APWG and the eCrime Exchange: A Member Network Providing Collaborative Threat Data Sharing

Foy Shiver

APWG Who Are We

Founded in 2003 to focus on Phishing

Began collecting data and create process for tracking Phishing

Membership includes a blend of cybercrime stakeholders:

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

E-commerce sites and solutions providers

Research partners – (country CERTs, universities, industrial laboratories, volunteer responder organizations)

Current Spheres of Influence

As CyberCrime and Fraud evolved so have we

- Cyber Policy
- Education / User Awareness
- Research
- Tracking Trends and Malicious Activities

Cyber Policy

Internet Policy Committee

Help developers of Internet policy understand evolving electronic-crime threats and assist in the development of domain name system (DNS) and other Internet-related policies that protect Internet users and organizations from e-crime.

Host bi-weekly conference calls to discuss onging cyber policy issues

Symposium on Policy Impediments to Cybercrime Data Exchange

Engage issues in law, regulation, treaty conventions and industrial interpretations thereof that have introduced impedance to systematic exchange of cybercrime event data.

- Annual Meeting and report out
  - Rotates between US and EU
  - Considering other regions

Education and User Awareness

Time to Upgrade our Users

Online Cyber-Safety 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

An Engine 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
  - 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

Unified Cybersecurity Awareness Messaging
The Keystone to Upgrading User Awareness at Scale

STOP | THINK | CONNECT™

- The first and only globally coordinated cybersecurity messaging suite to help all digital citizens stay more secure online
- The campaign maintains a service-mark slogan, logo and brief advisory suite
- The program and assets are managed by STOP. THINK. CONNECT. Messaging Convention, Inc.
  - a Georgia Non-Profit Corporation co-managed by two not for profit NGO organizations: APWG and NCSA

24 Memorandums of Cooperation With National Ministries, CERTs and NGOs

Armenia – Armenia Education Center and Internet Society of Armenia
Antigua and Barbuda – Ministry of Information, Broadcasting, Telecommunications & Information Technology
Bangladesh – Bangladesh Computer Council
Canada – Public Safety Canada (2012/Harper Administration)
Colombia - MinTIC
Czech Republic – NCBI / SaferInernet.cz
Dominica - Ministry of Information Science Telecommunications and Technology
Ecuador - Centro de respuesta a incidentes informáticos del Ecuador
France – CECyF (Ministère de l'intérieur / Ministère des finances)
Italy – Poste Italiene
Japan – Council of Anti-Phishing Japan (JP CERT)
Jamaica – Ministry of Science, Technology, Energy and Mining
Latvia – IMCS UL / CERT.LV
Spain – Instituto Nacional de Ciberseguridad de España, S.A.
Mongolia – Mongolia CERT
Nigeria – CSEAN
Panama – Autoridad Nacional para la Innovación Gubernamental
Paraguay – Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS)
Poland – NASK
Slovakia – Preventista.sk
Slovenia– Slovenian Computer Emergency Response Team (SI-CERT)
Swaziland – Office of the Secretary to Cabinet
Switzerland – Swiss Internet Security Alliance (SWITCH/SwissPost)
Kingdom of Tonga – Ministry of Information & Communications
Uruguay – Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

Latest Memorandums of Understanding signed:

- Colombia
- Slovenia
- Czech Republic
- Latvia
- Slovakia

Latest Memorandums of Understanding shipped for due diligence:

- Bhutan (CERT)
- Sudan (CERT)

Global Multi-Lateral Treaty Organizations

APWG is working with multi-lateral treaty organizations to encourage their member nations adopt STC:

Organization of American States

2012 Memorandum of Cooperation

Commonwealth Secretariat

Advising in development of Commonwealth Cybercrime capacity development strategy

Europol (EU)

Presented at INTERPOL-Europol cybercrime conference 2015

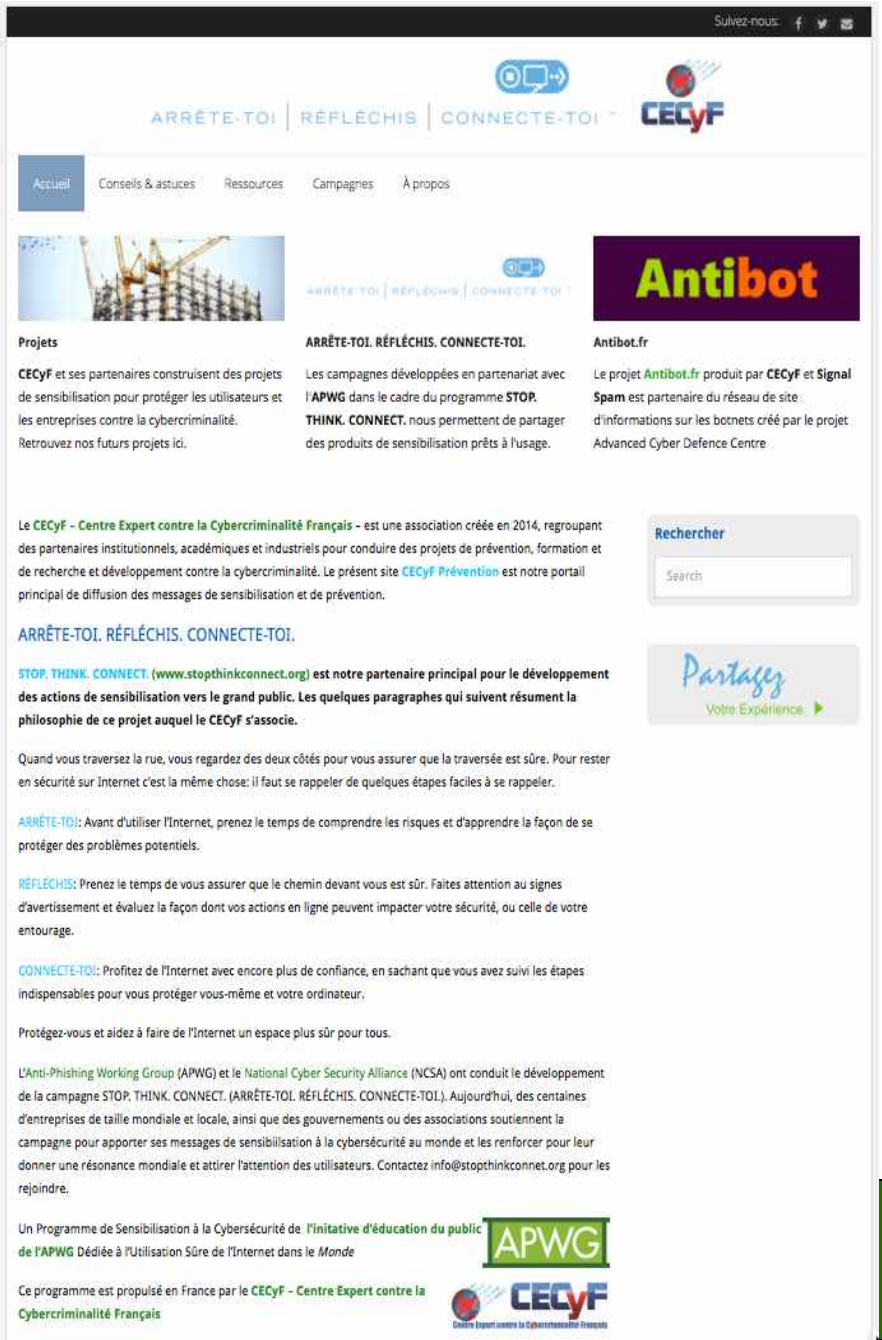
Hybrid Approach Invites Flexibility in Deployment

Participants can target materials to their local audiences

Japan

- First national STOP. THINK. CONNECT. campaign in East Asia
- The STOP. THINK. CONNECT.™ campaign in Japan is curated by the **Council of Anti-Phishing Japan** which recruited a group of some 20 technology companies, e-merchants and business infrastructure firms to manage its deployment
- Operational as of December 2014
- February 2016 deployed original STC posters at all 160 subway stations of the massive Tokyo Metro
- Leadership is shared by **JP CERT**, **Trend Micro** and **Hitachi Data Systems**.
- ɔnnect.jp

フィッシング対策協議会
Council of Anti-Phishing Japan



France

- Memorandum of Cooperation completed for the Republic of France in December 2015 by the French Center of Excellence Against Cybercrime, signed by IG of **Gendarmerie Nationale**
- CECyF is a public private partnership with management provided by French Interior
- Website launched in February 2016
- SEE: cyberprevention.fr

Switzerland

- **SWITCH**, the national CERT and ccTLD manager, arranged for the MoC through Swiss Internet Security Alliance (SISA), an NGO largely managed by SWITCH and PostBank Switzerland
- Campaign launched in late 2015. First in Europe to prepare and present materials for local languages. So far, German and French.
- See: stopthinkconnect.ch

Spain

- **Cibervolunterios**, a national-scope NGO dedicated to young people's online safety, entered into licensing agreement with the Messaging Convention in 2013 and launched their own national STCcampaign website.
- **INCIBE** (national CERT of Spain) signed the MoC in late 2015 and will be coordinating with Cibervolunteros and other organizations going forward
- See: parapiensaconectate.es

eCrime Research

eCrime Researcher Program

- Founded in 2006
- Only peer reviewed electronic crime research program
- Accepted papers are published through IEEE
  - 90+ papers published to date
- Unique blend of Academia and Industry
  - Research Track
  - Industry Track

eCrime 2017

Symposium on Electronic Crime Research

Sponsors / Partners

PayPal™

EASYSOLUTIONS

CUING.ORG
CRIMINAL USE OF INFORMATION HIDING

IEEE

April 25/26/27 - Scottsdale, Arizona

Accepting Research Papers Through Feb 8
Session / Panel Proposals through March 3

Research & Awareness Focus

Growing in Europe

APWG.EU

- Founded 2013
  - European Foundation based in Barcelona, Spain
  - Cofounded with support from CaixaBank
    - Board split between CaixaBank and APWG.ORG
- Focus on User Awareness, Policy and Research in Europe
- First meetings
  - Joint with .ORG 2015
  - 2nd Data Exchange Symposium – Brussels, Belgium
  - eCrime2016.EU – Bratislava, Slovakia

APWG.EU

Founding Members
Board of Trustees

Platinum Members
Advisory Board (voting rights)

Gold & Silver Members,
Event Sponsors,

Research Partners

APWG.EU
Event Outreach 2017

- 3rd Data Exchange Symposium

  3 July, Washington, DC, USA
- Cyber Awareness Symposium II

  21 September, The Hague
- eCrime2017.EU

  24-26 Ocober, Porto, Portugal
- Cyber Awareness Days

  Ancone (Italy), Plovdiv (Bulgaria), Košice (Slovakia), Vienna (Austria), Madrid & Barcelona (Spain)

APWG.EU
Research & Projects

- VIVET (Erasmus+)
  - Goal: designing educational materials on cybersecurity for vocational training students; multilingualism is key to the project, as an extension of the Stop.Think.Connect. campaign
  - APWG.eu's duties: prepartion of a short film and an exchange platform; dissemination
  - Consortium: APWG.eu + Forum Berufsbildung (DE) + VU PO Agrobiznes i Razvitie na Regionite (BU) + Centro Libero Analisi e Ricerca (IT)
- CyberVolunteers
  - Network of Cyber Experts with App to track skills and schedules

APWG.EU
Ongoing Research

- TrueSec (H2020)
  - TRUst-Enhancing Certified Solutions for the SECurity & Protection of Citizens' Rights in Digital EU
  - Goal: creating a platform and a quality certificate (RETEL) for European response teams
  - APWG.eu's duties: technical design and implementation of the platform; dissemination
  - Consortium: APWG.eu + UPM (ES) + Asociación Usuarios Internet (ES) + UniGraz (AT) + Université de Lille (FR) + Catapult (UK) + Knowledge Transfer Network (UK)

Tracking Trends and Malicious Activities

APWG: 12 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

APWG eCrime Exchange: A Member Network Providing Collaborative Threat Data Sharing

eCrime Exchange

Prime directives:

- Share cyber threat data
- User base of known 'good actors'
- Warehouse virtually any type of threat data
- Robust API for data consumption

eCrime Exchange History

- Originally developed in 2003
- Banking industry users
- Sharing phishing URLs
- Built using PERL scripts and MySQL, with users emailing CSV data
- 'Lists' were available for download

eCrime Exchange History

Phish List Input

- 2 or 3 different input formats

Phish List Output

- The name of the brand under attack
- URL
- Date first seen
- Strength of confidence factor

'Lists' were available for download from FTP server

Threat Data Warehouse

- Social Networking Emerging
- "The enemy of my enemy is my friend"
- Symposium on Electronic Crime Research, Toronto 2016
  - Over 80 companies who do business in over 20 countries throughout the world working in over 15 different types of entrerprises that are all focused in some way towards cyber threat prevention
- What do they all have in common?

eCrime Exchange

- Data
- Well organized, well classified, timely, well defined and structured, high availability
- Actionable


```
{
  "url": "http://www.mike_at_apwg.org/phishy_attack/bad_thing.html",
  "brand": "APWG",
  "date_discovered": 1464454781,
  "confidence_level": 100
}
```

eCrime Exchange Framework

Modules

- Phish
- Malicious URL
- Facebook

Workgroups

- User generated modules

REST API interface

Phishing Module

- 10+ million historical entries
- Updated instantly
- Feeds browser warning systems and anti-phishing tool bars
- CERTs, brand-holders, telecom companies, security companies, software developers and the public

Malicious IP Module

- Unique feed from Paypal
- 30+ million entries since Jan 16, 2016
- Updated instantly
- Mostly IP's performing botnet port scanning
- All attack traffic of some sort

Facebook Module

- Unique feed, but for different reasons
- No longer active
- 450+ million records
- Contains phish, spam, malware payloads, and other types of offensive URLs
- 99.9% are URL shorteners, most multiple levels of redirection logic

User Workgroups

- An industry "game changer"
- ECX users create their own modules
- Store virtually any type of cyber threat data
- Data can be public or private
- Same high performance API interface as eCX Modules
- Owner has full member control

eCX REST API

- Available for every eCX Module and User Workgoup
- Very fast
- Insert data in 180ms
- Retrieve data in ~600ms
- Extensive sorting, filtering, and searching options
- Supports adding, changing, updating all data
- Averaging 6 million requests per month, returning 140 million records
- Used by ~150 users

Notifications

- Users can set notification alerts when new data arrives
- Any new data, or data matching some criteria

Collaboration

- Mark an interest in a record
- eCX makes the introduction

Query

- Allows site wide search in one operation

"Last Kilometer"

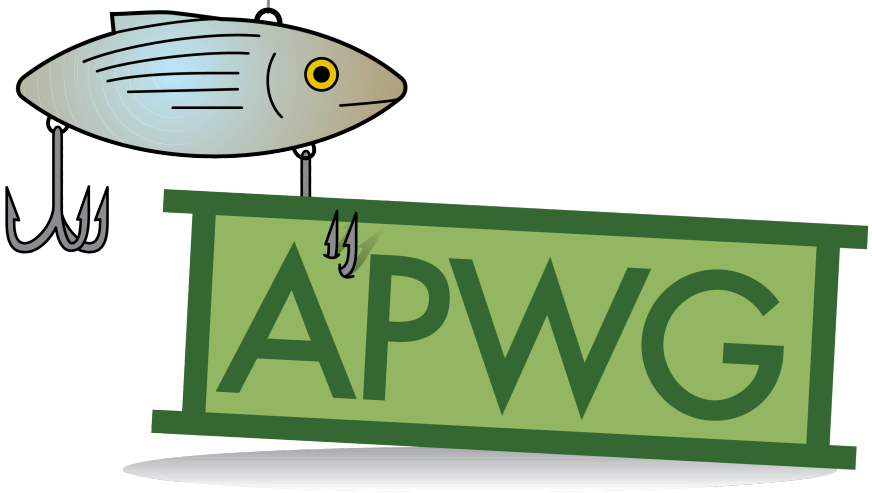
Having data is good

But how do we know if it is being used?

No reason data should not protect the public instantly

New "Time To Protect" report will begin to be published in 2017

Thank You



foy@apwg.org

support@ecrimex.net