

Introduction

CS 161: Computer Security

Prof. Vern Paxson

TAs: Paul Bramsen, Apoorva Dornadula,
David Fifield, Mia Gil Epner, David Hahn, Warren He,
Grant Ho, Frank Li, Nathan Malkin, Mitar Milutinovic,
Rishabh Poddar, Rebecca Portnoff, Nate Wang

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

January 17, 2017

Course Size

- The course has reached its capacity (= room, TAs) of 481 students ...
- ... with many more on the waiting list
- *We do not have resources available to expand further*
 - If you're enrolled & decide not to take it, please drop ASAP

What is Computer Security?

- Keeping computing systems functioning as intended
 - Free of **abuse**
- Keeping data we care about accessed only as desired
- Securing **access** to our resources & capabilities
- Enabling privacy and anonymity
 - *if* these fit with our usage goals
- Doing all of this:
 - ... in the presence of an **adversary**
 - and on a **budget**

What Makes Security Challenging?

- Intelligent adversary can induce “**zero probability**” faults!
- Difficult to reason about our systems’ security
 - Blinded by abstractions; **attackers cheat!**
- An evolving field:
 - **Arms race** (“co-evolution”) ...
 - ... and computing itself keeps evolving
- **Asymmetries:**
 - Must defend everywhere; attacker **chooses** where to attack
 - Defenses are public, attacker tests/develops in private
 - Attackers are **nimble**; defenders have **sunk costs**

What Makes Security Challenging?, con't

- Minimal **deterrence**
 - Internet's flexibility hugely facilitates anonymity (if you're willing to break the law)
- Security comes with costs **\$\$\$** ...
 - Overhead
 - Time-to-market
- ... and you often don't see its benefits
 - Difficult to measure the gains, other than a **lack of disaster**

Some General Themes

- Computers do **precisely** what they're told
- **Code** is **data** & **data** is **code**
- Our lust for flexibility & features in our systems creates all sorts of vulnerabilities
- Our (very powerful) masking of the complexity of our systems leaves our users vulnerable due to **foggy “mental models”**
- Our general security goal is **risk management**, **not** bullet-proof protection

A Class Poll

- I'm going to make a statement and ask you to
 - (1) **discuss** it with a seatmate, and then
 - (2) **hum** in support of one of the following cases:
 - I think there's no chance of this.
 - I think there's a small possibility of this.
 - I think it's likely.
 - I think it's certain.
 - I don't know.
- Everyone should **hum** for (exactly) one of these.
- Then I'll ask **volunteers** from each case to explain their reasoning.
- *There Is No Right Or Wrong Answer*

Statement

- *While attending this lecture, your laptop / mobile device has been hacked into by the CS161 staff.*
- Time to **discuss** with your seatmate
- Time to **hum**:
 - I think there's no chance of this.
 - I think there's a small possibility of this.
 - I think it's likely.
 - I think it's certain.
 - I don't know.
- **Volunteers?**

Themes :

Trust

Ethics

Worrisome complexity

Threat model

What Will You Learn In This Class?

- How to **think adversarially** about computer systems
- How to **assess threats** for their significance
- How to build programs & systems w/ **robust security properties**
- How to gauge the protections / limitations provided by today's technology
- How attacks work in practice
 - **Code injection, logic errors, browser & web server vulnerabilities, network threats, social engineering**

What's Involved in the Learning?

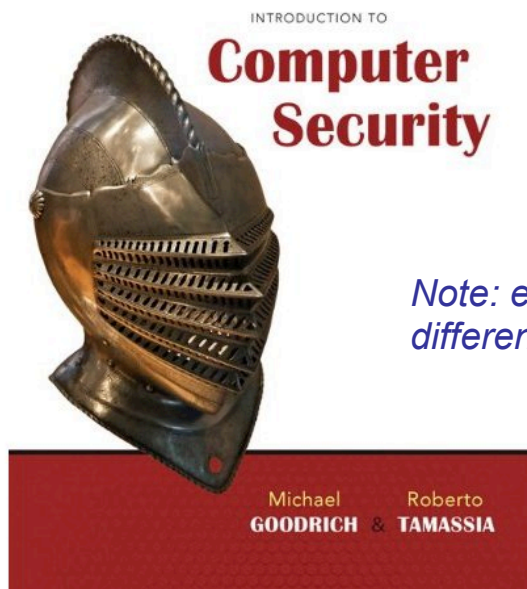
- Absorb material presented in lectures and section
- 2 or 3 course **projects** (24% total)
 - Done individually or in pairs
- ~4 **homeworks** (16% total)
 - Done individually
- Two **midterms** (30%)
 - 80 minutes long: Thu Feb 16 & Thu Mar 23
- A comprehensive **final** exam (30%)
 - Fri May 12, 11:30AM-2:30PM

What's Required?

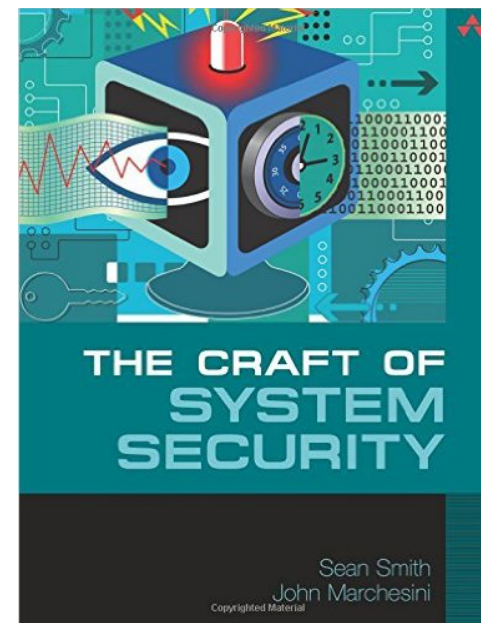
- Prerequisites:
 - CS 61B, 61C, 70
 - Familiarity with Unix, C, Java, Python
- Engage!
 - In lectures, in section
 - Note: I'm **hearing-impaired**; be prepared to repeat questions!
 - Feedback is highly valuable
- Class accounts – see course home page
- Participate in *Piazza* (use same name as glookup)
 - Send course-related questions/comments there, or ask in Prof/TA office hours
 - For private matters, contact Prof or TA using Piazza direct message
 - **Do not post specifics about problems/projects**

What's Not Required?

- *Optional: Introduction to Computer Security*, Goodrich & Tamassia
- *Optional: The Craft of System Security*, Smith & Marchesini.



Note: emphasis different in parts



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** (or with a single partner, if assignment states this).
- 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.

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**

Cheating

- While we will extensively study how attackers “cheat” to undermine their victims ...
- ... we treat cheating on coursework/exams very seriously
- Along with heavy sanctions (see class page) ...
- ... keep in mind that your instructors are all highly trained in **adversarial thinking!**

5 Minute Break

Questions Before We Proceed?

Threats evolve ...

- 1990's, early 2000's: **bragging rights**

Meet Mafiaboy, The 'Bratty Kid' Who Took Down The Internet

In 2000, a high school student named Michael Calce, who went by the online handle Mafiaboy, brought down the websites of Amazon, CNN, Dell, E*Trade, eBay, and Yahoo!. At the time, Yahoo! was the biggest search engine in the world.

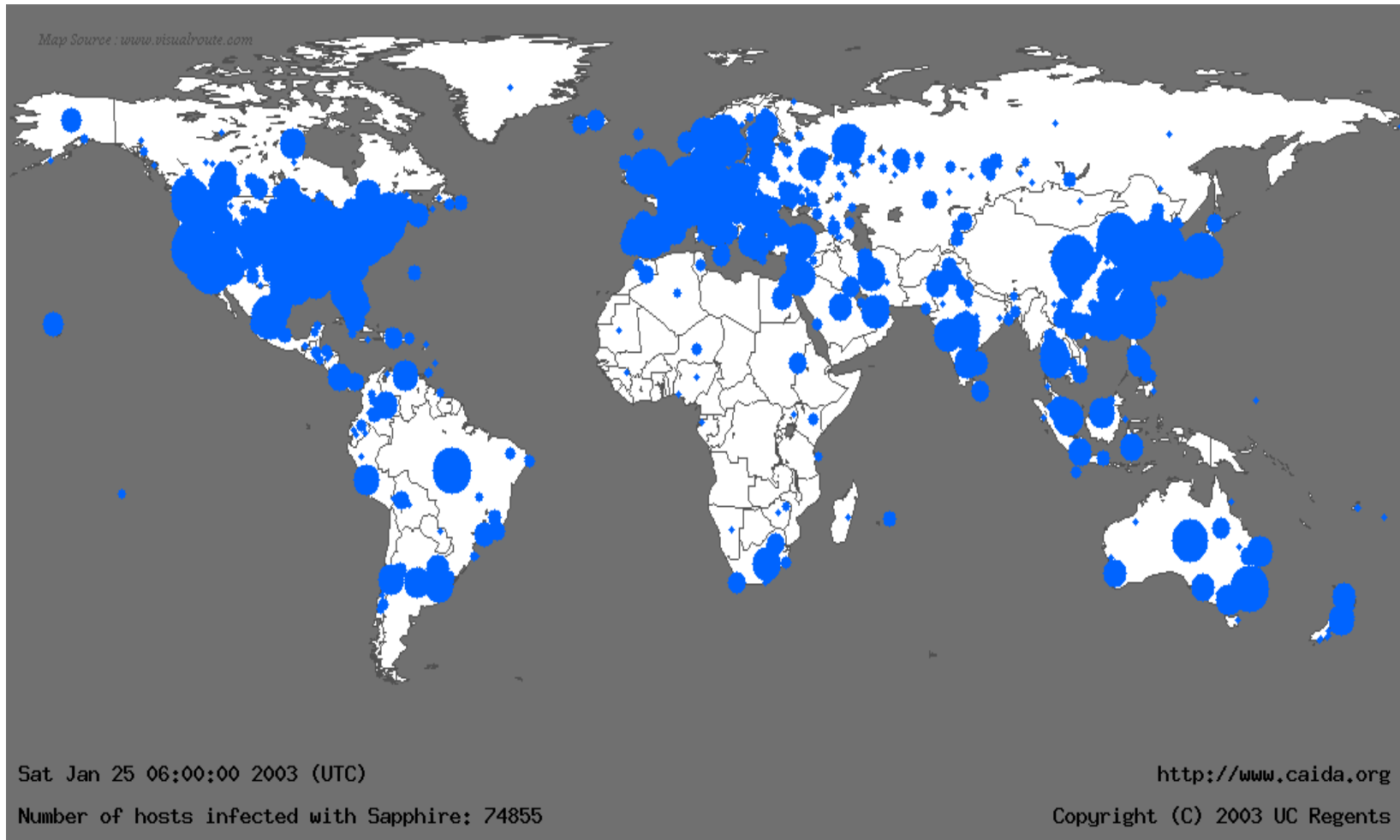


"The New York Stock Exchange, they were freaking out, because they were all investing in these e-commerce companies," he remembers.

"And then it's like, 'OK — a 15-year-old kid can shut us down at any point? Is our money really safe?' "



Slammer Worm Spreads Across Entire Internet in < 10 Minutes



Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated **cybercrime**
 - Spam, pharmaceuticals, credit card theft, identity theft
 - 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

BuyAcCs.com

СЕРВИС РЕГИСТРАЦИИ АККАУНТОВ

Наш магазин аккаунтов рад предложить аккаунты различных **почтовых служб** и **бесплатных хостингов** для любых задач. Вы получите аккаунты **СРАЗУ после оплаты** заказа через Webmoney.

Также доступна услуга залива редиректов на **Pochta.ru**, **Cwahi.net** и **0catch.com** что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ

[Мега Софт для дорвеев - Zerber](#)

[Одобрятел друзей - Мой мир](#)

[Twidium - безопасный и профессиональный инструмент для раскрутки твиттера накрутить фолловеров в Твиттер](#)

[Заработай на продаже аккаунтов](#)

[Купить аккаунты Одноклассников](#)

[Купить аккаунты Вконтакте](#)

Сейчас в продаже

Служба	Кол-во акков	Цена за 1К аккаунтов
Mail.ru	165685	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Mix	104014	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Mail.ru Second Hand	0	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Mail.ru Mix S/H	17892	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3
Yandex.ru	4055	до 10К: \$20 от 10К до 20К: \$19 от 20К: \$18
Narod.ru	5285	до 10К: \$50 от 10К до 20К: \$50 от 20К: \$50
Qip.ru (Pochta.ru)	0	до 10К: \$50 от 10К до 20К: \$50 от 20К: \$50
Hotmail.com	425227	до 10К: \$5 от 10К до 20К: \$4.5 от 20К: \$4
Hotmail.com Plus	505448	до 10К: \$6 от 10К до 20К: \$5.5 от 20К: \$5
Outlook.com Plus	83541	до 10К: \$4 от 10К до 20К: \$3.5 от 20К: \$3

Новости

12 Апр 2013

Вновь в продаже аккаунты **Twitter.com!**

15 Мар 2013

Отличная цена на аккаунты **Facebook.com!** Всего **\$80** за **1000 шт.** Дешевле не бывает!

07 Фев 2013

Сенсационная цена на аккаунты **Yahoo.com.** Теперь отличные аккаунты **со всеми регистрационными данными** по цене **от \$7** за **1000 шт!**

06 Фев 2013

Добавлены аккаунты **Tabor.ru** и **Drugvokrug.ru** по очень интересным ценам

21 Янв 2013

Распродаем аккаунты **Одноклассников!** Теперь всего по **9 руб** за шт!

20 Дек 2013

BuyAcCs.com

BUY BULK ACCOUNTS AT BEST PRICES

If you need quality **bulk accounts**, you've come to the right place. You can get your accounts **immediately** after your payment - there is no need to wait.

All the accounts are provided in **any format** you like. Just use our **[free account converter](#)** to get them in the way you need.

Special rates are applied if you purchase less than 1000 accounts.

We accept Liberty Reserve and Paypal.

Please, review our [terms and conditions](#) before purchasing any accounts.

[Buy Yahoo Accounts](#)

[Buy Twitter Accounts](#)

[Buy Livejournal Accounts](#)

[Buy Hotmail Accounts](#)

For sale

Provider	Quantity	Rate for 1000
Hotmail.com	425227	1K-10K: \$5 10K-20K: \$4.5 20K+: \$4
Hotmail.com Verified	505448	1K-10K: \$6 10K-20K: \$5.5 20K+: \$5
Outlook.com Plus	83541	1K-10K: \$4 10K-20K: \$3.5 20K+: \$3
Gmail.com USA PVA	6661	1K-10K: \$100 10K-20K: \$95 20K+: \$90
Yahoo.com	3403	1K-10K: \$8 10K-20K: \$7.5 20K+: \$7
Yahoo.com USA	0	1K-10K: \$15 10K-20K: \$15 20K+: \$15
Nokiamail.com	47823	1K-10K: \$10 10K-20K: \$10 20K+: \$9
AOL.com	3365	1K-10K: \$20 10K-20K: \$20 20K+: \$20
GMX.com	563	1K-10K: \$25 10K-20K: \$25 20K+: \$25
Mail.com	265	1K-10K: \$20 10K-20K: \$20 20K+: \$20
Facebook.com	33102	1K-10K: \$80 10K-20K: \$80 20K+: \$80

News

12 Apr 2013

Twitter accounts are **available again!**

07 Feb 2013

Added **Instagram** accounts at a great rate: **\$50 per 1000**.

04 Dec 2012

Just added **Fully Profiled Twitter Accounts** at a great rate - **\$30 per 1000**. Accounts come with **avatar, bio and random background**.

19 Nov 2012

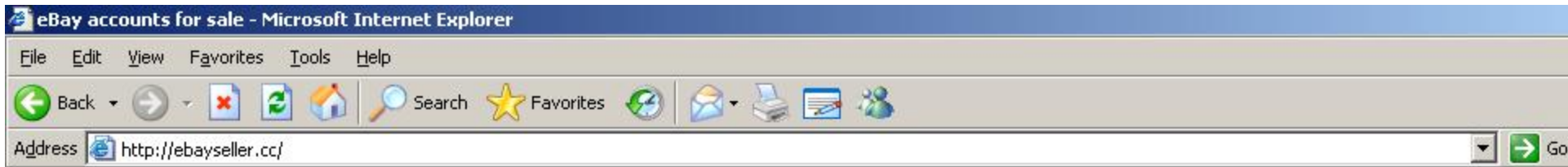
Great prices for wholesale **Twitter.com** and **Hotmail.com** orders!

17 Nov 2012

Added **Pinterest.com** accounts at a great price - **\$70 per 1000!**

03 Nov 2012

Added **AOL accounts** with **POP3** and **SMTP** enabled at an unbeatable price: starting from **\$8 per 1000**.



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\$

Welcome to PP24 ! Please use Width Fluid to view full details

You balance is empty, please deposit money to buy paypals

SEARCH PAYPALS

VERIFY (+\$0.10)

TYPE (+\$0.15)

COUNTRY (+\$0.20)

MAIL (+\$0.20)

BALANCE (+\$0.20)

All Verify

All Type

All Country

SEARCH

AVAILABLE PAYPALS 89

Show **50** entries

Search:

PAYPAL EMAIL	^	VERIFY	TYPE	CARD	BANK	MAIL	BALANCE	FIRST NAME	ADDRESS	COUNTRY	PRICE	<input type="checkbox"/>
****alksmommy@yahoo.com		Yes	Premier	✓	✓	—	\$6.42	Joanna	Panama City	USA	\$2.50	<input type="checkbox"/>
****eans123@yahoo.com		Yes	Premier	✓	✓	—	\$1.00	Regina	Clifton Park	USA	\$2.50	<input type="checkbox"/>
****ibsack@gmail.com		Yes	Premier	✓	✓	—	\$121.07	Abigail	Jefferson	USA	\$15.00	<input type="checkbox"/>
****ie@gambit.net		Yes	Premier	✓	✓	—	\$1,102.37	Gwynn	Tallmadge	USA	\$45.00	<input type="checkbox"/>
****l.stevenson@gmail.com		Yes	Premier	✓	✓	—	\$209.03	Michal	Galloway	USA	\$20.00	<input type="checkbox"/>
****ney_bruesch@yahoo.com		Yes	Premier	✓	✓	—	\$18.41	Courtney	Gurnee	USA	\$4.00	<input type="checkbox"/>

Offers**Services****Proofs****Free Logins****Payment method**

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 pharmaco-economic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	\$399
http://www.woodlands.edu.uy/	Woodlands 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

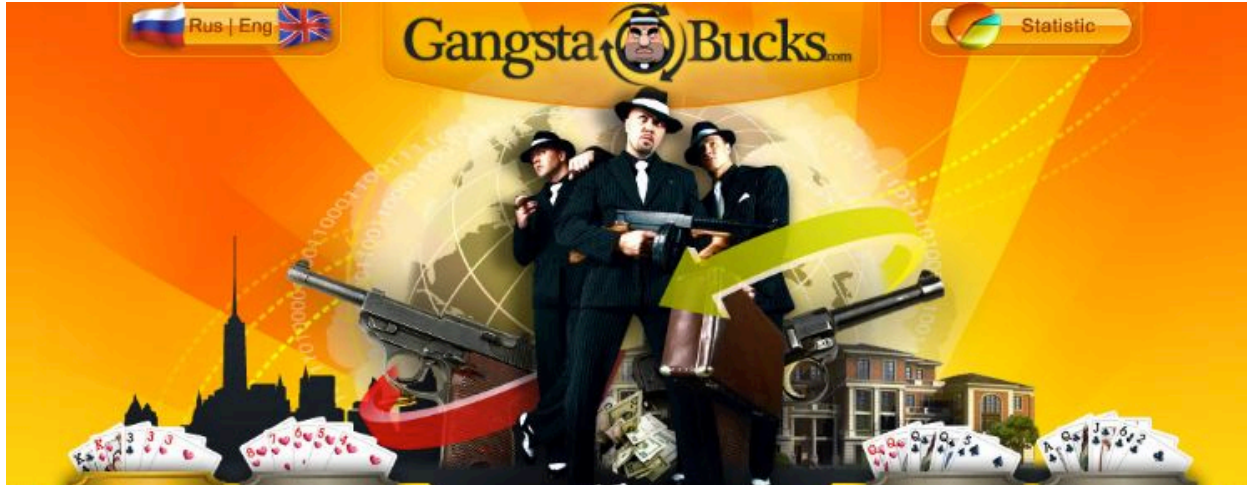
- Daily updated -

[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 Exploiter + Google Ripper + SQLi + Proxy Exploiter - 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.



Home



Conditions

Registration



Tariffs



Contacts



An individual approach to everyone



Guaranteed weekly payouts



Round-the-clock support



Detailed statistics



User-friendly software

GangstaBucks.com - it pays on time!
We pay for all installs!

Join our ranks and by tomorrow
 you could get your first payout!

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\$

Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated cybercrime
 - Spam, pharmaceuticals, credit card theft, identity theft
 - Facilitated by a well-developed “underground economy”
- 2010's: politically motivated
 - Governments: **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 Tian/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.

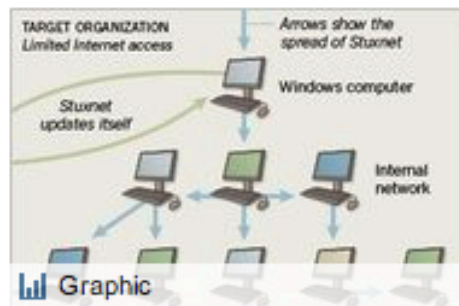
[Enlarge This Image](#)



Nicholas Roberts for The New York Times

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

Multimedia



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



Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated cybercrime
 - Spam, pharmaceuticals, credit card theft, identity theft
 - Facilitated by a well-developed “underground economy”
- 2010's: politically motivated
 - Governments: espionage, **censorship**, surveillance

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

Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated cybercrime
 - Spam, pharmaceuticals, credit card theft, identity theft
 - Facilitated by a well-developed “underground economy”
- 2010's: politically motivated
 - Governments: espionage, censorship, surveillance, hot wars

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.

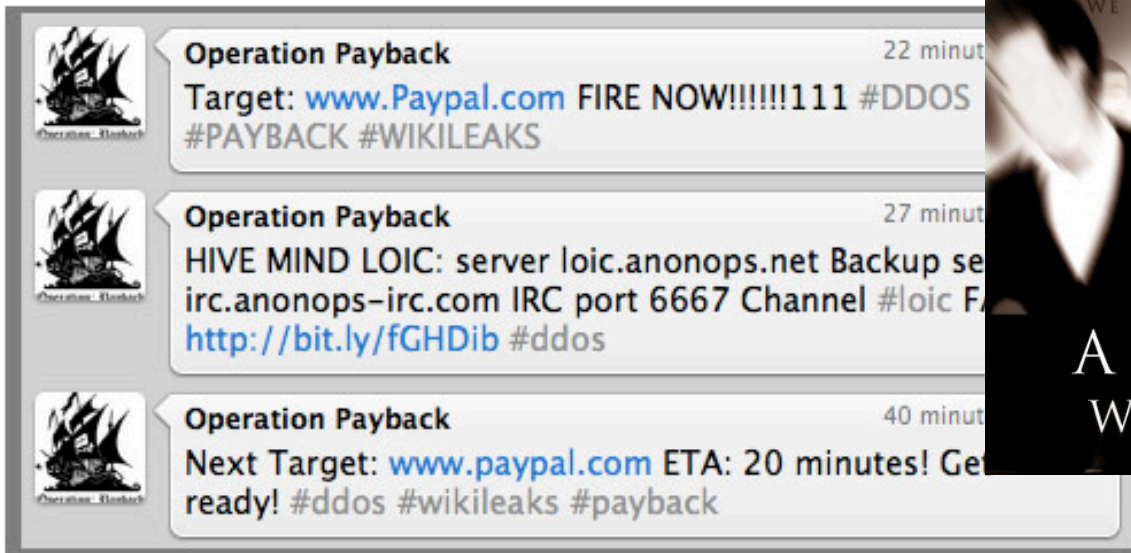
Country	IPs	Blocked	Blocked	Blocked	Blocked
Florida, U.S.A.	Okay	19.4	19.9	19.1	
Washington, Netherlands	Okay	149.3	144.6	170.4	
Melbourne, Australia	Okay	179.5	174.1	178.9	
Singapore, Singapore	Okay	209.5	214.0	209.6	
New York, U.S.A.	Packet Loss (100%)				
Amsterdam, Netherlands	Packet Loss (100%)				
Atlanta, U.S.A.	Packet Loss (100%)				
London, United Kingdom	Packet Loss (100%)				
Stockholm, Sweden	Packet Loss (100%)				
Oslo, Norway	Packet Loss (100%)				
Chicago, U.S.A.	Packet Loss (100%)				
Seattle, U.S.A.	Packet Loss (100%)				
Amsterdam, Netherlands	Packet Loss (100%)				
Helsinki, Finland	Packet Loss (100%)				
Paris, France	Packet Loss (100%)				
Copenhagen, Denmark	Packet Loss (100%)				
San Francisco, U.S.A.	Packet Loss (100%)				
Toronto, Canada	Packet Loss (100%)				
Madrid, Spain	Packet Loss (100%)				
Shanghai, China	Packet Loss (100%)				
Lille, France	Packet Loss (100%)				
Zurich, Switzerland	Packet Loss (100%)				
Munich, Germany	Packet Loss (100%)				
Cape Town, South Africa	Packet Loss (100%)				
Porto Alegre, Brazil	Packet Loss (100%)				
Sydney, Australia	Packet Loss (100%)				
Mumbai, India	Packet Loss (100%)				
Stockholm, U.S.A.	Packet Loss (100%)				

Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated cybercrime
 - Spam, pharmaceuticals, credit card theft, identity theft
 - Facilitated by a well-developed “underground economy”
- 2010's: politically motivated
 - Governments: espionage, censorship, surveillance, hot wars
 - *Hacktivism*

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

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



The image shows a screenshot of three tweets from a user named 'Operation Payback'. Each tweet includes a small icon of a sailing ship. The tweets are as follows:

- 22 minutes ago:** Target: www.Paypal.com FIRE NOW!!!!!!111 #DDOS #PAYBACK #WIKILEAKS
- 27 minutes ago:** HIVE MIND LOIC: server loic.anonops.net Backup server irc.anonops-irc.com IRC port 6667 Channel #loic FIRE <http://bit.ly/fGHDib> #ddos
- 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.

Threats evolve ...

- 1990's, early 2000's: bragging rights
- Mid 2000's – today: financially motivated cybercrime
 - Spam, pharmaceuticals, credit card theft, identity theft
 - Facilitated by a well-developed “underground economy”
- 2010's: politically motivated
 - Governments: espionage, censorship, surveillance, hot wars
 - *Hacktivism*
 - *Targeting* of political organizations, individuals

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.

VANITY FAIR

HOW A GRAD STUDENT FOUND SPYWARE THAT COULD CONTROL ANYBODY'S IPHONE FROM ANYWHERE IN THE WORLD

Last summer, Bill Marczak stumbled across a program that could spy on your iPhone's contact list and messages—and even record your calls. Illuminating shadowy firms that sell spyware to corrupt governments across the globe, Marczak's story reveals the new arena of cyber-warfare.



BY BRYAN BURROUGH

NOVEMBER 28, 2016 5:00 AM



“APPLE HAD NEVER SEEN ANYTHING LIKE THIS . . . INCREDIBLY SOPHISTICATED NATION-STATE ATTACK.”

“The Hacking Team thing was monumental,” says Chris Soghoian. “Prior to that, the only thing that researchers had was circumstantial evidence that this was going on. They would find a FinFisher server in Morocco and say that’s evidence the government was using it. Before Hacking Team, there was no smoking gun.”



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account

Details:

Tuesday, 22 March, 14:9:25 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team



Russia-linked phishing campaign behind the DNC breach also hit Podesta, Powell

Bit.ly-based phishing links targeted former Sec. of State, Clinton campaign chair.

SEAN GALLAGHER - 10/20/2016, 3:40 PM

Someone

Hi William

Someone just used your password to try to sign in to your Google Account

Details:

Tuesday, 22 March, 14:9:25 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team

The Smoking Gun

You received this mandatory email service announcement to update you about important changes to your Google product or account.

The spear-phishing e-mail received by Clinton campaign staffer William Rinehart matches messages received by both former Secretary of State Colin Powell and Clinton campaign chairman John Podesta.