Update on Global Efforts to fight Cyber Crime

Foy Shiver
APWG.ORG

Jordi Aguilà
APWG.EU / CaixaBank
APWG Spheres of Influence

• Tracking Trends and Activities
• eCrime Research
• Cyber Policy
• Education / User Awareness
• Data Logistics
APWG: 11 years of Statistics

APWG Phishing Activity Trends Report
- Published since February 2004
- Initially monthly, now quarterly or semi-annually
- An in-depth review of the ongoing state of Phishing

Global Phishing Survey: Trends and Domain Name Use
- Published since 2H 2007
- Semi-annual attempt to understand trends and their significances by quantifying the scope of attacks with a focus on DNS

Mobile Threats and the Underground Marketplace
- New for 2013
- Attempt to defines the malware markets and demonstrates the modus operandi of an industry that is self-funding, prosperous, vertically stratified and agile.
Online Cybersafety Awareness Messaging

• Problem: How do you raise awareness in the largest number of people without heroic effort or cost

• Logistics imperative: Reach customers and citizen where they are – and through channels they already trust

• Solution: Unify messaging across trusted-parties with shared, and therefore unified, messaging instruments
The STOP. THINK. CONNECT.™ cybersecurity public-awareness suite, first proposed by the APWG to its members in 2009, is the only year-round, globally coordinated messaging scheme to help all digital citizens stay safer and more secure online.

The slogan and logo was created by an unprecedented coalition of private companies, nonprofits and government agencies in 2009 and 2010 who recognized the power of a unified cybersecurity awareness campaign compared to an uncountable number of uncoordinated efforts.
Engines of Mass Behavior Upgrade

• The STOP. THINK. CONNECT.™ campaign travels on two rails:

• Shared cybersecurity messaging assets: the logo, slogan and advisory suite are free for all to use – everywhere – for forever and a day

• Ubiquitous deployment: Every enterprise, government and NGO can deploy the campaign, providing global resonance required for users to retain the principles imparted by the campaign’s messaging assets
End Game: National Campaigns Merge Into Global Program of Measurable User Upgrade

- Transborder
  - Transcultural
- Translingual
- **Transformational**

- Self-possessed, resilient users will deny cybergangs the easy returns of the cybercrime era’s early days
- Campaign is first step in a global program to make users an instrument of network maintenance and defense
- Join us and a part of that transformation in user posture and participation
National Memorandums of Cooperation

- **Bangladesh** – Bangladesh Computer Council
- **Canada** – Public Safety Canada
- **Dominica** – Ministry of Information Science Telecommunications and Technology
- **France** – CECyF (Ministère de l’intérieur / Ministère des finances)
- **Japan** – Council of Anti-Phishing Japan (JP CERT)
- **Jamaica** – Ministry of Science, Technology, Energy and Mining
- **Spain** – Instituto Nacional de Ciberseguridad de España, S.A.
- **Panama** – Autoridad Nacional para la Innovación Gubernamental
- **Paraguay** – Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS)
- **Poland** – NASK
- **Switzerland** – Swiss Internet Security Alliance (SWITCH/SwissPost)
- **USA** – NCSA (Department of Homeland Security)
- **Uruguay** – Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

- The public-private partnership is the prevailing model in national campaign deployments to date
  - Of the 13 national campaigns under MoU, curators that were not governmental entities have substantial national ministry involvement
National Deployments to Date

The national deployments to date have been launched by a mix of national government agencies, NGOs and trade associations.

- **Jamaica** – MSTEM, government ministry and national banking consortium + Jamaica Bankers Association
- **Japan** – Council of Anti-Phishing Japan
- **Spain** – Cibervolunteros + INCIBE
- **Switzerland** – SISA Swiss banks and tech companies + SWITCH and Post Finance
- **USA** – NCSA (NGO underwritten by DHS and industry)
Step Up and Help Everyone

• The Messaging Convention Empowers Three Primary Roles
  – Commercial Licensee
    • No-cost license for commercial enterprises who want to integrate Stop. Think. Connect. Messaging Convention messaging instruments into their own online safety education programs
  – Non-commercial STC Messaging Convention Content User
    • Pre-packaged Stop. Think. Connect. online safety education materials for educational agencies and ministries and NGOs to instruct their constituencies
  – International Program Partners
    • National and regional governments, multilateral treaty organizations, NGOs who recruit licensees and users within an industrial sector or polity
• Find your own best-fitting role to get your organization involved
  http://www.stopthinkconnect.org/get-involved/overview/
eCrime Researcher Program

• Founded in 2006
• Only peer reviewed electronic crime research program
• Accepted papers are published through IEEE
  – 80+ papers published to date
• Unique blend of Academia and Industry
  – Research Track
  – Industry Track
eCrime 2016
Symposium on Electronic Crime Research

Sponsors / Partners

PayPal™
MarkMonitor
Interac
EASY SOLUTIONS

CeCoS XI Toronto
May 24-26, 2016

Unifying the Global Response to Cybercrime
APWG eCrime Exchange: A Member Network For Collaborative eForensics
Phishing Repository and URL Block List

• APWG Phishing Attack Data Repository
  – 10+ 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
New REST-based API

• Implemented on all feeds
  – URL Block List
  – Facebook external block list
  – malicious IP database (beta rolling out soon)
    • each IP had an unknown type of bad actor of some sort behind it
    • bad actor is/was pushing the system at the IP in question to attack a top level online financial institution

• Provide new access to the data
  – sorting, filtering, and searching options
  – support for new submissions and updates to existing phish
Other eCX Updates
(rolling out now)

• Expand shorteners to (all) their endpoints
• Grabbing and store more details
  – screenshots in pdf
  – page source
  – any viral payloads
• Ability to mark interest in a phish/url/ip the all threat modules
  – that data goes out with the api data so people can see who else is interested in something that they are interested in
• New front end to the dashboard
  – lots of metrics to see what is happening within the data at a glance
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
AMDoS Goals

• 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
  – Hold reporting parties to a standard of practice and accountability

• Replace ad hoc processes used to suspend domains with a uniform, auditable process based on signed attestations
AMDoS: Goals

• 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

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

• Benefits to Registry/Registrar 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
Thank You

Foy Shiver
foy@apwg.org

Jordi Aguilà
jaguila@lacaixa.es