

Spyware Recommendations

- NOD32 Anti Virus ($40 w/free 1 month trial)
  - http://www.nod32.com/download/trial.htm
- Counterspy 1.5 from Sunbelt (Spyware - $20 free 15 day trial)
  - http://www.sunbelt-software.com/CounterSpy.cfm
- Ewido Security Suite ($29.95 w/free 1 month trial)
  - http://www.ewido.net/en/
- Netcraft Toolbar for Internet Explorer
  - http://www.toolbar.netcraft.com
- Spysweeper from Webroot ($20-30)
  - http://www.webroot.com/



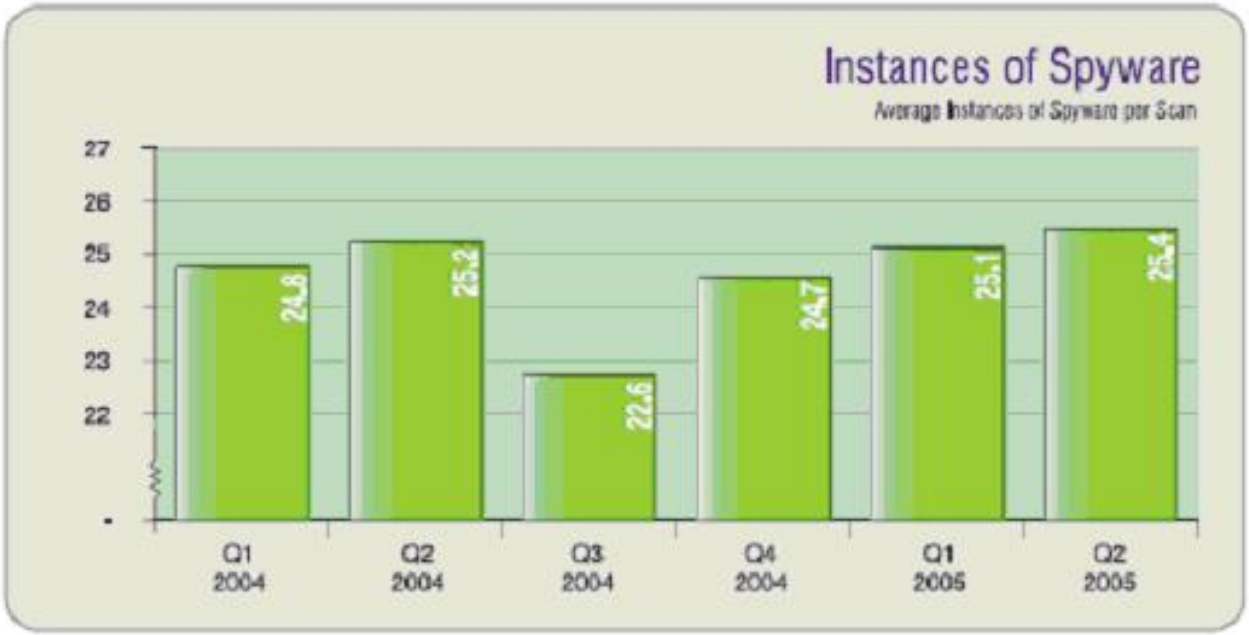
Spyware Recommendations (cont'd)

- Spyware Blaster (free spyware protection)
  - http://www.javacoolsoftware.com/spywareblaster.html
- Spyware Guard (free spyware protection)
  - http://www.javacoolsoftware.com/spywareguard.html
- Cleanup 4.0 (free cleaner - you need this)
  - http://cleanup.stevengould.org
- RegSupremePro (Registry cleaner - $16.95 w/free 1 month trial)
  - http://www.macecraft.com/regsupremepro/

80% of Consumer PC's are Infected

Overall Results

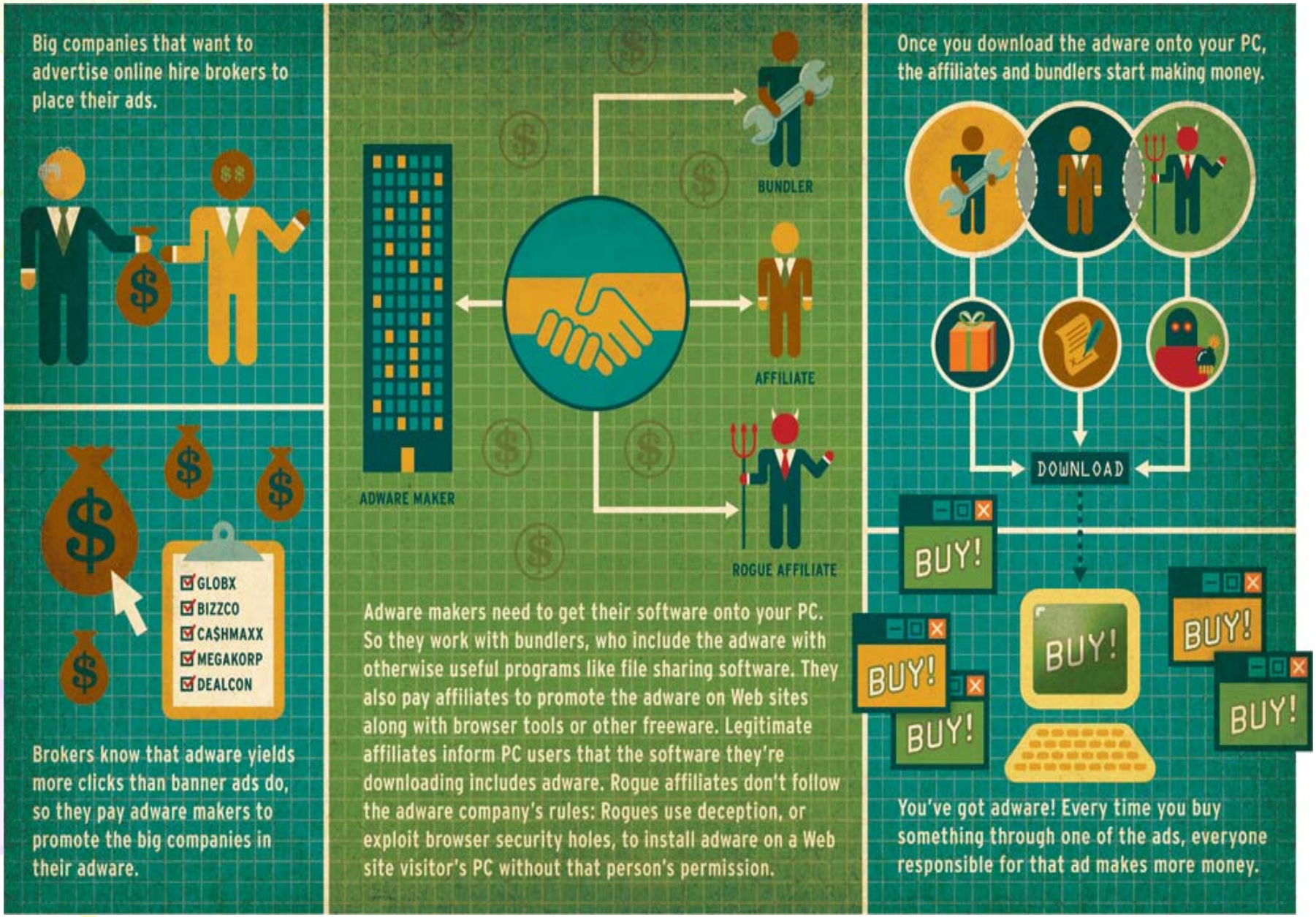
In Q2 2005, the Consumer SpyAudit results showed that the percentage of infected consumer PCs remained elevated at more than 80 percent. The number of spyware instances per machine has increased to an all-time high of 25.4 per machine, up from 22.8 instances per PC from Q1 of 2005.



System Monitor Infection

- Six percent of PC's scanned are infected
- Between 1-2 Instances per infected PC
- Trojan horse via email or Instant Message
- Creates Zombies for Denial Of Service & Email Programs for sending Spam
- Acts as fake website for Phishing
- Trojan allows hacker to 'own' PC

Adware


Big companies that want to advertise online hire brokers to place their ads.
GLOBX
BIZZCO
CA$HMAXX
MEGAKORP
DEALCON
Brokers know that adware yields more clicks than banner ads do, so they pay adware makers to promote the big companies in their adware.
BUNDLER
AFFILIATE
ADWARE MAKER
ROGUE AFFILIATE
Adware makers need to get their software onto your PC. So they work with bundlers, who include the adware with otherwise useful programs like file sharing software. They also pay affiliates to promote the adware on Web sites along with browser tools or other freeware. Legitimate affiliates inform PC users that the software they're downloading includes adware. Rogue affiliates don't follow the adware company's rules: Rogues use deception, or exploit browser security holes, to install adware on a Web site visitor's PC without that person's permission.
Once you download the adware onto your PC, the affiliates and bundlers start making money.
DOWNLOAD
BUY!
BUY!
BUY!
BUY!
BUY!
BUY!
You've got adware! Every time you buy something through one of the ads, everyone responsible for that ad makes more money.

Basic Tutorial on Email



president@whitehouse.gov

http://www.whitehouse.gov

rzornetzer@cox.net
bobzorn@gmail.com
bzorno@hotmail.com

Email Tutorial

- What is it?
  - Web based or Email Client
  - IMAP vs POP3
- How it works
  - ISP Server
  - Email Address
    - Domain/Server
  - Send/Retrieve Mail
  - Email Account Setup
- Security
  - Phishing, Pharming, and Spoofs

Email Tutorial (cont)

- Spam
  - How to Recognize
  - What to do
    - Qurb your Spam
- Other
  - On the Road
    - Webmail vs. Outlook
    - Setup for other ISP
  - Backups and Storage on Hard Drive
    - Saving Email Messages
    - Backup Client Files (eg., Outlook)
  - Address Book
    - How it Works
    - How to Save

EMail Client (local)

What is an EMail client?

- Email software that resides on your computer.

Where can I get an EMail client?

- Outlook Express
- Outlook
- Mozilla Thunderbird
- Eudora (Qualcom)
- Opera

EMail Servers

EMail servers exist at:

- Your Internet Service Provider (ISP e.g. Cox)
- Yahoo (Yahoo mail)
- Google (Gmail)
- MSN (Hotmail)

Webmail vs Local Client

- Protocol – Set of rules for computer to talk to each other
  - IMAP Internet Message Access Protocol
    - Mostly used for business groups
  - POP3 Post Office Protocol
    - Supported by most email client software
  - SMTP Simple Mail Transfer Protocol

Webmail vs Local Client (cont)

- Local Clients use POP3
  - POP3 Supports offline email processing (fast)
  - Usually removed from server after download
  - Server is just a waystation for the mail
  - Storage is only limited by your local computer
- Webmail
  - Mail is always on server
  - Can work with any PC connected to internet
  - Speed is limited by your connection
  - Attachments could be missing (AOL)

Local Client (PC World)

Email Software	Basics	Spam Test Results	Performance
Microsoft Outlook	$109 IMAP,POP3 Custom rules/filters, Spell check	Spam Identified 94% False positive .8%	Ease: Very Good Features: Very Good
Mozilla Thunderbird*	Free IMAP, POP3 Custom rules/filters, Spell check	Spam Identified 95% False positive .8%	Ease: Outstanding Features: Very Good
Eudora	Free ($50) IMAP, POP3 Custom rules/filters	Spam Identified 94% False positive .8%	Ease: Very Good Features: Very Good

Webmail (PC World)

Web Based	Basics	Performance	Extras
Google Gmail*	Free - 1 Gb No Ads	Ease: Outstanding Features: Outstanding Spam Filter: Very Good Speed: Very Good	Mail forwarding Accessed from POP3 Accts
MSN Hotmail	Free - 250 Mb $20 - 2 Gb Lots of Ads	Ease: Fair Features: Fair Spam Filter: Good Speed: Fair	Read with Outlook/Express Adjustable spam filter, Calendar, Tasks, Notepad
Yahoo Mail	Free - 250 Mb $20 - 2 Gb Lots of Ads	Ease: Very Good Features: Very Good Spam Filter: Good Speed: Fair	Virus scan, POP3 accts, Mail forwarding, Calendar, Tasks, Notepad
FAST Mail	Free - 10 Mb $20 - 600 Mb	Ease: Very Good Features: Outstanding Spam Filter: Fair Speed: Very Good	Virus scan, Adjustable spam filters, HTML editor, Notepad, Mail forwarding
Cox	100 Mb	Webmail	Tutorial online
AOL (?)			

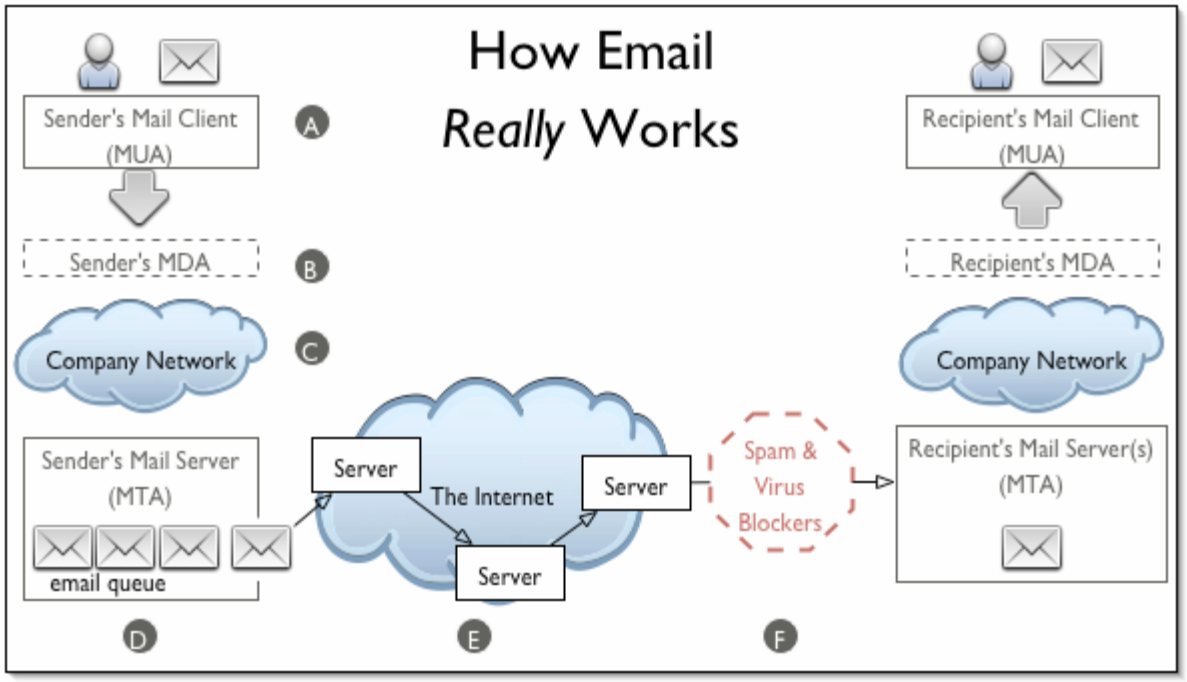
EMail Appearance



Terminology

- MUA - Mail User Agent (client)
- MDA - Mail Delivery Agent
- MTA – Mail Transfer Agent (Server Software)
- DNS – Domain Name Server
- TLD – Top Level Domain (com, net, gov, ...)
- Email Address:
  - username@domain.TLD
- URL Address: (Universal Resource Locator)
  - http://domain.TLD

EMail Actuality



13 Top level domains (.com, .org, .gov…each having its own DNS root server

Email Account Setup

In Outlook or Outlook Express

- Go to Tools Tab
- Select Account
- Click Add/ Mail
- Enter your name (John Smith)
- Enter your email ID (jsmith@cox.net)
- Under Incoming mail server enter:
  - pop.east.cox.net (from cox)
- Under Outgoing mail server enter:
  - smtp.east.cox.net (from cox)
- Under account name type your email ID
- Under password type your password
- Click Finish

Can then go to configure new account

EMail Security

SPAM

Definition:

Unsolicited bulk or junk mail

Obtained by companies that specialize in creating e-mail distribution lists.

Phishing and Pharming

Definition:

An attempt to steal your personal identity data and financial account credentials.

Phishing: through emails

Pharming: through malware infections

Phishing

- Use 'spoofed' e-mails to lead you to counterfeit websites.
- Designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords, social security numbers)
- By hijacking brand names, **Phishers** often convince recipients to respond.

Pharming

- **Crimeware is planted** to steal credentials directly, often using Trojan keylogger spyware.
- **Pharming** crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

Phishing

Report for August 2005

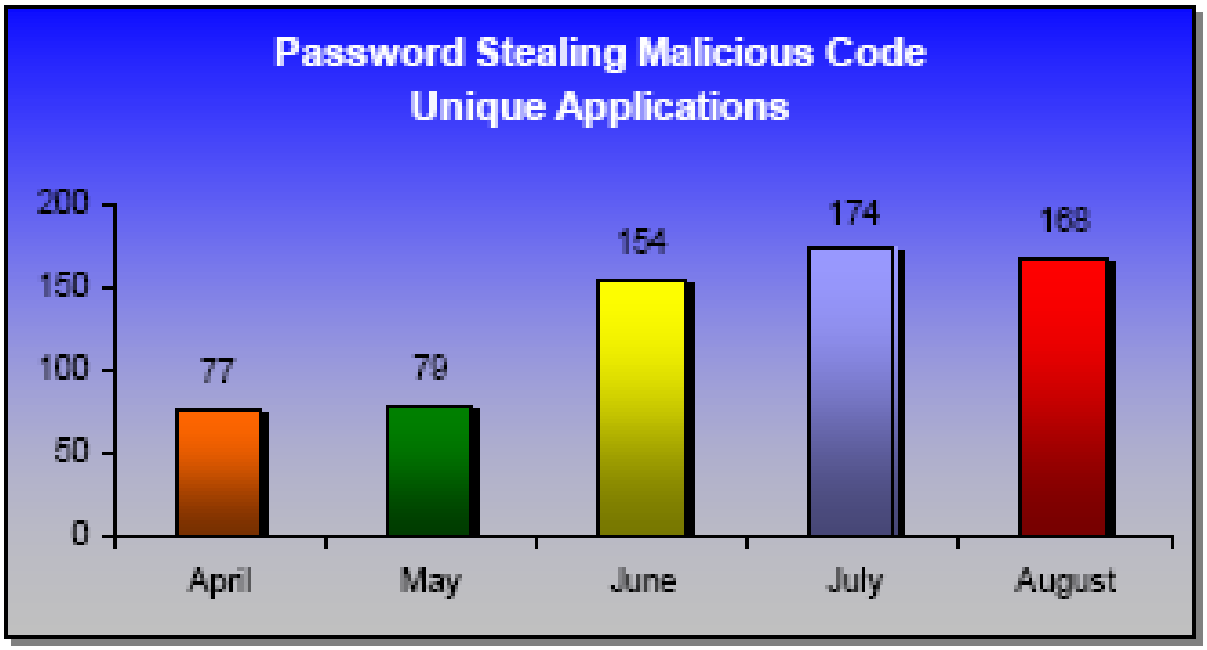
Highlights

- # of unique phishing reports received: **13776**
- # of unique phishing sites received: **5259**
- # of brands hijacked by phishing campaigns: **84**
- # of brands comprising top 80% of phishing campaigns: **3**
- Country hosting the most phishing websites in: **US**
- Contain some form of target name in URL: **49 %**
- No hostname just IP address: **36 %**
- Percentage of sites not using port 80: **6 %**
- Average time online for site: **5.5 days**
- Longest time online for site: **31 days**

Phishing and Pharming

August 2005 – Unique Keyloggers

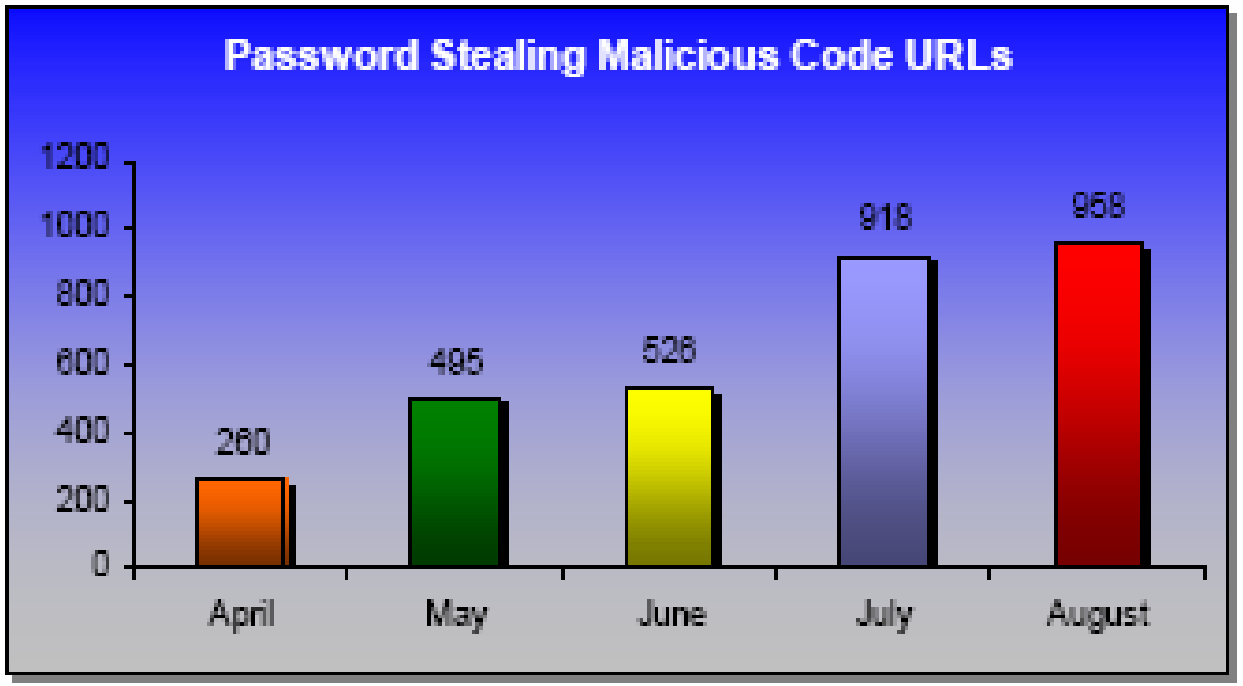
Phishing-based Trojans – Keyloggers, Unique Variants



Phishing and Pharming

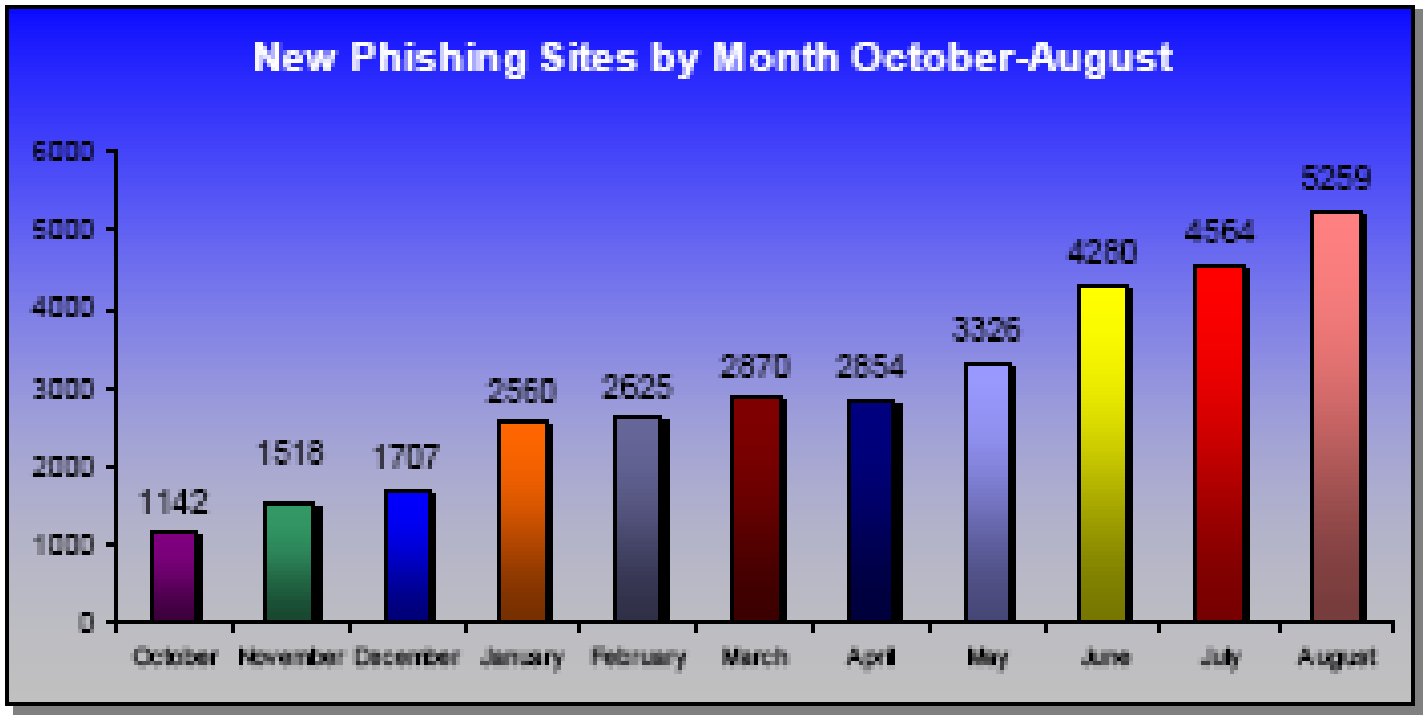
August 2005 – Unique URLs

Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers



Increase in Phishing Sites

It is important to note that the number of unique phishing websites detected by APWG was 5,259 in August 2005, the highest number. This may reflect an increasing tendency for phishers to target a diverse group of smaller brands, and also an increased use of multiple sites to host a single attack, in order to increase their resiliency to takedown efforts.



Phishing and Pharming

Protection Elements

- Be suspicious of emails prompting for account information
- Look for lock symbol on browser to validate secure site
- Look for URL prefix
  https://www.paypal.com
- Sign-on at typed in or bookmarked URLs and check if information is required.
- Report Phishing or Pharming to:
  http://www.antiphishing.org
  and click on 'Report Phishing'
  or **spoof@paypal.com**

Keyboard Shortcuts

- Press CTRL+D to delete the current email message.
- Press CTRL+R to reply to the current email message.
- Press CTRL+F to forward the current email message.
- 5 Tips for Managing your Outlook Mailbox

  http://office.microsoft.com/en-us/assistance/HA010429731033.aspx

Junk Email

To enable Junk Email in Outlook

1. On the **Tools** menu, click **Organize** and then click **Junk E-Mail**.
2. Set options for handling junk mail and/or adult content message and the click **Turn on**. You can now use the following shortcuts to manage your junk email:
   - Press ALT+A,J,J to add the current email message's sender to your Junk Senders List.
   - Press ALT+A,J,A to add the current emial message's sender to you Adult content Senders List.

   Then press CTRL+D to delete current email message.

Manage Incoming Messages
(How to set up rules)

1. On the **Tools** menu, click **Rules Wizard**.
2. Click **New**.
3. Click an action in the upper list.
4. Customize the action in the lower list.
5. Click **Next**.
6. Provide any additional information based on the action that you selected.
7. Click **Finish**.

Outlook/Outlook Express Data Locations

- Outlook Express (dbx files):

  C:\Documents and Settings\owner\Local Settings\ApplicationData\Identities\{F*-*}\Microsoft\OutlookExpress

- Outlook (PST files):

  C:\Documents and Settings\owner\Local Settings\Application Data\Microsoft\Outlook

- Outlook Express Address Book (owner.wab):

  C:\Documents and Settings\owner\Application Data\Microsoft\Address Book

Questions??

