Just How Bad Is It?

Oregon Safe Cyberspace Initiative
February 22nd, 2008

Joe St Sauver, Ph.D. (joe@uoregon.edu)
http://www.uoregon.edu/~joe/howbad/

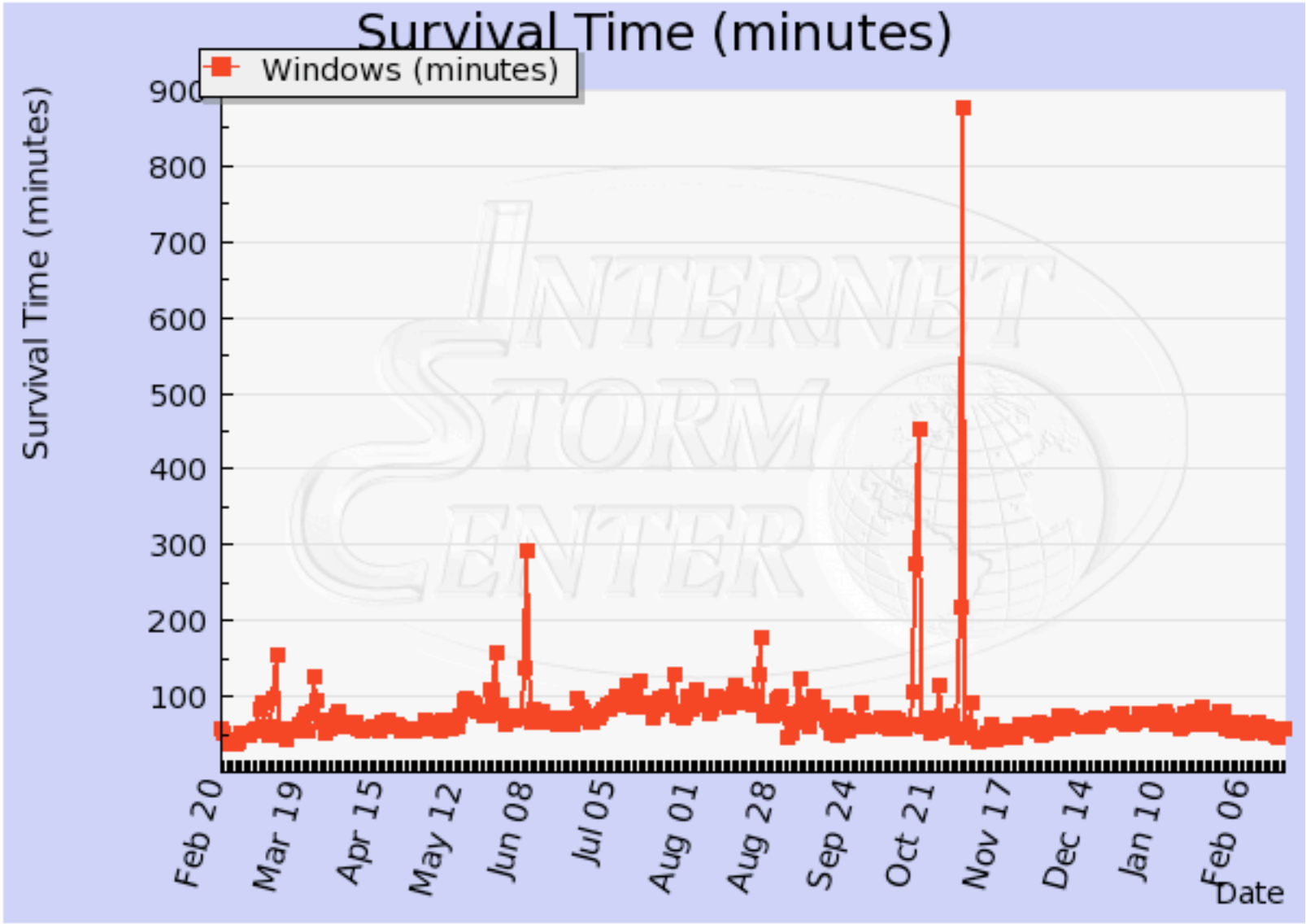
Disclaimer: all opinions are strictly my own, and do not necessarily represent the opinion of any other party

1. Introduction

Sean Asked Me
"*So Just How Bad Is It Online?*"

- My answer is, "It really depends."
- For example, things can really be pretty bad if you have an unpatched older Windows system with no firewall, no antivirus, and no antispyware software installed. Life gets even worse if you're using an Internet Service Provider which doesn't filter email spam, or you use an out-of-date web browser to surf in seedy neighborhoods on the web, or you pick a weak password for your account.
- In fact, if pretty much **any** of those things are true, I can virtually **guarantee** that your computer will quickly become infected with a virus or other malware, and probably begin spewing spam. If/when that happens, your ISP will usually cut you off, and you may have a very hard time getting your system secured.

Survival Time Graph



Source: http://isc.sans.org/survivaltime.html

On The Other Hand, If…

- You use an operating system that's less commonly targeted by cyber attackers (for example, I run and like Mac OS X)
- And you keep your operating system (and apps!) up-to-date
- And you run antivirus and antispyware software
- And use a software (and/or hardware) firewall
- And your ISP helps you out by doing a good job filtering spam, phishing and malware that may be sent to you via email
- And you use a secure web browser, and do your best to avoid bad neighborhoods online
- And you avoid P2P file sharing and instant messaging apps
- And you pick a long, tough-to-crack password
- And you stay alert and skeptical about what you see…
- WELL, THEN there's an excellent chance that you'll do just fine and have no problems online (although there are no guarantees)

Let's Just Briefly Consider A Few Other Areas of Concern

- Spam
- Malware
- Unauthorized Access to Information
- DDoS
- Fraud
- Control Systems
- Non-Technical Vulnerabilities (Insiders and Acts of God)

2. Spam

Spam Has Reached Absurd Levels

http://www.senderbase.org/home/detail_spam_volume?displayed=lastmonth&

Date	Spam Volume (Billions)	% of Global Email Volume
02/22/08	49.7	90.6%
02/21/08	57.2	90.7%
02/20/08	69.1	90.4%
02/19/08	70.8	90.8%
02/18/08	46.1	92.5%
02/17/08	58.9	93.2%
02/16/08	62.1	91.2%
02/15/08	44.8	90.2%
02/14/08	150.2	90.9%
02/13/08	66.6	90.6%
02/12/08	44.4	90.7%
02/11/08	42.8	92.6%
02/10/08	40.2	92.8%
02/09/08	49.6	91.0%
02/08/08	44.7	90.5%
02/07/08	41.7	90.6%

Millions of Compromised PCs Are Used To Send Spam

- For example, there are roughly 5.5 million systems listed on the CBL DNS (http://cbl.abuseat.org/) blocklist, all systems which were added to that block list for having sent **spam**
- While spam is unquestionably annoying (and an insidious drain on business productivity and email usability), those same compromised systems could just as easily be used for a host of other far more nefarious purposes including:
  -- hosting phishing sites, malware, pirated software or child porn
  -- scanning the network to find other vulnerable hosts
  -- sniffing traffic on the wire to compromise passwords
  -- DDoS'ing online businesses or even
  -- attacking US government sites or critical online infrastructure.
- Most of those compromised hosts, however, will be used to send spam. How much spam can a single host send?

Billion Spam/Day Botnets…

- "[…] SpamThru acts as massive distributed engine for sending spam, but without the cost of maintaining static servers. Total spam capacity is fairly high - with 73,000 bots, given an average SMTP transaction time of 5 seconds, **the botnet is theoretically capable of sending a billion spams in a single day**. This number assumes one recipient per message, however in reality, most spams are delivered in a single message with multiple recipients at the same domain, so **the actual number of separate spams landing in different inboxes could be even higher**, assuming the spammer possesses that many email addresses."

  Joe Stewart, http://www.secureworks.com/research/threats/view.html?threat=spamthru-stats

https://nssg.trendmicro.com/nrs/reports/rank.php?page=1

Network Reputation - Estimated Spam Volume by ISP

Jump to: [Page 1][Page 2][Page 3][Page 4]

Rank data last updated: February 22 2008, 08:21 PST

Rank This Week	Rank Last Week		ASN	ISP Name	Est. Spam Volume(24hrs)	Botnet Activity
001	001	→	9121	TTNET TTnet Autonomous System	3.98B	-5.9
002	002	→	3269	ASN-IBSNAZ TELECOM ITALIA	2.80B	-5.5
003	003	→	19262	VZGNI-TRANSIT - Verizon Internet Services Inc.	2.09B	-5.9
004	004	→	5617	TPNET Polish Telecom's commercial IP network	1.68B	-11.3
005	006	↑	6147	Telefonica del Peru S.A.A.	1.46B	-18.6
006	007	↑	4134	CHINANET-BACKBONE No.31,Jin-rong Street	1.29B	17.1
007	005	↓	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	1.17B	26.1
008	010	↑	4766	KIXS-AS-KR Korea Telecom	1.14B	14.4
009	008	↓	7738	Telecomunicacoes da Bahia S.A.	1.29B	-6.7
010	009	↓	15557	LDCOMNET NEUF CEGETEL (formerly LDCOM NETWORKS)	1.07B	-8.2
011	011	→	22927	Telefonica de Argentina	992.6M	-5.3
012	012	→	1267	ASN-INFOSTRADA Infostrada S.p.A.	836.2M	-7.5

Where Do Spamming Botted Hosts Live?

country	Count	%total	%cumulative	Rank	P
Total	5498263	100			9
CN	563904	10.26	10.26	1	
BR	486472	8.85	19.10	2	
TR	467693	8.51	27.61	3	4
RU	352256	6.41	34.02	4	
IN	303124	5.51	39.53	5	
US	291426	5.30	44.83	6	1
DE	197652	3.59	48.42	7	
CO	183797	3.34	51.77	8	
IT	182976	3.33	55.10	9	1
AR	172637	3.14	58.24	10	
PL	166995	3.04	61.27	11	
ES	143866	2.62	63.89	12	
CL	129459	2.35	66.24	13	
VN	124727	2.27	68.51	14	
UK	121852	2.22	70.73	15	
PE	117198	2.13	72.86	16	
KR	97012	1.76	74.62	17	
TH	89142	1.62	76.25	18	
UA	78163	1.42	77.67	19	
FR	73408	1.34	79.00	20	
MX	59884	1.09	80.09	21	

3. Malware

What Compromises All Those Systems?

- While some of those systems may have had weak passwords or other vulnerabilities, most of those systems were compromised by malware: viruses, trojan horses, worms and other things that go bump in the night…

- Q. But how is this possible? Isn't everyone running antivirus software?
  A. Most people do run an antivirus program, but even when do you run antivirus software, you can still end up infected.

The Problem With AV Products

- Most AV products are "signature based," and identify viruses based on peculiarities ("signatures") unique to each virus.
- New virus signatures only get released by the vendor and downloaded by the end user perhaps once a day, while miscreants can release new not-yet-detectable versions of their malware as often as they want (e.g., multiple times a day). The virus writer can thus guarantee that they will have a period of time during which user systems will be vulnerable.
- Virus writers also enjoy another key advantage: they can empirically test and repeatedly tweak their code and its packaging until their exploit doesn't get detected by current popular antivirus products. Thus, it is a virtual certainty that at least some malware will get past your current AV solution… But most users don't understand that... AV software is way too nice of a convenient security blanket

The Pace of Malware Release Is Accelerating

- "At the start of 2007, computer security firm F-Secure had about 250,000 malware signatures in its database, the result of almost 20 years of antivirus research. Now, near the end of 2007, the company has about 500,000 malware signatures.

  "'We added as many detections this year as for the previous 20 years combined,' said Patrik Runald, security response manager at F-Secure.

  http://news.yahoo.com/s/cmp/20071206/tc_cmp/204701370
  December 5th, 2007

Example: "Video Codec" malware

- If you Google for a sex-related term and limit the returned results to the cn (China) domain, one or more of the top returned pages will likely be a web page which will attempt to trick you into downloading a "new codec" that's "required" for you to view free sex-related videos.
- If you do intentionally or accidentally download and run that "new codec" you will actually be infecting your system with poorly detected malware (checking an example of this malware at Virustotal, only 5 of 32 antivirus products detected this malware, and the two antivirus products with the largest market share, Symantec and McAfee, don't catch it at all).
- See the report on the next page…

File **setup.exe** received on **01.01.2008 03:01:21 (CET)**

Current status: **finished**

Result: **5/32 (15.63%)**

Compact Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.1.1.10	2007.12.31	-
AntiVir	7.6.0.46	2007.12.31	-
Authentium	4.93.8	2007.12.31	-
Avast	4.7.1098.0	2007.12.31	Win32:Zlob-AHS
AVG	7.5.0.516	2007.12.31	-
BitDefender	7.2	2008.01.01	-
CAT-QuickHeal	9.00	2007.12.31	-
ClamAV	0.91.2	2008.01.01	Trojan.Dropper-2529
DrWeb	4.44.0.09170	2007.12.31	Trojan.Popuper.origin
eSafe	7.0.15.0	2007.12.31	-
eTrust-Vet	31.3.5421	2008.01.01	-
Ewido	4.0	2007.12.31	-
FileAdvisor	1	2008.01.01	-
Fortinet	3.14.0.0	2007.12.31	-
F-Prot	4.4.2.54	2007.12.31	-
F-Secure	6.70.13030.0	2007.12.31	-

Ikarus	T3.1.1.15	2008.01.01	-
Kaspersky	7.0.0.125	2008.01.01	Trojan-Downloader.Win32.Zlob.fpi
McAfee	5196	2007.12.31	-
Microsoft	1.3109	2008.01.01	TrojanDownloader:Win32/Zlob.gen!AL
NOD32v2	2758	2007.12.31	-
Norman	5.80.02	2007.12.31	-
Panda	9.0.0.4	2007.12.31	-
Prevx1	V2	2008.01.01	-
Rising	20.24.52.00	2007.12.29	-
Sophos	4.24.0	2008.01.01	-
Sunbelt	2.2.907.0	2007.12.30	-
Symantec	10	2008.01.01	-
TheHacker	6.2.9.176	2008.01.01	-
VBA32	3.12.2.5	2007.12.31	-
VirusBuster	4.3.26:9	2008.01.01	-
Webwasher-Gateway	6.6.2	2007.12.31	-

Additional information

File size: 80139 bytes

MD5: cf46a1a8b4e94711ed779eba26d17eae

SHA1: e76b73e902184cdfd900bc3b355efc877bc66464

PEiD: -

"A Worst Case Worm"

- Weaver and Paxson, "A Worst Case Worm," June 8, 2004, http://www.icir.org/vern/papers/worst-case-worm.WEIS04.pdf

  "Abstract

  "Worms represent a substantial economic threat to the U.S. computing infrastructure. An important question is how much damage might be caused, as this figure can serve as a guide to evaluating how much to spend on defenses. We construct a parameterized worst-case analysis based on a simple damage model, combined with our understanding of what an attack could accomplish. **Although our estimates are at best approximations, we speculate that a plausible worst-case worm could cause $50 billion or more in direct economic damage** by attacking widely used services in Microsoft Windows and carrying a highly destructive payload."

4. Unauthorized Access to Information

Unauthorized Access to Information: The 2nd Most Expensive Type of Information Security Incident

- According to the 11th Annual CSI/FBI Computer Crime and Security Survey (see page 16 of http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf):

  -- viruses were the single most expensive type of information security incident (costing 313 respondents a total loss of $15,691,460, an average of $50,132 each)

  -- **unauthorized access to information was the second most expensive type of information security incident**, costing those same respondents a total loss of $10,617,000 (an average of $33,920 each).

Feb. 13, 2008	Lifeblood (Memphis TN)	Laptop computers with birth dates and other personal information of roughly 321,000 blood donors are missing and presumed stolen. Stored inside both computers were names, birth dates and addresses at the time of the individual's last donation or attempted donation. In most cases, the donors' Social Security numbers were also stored, along with driver's licenses, telephone numbers, e-mail addresses, ethnicity, marital status, blood type and cholesterol levels. Social Security numbers had been used to track blood from the donor to the recipients.	321,000
Feb. 13, 2008	Middle Tennessee State University (Murfreesboro, TN)	A professor left the university computer unattended in the mass communication department about two weeks ago and an unidentified person is believed to have used the machine to send spam e-mails. The computer contained the names and Social Security numbers of past and current students.	1,500
Feb. 14, 2008	Tenet Healthcare Corporation (Dallas, TX)	A ex-employee worked at a Frisco, Texas, billing center for less than two years, and is confirmed to have stolen the names, Social Security numbers and other personal information of about 90	37,000

5. Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service Attacks

"More than five years after the initial flurry of network attacks, and the news articles and research papers that followed, DDoS remains the number one concern for large IP network operators. Sixty-four percent of the survey participants said, '**DDoS is the most significant operational security issue we face today.**'"

Worldwide ISP Security Report, September 2005
http://www.arbornetworks.com/downloads/Arbor_Worldwide_ISP_Security_Report.pdf

"What *Is* A Distributed Denial of Service Attack?"

- In a distributed denial of service attack, network traffic from thousands of hacked computer systems -- often systems located all over the Internet -- gets used in a coordinated way to overwhelm a targeted network or computer, thereby preventing it from doing its normal work. For example:

  -- a company's connection or connections to the Internet may be made to overflow with unsolicited traffic (a so-called "packet flood")
  -- web servers may be inundated with malicious repeated requests for web pages
  -- an ISPs name servers may become swamped so that customers have problems visiting either local web sites or web sites on the Internet

http://www.heise-security.co.uk/news/90461

Report of 31.05.2007 17:36 [<< previous] [next >>]

Estonian DDoS - a final analysis

In the aftermath of the recent distributed denial of service (DDoS) targeting Estonia, information has emerged that suggests this was not a concerted attack orchestrated by some single agency, but rather the spontaneous product of a loose federation of separate attackers. It appears to have been a statement of disapproval at the relocation of the Bronze Soldier, a memorial to the WW2 Russian Unknown Soldier, from the centre of Tallinn to a suburban cemetery. The social significance of this should not be underestimated - to the indigenous Russians the statue represents the wartime sacrifice, whereas to the native Estonians it represents Russian occupation of their country.

Data gathered by Arbor Networks showed that sources of attack were worldwide rather than concentrated in a few locations. Attack bandwidths ranged from under 10 Mbps to 95Mbps, with the majority in the range 10-30 Mbps. 75 per cent of attacks lasted no longer than one hour and only 5.5 percent, over 10 hours. However the peak global effect was of a botnet with up to 100Mbps capacity. Bearing in mind the level of IT power available in Estonia, this had a crippling effect on those services that were targeted.

Gambling Site DDoS Extortion Threats

DK Matai of MI2G, which monitors unauthorised computer hacking says criminal syndicates operating from Russia have targeted large online payment systems belong to gambling sites.

A typical criminal syndicate extortion to online gambling and payment companies would range from 'You have to pay us $50,000 or we will start Dos attacks' to 'If you don't pay us what we want, then we'll make sure you don't have any customers'.

Several companies, with high stakes in terms of revnues or large customer base are giving in as they have revenues of over $50,000 per week, and the damage would be more, from the Dos attacks.

"What If We Treat A DDoS Like A Blizzard, And Just Try To 'Ride It Out?'"

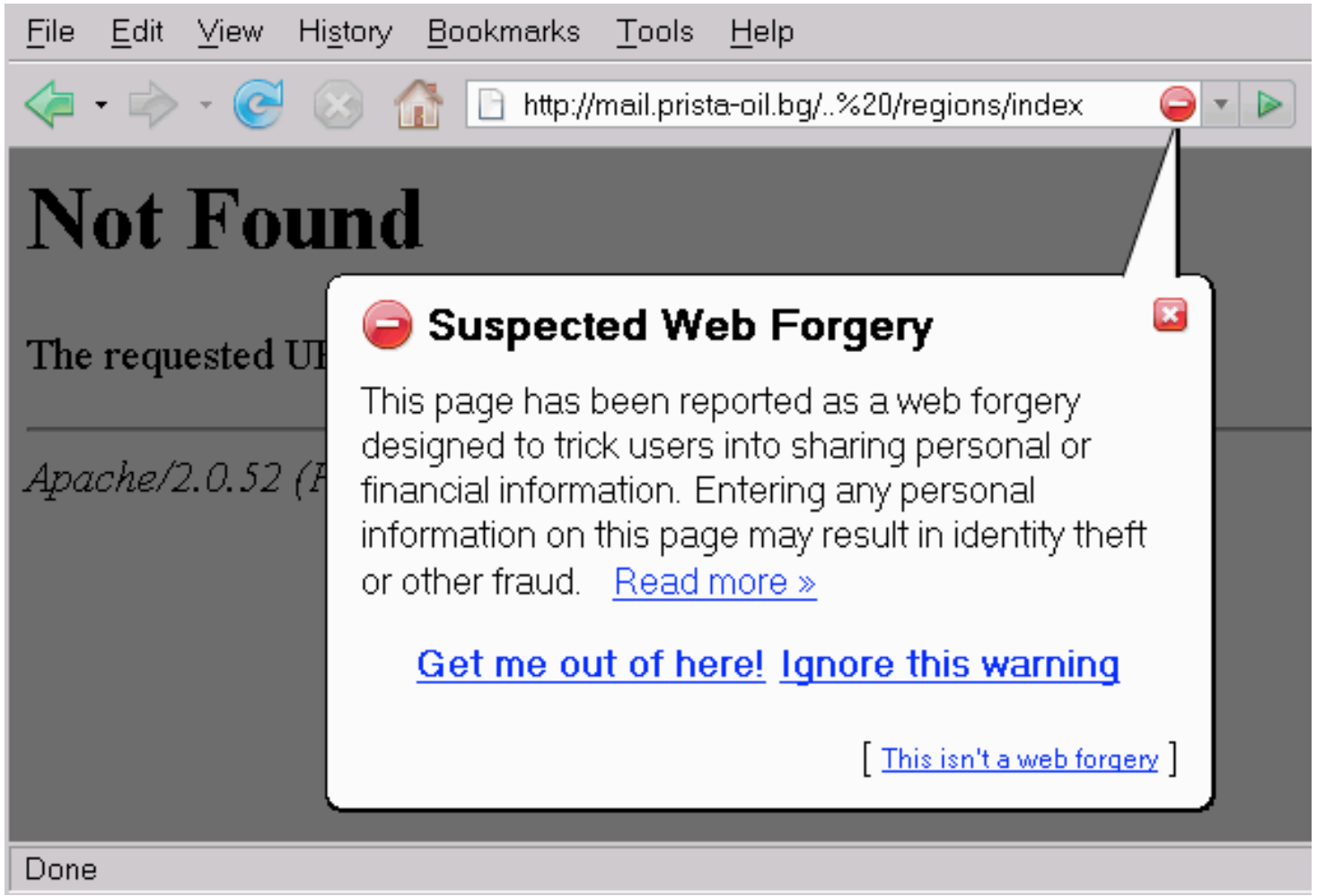
- While there is a certain insouciance to the idea of having "denial-of-service days" (sort of like more traditional "snow days"), you should understand that denial of service attacks can be sustained for days -- or even weeks or more -- at a time. For example, Spamhaus, a major anti-spam activist organization, was subject to an attempted denial of service attack that lasted for **three months**. (http://www.spamhaus.org/news.lasso?article=13)

  Taking an entire denial-of-service quarter off would have material impacts on pretty much any organization's ongoing operations, and probably would simply be unacceptable.

6. Fraud

[Total phishing reports made to APWG 10/06-9/07: **318,887**]

What A Firefox User Sees When Attempting to Visit Most Phishing Sites



Internet Auction Fraud

- "In 2006, IC3 processed more than 200,481 complaints that support Internet crime investigations by law enforcement and regulatory agencies nationwide. [* * *]

  Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints.

  2006 Internet Crime Report,
  [FBI] Internet Crime Complaint Center,
  http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf
  at pdf pages 3 and 7.

Pay-Per-Click Click Fraud

- Many leading Internet companies earn a majority of their revenue by selling pay-per-click advertisements. In pay-per-click (PPC) advertising models, true to the model's name, an advertiser agrees to pay whenever someone clicks on one of their ads.

- PPC ads are placed both on things like search engine results, and on relevant syndicated web pages authored by 3rd parties. To compensate 3rd parties for inserting ads on their web pages, the company shares part of what they've been paid with the 3rd parties.

- Priority for ad placement is determined by what advertisers are willing to pay -- the highest bids get the best placement on a given page which contains the term of interest

Google CFO: Fraud a big threat

Google exec calls click fraud the "biggest threat" to the Internet economy, urges quick action.

December 2, 2004: 6:30 PM EST

By Krysten Crawford, CNN/Money staff writer

NEW YORK (CNN/Money) - A top Google official said that growing abuse of the company's lucrative sponsored ad-search model jeopardizes the popular Internet search engine's business.

"I think something has to be done about this really, really quickly, because I think, potentially, it threatens our business model," Google Chief Financial Officer George Reyes said Wednesday.

Reyes, speaking at an investor conference sponsored by Credit Suisse First Boston, was referring to an illegal practice known as "click fraud" that occurs when individuals click on ad links that appear next to search results in order to force advertisers to pay for the clicks.

In cost-per-click advertising, marketers pay a search engine, like Google, Yahoo! or FindWhat.com, when users click on links to the advertisers' Web sites. Google and others also generate revenue by posting sponsored ad links on other Web sites and splitting the fees generated by user clicks.

The paid-search model is now the fastest-growing form of Internet advertising, according to the Interactive Advertising Bureau.

But analysts, fraud experts and now Google (down $0.56 to $179.40, Research) are openly fretting about the rise of click fraud.

The main perpetrators appear to be competitors of advertisers and also scam sites set up for the sole purpose of hosting ad links provided by Google, through its AdSense unit, or Yahoo!, through its Overture service. Humans or specially designed software then click on those ad links in order to "steal" revenue from advertisers.

Estimates of how prevalent click fraud has become since it appeared four years ago are all over the map. Jessie Stricchiola, the president of Alchemist Media, estimated that as much as 20 percent of all clicks on paid search ads are shams.

419: Truth Can Be Stranger Than Fiction

ABUJA, Nigeria (AP) --Nigerian prosecutors leveled 86 counts of fraud and conspiracy against five people Thursday for allegedly swindling a Brazilian bank of $242 million, in the biggest crackdown yet on the West African nation's advance-fee fraud or "419" scams.

The five are accused of luring an employee of Sao Paulo's Banco Noroeste into siphoning off the funds from his employer, persuading him he could land a share in a lucrative Nigerian construction contract if he just paid enough handling fees up front.

The five appeared in court in Nigeria's capital, Abuja, in handcuffs to hear the charges Thursday. All the suspects, including housewife Amaka Anajemba, lawyer Obum Osakwe, and businessman Emmanuel Nwude -- described by prosecutors as "a major shareholder" in a leading Nigerian bank -- pleaded innocent.

Penalties for each of the counts range between seven and 10 years.

Four Nigerian companies -- Ocean Marketing, Fynbaz, Emrus, and the African Shelter Bureau -- also accused of involvement in the alleged crime were not represented in court.

Presiding Judge Lawal Gumi entered innocent pleas on behalf of the companies and postponed proceedings until Wednesday, when he will consider requests for bond.

There was mild drama in court when suspect Nzeribe Okoli, while making his plea, declared he would make "shocking revelations" during the trial.

"There are so many hidden things which Nigerians should know," Okoli said before he was interrupted by the judge, who told him to restrict his answers to the questions he was asked.

Nigeria's anti-fraud body, the Economic and Financial Crimes Commission, alleges in court papers the suspects told the Brazilian bank worker he would receive $13.4 million from an $187 million Nigerian airport contract -- if he invested money up front.

The bank worker allegedly dug illegally into his bank's funds, transferring the $242 million -- in segments as high as $4.75 million at a time -- to accounts around the world designated by the suspects, the papers showed.

Nigeria has gained global notoriety as a base for such advance-fee fraud, known as '419' schemes after the section of the country's criminal code that prohibits fraud.

http://www.cnn.com/2004/WORLD/africa/02/05/nigeria.419.trial.ap/index.html

SEC Charges Two Texas Swindlers In Penny Stock Spam Scam Involving Computer Botnets

Washington, D.C., July 9, 2007 - The Securities and Exchange Commission has filed securities fraud charges against two Texas individuals in a high-tech scam that hijacked personal computers nationwide to disseminate millions of spam emails and cheat investors out of more than $4.6 million. The scheme involved the use of so-called computer "botnets" or "proxy bot networks," which are networks comprised of personal computers that, unbeknownst to their owners, are infected with malicious viruses that forward spam or viruses to other computers on the Internet. The scheme began to unravel, however, when a Commission enforcement attorney received one of the spam emails at work.

The Commission alleges that Darrel Uselton and his uncle, Jack Uselton, both recidivist securities law violators, illegally profited during a 20-month "scalping" scam by obtaining shares from at least 13 penny stock companies and selling those shares into an artificially active market they created through manipulative trading, spam email campaigns, direct mailers, and Internet-based promotional activities. Scalping refers to recommending that others purchase a security while secretly selling the same security in the market.
[http://www.sec.gov/news/press/2007/2007-130.htm]

7. Control Systems

"The Most Monumental Non-Nuclear Explosion and Fire Ever Seen From Space."

- Thomas C. Reed, Ronald Regan's Secretary of the Air Force, described in his book At The Abyss (Ballantine, 2004, ISBN 0-89141-821-0) how the United States arranged for the Soviets to receive intentionally flawed ***process control software*** for use in conjunction with the USSR's natural gas pipelines, pipelines which were to generate critically needed hard currency for the USSR.

  Reed stated that "The pipeline software that was to run the pumps, turbines, and values was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds." The result? A three-kiloton blast in a remote area of Siberia in 1982, which, only by some miracle, apparently didn't result in any deaths. (For context, the Halifax Fire Museum lists the massive 1917 Mont Blanc ship explosion in the Halifax Harbor at a force of 2.9 kilotons.)

($50B) 9/14/03 US Blackout

- "Starting around 14:14, FE [FirstEnergy] control room operators lost the alarm function that provided audible and visual indications when a significant piece of equipment changed from an acceptable to problematic status. Analysis of the alarm problem performed by FE after the blackout suggests that the alarm processor essentially "stalled" while processing an alarm event. With the software unable to complete that alarm event and move to the next one, the alarm processor buffer filled and eventually overflowed. After 14:14, the FE control computer displays did not receive any further alarms, nor were any alarms being printed or posted on the EMS's alarm logging facilities.

  "FE operators relied heavily on the alarm processor for situational awareness, since they did not have any other large-scale visualization tool such as a dynamic map board. **The operators would have been only partially handicapped without the alarm processor, had they known it had failed. However, by not knowing that they were operating without an alarm processor, the operators did not recognize system conditions were changing and were not receptive to information received later from MISO and neighboring systems. The operators were unaware that in this situation they needed to manually, and more closely, monitor and interpret the SCADA information they were receiving."**

ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf [emphasis added]

8. Not All Network Vulnerabilities And Issues Are Technical: Insiders and Acts of God

An Insider Attack?

- "According to reports, Canadian telecommunications company **Aliant** (aliant.com) suffered an attack of vandalism on its network Tuesday night. The vandals reportedly cut fiber optic cables, leaving thousands of users in Nova Scotia and Newfoundland without phone and Internet service. **Approximately 125,000 people in Newfoundland (half its population) and 5,000 in Nova Scotia were affected.** Services were taken down at about 10:30 p.m. Service was not restored until 7:00 a.m. Cables were cut in two separate locations. In Newfoundland, a connection to the main network and the backup was targeted. In Nova Scotia, one piece of fiber optic cable was cut. **According to Aliant, the individual or individuals responsible had extensive knowledge of telecommunications networks. Aliant is currently embroiled in a major labor dispute with its 4,200 employees. Several reports have already noted the possible link between the dispute and the attack.** The Royal Canadian Mountain Police are investigating. As of Thursday, Aliant said service had been almost completely restored." http://www.thewhir.com/marketwatch/van061004.cfm

http://www.washingtonpost.com/wp-dyn/content/article/2006/12/27/AR

Big Quake Cuts Communications in Taiwan

By PETER ENAV and PETER SVENSSON
The Associated Press
Wednesday, December 27, 2006; 11:03 PM

TAIPEI, Taiwan -- Undersea fiber-optic cables were damaged by a powerful earthquake off the southern tip of Taiwan, causing the largest outage of telephone and Internet service in years and demonstrating the vulnerability of the global telecommunications network.

Two residents were killed and more than 40 injured in the magnitude-6.7 tremor that hit offshore, near the southern Taiwanese town of Hengchun late Tuesday.

Up to a dozen fiber-optic cables cross the ocean floor south of Taiwan, carrying traffic between China, Japan, Korea, Southeast Asia, the U.S. and the island itself. Chunghwa Telecom Co., Taiwan's largest phone company, said the quake damaged several of them, and repairs could take two to three weeks.

Enlarge This Photo

Taiwanese rescuers clear rubble from a collapse
building after a 6.7 magnitude earthquake struc

Conclusion

- It can be a pretty rough-and-tumble world out there
- There are some steps you can take to avoid at least some of those issues, and if you do so, the Internet remains pretty livable
- There are some issues (like control system vulnerabilities, intentional acts by insiders and acts of God) which remain difficult for individuals to directly control
- It's going to continue to take a lot of effort by everyone to work on dealing with all these issues
- Thanks for the chance to talk today!
- Are there any questions?