01. Course Introduction

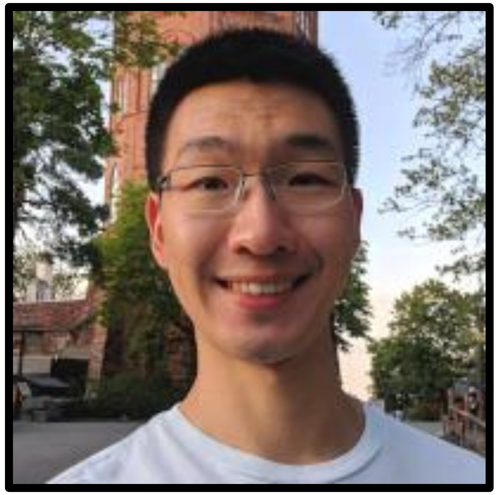
Blase Ur and Grant Ho
January 3rd, 2024
CMSC 23200

THE UNIVERSITY OF CHICAGO

Part 1: Course Logistics

Two Instructors

Blase Ur



Grant Ho

Five TAs

Arthur Borém

Emma Peterson

Madison Pickering

Tian Yang

Zachary Rothstein

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2024/winter/23200-1/

(Also linked from Canvas)

Lectures

- Mondays and Wednesdays
  - 1:30pm - 2:50pm (Section 1)
  - 3:00pm - 4:20pm (Section 2)
- Hinds 101
  - Will **not** be recorded
  - Will generally **not** be livestreamed unless a student is ill and has requested a livestream

Textbook

- Paul van Oorschot, Computer Security and the Internet: Tools and Jewels (2nd Edition)
  - Free PDFs linked from the course website

Course Requirements

- 9 Reading Responses (9%)
  - Typically due Tuesdays at 11:59pm
  - Exception: First one is due tomorrow (Thursday, 1/4)
- 8 Assignments (64%)
  - Generally due Thursdays 11:59pm
  - First one is due next Thursday (1/11)
- Final Exam (27%)

Communication

- **Canvas** for assignment distribution
- **Ed** for questions
  - Questions about assignments, course material, logistics
  - Extension requests
- Submissions: **Gradescope (prose)** / **Canvas (code)**
- **Don't email any members of the course staff!** Use Ed!
  - **We will add you in the next 24 hours**
  - Not added? blase@uchicago.edu

Key Course Policies (1/2)

- Late submissions
  - Assignments and reading responses can be submitted up to 24 hours late for a 15-point penalty
- Extensions
  - Only granted for medical and family emergencies
  - **Not** granted for clubs, sports, job interviews, midterm week, etc.
- Wellness
  - Reach out to the course staff in a private (staff-only) post on Ed

Key Course Policies (2/2)

- P/F grading
  - C- or higher = Pass
  - Request on Ed by the end of 9th week
  - Probably won't count for your major

Communication on Ed

- See course website for guidelines about asking questions
- Private posts (visible to instructors) for:
  - Personal logistics, extensions, wellness, etc.
  - Questions about assignments that **include code or specific insights about your solution**
- Public posts for general questions / clarifications
- Feel encouraged to answer questions!

Academic Integrity Policy (1/2)

- Detailed on syllabus
- All work submitted must be your own
- You may speak in general terms about approach, but not share code; **do not look at each other's code**
- Encouraged to talk to classmates and form study groups
- On each Gradescope submission, you **must document everyone in the class you spoke to, as well as every major resource you consulted** other than what we provide

Academic Integrity Policy (2/2)

- Example for the top of your Gradescope submission:
  - "I discussed the whole assignment with Jane Smith. We also discussed Part 3 with John Doe. I consulted: *https://www.helpfuldomain.com/helpfulpage.html* to understand the fetch() API and I used two lines from *https://www.other.com/page.html* in Part 3."
- Code reuse from websites, Stack Overflow, and published resources only allowed if **all** of the following apply:
  - Around 4 lines of code or fewer
  - Doesn't solve the intellectual point of that part of the assignment
  - Documented at top (see above) or as comment

Ethical Hacking Policy

- In this course, you will learn hacking techniques that can actually compromise some systems
- **You may only use these techniques on systems with the explicit knowledge and explicit consent from everyone who owns and uses that system**
- You must stay within the bounds of each assignment
- **Do not** use these techniques on any machine, network, or system not specified in the assignment

Office Hours

- Office hours will typically be held in person
- TA and instructor **assignment office hours**
  - Primary venue for help with assignments
  - Each assignment will have two TAs assigned
- Monday instructor office hours (or by appointment)
  - Talk about lectures / concepts in general
  - Talk about life / career / computing
  - Get to know us!

Part 2: Course Goals and Topics

Course Learning Objectives

- The security mindset
- Core security principles & properties
- Computer security attacks
- Computer security defenses

Schedule of Topics By Week

1. Course overview, threat modeling
2. OS security, memory vulnerabilities / protection
3. Cryptography basics
4. More cryptography basics, TLS
5. Network basics and network attacks
6. Web basics, web attacks
7. Web tracking, protecting corporate networks
8. Authentication
9. Hardware security, security in practice

Assignments

1. Threat modeling, TOCTOU attacks, UNIX basics
2. Buffer overflows and memory attacks
3. Attacking crypto implementations
4. Measuring X.509 cert usage
5. (Mostly manual) side-channel analysis of network traffic
6. Automating side-channel analysis of network traffic
7. Web attacks and defenses
8. Modeling and cracking passwords

Part 3: The Evolution of Computer Security Attacks & Incidents

(These slides adapted from Vern Paxson)

Threats Evolve

- 1990s, early 2000s: bragging rights

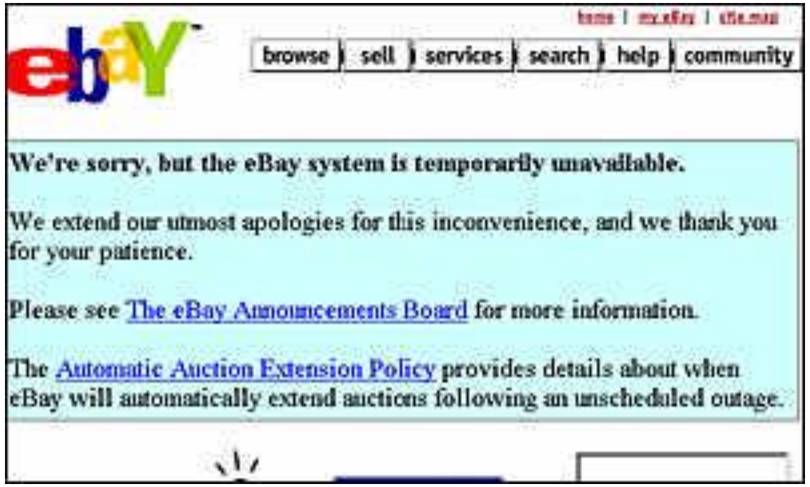
PRIVACY & SECURITY

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?' "



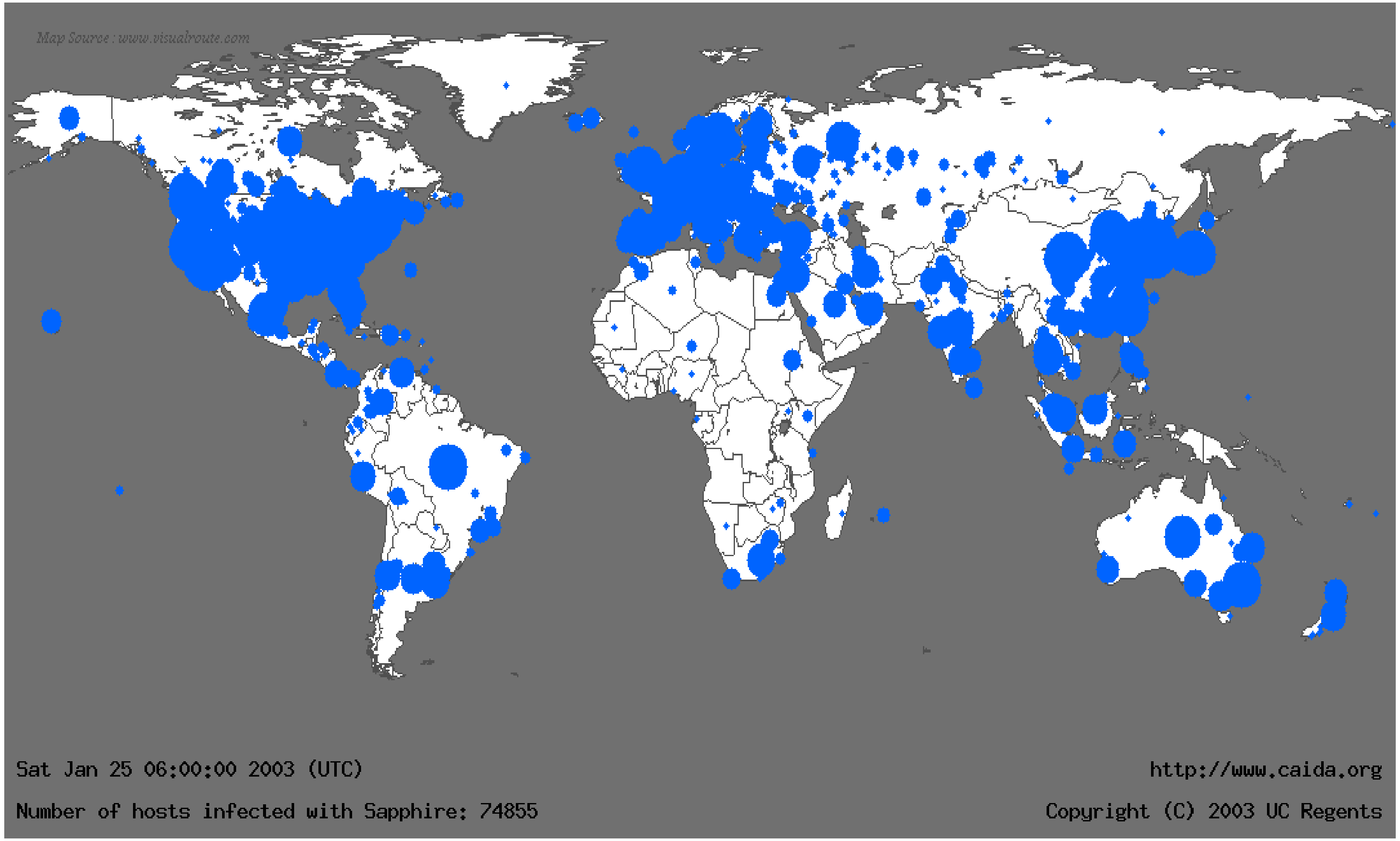
We're sorry, but the eBay system is temporarily unavailable.

We extend our utmost apologies for this inconvenience, and we thank you for your patience.

Please see The eBay Announcements Board for more information.

The Automatic Auction Extension Policy provides details about when eBay will automatically extend auctions following an unscheduled outage.

Slammer Worm Spreads Across Entire Internet in Under 10 Minutes



Sat Jan 25 06:00:00 2003 (UTC)

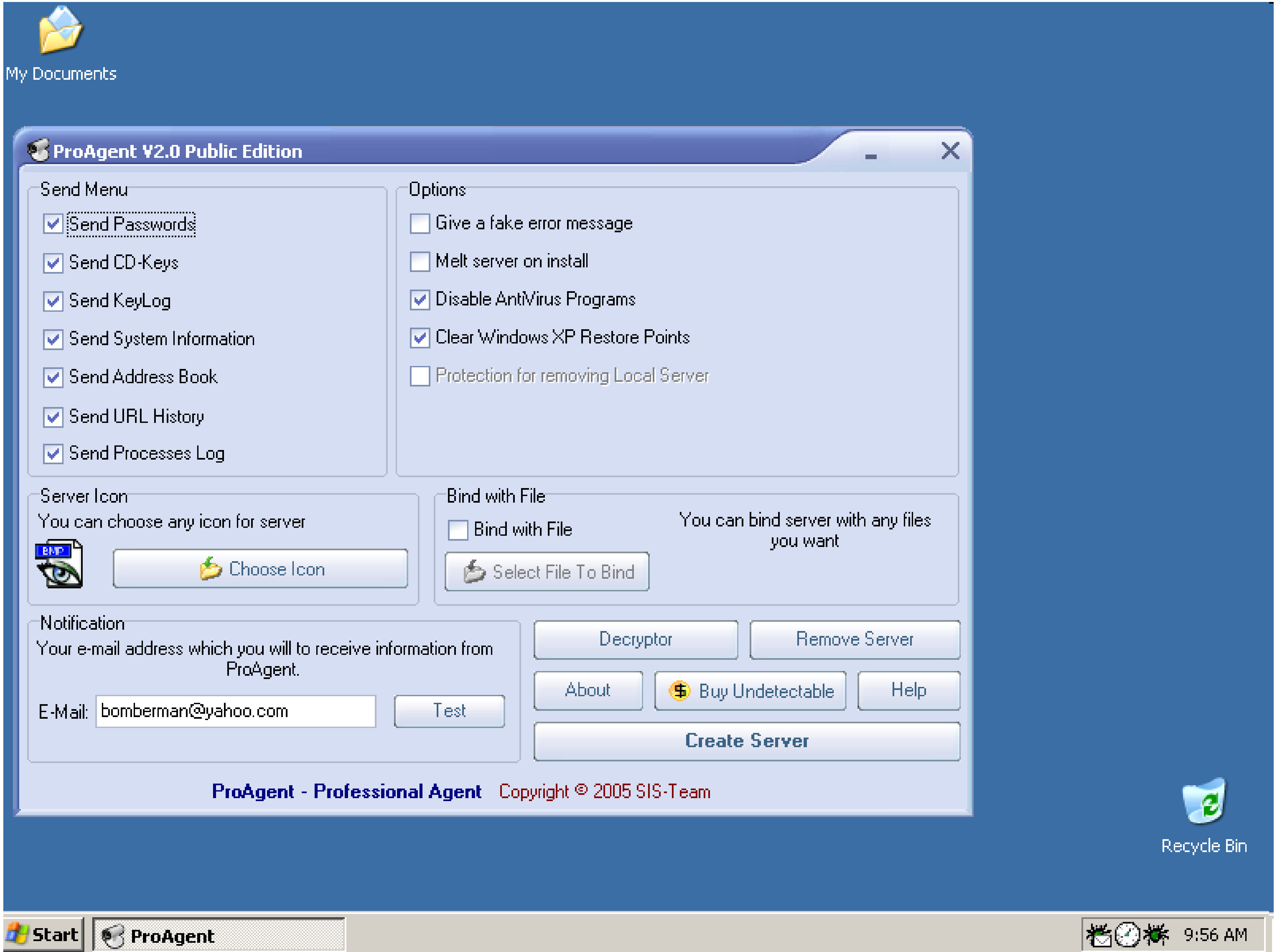
Number of hosts infected with Sapphire: 74855

http://www.caida.org

Copyright (C) 2003 UC Regents

Threats Evolve

- 1990s, early 2000s: bragging rights
- Mid 2000s – today: financially motivated cybercrime
  - Spam, phishing, credit card theft, identity theft
  - Facilitated by a well-developed “underground economy”



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

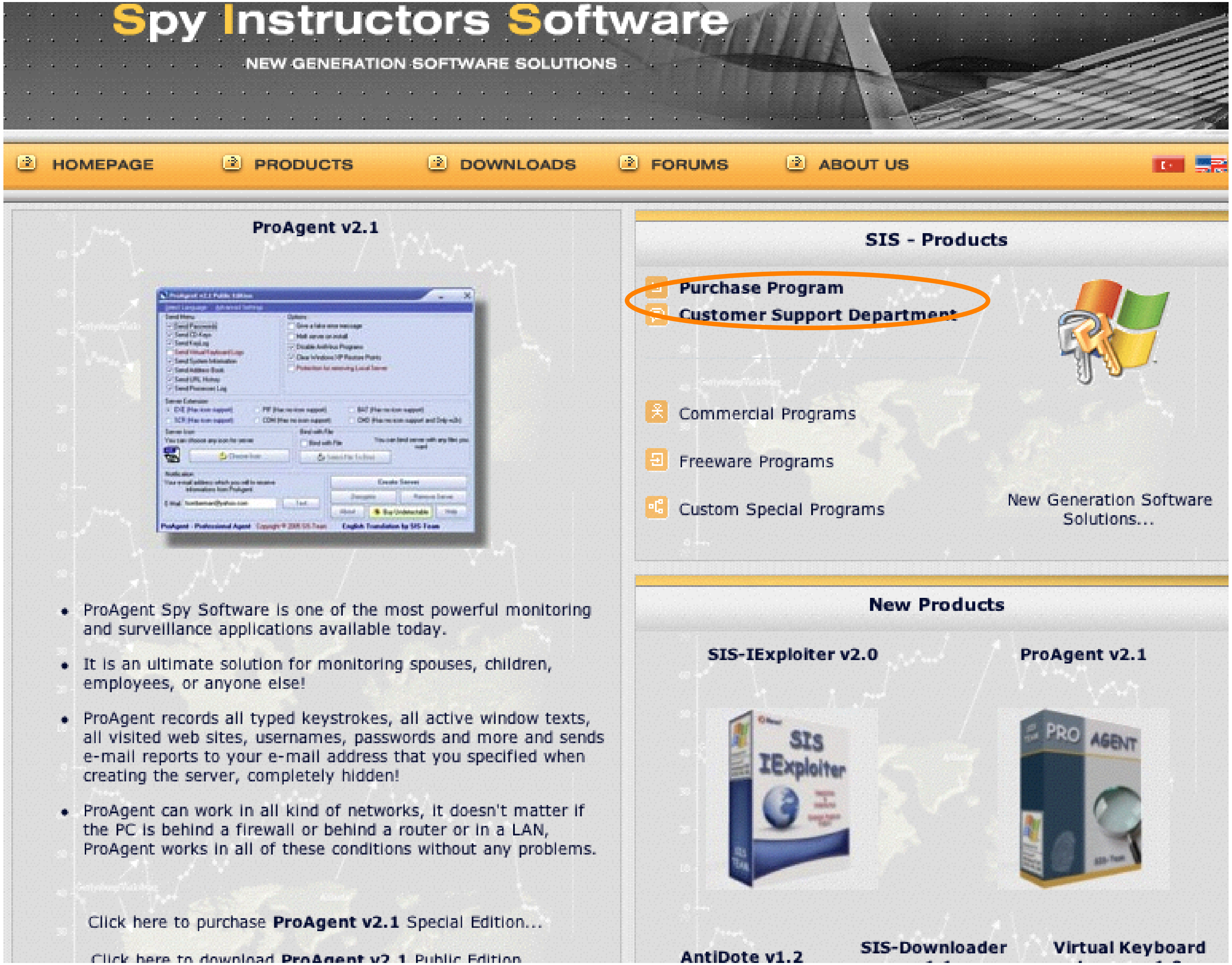
You can bind server with any files you want

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



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.

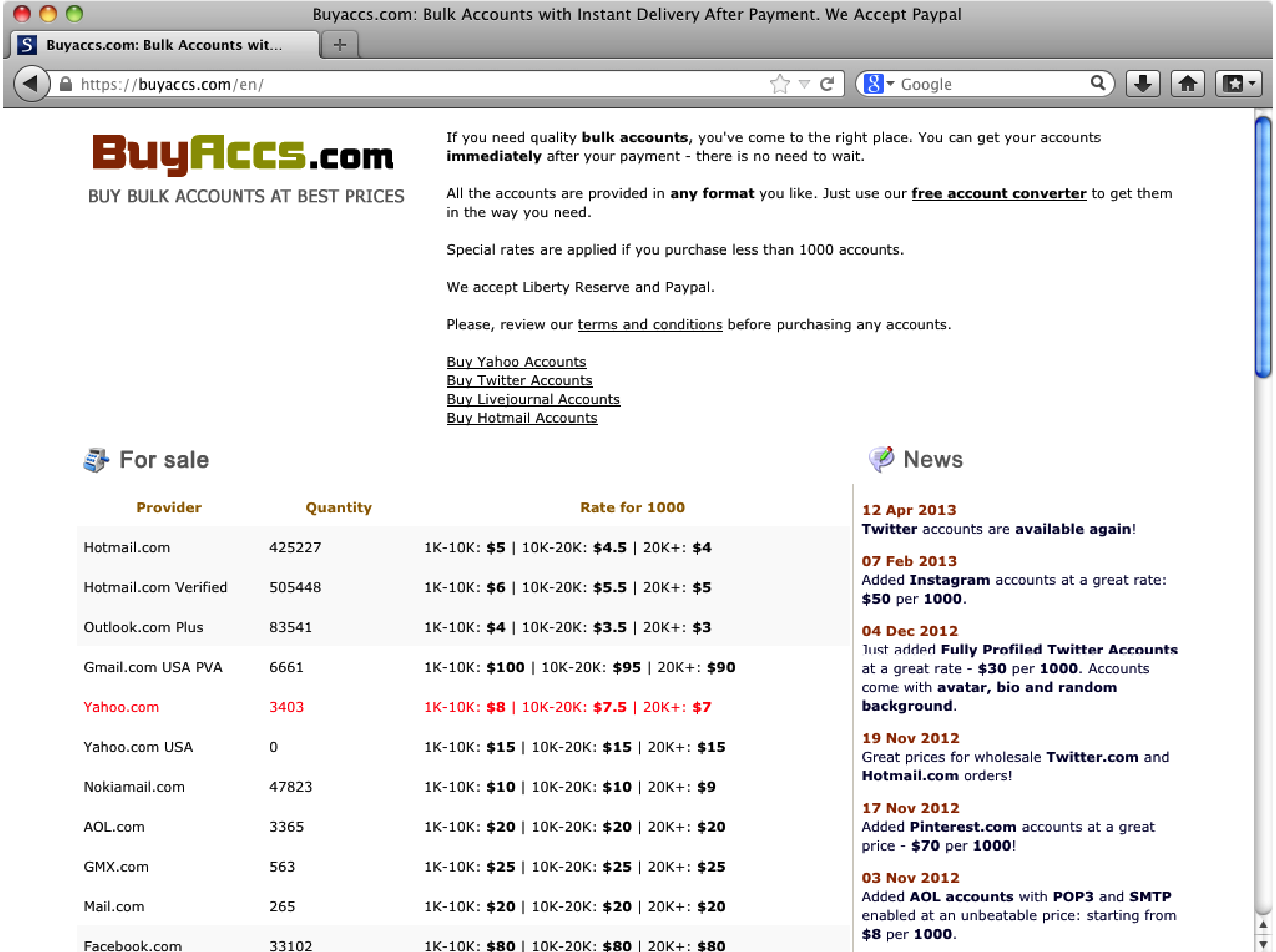
Click here to purchase **ProAgent v2.1** Special Edition...

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

SIS - Products

New Generation Software Solutions...

New Products


Buyaccs.com: Bulk Accounts with Instant Delivery After Payment. We Accept Paypal
Buyaccs.com: Bulk Accounts wit...
https://buyaccs.com/en/
Google

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**!

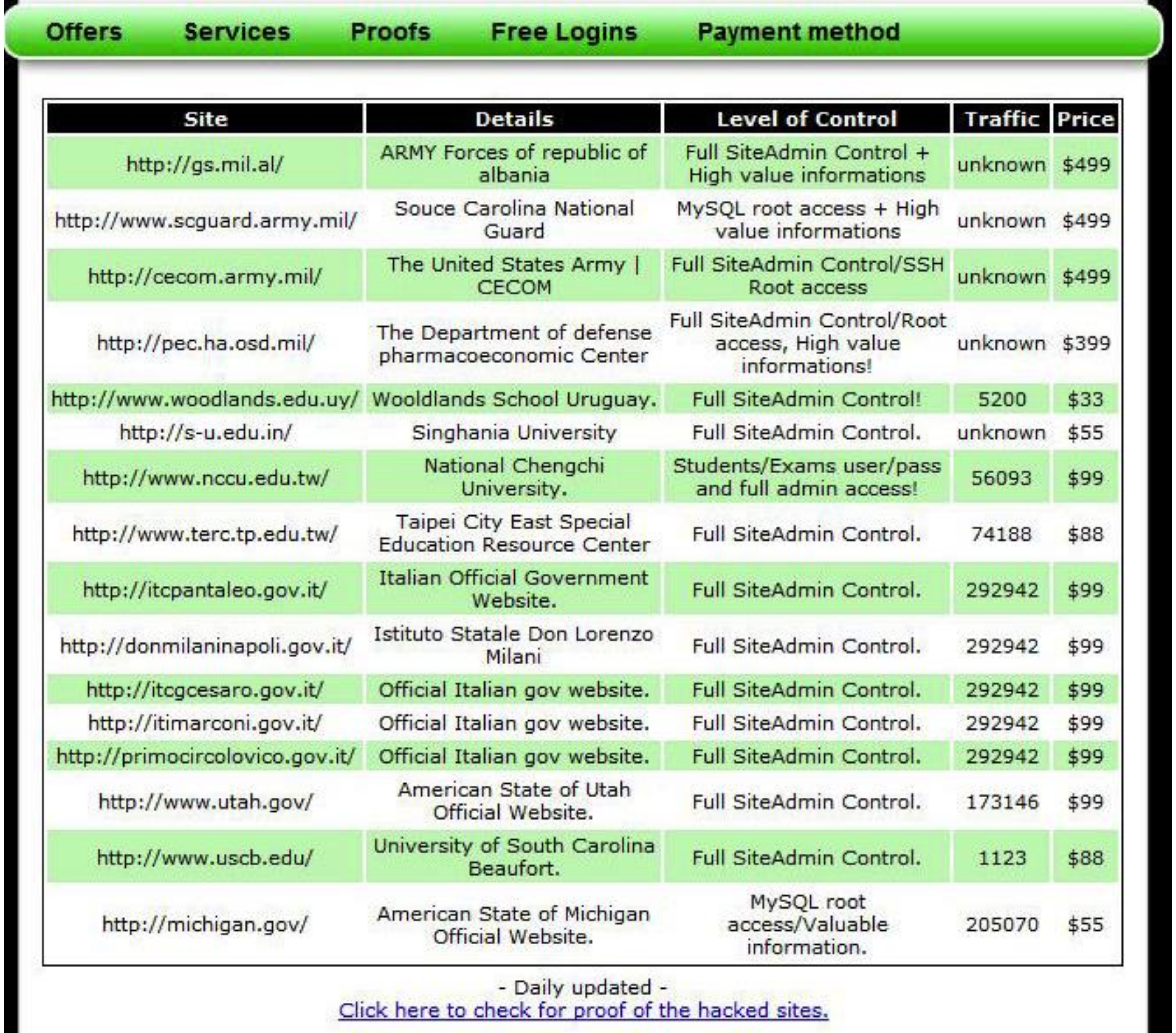
07 Feb 2013
Added **Instagram** accounts at a great rate: **$50** per **1000**.

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**!

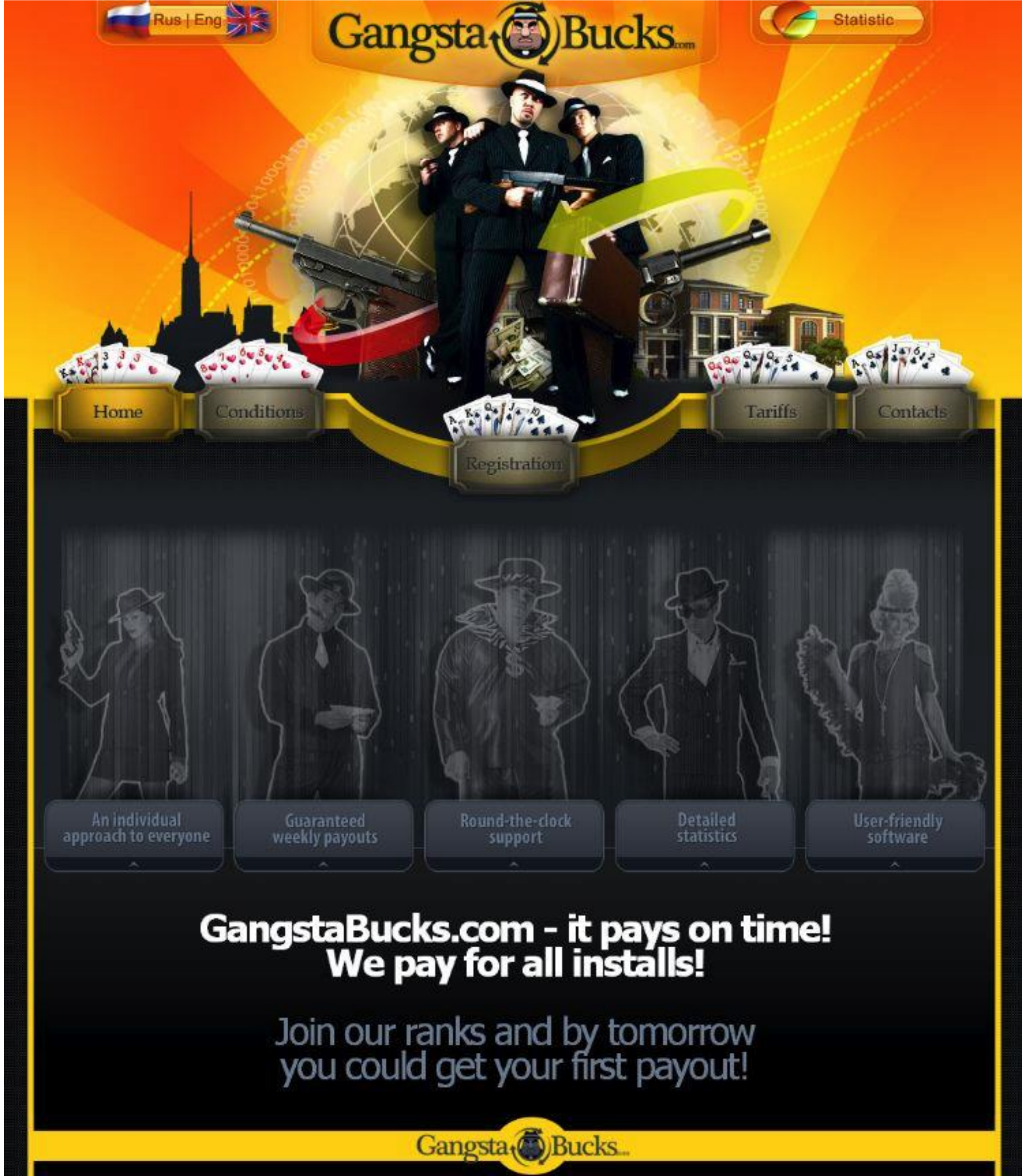
03 Nov 2012
Added **AOL accounts** with **POP3** and **SMTP** enabled at an unbeatable price: starting from **$8** per **1000**.



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.

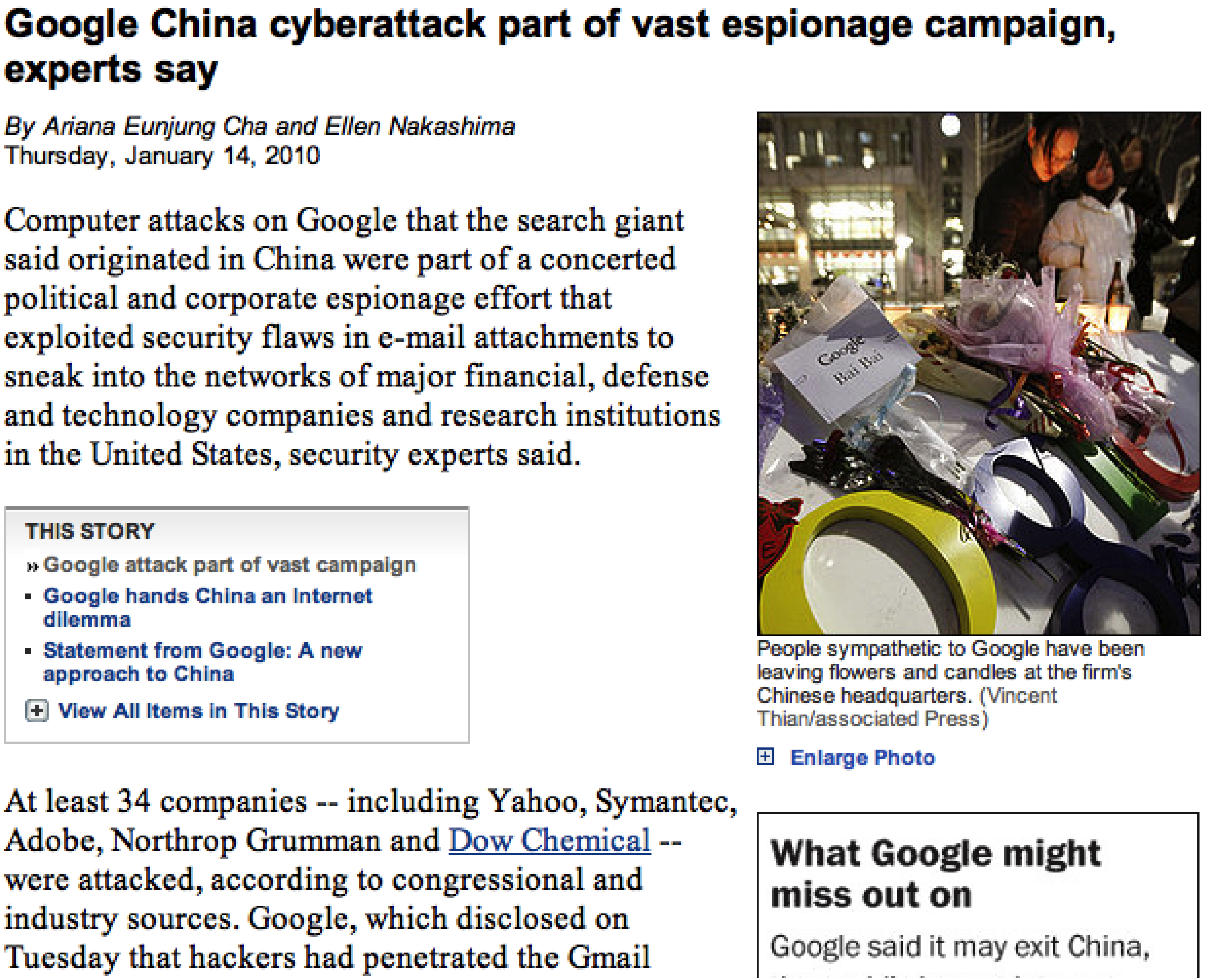


GangstaBucks.com - it pays on time!
We pay for all installs!

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

Threats Evolve

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

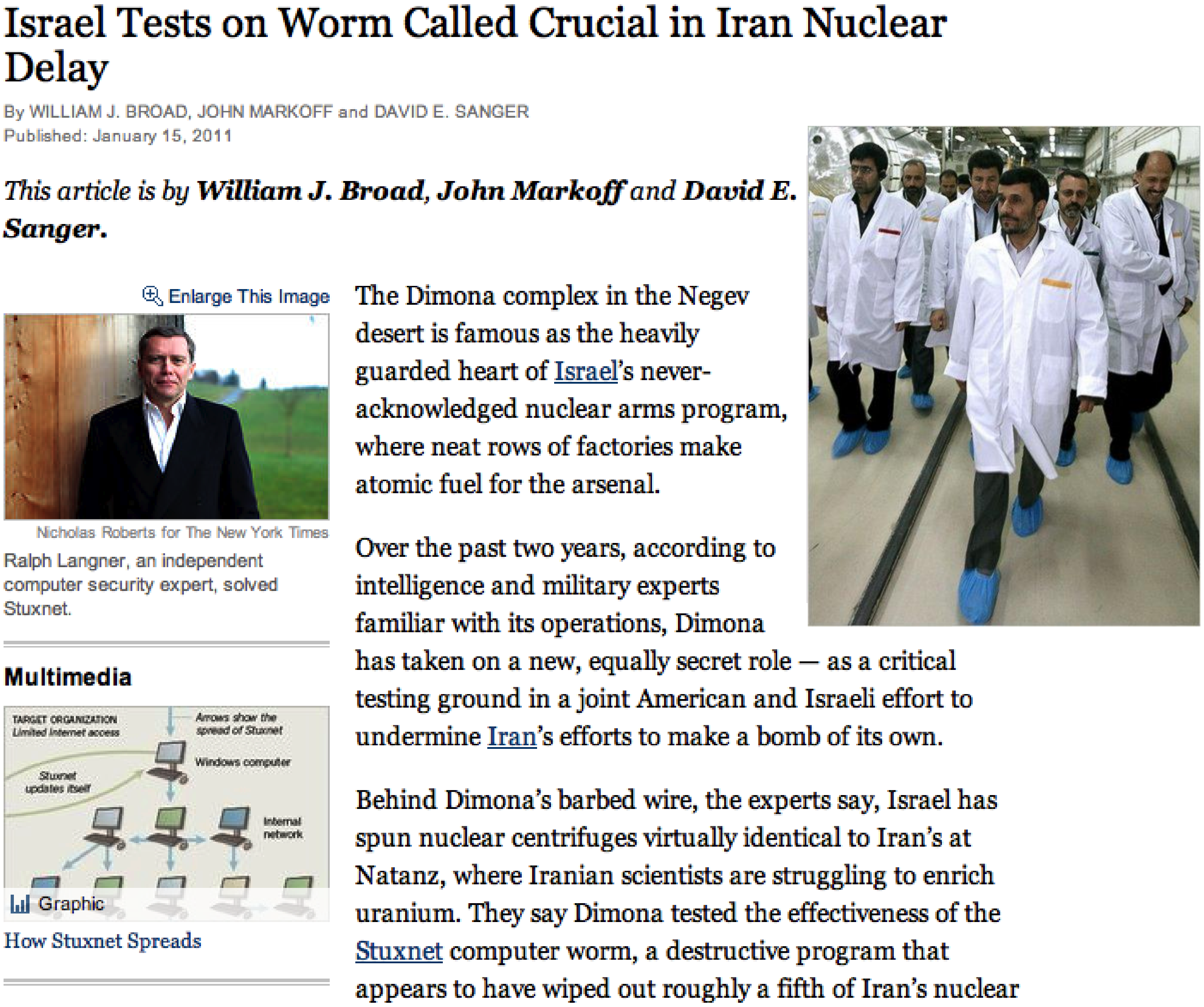
People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

⊞ 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.

Multimedia

Graphic

How Stuxnet Spreads

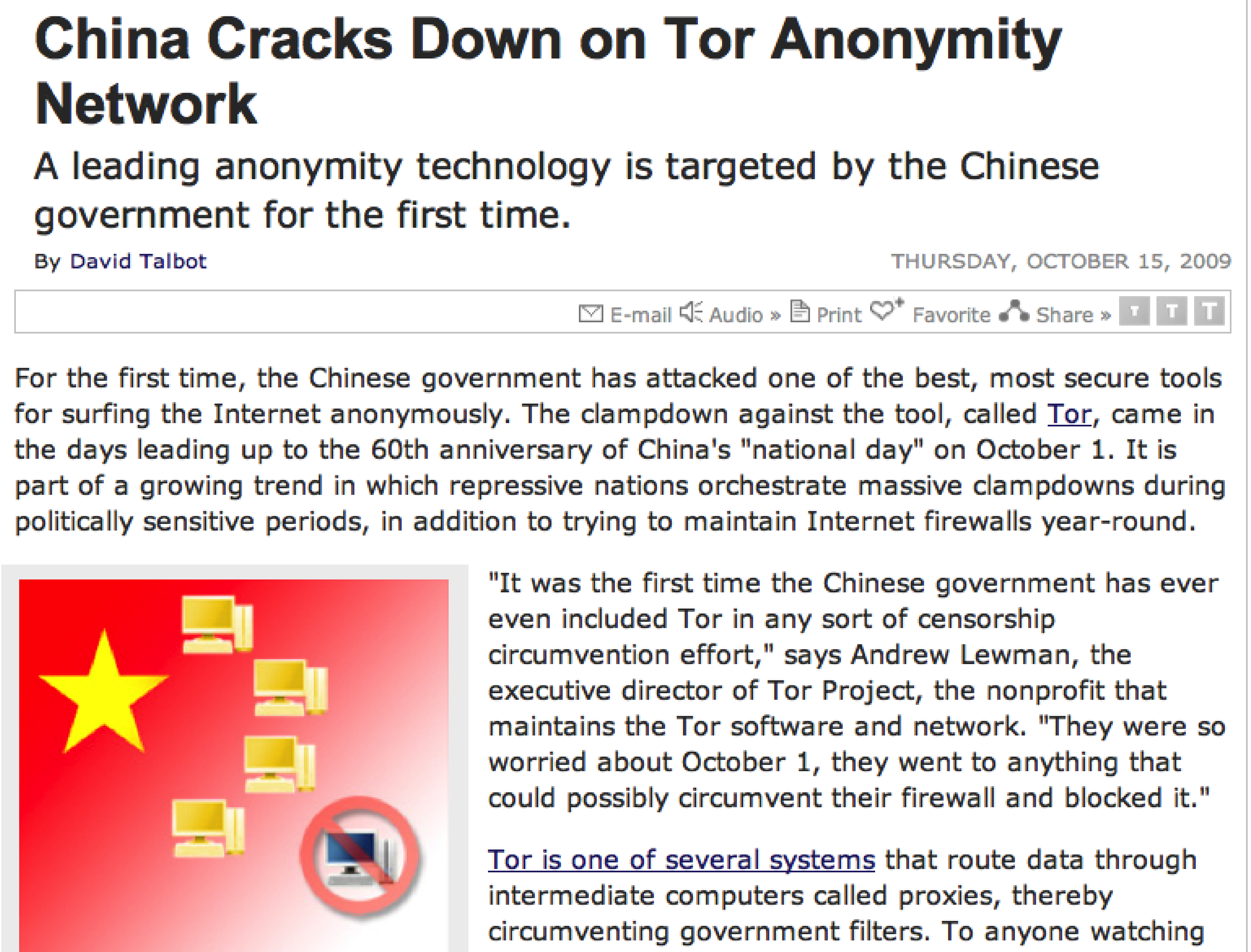
The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

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

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

Threats Evolve

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

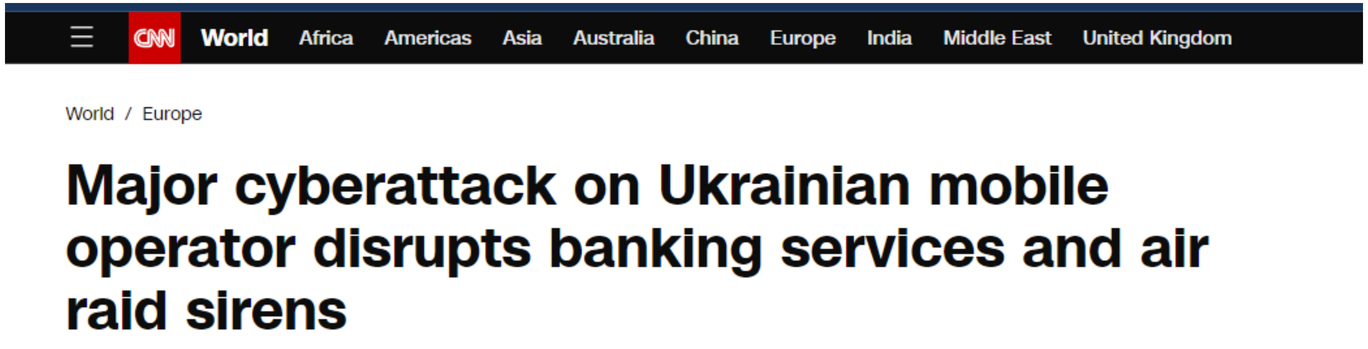
For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor, came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which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

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

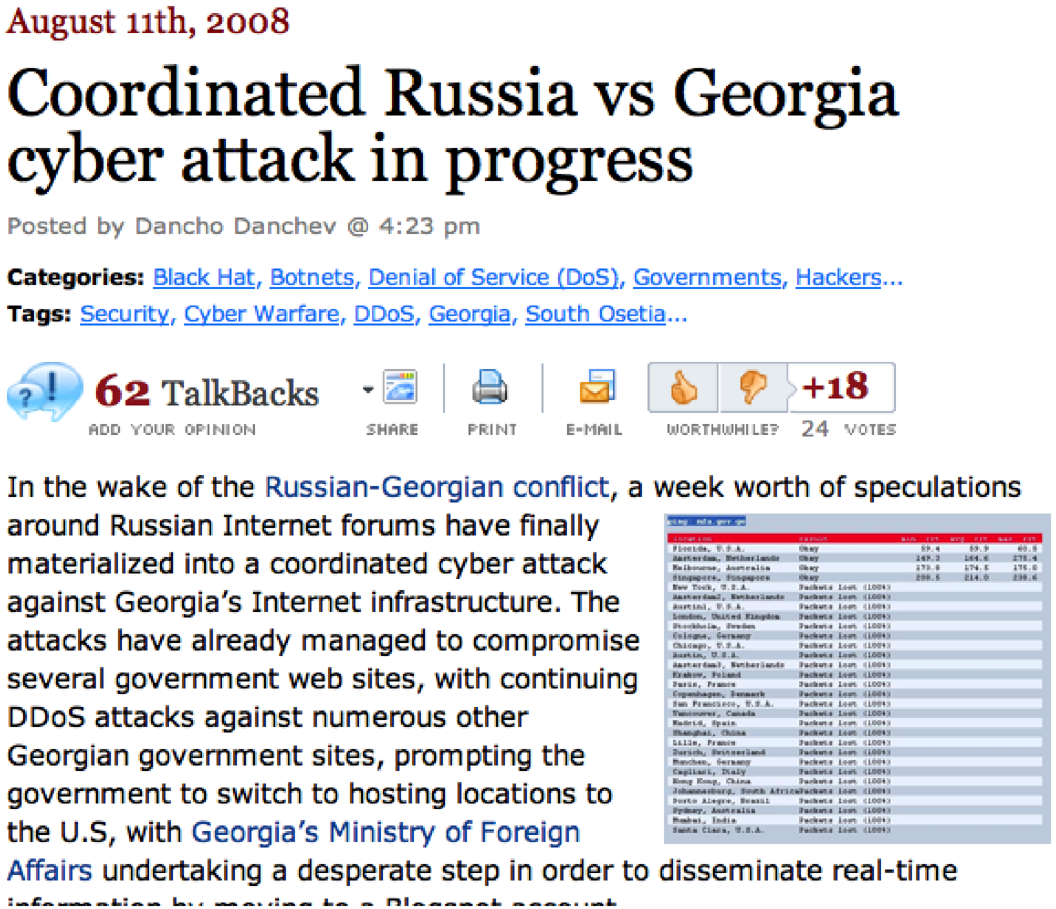


World / Europe

Major cyberattack on Ukrainian mobile operator disrupts banking services and air raid sirens

By Sean Lyngaas, CNN

4 minute read · Updated 9:36 PM EST, Tue December 12, 2023



August 11th, 2008

Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

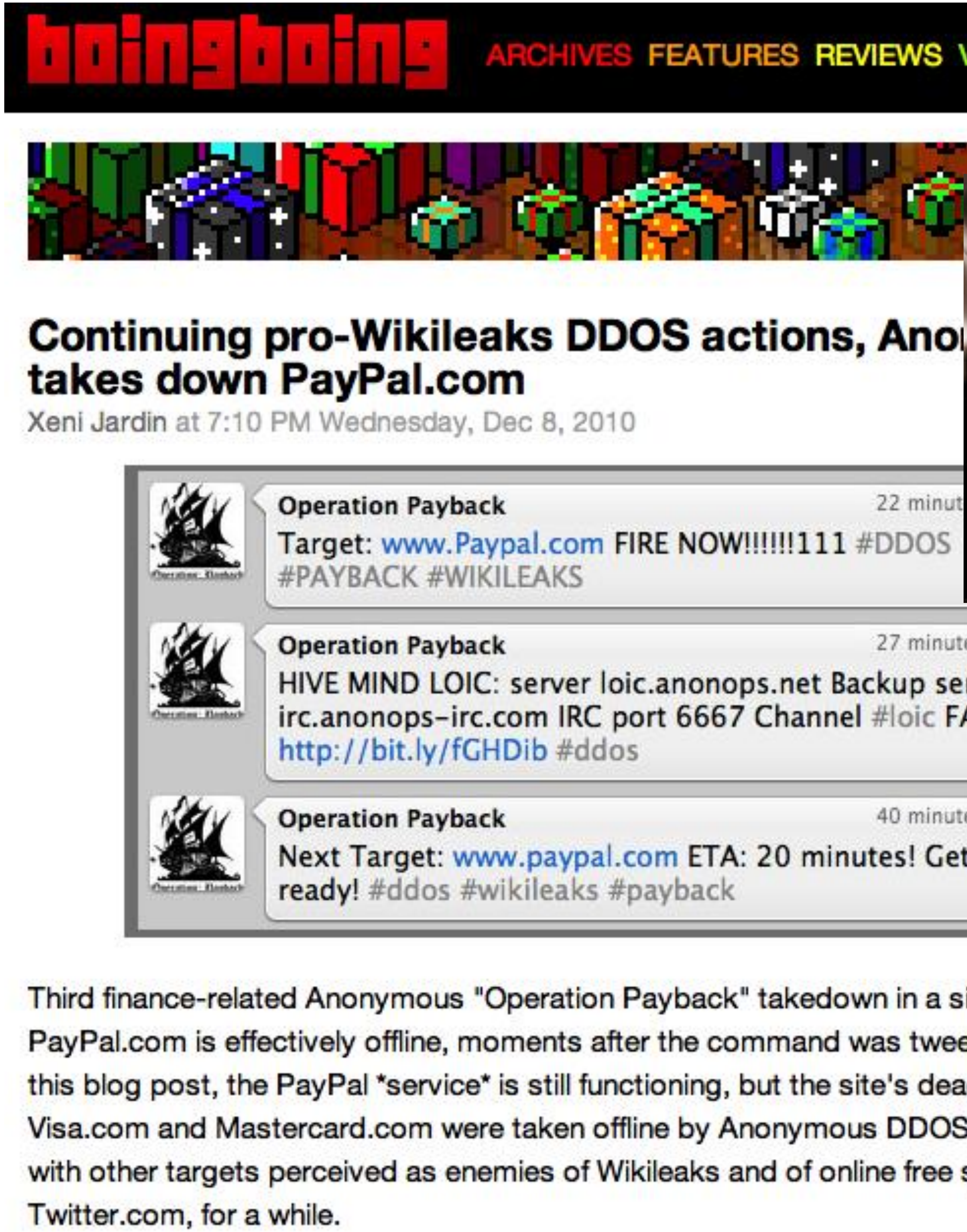
Categories: Black Hat, Botnets, Denial of Service (DoS), Governments, Hackers...

Tags: Security, Cyber Warfare, DDoS, Georgia, South Osetia...

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 Blogspot account.

Threats Evolve

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



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

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

Operation Payback 22 minut

Target: www.Paypal.com FIRE NOW!!!!!!111 #DDOS #PAYBACK #WIKILEAKS

Operation Payback 27 minutes ago

HIVE MIND LOIC: server loic.anonops.net Backup server irc.anonops-irc.com IRC port 6667 Channel #loic FAQ: http://bit.ly/fGHDib #ddos

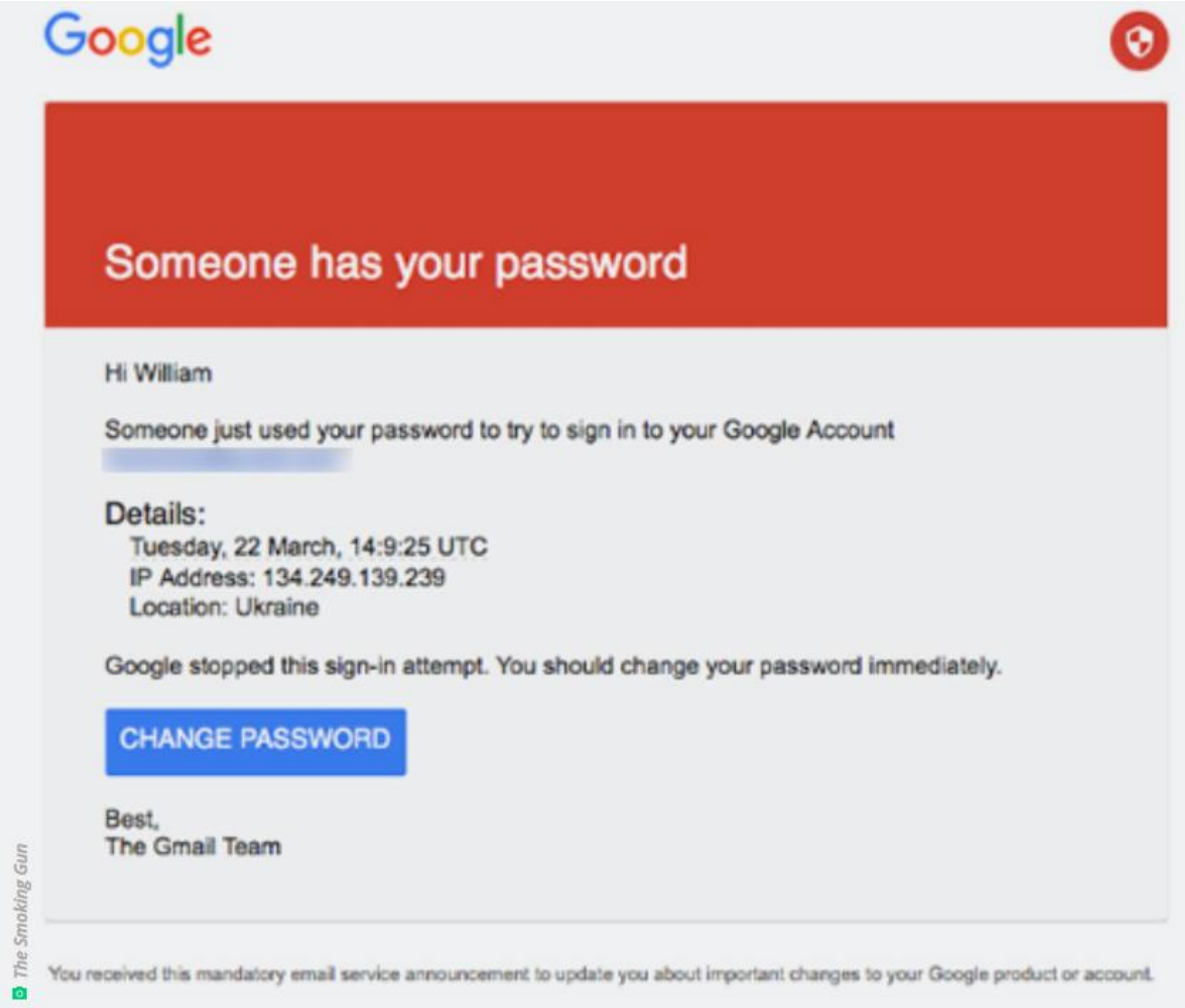
Operation Payback 40 minutes ago

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.

Threats Evolve

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



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]

Details:

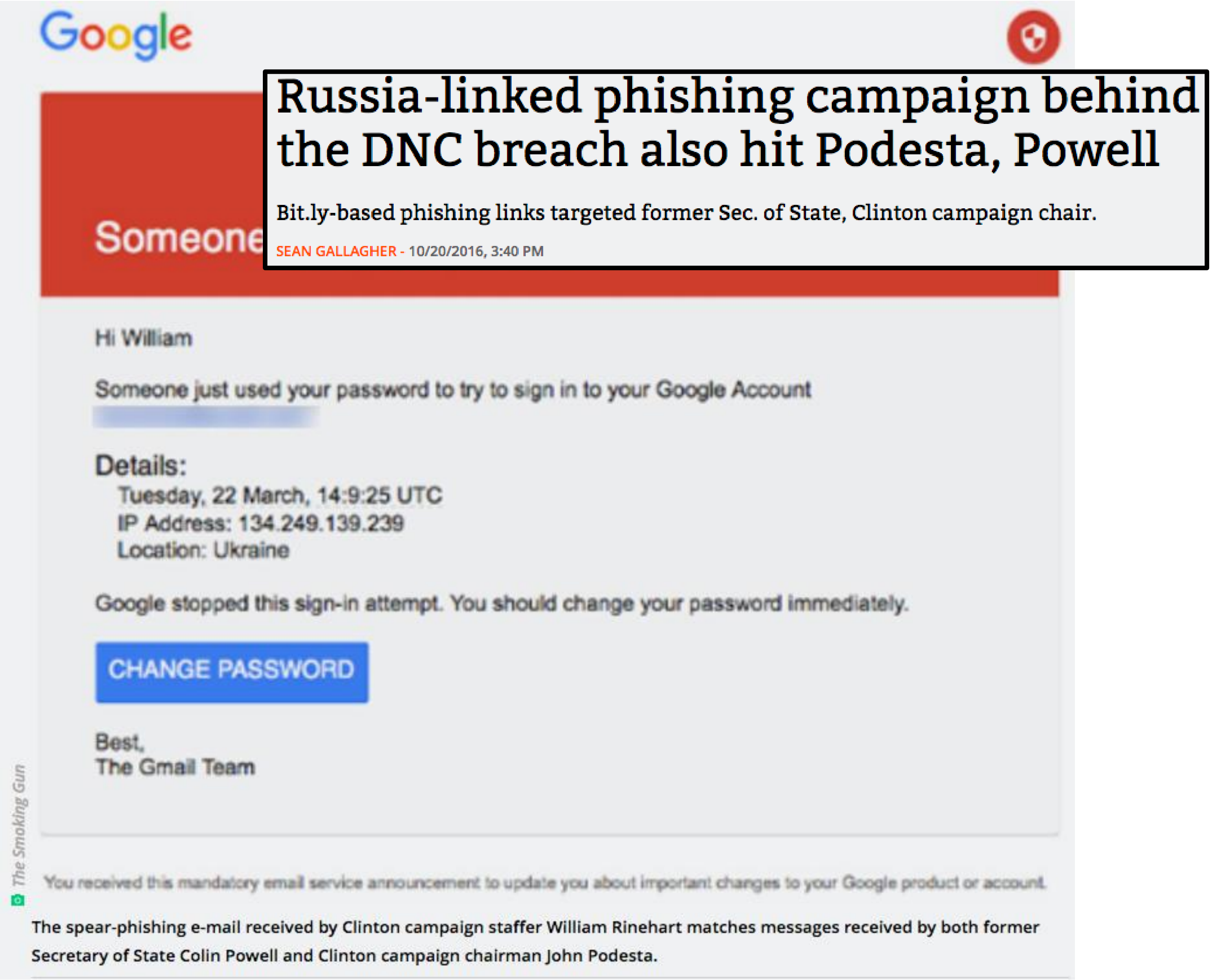
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

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

Best,
The Gmail Team

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

The Smoking Gun



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

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.

Best,
The Gmail Team

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

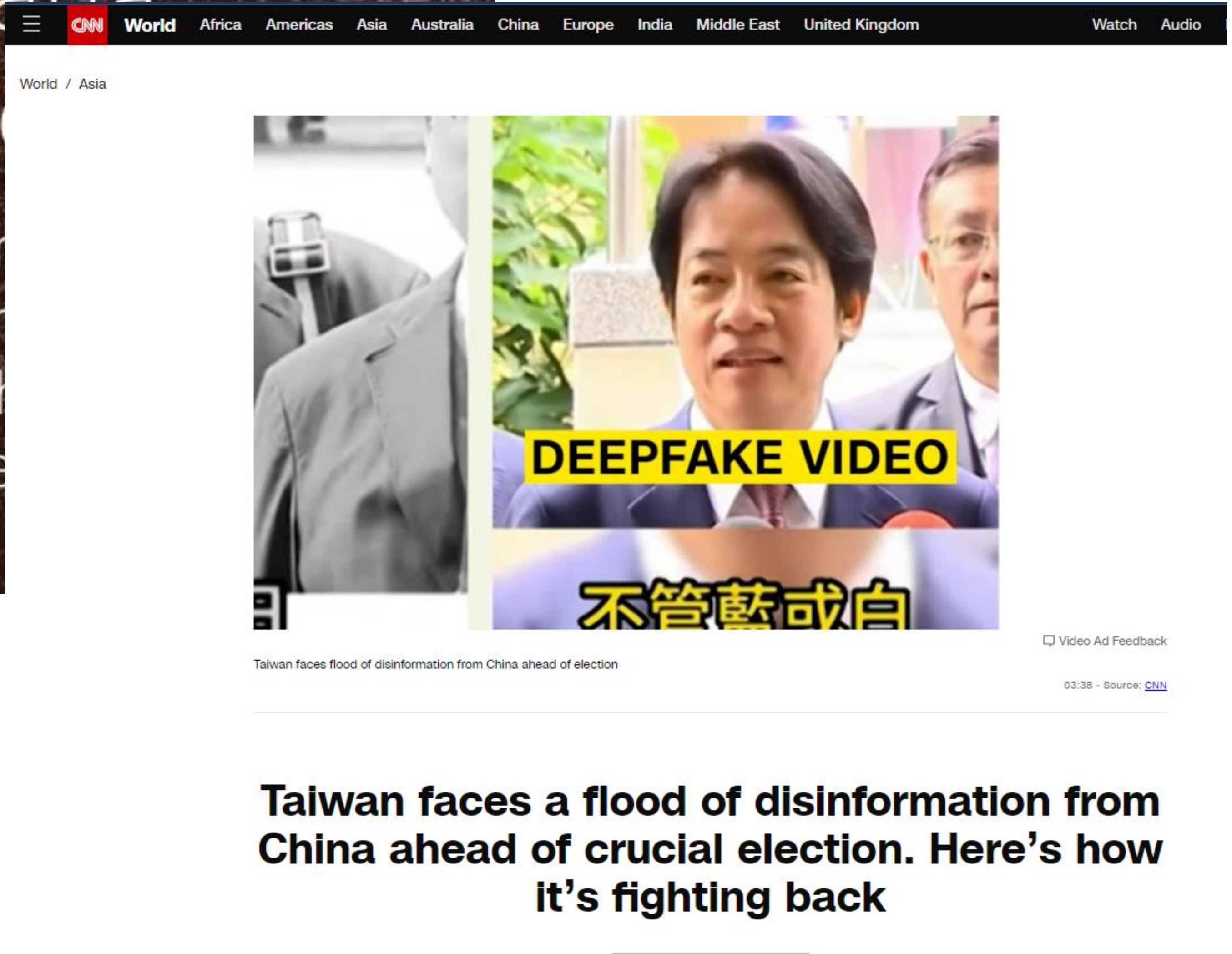
The Smoking Gun

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.

Graphika

IRA in Ghana: Double D

Russian operatio
IRA associates em
media users in Gh
black communitie



World / Asia

Taiwan faces flood of disinformation from China ahead of election

03:38 - Source: CNN

Taiwan faces a flood of disinformation from China ahead of crucial election. Here's how it's fighting back

Lessons From History

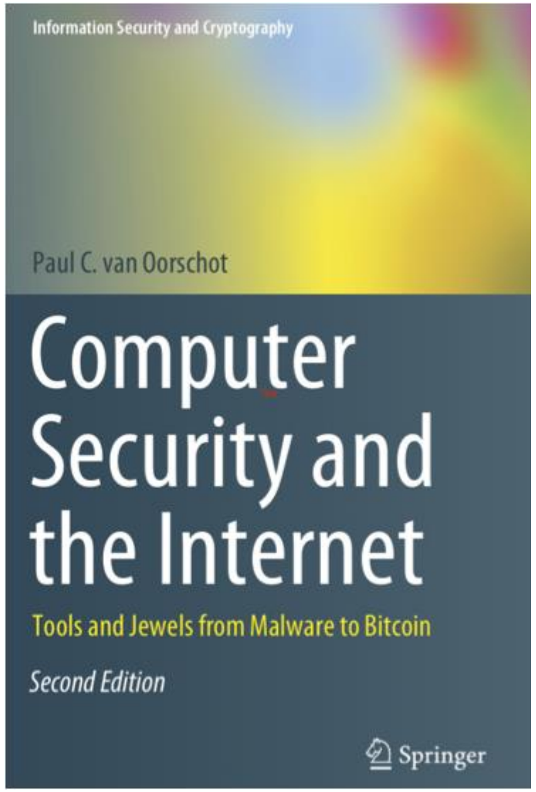
- Attacks continue to evolve and improve over time
- Security is very, very, hard, even for well-resourced, motivated organizations
- We need systematic tools and techniques to organize our thinking rather than scattershot approaches

Part 4: Key Security Properties

Towards Achieving Security

Some key points from Chapter 1 for today

- Fundamental goals of computer security
- Adversary modeling and security analysis



Information Security and Cryptography

Paul C. van Oorschot

Computer Security and the Internet

Tools and Jewels from Malware to Bitcoin

Second Edition

Springer

What Properties Do We Want For Security?

- Confidentiality: Information kept private
- Integrity: Information not secretly modified
- Availability: Information readily accessible

What Properties Do We Want For Security?

- **Confidentiality:** Information kept private
- **Integrity:** Information not secretly modified
- **Availability:** Information readily accessible
- **Authorization:** Resource accessible only by certain entities
- **Authentication:** Principal/data is genuine
- **Accountability:** Responsible for past actions

Part 5: Threat Modeling

An Example: Police Body Cams

- Worn continuously by police while on duty
- Records activity to storage
- Used in court, training, adjudicating complaints, …

These should be "secure," right? → Where to start?

Assessing a System’s Attack Surface

1. Articulate security policies around data and other assets
2. Diagram the system in a simple, yet useful, way
3. Model the adversaries about whom we are worried
4. Engage in “threat modeling” to enumerate relevant attacks by adversaries against the diagrammed system

Step 1: Assets

1. Video data
2. Actual cameras
3. Camera configuration equipment
4. Administration server
5. Remote storage server & account (third party)

Step 1: Policies

- How do you create a security policy?
- One approach:
  - Identify on the functional goals of the system
  - Think about what security properties are necessary to maintain these functional goals
  - Develop policies around what actions do/don’t violate these properties

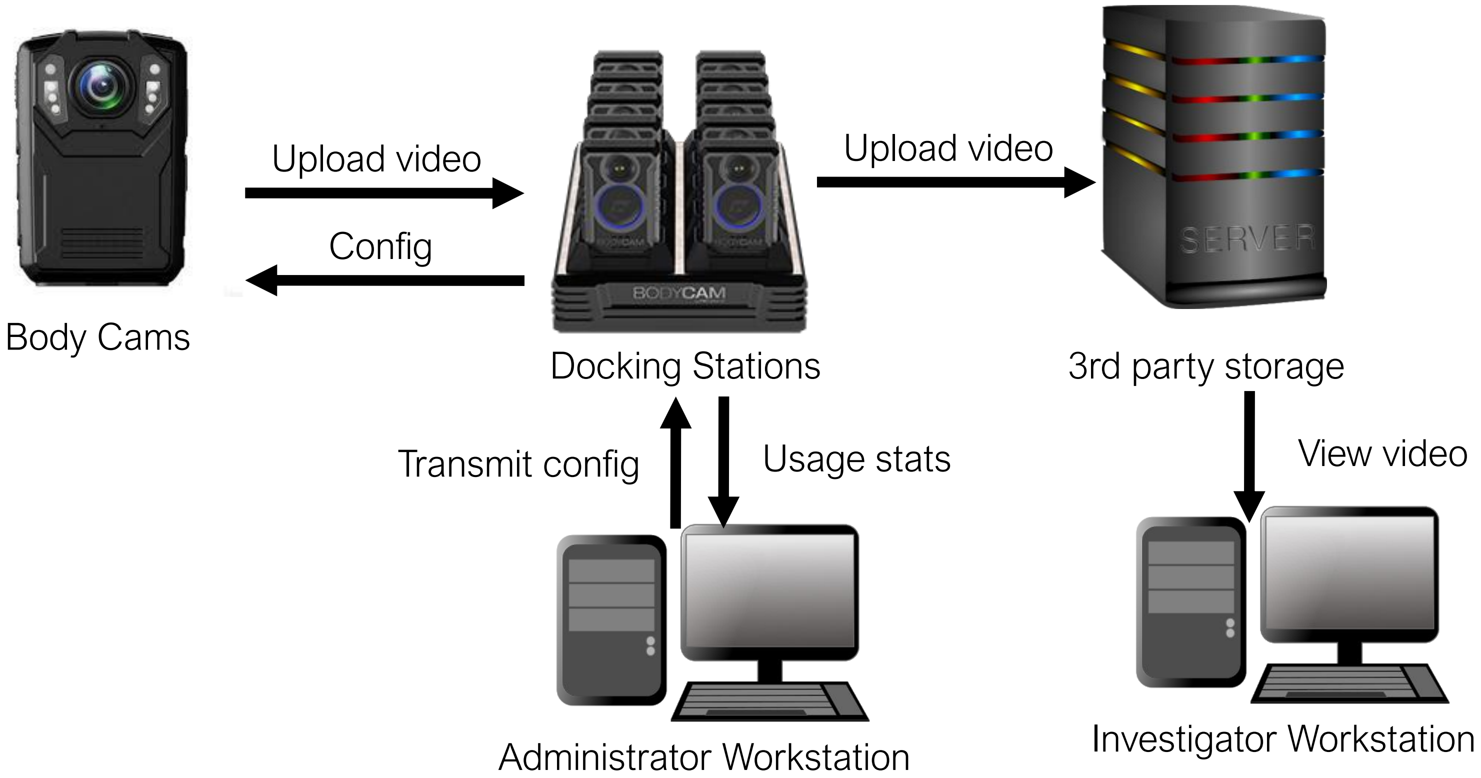
Step 1: Policies

- **Functional Goal:** Accurately capture police behavior and make videos available for authorized viewing

- **Security Policies:**
  - Only authentic videos from official cams should be stored [Authentication]
  - Police cannot turn camera off without being logged [Accountability]
  - Videos cannot be modified or edited, except via a formal process to redact accidental recordings (e.g., bathroom use) [Integrity, Confidentiality]
  - Video data should be retained for X years [Availability]
  - Video should only be accessible with court approval [Confidentiality, Authorization]

Step 2: Diagram the System

- Principal components and interactions
- Sometimes "trust boundaries" (e.g. cloud vs. on-premises)

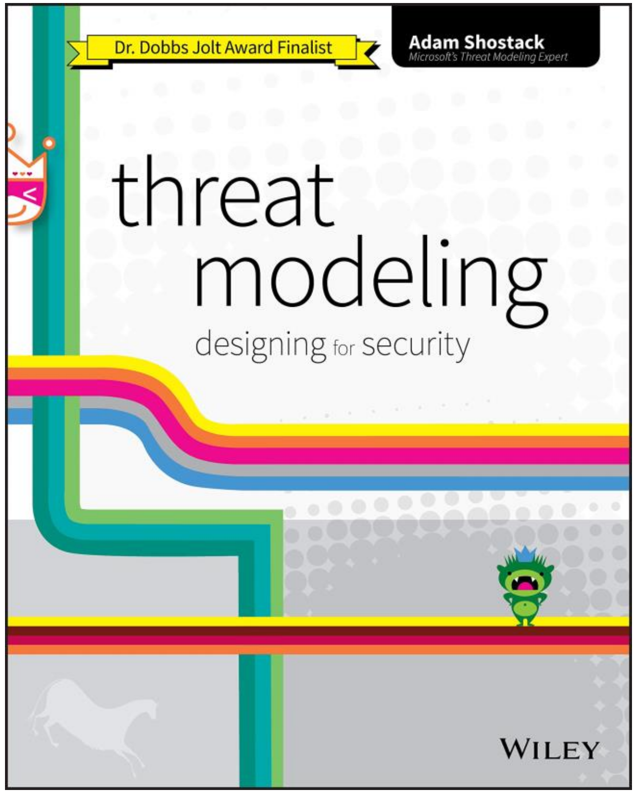


Step 3: Begin Adversary Modeling

- Goal: Scoping the capabilities of realistic attackers about whom we’re worried (what they **can** and **cannot** do)
  - Criminal trying to delete video
  - Domestic hacker (outsider) seeking videos
  - Corrupt police officer hiding activity
  - Corrupt police department hiding activity
  - Corrupt administrator spying
  - Insider at body cam vendor planting backdoor
  - Insider at storage provider snooping videos
  - Foreign government-level hackers fomenting distrust of government

Step 4: Threat Modeling

- Threat Modeling = brainstorming crutch for “what could go wrong?”
- Examples:
  - STRIDE (Microsoft)
  - Attack Trees
  - Center of Gravity (CoG)
  - PASTA
  - DREAD


Dr. Dobbs Jolt Award Finalist
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY

STRIDE Threat Modeling

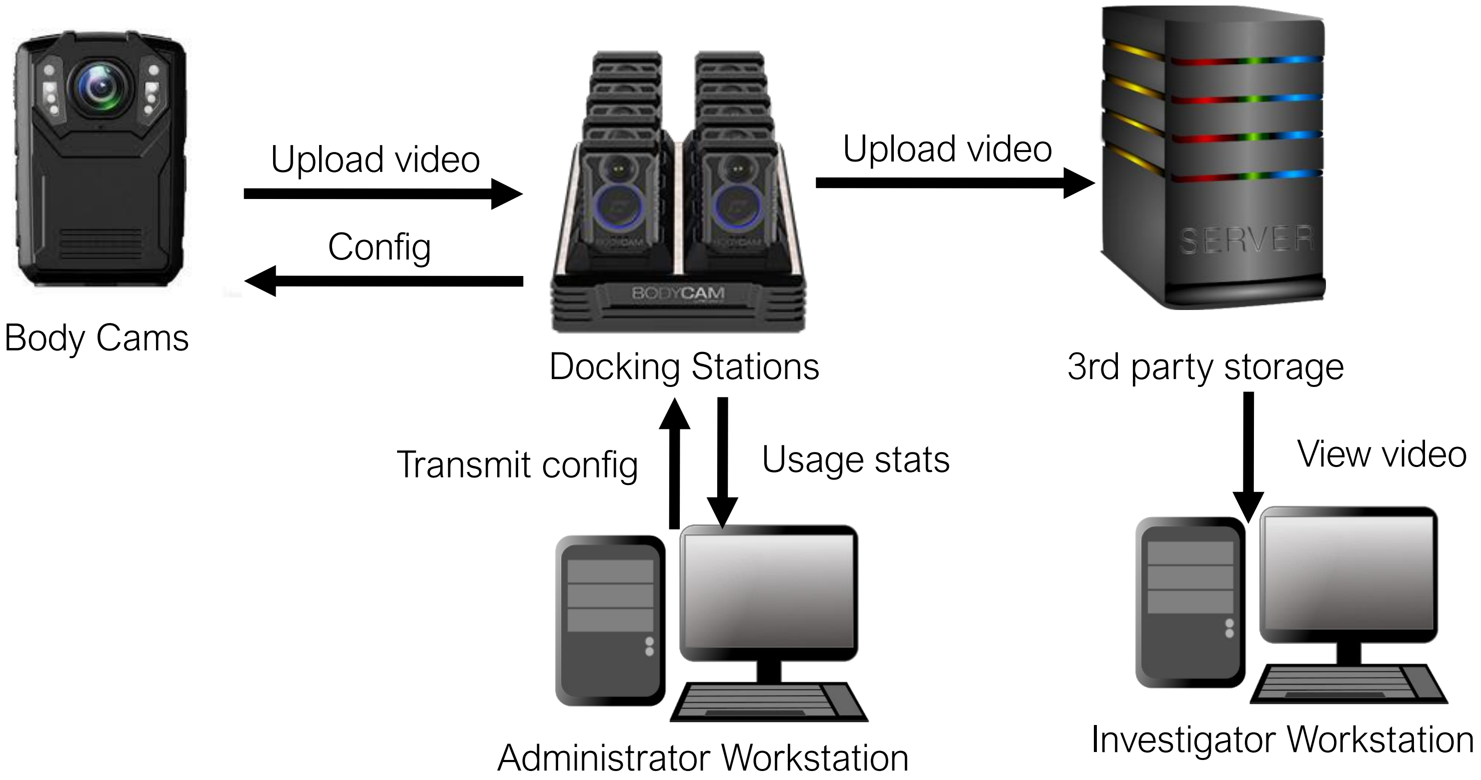
- Brainstorm attacks that fit each of six categories:

  Spoofing [Authenticity]
  Tampering [Integrity]
  Repudiation [Accountability]
  Information disclosure [Confidentiality]
  Denial of service [Availability]
  Elevation of privilege [Authorization]

- Can search for each type against each component in diagram
- Can search for each type as mounted by each adversary

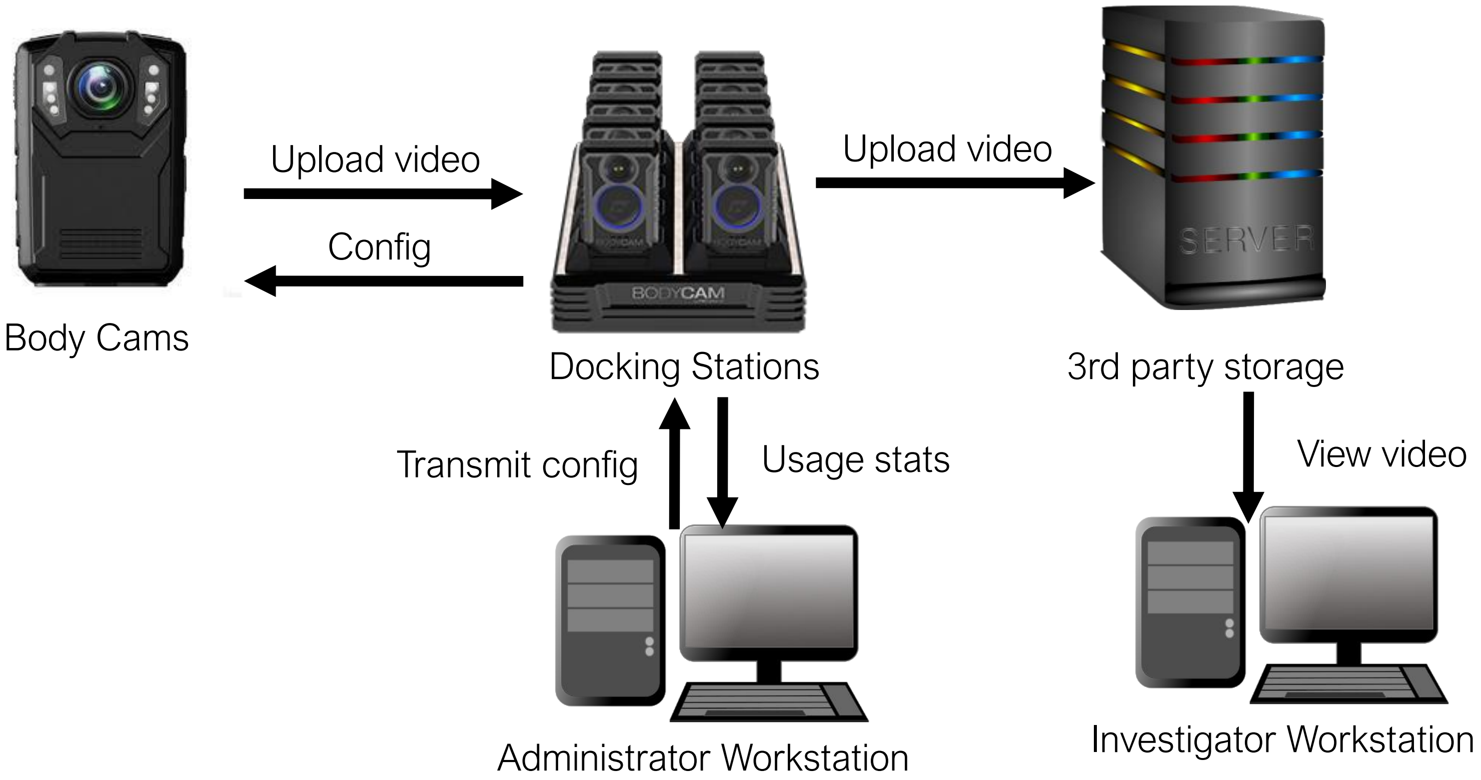
STRIDE-by-Component Exercise

- Spoofing



STRIDE-by-Component Exercise

- Tampering



The Security Mindset

- Security is highly dependent on context and relies on experience for accurate threat modeling

- One approach for analyzing the security of a system:
  - Craft a security policy based on the assets, functional goals, and desired security properties
  - Carefully understand the architecture of our system
  - Proactively threat model to brainstorm possible attack space

The Security Mindset

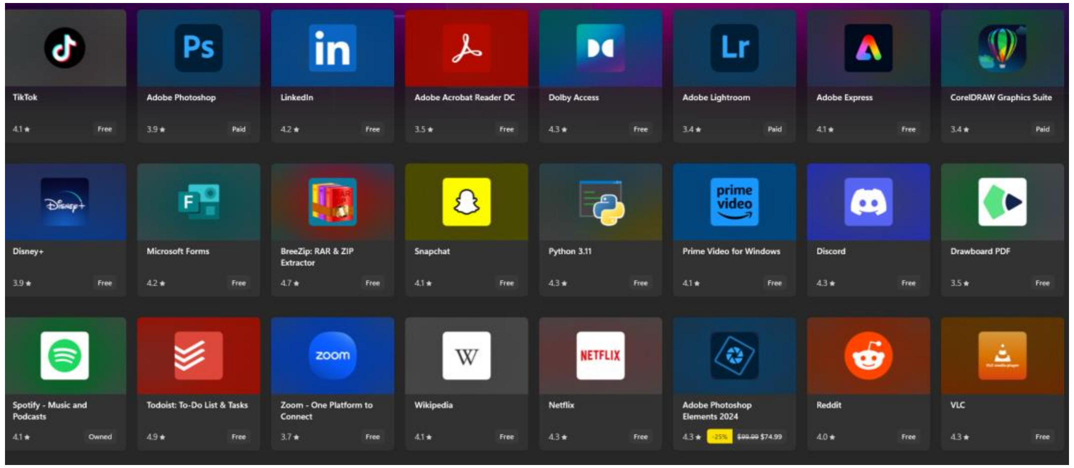
This course will look at security issues in many different settings

- Common threat models and security pitfalls (attacks)
- Secure design patterns & classical mitigations

Up Next: OS & Software Security

- How can we prevent simultaneously running programs from interfering with each other?

- How can software bugs circumvent these protections?


TikTok 4.1 ★ Free
Adobe Photoshop 3.9 ★ Paid
LinkedIn 4.2 ★ Free
Adobe Acrobat Reader DC 3.5 ★ Free
Dolby Access 4.3 ★ Free
Adobe Lightroom 3.4 ★ Paid
Adobe Express 4.1 ★ Free
CorelDRAW Graphics Suite 3.4 ★ Paid
Disney+ 3.9 ★ Free
Microsoft Forms 4.2 ★ Free
BreeZip: RAR & ZIP Extractor 4.7 ★ Free
Snapchat 4.1 ★ Free
Python 3.11 4.3 ★ Free
Prime Video for Windows 4.1 ★ Free
Discord 4.3 ★ Free
Drawboard PDF 3.5 ★ Free
Spotify - Music and Podcasts 4.1 ★ Owned
Todoist: To-Do List & Tasks 4.9 ★ Free
Zoom - One Platform to Connect 3.7 ★ Free
Wikipedia 4.1 ★ Free
Netflix 4.3 ★ Free
Adobe Photoshop Elements 2024 4.3 ★ -25% ~~$99.99~~ $74.99
Reddit 4.0 ★ Free
VLC 4.3 ★ Free