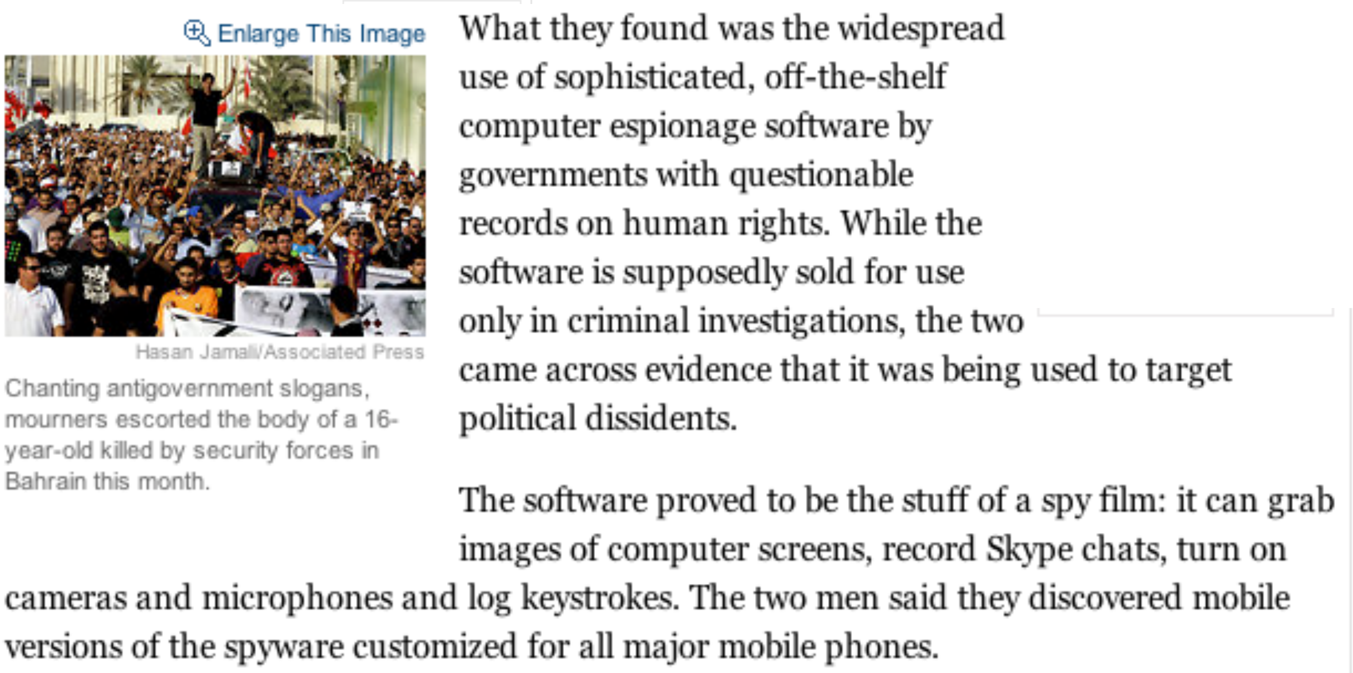
Software Meant to Fight Crime Is Used to Spy on Dissidents

Thor Swift for The New York Times

Morgan Marquis-Boire, left, and Bill Marczak have been looking at the use of computer espionage software by governments.

By NICOLE PERLROTH

Published: August 30, 2012



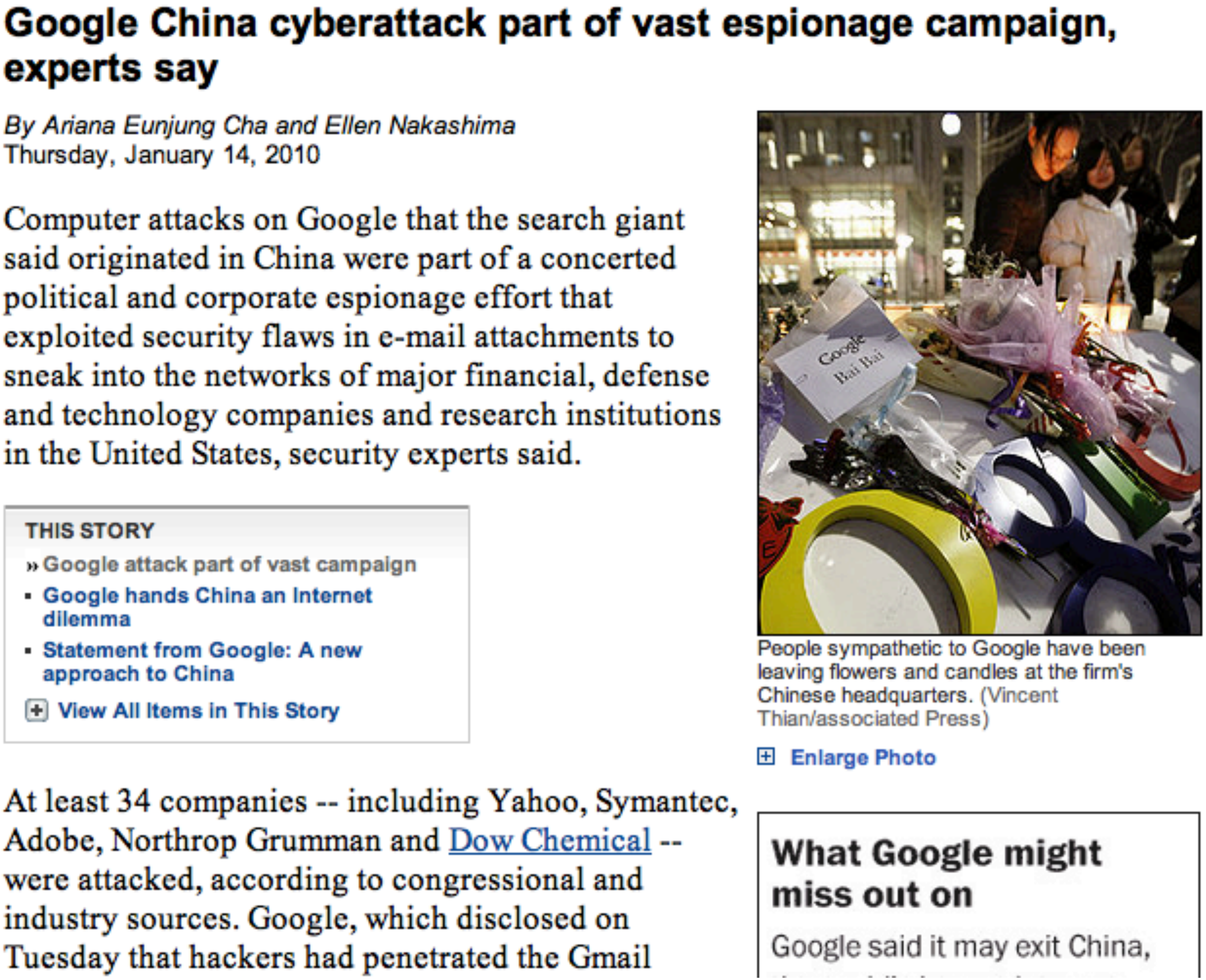
Enlarge This Image

Hasan Jamali/Associated Press

Chanting antigovernment slogans, mourners escorted the body of a 16-year-old killed by security forces in Bahrain this month.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.



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

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

⊞ Enlarge Photo

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

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

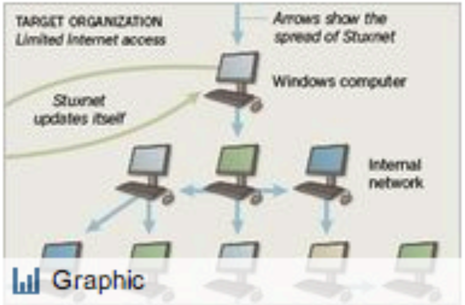
Ralph Langner, an independent computer security expert, solved Stuxnet.

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

Multimedia



How Stuxnet Spreads

Lesson

- To protect computer systems, you must know your enemy

- Security is not about perfection: it’s about defenses that are good enough to stop the threats you’re likely to encounter

AMAZING EXPLOITS

Epic Hack: Internet worm

- The first Internet worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out.

Epic Hack: Internet worm

- The first Internet worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out.
- And took down the Internet.

Epic Hack: Internet worm

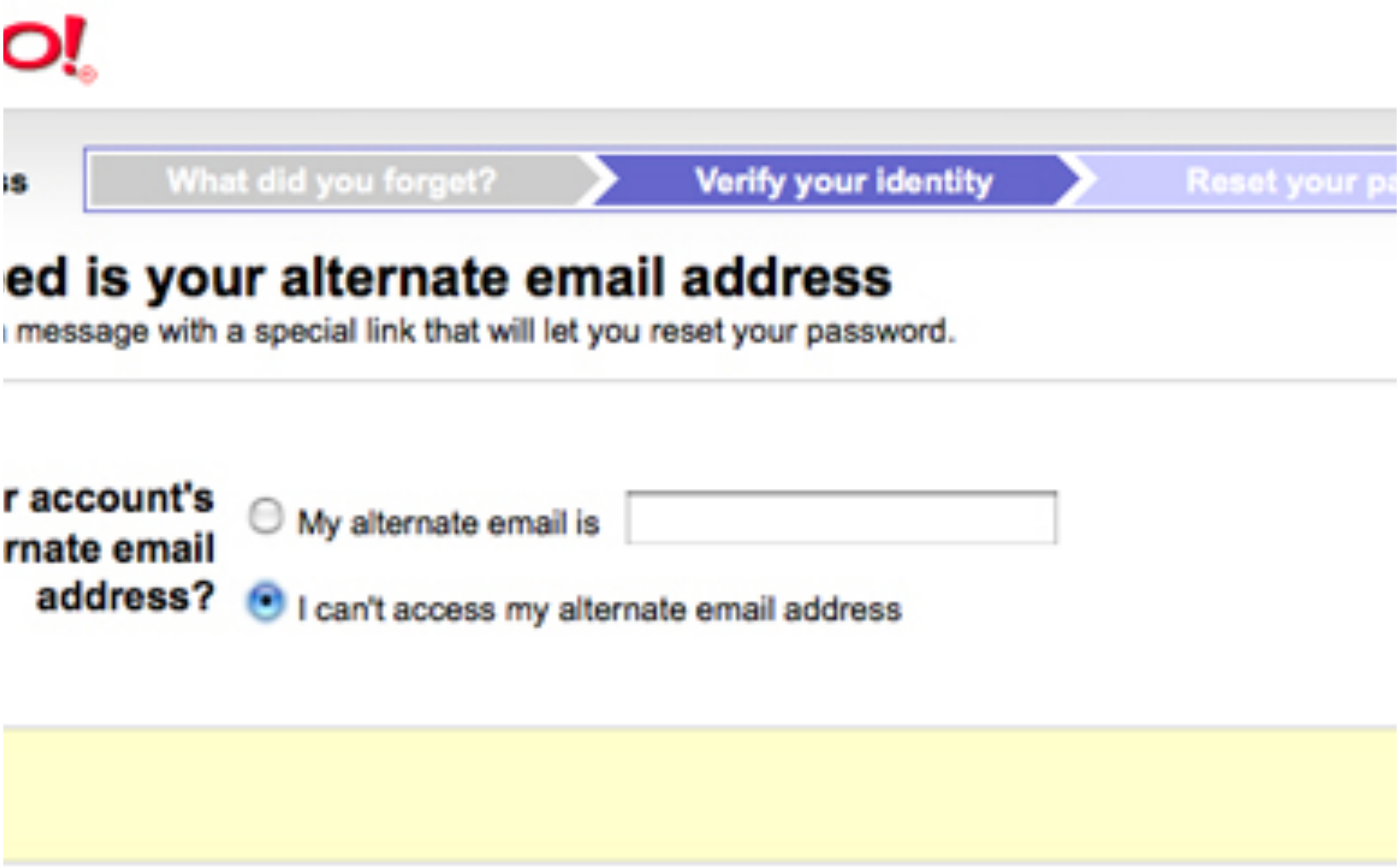
- The first Internet worm
- A grad student experimented (in the lab) with self-spreading malware
- It got out.
- And took down the Internet.

- There is a lesson here.

Epic Hack: Sarah Palin

- Guy wants to mess with Sarah Palin’s campaign
- Tries logging into her Yahoo Mail account, sees her security questions…

Epic Hack: Sarah Palin



ed is your alternate email address

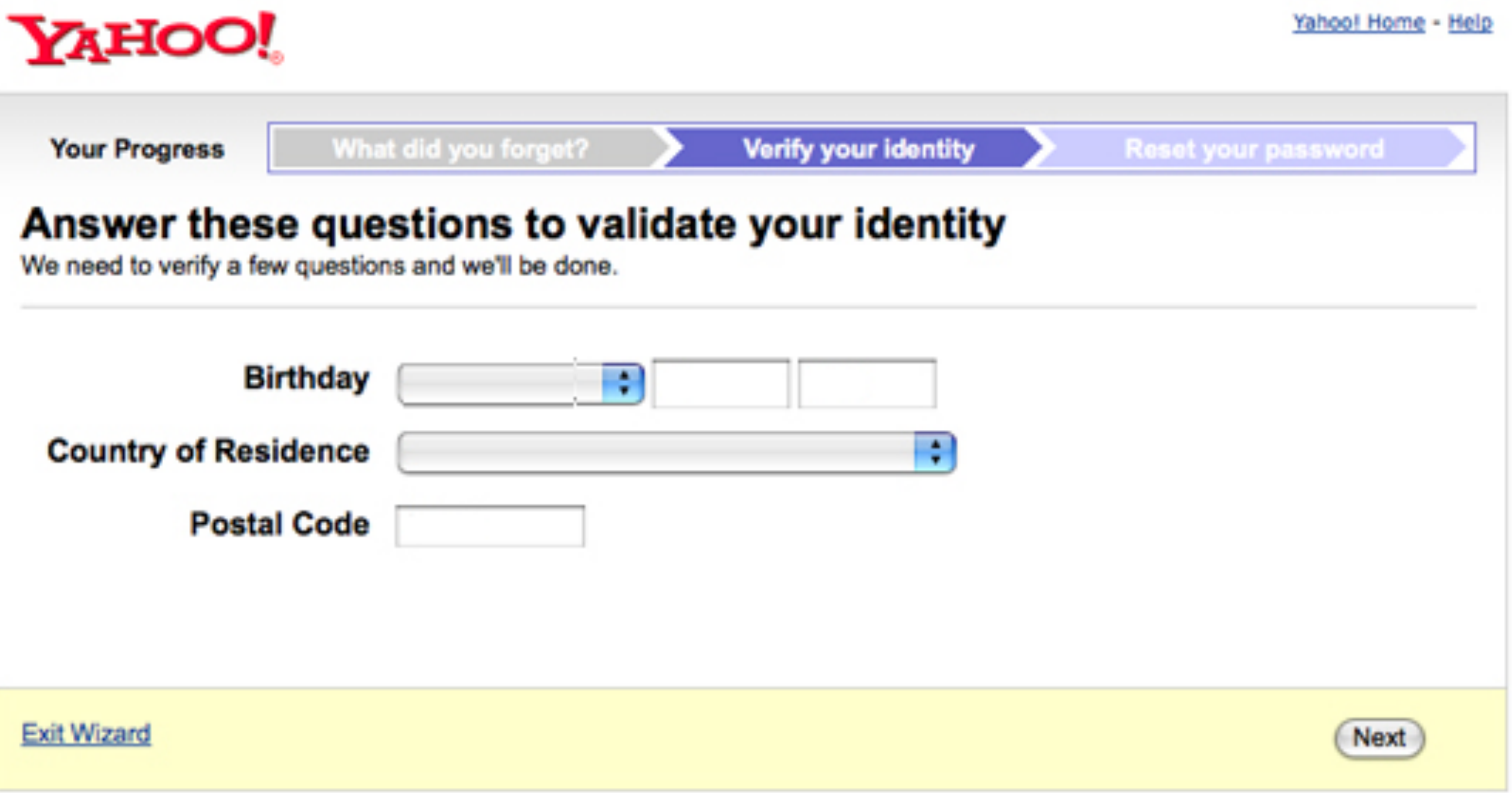
message with a special link that will let you reset your password.

r account's rnate email address?

○ My alternate email is

● I can't access my alternate email address

Epic Hack: Sarah Palin



Your Progress

What did you forget? | Verify your identity | Reset your password

Answer these questions to validate your identity

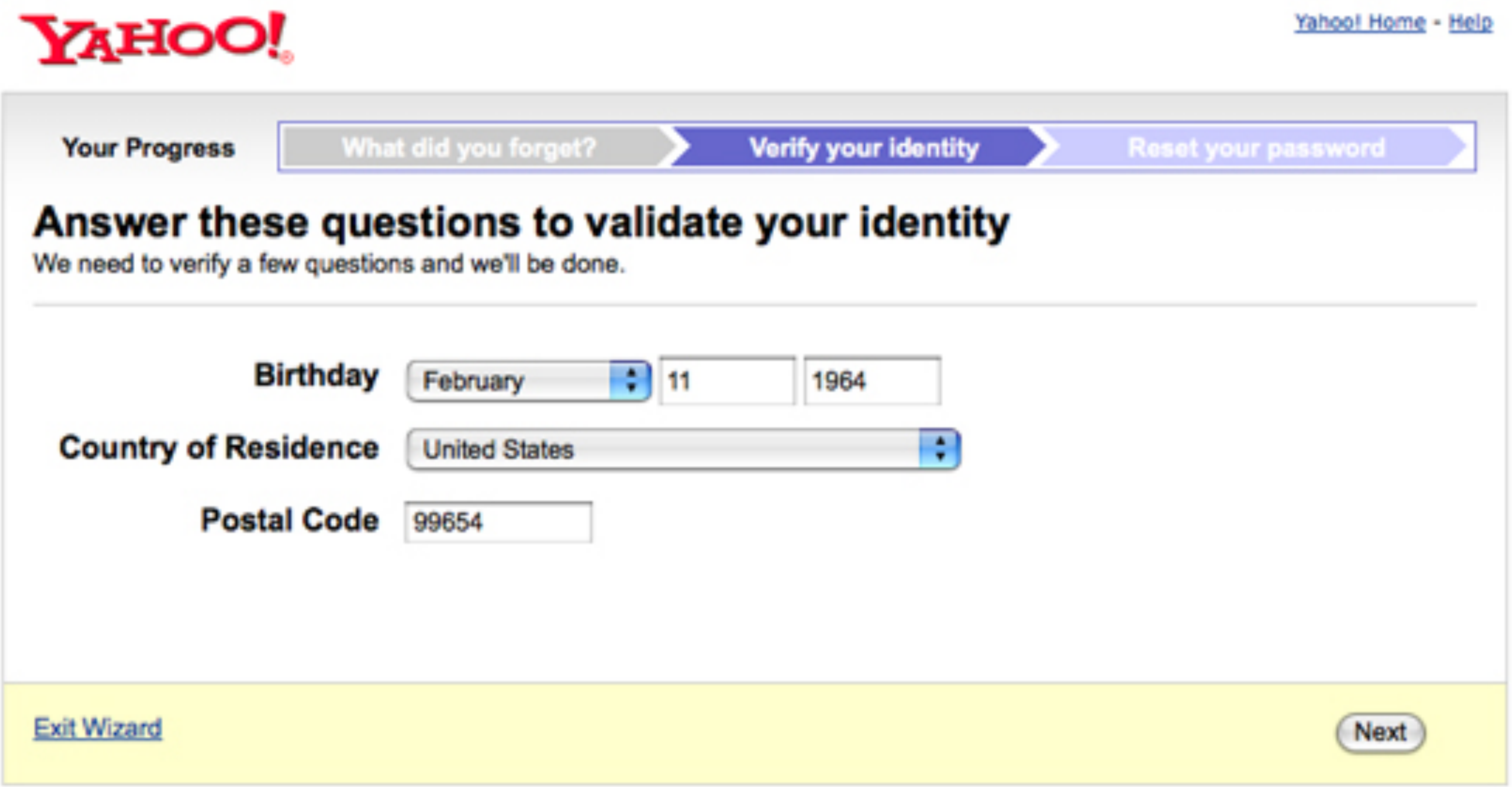
We need to verify a few questions and we'll be done.

Birthday

Country of Residence

Postal Code

Epic Hack: Sarah Palin

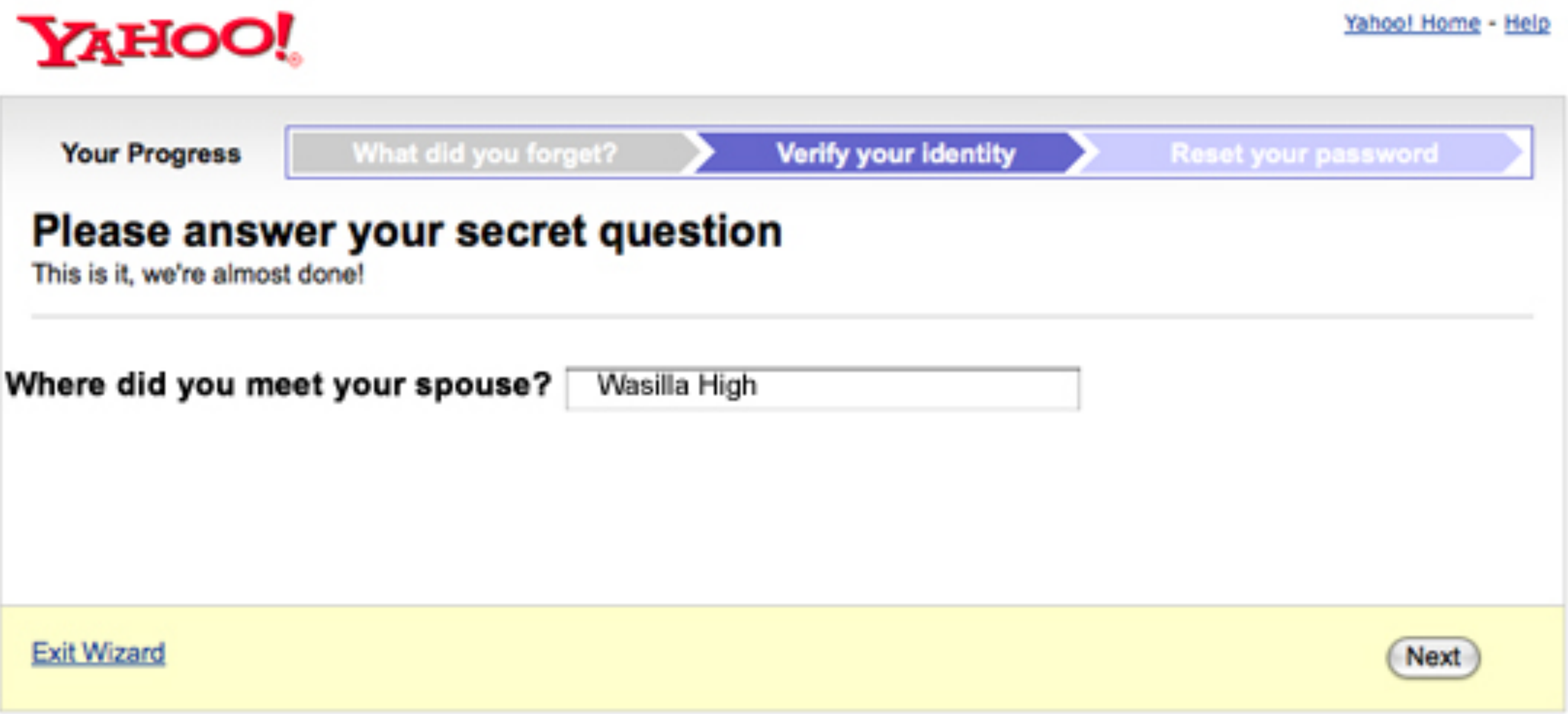


Answer these questions to validate your identity

We need to verify a few questions and we'll be done.

Birthday	February	11	1964
Country of Residence	United States		
Postal Code	99654		

Epic Hack: Sarah Palin

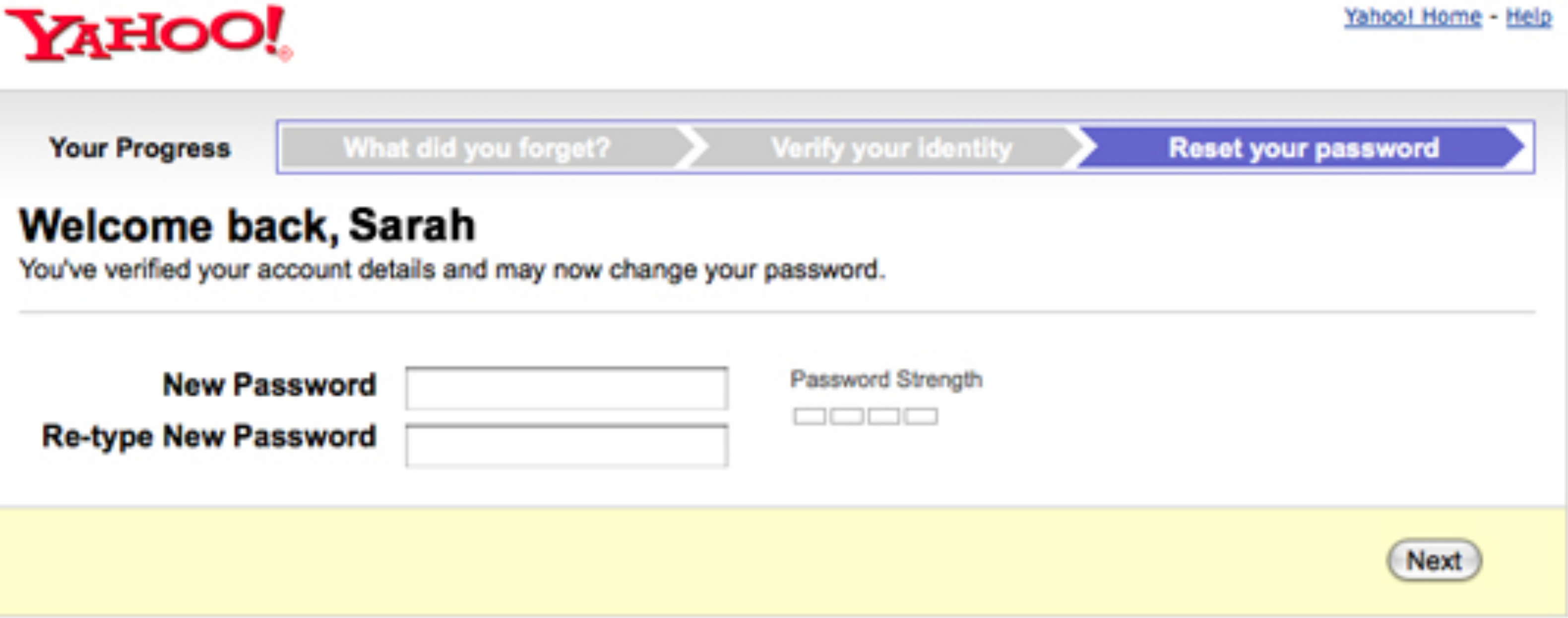


Please answer your secret question

This is it, we're almost done!

Where did you meet your spouse? Wasilla High

Epic Hack: Sarah Palin



Yahoo! Home - Help

Your Progress

What did you forget? Verify your identity Reset your password

Welcome back, Sarah

You've verified your account details and may now change your password.

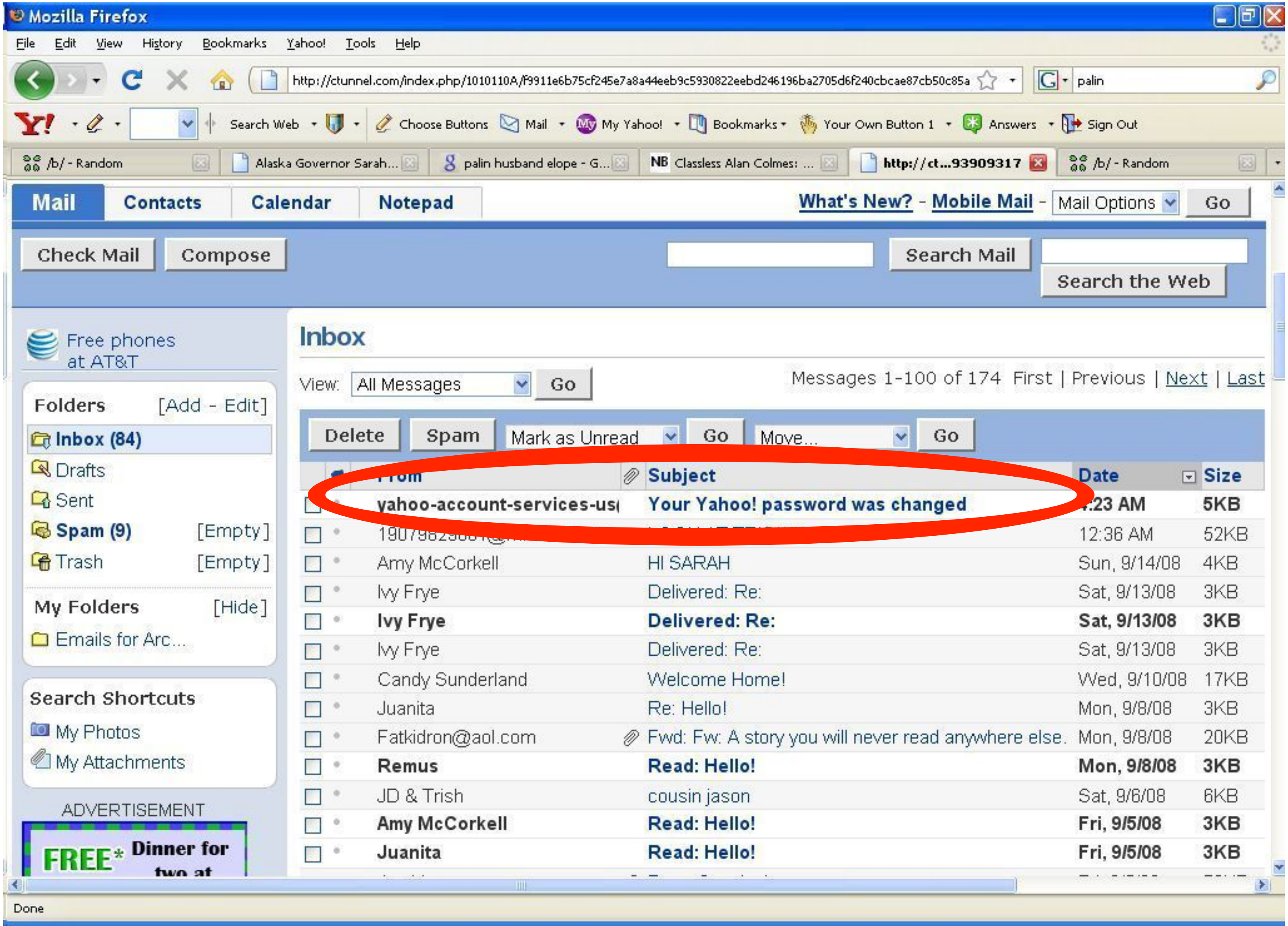
New Password

Re-type New Password

Password Strength

Next

Epic Hack: Sarah Palin



Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://ctunnel.com/index.php/1010110A/f9911e6b75cf245e7a8a44eeb9c5930822eebd246196ba2705d6f240cbcae87cb50c85a
palin
Search Web Choose Buttons Mail My Yahoo! Bookmarks Your Own Button 1 Answers Sign Out
/b/ - Random
Alaska Governor Sarah...
palin husband elope - G...
Classless Alan Colmes: ...
http://ct...93909317
/b/ - Random
Mail Contacts Calendar Notepad
What's New? - Mobile Mail - Mail Options Go
Check Mail Compose
Search Mail
Search the Web
Free phones at AT&T
Folders [Add - Edit]
Inbox (84)
Drafts
Sent
Spam (9) [Empty]
Trash [Empty]
My Folders [Hide]
Emails for Arc...
Search Shortcuts
My Photos
My Attachments
ADVERTISEMENT
FREE* Dinner for two at
Done

Inbox

View: All Messages Go

Messages 1-100 of 174 First | Previous | Next | Last

Delete Spam Mark as Unread Go Move... Go

	From	Subject	Date	Size
□	**yahoo-account-services-us**	**Your Yahoo! password was changed**	**[illegible]:23 AM**	**5KB**
□	190798[illegible]	[illegible]	12:36 AM	52KB
□	Amy McCorkell	HI SARAH	Sun, 9/14/08	4KB
□	Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
□	**Ivy Frye**	**Delivered: Re:**	**Sat, 9/13/08**	**3KB**
□	Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
□	Candy Sunderland	Welcome Home!	Wed, 9/10/08	17KB
□	Juanita	Re: Hello!	Mon, 9/8/08	3KB
□	Fatkidron@aol.com	Fwd: Fw: A story you will never read anywhere else.	Mon, 9/8/08	20KB
□	**Remus**	**Read: Hello!**	**Mon, 9/8/08**	**3KB**
□	JD & Trish	cousin jason	Sat, 9/6/08	6KB
□	**Amy McCorkell**	**Read: Hello!**	**Fri, 9/5/08**	**3KB**
□	**Juanita**	**Read: Hello!**	**Fri, 9/5/08**	**3KB**

Epic Hack: Sarah Palin

- Sentenced to 1 year in federal prison

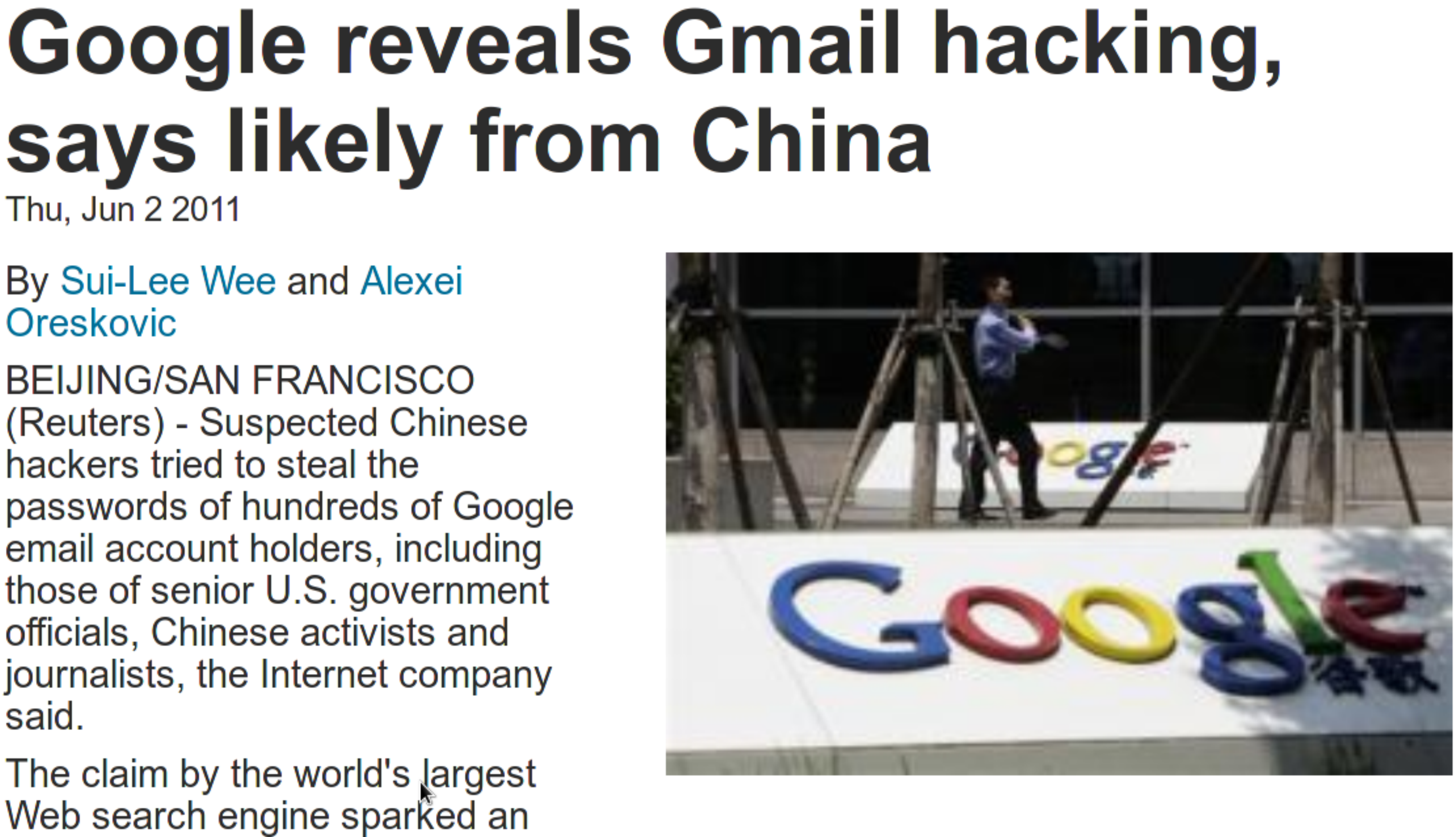
Epic Hack: Sarah Palin

- Aftermath: in 2012, someone hacks Mitt Romney’s email account

Epic Hack: Sarah Palin

- Aftermath: in 2012, someone hacks Mitt Romney’s email account
- … by guessing the name of his pet dog

Epic Hack: Google



Google reveals Gmail hacking, says likely from China

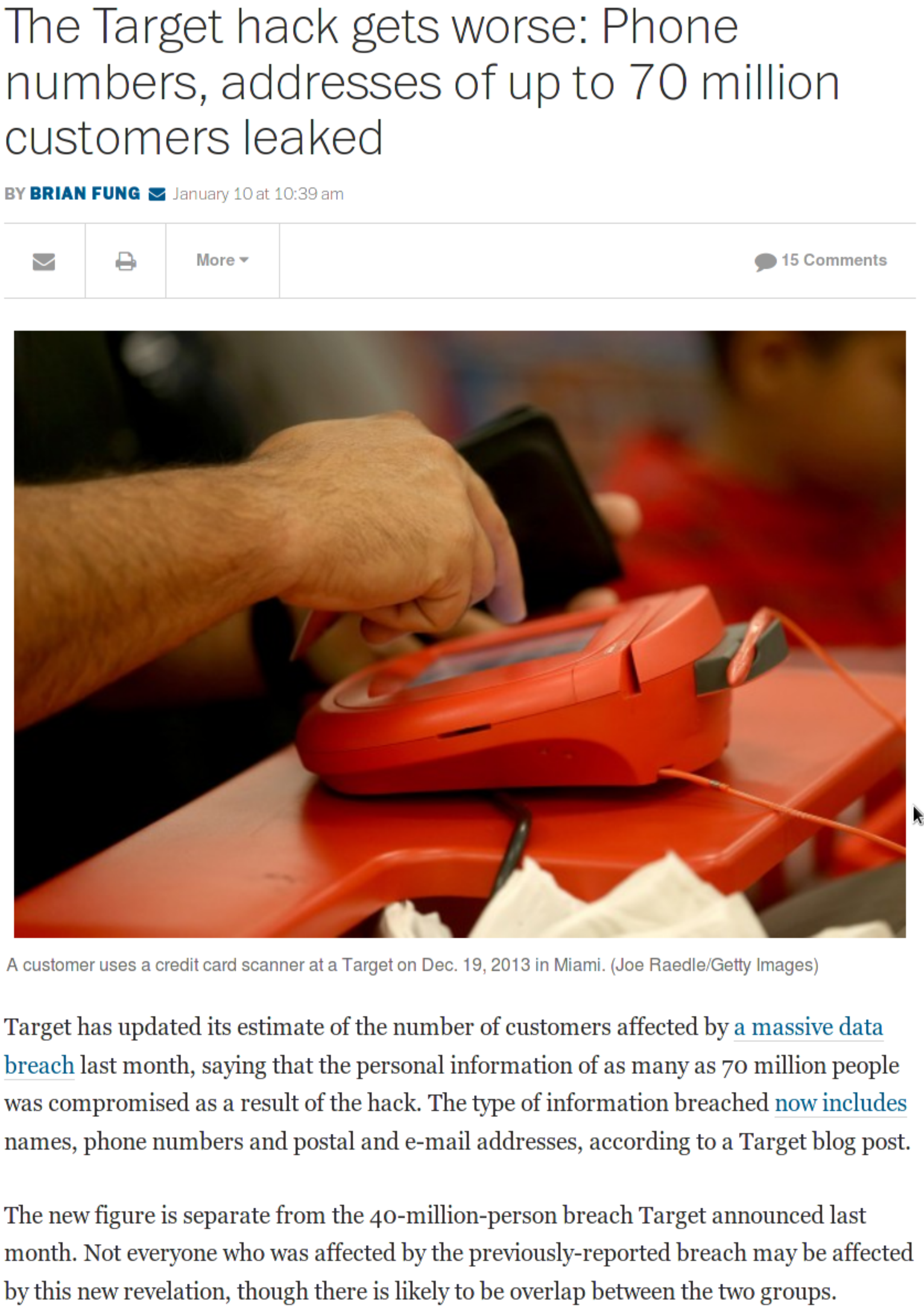
Thu, Jun 2 2011

By Sui-Lee Wee and Alexei Oreskovic

BEIJING/SAN FRANCISCO (Reuters) - Suspected Chinese hackers tried to steal the passwords of hundreds of Google email account holders, including those of senior U.S. government officials, Chinese activists and journalists, the Internet company said.

The claim by the world's largest Web search engine sparked an

Epic Hack: Target



The Target hack gets worse: Phone numbers, addresses of up to 70 million customers leaked

BY **BRIAN FUNG** ✉ January 10 at 10:39 am

A customer uses a credit card scanner at a Target on Dec. 19, 2013 in Miami. (Joe Raedle/Getty Images)

Target has updated its estimate of the number of customers affected by a massive data breach last month, saying that the personal information of as many as 70 million people was compromised as a result of the hack. The type of information breached now includes names, phone numbers and postal and e-mail addresses, according to a Target blog post.

The new figure is separate from the 40-million-person breach Target announced last month. Not everyone who was affected by the previously-reported breach may be affected by this new revelation, though there is likely to be overlap between the two groups.

Questions?

Coming Up …

- Friday’s lecture: *Buffer overflows, memory safety, and more*
- Join Piazza
- Get your class account online

BONUS FOR THE BORED

Epic Hack: Prisoner’s Dilemma

- You and a conspirator are arrested. Do you stay silent (“cooperate”), or rat out your conspirator (“defect”)?

	B: Cooperate	B: De
A: Cooperate	-1, -1	-3, 0
A: Defect	0, -3	-2, -2

What would your strategy be?

- Competition: Submit a program to play prisoner’s dilemma. Submit multiple entries, if you like. Tournament held to play off entries against each other.