APWG

Data, Communications and Public Education Resources for eCrime Response

Peter Cassidy
Secretary General – APWG
www.antiphishing.org
pcassidy@antiphishing.org
APWG Membership Profile

• US based. Global focus
• More than 3000+ members from 1800 companies and agencies worldwide
• Membership restricted to ecrime stakeholders:
  – Law enforcement agencies
  – Government agencies
  – Financial institutions
  – ISPs
  – E-commerce sites
  – Technology companies
  – Research partners (CERTs, universities, industrial laboratories, volunteer responder organizations)
  – Consumer groups
• APWG turned 5 in October
APWG Institutional Roles
Institutional Roles: Overview

- eCrime Statistician
- Mustering Point for Stakeholders
- Advisor to Government and Industry – Technical Diplomat
- Data & Counter eCrime Communications Clearinghouse
- Counter-eCrime Educational Resources Developer
Institutional Role: Statistician

APWG Phishing Activity Trends reports delineate the phishing experience, enumerating phishing's growth and characterizing phishing's evolution to inform the stakeholders' dialog.

Quarterly reports cover social engineering phishing attacks and crimeware threats:
- Developing data sets: DNS abuse and meaningful botnet metrics
Institutional Role: Mustering Point

– Association where stakeholders meet and pull together projects for stakeholder benefit
  • Data and technology projects draw contributions from industry, academe, law enforcement and standards-making communities

– Projects proceed from dialogs at conferences
  • Phishing Education Landing Page
  • Network Address Intelligence Clearinghouse
  • Counter Muling Project

Three Established Annual Conferences

Annual General Members Meeting

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

eCRS for academic and industrial research into eCrime
Institutional Role: Advisor

- APWG has contributed data; live presentations and institutional educational materials to:
  - U.S. Office of Comptroller of the Currency
  - U.S. Federal Trade Commission
  - U.S. Federal Deposit Insurance Corporation (FDIC)
  - U.S. Department of Justice
  - U.S. Department of Treasury
  - United Nations Office of Drugs and Crime (UNODC)
  - European Commission
  - Council of Europe
  - International Telecommunications Union (ITU)
  - Organization of American States (OAS)
  - U.S. Congress committees, Representatives, Senators’ staffs
  - ICANN
  - Law enforcement agencies, government agencies and administrative law courts worldwide
Institutional Role: Technical Diplomat

• Internet Policy Committee
  – Studies and formally reports out on technical aspects of eCrime enterprise to inform industrial and government policies
  – Advisors to: ICANN; US Congress; ISP industry and global industry associations

• Emergent Law Enforcement-Network Security Initiative
  – Developing uniform data exchange (discovery, acquisition, sharing, disclosure) guidelines/standards for industry and LE
    • Define acceptable exchange practices across the full life cycle of data flows
    • Interrogate legality of capturing, collecting and observing network activity
      – Evidentiary care
      – Responsible disclosure and disposition
APWG eCrime Data Resources

- APWG Phishing Attack Data Repository
- Phishing Attack URL Block List (UBL)
- Network Address Intelligence Clearinghouse
- APWG eCrime Exchange Network
- IODEF Extensions for eCrime Reporting
- Accelerated Suspension Program for Domains
  Established Exclusively for Criminal Enterprise
Institutional Role: eCrime Data and Counter eCrime Communications Clearinghouse

- Clearinghouse model forces examination of data governance and usage issues in private and public sectors
  - Clearinghouse success owes a lot of governance innovation established by APWG in user agreement
  - User agreement that assigns no new liability
  - Some 50+ Signatories from CERTs, brandholders, telecommunications companies, security companies, software developers, academic researchers
  - **Clearinghouse model** operates similarly to the genomic databases used by life sciences researchers in the US and Europe
  - Third-party position gives assurance of neutrality
Phishing Attack Repository & URL Block List

APWG Phishing Attack Data Repository
3 Million + historical records of phishing events and related data

Phishing Attack URL Block List (UBL)

- Updated every 5 minutes; listing of previous 72 hours attacks with URLs
- Used to power warning systems in browsers and tool bars
- Inform signaling systems for security teams
- Inform research and development of counter-eCrime technology
APWG Network Address Intelligence Clearinghouse

- Network Address Intelligence Clearinghouse (NAIC), a members’ only, limited access database to archive network addresses specifically tied to an electronic crime event or an instance of attempted or successful fraud.
- Different from URL Block List which archives location of sites; focus is on network address location of cash-out attempts or account-hacking activities – from telephone numbers to Internet Protocol (IP) addresses.
The AeCEN is a private online data exchange platform that allows users to securely exchange eCrime data

- Brandholders, security companies and law enforcement can share information in real time about phishing attacks, malware attacks, and other cyber crime activities

Leveraging the APWG UBL, the system distributes in real time all known and suspected phishing site addresses domains known to host malware and phishing sites

The AeCEN consists of a group of individuals within a company, an association and organization - or an "invite only" group created by a user. Individuals interact within groups and securely share eCrime-related data collected within the system. They can post their own eCrime data and consume privately shared data via web interface or https feeds.
IODEF Extensions XML Schema for eCrime Reporting

Extensions to the IODEF-Document Class for Phishing, Fraud, and Other Crimeware proffers:

- 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

XML makes reports readable by people and assists in the editing of ecrime reports, adding data & organizing human-driven workflows
APWG eCrime Reporting Tool

Java-based eCrime Reporting Tool console runs on any machine that plays Java. Simple interface allows anyone to make out a report by stepping through and populating tabbed templates. A network engineer can use it. More importantly, a local cop with minimal technical vocabulary can use it.

Working betas established for US-EN, UK-EN and ES-ES (Spain-native Spanish.) More languages to come. **Goal:** create eCrime Reporting Tool available in every language in which electronic crime is a problem to help establish and feed private sector, public sector and non-profit eCrime data repositories.
The APWG eCrime Reporting Tool assures complete reports are made and are written to a universally readable and writable XML format. Console can be set for local filing, remote or third-party repository filing or submission directly to the APWG repository.

**Next Step**: Creation of open source tools to translate data sources into IODEF Extensions format to mobilize now islanded data of forensic value.
Accelerated Suspension Plan

• Effort to fight criminal registration of domain names at the registry level

• Involve registries in well-defined, accredited process with interveners to render fraudulent domains harmless if registrar unresponsive

• Started development over a year ago with the .ASIA Registry

• Active development has begun; deliverables began landing on the bench this month
Accelerated Suspension Plan

- APWG accredited entities
- Special, secure communications to registry
- Standard process leading to rapid suspension of domain
- Appeal process and penalties for mistakes
Accelerated Suspension Plan

• Demand for this program from registries around the world – at least half a dozen serious requests

• Working to finish up all necessary tasks to enroll beta users this summer

• APWG will run
  – Providing secure messaging platform
  – Accreditation and monitoring of program
Institutional Role: Counter eCrime
Educational Resource Developer

Phishing Education Landing Page Project
Redirects consumers who’ve clicked on links in phish mails to an educational page in their language in the appropriate format for their browser client.

Counter Muling Project
Developing a series of video podcasts for the intervention and instruction of consumers who are at risk for being inducted into criminal enterprise as a money mule.

The APWG Public Education Initiative (PEI) organizes counter-eCrime educational programs and forges the essential logistics to deliver them to the largest victimized cohort possible.
Counter-eCrime Education
Resources Developer

[Blackboard 1: APWG CMU
Phishing Education
Landing Page Program]

[Blackboard 2: APWG/NCSA
Counter Muling Project]
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 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.

How to Help Protect Yourself

1. Don't trust links in an email.
2. Never give out personal information upon email request.
3. Look carefully at the web address.
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.
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, CMU'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 phished 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 being phished, but these are steps that you should consider if a phishing attack has been attempted against you.
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
- 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)
Implementation and results

• It works
• In English, French and Spanish
• Being translated into 15 languages
• 1 Oct, 2008 – 1 March, 2009
  – 56,699 “teachable moments”
  – Average number of days: 34.9 days
  – 87.8% hits are from the US
Development Program

• Keep developing translations for every language in which phishing becomes a problem
• Promote usage among ISPs
• Analyze data for trends and insights
The APWG Counter Muling Project development team is developing a series of video podcasts for distribution among our member companies and agencies, research partners, government agencies, trade and law enforcement associations and traditional electronic media. **Message**: Muling is a crime, whether you are fooled or not; here’s how to avoid it.

A number of electronic educational instruments are being developed, to be delivered in broad media campaigns and in a just-in-time modality like the [APWG/CMU Phishing Education Landing Page Program](http://www.apwg.org/CMUPhishingLandingPage) which delivers counter-phishing instruction to consumers who have clicked on links in phishing emails.
Thank You

pcassidy@antiphishing.org

+1 617 669 1123