APWG Committed to Wiping Out Internet Scams and Fraud

APWG and e-la Caixa CSIRT

The role of the CERTs/CSIRTs in the accelerated domain suspension plan

APWG Committed to Wiping Out Internet Scams and Fraud

Index

Committed to Wiping Out Internet Scams and Fraud

e-la Caixa CSIRT

- **Team information**
  - Official Team Name: e-la Caixa CSIRT
  - Membership Type: Full Member
  - Date of establishment: March 29th, 2005

- **Constituency**
  - The constituency of the CSIRT is the electronic channel of the savings bank, “la Caixa”: e-la Caixa S.A. and its customers.

- **Team contact information**
  - E-mail address: GE_e_CSIRT at elacaixa.com
  - Telephone number: +34 93 404 65 72
  - http://www.first.org/members/teams/e-lc_csirt/

e-la Caixa CSIRT

- **Team Structure**
  - Steering Committee: 5 members
  - Incident Response: 11 members
  - Profiles: Information Security, Law Enforcement, Lawyers, Computer Linguists, etc.
  - Departments: Physical Security, Information Security and Legal.

- **Incident Response**
  - Phishing, Fast-Flux Phishing and Rock Phishing
  - Malware
  - 419 Scam
  - Trademark Abuse
  - All other threat coming from the Internet

- **Compliance**
  - Certified with ISO/IEC 27001

Committed to Wiping Out Internet Scams and Fraud

APWG

- Created in 2004
- The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks.
- Mr. Foy Shiver will widely explain about the APWG and APWG activities on his presentation this afternoon.

Justification: Conclusions from the global phishing survey conducted by Greg Aaron and Rod Rasmussen (CECOS III Barcelona)

- **Phishers move from registrar to registrar, and TDL to TLD to exploit the best phishing "holes"**
- **Moving away from IP-based phishing.**
- **The amount of Internet names and numbers for phishing has remained fairly steady over the past two years.**
- **Sub domain registration services are nearly as abused as standard domain registrars**
- **Malicious registrations>18%**
- **Phishers are happy to use any domain name**
- **Registry anti-abuse programs have an effect**

APWG Committed to Wiping Out Internet Scams and Fraud

The group: APWG Internet Policy Committee IPC

- **Goal**

Ensure anti-phishing concerns are represented during the creation or modification of Internet policies.

- **91 members**
  - Registries and registrars
  - ISPs
  - CERTs
  - Law enforcement
  - Brand Owners
  - Vendors
  - Academia

The plan: Accelerated Suspension Plan

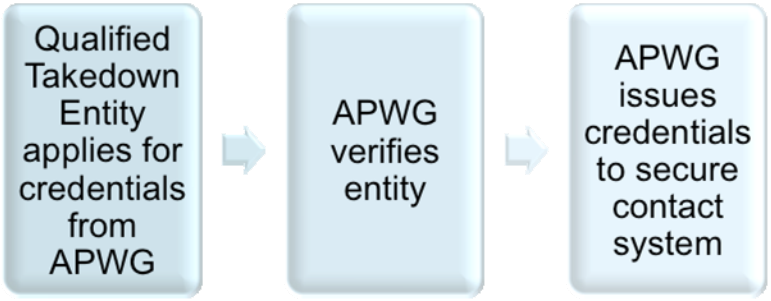
- To fight criminal registration of domain names.
- Covers domains registered with the intention of performing a criminal attack or action.
- Involves registries and registrars in a well-defined, accredited process with a final goal to suspend fraudulent domains.
- The model is being discussed within the APWG IPC, ICANN, registries and other key players.
- Started development a year ago with. Asia registry.
- Other registries .org, .info have established regulations to fight criminal domains and are included in this development process.
- Model is based on process designed by the APWG
- Domains eligible for suspension include:
  - Must be registered in the TLD of a participating registry
  - involved in a current phishing attack or host Malware that steals personal information
- Eligible domains do not include those in use for legitimate internet activities, yet also in current use for phishing or Malware distribution. (Phish site hosted under a legitimate domain).

APWG Committed to Wiping Out Internet Scams and Fraud

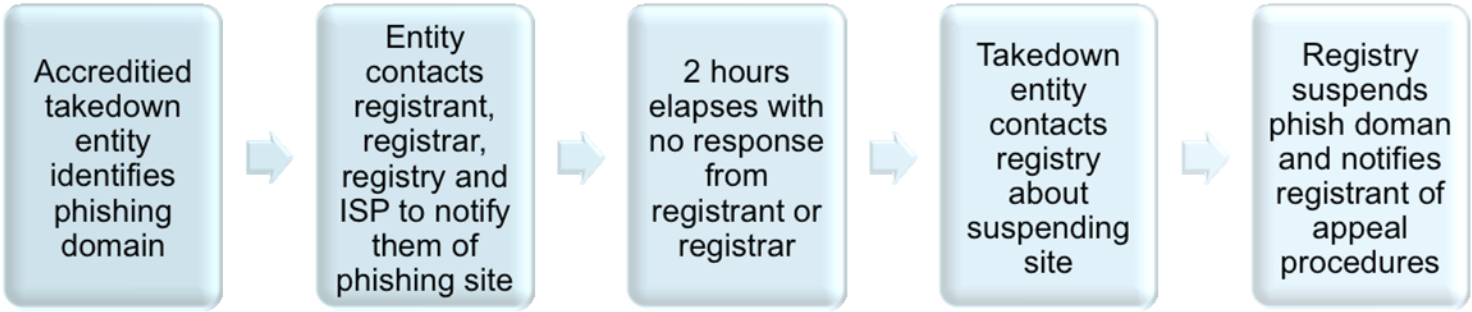
The plan: Accelerated Suspension Plan II

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

Becoming a Takedown Entity



Takedown Process



REQUIREMENTS (still in Draft stage)

- **Accredited by the APWG: accreditation efforts are designed to mitigate likelihood of abuse or negligence of the domain eligibility criteria and /or suspension process.**
  - **Accreditation criteria and process.**
- **Entities to apply:**
  - **Corporations with their own anti-phishing units**
  - **Third party providers that perform anti-phishing services**
  - **Experts in security : CERTS & CSIRTs**
  - **Others**
- **Basic concepts**
  - **Entity qualified: to properly qualify a site as a phishing site eligible for suspension process according to the domain eligibility criteria.**
  - **Experienced: By providing a history of successful anti-phishing services**
  - **Insured: Maintains commercial liability and/or professional liability insurance with a minimum limits to be defined.**

ACCREDITED ENTITIES and the CERTS and CSIRTs

- **Within those ACCREDITED ENTITIES the CERTs and CSIRTs can play an important role.**
- **Experts on security, the majority dealing with phishing and Malware since the beginning.**
- **Can easily identify a Phish site.**
- **Can easily identify and describe an Internet infrastructure designed to maintain Malware in activity such as the download site/domain, the receiving stolen data place, etc.**
- **The credibility coming from a CERT/CSIRT is a high value**
- **Is a long time experienced entity in Internet security matters.**
- **Can be easily insured to play the role.**
- **We hope to encourage all FIRST members to join the initiative and help to create a 'cleaner' Internet**

Q & A

Thank you