Inside the Mind of a Criminal

October, 2010

Patrick Cain

Research Fellow
APWG
pcain@antiphishing.org

President
The Cooper-Cain Group, Inc.
pcain@coopercain.com
Me

• “Involved” in internet security for ~26 years
  • Gov’t Research & Development
  • Operations support
  • Author, IETF RFC 5901 (helped on 3161 & 5280)

• Checkmarks:
  • CISA (Certified Information Systems Auditor)
  • Ordained by the ‘Street Bishops’ 😊

• Member…
  • Associate, American Bar Association
  • International Association of Privacy Professionals

• I get Around..
  • Member, UNODC Core Group of Experts on Identity-related Crime
The “Big Plan”

- Introduction
- Let’s Think Like a Criminal
- Some Novel Countermeasures
- Conclusion
You may know the APWG…

Password Stealing Malicious Code URLs

- January: 3,362
- February: 4,500
- March: 6,500
- April: 4,080
- May: 3,113
- June: 9,529
- July: 5,680
- August: 11,666
- September: 6,068
- October: 4,775
- November: 11,834
- December: 31,173

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud
Anti-Phishing Working Group

• Launched in 2003
• 3000+ members
  – 1700+ companies and agencies (worldwide)
  – e-Commerce, financial, telecomm, ISP’s, solution vendors, law enforcement, academics, national CERTs, etc.
• Focus: Eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types
Partial List of Members

- Websense
- PassMark
- GeoTrust
- Symantec
- McAfee
- Experian
- MasterCard
- Trend Micro
- WholeSecurity
- RSA Security
- VASCO
- Tricipher
- Entrust
- Visa
- Go Daddy
- MarkMonitor
- 41st Parameter
- Panda Software
- SIGABA
- SAIC
- Tumbleweed Communications
- QUOVA
- Anti-Phishing
- Cloudmark
- DATANAUTICS
- MessageLevel.com
- Anakam
- Affinity
- NameProtect
- VeriSign
- Sophos
- C-M-O-D-O
- SecureBrain
- Anonymizer
- Microsoft
- Corillian
- Aladdin
- Digital Envoy
- aXs Guard

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud
Partial List of Research Partners

- CAIS
- Korea CERT/CC
- APACS
- TRUSTe
- JPCERT/CC
- VTT
- cert.br
- American Bankers Association
- SPARTA
- CERT
- Software Engineering Institute
- Carnegie Mellon
- camara-e.net
- Red IRIS
- Institute for Security Technology Studies
- US-CERT
- MAAWG
- Anti-Phishing Working Group
- APWG
Current APWG Activities

- Repository/UBL
- Blind Contact System
- Semi-annual Gatherings
  - Spring → Operations-focused
  - Fall → Research-focused
- Speaker Bureau

- Working Groups
  - Internet Policy & ICANN
  - Crimeware Future
  - LEA Interactions
  - Data Collection
  - Data Sharing
The Real APWG Mission

Fighting Phishing & Internet Fraud is hard!
1. When someone discovers a novel way to reduce their exposure, they should be able to share their experiences with others
2. There should be a non-threatening way to explain the Internet phraud problems
Phishing Definition

- Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and/or financial account credentials.
The Criminal’s Goals

• Have fun
  – I Love You Worm
  – Be 1337 (Melissa, Slammer)

• Take Your Money
  – Phishing to bank sites → $$

• Grab something of Value
  – Phishing to corporate sites → PII, Sekretz

• Retaliate
  – You called me lame, I DOS you!

• **GET YOU TO RESPOND TO THE LURE**
Subject: National City Alert
Date: Tue, 18 Apr 2006 07:46:38 -0600
From: Support <rusvisa@intourist.ru>
To: <chaba@speakeasy.net>
CC: <cosmos@speakeasy.net>, <billcosby@speakeasy.net>, <acct_service@speakeasy.net>

Dear Customer,

Your current login & password combination are out of date.
To renew please click Reply and get back to us with the following information:
Your Name, Account Number, Login and Password.

Regards,
National City Support
How to Make a Good a Lure?

• Use IMMEDIATELY
• Point out the GRAVE DANGER!!!
  – Be polite and point out bigger danger!!!
• Say “If you don’t do this…. “
  – We’ll keep your money
  – God will punish you
• Use a web address that looks official when viewed quickly
  – http://bankofamerica.h35.com/Login?p=Security
  – Hide behind a link www.irs.gov ➔ http://e.h35.com/~patt
Several VISA Credit Card databases have been LOST!

From: VISA Card Support [VisaService@visa.com]
Sent: Friday, February 03, 2006 4:36 PM
To: domain@coopercain.com
Subject: Attention! Several VISA Credit Card bases have been LOST!

Good afternoon, unfortunately some processings have been cracked by hackers, so a new secure code to protect your data has been introduced by visa.

You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank.

If all transactions are alright, it doesn't mean the card is not lost and cannot be used. Probably, your card issuers have not updated information yet.

That is why we strongly recommend you to visit our web-site and update your profile, otherwise we cannot guarantee stolen money repayment.

Thank you for your attention.

Click here <http://72.36.222.12/lostvisa/index.php> and update your profile.
Some of my Favourite Lures

• An email warning of phishing and asking you to confirm your bank details
• “Chase and McDonald’s FREE Fry Offer!”
• “We’ve accidentally deleted our credit card database. Please re-enter your card data…”
• A malware that scans for 300 bank names through your browser history file; then captures the screen images when you go to them and sends them off via IRC
Victims got smarter, kind of

- Microsoft added filters and more security to Windows
- Users were educated, slightly
- Corporations/Banks started caring about security
  - Security tokens proliferated

- The criminals had to get smarter, too
  - Move away from Microsoft → into the browser
  - Use redirection to hide from the coppers
    - Phish from country A; collector in country B; criminal in country C
  - Get user to install the trojan/malware/etc
## Recent Stats

### Basic Statistics

<table>
<thead>
<tr>
<th></th>
<th>1H2010</th>
<th>2H2009</th>
<th>1H2009</th>
<th>2H2008</th>
<th>1H2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing domain names</td>
<td>28,646</td>
<td>28,775</td>
<td>30,131</td>
<td>30,454</td>
<td>26,678</td>
</tr>
<tr>
<td>Attacks</td>
<td>48,244</td>
<td>126,697</td>
<td>55,698</td>
<td>56,959</td>
<td>47,324</td>
</tr>
<tr>
<td>TLDs used</td>
<td>177</td>
<td>173</td>
<td>171</td>
<td>170</td>
<td>155</td>
</tr>
<tr>
<td>IP-based phish (unique IPs)</td>
<td>2,018</td>
<td>2,031</td>
<td>3,563</td>
<td>2,809</td>
<td>3,389</td>
</tr>
<tr>
<td>Maliciously registered domains</td>
<td>4,755</td>
<td>6,372</td>
<td>4,382</td>
<td>5,591</td>
<td>-</td>
</tr>
<tr>
<td>IDN domains</td>
<td>10</td>
<td>12</td>
<td>13</td>
<td>10</td>
<td>52</td>
</tr>
</tbody>
</table>
More Complex Lure

From: The National City Corporation Online Treasury '08
[customer_department_reference-67kmz@nationalcity.com]
Sent: Friday, January 25, 2008 11:38 AM
To: security@bc.edu
Subject: The National City Bank Treasury Management Customer E-mail: Password Verification

Dear National City Corporation Cash Management customer!

Our Support Subdivision is running a scheduled Treasury Services upgrade. By visiting the link below you will launch the procedure of the customer details approval:

These directives are to be emailed and followed by all Business Treasury Services members of the National City Bank.

National City Bank does apologize for any problems caused, and is very appreciative for your collaboration.

If you are not user of the The National City Bank Cash Management please delete this e-mail!
Social Engineering at its finest…

From: Admin [mailto:admin@southsouthwestern.edu]
Sent: Friday, January 27, 2009 5:38 PM
To: Wheeler, Kay
Subject: Rape on Campus
Attachments: Suspect_picture.jpeg

Hello,
During the early morning of January 25 2009, a campus student was the victim of a horrific sexual assault within college grounds. Eyewitnesses report a tall black man in grey pants running away from the scene. Campus CCTV has caught this man on camera and are looking for ways to identify him. If anyone recognises the attached picture could they inform administration immediately
Regards,
Robert Atkins
Campus Administration

←W32/Brepibot.gen
(Keystroke Logger +Bot backdoor)
Criminals Organised

- The virus, infector, and exploit writers found each other. It was luv at first infection.
  - Most online crime is performed by a few ‘gangs’.
- If users were only going to be fooled once, let’s make it good 😊
  - ‘Pay to infect’ schemes started
  - Buying/Selling of infected machines (botz) arose
- Regulatory arbitrage arrived
  - Put servers in tolerant countries
Top 10 Phishing TLDs*

<table>
<thead>
<tr>
<th>RANK</th>
<th>TLD</th>
<th>TLD Location</th>
<th># Unique Phishing attacks 1H2010</th>
<th>Unique Domain Names used for phishing 1H2010</th>
<th>Domains in registry May 2010</th>
<th>Score: Phish per 10,000 domains 1H2010</th>
<th>Score: Attacks per 10,000 domains 1H2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>th</td>
<td>Thailand</td>
<td>86</td>
<td>62</td>
<td>49,000</td>
<td>12.7</td>
<td>17.6</td>
</tr>
<tr>
<td>2</td>
<td>kr</td>
<td>Korea</td>
<td>2,888</td>
<td>989</td>
<td>1,079,298</td>
<td>9.2</td>
<td>26.8</td>
</tr>
<tr>
<td>3</td>
<td>ie</td>
<td>Ireland</td>
<td>102</td>
<td>79</td>
<td>145,724</td>
<td>5.4</td>
<td>7.0</td>
</tr>
<tr>
<td>4</td>
<td>pl</td>
<td>Poland</td>
<td>1,582</td>
<td>744</td>
<td>1,805,894</td>
<td>4.1</td>
<td>8.8</td>
</tr>
<tr>
<td>5</td>
<td>cl</td>
<td>Chile</td>
<td>159</td>
<td>111</td>
<td>282,526</td>
<td>3.9</td>
<td>5.6</td>
</tr>
<tr>
<td>6</td>
<td>my</td>
<td>Malaysia</td>
<td>61</td>
<td>39</td>
<td>99,736</td>
<td>3.9</td>
<td>6.1</td>
</tr>
<tr>
<td>7</td>
<td>gr</td>
<td>Greece</td>
<td>130</td>
<td>93</td>
<td>260,000</td>
<td>3.6</td>
<td>5.0</td>
</tr>
<tr>
<td>8</td>
<td>ro</td>
<td>Romania</td>
<td>324</td>
<td>156</td>
<td>443,700</td>
<td>3.5</td>
<td>7.3</td>
</tr>
<tr>
<td>9</td>
<td>vn</td>
<td>Vietnam</td>
<td>64</td>
<td>48</td>
<td>153,002</td>
<td>3.1</td>
<td>4.2</td>
</tr>
<tr>
<td>10</td>
<td>cz</td>
<td>Czech Republic</td>
<td>480</td>
<td>207</td>
<td>689,813</td>
<td>3.0</td>
<td>7.0</td>
</tr>
</tbody>
</table>
New Lure Enhancements

• Now, the lure is used to drop all types of crime-ware onto a computer
  – Keystroke loggers, virii, etc
  – Very sophisticated crime-ware
• Hit many banks with one click!
• A victim that ‘clicks’ on a picture may get a keystroke logger for *your* secrets.
• Malicious Ads get you to click
  – Fake AV
  – “Required Flash Player Upgrade”
  – “You need a new codes to watch this video”
The Rise of ‘bots’

- **Internet bot**, computer program which does automated tasks
- **Botnet**, network of "zombie" computers used to carry out automated tasks such as spamming
- Good* bots – Windows update, IM
- Bad* bots – Zeus, Hiloti, Avalanche, (java updater)

If you’re “botted”, someone else controls your system (and your data)
# Zeus

**Available commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot</td>
<td>Reboot computer.</td>
</tr>
<tr>
<td>kos</td>
<td>Kill OS.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown computer.</td>
</tr>
<tr>
<td>bc_add [service] [ip] [port]</td>
<td>Add backconnect for [service] using server with address [ip]:[port].</td>
</tr>
<tr>
<td>bc_del [service] [ip] [port]</td>
<td>Remove backconnect for [service] (mask is allowed) that use connection to [ip]:[port] (mask is allowed).</td>
</tr>
<tr>
<td>block_url [url]</td>
<td>Disable access to [url] (mask is allowed).</td>
</tr>
<tr>
<td>unblock_url [url]</td>
<td>Enable access to [url] (mask is allowed).</td>
</tr>
<tr>
<td>block_fake [url]</td>
<td>Disable executing of HTTP-fake/inject with mask [url] (mask is allowed).</td>
</tr>
<tr>
<td>unblock_fake [url]</td>
<td>Enable executing of HTTP-fake/inject with mask [url] (mask is allowed).</td>
</tr>
<tr>
<td>rexec [url] [args]</td>
<td>Download and execute the file [url] with the arguments [args] (optional).</td>
</tr>
<tr>
<td>lexeci [url] [args]</td>
<td>Download and execute the file [url] with the arguments [args] (optional) using interactive user.</td>
</tr>
<tr>
<td>lexec [file] [args]</td>
<td>Execute the local file [file] with the arguments [args] (optional).</td>
</tr>
<tr>
<td>lexeci [file] [args]</td>
<td>Execute the local file [file] with the arguments [args] (optional) using interactive user.</td>
</tr>
<tr>
<td>delsf [file_mask...]</td>
<td>Remove file masks [file_mask] from local search.</td>
</tr>
<tr>
<td>getfile [path]</td>
<td>Upload file or folder [path] to server.</td>
</tr>
<tr>
<td>getcerts</td>
<td>Upload certificates from all stores to server.</td>
</tr>
<tr>
<td>resetgrab</td>
<td>Upload to server the information from the protected storage, cookies, etc.</td>
</tr>
<tr>
<td>upcfg [url]</td>
<td>Update configuration file from url [url] (optional, by default used standard url)</td>
</tr>
<tr>
<td>rename_bot [name]</td>
<td>Rename bot to [name].</td>
</tr>
<tr>
<td>getmff</td>
<td>Upload Macromedia Flash files to server.</td>
</tr>
<tr>
<td>delmff</td>
<td>Remove Macromedia Flash files.</td>
</tr>
</tbody>
</table>
2. Setting up the server.
   2.1. HTTP-server.
   2.2. The interpreter PHP.
   2.3. MySQL-server.
   2.4. Control Panel.
      2.4.1. Installation.
      2.4.2. Update.
      2.4.3. File / system / fsarc.php.

4. Working with BackConnect.
5. Changelog.
6. F.A.Q.
7. Myths.

====================================
1. Description and features. =
====================================
ZeuS - software to steal personal user data from remote systems, Windows. On
plain language of "trojan", "backdoor", "virus". But the author does not like these words, therefore, further documentation
He will call this software "Bot".

Bot is fully based on the WinAPI Interception in UserMode (Ring3), this means that the bot does not use
drivers or treatments in Ring0. This feature makes it possible to run even on
Guest Account. Plus, it ensures greater stability and adaptability
on next versions of Windows.

Bot is written in Visual C ++ version 9.0 +, with no additional libraries are used
(no msvcr70.dll, ATL, MFC, QT, etc. used). Code is written with the following priorities (in descending order):
   1. stability (carefully checked all the results of the call functions, etc.)
   2. size (to avoid duplication of algorithms, repetitive calls, functions, etc.)
   3. speed (not the type of instruction while {1*i++; for (int i = 0; i < strlen (str); i++)}

Functions and features bot:
   1. Sniffer traffic for the protocol TCP.
      1.1. Interception of FTP logins on any port.
      1.2. Interception of POP3 logins on any port.
      1.3. The interception of any data from the traffic (a personal request).

2. Intercepting HTTP / HTTPS requests to wininet.dll, ie all programs working with this
   library. This includes Internet Explorer (any version), Maxton, etc.
   2.1. Substitution ..

3. The functions of the server.
   3.1 Socks4/5.
   3.2 Backconnect for any services (RDP, Socks, FTP, etc.) on the infected machine. You can
      access to a computer that is behind a NAT, or, for example, that
      banned from the internet connection.
   3.3 Getting a screenshot of your screen in real time.
Number of ‘Active’ Botz

From shadowserver.org
From shadowserver.org:
Current Oddity/Status/Etc
New Types of Lures

- Email lure with “call this phone number”
  - Phone tree recorded directly from bank
  - Compromised Asterisk (VoIP PBX) that relays to odd countries
- Cold-call to home phone number
- Targeted with info from corporate filings
URL Shorteners

URL Shortener Phish
1H2009 - 1H2010

Domain % of URL Shortener Phish
1H 2010

- tinyurl.com: 50.3%
- Other (53): 24.0%
- dickensurl.com: 2.4%
- su.ly: 2.6%
- path.to: 2.8%
- bit.ly: 3.0%
- doiop.com: 4.5%
- snipurl.com: 5.1%
- twurl.nl: 5.3%

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud
Technology isn’t the Panacea

• This *is* social engineering
  – Many users will not like you putting stuff on their computer (bank SW, proxies, AV, etc)
  – Some % of victims will never learn
  – The phishers react to new technology
    • See “2-factor authentication”
Multi-Something or Other Factors

Screen scraper used against Brazilian Bank

Lesson: Thinking Three Generations Ahead in Attack Scenarios Imperative
Keylogger Output

Online Computer Library Center, "
Winword.exe, 4:07 PM
Outlook.exe, 4:12 PM
Untitled - Message (HTML)
Mary,
I noticed that the footnotes are not all correct; I have already corrected them in Excel. Please paste them in when I do the exhibits. Thought it best to send this right over to you.

Ocal.exe, 4:14 PM
Sign-In

[PASSWORD CAPTURED: oo]
[PASSWORD CAPTURED: oat]

Wednesdays

Recommendation: delete records for previous dates

Click an image to enlarge.

Screenshot made at 12:18:40 PM

Screenshot made at 12:46:53 PM
The Use of Mules

- The criminals convince others to do their work
  - Criminals can hide
  - Money can be laundered with less detection

- Note that *you* are performing the crime 😞
- The number of people doing this is staggering
I know how many people are fooled into believing they can make ridiculous amounts of money from home, but get nothing more than crushed hope.

What you really need is something safe, secure and proven to work.

Finally, a real work from home job that can be done anywhere you have the internet and you'll be doing work for very large companies who need your help from home.

And I know the sound of the word job scares some people but it's a great opportunity for anyone who wants to work from home and take control of their financial situation.

The only catch is that positions are limited so you need to move on this and apply here: http://gjlo.usselsumload.com/3548bc66a8cb6475312411944dad570639590b

Kelly Andrews

P.S. - Grab your home job now before it's too late. If you don't take advantage of this now you'll hate yourself later.
2010 Trends

• Phishing isn’t only Banks !!!!
  – Big stores’ debit cards
  – Internet Registrars
  – Corporate VPN accounts
  – (Online gambling, porn sites)

• Muling grew up

• *Very* targeted lures

• Criminals think they get one shot at you:
  – Install everything you can!
Odd Trends

• A *large* number of cold calls via phone
• SMS Text message lures are growing quickly
• From the good economy: resume grabbers
  – “Send me your resume with ALL details…”
• Social network sites are getting into the game
• Phishing lures give you ‘presents’, too 😊
  • Malware, keyloggers, etc
• Most viruses are not new
More disturbing news

- The media sees blood, err, a story!
  - Every bump is a media event
- We tell users that a virus/infection is bad
  - Scan WSJ, NYT, Herald for the poor sucker stories
- When a user visit some web pages, they get the little “you’re infected” message. “Click here to save your machine!”
  - The download is a virus + keystroke logger.
  - Welcome to scareware.
- Phishers use our countermeasures against us
Better news

- The amount of crime is causing hesitant people to share data
  - Data correlation works wonders!
  - It looks like most fraud crime comes from a small set of people

- Many countries are now paying attention
  - Regulatory arbitrage is receding
Stop. Think. Connect.

• How to protect yourself?
  – Keep machine patched
  – Run an anti-virus (even a free one)
  – Back-up the system regularly
    • If it gets infected → re-image and restore the backup
  – Don‘t believe links
    • If you don’t know the sender, ignore them. They’ll come back.
  – Sensitive transactions should be done on a restricted system
    • Use a dedicated system for those that process attachments.
I sent ALL MY MONEY to NIGERIA
...and all I got was this sticker
Thank You

Pat Cain

pcain@antiphishing.org