

Spam, Phishing & Trojans

CSH5 Chapter 20

“Spam, Phishing & Trojans:
Attacks Meant to Fool”

Stephen Cobb

1

Copyright © 2011 M. E. Kabay. All rights reserved.

CSH5 Chapter 20

Topics

- Introduction
- E-mail Basics
- Spam (not SPAM™)
- Fighting Spam
- Phishing
- Trojan Code



2

Copyright © 2011 M. E. Kabay. All rights reserved.

Introduction

- Definitions
 - ❑ Spam = unsolicited commercial e-mail
 - ❑ Phishing = use of deceptive spam to obtain confidential personal information
 - ❑ Trojan code = programs that have covert unauthorized functions (usually malicious)
- Serious consequences
 - ❑ Degradation in trustworthiness of e-mail
 - ❑ High volume of spam uses bandwidth
 - ❑ E-mail has become vector for technological & social harm



3

Copyright © 2011 M. E. Kabay. All rights reserved.

Common Elements

- All use deception
 - ❑ Prey on gullibility
 - ❑ Some exploit greed
 - ❑ All depend on ignorance
- Enabled by system services
- Run at the application layer
- Often combined for additional power & harm
- Consistently underestimated at time of emergence – warnings met with skepticism & hostility
- Rapid proliferation
- Enormous social & technological costs
- Associated with growth of financial gain as prime motivator for malware & Internet abuse



4

Copyright © 2011 M. E. Kabay. All rights reserved.

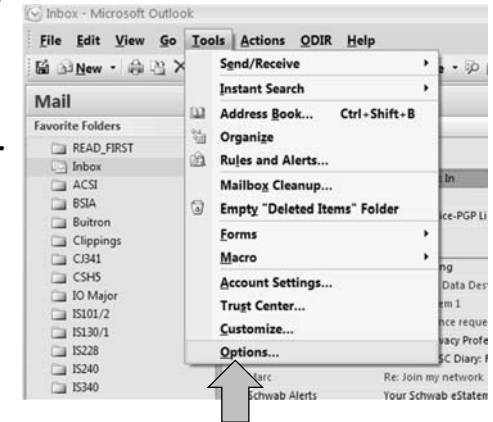
E-mail Basics

- E-mail at core of delivery method
 - ❑ SMTP – Simple Mail Transport Protocol
 - ❑ No process for verifying validity of FROM and TO data
- Attempts to add security to e-mail transmission
 - ❑ Whitelist: allowable senders
 - ✓ Difficult to maintain
 - ✓ Slows processing significantly
 - ❑ Blacklist: forbidden senders
 - ✓ Often wrong
 - ✓ Can be fooled by bad actors into adding legitimate sites (e.g., University e-mail being auto-forwarded to external e-mail system)

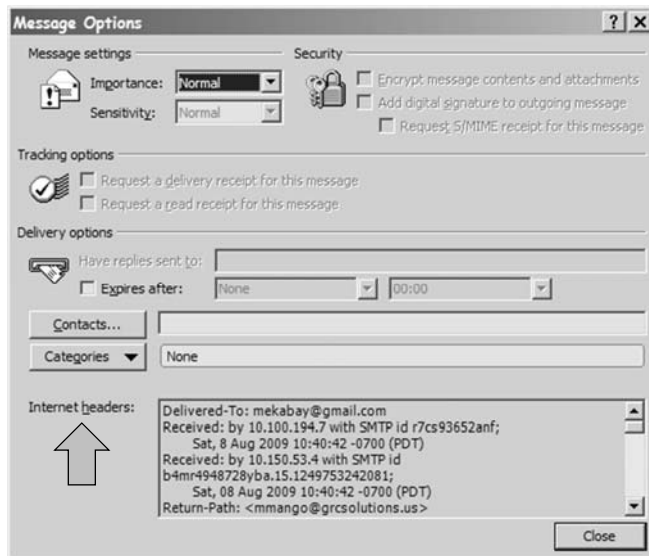


E-mail Headers (1)

- Every step in multistage transmission of e-mail adds information to the *header*
- E-mail programs usually
 - ❑ Suppress header but
 - ❑ Allow user to examine header on demand
 - ❑ No guarantee of locating original sender



E-mail Headers (2)



E-mail Headers (3)

```

Delivered-To: mekabay@gmail.com
Received: by 10.100.194.7 with SMTP id r7cs31769anf;
    Fri, 7 Aug 2009 08:37:11 -0700 (PDT)
Received: by 10.210.59.5 with SMTP id h5mr1550646eba.48.1249659430313;
    Fri, 07 Aug 2009 08:37:10 -0700 (PDT)
Return-Path: <register@caloga.com>
Received: from xb73.caloga.com (xb73.caloga.com [195.154.149.73])
    by mx.google.com with ESMTTP id
    5si9030773ewy.76.2009.08.07.08.37.08;
    Fri, 07 Aug 2009 08:37:09 -0700 (PDT)
Received-SPF: pass (google.com: domain of register@caloga.com designates
195.154.149.73 as permitted sender) client-ip=195.154.149.73;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
register@caloga.com designates 195.154.149.73 as permitted sender)
smtp.mail=register@caloga.com; dkim=pass header.i=@caloga.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=caloga.com; s=b; h=To:Subject:From:Reply-To:Mime-Version:
Content-Type:Message-Id:Date; bh=bJnEbQ995zW/silLnUF/1gdmA+VT9cP
VDv3YTFIT6HM=; b=Nf5f1SEZsZymFZFJzqJE+LDcl2bENbaf0rs9yBwyuBaOVne
epBUZJY2sVa505th4NdFkSkg21t6YM5AhAvM+8VtowOt6htpvWkyyf8KXcDNzliB
LAnEnBDEapmQxu+X/1JP2iHQHdzwrpyGHwvNh0zdFh0TjvrQiQ4pQ3EdTdj=
  
```

E-mail Headers (4)

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=simple; s=a; d=caloga.com;
h=Received:To:Subject:From:Reply-To:Mime-Version:Content-
Type:Message-Id:Date;
b=IchDBRKGQyNhQ4rUhJM6OXsRYZ7U1JkzYByQfPtzj7D8asqfE1kI/DjuAlPQOJ5
WuiR2c99CpmN2hSTRPCi1EsbRqDGZ9rVs5Y2ZjedCbblCMvevENZq2stmyntb0ISb;
Received: from www-data by caloga-deux.caloga.com with local (Exim 4.69)
(envelope-from <register@caloga.com>)
id 1MZRUd-0IAMxj-F9
for mekabay@gmail.com; Fri, 07 Aug 2009 17:36:31 +0200

To: mekabay@gmail.com
Subject: Profitez de 30 euros offerts pour en gagner plus
From: PMU par Caloga <register@caloga.com>
Reply-To: PMU par Caloga <register@caloga.com>
Mime-Version: 1.0
Content-Type: multipart/alternative;
boundary="Part4a7bdac8ac973"; charset="iso-8859-1"
Message-Id: <E1MZRUd-0IAMxj-F9>
Date: Fri, 07 Aug 2009 17:36:31 +0200
```

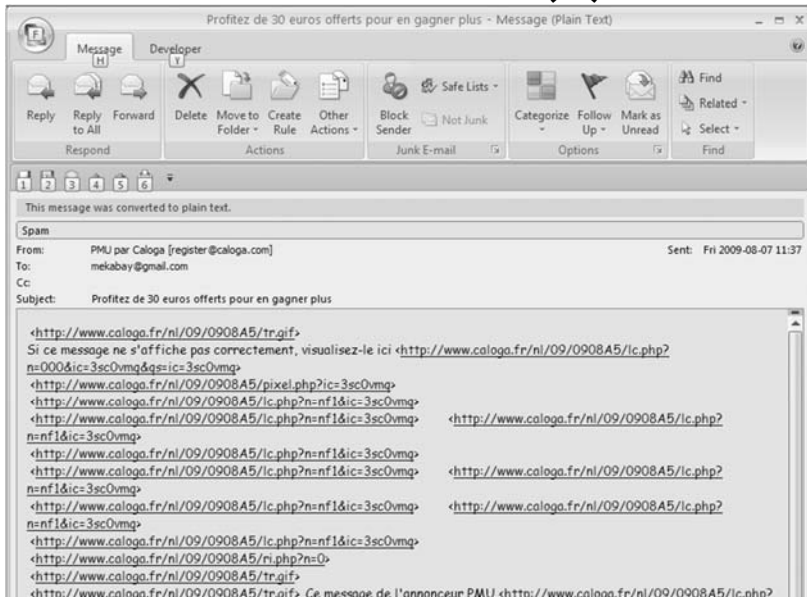
Visible in usual short header

E-mail Source Code (1)

- Early e-mail systems transmitted plaintext messages
 - EBCDIC for IBM systems
 - ASCII for everything else
- HTML e-mail
 - Supports formatting, stationery, visual signatures
 - Also supports malware, phishing



E-mail Source Code (2)



Spam Topics

- Origins & meaning of Spam (not SPAM™)
- Digging into Spam
- Spam's Two-Sided Threat
- Fighting Spam



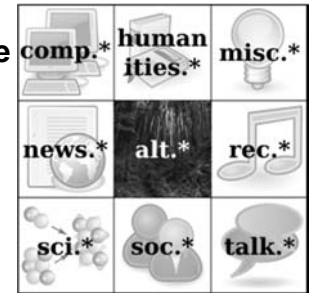
Spam (not SPAM™)

- SPAM™ is a trademark of the Hormel Corporation for a canned meat product
 - ❑ Do NOT use SPAM in all uppercase to refer to unsolicited commercial e-mail...
 - ❑ ... except if entire text is uppercase, as in a title
 - ❑ May use “Spam” as first word in a sentence or “spam” elsewhere (Hormel does not object to these usages)
- Origin is the Monty Python skit about a restaurant where almost all the dishes have SPAM™ in them
 - ❑ <http://pythonline.com/node/18297641>
- Applied 1st to MUDs, then BBS, then USENET



Spam & the USENET

- USENET is early form of social networking
 - ❑ Vast array of special-interest discussion groups
 - ❑ Spammers ruined USENET as medium of exchange – barrage of repetitious, unwanted commercial messages
- Spammers harvested e-mail addresses from USENET posts
 - ❑ Was the custom to include e-mail address in postings
 - ❑ Custom declined after mid-1990s due to abuse by spammers
- Spam volume reached 85% of all e-mail by 2005



Digging Into Spam

- Definitions
- Get Rich Quick
- Crime & Punishment
- Wasteful Game
- Magnitude of the Problem



Defining Spam

- Unsolicited Commercial E-mail (UCE)
 - ❑ Early definition
 - ❑ Emphasized types of unwanted e-mail that involved money
- Other forms of unsolicited e-mail criticized or defended
 - ❑ Political messages
 - ❑ Announcements of noncommercial events (conferences, art shows....)
 - ❑ Charity requests
- Questions about meaning of “unsolicited”
 - ❑ Spammers use any excuse to weasel around definitions of *unsolicited*
- Even legitimate companies tempted to spam



Get Rich Quick (1)

- Spamming can be profitable
 - ❑ Costs low or zero (esp. for pirate users of open spam relays – SMTP servers without security and botnet herders)
 - ❑ Even tiny % of responses from suckers can generate significant profit through fraud/theft
- C. P. Direct (spammers in Arizona) shut down 2002
 - ❑ Sold \$70M worthless anatomy-expanding pills
 - ❑ Refused to grant refunds when victims complained
 - ❑ Significant assets found by FBI
 - ✓ \$3M cash + jewelry
 - ✓ Bank account balances totaled >\$20M
 - ✓ 12 imported luxury cars (e.g., Lamborghini)
 - ✓ Owned office building + luxury real estate



Get Rich Quick (2)

- Selling spam also source of profit for criminals
 - ❑ Approach naïve companies
 - ❑ Claim to have huge lists of highly tailored opt-in targets
 - ❑ Charge for spam sent indiscriminately to anyone on lists
- Victims typically businesses in developing world
 - ❑ Growing frequency of such cases from PRC
 - ❑ Exacerbated by language difficulties
 - ❑ Hardworking people are primary victims; recipients are secondary victims



Crime & Punishment

- Risk of prosecution and severity of punishment are minor
- C. P. Direct perpetrators
 - ❑ Michael Consoli & Vincent Passafiume pled guilty Aug 2003
 - ❑ Out of jail before May 2004
 - ❑ Petitioned Arizona Court of Appeals to overturn convictions and return their loot
- Jeremy Jaynes: a Top-Ten Spammer in 2003
 - ❑ Sent out 10M spam msg/day for \$750K/mo profit
 - ❑ Convicted 2004, sentenced to 9 years prison
 - ❑ Appealed conviction on constitutional grounds (see next slide)



Jeremy Jaynes Absolved



- Grounds in case before VA Court of Appeals (2006)
 - ❑ VA anti-spam law violates Commerce Clause by regulating e-mail sent outside state
 - ❑ Violates First Amendment because spam is form of free speech
 - ❑ Court rejected both arguments
- VA Supreme Court first round (Feb 2008)
 - ❑ Rejected standing to raise 1st amendment defense
- VA Supreme Court second round (Sep 2008)
 - ❑ Rehearing: accepted standing for 1st Amendment
 - ❑ Reversed its earlier ruling and vacated convictions on grounds that anti-spam statute violated 1st Amendment by being overbroad
- SCOTUS refused writ of *certiorari* and declined to review case – ruling stands as a precedent

Spam a Wasteful Game (1)

- Play on gullibility
 - ❑ Send money to learn how to earn money easily
 - ❑ Sometimes response is to send spam teaching how to earn money by sending spam....
- Other widespread scams
 - ❑ Pump 'n' dump schemes (raise/lower value of stock through spammed lies)
 - ❑ Phishing schemes discussed later
 - ❑ Nigerian 419 fraud & fake lottery winnings (advance-fee fraud)



Wasteful Game (2)

Costs borne by

- E-mail recipients
 - ❑ Waste time sorting through spam to find good e-mail
 - ❑ Pays to receive e-mail (someone always pays for Internet connection)
- Enterprises
 - ❑ Lost productivity due to delay in finding real e-mail
 - ❑ Costs of anti-spam measures
 - ❑ Wasted resources (bandwidth, disk space, CPU)



Wasteful Game (3)

- ISPs
 - ❑ Wasted resources (bandwidth, disk space, CPU)
 - ❑ Spam filtering costs, | administration
 - ❑ Policing users to prevent blacklisting
- Other economic factors
 - ❑ Depressed economy seems to increase gullibility & therefore spam
 - ❑ Spammers use as much bandwidth as they can get, so battle is never-ending

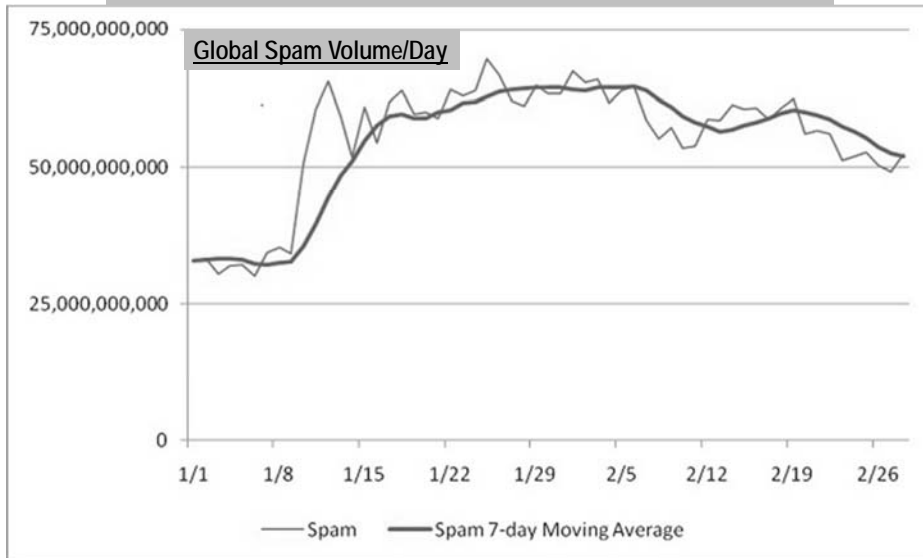


Magnitude of the Problem (1)

- Misperception that spam is not significant
 - ❑ Newbies
 - ❑ Office-only users whose e-mail is filtered before they see it – thus little spam in their inbox
- Proportion of all e-mail that is spam has grown rapidly
 - ❑ 1994 – 0%
 - ❑ 2002 – 50%
 - ❑ 2011 – 80-90% depending on source of statistics
- Major effects on ISP infrastructure
 - ❑ Disk storage
 - ❑ Bandwidth
- See graphs from Symantec on next 2 slides

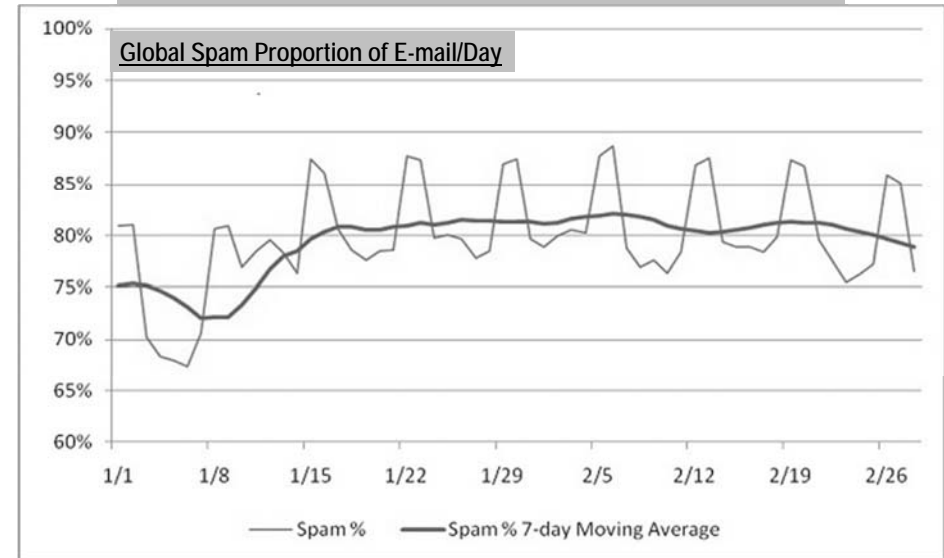
Magnitude of the Problem (2)

<http://www.symantec.com/connect/blogs/update-global-spam-volume>



Magnitude of the Problem (3)

<http://www.symantec.com/connect/blogs/update-global-spam-volume>



Spam's Two-Sided Threat

- Threat to resources well documented
 - ❑ As discussed in previous sections
 - ❑ Damages to a modest company can easily be counted in \$M/year
- But other side is risk that employee will involve organization in sending spam
- Topics of following slides:
 - ❑ Threat of Outbound Spam
 - ❑ Mass E-Mail Precautions
 - ❑ Appending & Permission Issues

Threat of Outbound Spam

- Rogue marketers can be tempted to spam for what they hope will be cheap, quick results
- Damage to organization
 - ❑ Damage relations with existing customers
 - ❑ Alienate potential customers
 - ❑ Tarnish reputation
 - ❑ All outbound e-mail may be blocked once company associated with spamming
 - ❑ Retaliation (see next slide)

Network World (Dec 1994)

Anonymous executive writing in *Network World* (1994)

- Posted advertising to 20 USENET news groups
 - ❑ Stupidly posted message 20 times instead of once to 20 groups – readers received *multiple copies* of spam
- Thought people would be interested
- Consequences
 - ❑ E-mail bombs sent to company e-mail addresses
 - ❑ Toll-free number posted in *alt.sex* groups
 - ✓ Thousands of obscene phone calls
 - ✓ Receptionist quit
 - ✓ All toll-free calls sent directly to his phone
 - ❑ Nearly destroyed his career
- Urged readers never to do such a stupid thing!

Mass E-Mail Precautions

- Never send e-mail unless you are sure you know what it will look like to recipient
 - ❑ Don't assume formatted e-mail accepted
 - ❑ Perhaps append a PDF formatted document
- Address field
 - ❑ Use TO: only for few people directly involved
 - ❑ Use CC: only for few people who may want to respond to each other
 - ❑ OTHERWISE, use BCC to hide all the addressees
 - ✓ Reduce wasted e-mail from REPLY ALL
 - ✓ Protect confidentiality of recipients
 - ✓ Reduce access to addresses by spammers

Six Resolutions for Responsible E-Mailers

1. Don't falsify origin or use dummy IP address
2. Don't use misleading/false SUBJECT line
3. Include option in message for unsubscribing
4. Inform respondent of purpose of collecting e-mail address
5. Don't harvest e-mail addresses to spam people
6. Do not send bulk unsolicited e-mail to people who do not have a *prior established business or personal relationship* to the sender



Council for Responsible E-Mail
Association for Interactive Marketing
Direct Market Association

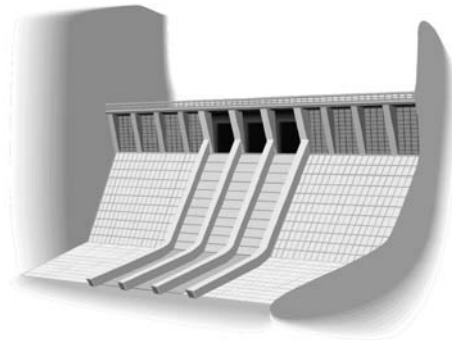
Appending & Permission Issues

- Companies called *e-mail appenders* offer to find e-mail addresses for customers who have not provided them
- Some of the e-mail addresses are wrong: not right person – raises privacy issues
- Some recipients object to harvesting and use of their e-mail address without permission
- May violate written privacy policy: legal liability



Fighting Spam

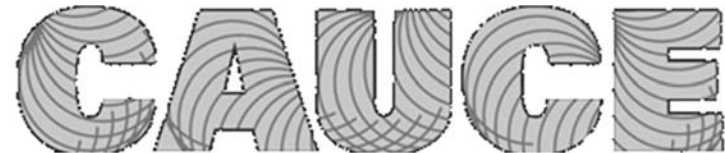
- Spam Fighters
- Good Reputation
- Relaying Trouble
- Black Holes & Block Lists
- Spam Filters
- Network Devices
- E-mail Authentication
- Industry Initiatives
- Legal Remedies



Spam Fighters: CAUCE

Coalition Against Unsolicited Commercial E-mail

- <http://cauce.org>
- CAUCE US founded 1997 by USENET members in news.admin.net-abuse.email & SPAM-L mailing list
- CAUCE North America joined CAUCE US & CAUCE Canada.
- Instrumental in passing antis spam laws



Spam Fighters: Spamhaus (1)

Spamhaus Project founded 1998 by Steve Linford

- <http://www.spamhaus.org>
- Goals
 - ❑ Tracks the Internet's spammers, spam gangs & spam services
 - ❑ Provides dependable realtime anti-spam protection for Internet networks
 - ❑ Works with law enforcement to identify and pursue spammers worldwide
- (cont'd on next slide)



Spam Fighters: Spamhaus (2)

- SBL: Spamhaus Block List **SBL Advisory**
 - ❑ <http://www.spamhaus.org/sbl/index.lasso>
 - ❑ Realtime database of IP addresses
 - ✓ Verified spam sources & operations
 - ✓ Free for e-mail administrators
- XBL: Exploits Block List **XBL Advisory**
 - ❑ <http://www.spamhaus.org/xbl/index.lasso>
 - ❑ Realtime database of IP addresses of hijacked PCs
 - ❑ Including open proxies, worms/viruses with spam engines...
- PBL: Policy Block List **PBL Advisory**
 - ❑ <http://www.spamhaus.org/pbl/index.lasso>
 - ❑ Database of IP address ranges that should never deliver SMTP e-mail to Internet mail server except their own
 - ❑ Maintained in collaboration from ISPs and network admins

Commercial Antispam Products

- Began in late 1990s as filters for individuals
- Some well-known appliances & services
 - ❑ Brightmail (Symantec) <http://tinyurl.com/lcyl33>
 - ❑ Postini (Google) <http://tinyurl.com/r77p7v>
 - ❑ IronPort (Cisco) <http://www.ironport.com/>
 - ❑ Cloudmark <http://www.cloudmark.com/>
 - ❑ SPAMfighter <http://www.spamfighter.com/>
- Open-source: Apache SpamAssassin Project
 - ❑ <http://spamassassin.apache.org/>

These references are not endorsements.

Whitelisting

- Respond to unknown senders
- Ask for human interaction
- Approve once forever
- Use CAPTCHA* to prevent automated response



ALLOWED SENDER REQUEST FORM EarthLink spamBlocker

To prevent unsolicited email, billr@footepartners.com has enabled this verification step.

Please complete the short form below. If billr@footepartners.com chooses to allow email from your address, the message(s) that have been intercepted will be delivered immediately, and any future message(s) will be delivered without delay.

Your First Name: M.I. Your Last Name:

Enter your additional email addresses here:
Address 1: mekabay@gmail.com
Add other addresses (if you have more than one).

Please type a short message to billr@footepartners.com. (100 characters, max.)

This step provides added security.
Type the text from the image below into the box to the right.

 Request New Text

Text | Audio
Help for the visually impaired

*Completely Automated Public Turing test to tell Computers and Humans Apart

SEND REQUEST NOW

Good Reputation

- Theory: recognize reliable/trustworthy sources
- Challenge-response
 - ❑ Earthlink ISP rolled out system in 2003
 - ❑ First time one sends e-mail to Earthlink customer, must respond to query e-mail before being allowed through
 - ❑ But some legitimate sources have no-response return addresses
- Whitelist
 - ❑ Maintain list of sources that are deemed reliable
- Cryptographic seal
 - ❑ Establish authentic origin
 - ❑ ePrivacy Group project failed to win sufficient market share to be effective
 - ❑ S/MIME digital signatures might also work

Relaying Trouble

- ISPs almost universally ban spamming
 - ❑ Exceptions are criminal organizations providing spam services
- Open spam relays
 - ❑ SMTP servers that do not require identification & authentication to send mail
 - ❑ Grounds for black-holing
 - ❑ Still some open relays left on the 'Net due to administrative laziness / irresponsibility
- Botnets create their own SMTP servers (daemons) on compromised computers



Black Holes & Block Lists

- Catalog IP addresses that have sent out significant volumes of spam
 - Direct originators
 - Open spam relays
 - Compromised by botnet daemons
- User systems check list before passing on e-mail – or drop packets

Original black hole list: MAPS RBL

 - Mail Abuse Prevention System Realtime Blackhole List (1997, Paul Vixie)
 - Sold to TREND Micro in 2005
 - Renamed *Email Reputation Services*
 - <http://tinyurl.com/43g9dp>
- Other products also include black holes (see earlier slides)



Spam Filters

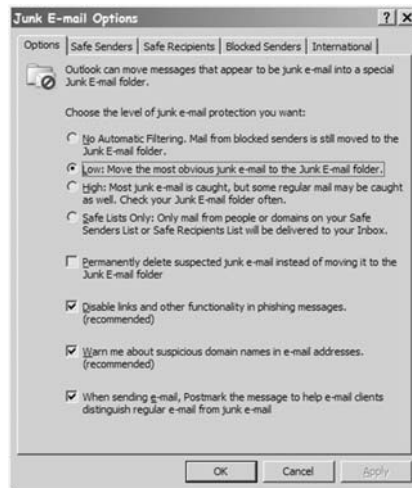
Content filtering another approach

- End-user Filters
- ISP Filtering
- Filtering Services
- Collateral Damage



End-user Filters

- Individual e-mail client settings available
 - Can automatically file e-mail from known correspondents into separate mailboxes
 - Rest can be examined more quickly
- Commercial products compile databases of signatures
 - Anything missed can be reported by user



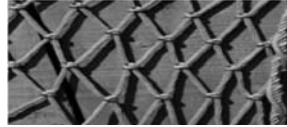
ISP Filtering

- Concern about content-based filtering
 - Construed as privacy invasion
 - Risks of false-positives
- Focused on SUBJECT field
 - Hence spammers use variant spellings & bizarre punctuation to avoid filters
- Public ISPs face legal issues
 - Status as equivalent of common carriers at risk if they filter too aggressively
- Individual corporations have no legal constraints
 - No privacy rights involved
 - No legal obligation to deliver unwanted e-mail



Filtering Services

- Redirect all client's e-mail to their servers
- Use wide range of spam-spotting techniques
 - ❑ Block lists
 - ❑ Header analysis
 - ❑ Content analysis
 - ❑ Known-spam signature comparisons
 - ❑ Heuristic filtering for spam-like features
 - ❑ Whitelisting
- Enormous volumes allow refinements in filtering algorithms
- Collective intelligence schemes rely on users to vote on whether message is spam
 - ❑ E.g., Cloudmark
 - ❑ Reliability of voter determines weight (thus eliminating spammers' votes for their own spam)



45

Copyright © 2011 M. E. Kabay. All rights reserved.

Collateral Damage

- Spammers can keep spamming
 - ❑ Costs of resources fall on the victims, not the spammers
 - ❑ Nothing prevents spammers from trying new methods
 - ❑ Overall resource utilization slows e-mail, uses processing & other resources on many systems
- Type I & Type II errors
 - ❑ Type I error: false positive – mistakenly classifying legitimate e-mail as spam
 - ❑ Type II error: false negative – failing to recognize spam

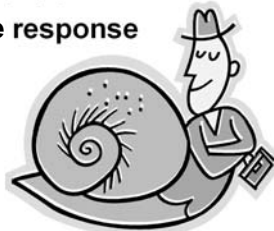


46

Copyright © 2011 M. E. Kabay. All rights reserved.

Network Devices

- One approach to attacking spammers is to track the money
- Most spam designed to generate revenue
 - ❑ Therefore always some legitimate response address
 - ✓ E-mail
 - ✓ Web site
- But Web addresses for spammers disappear / mutate rapidly
- Therefore key response is to *slow spam down*
 - ❑ Delay spam (or spam suspects) using antispam router and *traffic shaping*
 - ❑ Delay is disaster for spammer, negligible for legitimate traffic



47

Copyright © 2011 M. E. Kabay. All rights reserved.

E-mail Authentication

- If real sender of e-mail were known, would greatly interfere with spammers' spoofing
 - ❑ Several attempts to add authentication of sender's domain name to e-mail
- Sender Policy Framework (SFP)
<http://www.openspf.org/>
- Certified Server Validation (CSV)
<http://mipassoc.org/csv/>
- SenderID (Microsoft)
<http://tinyurl.com/9rs9b>
- DomainKeys Identified Mail (DKIM)
<http://www.dkim.org/>



48

Copyright © 2011 M. E. Kabay. All rights reserved.

Industry Initiatives

- Major e-mail service providers tried to cooperate
 - ❑ Started in 2002
 - ❑ AOL, Microsoft, Earthlink, Yahoo = *AMEY*
- US FTC convened conference on spam in 2003
- Bill Gates announced the end of spam
 - ❑ Jan 2004 at World Economic Forum
- Mar 2004: AMEY launched lawsuits against major spammers
- But project failed
 - ❑ Companies tried to protect their intellectual property
 - ❑ Refused to cooperate on open-source software

Legal Remedies

- US CAN-SPAM Act of 2003
 - ❑ Controlling the Assault of Non-Solicited Pornography and Marketing Act
 - ❑ Enforced by FTC
 - ❑ Bans false / misleading header info
 - ❑ Prohibits deceptive subject lines
 - ❑ Requires inclusion of opt-out method
 - ❑ Requires self-labeling as advertisement & valid physical postal address
- Complete failure – no visible effect whatsoever
- Led to Prof Kabay's favorite Network World Security Strategies column title: CAN CAN-SPAM CAN SPAM?



Phishing

- Defining Phishing
- What Phish Look Like
- Growth & Extent of Phishing
- Where is the Threat?
- Phish Fighting



Image provided courtesy of
How Stuff Works.com
<http://computer.howstuffworks.com>

Defining Phishing

- Use of spam to fish for personally identifiable information (PII)
- Try to simulate official-looking e-mail to fool victims into cooperating
- Aim is financial fraud
- Began ~2004
- Has grown steadily & become major problem
- Variants include *spear phishing*
 - ❑ Claiming that e-mail comes from recognizable origin; e.g., HelpDesk at specific company
 - ❑ Targets employees in specific organization

What Phish Look Like (1)

- Simulate appearance of legitimate-looking e-mail
 - ❑ Logos
 - ❑ Typefaces
 - ❑ Links *labeled* with credible URLs
- Glaring errors
 - ❑ Many phishing scams run by non-native English speakers
 - ❑ Full of spelling & grammar mistakes
- Logic errors that should be caught by recipients (but are often overlooked)
 - ❑ Why would anyone sign into a Web site to confirm a compromised userID/password combo? Doesn't make sense!

What Phish Look Like (2)

- Clues that a message is bogus
- Deceptive links – check source of e-mail
 - ❑ Descriptions don't match underlying URLs
 - ❑ Numerical IP addresses conceal foreign sites
- Request to change PIN or password
 - ❑ As described in previous slide, does not make sense
 - ❑ No legitimate agency/bank would request such a thing
- Generic greetings (Dear Customer – or “Cutsomer”)
- Bad spelling and grammar
- Masking specific details (e.g., no name of bank)

Examples of Attacks

- People's Bank - 'New Mail'
- Citibank - 'Alert Service'
- Paypal - 'Your Account Will Be Suspended'
- Sovereign Bank - 'Unauthorized Account Access'
- Citibank - 'Security Alert on Microsoft Internet Explorer'
- eBay - 'TKO NOTICE: Verify Your Identity'
- Verizon - 'Update your Verizon billing profile'
- Washington Mutual Bank – 'Internet Banking Account'

People's Bank

peoples.com

Dear People member.

We ask you to confirm immediately of your parity the account to given e-mail.

www.people-onlinebank.net

Otherwise we stop temporarily service of your account.

Thank you for using Suntrust Bank!

Not the proper domain for peoples.com

Please do not reapy this letter.

Again, thank you for using People.com

Citibank (Nov 10)

Dear Citibank Customer

We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking [here](#).

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Links to
<http://82.90.165.65/citi>

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

PayPal (1)



Security Center



Military Grade Encryption is Only the Start

At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.

PayPal (2)

Actually links to
<http://212.45.13.185/paypal/index.php>

<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend to verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,
PayPal Account Review Department
PayPal, an eBay Company



Citibank (Nov 1, 2004)

Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced some new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

This security update will be effective immediately. Please sign on to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.

Citibank Online

Copyright © 2004 Citicorp

Links to
<http://200.189.70.90/citi/>

eBay (1)



Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

<http://signin-ebay.com/cgi-bin.tk/eBay.dll.php>

Please update and verify your information by clicking the link below:

<https://scgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo>

If your account information is not updated within 48 hours then your ability to sell or bid on eBay will become restricted.

eBay (2) – Detailed Analysis

Received by MK 2004-11-17



Dear valued customer

[Need Help?](#)

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please [click here](#) and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.

This is an automatic message. Please do not reply.



eBay(2) Source Code

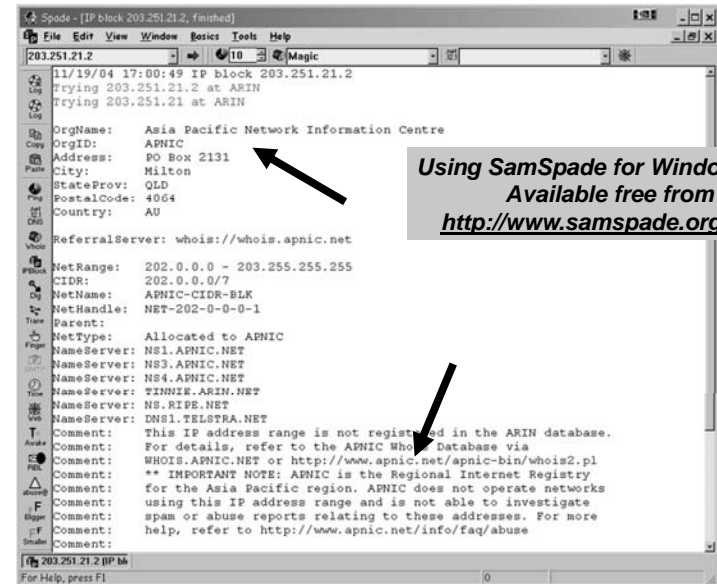
Extract of relevant section:

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please

<http://203.251.21.2/signin.ebay.com/ws2/eBayISAPl.dll/b2baf0b6a57d39abd6c44b48d6fe3559112c21e54b7e705ecc5116b3c7c38c37949e8aa81848934faf0821be04210e8c2ded3c4159edbee3ee1439f3892a3e91/>

click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

eBay (2) Reverse IP Lookup



Using SamSpade for Windows v1.4
Available free from
<http://www.samspace.org/ssw/>

eBay (2) APNIC R-IP Lookup



Asia Pacific Network Information Centre
 APNIC Info & FAQ | Resource services | Training | Meetings | Membership | Documents |
 Whois & Search | Internet community

You're Here: Home → Database Quick Links

Query the APNIC Whois Database

Need help?

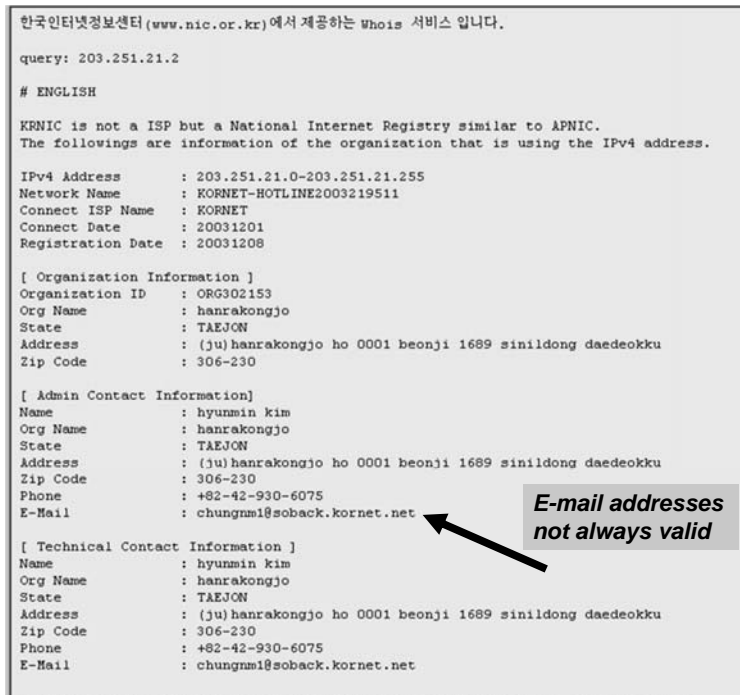
- General search help
- Help tracking spam and hacking
- To assist you with debugging problems, this whois query was received from IP Address [148.84.98.189]. Your web client may be behind a web proxy.

% [whois.apnic.net node-2]
 % Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

```
inetnum:      203.249.0.0 - 203.251.255.255
netname:      KRNIC-KR
descr:        KRNIC
descr:        Korea Network Information Center
country:      KR
admin-c:      HM127-AP
tech-c:       HM127-AP
remarks:      *****
remarks:      KRNIC is the National Internet Registry
remarks:      in Korea under APNIC. If you would like to
remarks:      find assignment information in detail
remarks:      please refer to the KRNIC Whois DB
remarks:      http://whois.nic.or.kr/english/index.html
remarks:      *****
ant-by:       APNIC-HM
ant-lower:    NNT-KRNIC-AP
changed:      hostmast@rs.krnic.net 19981015
changed:      ha-changed@apnic.net 20010606
changed:      ha-changed@apnic.net 20040229
status:       ALLOCATED PORTABLE
source:       APNIC
```

Asia-Pacific Network
Information Center
Routes to KoreaNIC

eBay (2) KRNIC R-IP Lookup



한국인터넷정보센터 (www.nic.or.kr)에서 제공하는 Whois 서비스입니다.

query: 203.251.21.2

ENGLISH

KRNIC is not a ISP but a National Internet Registry similar to APNIC.
 The followings are information of the organization that is using the IPv4 address.

IPv4 Address : 203.251.21.0-203.251.21.255
 Network Name : KORNET-HOTLINE2003219511
 Connect ISP Name : KORNET
 Connect Date : 20031201
 Registration Date : 20031208

[Organization Information]
 Organization ID : ORG302153
 Org Name : hanrakongjo
 State : TAEJON
 Address : (ju)hanrakongjo ho 0001 beonji 1689 sinildong daedeokku
 Zip Code : 306-230

[Admin Contact Information]
 Name : hyunmin kim
 Org Name : hanrakongjo
 State : TAEJON
 Address : (ju)hanrakongjo ho 0001 beonji 1689 sinildong daedeokku
 Zip Code : 306-230
 Phone : +82-42-930-6075
 E-Mail : chungnm1@soback.kornet.net

[Technical Contact Information]
 Name : hyunmin kim
 Org Name : hanrakongjo
 State : TAEJON
 Address : (ju)hanrakongjo ho 0001 beonji 1689 sinildong daedeokku
 Zip Code : 306-230
 Phone : +82-42-930-6075
 E-Mail : chungnm1@soback.kornet.net

E-mail addresses not always valid

Growth & Extent of Phishing

➤ Anti Phishing Working Group (APWG) documents phenomenon

☐ <http://apwg.org/>

☐ Extensive reports with graphs & analysis

➤ See extracts from 2010 July-Dec report on next slides



2011 H1 (APWG)

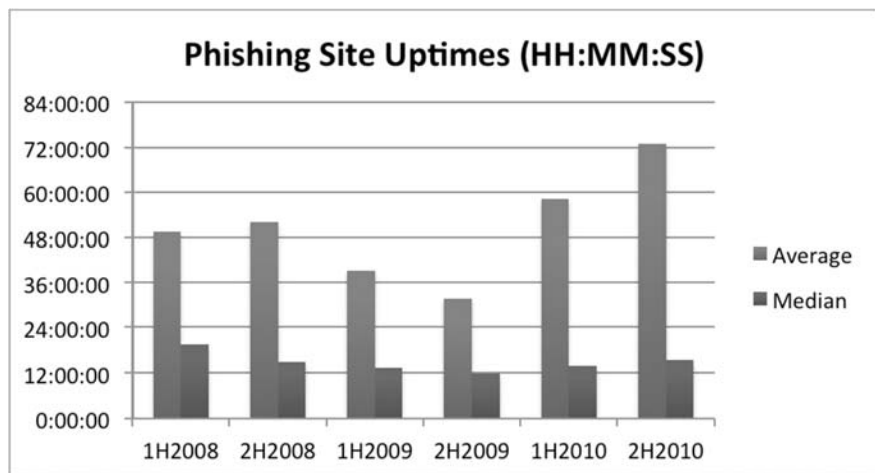
Basic Statistics

	2H2010	1H2010	2H2009	1H2009	2H2008
Phishing domain names	42,624	28,646	28,775	30,131	30,454
Attacks	67,677	48,244	126,697	55,698	56,959
TLDs used	183	177	173	171	170
IP-based phish (unique IPs)	2,318	2,018	2,031	3,563	2,809
Maliciously registered domains	11,769	4,755	6,372	4,382	5,591
IDN domains	10	10	12	13	10

Each domain name's registrar of record was not reported at the time the phish was live. Obtaining accurate registrar sponsorship data for a domain name requires either time-of-attack WHOIS data, or historical registry-level data. These data have not been collected in a comprehensive manner by the anti-phishing community.

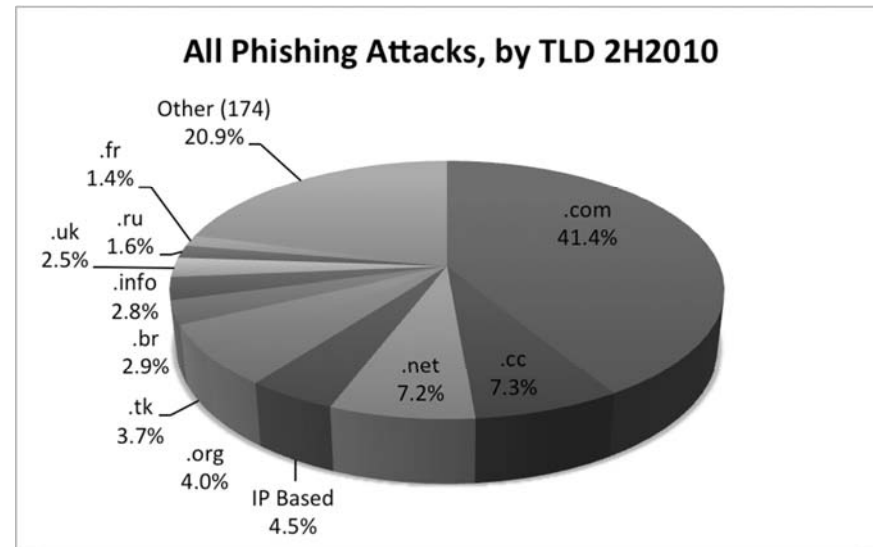


2011 H1 (APWG)



69 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

2011 H1 (APWG)



70 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

2011 H1 (APWG)

Top 10 Phishing TLDs by Domain Score

Minimum 25 phishing domains and 30,000 domain names in registry

RANK	TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010
1	.th	Thailand	125	65	51,438	12.6
2	.ir	Iran	295	169	175,600	9.6
3	.ma	Morocco	73	34	36,669	9.3
4	.ie	Ireland	112	96	151,023	6.4
5	.tk	Tokelau	2,533	2,429	4,030,709	6.0
6 (tie)	.kz	Kazakhstan	49	28	50,534	5.5
6 (tie)	.cc	Cocos Islands	4,963	55	100,000	5.5
7	.in	India	523	421	791,165	5.3
8	.my	Malaysia	68	55	108,211	5.1
9	.hu	Hungary	365	255	542,000	4.7

71 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

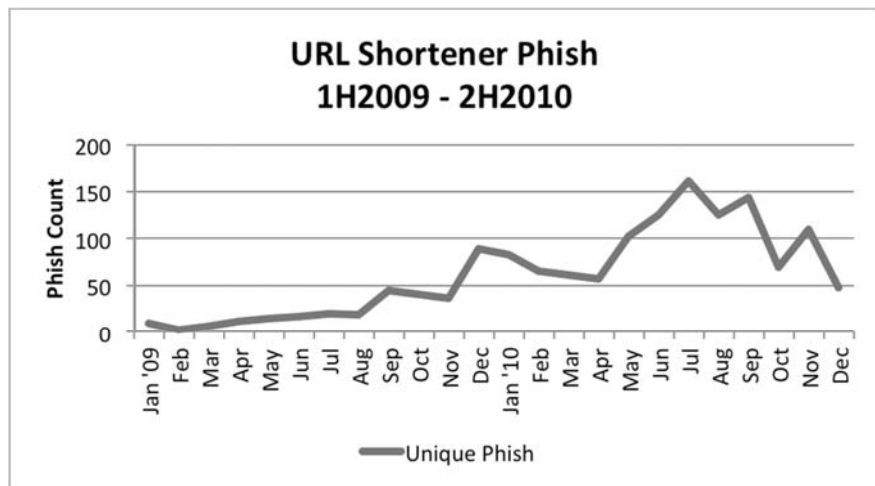
2011 H1 (APWG)

Top 10 TLDs for Maliciously Registered Phishing Domains, 2H2010

Rank	TLD	TLD Location	Total Attacks
1	.com	generic TLD	5,617
2	.tk	Tokelau	2,429
3	.net	generic TLD	1,258
4	.info	generic TLD	1,164
5	.us	United States	255
6	.org	generic TLD	254
7	.in	India	251
7	.cn	China	131
9	.uk	United Kingdom	57
10	.nl	Netherlands	39

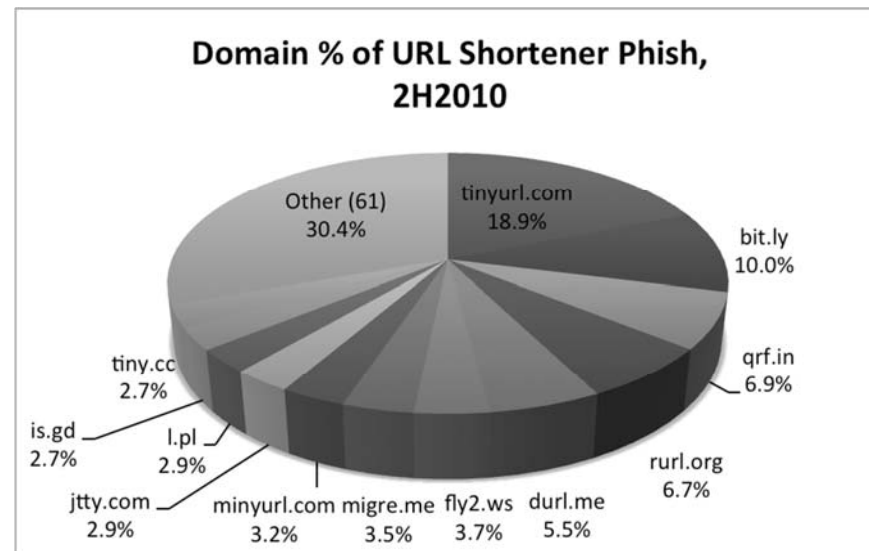
72 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

2011 H1 (APWG)



73 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

2011 H1 (APWG)



74 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

Keyloggers & Redirectors

- Keyloggers record and upload your passwords (and everything else) typed on keyboard
- Redirectors send compromised users to dangerous Web pages
 - Can modify Domain Name System (DNS) servers to pass back wrong addresses
 - Or install local drivers on infected workstations to send traffic to fraudulent DNS servers
 - Or filter lookups for specific redirection to criminal sites



Where is the Threat?

- Individuals
 - Victimized by gullibility, ignorance
 - FTC & others trying to teach public wariness
 - Not working very well
- Companies & e-commerce
 - Too many people use same password / PIN on all their accounts
 - Compromise using phishing on personal info may open up corporate systems, national security assets
 - Undermine consumer trust in vendor



Phish Fighting

- Consumer education
 - ❑ E.g., Phishing Education Landing Page Program
 - ✓ Simple method to put educational page in place of 404 when phishing page taken down
 - ✓ <http://education.apwg.org/r/about.html>
- Fix e-mail (will be a while)
- Blacklisting through browser
- Authenticate Web sites
 - ❑ SiteKey
(see <http://tinyurl.com/3mepsz>)
 - ❑ SafePass mobile phone text messaging
(see <http://tinyurl.com/knegax>)
 - ❑ Token-based authentication instead of shared secrets (passwords & PINs)



Trojans

- Trojan Code
- Basic Anti-Trojan Tactics
- Lockdown & Quarantine



Trojan Code

- Trojan horse used by Greeks to trick Trojans into allowing soldiers hidden in belly of wooden statue into city
- Common Trojans include
 - ❑ Screensavers
 - ❑ Pornography
- Trojan droppers are programs that bundle Trojans along with harmless code
 - ❑ Typically in compressed archive
 - ❑ Created by *joiner* programs
 - ❑ May install components directly into RAM
 - ❑ Often used to install spyware / adware / viruses
 - ❑ See F-SECURE page at <http://tinyurl.com/lqcbic>



"Ulysses, I finished the welding project."

Basic Anti-Trojan Tactics

- Well-educated users who don't
 - ❑ Execute random code
 - ❑ Open attachments from strangers
 - ❑ Open unexpected attachments even from known sources
- Keep operating systems and applications up to date: versions & patches
- Run good antimalware/antivirus ("AV") software at all times
- Scan system regularly using AV
- Beware messages claiming to be malware alerts – classic scam to trick users
- Don't fall for "scan-your-system-for-malware" ads

Lockdown & Quarantine

- Prevent unauthorized changes to code
- Prevent connections to unauthorized networks
- Scan all systems for safety before allowing connection; e.g., *Cisco Clean Access Agent*
 - ❑ Now called Cisco NAC (Network Admission Control) Appliance
 - ❑ <http://www.cisco.com/en/US/products/ps6128/>
 - ❑ Evaluates & remediates compliance with security policies; e.g.,
 - ✓ Up-to-date AV strings
 - ✓ Current patches
 - ❑ Blocks non-compliant systems



DISCUSSION