CS 161: Computer Security

Prof. David Wagner

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

January 22, 2014

First off

- Can I have a volunteer, please?

THE CS161 EPIC HACK CONTEST

Featuring:

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: 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

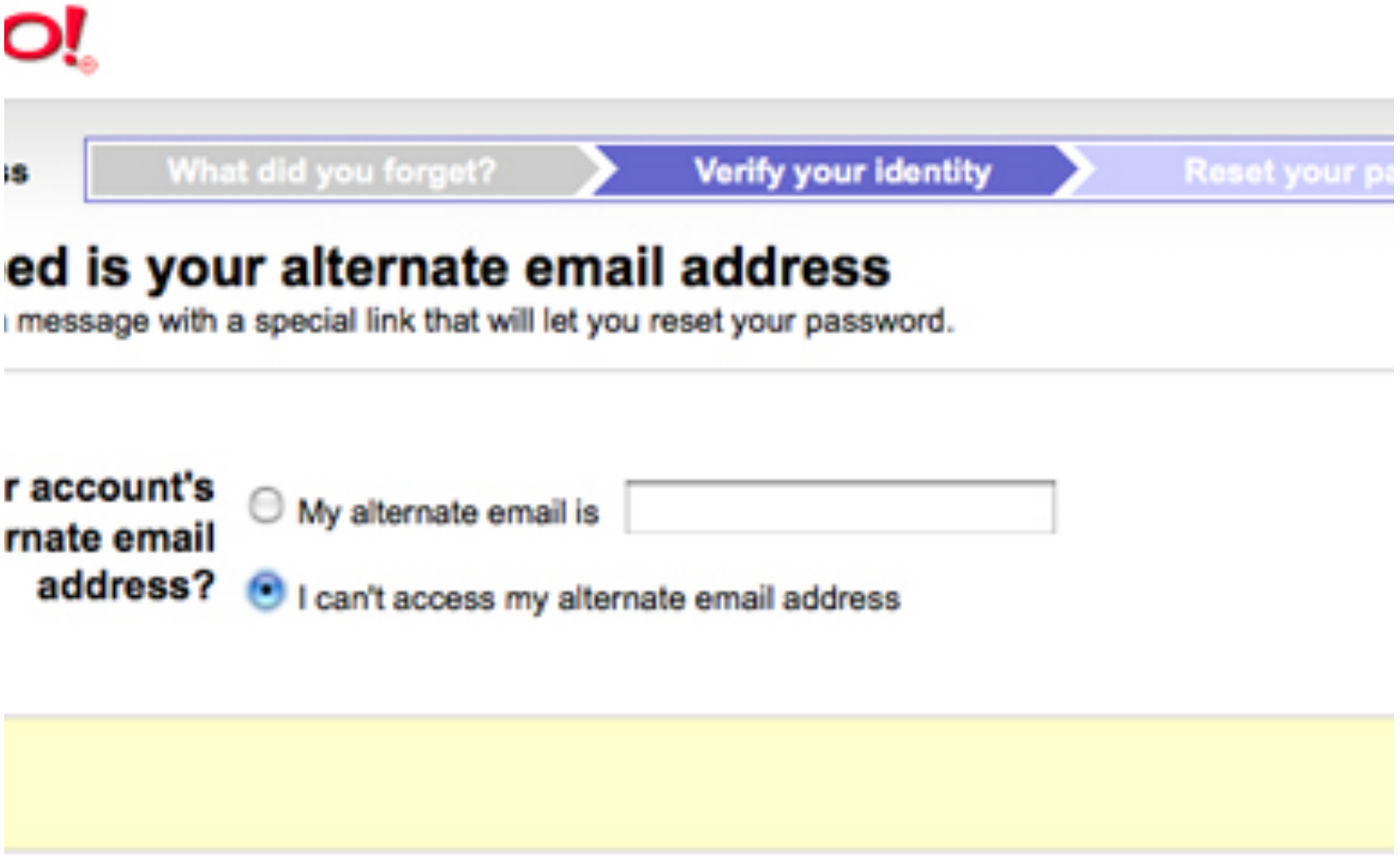
What would your strategy be?

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

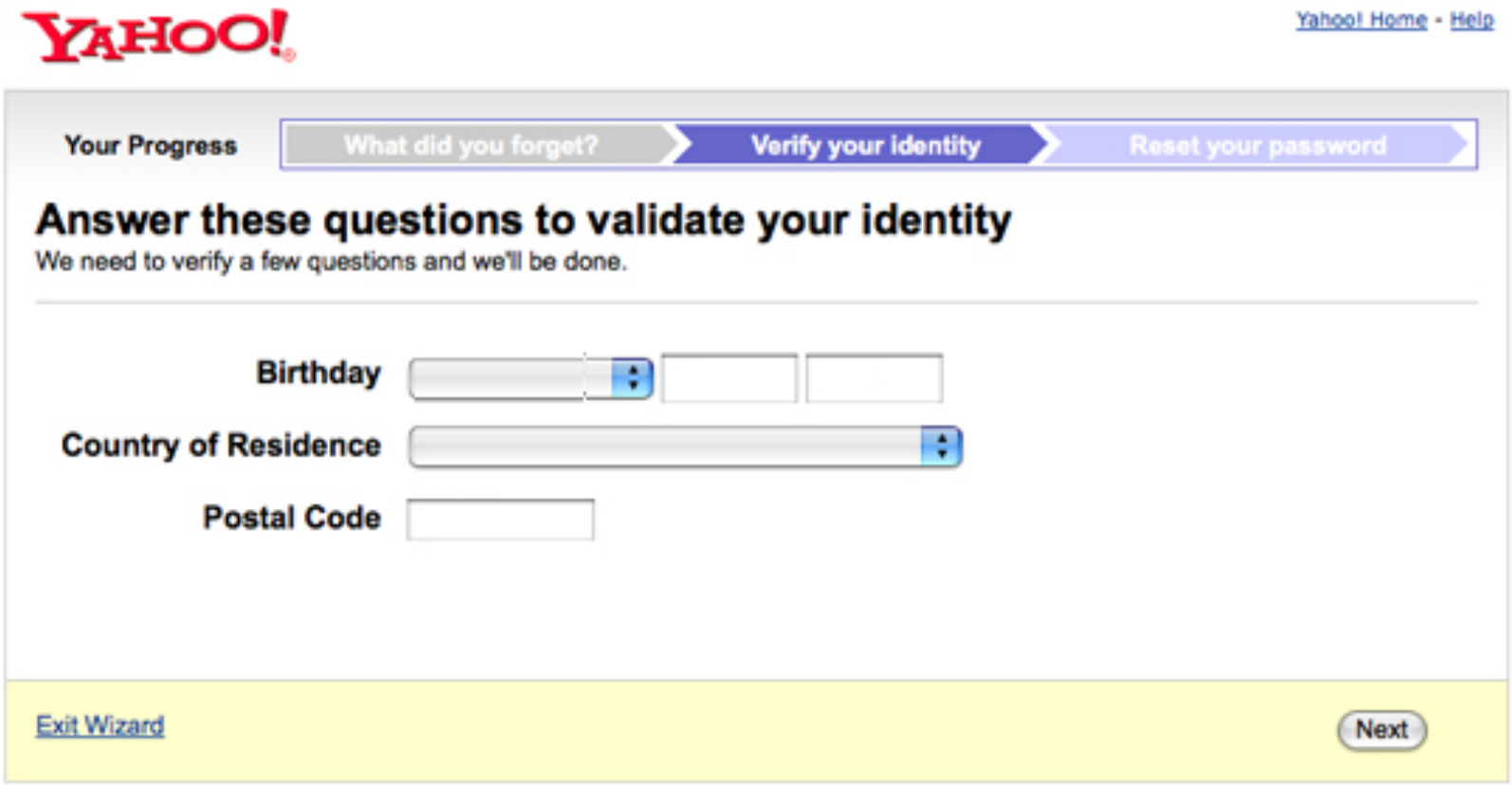
Epic Hack: Sarah Palin

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

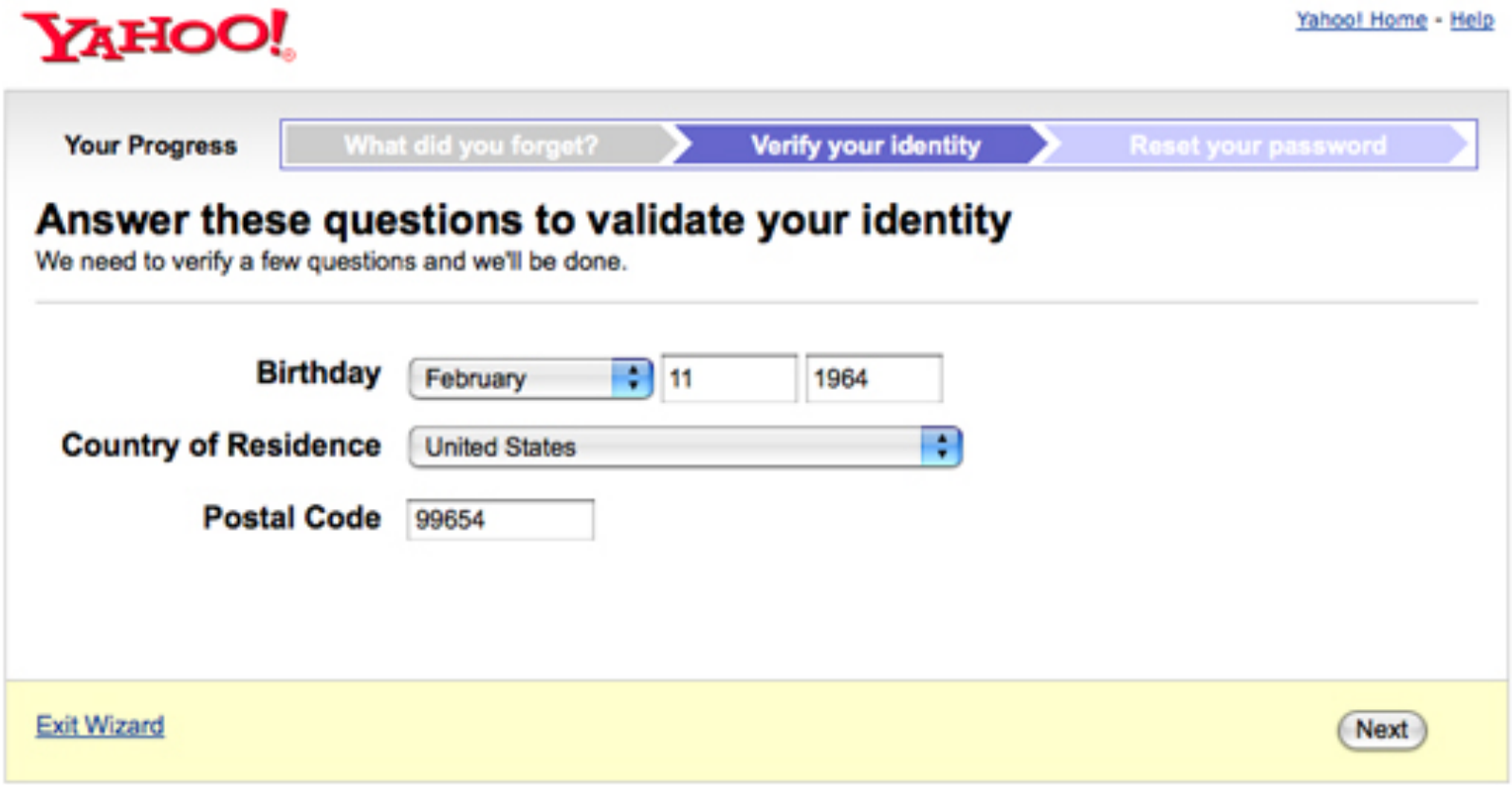
Epic Hack: Sarah Palin



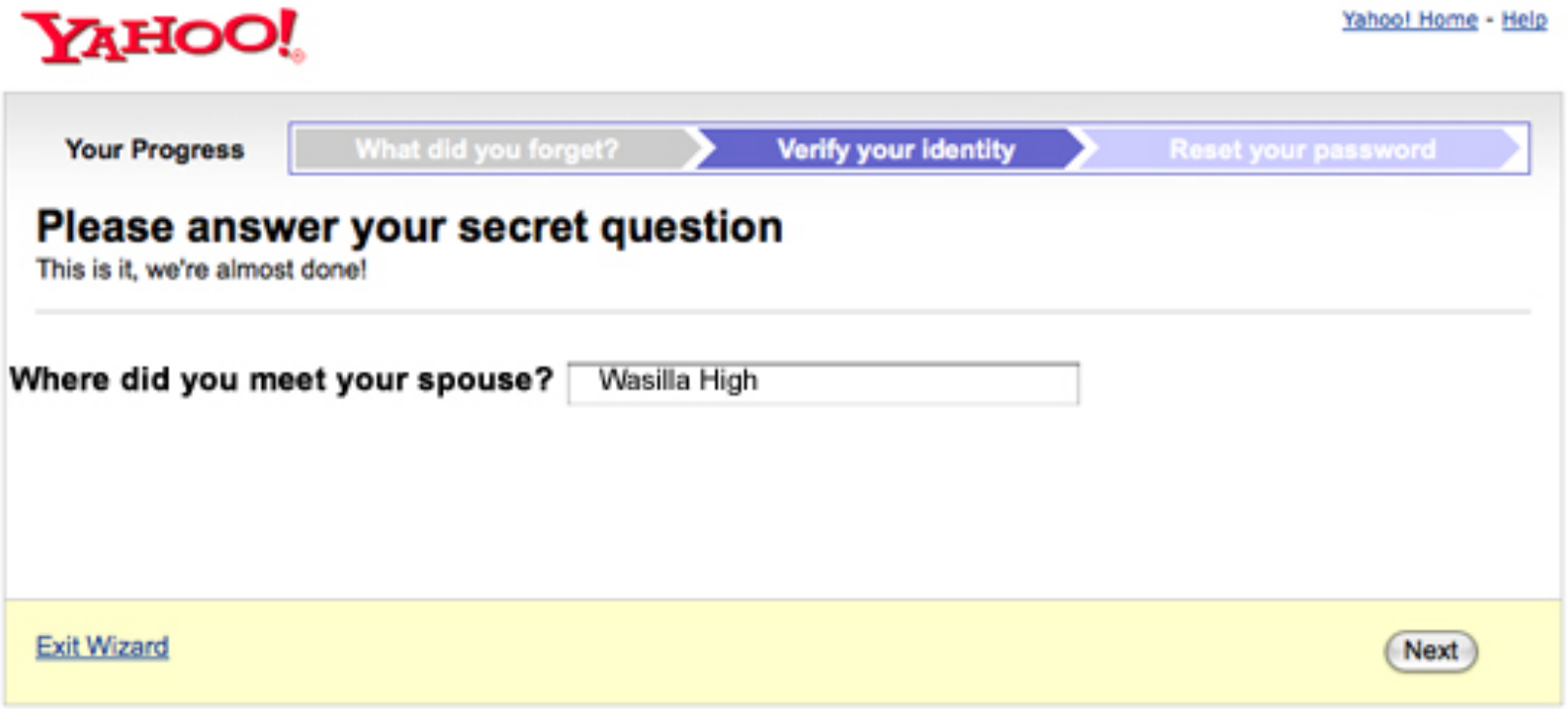
Epic Hack: Sarah Palin



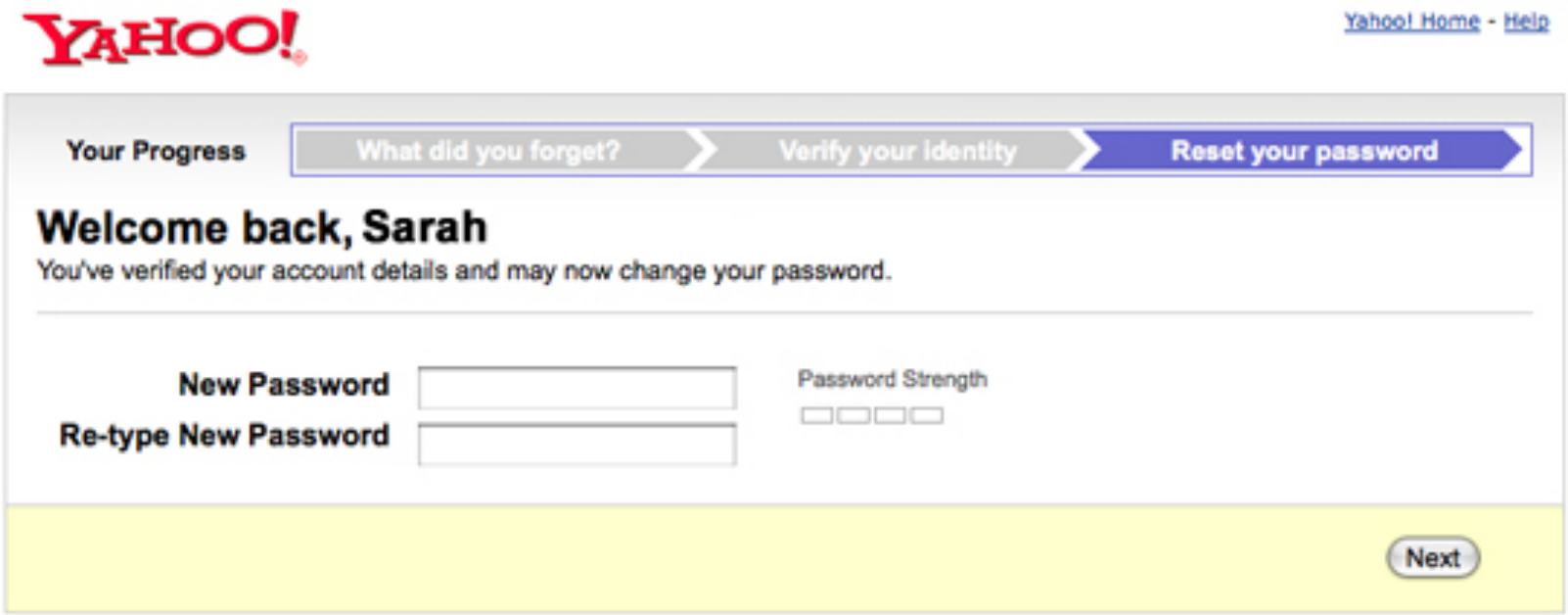
Epic Hack: Sarah Palin



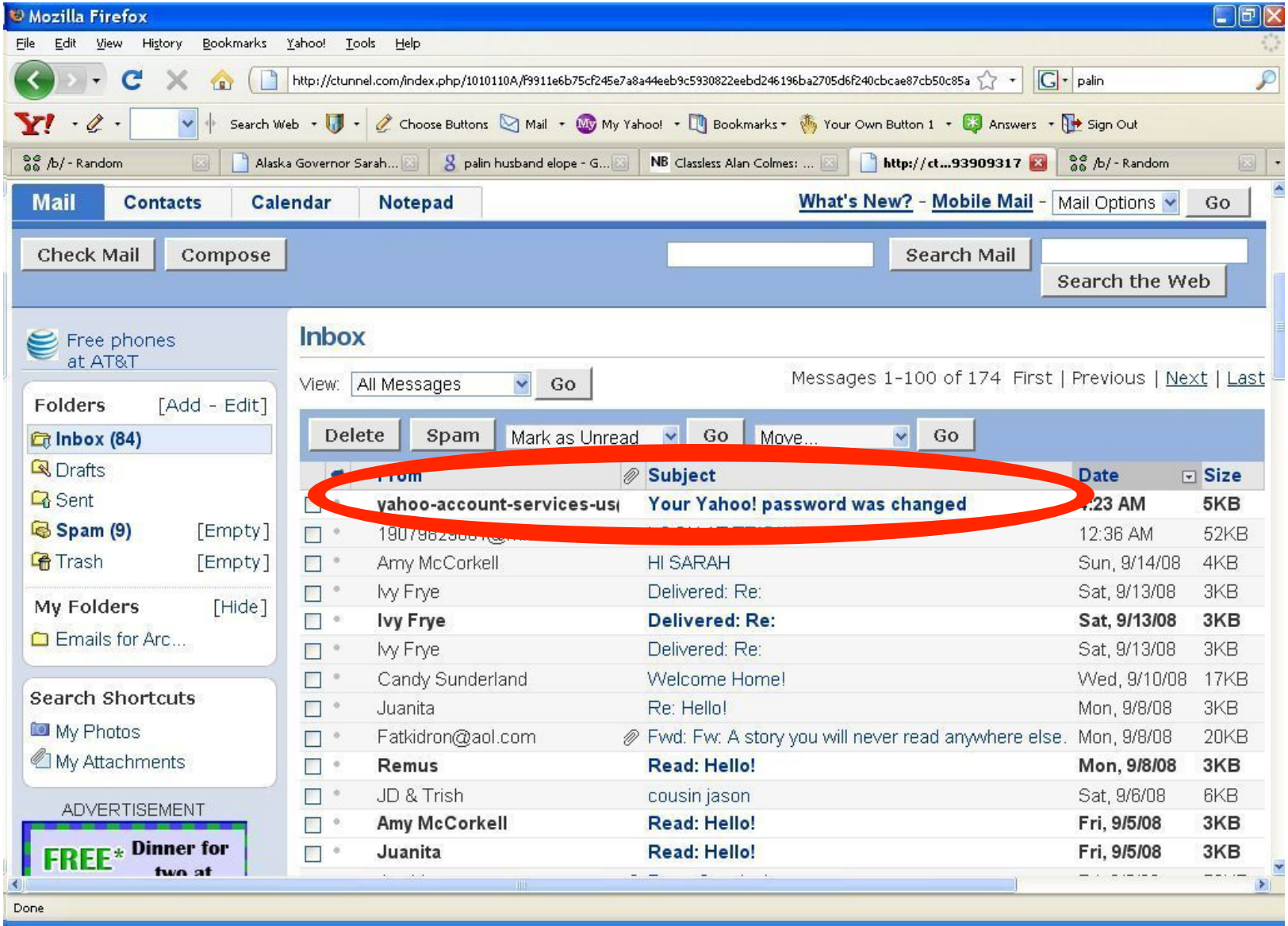
Epic Hack: Sarah Palin



Epic Hack: Sarah Palin



Epic Hack: Sarah Palin



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

More 15 Comments

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.

Let’s step back…

- Why am I showing you this?

LOGISTICS

Course Size

- The course has a capacity (= TAs) of 384 students …
- … with many more on the waiting list
  - (preference to graduating CS/EECS majors)

- *We do not have sufficient resources available to expand further*
  - If you're enrolled & decide not to take it, please drop ASAP
  - FYI, CS 161 scheduled for teaching in Fall 2014

Course Structure

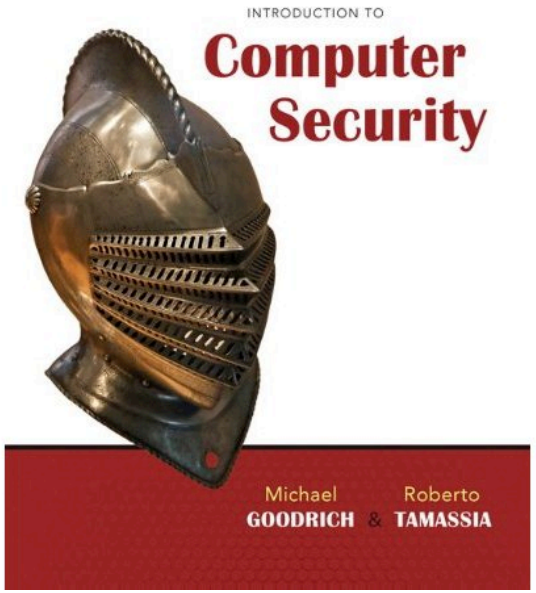
- Absorb material presented in lectures and section
- 3 course projects (24% total)
  - Done individually or in small groups
- ~4 homeworks (16% total)
  - Done individually
- Two midterms (30%)
  - Mon Feb 24 and Fri Apr 4, in class
- A comprehensive final exam (30%)
  - Wed May 14, 7-10pm

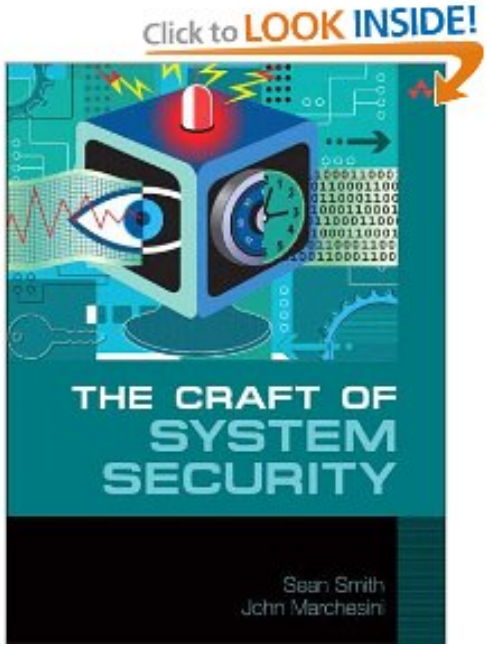
What's Required?

- Prerequisites:
  - CS 61B, 61C (= Java + C), 70
  - Familiarity with Unix
- Class accounts - pick up at end of lecture today
- Participate in Piazza
  - Send course-related questions/comments there, or ask in Prof/TA office hours
  - No email please: it doesn't scale

What's Not Required?

- *Optional But Recommended*: *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

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

- 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 …

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:

Modern Threats

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

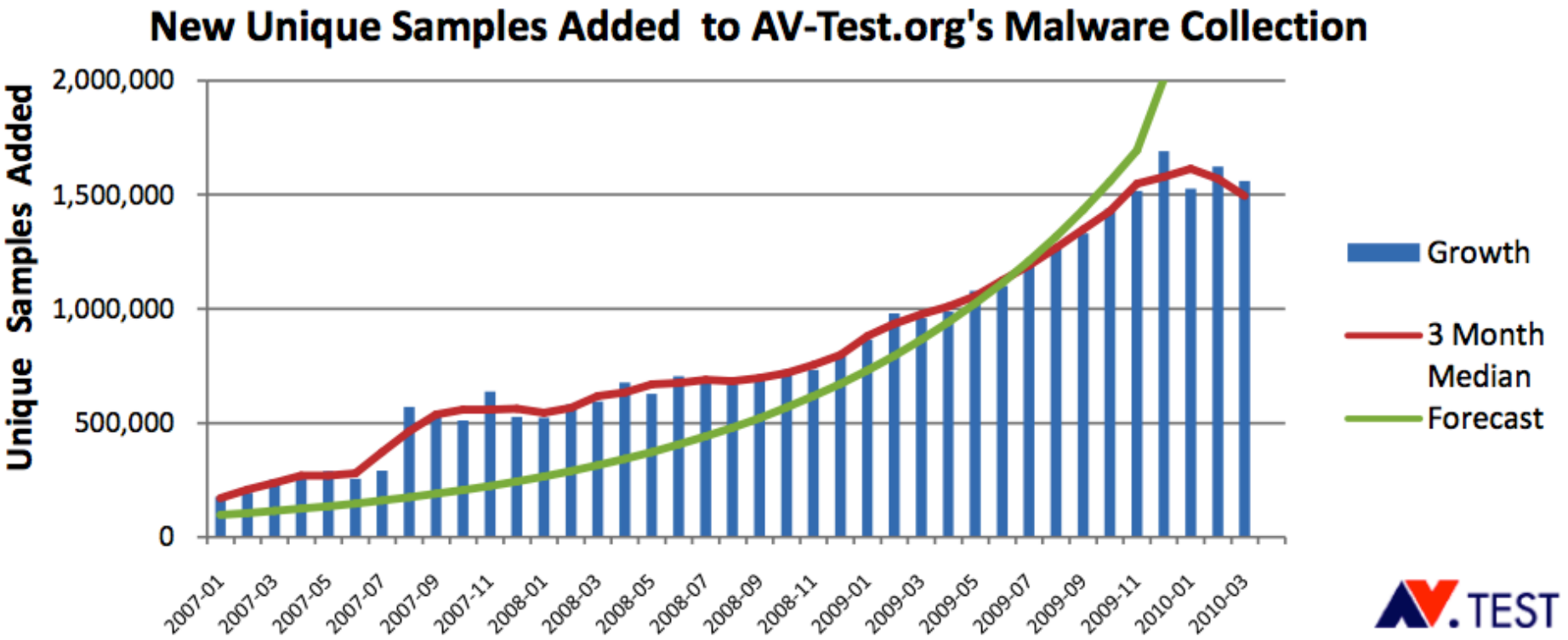

New Unique Samples Added to AV-Test.org's Malware Collection
Unique Samples Added
2,000,000
1,500,000
1,000,000
500,000
0
2007-01
2007-03
2007-05
2007-07
2007-09
2007-11
2008-01
2008-03
2008-05
2008-07
2008-09
2008-11
2009-01
2009-03
2009-05
2009-07
2009-09
2009-11
2010-01
2010-03
Growth
3 Month Median
Forecast
AV-TEST

Figure 20. The locations with the most computers reporting detections and removals by Microsoft desktop antimalware products in 1H12

	Country/Region	1Q12	2Q12	Chg. 1Q to 2Q
1	United States	9,407,423	12,474,127	32.6% ▲
2	Brazil	3,715,163	3,333,429	-10.3% ▼
3	Korea	2,137,136	2,820,641	32.0% ▲
4	Russia	2,580,673	2,510,591	-2.7% ▼
5	China	1,889,392	2,000,576	5.9% ▲
6	Turkey	1,924,387	1,911,837	-0.7% ▼
7	France	1,677,242	1,555,522	-7.3% ▼
8	United Kingdom	1,648,801	1,509,488	-8.4% ▼
9	Germany	1,544,774	1,486,309	-3.8% ▼
10	Italy	1,361,043	1,341,317	-1.4% ▼

Figure 29. Threat category prevalence worldwide and in the 10 locations with the most detections in 2Q12

Category	World	US	Brazil	Russia	France	Germany	China	Korea	Turkey	UK	Italy
Misc. Trojans	37.9%	43.6%	32.6%	41.8%	28.8%	35.0%	29.9%	23.6%	35.9%	43.2%	31.8%
Misc. Potentially Unwanted Software	32.2%	22.7%	38.1%	57.1%	29.3%	26.6%	45.0%	11.0%	31.2%	23.3%	29.4%
Worms	19.3%	12.3%	23.3%	16.4%	12.6%	8.8%	11.1%	4.9%	34.5%	6.6%	13.6%
Adware	18.5%	19.1%	7.5%	4.9%	31.5%	19.0%	22.4%	38.0%	24.6%	26.1%	24.1%
Trojan Downloaders & Droppers	16.4%	13.1%	22.4%	13.0%	16.1%	10.8%	12.6%	53.8%	13.0%	13.3%	23.2%
Exploits	14.8%	18.7%	5.8%	17.8%	16.2%	28.2%	10.3%	3.5%	6.4%	24.0%	19.7%
Viruses	7.8%	4.4%	9.1%	5.1%	2.2%	2.2%	10.6%	2.0%	15.0%	3.1%	2.5%
Password Stealers & Monitoring Tools	6.3%	4.6%	15.7%	4.1%	4.6%	10.7%	3.2%	2.6%	6.2%	4.8%	7.6%
Backdoors	4.2%	3.4%	3.9%	3.2%	2.8%	3.2%	5.9%	2.0%	4.2%	3.0%	2.9%
Spyware	0.2%	0.3%	0.1%	0.2%	0.1%	0.2%	1.3%	0.1%	0.0%	0.2%	0.1%

Totals for each location may exceed 100 percent because some computers reported threats from more than one category.

Microsoft finds malware on new computers in China

By RICHARD LARDNER | Associated Press – Thu, Sep 13, 2012

WASHINGTON (AP) — A customer in Shenzhen, China, took a new laptop out of its box and booted it up for the first time. But as the screen lit up, the computer began taking on a life of its own. The machine, triggered by a virus hidden in its hard drive, began searching across the Internet for another computer.

The laptop, supposedly in pristine, super-fast, direct-from-the-factory condition, had instantly become part of an illegal, global network capable of attacking websites, looting bank accounts and stealing personal data.

For years, online investigators have warned consumers about the dangers of opening or downloading emailed files from unknown or suspicious sources. Now, they say malicious software and computer code could be lurking on computers before the bubble wrap even comes off.

The shopper in this case was part of a team of Microsoft researchers in China investigating the sale of counterfeit software. They received a sudden introduction to malware called Nitol. The incident was revealed in court documents unsealed

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

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.

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 ►

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,

November 15, 2011, 2:26PM

Android Malware, Up 472 Percent, Seeing Fastest Growth Ever

by Christopher Brook

7 Comments

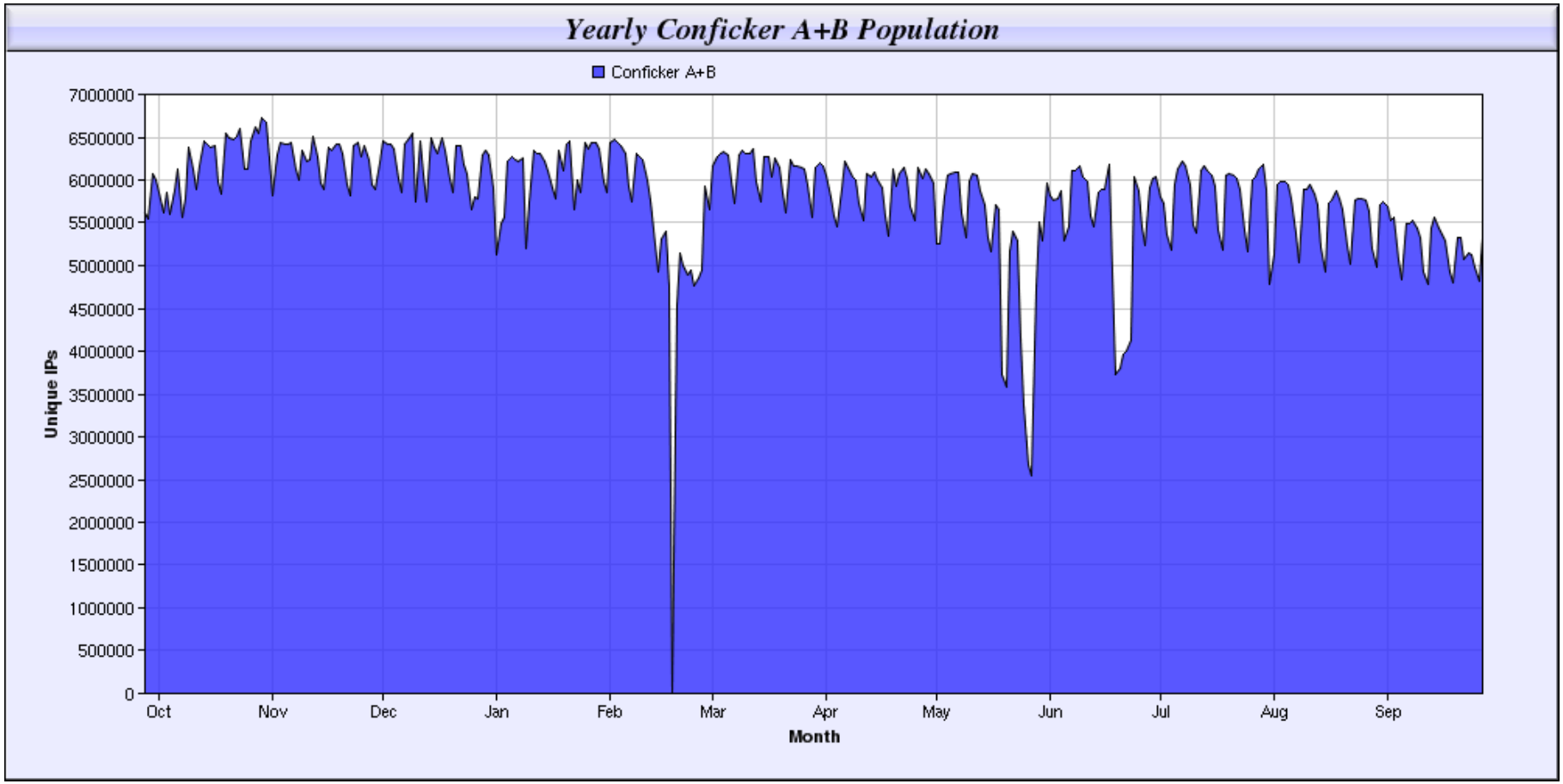
As Android market share has shot up in recent months, so has the volume of malware designed for the mobile platform. There's been a whopping 472 percent increase in Android malware samples in the last three months alone, according to research from Juniper Networks.

While September saw a 28 percent jump in malware samples, in particular, the numbers for the months of October and November are trending upwards and might translate into the fastest growth of Android malware the platform's ever seen. October's numbers spiked up to a 110 percent increase over September, a 171 percent increase from what was collected up to July of this year, the company said on its Global Threat Center blog.

Juniper's research found the bulk of Android malware is behaving one of two ways: 55 percent was disguised as spyware while 44 percent hijacked phones and utilized a SMS Trojan to send expensive messages without the user's knowledge.

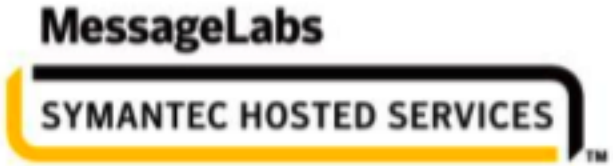
Modern Threats

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



Botnet Population: 2009 - 2010

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			



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

SEARCH THIS BLOG

Go

RECENT POSTS

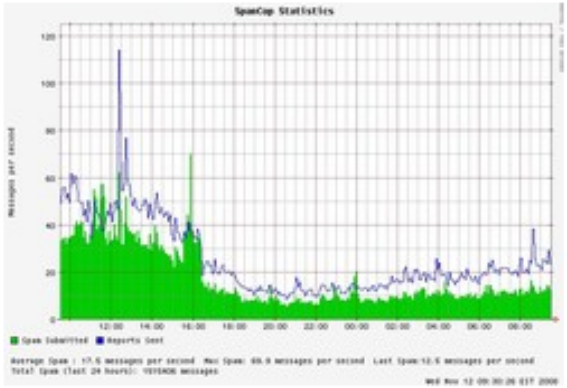
- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

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.)



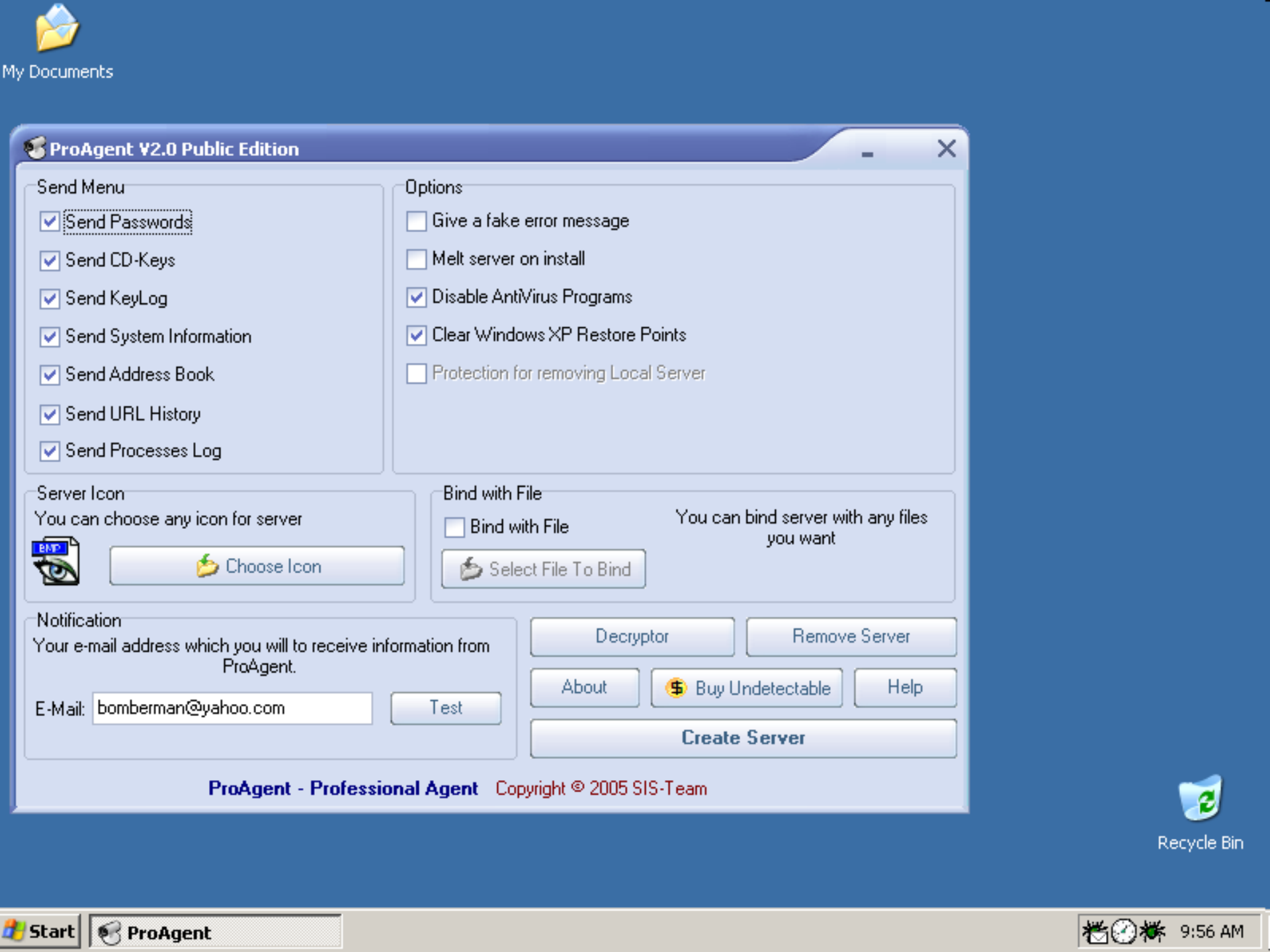
Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

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: bomberman@yahoo.com
Test
Decryptor
Remove Server
About
Buy Undetectable
Help
Create Server
ProAgent - Professional Agent
Copyright © 2005 SIS-Team
Recycle Bin
Start
ProAgent
9:56 AM

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

Список доступных акков

Сервис по продаже аккаунтов аукцыона eBay.

Добрые юзеры аукцыона 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.

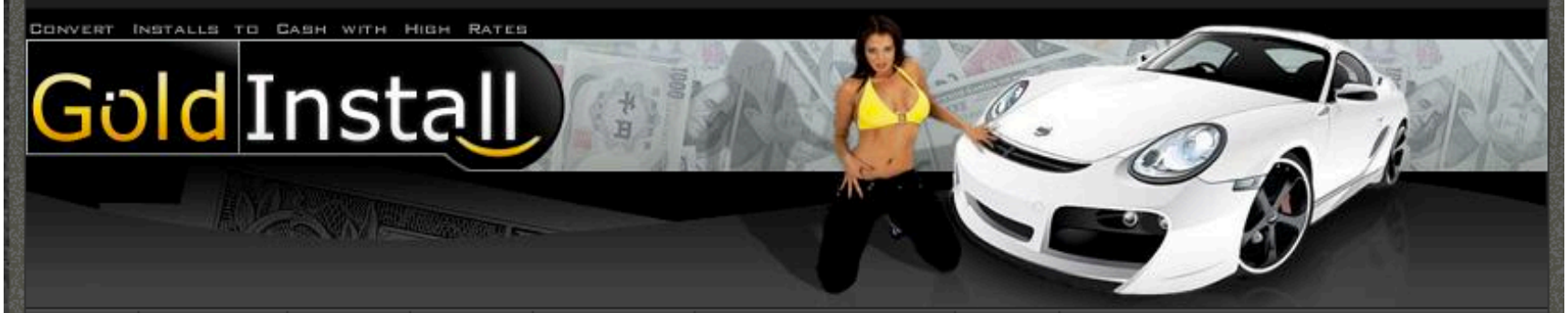
Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

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$

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$

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.

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.

Breach Subtotal

Breaches currently displayed:
Breach Types: DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN
Organization Types: BSO, BSF, BSR, EDU, GOV, MED, NGO
Years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013
606,810,255 Records in our database from.
3573 Breaches made public fitting this criteria

3549	26-Dec-12	Integris Health	MED	HACK	Oklahoma City	Oklahoma		Unknown		A team of cyber security consultants discovered vulnerabilitie
3550	28-Dec-12	East San Gabriel Valley R	GOV	DISC	West Covina	California		Unknown		A sensitive document was accidentally attached to an email t
3551	28-Dec-12	Gibson General Hospital	MED	PORT	Princeton	Indiana	29,000	29,000		The November 27 theft of a laptop may have resulted in the e
3552	28-Dec-12	Carewise Health, Hewlett	MED	HACK	Louisville	Kentucky		1,090 (unknown		An employee responded to a telephone computer phishing sca
3553	29-Dec-12	US Army Fort Monmouth	GOV	HACK	Oceanport	New Jersey	36,000	36,000	Those w	Hackers were able to access database information from Comm
3554	31-Dec-12	Sunview Vineyards Of Ca	BSR	PORT	Delano	California		Unknown		An office theft of an unencrypted laptop on or around Decem
3555	2-Jan-13	Rosenthal Collins Group	BSF	HACK	Chicago	Illinois		Unknown	Anyone	An unauthorized intrusion was detected on the morning of Tue
3556	2-Jan-13	Mid America Health, Inc.	MED	PORT	Greenwood	Indiana		Unknown	The loca	The theft of a laptop resulted in the exposure of patient infor
3557	2-Jan-13	Hospice of North Idaho (I	MED	PORT	Hayden	Idaho		441 (No	Read the	The June 2010 theft of an unencrypted laptop from an employ
3558	3-Jan-13	Mission Hospital, St. Jose	MED	PORT	Mission Lagun	California		Unknown		Someone called Mission Hospital on August 28, 2012 and clain
3559	3-Jan-13	King Drug & Home Care	MED	PORT	Owensboro	Kentucky	13,619	13,619		An employee reported that a portable hard drive was missing
3560	4-Jan-13	Reyes Beverage Group	BSR	DISC	Rosemont	Illinois		Unknown	Those w	A report containing the names and Social Security numbers of
3561	4-Jan-13	Healing Hearts	MED	INSD	Jacksonville	North Carolina		Unknown		The owner of a group of childcare services pleaded guilty to c
3562	6-Jan-13	Oldcastle APG, Inc.	BSR	PORT	Atlanta	Georgia	5,083	5,083		A laptop was stolen from an employee's car on or around Dec
3563	7-Jan-13	Centric Group, LLC	BSR	UNKN	St. Louis	Missouri		Unknown	It is not	Anyone who purchased items on www.accesscatalog.com usi
3564	7-Jan-13	Office of Dr. Calvin L. Sch	MED	STAT	Reedley	California		532 (No	Those w	A computer was stolen during an office burglary that occurred
3565	7-Jan-13	Woodwinds Hospital	MED	INSD	Woodbury	Minnesota		Unknown		An employee kept 200 pages of confidential information in an
3566	8-Jan-13	Morgan Road Middle Scho	EDU	PORT	Hephzibah	Georgia		Unknown		An unencrypted flash drive was stolen from a teacher's car. ¬
3567	8-Jan-13	Charlotte-Mecklenburg S	EDU	PHYS	Charlotte	North Carolina	80	80		An employee working in human resources was robbed while tra
3568	8-Jan-13	Texas Department of Hea	MED	INSD	Austin	Texas		Unknown		A dishonest employee was arrested on suspicion of misusing c
3569	10-Jan-13	City of Macon Georgia	GOV	STAT	Macon	Georgia		Unknown		A computer repair shop bought used computers on govdeals.c
3570	10-Jan-13	KTSU Texas Southern Un	EDU	INSD	Houston	Texas		Unknown		Texas Southern University's radio station KTSU gave a volunte
3571	10-Jan-13	Office of Dr. Sandra Buja	MED	PHYS	Aurora	Colorado		Unknown		Employees accidentally threw out hundreds of patient records
3572	11-Jan-13	EJ Phair Brewing Compan	BSR	HACK	Concord	California		Unknown		Customers who used credit or debit cards at EJ Phair discover
3573	17-Jan-13	St. Mark's Medical Cente	MED	HACK	La Grange	Texas	2,988	2,988		An employee's computer was found to contain malware. ¬†Th

Security

May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

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.

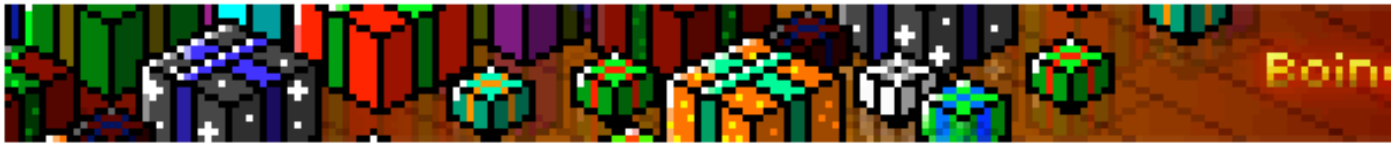
By David Talbot

THURSDAY, OCTOBER 15, 2009

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.

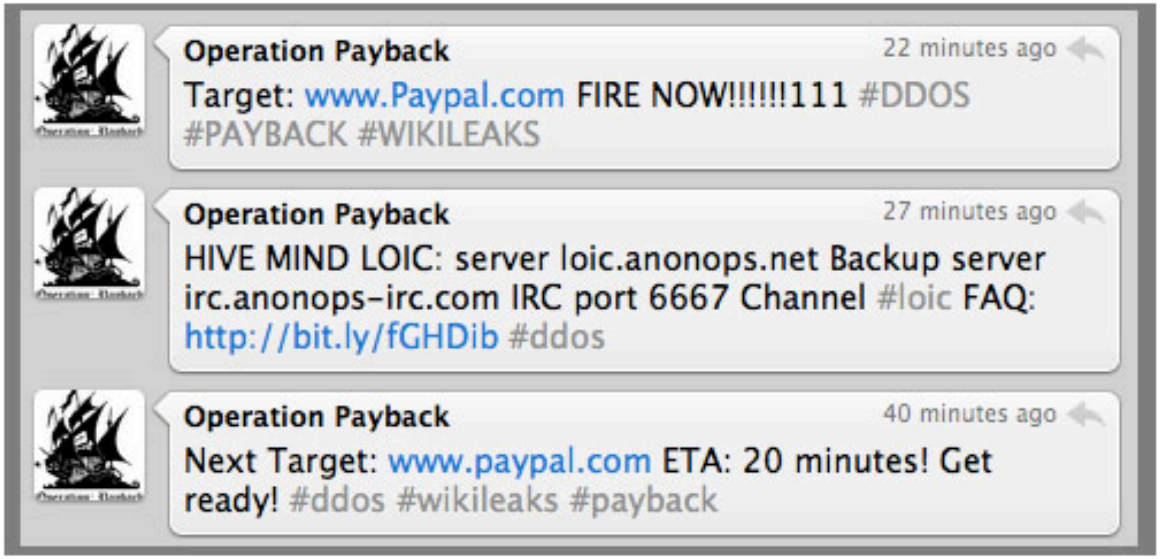
"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything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

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.

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

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

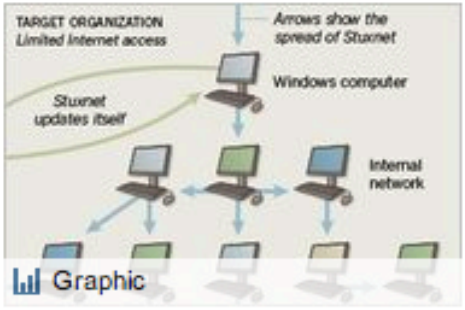
Ralph Langner, an independent computer security expert, solved Stuxnet.

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

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 | WORTHWHILE? +18 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

Mullen Offers 40-year Perspective on Social, Military Issues

By Karen Parrish
American Forces Press Service

WASHINGTON, Sept. 20, 2011 – As the last month ticks down in a career that began with his graduation from the U.S. Naval Academy in 1968, Navy Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, today offered his view of how war, peace, society and the world have changed over those 40-plus years.

He's seen some of the most significant military changes ever during his tenure as chairman, he told the audience gathered here at the Carnegie Endowment for International Peace.

Mullen Offers 40-year Perspective on Social, Military Issues

By Karen Parrish
American Forces Press Service

WASHINGTON, Sept. 20, 2011 – As the last month ticks down in a career that began with his graduation from the U.S. Naval Academy in 1968, Navy Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, today offered his view of how war, peace, society and the world have changed over those 40-plus years.

He's seen some of the most significant military changes ever during his tenure as chairman, he told the audience gathered here at the Carnegie Endowment for International Peace.

"I talk about two existential threats to the United States right now," he said. "One is obviously the nuclear weapons that exist in Russia; we think that we've got that well controlled inside the [current strategic arms reduction, or New START] treaty and inside the relationship."

The other is cyber attacks, which "I think … actually can bring us to our knees," he added.

The cyber threat has no boundaries or rules, and can issue from other nations, nongovernment actors – "You pick it," – but the danger it poses warrants a structure of doctrine and regulation like that used to control the nuclear threat, he said.

"We're a long way from that right now," he said.

Questions?

Coming Up …

- Friday's lecture: *Buffer overflows, memory safety, and more*
- Join Piazza
- HW0 due next Wednesday:
  - Get your class account set up
  - Use it to submit your solution to HW0

News Front Page

Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

England

Northern Ireland

Scotland

Wales

UK Politics

Education

Magazine

Business

Health

Science & Environment

Technology

Entertainment

Also in the news

Video and Audio

Programmes

Page last updated at 07:41 GMT, Tuesday, 2 February 2010

E-mail this to a friend

Printable version

Conficker virus hits Manchester Police computers

Greater Manchester Police (GMP) has been cut off from a national criminal database for more than three days because of a computer virus.

The virus can be spread through devices such as memory sticks

IT experts disconnected GMP from the Police National Computer (PNC) after finding the conficker virus on Friday.

It means officers have been asking neighbouring forces to carry out national checks on names and vehicles.

The conficker virus, a malicious worm, is believed to have infected up to 15 million computers around the world.

It was identified in the GMP system on Friday and quickly spread through the force, leading to the decision to cut off access to the PNC.

Assistant Chief Constable Dave Thompson said the virus was not destructive and no data had been lost.

COMBATING CONFICKER

- Microsoft offers bounty for worm creator
- Q&A: How do I protect myself?

BBC Manchester
Sport, travel, weat
to do, features and
more

SEE ALSO

- Conficker begins stealthy update
  09 Apr 09 | Technology
- Worm attack chaos fails to strike
  01 Apr 09 | Technology
- Microsoft bounty for worm creator
  13 Feb 09 | Technology

RELATED INTERNET LINKS

- Greater Manchester Police

The BBC is not responsible for the content
internet sites

TOP MANCHESTER STORIES

- Striker's daughter found hanged
- Rooneys face £4.3m legal action

Energizer Battery Charger Software Included Backdoor

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.