

# Messaging and Network Security: Guest Lecture, Current Topics in Information Systems and Technology

Joe St Sauver, PhD (joe@uoregon.edu or joe@internet2.edu)  
Security Programs Manager, Internet2

Utah Valley University, Orem Utah  
December 1st, 2009

<http://www.uoregon.edu/~joe/uvu/>

# Introduction; Disclaimer; Agenda

- It's a real pleasure to meet with you tonight by telephone from the University of Oregon to talk with you a little about messaging and network security. Let me thank your instructor, and my colleague, Jaren T. Angerbauer, for the invitation to be with you tonight.
- Let me also note for the record that while Jaren invited me to be with you, the opinions I'll express tonight are solely my own, and do not necessarily represent the opinion of Jaren, nor the Utah Valley University, the University of Oregon, Internet2, or any other party.
- I've got some material I've put together to set the stage for tonight's session, and when we're through with that, since this is a small group, we can either spend the rest of the time talking, or I can cover some other material I've previously delivered.

# Utah and Networking

- You're fortunate to live in Utah, a wonderful state with great people, and to be studying systems and networks.
- You may know that Utah has the honor of having hosted one of the earliest nodes on what grew to become the Internet: e.g., the fourth node on ARPANET (after only UCLA, SRI at Stanford, and UCSB). It was a DEC PDP-10 running Tenex at the University of Utah graphics department, and the year was December 1969.\*
- Utah continues to be in the forefront of networking. For example, Utah National Guard Camp Williams was recently announced as the location for a major new data center which will support the intelligence community.\*\*

----

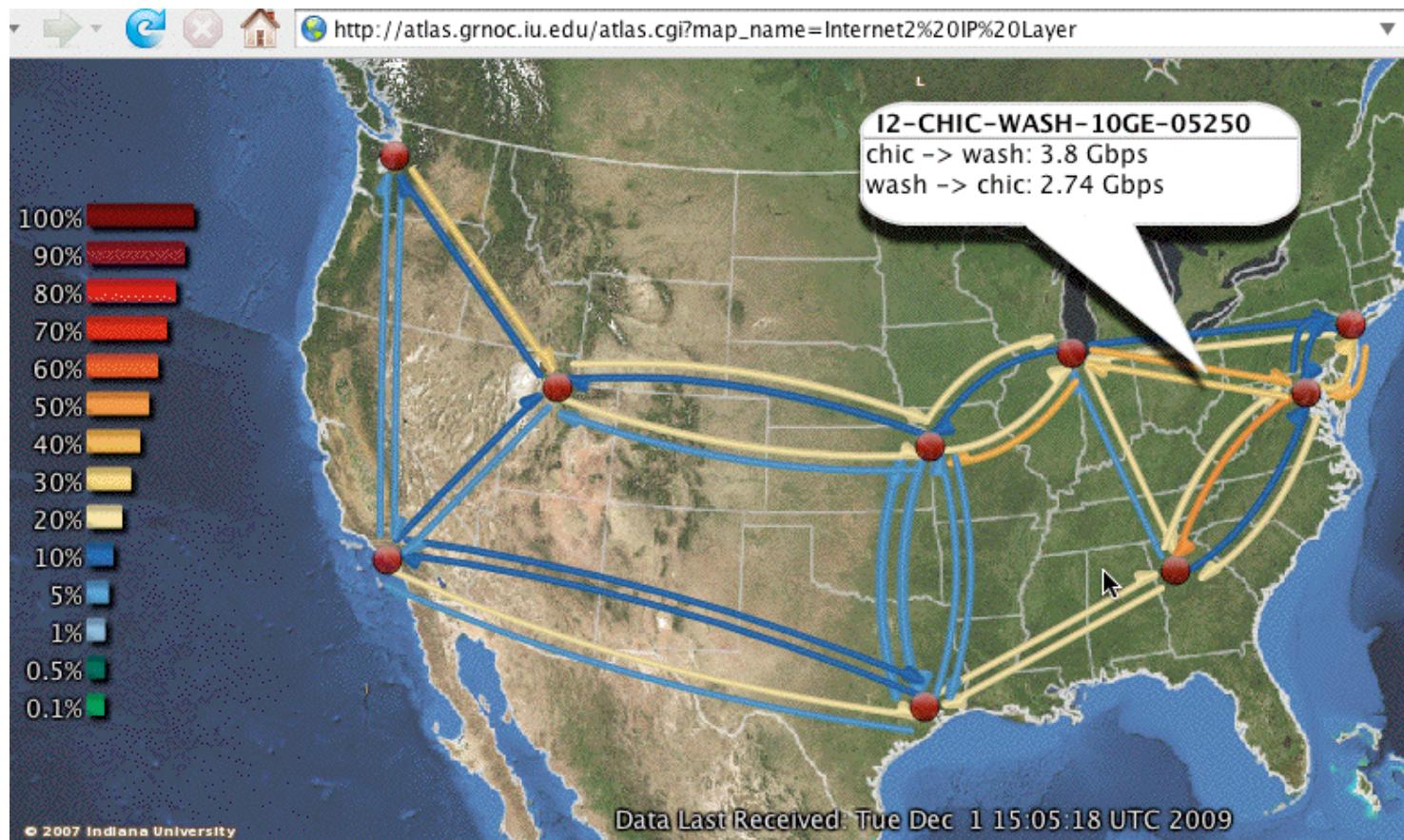
\* [http://www.livinginternet.com/i/ii\\_arpanet.htm](http://www.livinginternet.com/i/ii_arpanet.htm)

\*\* [http://www.odni.gov/speeches/20091023\\_speech.pdf](http://www.odni.gov/speeches/20091023_speech.pdf)

# A Little About Me, and About Internet2

- My Ph.D. is in Productions and Operations Management from the University of Oregon (UO) School of Business, and I work as Internet2's Security Program Manager under contract through UO Information Services.
- If you're not familiar with Internet2, you can read all about it at <http://www.internet2.edu/> at your leisure, but for now, you can think of it as "higher education's high speed national network backbone" (plus a lot more).
- Internet2 doesn't replace the conventional commercial Internet, it runs "along side it."
- Internet2 carries conventional IPv4 packet traffic between leading higher education sites, while also supporting advanced services such as jumbo frames, IPv6, IP multicast and dynamic circuit connections.

# The Internet2 Backbone This Morning



Yes, the third red dot from the left represents an Internet2 routing node that's in Salt Lake City, one of only nine in the country. See, Utah is special! :-)

# A Brief Geek Discursion: The Internet2 Path From Me to You at UVU

- Whether you're aware of it or not, UVU has connectivity to Internet2 via Westnet/the Utah Education Network.
- % traceroute www.uvu.edu  
traceroute to webprod.uvu.edu (161.28.25.131), 30 hops max, 40 byte packets  
1 vl-214.uonet2-gw.uoregon.edu (128.223.214.3) 1.785 ms 0.384 ms 0.347 ms  
2 0.ge-0-1-0.uonet8-gw.uoregon.edu (128.223.3.8) 0.374 ms 0.601 ms 0.464 ms  
3 vl-105.ge-2-0-0.core0-gw.pdx.oregon-gigapop.net (198.32.165.89) 2.807 ms  
2.886 ms 2.849 ms  
4 vl-101.abilene-losa-gw.oregon-gigapop.net (198.32.165.66) 29.27 ms 24.87 ms  
24.851 ms  
5 so-3-1-0.0.rtr.salt.net.internet2.edu (64.57.28.47) 48.245 ms 48.221 ms  
48.231 ms  
6 i2-urn-salt.net.internet2.edu (64.57.28.30) 48.501 ms 48.63 ms 48.516 ms  
7 140.197.252.87 (140.197.252.87) 48.458 ms 48.44 ms 48.48 ms  
8 140.197.252.98 (140.197.252.98) 49.44 ms 49.527 ms 49.471 ms  
9 140.197.252.109 (140.197.252.109) 49.516 ms 50.778 ms 49.438 ms  
10 204.113.112.98 (204.113.112.98) 49.807 ms 49.776 ms 49.757 ms  
11 webprod.uvu.edu (161.28.25.131) 51.131 ms 50.658 ms 50.207 ms

# Whois

- How could we find out who is responsible for some of the IP's that don't have reverse DNS on the preceding slide? We could use whois...
- % whois -h whois.arin.net 140.197.252.87

OrgName: Westnet West Regional Network

OrgID: WWRN

Address: Computer Center

Address: 3440 Merrill Engineering Building

Address: Univiersity of Utah

City: Salt Lake City

StateProv: UT

PostalCode:

Country: US

NetRange: 140.197.0.0 - 140.197.255.255

CIDR: 140.197.0.0/16

NetName: WESTNETW-NET

[continues next slide]

# Whois (continued)

[continuing from preceding slide]

NetHandle: NET-140-197-0-0-1

Parent: NET-140-0-0-0-0

NetType: Direct Assignment

NameServer: NS.UTAH.EDU

NameServer: NS1.WESTNET.NET

Comment:

RegDate: 1990-06-01

Updated: 1991-02-15

RTechHandle: AC98-ARIN

RTechName: Cole, Allen

RTechPhone: +1-801-581-8805

RTechEmail: cole@cc.utah.edu

FWIW, Allen Cole doesn't show up in the University of Utah online directory, and that phone number is listed as belonging to someone in Environmental Health & Safety. After going on twenty years, you have to expect some changes, I guess. :-)

# Back To More Boring Background Stuff

- In addition to the work I do for the University of Oregon and Internet2, I'm also am active in a variety of national and international security-related initiatives.
- For example, I serve as one of half a dozen senior technical advisors for the Messaging Anti-Abuse Working Group (MAAWG), the carrier anti-spam forum. MAAWG participants include AOL, AT&T, Bell Canada, Cablevision, Comcast, Cox, Earthlink, France Telecom, Google, HP, Microsoft, Sprint, Sun, Time Warner, Verizon, Yahoo and many others key companies. To read more about MAAWG, see <http://www.maawg.org/>
- I've got some fairly uncommon talks about network security-related topics available on my home page at <http://www.uoregon.edu/~joe/>

# The Odd Format Of This (And All My) Talk(s)

- Pretty much all of my talks have a fairly distinctive format, much like the one you're looking at right now.
- Don't let this strange format shake you up. You're not expected to read it as I go along, nor, hopefully, will I be reading my slides to you.
- So why do detailed slides?
  - without them, I tend to ramble and get side tracked
  - I often share a lot of detail, and detailed slides mean that you don't need to scramble to take notes
  - detailed slides mean I hopefully won't be misquoted
  - detailed slides are helpful if you're hard of hearing or deaf, or if you're a non-native english speaker, and
  - detailed slides index better in Internet search engines than sparse "bulleted outline"-format talks

# I. How Did We Get Where We Are Today?

# I'm From the Old School

- My earliest computing experience dates all the way back to my high school years, when I'd write BASIC programs on an ASR 33 teletypewriter. That TTY connected via a 110 baud acoustical coupler over a dialup phone line to an HP time sharing system at St Johns University in Collegeville, Minnesota. My programs were stored on, and read from, punched paper tape.
- When I graduated from that TTY, I moved on to punched cards, COBOL and a large Amdahl (an IBM mainframe clone), courtesy of a Boy Scouts of America Explorer Scout program offered at Burlington Northern Railroad.
- Things were different back then, most notably because that was still 10 years before the Internet took off (even NSFNet, a 56kbps network, only dates to ~1985)

# Acoustic Coupler; ASR 33; Punched Cards



[http://commons.wikimedia.org/wiki/File:AJ\\_311\\_Acoustic\\_modem.JPG](http://commons.wikimedia.org/wiki/File:AJ_311_Acoustic_modem.JPG)

[http://commons.wikimedia.org/wiki/File:ASR-33\\_1.jpg](http://commons.wikimedia.org/wiki/File:ASR-33_1.jpg)

<http://commons.wikimedia.org/wiki/File:Punch-card--fortran.jpg>

# Yes, There Was Life Before The Internet

- Do you remember:
  - computing that didn't emphasize networking? :-;
  - when doing research for a paper involved visiting a library and using a card catalog, and writing that paper meant using a typewriter?
  - when communicating with a remote friend or relative involved mailing a letter or calling "long distance?" (to say nothing of telegrams, cables, and ham radio!)
  - when news came from morning & evening newspapers?
  - when music came from a radio, or on records?
  - when pictures and movies were shot on film?
  - when shopping was done in person?
  - when friends were usually people we'd met in person?
- Much has changed as a result of the Internet, most things for the better.

# But Do You Also Remember...

- What life was like before...
  - you had to apply a never-ending cycle of computer patches and updates?
  - spam grew to be >90% of all email?
  - you even knew what malware was?
  - phishing and online scams had become routine part of your life?
  - you enjoyed some measure of personal privacy?
  - you had to be continually “connected” and reachable?
- Simpler times, no question about it. We were all to some degree innocents.
- Now we live and work in a “flattened world.”

**Distance Is Now (Largely) Irrelevant;  
The Whole World's Our Neighbor**

# Accra, Ghana, The Old Way

- I recently attended the 7th Open Access Conference in Accra, Ghana (see [www.wideopenaccess.net](http://www.wideopenaccess.net) ), as well as the West and Central African National Research and Education Networks meeting held at the same time.
- To be able to go to Ghana, I had to apply for a visa by sending my passport, four recent photos and a fee to the Embassy of Ghana in Washington DC.
- I also needed to be vaccinated for yellow fever and to take a course of mefloquine for malaria prophylaxis.
- When it was actually time to travel, I took a half hour flight to PDX, then an eleven hour flight from PDX to AMS, plus a seven hour flight from AMS to ACC.
- I also needed to go through customs going into Ghana, and coming back into the United States.

# Accra, Ghana, The New Way

- # tcptraceroute www.ug.edu.gh

Tracing the path to www.ug.edu.gh (80.87.82.10) on TCP port 80 (http), 30 hops max

```
1 vl-214.uonet2-gw.uoregon.edu (128.223.214.3) 0.477 ms 0.624 ms 0.242 ms
2 0.ge-0-1-0.uonet8-gw.uoregon.edu (128.223.3.8) 0.333 ms 0.404 ms 0.310 ms
3 vl-3.uonet9-gw.uoregon.edu (128.223.3.9) 0.262 ms 0.405 ms 0.296 ms
4 euhn-car1-gw.nero.net (207.98.68.181) 0.257 ms 0.403 ms 0.322 ms
5 euhn-core2-gw.nero.net (207.98.64.162) 0.446 ms 0.496 ms 0.395 ms
6 ptck-core2-gw.nero.net (207.98.64.10) 2.835 ms 2.942 ms 2.879 ms
7 ptck-core1-gw.nero.net (207.98.64.137) 2.907 ms 3.198 ms 3.085 ms
8 so-6-1.hsa2.seattle1.level3.net (63.211.200.245) 6.209 ms 6.135 ms 6.206 ms
9 ae-31-51.ebr1.seattle1.level3.net (4.68.105.30) 6.630 ms 14.064 ms 17.981 ms
10 ae-1-100.ebr2.seattle1.level3.net (4.69.132.18) 17.136 ms 16.708 ms 17.913 ms
11 ae-2.ebr2.denver1.level3.net (4.69.132.54) 33.939 ms 33.542 ms 41.370 ms
12 ae-3.ebr1.chicago2.level3.net (4.69.132.62) 57.202 ms 56.552 ms 57.010 ms
13 ae-1-100.ebr2.chicago2.level3.net (4.69.132.114) 56.631 ms 56.916 ms 56.728 ms
14 ae-2-2.ebr2.washington1.level3.net (4.69.132.70) 74.551 ms 74.285 ms 74.528 ms
15 ae-62-62.cswh1.washington1.level3.net (4.69.134.146) 84.909 ms 74.636 ms
84.055 ms
16 * ae-1-69.edge1.washington4.level3.net (4.68.17.18) 75.758 ms 76.137 ms
17 * cable-wire1.edge1.washington4.level3.net (4.53.112.2) 76.115 ms 75.688 ms
18 ge-1-0-0.dcr1.ash.cw.net (195.2.21.185) 75.964 ms 77.243 ms 76.054 ms
19 so-7-0-0-ecr2.mia.cw.net (195.2.3.54) 89.878 ms 90.129 ms 90.064 ms
20 ptcomm3.mia.cw.net (195.2.6.22) 233.013 ms 223.828 ms 229.685 ms
21 lis2-br1-gi-12-0-0.cprm.net (195.8.0.90) 234.631 ms 234.512 ms 243.170 ms
22 ghanatel1.10.8.195.in-addr.arpa (195.8.10.182) 299.999 ms 309.304 ms 330.711 ms
23 arn-m10i-core-ge-0-1-0-vlan2.4u.com.gh (80.87.78.2) 417.906 ms 382.507 ms 343.059 ms
24 * * *
```

# www.ug.edu.gh

http://www.ug.edu.gh/ Google

UNIVERSITY OF GHANA

Home | SiteMap | Enquiry

SEARCH  GO

About US | Central Administration | Academics | Library | Staff |  
Students | Alumni | International Programmes |  
News, Events & Announcements | Block

Welcome to the University of Ghana  
Aerial view of the Great Hall.

Next

**EVENTS**

Sunday **DEC 13** Volta Hall's 50th Anniversary; Praise & Thanksgiving Service  
Time: 10:30 am  
Venue: Volta Hall

**HIGHLIGHTS**

 **University of Ghana Campus Update**  
A quarterly news letter of the University of Ghana...[read more]

**ANNOUNCEMENTS**

**Dec. 01**  
Invitation to the 'Heritage Matters' Conference, 15-17 December 2009, AICC, Accra

**Nov. 26**  
Vacancies: University of Ghana -

**UNIVERSITY NEWS**

24/11/2009 **Victorious UG Team Calls on Vice-Chancellor**  
  
The University of Ghana has emerged winners at this year's Inter-University Cross Country race, held at the University of Education, Winneba, recently...  
[read more]

**QUICK LINKS**

» Annual Report  
» Staff Directory  
» About UG  
» National Service PINS  
» ICT Directorate  
» Staff Webmail  
» MIS Web  
» Employment Opportunities

**SPOTLIGHT**

**EXAMS SCHEDULE**

schedule	SUN	MON	TUES

# Some of The Differences, Old vs. New

- In the new way:
  - I didn't need to get a visa
  - No one in Ghana even knew that I'd "visited"
  - I didn't need any inoculations or other medications
  - My "travel time" was half a second
  - My travel cost was zero
  - There was no border control
- On the other hand, in the old way:
  - I made some great new friends, and
  - I experienced the tastes, smells and sounds of Ghana.
- The key point is that distance has (largely) become irrelevant. The world has become flat, and people in West Africa are now as much my neighbors as people in Eugene or Springfield or Portland or Orem.

# We're Connected to the Whole World

- Having all those new neighbors in all the countries of the Americas, Europe, Asia, Africa, and Oceania is generally an amazing and wonderful thing.
- I'm now connected to the world!
- However there are still a few "minor" issues:
  - I should have paid more attention in geography class
  - we don't speak the same language (although as an english speaker, I'm far more fortunate than many)
  - we don't even use the same alphabet(s) (again, using the latin alphabet is far easier than using hangul, say)
  - we aren't up and active at the same time (try finding a time for a conference call if you've got people on the East and West Coast of the United States, Europe, and Asia who all need to participate!)
  - we still lack adequate bandwidth to some locations<sup>21</sup>

**There's Good and Bad In Everything**

# Oh, and One Other Problem: Bad Neighbors

- There's one other problem that I should mention, and that is the problem of bad online neighbors.
- Let's assume that 99.999% of all people online are good, regardless of where they live, are honest, hardworking people, just like you and I. Unfortunately, that still leaves a residual,  $100\%-99.999\% = 0.001\%$ , or 1 in 100,000, of all people online who are NOT good.
- If we assume that there are 6,800,589,053 people in the world as of 17:27 UTC on Dec 01, 2009, and that one quarter of them are online, that implies that there are still  $6,800,589,053 * .25 * .00001 = 17,001$  bad people online.
- Those 17,001 bad online neighbors all have the ability to raise heck online, doing things like sending spam, phishing for your credentials, hacking/cracking systems, etc.

# Real World vs. Online

- Of course, my 99.999 vs. 0.001 split may be optimistic, as is the assumption that that sort of split is consistent across countries. Let's just consider the proportion of people incarcerated\* in some common countries as one benchmark for our 1-in-100,000 estimate:

United States	2,310,984 prisoners (760/100,000)
Russian Federation	877,595 prisoners (620/100,000)
Brasil	469,546 prisoners (242/100,000)
UK (England & Wales)	84,622 prisoners (154/100,000)
China	1,565,771 prisoners (119/100,000)
France	59,655 prisoners (96/100,000)
Switzerland	5,780 prisoners (76/100,000)

----

\* <http://www.kcl.ac.uk/depsta/law/research/icps/worldbrief/>

# Hmm... Adjusting Our Estimate

- Of course, most people in prison (hopefully!) aren't online, and many criminals reform while in prison, but what if everyone who was in prison got out and went online to engage in criminal behavior?
- If the \*real\* rate of online badness worldwide is 760/100,000 (e.g., the US incarceration rate), that would imply we'd have 12,921,119 bad people online. If the \*real\* rate of online badness worldwide was "just" 76/100,000 (e.g., the rate of incarceration in CH), that would imply we'd "only" have 1,292,112 bad people online.
- One way or the other, however, whether we're talking about 17,001 or 1,292,112 or 12,921,119 bad people online, there ARE bad people online these days, and we see them when they spam, scam, phish, hack/crack, etc.

# International Law and Cyber Crimes

- While all the world's our neighbor now, law enforcement is still largely a national (or local!) matter.
- If I violate the law here in Eugene, I will likely deal with the Eugene Police Department, or the Lane County Sheriff, or the Oregon State Police, or perhaps the Federal Bureau of Investigation. I will not be arrested by some pan-national police force. This is as true elsewhere as it is here.
- But now remember that I may be subject to an online attack coming from a compromised computer that's located somewhere I've never heard of before, and where the police don't speak english, and where they have more serious violent crime problems than someone trying to hack/crack one of my systems. In fact, many countries may not even have any laws covering cyber crime. 26

# The International Corruption Problem

- While it would be great if international corruption wasn't a problem, unfortunately, it is. For international corruption rankings, see Transparency International's Annual Corruption Report, [www.transparency.org](http://www.transparency.org)
- We must recognize that cyber criminals will pay relevant authorities to "look the other way" when it comes to cyber crimes, particularly if the cyber crimes appear "minor" ("it's only a little spam, after all"), or the official in question is underpaid and has a hungry family he/she's trying to keep alive (this doesn't excuse that corruption, but it does make it understandable).
- Combine tottering economies, out-of-date laws, corruptable officials and good connectivity, and you have a recipe for cybercrime activity hotspots.

**Bringing This Back to Messaging**

# What Does This All Have to Do With Messaging?

- Contrary to what you might think, the first networks were not designed for email. :-)
- Initially, networks were meant as a way for scientists to be able to login and work on remote systems (think of the “telnet” protocol, although that wasn’t what was actually used at that time), and to copy files from one system to another (think of “ftp”, although again, that wasn’t the actual protocol in question).
- For a discussion of how email did arise, see “Email History,” <http://www.livinginternet.com/e/ei.htm> and “First Email Message,” <http://www.velocityguide.com/internet-history/first-email-message.html> and <http://www.nobell.org/~gjm/about/ihnp4.html>

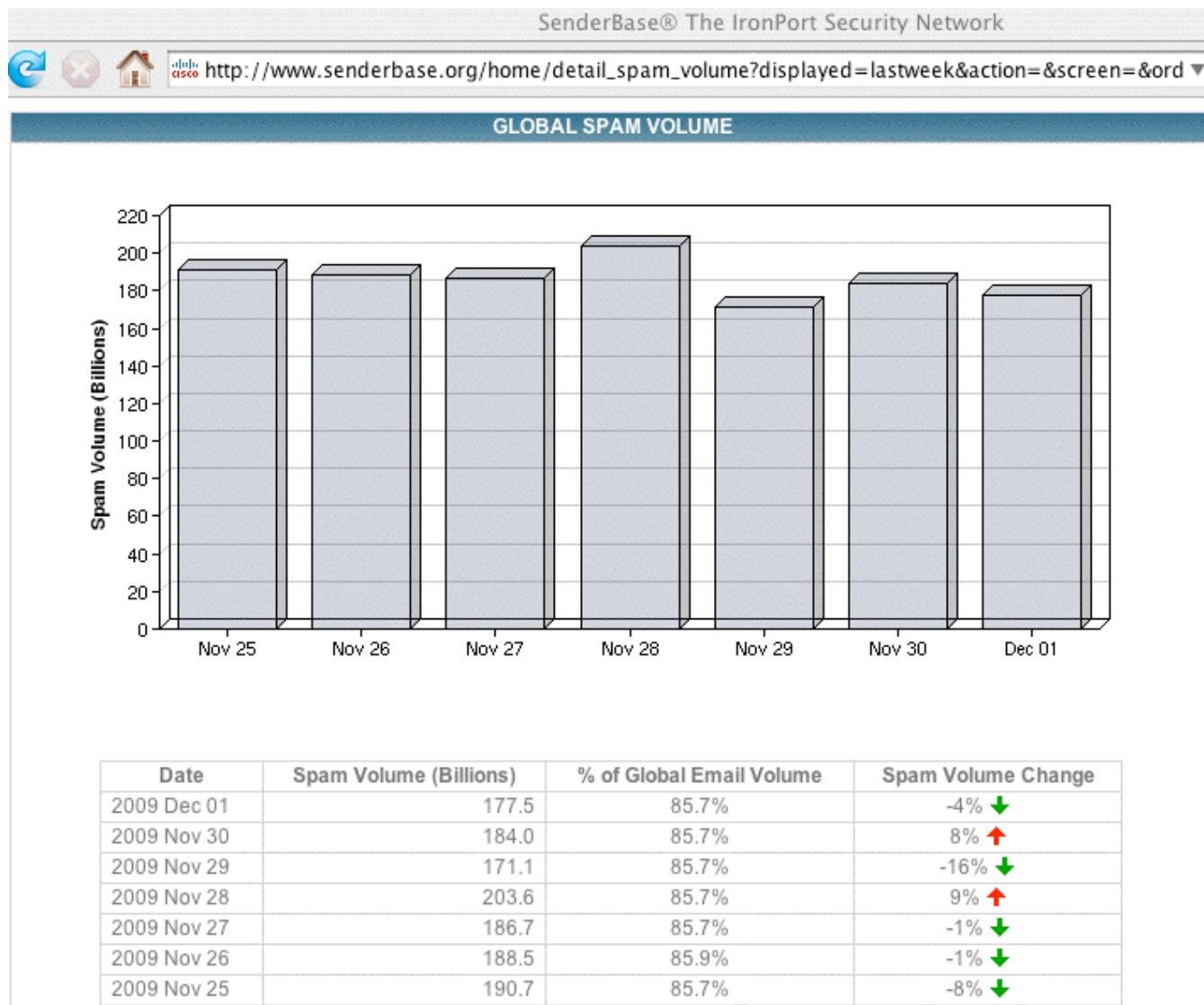
# The First Spam and Commercial Use

- The first spam sent on the Arpanet was sent on May 1st, 1978, from a Digital Equipment Corporation (DEC) marketing representative, Gary Thuerk, touting a product presentation for some of their systems in California. (See <http://www.templetons.com/brad/spamreact.html#msg> )
- Because the ARPANET was non-commercial/for official government business only, this message represented a flagrant violation of ARPANET policy.
- That ban on commercial use persisted in one form or another until 1992, when Congress passed the “Scientific and Advanced-Technology Act,” legalizing interconnection of the NSFNet with commercial networks, although commercial usage remained limited through May 1995 when the NSF stopped underwriting the backbone.

# Usenet Green Card Spammers

- Email was not, and is not, the only form of messaging. For example, there was (and is) a distributed one-to-many messaging system called USENET.
- Messages in USENET are organized hierarchically by topic, and are propagated from USENET server to USENET server via NNTP (Network News Transport Protocol). Users read USENET using a news reader such as Free Agent (for Windows), trn, or tin (for Unix). Google makes at least some USENET Groups available to the public via <http://groups.google.com/>
- The first commercial spam on USENET was the famous “Green Card Spam” from Canter and Siegel, on April 12th, 1994, spamvertising their legal services to over 6,000 USENET groups.

# Spam Volumes Today



# Cybercrime Motivations

- Let there be no confusion about motivations: spammers and other cybercriminals want to make money.
- It doesn't really matter if we're talking about DEC in 1978, Canter and Siegel in 1994, or Canadian Pharmacy today, spammers are in it for the bucks.
- A couple of books that makes this entirely clear include: "Inside the SPAM Cartel: by Spammer-X," and "Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills and %\*@)# Enlargements"
- Most spammers do not operate on their own. Instead, most spammers work as part of an "affiliate program." Affiliate programs pay "affiliates" for each person they successfully "convert," or make a sale to. Payments may range from pennies to hundreds of dollars per conversion.

# Affiliate Programs

- It isn't hard to find affiliate programs -- they advertise on the web like any other business. Try googling for "affiliate programs" to see some examples.
- You should understand that there's a complete spectrum of affiliate programs, ranging from "white hat" affiliate programs do not allow their affiliates to spam to "grey hat" affiliate programs which may be ambivalent about spamming, to "black hat" affiliate programs which may affirmatively permit or even encourage spamming.
- Many affiliate programs rely on products which have huge markups, or for which legitimate online and/or bricks-and-mortar sales channels have problems.
- For example, consider erectile dysfunction ("ED") drugs such as Viagra, Cialis or Levitra.

# ED Pillz Sales From the Bad Guy's POV

- At least some erectile dysfunction ("ED") drugs sell for ~\$20/pill at neighborhood pharmacies, but just ~\$2/pill online (and those pills only cost spammers pennies/pill in bulk from overseas manufacturers). Markups are good.
- Insurance plans won't cover ED drugs, and neither are ED drugs available as generics from large discount chain store under chain store \$4 per-month-or-\$10-for-a-90-day-supply plans. Unable to afford the real thing, users will do what they feel they must.
- At least some users are also embarrassed when it comes to getting a legitimate prescription from their family doctor and then buying ED drugs from a local pharmacy. Online, they're "anonymous."

## ED Pillz Sales From the Bad Guy's POV (2)

- Law enforcement risks from selling pillz via spam are minimal (from the bad guy's point of view).
- Spam cases are complex and hard to prosecute, and spam, like most white collar crimes, isn't viewed as being "on par" with crimes of violence. That is, you're unlikely to be investigated; if investigated, you probably won't be prosecuted; if prosecuted you're unlikely to be convicted; if convicted, you won't get hard time.
- While the DEA focuses on enforcement of laws relating to controlled substances, online pharmacies which avoid controlled substances are under the jurisdiction of the FDA, an understaffed and overworked agency.
- ICE can only inspect a small fraction of each day's flood of incoming parcels. Our borders are pretty porous.

# Sometimes, However, They're Wrong...

Court Orders Australia-based Leader of International Spam Network to Pay \$15.15 Million

http://www.ftc.gov/opa/2009/11/herbalkings.shtm

**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

Home News Competition Consumer Protection Economics General Counsel Actions Congressional Policy International

About Public Affairs | Public Events | Speeches | Testimony | Webcasts | Blogs | Reporter Resources | Noticias en Español

For Release: 11/30/2009

## Court Orders Australia-based Leader of International Spam Network to Pay \$15.15 Million

### U.S. Co-Defendant Forfeits More Than \$800,000 and Faces Jail Time

At the request of the Federal Trade Commission, a federal judge has ordered the mastermind of a vast international spam network to pay \$15.15 million in a default judgment for his role in what was identified by the anti-spam organization Spamhaus as the largest "spam gang" in the world. The spam gang deceptively marketed products such as male-enhancement pills, prescription drugs, and weight-loss pills. Ringleader Lance Atkinson, a New Zealand citizen and Australian resident, last December admitted his involvement in the spam network to New Zealand authorities and has already paid more than \$80,000 (nearly \$108,000 New Zealand dollars). Atkinson's accomplice, U.S. resident Jody Smith, agreed to an order requiring him to turn over nearly all of his assets to the FTC, to settle FTC charges.

Atkinson and Smith recruited spammers from around the world, according to the FTC's complaint filed last year. The spammers sent billions of e-mail messages directing consumers to Web sites operated by an affiliate program called "Affking," according to the complaint. By using false header information to hide the origin of the messages, and by failing to provide an opt-out link or list a physical postal address, the defendants are alleged to have violated the CAN-SPAM Act of 2003.

The FTC charged that, using the "Canadian Healthcare" brand name and other labels, the defendants' spam messages deceptively marketed a male-enhancement pill, prescription drugs,

E-mail this News Release  
If you send this link to someone else, the FTC will not collect any personal information about you or the recipient.

**Related Items:**

[Federal Trade Commission v. Lance Thomas Atkinson, Inet Ventures Pty Ltd., an Australian proprietary company, Jody Michael Smith, Tango Pay Inc., a Delaware corporation, Click Fusion Inc., a Delaware corporation, TwoBucks Trading Limited, a Cyprus limited liability company.](#)  
(United States District Court for the Northern District of Illinois Eastern Division)  
FTC File No. 072 3085  
Civil Action No. 08CV5666

**Consumer Information:**

[On Guard Online Email](#)

# Sometimes, However, They're Wrong (2)



## Department of Justice

---

FOR IMMEDIATE RELEASE  
MONDAY, NOVEMBER 23, 2009  
[WWW.JUSTICE.GOV](http://WWW.JUSTICE.GOV)

CRM  
(202) 514-2007  
TDD (202) 514-1888

### DETROIT SPAMMER AND THREE CO-CONSPIRATORS SENTENCED FOR MULTI-MILLION DOLLAR E-MAIL STOCK FRAUD SCHEME

WASHINGTON – Four individuals were sentenced today by U.S. District Judge Marianne O. Battani in federal court in Detroit for their roles in a wide-ranging international stock fraud scheme involving the illegal use of bulk commercial e-mails, or “spamming,” announced Assistant Attorney General of the Criminal Division Lanny A. Breuer and U.S. Attorney for the Eastern District of Michigan Terrence Berg.

Alan M. Ralsky, 64, of West Bloomfield, Mich., and Scott Bradley, 48, also of West Bloomfield, were sentenced to 51 months and 40 months in prison, respectively, for conspiring to commit wire fraud, mail fraud, and to violate the CAN-SPAM Act, and also for committing wire fraud, engaging in money laundering and violating the CAN-SPAM Act. Ralsky and Bradley were also each sentenced to five years of supervised release following their respective prison terms, and were each ordered to forfeit \$250,000 that the United States seized in December 2007.

How Wai John Hui, 51, a resident of Hong Kong and Canada, was sentenced to 51 months in prison for conspiring to commit wire fraud, mail fraud and to violate the CAN-SPAM Act, and also for committing wire fraud and engaging in money laundering. Hui was sentenced to three years of supervised release following his prison term, and agreed to forfeit \$500,000 to the United States.

# Spammers Aren't Repacking Pillz in the Garage

- Sometimes people have a mental image of spammers taking orders in their home office and then repacking bulk pillz into retail quantities in their garage or something of the sort. This is not a correct mental model (or at least it isn't most of the time)
- A more realistic model would be a specialized ecosystem, with various interlocking specialized parts:
  - affiliate programs generate visits to pharma web sites, typically via email spam or web spam
  - high risk payment processing firms specialize in handling credit card for those online drug orders
  - drop shippers handle actual backend order fulfillment
  - the bad guys make lots of \$\$\$, and that's without hustling sales leads themselves, or counting pills, or taking much risk.

- Pharmacy dropshipping Generic Viagra online, Generic Cialis and Generic medicines from Cipla, Ranbaxy, Ajant... .com/ Google

Home Products Price List Contact Us About Us

UK DE ES

-:: Medicine Price ::-

\$0.40 / Generic Levitra 20mg

Categories:

Home  
Price List  
Products  
Manufacturers  
Dropshipping Information  
Frequently Asked Questions  
About Us  
Contact Us

1 Choose your Medicine

2 Open an Account

3 We Ship Orders

Check the prices of the medicines we have to offer.

Open an account. Send an initial deposit. Could be as low as \$500.00

We start sending medicines to your customer. They receive it within 5 days.

1. [Check the pricelist of medicines](#)

2. [Contact Us](#)

Methods of initial deposit.

1. Wire Transfer  
2. Western Union  
3. MoneyGram

1. Shipment sent through EMS  
2. Package is Trackable Online  
3. Delivery in 5 days.

**GUARANTEED DELIVERY**

Instant Contact

Skype: [REDACTED]  
Email: [REDACTED]  
Email-2: [REDACTED]

Generic Cialis - \$0.20

Generic Levitra - \$0.68

Generic Viagra - \$0.16

Generic Viagra SOFT - \$0.33

http://www.spamhaus.org/rokso/sbl\_listings.lasso?spa ▾ G Google

**Canadian Pharmacy** Canadian Pharmacy Records | Archived

**Current Spamhaus Block List (SBL) Listings**

email protected by  
SBL Advisory

IPs currently on the SBL	ISP	SBL Reference	Added ↑
74.208.59.0/32	1and1.com	<a href="#">SBL82324</a>	2009-11-30 14:45:45
200.26.189.141/32	viafacil.com	<a href="#">SBL82322</a>	2009-11-30 14:14:26
74.55.116.88/29	theplanet.com	<a href="#">SBL82307</a>	2009-11-30 09:53:36
61.91.112.92/32	asianet.co.th	<a href="#">SBL82131</a>	2009-11-27 13:52:36
12.150.225.112/32	ibbsonline.com	<a href="#">SBL82130</a>	2009-11-27 13:52:04
200.59.250.202/32	neunet.com.ar	<a href="#">SBL82129</a>	2009-11-27 13:51:26
79.149.128.75/32	telefonica.es	<a href="#">SBL82128</a>	2009-11-27 13:50:47
61.158.167.98/32	unicom-ha	<a href="#">SBL82114</a>	2009-11-27 10:13:46
190.190.232.4/32	fibertel.com.ar	<a href="#">SBL82099</a>	2009-11-27 01:51:07
200.157.252.20/32	intelignet.com.br	<a href="#">SBL82097</a>	2009-11-27 00:22:27
75.151.176.2/32	comcast.net	<a href="#">SBL82096</a>	Spamhaus – The TOP 10 Spammers
74.211.23.130/32	ibbsonline.com	<a href="#">SBL82095</a>	
59.165.23.186/32	tatacommunications.com	<a href="#">SBL82094</a>	
201.156.16.39/32	avantel.net.mx	<a href="#">SBL82093</a>	
216.180.178.140/32	atcnet.net	<a href="#">SBL82092</a>	
93.126.7.32/32	asmanfaraz.com	<a href="#">SBL82091</a>	
88.30.231.53/32	telefonica.es	<a href="#">SBL82090</a>	
76.11.235.205/32	newwavecomm.net	<a href="#">SBL82089</a>	
79.149.204.47/32	telefonica.es	<a href="#">SBL82088</a>	

**The 10 Worst ROKSO Spammers** As at 01 December 2009

Rank	Photo	Spammer or Spam Gang	Country
1		<b>Canadian Pharmacy</b> A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.	Ukraine

# The SBL Listings On the Preceding Page

- Spammers face some problems when it comes to spamvertising their products, including, most notably, having the systems they've used listed on block lists such as the Spamhaus Zen list ([www.spamhaus.org/zen](http://www.spamhaus.org/zen))
- Once listed on Spamhaus (or other block lists), systems sending spam have a much harder time doing so. Many sites will block connections from those systems outright, subject traffic from those systems to extra scrutiny, rate limit traffic from those systems, etc.
- Spammers thus are constantly on a quest for alternative channels which they can use to send spam.
- The original alternative channel used by spammers many years ago was the “open SMTP relay.”

# Open SMTP Relays

- Mail servers were originally designed to accept and attempt to deliver all email traffic. If mail was for a local user, the email would be delivered locally, otherwise the email would be forwarded, or “relayed,” on toward its ultimate destination. If the mail that a server was seeing was from a local user, or was for a local user, this was entirely normal and appropriate.
- If, however, the mail that a server saw was neither from a local user nor to a local user, there’s no reason why that email should be going via that mail server. Servers that failed to correctly reject misdirected relay email were and are known as “open SMTP relays” and were and are beloved by spammers as a way of doing an “end run” around direct blocks on the spammer’s own address space.

# Open Proxies

- Eventually, the community succeeded in eliminating most open SMTP relays, either through education or through direct blocklisting. Spammers moved on to open proxies.
- Proxies are much like SMTP relays in that a proxy is designed to accept a connection from a client, and then act on the client's behalf to get/process some content. For example, many international sites force customer web traffic through a caching web proxy so that popular (and invariant) content can be served from a local copy, rather than having to be pulled from an international site each time it's needed by a local user.
- Unfortunately, some proxies would proxy ANY type of connection, including SMTP sessions, for ANY user, ANY where, sometimes even concealing the requesting IP address.

# Closing Open Proxies; Bots

- Spammers quickly burned through all the organically occurring natural proxies (contrary to popular belief, there was not and is not an infinite supply of mis-configured systems connected to the Internet :-)).
- Q: What were the spammers to do then? A: custom create their own abusable systems using either exploitable vulnerabilities (“scan and exploit”) or malware
- These hijacked systems (created by scan and exploit or malware), are often called “spam zombies,” or “bots.” “Botmasters” run collections of “bots” as “botnets.”
- Historically, they were controlled by IRC, although modern bots use improved C&C’s.
- Bots can be used to send spam, but they’re like potatoes or tofu, very adaptable for a variety of needs

# The Many Faces of Bots

- Besides being used for spam, bots can also be used for:
  - hosting phishing sites, malware, pirated software, etc. (this is often done via a technique known as “fast flux hosting”)
  - conducting distributed denial of service (DDoS) attacks by flooding sites with traffic
  - pay-per-click click fraud meant to cheat advertisers
  - scanning hosts for vulnerabilities
  - sniffing network traffic for unencrypted login credentials or passwords
  - etc.
- There are currently over six million known bots listed on the Composite Blocking List, the CBL

# Where Do Bots Live? (countries with >1% of total as of Dec 1st)



The screenshot shows a web browser window with the title "CBL country". The address bar contains the URL "http://cbl.abuseat.org/country.html". The main content is a table with 22 rows, each representing a country. The columns include: country, Count, %total, %cumulative, Rank, PBLisp, %CBL, PBLdyn, %CBL, Traffic, %Traffic, and Spams/Bot. The data shows that Brazil (BR) has the highest number of bots (105,8096), followed by India (IN) and Vietnam (VN). The cumulative percentage of these top countries reaches nearly 100%.

country	Count	%total	%cumulative	Rank	PBLisp	%CBL	PBLdyn	%CBL	Traffic	%Traffic	Spams/Bot
Total	6170676	100			875914	14.19	4874999	79.00	292060320	100	47.33
BR	1058096	17.15	17.15	1	41928	3.96	987215	93.30	42130346	14.43	39
IN	679816	11.02	28.16	2	142566	20.97	525388	77.28	14520832	4.97	21
VN	424477	6.88	35.04	3	184700	43.51	237290	55.90	34203118	11.71	80
RU	377105	6.11	41.15	4	25064	6.65	329195	87.30	10267185	3.52	27
PL	259399	4.20	45.36	5	6613	2.55	235805	90.90	7384381	2.53	28
TH	240717	3.90	49.26	6	78656	32.68	159243	66.15	4339704	1.49	18
CN	228614	3.70	52.96	7	112	0.05	193868	84.80	16440084	5.63	71
CO	164379	2.66	55.63	8	36093	21.96	122793	74.70	8855434	3.03	53
UA	153063	2.48	58.11	9	10494	6.86	136563	89.22	4300093	1.47	28
AR	142610	2.31	60.42	10	244	0.17	132009	92.57	6750813	2.31	47
IT	132401	2.15	62.56	11	61782	46.66	61816	46.69	3444412	1.18	26
KR	131945	2.14	64.70	12	2683	2.03	82639	62.63	25099675	8.59	190
DE	119881	1.94	66.65	13	13315	11.11	103254	86.13	4967611	1.70	41
ID	112376	1.82	68.47	14	25	0.02	107946	96.06	4158448	1.42	37
MX	109481	1.77	70.24	15	17	0.02	103198	94.26	6067591	2.08	55
US	107704	1.75	71.99	16	54727	50.81	22577	20.96	14208588	4.86	131
SA	104708	1.70	73.68	17	0	0.00	103715	99.05	2697620	0.92	25
RO	103308	1.67	75.36	18	56153	54.35	30268	29.30	6722395	2.30	65
ES	102079	1.65	77.01	19	2453	2.40	84977	83.25	3821696	1.31	37
CL	89934	1.46	78.47	20	5187	5.77	82190	91.39	4236278	1.45	47
PK	76909	1.25	79.72	21	5371	6.98	70390	91.52	2491877	0.85	32
MA	69471	1.13	80.84	22	0	0.00	69294	99.75	1541355	0.53	22
...	...	...	...	...	...	...	...	...	...	...	...

Note: just 22 countries account for >80% of all bots 47

# How Do All Those Systems Get Own3d?

- Many different reasons, including:
  - failure to patch the operating system and applications: try running Secunia's PSI on your own Windows PC sometime, you'll be surprised at what you see: [secunia.com/vulnerability\\_scanning/personal/](http://secunia.com/vulnerability_scanning/personal/)
  - failure of signature-based antivirus: if the good guys release new antivirus signatures a couple of times a day, but the bad guys release new variants of their malware every hour, guess what? At least some folks will ALWAYS be vulnerable even if the good guys had signatures for everything they've seen
  - operator error: weak password, no password, sent password to bad guy in response to phishing attack, shared entire hard drive read/write with the world, etc., etc., etc.

# “And I Bet They Didn’t Use a Firewall!”

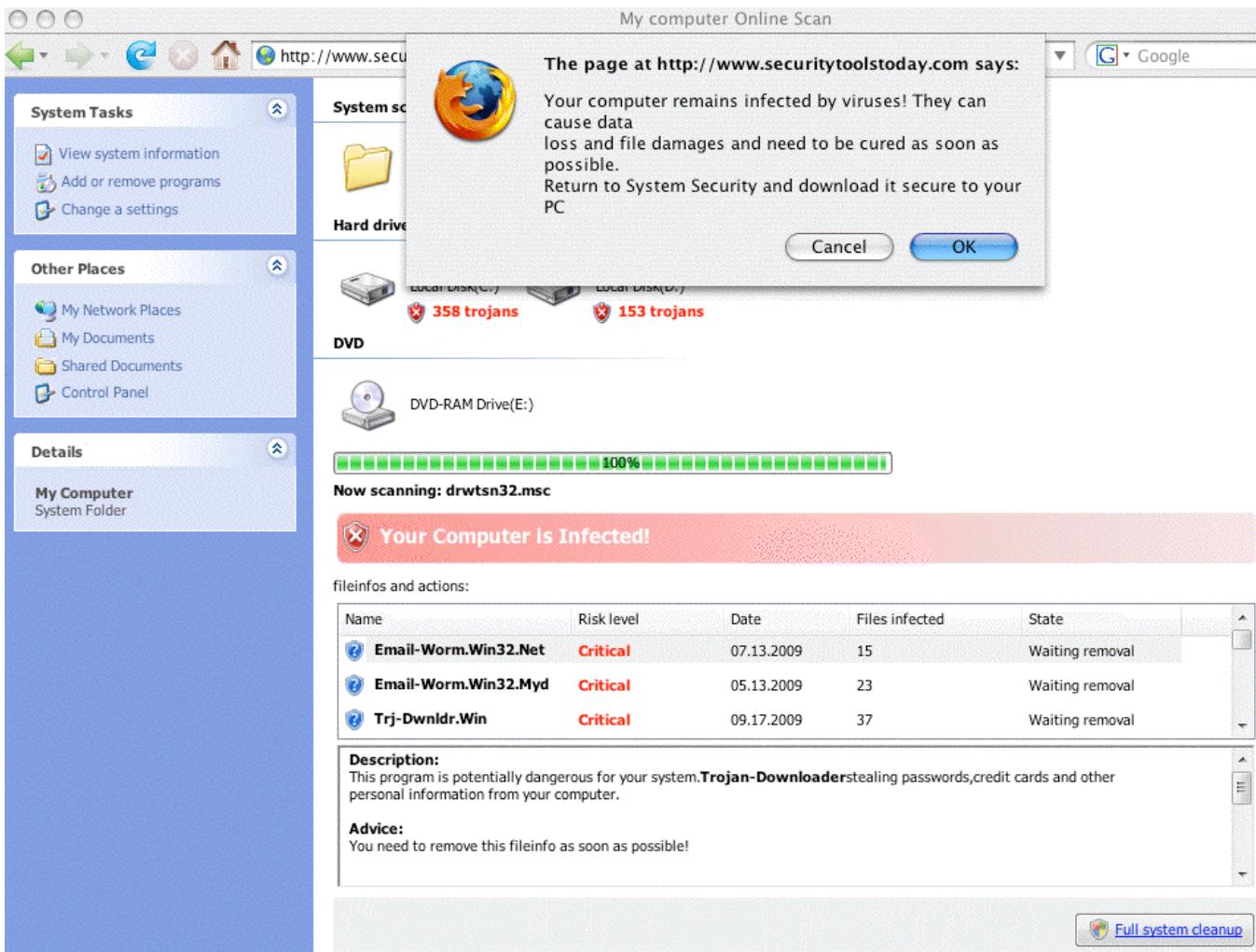
- Unlike most guys, I’m not here to preach the firewall “gospel.” If a firewall works well for you, that’s great, keep using it, more power to you.
- However, recognize that firewalls, particularly if they’re deployed at a campus border in front of 20,000 of your closest friends, really don’t provide all that much protection. Firewalls can interfere with advanced applications and hinder the detection and remediation of incidents (particularly if deployed as NAT/PAT).
- There’s a lot more to the Internet than just the web and email, so don’t settle for crippled Internet access where that’s all that’s allowed through a firewall. Strive to preserve Internet transparency and the end-to-end model that’s enabled so much innovation!

# Patching In the Developing World

- Network security is particularly tough in the developing world where bandwidth is scarce and expensive. If you're only getting 20 or 30 Kbps throughput, are you really going to take \*hours\* to download a 70 MB service pack? (do the math:  $70,000 \text{ KByte} * 8 \text{ bits/byte} / 30 \text{ K bits/second} / 3600 \text{ seconds/hour} ==> 5.18 \text{ hours}$ )
- Besides, if you're running a pirated copy of your operating system or major applications, you may be reluctant to try patching it anyhow!
- A little additional problem: for many in the developing world, virtually all the information about securing your system is written in a language you don't understand, English, rather than your native language.
- But what about antivirus software? Won't it help?

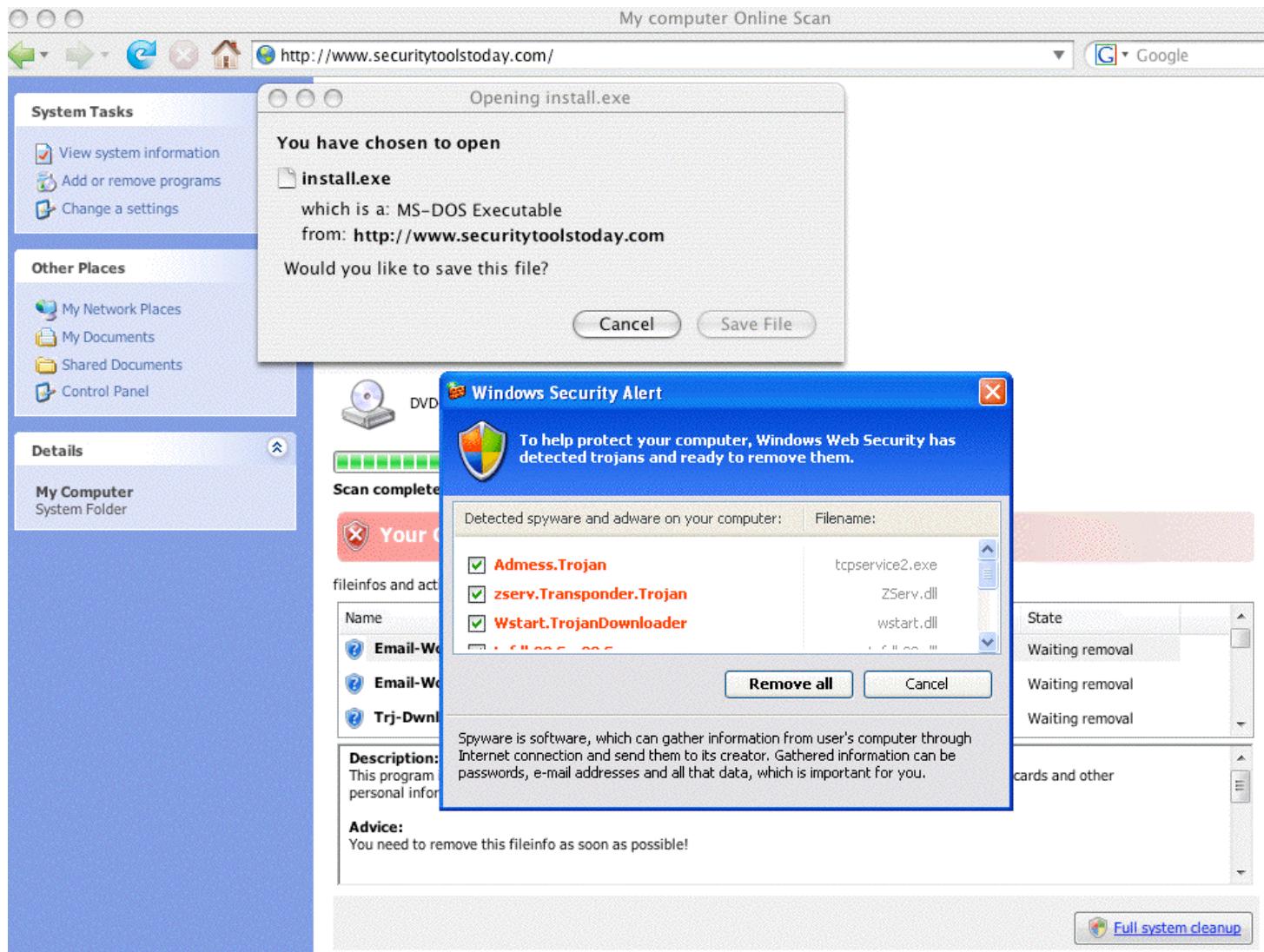
# Why The World Gets Confused

## [CAUTION: SITE CONTAINS MALWARE]



# Why The World Gets Confused (2)

## [CAUTION: SITE CONTAINS MALWARE]



# Why The World Gets Confused (3)

- Note that that report came from my Mac, which doesn't run Windows nor does it have a C:\ drive nor is it infected  
:-)
- If you were to download the recommended installer, it contains malware, although only one antivirus product in five currently detects it. See the Virustotal report on the next slide...

# The Widespread Failure of Antivirus

VirusTotal – Free Online Virus and Malware Scan – Result

http://www.virustotal.com/analisis/7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0e

File **install\_5\_.exe** received on 2009.12.01 22:53:59 (UTC)  
Current status: **finished**  
Result: **8/40 (20%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.43	2009.12.01	-
AhnLab-V3	5.0.0.2	2009.12.01	-
AntiVir	7.9.1.88	2009.12.01	-
Antiy-AVL	2.0.3.7	2009.12.01	-
Authentium	5.2.0.5	2009.12.01	W32/FakeAlert.DX3.gen!Eldorado
Avast	4.8.1351.0	2009.12.01	-
AVG	8.5.0.426	2009.12.01	FakeAlert.NV
BitDefender	7.2	2009.12.01	-
CAT-QuickHeal	10.00	2009.12.01	-
ClamAV	0.94.1	2009.12.01	-
Comodo	3103	2009.12.01	-
DrWeb	5.0.0.12182	2009.12.01	-
eSafe	7.0.17.0	2009.12.01	-
eTrust-Vet	35.1.7151	2009.12.01	-
F-Prot	4.5.1.85	2009.12.01	W32/FakeAlert.DX3.gen!Eldorado
F-Secure	9.0.15370.0	2009.11.29	-
Fortinet	4.0.14.0	2009.12.01	-
GData	19	2009.12.01	-
Ikarus	T3.1.1.74.0	2009.12.01	-
Jiangmin	11.0.800	2009.12.01	-
K7AntiVirus	7.10.906	2009.11.27	-
Kaspersky	7.0.0.125	2009.12.01	-

# The Widespread Failure of Antivirus (2)

VirusTotal – Free Online Virus and Malware Scan – Result

http://www.virustotal.com/analisis/7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0a

Antivirus	Version	Date	Result
K7AntiVirus	7.10.906	2009.11.27	-
Kaspersky	7.0.0.125	2009.12.01	-
McAfee	5819	2009.12.01	-
McAfee+Artemis	5819	2009.12.01	-
McAfee-GW-Edition	6.8.5	2009.12.01	Heuristic. LooksLike.Trojan.PCK.Krap.H
Microsoft	1.5302	2009.12.01	-
NOD32	4652	2009.12.01	-
Norman	6.03.02	2009.12.01	-
nProtect	2009.1.8.0	2009.11.28	-
Panda	10.0.2.2	2009.12.01	Suspicious file
PCTools	7.0.3.5	2009.12.01	RogueAntiSpyware.SecurityToolFraud
Rising	22.24.01.09	2009.12.01	-
Sophos	4.48.0	2009.12.01	Mal/FakeAV-AD
Sunbelt	3.2.1858.2	2009.12.01	FraudTool.Win32.RogueSecurity (v)
Symantec	1.4.4.12	2009.12.01	-
TheHacker	6.5.0.2.083	2009.12.01	-
TrendMicro	9.100.0.1001	2009.12.01	-
VBA32	3.12.12.0	2009.11.30	-
ViRobot	2009.12.1.2065	2009.12.01	-
VirusBuster	5.0.21.0	2009.12.01	-

**Additional information**

File size: 1256004 bytes

MD5...: 544059650c3a2be8061bcc65eabc98a6

SHA1...: 1120ad8355211cdf2d33a6bc4c4b3eb44e6f2c1a

SHA256: 7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0a2d4d1afc4895e708

# Looking At That Infested Site Just A Little

- % dig www.securitytoolstoday.com +short  
94.102.63.245
- % whois -h whois.ripe.net 94.102.63.245  
inetnum: 94.102.63.128 - 94.102.63.255  
netname: KINGH-NET  
descr: The King Host  
country: NL  
admin-c: AW137-RIPE  
tech-c: AW137-RIPE  
status: ASSIGNED PA  
mnt-by: ECATEL-MNT  
mnt-lower: ECATEL-MNT  
mnt-routes: ECATEL-MNT  
source: RIPE # Filtered  
  
person: Andrew Willson  
address: Honderdland 112F, 2677LT Maasdijk  
phone: +31174712185  
abuse-mailbox: ipadmin@thekinghost.biz  
nic-hdl: AW137-RIPE [...]

# Looking At That Infested Site A Little (2)

- % whois securitytoolstoday.com  
Domain name: securitytoolstoday.com

Name servers:

ns1.securitytoolstoday.com  
ns2.securitytoolstoday.com

Registrar: Regtime Ltd.

Creation date: 2009-11-25

Expiration date: 2010-11-25

Status: active

Registrant:

Kevin Neely

Email: kevinrneely@trashymail.com

Organization: Private person

Address: 3809 Hillview Drive

City: Oakland

State: CA

ZIP: 94612

Country: US

Phone: +1.7072310192

[etc]

# Looking At That Infested Site A Little (3)

Anonymous Email and Free Spam Blocker

[X](#) [Home](#) [http://www.mytrashmail.com/myTrashMail\\_inbox.aspx?email=kevinrneely](http://www.mytrashmail.com/myTrashMail_inbox.aspx?email=kevinrneely) [▼](#) Google

**myTrashMail.com**  
smart email services

[Login](#)  
[Register](#)  
[About](#)  
[FAQ](#)

**News!!!**

@trashymail.com domain is not active anymore.  
Use our new anonymous email domain **@trash2009.com**

Email Account  
  
 Remember Me

<input type="checkbox"/>	Sender	Subject	Date	Size	Delete
No messages found!					

[Delete Selected](#)

# Looking At That Infested Site A Little (4)

USPS – ZIP Code Lookup – Search By Address

http://zip4.usps.com/zip4/zcl\_0\_results.jsp

UNITED STATES POSTAL SERVICE

USPS Home | FAQs

ZIP Code Lookup

**ZIP Code Lookup**



Search By Address » Search By City » Search By Company » Find All Cities in a ZIP Code™ »

Find a ZIP Code by entering an address.  
(You can also search for a partial address, such as "Main Street, Fairfax, VA.")

We're sorry! We were unable to process your request.

The address was not found. Please check the address below.  
You may want to utilize the Yellow Pages and/or White Pages below.

\* Required Fields

\* Address 1

Address 2  Apt, floor, suite, etc.

\* City

\* State  [Find state abbreviation](#)

ZIP Code

**Submit >**

## If You're So Inspired...

- You can report the bogus whois data in this (or other) domain whois records to Internic using the form at:

<http://wdprs.internic.net>

- Note that the WDPRS process isn't particularly rapid, and by the time you make progress on this one, the bad guys will usually have moved on and will be using another domain.
- Dot cn domains have been particularly popular because there is no WDPRS system for them, and they can cost as little as one yuan (USD ~\$0.15) to buy.

# Are There Potentially-Related Sites?

BFK edv-consulting GmbH – Sicherheit

[http://www.bfk.de/bfk\\_dnslogger.html?query=94.102.63.245#result](http://www.bfk.de/bfk_dnslogger.html?query=94.102.63.245#result) ▾

The server returned the following data:

onlineworldclub.com	A	94.102.63.245
ns1.onlineworldclub.com	A	94.102.63.245
antispywaresoftworld.com	A	94.102.63.245
ns1.antispywaresoftworld.com	A	94.102.63.245
securitytoolcode.com	A	94.102.63.245
ns1.securitytoolcode.com	A	94.102.63.245
scanonlinesite.com	A	94.102.63.245
ns1.scanonlinesite.com	A	94.102.63.245
antyspywaressite.com	A	94.102.63.245
ns1.antyspywaressite.com	A	94.102.63.245
securitytoolblog.com	A	94.102.63.245
ns1.securitytoolblog.com	A	94.102.63.245
bestfreecheck.com	A	94.102.63.245
ns1.bestfreecheck.com	A	94.102.63.245
webbillcheck.com	A	94.102.63.245
ns1.webbillcheck.com	A	94.102.63.245
thetoolsdiscount.com	A	94.102.63.245
ns1.thetoolsdiscount.com	A	94.102.63.245
securitytooltoday.com	A	94.102.63.245
ns1.securitytooltoday.com	A	94.102.63.245
securitytoolsimage.net	A	94.102.63.245
ns1.securitytoolsimage.net	A	94.102.63.245
securityutilitystore.net	A	94.102.63.245
ns1.securityutilitystore.net	A	94.102.63.245

# “What About Phishing?”

- What about it?
- You know what it is: phishing is when bad guys con you or me into providing login credentials, credit card information, or other sensitive information, typically in response to an “urgent” message insisting that we do so AT ONCE!
- If users wouldn’t “play along” and provide that information, phishing would largely cease to be an issue except for information stealing malware.
- Resist urgent commands! Be cynical! Refuse to do as you’re told! Never disclose passwords or private info!

# What About 4-1-9 (and Other) Scams?

- 4-1-9 scams, also known as advance fee fraud scams, rely on people's gullibility and greed.
- Miriam Abacha does not now, nor will she ever, have millions of dollars to share with you if you will only temporarily cover some "short term processing fees."
- Similarly, no legitimate company needs you to cash checks for them, nor do they need you to reship merchandise, nor will they pay you a percent a day to temporarily use your money.
- Don't be a sucker.

**“I Want To Harden My Email”**

# A Simple Recommendation: Use Plain Text Email ONLY

- Only read your email with a text-only email reader (such as Pine running in a Mac terminal window); do not use a graphical (point and click) email client
- Do not accept ANY HTML formated email
- Do not accept attachments (even from someone you know)
- Do not accept base64-encoded or even QP (quoted-printable) format messages
- If you run a mailing list, consider protecting your list participants by enforcing these same policies for all postings to your mailing list

# Use GPG To Sign and Encrypt Your Email

- Email usually travels the Internet unencrypted, and gets stored on disk unencrypted. Consider protecting your privacy by encrypting and signing your email with PGP or GPG.
- If you use do use a point-and-click mail reader such as Mozilla Thunderbird (email companion application to the Firefox Mozilla web browser), you can install GPG and Enigmail for a comparatively easy-to-use interface.
- See:
  - <http://www.mozilla.org/messaging/>
  - <http://www.gnupg.org/>
  - <http://enigmail.mozdev.org/>

# Use A Multi-Stage Process To Filter Spam

- The process that seems to work well for many sites is described at

[http://www.spamhaus.org/effective\\_filtering.html](http://www.spamhaus.org/effective_filtering.html)

and relies on a combination of block lists, URI-based blocklists (such as the SURBL), and final filtering with SpamAssassin.

- Be sure to whitelist known-good correspondents.
- If you don't run your own mail server, shop around for a mail server that's run the way you'd like it to be run.

# Even If A/V Isn't Perfect, Still Use It

- Flawed as signature-based antivirus software may be, you should still use it.
- Run one product on your mail server, and a different product on your desktop to get the benefit of overlapping coverage.
- You may also want to consider Procmail Email Sanitizer, [www.impsec.org/email-tools/procmail-security.html](http://www.impsec.org/email-tools/procmail-security.html) , which defangs structurally dangerous message constructs which might otherwise slip by
- I'm sure you also know and understand that some operating systems are more plagued with malware than others, for whatever reason. If malware is a concern for you, remember, you do have options.

# Thanks for The Chance to Talk Today!

- Are there any questions?

# If You're Still Not Tired/Bored to Tears...

- Some other areas we can explore if folks still have time and energy tonight (in alphabetical order):
  - 2009 Tour of Cybercrimes  
<http://www.uoregon.edu/~joe/cybercrime2009/>
  - Cyber War, Cyber Terrorism and Cyber Espionage  
<http://www.uoregon.edu/~joe/cyberwar/>
  - Doing DNS As If DNS Actually Mattered  
<http://www.uoregon.edu/~joe/dnssec-nd/>
  - Electromagnetic Pulse  
<http://www.uoregon.edu/~joe/infragard-2009/>
  - IPv6 and the Security of Your Network and Systems  
<http://www.uoregon.edu/~joe/i2mm-spring2009/>
  - SCADA Security and Critical Infrastructure  
<http://www.uoregon.edu/~joe/scadaig/>