Phishing Trends and Collaborative Efforts to Fight Cybercrime

Manel Medina
APWG.EU / esCERT-inLab-UPC

Jordi Aguilà
APWG.EU / CaixaBank

APWG Who Are We

- Founded in 2003 to focus on Phishing
- Began collecting data and create process for tracking Phishing
- Currently 2000+ companies, NGOs, government, law enforcement agencies, and treaty organizations worldwide
- Membership restricted to cybercrime stakeholders:

Financial institutions	ISPs
Technology companies	Law enforcement agencies
Government agencies	Treaty organizations

E-commerce sites and solutions providers
Research partners - (CERTs, universities, industrial laboratories, volunteer responder organizations)

APWG Spheres of Influence

- Tracking Trends and Activities
- eCrime Research
- Cyber Policy
- Education / User Awareness
- Data Logistics

Why APWG.EU

- Interest of APWG, Inc. USA for expanding activities in **Europe**, LATAM and Asia
- **Globalization: E-crime** as a global problem. IT governance is a must in Europe. Europe has its own personality fighting against cybercrime.
- Europe is a huge community on research with a long tradition (Universities, public research, private research)
- The European Union itself has specific research programs focused in e-crime. (H2020, etc.)
- Being a "**European something**" – business corporation, enterprise, research center, limited or anonymous society, foundation, etc. - is necessary to obtain grants from the European Union
- **Private companies** on the sector interested in APWG.EU

Activities of APWG.EU

APWG.EU is a scientific research foundation
which aims to provide focused RDI support to private industry by:

- ✓ Developing RDI activities
  - in consortium with other organizations:
    Universities, law enforcement, R&D centers, private companies
- ✓ Creating a European trust network
  - for sharing e-crime intelligence information and repositories of common interest information
- ✓ Promoting best practices, guidelines, and knowledge
  - in the areas of e-crime, phishing, malware, and other aspects related with the e-crime sectors
- ✓ Organizing European e-crime events
  - meetings, workshops, and scientific conferences

Research of APWG.EU

- Objective: Establish a network of high level talents to conduct RESEARCH PROJECTS of common interest over Europe in the cybercrime fields.
- Tools: Common clearinghouse with research centers (universities, private, law enforcement) to automatic sharing of information, knowledge and tools.
- Actually four main lines we are developing in europe H2020 programs
  - Research on information sharing
  - Research on advanced Authentication Systems
  - Dissemination of security information
  - Security on mobile systems
  - Cloud security

APWG's Big Question:

How Does a World of Localities Engage a Problem of Global Dimensions Like Cybercrime and Respond as a Unified Authority?

Data Logistics as Cybercrime Response Instrument

The design and optimization of processes to manage the movement and presentation of data to enable crybercrime responders and forensic analsysts to take action – or receive data – at a time and place for a specific counter-cybercrime application

Examples of APWG Cybersafety Data Logistics

- The Stop. Think. Connect. Messaging Convention
- Phishing Repository & URL Block List
- eCrime Exchange
- Malicious Domain Suspension System

- Phishing Education Landing Pages
- eCrime Classification System
- Bot-Infected System Alerting and Notification System

STOP. THINK. CONNECT.

- Re-animates the oldest logistical schema: standardization
- Over 20 international companies founded the project
- Rigorously informed, crafted and tested messaging instrumentation offered at no cost
- Repurpose communications avenues and networks of all the Messaging Convention participants
- Leverage every web page, ATM receipt, account statement and communications instrument to deliver awareness messaging

STOP ちょっと待て | THINK 考えてから | CONNECT™ つなげよう

APWG eCrime Exchange:
A Member Network
For Collaborative eForensics

Organizational Objective of eCX

Ganging Up on the Bad Guys

- Exchanging Data Programmatically

  Consolidating data across industries and geographies for more effective security routines

  Example: URL Block List

- Teaming Around eCrime Events

  Enterprises and groups recognizing they face common adversaries can combine data and insights needed to neutralize the attackers

Phishing Repository and URL Block List

- APWG Phishing Attack Data Repository
  - 8.5+ million historical entries
  - Informs research and development of counter-eCrime technology
- Phishing URL Block List (UBL)
  - Updated constantly
  - Informs browser warning systems and anti-phishing tool bars
  - Signaling systems for security teams
  - CERTs, brand-holders, telecom companies, security companies, software developers and the public

Accredited Reporter Data Submission Program

- Broadens the number of qualified contributors to APWG Systems
- Establishes a formal mechanism for an enterprise to be accredited by APWG and send reports to the UBL directly
- Qualifying organizations can use their credentials to submit reports in bulk for processing

APWG Malicious Domain Suspension Process (AMDoS)

World's First and Only Auditable, Scalable Malicious Domain Name Suspension Request System for Professional Interveners and the Registrys

What are we trying to accomplish?

- Complement (not circumvent) court orders or legal instruments to allow
  - Responsible (and transparent) action in
  - A timeframe measured by hours rather than days, weeks, or months and to
  - Hold reporting parties to a standard of practice and accountability
- Replace ad hoc processes used to suspend domains today with a uniform, auditable process based on signed attestations

APWG Malicious Domain Suspension Process

- AMDoS mediates formal correspondence between an **Accredited Intervener** and a **Registry Authority**
  - trusted-introducer/trusted-channel system
  - a medium for transmission of suspension requests for abusive domains
- Objectives
  - Enhance speed and scalability of interventions
  - Provide formal tracking
  - Provide accuracy, accountability. transparency

Trusted Introducer System

Accredited Intervener

[AMDoS]

Registry - Registrar Authority

formal, auditable communications channel

AMDoS Functional Overview

- Benefits to Interveners
  - Credibility. Your trustworthiness is not questioned
  - Your suspension requests are taken seriously
  - Fair, equitable evaluation process

- Benefits to Registry/Regisrar Authorities
  - Confidence. Suspension requests are from party with capacity to judge **criminality** of domains
  - Competitive advantage (trustworthy operator)

Domains Eligible for Suspension

- AMDoS is for maliciously registered domains
  - Domains registered with the intent to perpetrate phishing, malware distribution, financial fraud
- What is criteria for domain to be considered "criminally abusive"?
  - Use of a domain name exclusively for the animation of fraud to steal or coopt funds or personal data in order to further a fraud or theft

Registry Authority owns process

- Registry Authorities participate voluntarily
  - Under no obligation to participate or act
  - Registry can assess request against explicit criteria before making a decision to suspend
- Expectation is that
  - A signed attestation from
  - A vetted reporting party with
  - Documentation that demonstrates criminal use will be persuasive

Other Goals

- Metrics!!
- Shame bad registries/registrars into being good registries/registrars

Thank You

APWG Internet Safety Engineering

Manel Medina
manel@apwg.eu

Jordi Aguilà
jaguila@lacaixa.es