Crimeware Threats

Peter Cassidy
Secretary General
www.antiphishing.org
pcassidy@antiphishing.org
Director of Research – TriArche Research Group
www.triarche.com
pcassidy@triarche.com
ID Theft Top US Consumer Complaint

- ID Theft is the top consumer complaint to the US Federal Trade Commission (FTC) for the last 9 years.
- Between January and December 2008, FTC received over 1,223,370 ID theft and fraud complaints.
- Consumers reported losses from fraud of more than $1 billion.
- Through its online complaint form and toll-free hotline, the Commission receives approximately 15,000 to 20,000 contacts each week on ID theft.
Fraud and ID Theft on the Rise

Reports to FTC in 2008
Fraud: 643,000
ID Theft: 314,000
Other: 266,000

Media Used for Fraud
Email: 52%
Website: 11%
Telephone: 7%

Source: Federal Trade Commission
Identity Theft Schemes

- Credit card fraud: 20%
- Gov’t Documents/Benefits fraud: 15%
- Employment fraud: 15%
- Telephone or utilities bill fraud: 13%
- Bank fraud: 11%
- Load fraud: 4%
“Classic” Social Engineering Attack Still Predominant

- Majority of phishing attacks against consumers based on classic social engineering scheme:
  - A ‘call-to-action’ e-mail compelling a consumer to visit a counterfeit Web site.
  - There he or she is tricked into giving his personal financial data and credentials for some reason:
    - Your account needs to be reauthorized
    - There has been suspicious activity on your account
    - The company needs to update your accounts
    - There’s a special opportunity or offer for you
    - A charity needs your help right now
Trend: Conventional Phishing Campaign Numbers Relatively Flat

Phisher’s focus on targeted phishing campaigns against executives and personnel with access to intellectual property, commercial bank accounts and other high-value resources may explain some of the reduction in conventional phishing attacks against consumers near the end of 2008.
Trend: Emphasis on Campaign Durability
By Using Multiple Phishing Websites


FastFlux: Rapid changing of IP address associated with a domain changing every few minutes to frustrate take-down attempts. Often IP addresses resolve to proxies to redirect consumers to one of a large number of phishing sites
Most innovation in crimeware is invested in survivability, assuring that crimeware will not be detected or neutralized by anti-virus or anti-spyware systems. Brazil CERT reports: The best detection rate for AV software in 2005 was 88% - decreasing to 79% in 2007. Crimeware invisibility shields increasingly frustrate anti-virus technology.
Trend: Emphasis on Increasing Websites to Spread Crimeware

Emphasis by electronic crime gangs is increasingly on driving traffic to sites that have been prepared to infect PCs with crimeware or precursor code designed to download crimeware and complete felonious tasks.
Crimeware Genres

- Infrastructure development:
  - Commandeer resources for spam and phishing attacks
  - Provision survivability strategies
    - Fastflux

- Data theft: Server takeover for archival data theft

- Desktop attacks: Mostly to retrieve personal information such as user name and passwords for online enterprise and campus resources and personal financial resources like bank accounts
Desktop Crimeware Genres

- Host file overwrite: ‘pharming’
- Session hijackers: allows external party to launch session after authentic user login
- Man-in-the-middle attacks: reports from field successful against two-factor ID systems
  - Demo’ed in Chicago 2006 APWG Meeting
- Keyloggers: overwhelming choice of phishers, simple and effective
  - Variations such screen imaging developed to thwart counter-phishing technologies such as point-and-click login systems
Crimeware Delivery

- Emails with attachments bearing crimeware payloads to infect PCs and intercept credential data
- Rogue software – widgets, helpers, utilities that come backpacked with crimeware
- CD-ROMs and USB sticks mailed directly to targeted employees, also with crimeware payloads to infect PCs and intercept credential data
- Website will be programmed to infect computer directly or provoke a download to the user’s PC
End Game: Full Automation

- Majority of crimeware reported to APWG has been developed to intercept the consumer or student’s user name and password
- After 2004 or so, APWG saw reports of automated trojan systems
- Completely automated phishing is at hand now with all the components required reported in the field
Automated Account Theft

- Secretly perform transactions after you log in

Win32.Grams waits for a user to log into an e-Gold account, then creates a hidden browser session in the background which uses OLE automation to transfer the money from their account directly to another e-Gold account.

<table>
<thead>
<tr>
<th>Time (GMT)</th>
<th>Type</th>
<th>Batch</th>
<th>e-metal</th>
<th>Weight (troy oz.)</th>
<th>To/From Account</th>
<th>Entered Amount</th>
<th>Rate per oz.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1/05 12:33</td>
<td>Storage Fee</td>
<td>42444122</td>
<td>Gold</td>
<td>-0.000901</td>
<td></td>
<td>0.00 USD</td>
<td>434.90</td>
</tr>
<tr>
<td>3/2/05 06:40</td>
<td>Payment Received</td>
<td>42464379</td>
<td>Gold</td>
<td>+0.463177</td>
<td>156460</td>
<td>200.00 USD</td>
<td>431.80</td>
</tr>
</tbody>
</table>
Trend: Targeting Key Employees with Access to Competitive Data & Treasury

- Phishers targeting executives inside commercial enterprises, government agencies and laboratories
- Send phish mails to limited number of executives and key employees to phish data or infect their PCs with crimeware
- Corporate treasury increasingly the target of these phishing attacks - up to the CFO level
- Valuable competitive data are targeted goods that could be sold on the black market as ‘insider information’ and competitive intelligence
Measuring the Total Threat Potential of ID Theft and eCrime
Scope of Threat

- Phishing scams started with ‘white plastic’ card schemes using phished data for small-scale, high-volume thefts against ATM cards.
- But phishing and other eCrime is being used to inflict much larger and more important individual and corporate losses today.
- Tomorrow some forms of phishing could even substantially distort investment markets, injuring many investors and stock-held companies.
Individual Consumer Threat

- Credit Accounts (Credit Cards)
- Savings and Checking Accounts (ATM Cards)
- Retirement Accounts (Brokerage accounts and Mutual Funds)
- Property
  - Real Estate
    - Increasing numbers of cases in US and Canada of mortgage frauds, based on ID theft
      - Discharge existing mortgage (if there is one on the house)
      - Apply on line for a new one
      - Go to closing and walk away

- Next?
  - Loans against more real assets of persons and businesses:
    - Boats
    - Planes
    - Private Businesses
      » Business Assets and Property
Enterprise Threat

- Corporate treasury accounts are under attack
  - Increasing reports of focused phishing attacks on treasurers, CFOs and accounts managers
    - ‘Reverse phishing’ attacks
      - Phishers spoof IDs of companies and send trading partners notice of changes to bank account numbers
      - Company pays invoices – and funds end up in accounts controlled by phishers
    - Keylogging attacks on corporate treasury accounts
      - Credentials intercepted by keylogger and sent to criminals
      - Funds transferred out by ACH or international wire transfers, often through a number of accounts controlled by phishers or the mules they employ
  - Conventional Phishing Attack: North Kentucky Chamber of Commerce
    - $160,000 in losses in 2006
- Smoldering issue: conclusively determining insider collusion in a corporate phishing attack – and measuring the risk of that uncertainty
Enterprise Threat – Customer/Student Data

- Customer Data and Data Assets in Company’s Care are Prime Targets
  - Monster.com – Employer/jobs advertisers were phished for credentials to gain access to the resume database to fuel targeted phishing attacks against job seekers
  - Salesforce – Salesforce’s own employee’s credentials phished. Phishers went through customers client lists to drive targeted phishing attacks

- In both cases the data was valuable for creating much more focused and convincing phishing attacks
Enterprise Threat – IP and Customer Data

Intellectual property
- Phishing is now being used as a corporate espionage tool
  - APWG has taken reports about manufacturers being phished (email and crimeware) specifically to mine data about products in development
- Customer and student data is now currency and targeted at the enterprise level at the same intensity as consumer PII and financial data at the desktop level
Special Challenges for eCampus

Click-a-holics

– Studies show youngsters more likely to click first and think later
– A subset of this population will click on any link they see, maliciousness notwithstanding
– Infection local and likely designed to quickly propagate through campus networks
– Crimeware takes advantage of the first opportunity to propagate
Special Challenges for eCampus

Perpetual network scans from criminal organizations looking for vulnerable servers

– Mostly looking for servers to send spam/phish or to break into, looking for good data
– Relative openness and richness of computing resources makes the eCampus an attractive target for sourcing criminal enterprise
Special Challenges for eCampus

Compromised (mostly) student email accounts which are used to send spam via the campus email servers
Special Challenges for eCampus

'Losing' credit card or personal data due to staff lack of awareness

Universities have a laundry list of regs they have to follow regarding data management

Many people have sensitive data on their laptops, servers, PDAs, etc.

- Just *finding* the data, let alone getting owners to secure it, is a challenge.
Conclusions

- Crimeware is a permanent player in the online threatscape and growing in technical sophistication
- Technology has its place in securing users
- Education and awareness as important or more important in many instances
- Find and exploit teachable moments
APWG/CMU Phishing Education Landing Page

The landing pages instruct consumers on online safety at the “most teachable moment”: when they have just clicked on a link in a phishing communication

ISPs replace phish site content with an auto-redirect that brings the consumer to the education page. The system parses language and browser and delivers an appropriate version of the page to the user.
The Illustrated Page

WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank and is asking me to update my information. I better click on the link and update it.

STOP! Don’t fall for scam email.

My Inbox

From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.

How to Help Protect Yourself

1. Don’t trust links in an email.

2. Never give out personal information upon email request.
   [DANGER] Name: Jane Smith
   Credit Card: 1234 5678 9101 1213

3. Look carefully at the web address.
   [http://www.amazon.com]

4. Type in the real website address into a web browser.

5. Don’t call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

6. Don’t open unexpected email attachments or instant message unload links.

CarnegieMellon CyLab
Supporting Trust Decisions Project
http://cups.cs.cmu.edu/trust
Warning!

The web page you tried to visit might have been trying to steal your personal information. The link you clicked to get here was probably created by con artists.

That page was removed after being identified as a "phishing" web page. A phishing web page is created to trick people out of bank account information, passwords and other confidential information.

Help Protect Yourself from Identity Theft

- Don't trust 'urgent' demands for personal information such as passwords in email or in instant messages.
  > STOP. Think. Avoid being rushed into giving up secrets or personal information you will later regret giving away.
- Don't trust links in email or in instant messages. They can lead to viruses and infect your computer.
  > MANUALLY TYPE the URLs for websites you need to visit, or use bookmarks you have created.
- Don't trust company telephone numbers in email or in instant messages.
  > LOOK UP telephone numbers using an established source. Use a telephone directory, a paper account statement or the telephone numbers on the back of your ATM cards and credit cards.
- Don't trust unexpected email attachments or instant message download links.
  > SCAN all attachments for viruses even in expected emails from friends and colleagues.

Legal Disclaimer

- PLEASE NOTE: The APWG, CNU's Supporting Trust Decisions Project and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phishing or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid phishing attacks. For more information, please visit the APWG website at http://www.apwg.org. All rights reserved.

Committed to wiping out Internet scams and fraud
Working Specification

- Had to be nearly as nearly work-free as possible for ISPs to co-operate
- Had to work for all devices – handhelds as well as laptops and PCs
  - In many countries, online banking is mediated on a cell phone or handheld
- Had to work for all languages automatically
Working System

- PHP scheme
- ISP redirects users who’ve clicked on links to decommissioned websites to [http://education.apwg.org/r](http://education.apwg.org/r)
- PHP system reads Web access logs
  - Parses browser language setting
  - Parses browser type – indicating device
- PHP reaches into database and serves up version for user requirements
Final design

- Cartoon format designed with horizontal text in rectangular boxes so that text can all be HTML
- Suggests something for would-be victims to do (tell their friends)
- Only one link for more info, short URL spelled out in text
- Explain what APWG is at top
- Define phishing on first use
- Reduced number of instructions (omitted virus checking and patching)
Thank You

- Peter Cassidy
- pcassidy@antiphishing.org
- +1 617 669 1123