The State of Internet Phishing and Fraud and Useful Means to Combat It

Foy Shiver
Deputy Secretary-General
APWG

Agenda

- Some Apwg Background
- Phishing/Fraud is Evolving
- Reaction Strategies

APWG Institutional Profile

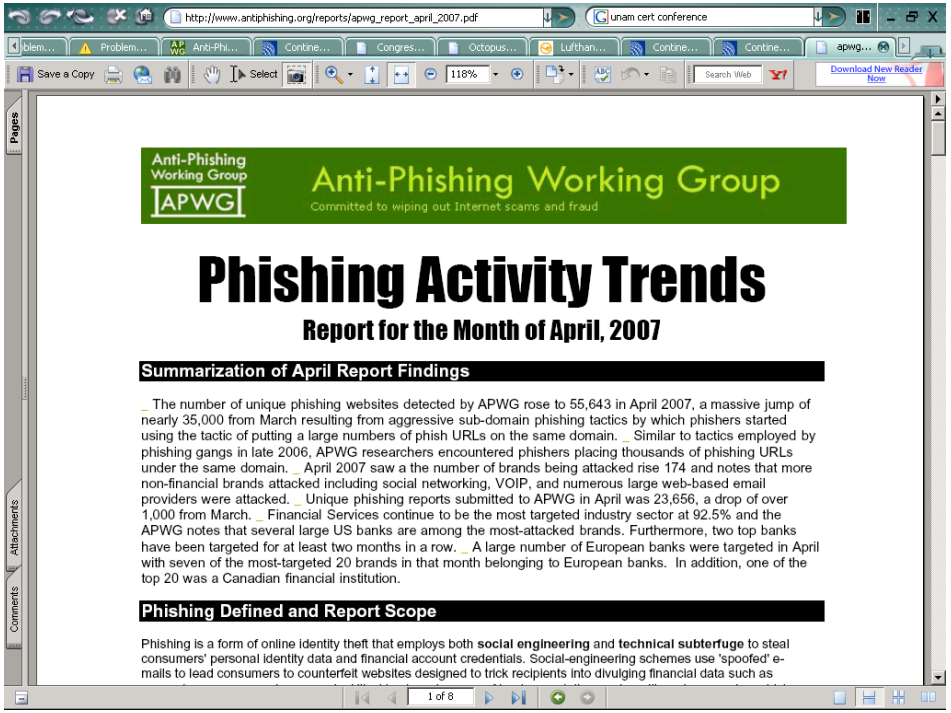
- **Founded October 2003**
  - Independently incorporated, 501c6 tax exempted association, directed by its directors, executives, steering committee, members and correspondent research partners
- **Mission**: Provide resources for information and solutions for eliminating the fraud, identity theft and electronic crime that result from phishing, pharming and email spoofing of all types
    - Initially focused on phishing, broadening focal length to include phraud and ecrime
    - Clearinghouse of ecrime data being developed on modified biomedical research model – open access; governed usage through user agreements

APWG Institutional Profile

- 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

Institutional Roles: Statistician

- APWG Phishing Activity Trends reports delineate the phishing experience, enumerating phishing's growth and characterizing phishing's evolution to inform stakeholder dialog
  - Monthly reports cover social engineering phishing attacks and crimeware threats
    - Developing: report segment on electronic crime infrastructure



Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends

Report for the Month of April, 2007

Summarization of April Report Findings

_ The number of unique phishing websites detected by APWG rose to 55,643 in April 2007, a massive jump of nearly 35,000 from March resulting from aggressive sub-domain phishing tactics by which phishers started using the tactic of putting a large numbers of phish URLs on the same domain. _ Similar to tactics employed by phishing gangs in late 2006, APWG researchers encountered phishers placing thousands of phishing URLs under the same domain. _ April 2007 saw a the number of brands being attacked rise 174 and notes that more non-financial brands attacked including social networking, VOIP, and numerous large web-based email providers were attacked. _ Unique phishing reports submitted to APWG in April was 23,656, a drop of over 1,000 from March. _ Financial Services continue to be the most targeted industry sector at 92.5% and the APWG notes that several large US banks are among the most-attacked brands. Furthermore, two top banks have been targeted for at least two months in a row. _ A large number of European banks were targeted in April with seven of the most-targeted 20 brands in that month belonging to European banks. In addition, one of the top 20 was a Canadian financial institution.

Phishing Defined and Report Scope

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as

Institutional Roles: Advisor

APWG has contributed data to the OCC, FDIC, European Commission, ITU, Congressional committees, ICANN, law enforcement agencies, government agencies and law courts worldwide

Institutional Roles: Mustering Point

- Association where stakeholders meet and pull together projects of stakeholder benefit
  - Data and technology projects draw contributions from industry, academe, law enforcement and standards-making communities
  - ICANN Policy Project
  - Abuse Manager Contact Federation Project Under Way
- Three Established Conferences

APWG MEMBER
www.antiphishing.org

Annual General Members Meeting

e-Crime Researchers Summit
APWG

eCRS for academic and industrial research into eCrime

APWG
ANTIPHISHING JAPAN
フィッシング対策協議会

CeCOS II 東京
Counter eCrime Operations Summit II
Tokyo, Japan - May 26 & 27, 2008

CeCOS for responders to eCrime events & managers of end-users' security

The Evolution of Phishing

Phishing Definition

•Old Version:
Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and/or financial account credentials.

•Updated Version:
Phishing attacks use both social engineering and technical subterfuge to steal personal identity data and/or system login credentials

Early Phishing Examples

- Started as ‘phishing’ for AOL screen names and passwords ~1995
- Initially performed via an email lure to social engineer user passwords
  - Send simple email to trick users into revealing account password.
- Picked up by criminals as internet banking flourished
  - Gather bank account, credit card, or corporate info

Evolution begins..

- HTML mail makes an entry
  - MS Outlook displays ‘pretty’ HTML
  - Many victims use Web-mail reader
  - Criminals say “<a ref=‘bad_URL’>” is your friend
- As FIs added more authentication features the criminals added more tricks
  - Use regulatory arbitrage for drops
  - Send victim to a web page
    - Easy to duplicate bank logos, etc
    - Use *-script to grab other stuff or make victim act
    - Craft authentication-specific lures

Further 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
- Many banks with one click!
  - A victim that 'clicks' on a picture may get a keystroke logger for *your* secrets.
- Note: Unlike conventional attacks the targeted institution may not even know the phishing is happening. ☹

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**

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

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 administraion immediatly
Regards,
Robert Atkins
Campus Administration

Social Engineering at its finest…

- FTC / IRS / US Court Phish
  - hoax e-mail is personalized, and contains the name of the recipient and their business
  - Attached you will find a copy of your complaint
  - You are due additional refund
  - Must appear in court
  - Detach this file and print . . .
  - Malware is installed

It's not only URLs; 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
- Vishing / Smishing

The Collection Sites Evolve, too

- Originally, most collectors were on a free-web hosting sites
  - Most fee web-hosters are responsive. Now.
  - We all play whack-a-mole
- Let's pwn (own) home computers since no one will ever know… or patch…. or …
  - Most phish collectors are now on compromised DSL/home/office computers
- The phishers thought "Can we make more moles than the good guys can whack?" ☺

The Collection Sites Evolve, too

- Fast-Flux
  - DNS uses nameservers to perform the DNS Name to real IP Address mapping
    - Every domain has at least one nameserver
      - "whois bank.com"
    - A query for host.bank.com asks those domain servers

      host.bank.com = 172.16.3.156
- An easy way to disable a collector is to:
  - remove its DNS entry in the domain nameserver
  - filter/block collector traffic to the nameserver
- Disablement becomes harder if I have ~50 nameservers and the nameservers change every few seconds
- … Welcome to fast-flux ☹

The Collection Sites Evolve, too

- Faster-Flux
  - We have seen a phish domain with over 1,000 nameservers, changing the primary server every 2 seconds
  - Most of the nameservers were on compromised home boxes
  - There have been two-level nameservers where both levels used fast-flux
- The Roc Phish
  - One kit – w/GUI – to infect, setup, launch
    - No skills required, whatsoever
  - Multiple collectors (as in 100) on one server
  - Very unique URLs used in lure and collector (they all have an 'r' in them)
  - Very easy to use, and script

Emerging Threats

- More targeted attacks at organization executives
- New tools for compromising users
  - e.g. Google calendar
  - Employment seeking sites used to gather user credentials (mule recruitment)
  - More VOIP attacks
- One large UK Company had a situation where the Chairman of the Board, a rather well known and public figure in the UK, was attacked in person by using faked 'social' networking sites profiles

Emerging Threats

- Another company had a busy two weeks of extensive meetings
  - Hardware was secured and locked in a room while they went to after meeting events
  - Machine was lifted, room was still secured when they returned
  - Executives were subjected to a number of well written and crafted communications, appearing to be fenuine, from both inter-company addresses (spoofed mails), as well as individuals purporting to have connections with the company, other workers, or employees.
- Blackmail / Ransomware
  - Virus encrypts hard drive
  - Send compromising information to family or co-workers

Emerging Threats

- Phishing and other such targeted attacks are no longer just based on chance internet finds or internet based targeting
- Often, especially where targets are high profile and valuable there is a present danger that such a phishing exercise will be multi-faceted to gain the end prize
- Thus, security must be interlinked end-to-end
- Personnel, physical security through to awareness on on-line threats

APWG Strategic Contributions to Counter-eCrime Efforts

Toward an eCrime Report Lingua Franca

- Industry research concluded there is no good way to electronically report fraud activities
  - No common format
  - Good reports need complete data sets
  - Reports need to support automatic processing
- Define a common report format
  - Started with phishing; added spam-mediated phraud and crimeware
- Goals
  - Make it easy to spot and report novel events & trends
  - Let vendors & researchers test their ideas/products against known attacks
  - Be vendor and application agnostic
- Approach: Try not to reinvent another format
  - Pick something acceptable to CERTs, ISPs, law enforcement and bank teams
- IETF Incident Object Description and Exchange Format (IODEF) XML schema (with eCrime-relevant extensions)
  - Flexible (simple through detailed)
  - Easy to read
  - Standard-brand XML, immediately useable

IODEF Extensions X*ML Schema*

- APWG proffers: **Extensions to the IODEF-Document Class for Phishing, Fraud, and Other Crimeware**
  - Structured data model allows forensic searches and investigations to be automated/scripted with greater ease using standard schema
    - Multiple language capability
    - Reports readable in any XML-capable browser
    - Multiple parties – brandholders; security professionals, CERT personnel and LE - can add to a report
    - Extensions specifically designed for electronic crime incidents and crimeware
      - Purpose built nature gives it unique relevance

IODEF Extensions RFC at the Moment

- APWG working within the IETF to make this XML schema an IETF standard for ecrime reporting
  - Base specification for IODEF passed
  - APWG has refilled its RFC for the IODEF-extensions
  - Expected to leave committee and be adopted Summer '08
- Asian, European and Australian companies, trade associations and CERTs (some already using IODEF) are already reviewing and/or adopting the format

- Pat Cain, IETF committeeman and APWG Senior Research Fellow
  pcain@antiphishing.org
  http://www.coopercain.com/incidents/index.htm

APWG eCrime Repository

APWG eCrime Data Repository & Block List

- **Collecting phishing data since October 2003**
  - 2,550,000-plus records archived thus far
    - 14,000-plus unique URLs added every month
- **Currently two principal Repository resources**
  - Historical archive
  - Block list updated every 5 minutes
    - Contains URLs from previous three days' reports
    - Generally, about a 10 megabyte file
    - Each URL has a 'confidence level' of certainty of its authenticity
    - Multiple uses in counter-ecrime technologies and forensics
      - Integrated browser anti-phishing systems
      - Standalone toolbars
      - Industrial research and development
      - University research
      - eCrime forensic analyses

Repository & Block List

- Repository and Block List Users
  - 129 agencies, companies and associations taking outbound feed
  - 60 agencies and companies making inbound contributions
  - A number of university researchers examining the full repository for research purposes
- Repository and Block List Sources
  - Brand holders send confirmed URLs directly to the Repository
  - APWG member security and take-down companies send confirmed URLs directly to the Repository
  - Reportphishing@antiphishing.org - unconfirmed reports to APWG for processing
    - Automated parsing pulls out relevant data and places it in Block list
  - Volunteer organizations (PIRT and PhishTank)
  - Research partners
- Why It's Working and Will Continue to Grow
  - Clearinghouse model operates similarly to the genomic databases used by life sciences researchers in the US and Europe
  - Assurance that the full resource available will be provided
  - User agreement that assigns no new liability
    - Role of NDAs, User Agreements often underappreciated in technical community
- New contributing companies, groups and associations coming online regularly

APWG Contact System for Abuse Managers

- Allows companies who need to communicate about a phishing attack (typically ISPs and victimized brandholders) to find each other without exposing a large database
- In Beta mode with-in the APWG Membership
  - Cleaning up enrollments now and will be moving membership to locate and enroll proper forwarding address or specific personnel to have listed for contact
- Throttled system to control abuse
- Organizing a standard User Agreement (Click through) for the Contacts system
  - User authorization to act on notices
  - Reasonable good faith effort
  - Refrain from using system for any other communications
- Established new APWG membership level with single benefit: enrollment in the contacts system
- Discussions to federate Abuse Manager Contact Systems under way with trade groups and response organizations

Data Fusion Working Group

Bring law enforcement, responders and financial institutions together to discuss the systematized and scrutinized sharing of forensic data

- Identify data sets that are being archived by disparate groups
- Find ways that they can systematically shared and fused for forensic applications
- Identify those legal and regulatory barriers to sharing/fusing them with an eye to negotiating/neutralizing them
- Conceptualize the construction of working data sharing/data fusion infrastructure
- First meeting at Heathrow March 2008
- Development of recommendations continue

Internet Policy Committee
(IPC)

APWG IPC Working Group

IPC Formed in 2007 at the request of ICANN to identify remedial solutions to eliminate or minimize the ability of phishers and e-criminals to co-opt the worldwide domain name registration system.

- Developing a comprehensive problem statement discussing the practices, policies and operational conventions that assist e-criminals in their enterprise
- Researching ameliorative solutions in terms of industry practices, governing policies, and operational conventions;
- Vote on the preferred remedial solution to cover specific domain name system issues

WHOIS Proposals at the ICANN

- ICANN's direction was to remove access to domain WHOIS information
- APWG Role largely reportorial, providing ICANN with operational insight on how DNS and WHOIS data are exploited
  - Developing ICANN's appreciation of the role of the DNS in different kinds of Internet-mediated crime

- Operational Point of Contact (OPoC)
  - Provides for third-party cache of WHOIS data
- Special Circumstances Proposal
  - Keeps WHOIS data public but allows redaction of data for safety and other "special circumstances"

- ICANN is still evaluating what to do about WHOIS information and is soliciting requests for studies on WHOIS. IPC submitted a request for a study of private and proxy WHOIS registrations and their impact on anti-phishing efforts.

Registry Accelerated Domain Suspension Plan

- What it is:
  A policy for registries to suspend domains used specifically for phishing
- Status:
  Working on arbitration specifications and accreditation process for phish site take down providers
- .asia is committed to being the first to roll-out the plan
  - .mx and others are looking and interested in the program

Other IPC Initiatives

- Registrar Best Practices
  - What it is: A document that describes best practices for registrars to protect themselves, their customers, and consumers against phishing
  - Status: Final version has been sent to ICANN's Registrar Constituency, discussion with the Registrar Constituency is scheduled at the Paris ICANN meeting in late June
- Redirect education pages
  - What they are: Web pages ISPs and registrars can redirect to when they take down a phishing site.
  - Status: Content is finalized, need legal review.

Completed IPC Initiatives

- ICANN domain tasting
  - ICANN requested comments on domain tasting
  - IPC submitted comments on how phishers don't appear to use domain tasting, but that domain tasting still impacts the anti-phishing efforts

  http://www.apwg.com/reports/DNSPWG_ReportDomainTastingandPhishing.pdf
- ICANN IDNs
  - ICANN requested comments on Internationalized Domain Names (IDNs)
  - Drafted best practices on how IDNs can be implemented without impacting the anti-phishing community
- I have been hacked FAQ & Education Redirect Page

Thank You

Foy Shiver

fshiver@antiphishing.org

+1 404.434.7282