Forum on DNS Abuse

Nii Narku Quaynor

Moderator

24 October 2011

ICANN

Dakar

SÉNÉGAL

N°42 23 - 28 October 2011

Session 1- Latest Developments in the Fight Against DNS Abuse

Pierre Danjineau
INFOCOM

Lanre Ajaya
Pinet Informatics

Frederick Gaudreau
Surete du Quebec

Gary Kibby
Serious Organized Crime Agency

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

Session 1- Latest Developments in the Fight Against DNS Abuse

Pierre Danjineau
INFOCOM

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

Session 1- Latest Developments in the Fight Against DNS Abuse

Lanre Ajaya
Pinet Informatics

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

Nigeria Cyber Security Challenges and Management

By

Lanre Ajayi

CEO
Pinet Informatics

Common Cyber Security Challenges

- Phishing
- Spam
- Scam mails
- Identity theft
- Denial of Service (DOS)
- Unauthorised access (Hacking)
- Cyber terrorism
- Viruses

The Nigerian Cybersecurity Challenges

Cybersecurity challenges	Nigeria Guilty?
Spam	YES
Scam Mail	YES
Phishing	YES
Identity theft	YES
Denial of Service	NO
Unauthorized access (Hacking)	NO
Cyber Terrorism	NO
Viruses	NO

Consequences

- Loss of Confidence in eCommerce transactions from Nigeria
- Non acceptance of credit cards issued in Nigeria by some merchants from other countries
- Blockage of Nigerian IPs on some networks
- Nigerians suffer embarrassing comments from new friends abroad

The Peak

- Some few years back, a senior citizen from one of the Eastern European countries fell into the hands of Nigerian online scammers
- The man lost his entire savings
- He complained to the Nigerian embassy in his country
- The embassy was unsuccessful in tracing the scammers in Nigeria
- The man got frustrated, went to the embassy requested to see the ambassador and shot the ambassador to death.

Nigerian Government ‘s response

- The Government set up a National Cybercrime Working Group to find solutions to the menace of cybercrime

Outcome of the Cybercrime Working Group

- Legal – The Working Group drafted a bill for cybercrime which among many other items introduces
  - Anti-spam laws
  - Lawful Intervention (LI)
  - Electronics evidence
- Industry self regulation encouraged
  - Codes of Conduct to be introduced and adopted by the industry – erring operators to be blacklisted.
- Education – Awareness to the general populace on the damage done to the economy by activities of cybercriminals
- **Government Domain names- .gov.ng mandatory for all Nigerian Government Ministries, Department and agencies**


THANK
YOU

Session 1- Latest Developments in the Fight Against DNS Abuse

Frederick Gaudreau
Surete du Quebec

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

FRANCOPOL

Réseau international francophone de formation policière

« On the Internet, nobody knows you’re a dog »

Peter Steiner, The New Yorker, 5 juillet 1993

POLICE INTERNET

BP 241 Abidjan 01 – police.interpol26@gmail.com – 00225 66 49 38 41

COMMISSION DE CONTROLE ET D'ENQUETE

N/REF : NLCN/12OA/0018/09 FAIT A ABIDJAN LE 22 SEPTEMBRE 2009

L'ACCUSE

Nom :

Prénoms :

Age :

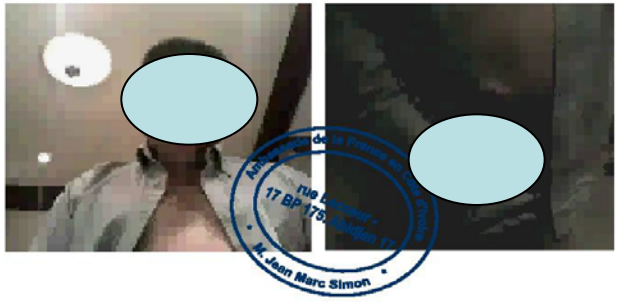
Adresse : @live.fr

@live.fr

Fonction: *Directeur*

Pays : *Canada*

Ville : *Québec*



Au vu des faits provenant de la conversation vidéo que vous avez eu le 21/09/2009 montrant des scènes pornographiques vers le domaine Internet Ivoirien. Nous avons le devoir de vous informer que la commission de contrôle et d'enquête a émis un AVIS D'ORDRE INCRIMINATION à l'encontre de Mr .

En effet, lors du contrôle de la vidéo soumis par notre serveur d'enregistrement, il ressort que la vidéo: CODE InternetQ93798/111355 n'est pas conforme aux normes de procédure de contrôle qu'impose la police Internet dans le cadre de la zone Internet Ivoirienne.

L'avis d'ordre d'incrimination étant déjà en cours vous êtes tenu à verser une amande de CINQ MILLE EUROS (5.000 EUROS). Pour ladite amande avant le 26/09/2009 Faute de quoi, cette présente vidéo sera publiée sur les chaînes d'informations telle que France24-TF1-CNN-YOUTUBE-M6-et bien d'autres. Le Tribunal de Première Instance d'Abidjan-Plateau promulguera un Mandat d'Arrêt International contre vous avec ampliation à l'Ambassade du Canada en Côte d'Ivoire et transmettra votre vidéo à la police nationale du Canada **http://www.rcmp-grc.gc.ca/ncecc-cncee/20090326-fra.htm**

INTERPOL
General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Réalité Africaine / African Reality

- Hausse de l'accessibilité à l'Internet / Increasing Accessibility to the Internet
- Hausse des cybercrimes / Increase in Cybercrime
- Besoins en formation / Need for Training
- Outils / Tools
- COOPÉRATION INTERNATIONALE / INTERNATIONAL COOPERATION

Initiative de formation de Dakar / Dakar Training Initiative

FRANCOPOL

Réseau international francophone de formation policière

Session 1- Latest Developments in the Fight Against DNS Abuse

Gary Kibby
Serious Organized Crime Agency

Criminal DNS Abuse

www.uhtzxyabiyw.com

www.cbahihuayus.com

www.ahpteijxqcj.com

www.gdedkxwghwf.com

www.maifoqxmyus.com

www.jhtiuatzfek.com

www.saikjixybus.com

www.gjiaorykjxw.com

One World

One Internet

Questions

Session 2 - Evolution of Domain Name Take-Downs

Michael Moran
INTERPOL
Rod Rasmussen
Anti-Phishing Working Group
Don Blumenthal
Public Interest Registry
Titi Akinsamni
University of Witwatersrand

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

Session 2 - Evolution of Domain Name Take-Downs

Michael Moran
INTERPOL

ICANN
Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

Session 2 Evolution of Domain Name Take-Downs

Rod Rasmussen
Anti-Phishing Working Group

Abusive Domain Name Resolution Suspension Process

An APWG Cybercrime Intervention Program

Rod Rasmussen

APWG IPC Co-Chair /

Industry Liaison

Purpose of ANDRS Program

- The **ADNRS Process Program** is a trusted-introducer/trusted-channel system that provides a medium for the rapid and contractually governed suspension of abusive domains between an **Accredited Intervener** and a **Registry** where a domain name has been identified as a tool of criminal enterprise
- Designed to enhance speed and scalability of interventions and provide tracking and auditing of suspension request and subsequent suspensions

Domains Eligible for Suspension

- For use only with maliciously registered domains, i.e. domains registered specifically to perpetrate phishing, malware distribution, or other crimes
  - About 12,000 such domains registered worldwide per year for phishing
  - Much larger problem with malware
- Not for use with compromised/hacked domains
  - 83% of domains used for phishing
- Indicators of bad intent include:
  - Domain registered recently
  - Suspect WHOIS data
  - The bad domain strives to spoof a financial institution's legitimate domain, or mimic well-known banking keywords.
  - No legitimate content ever associated with the domain.
  - Uses nameservers of ill repute (usually 100%) for previous fraudulent domains.

Old-Fashioned Domain Name Resolution Suspension Request

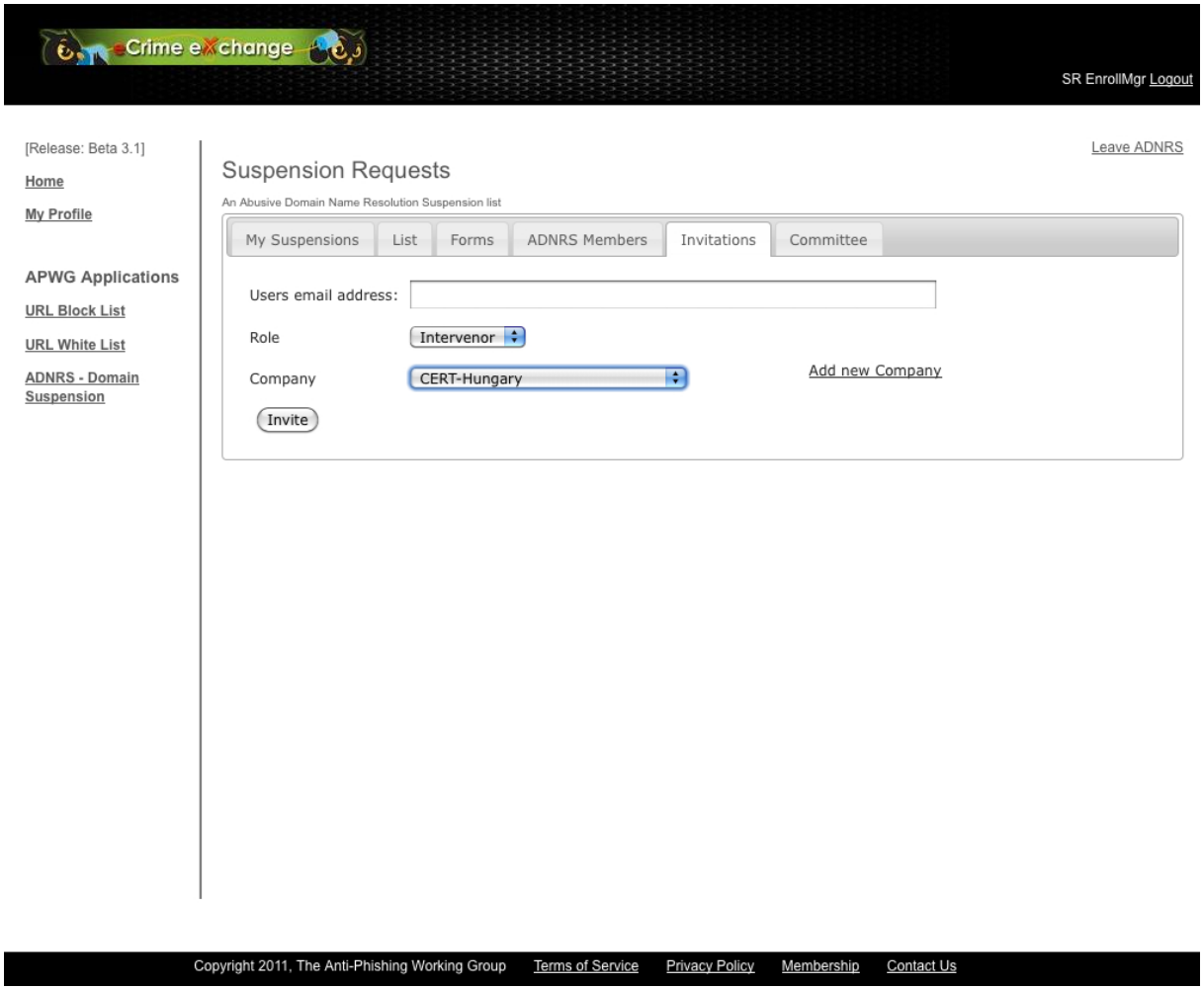
* Artist's rendering of traditional domain name suspension request

- Ad hoc email or phone call made between parties that may or may not know each other and probably don't have clear, shared criteria for suspension
- Risk laden by its nature
- Not auditable – so not a business process by definition

APWG Abusive Domain Name Resolution Suspension Process

- Replaces *ad hoc* communications between interveners and Registrys mediating domain name resolution suspension requests
- Process animates a formal trusted introducer/trusted channel scheme with audit trails
- Governed process will engender trust and routine use between non-correspondent entities
- With that trust, APWG hopes, will come scaling of process and conclusive impact in deterring abuse of the DNS

ADNRS @ Beta 3.1

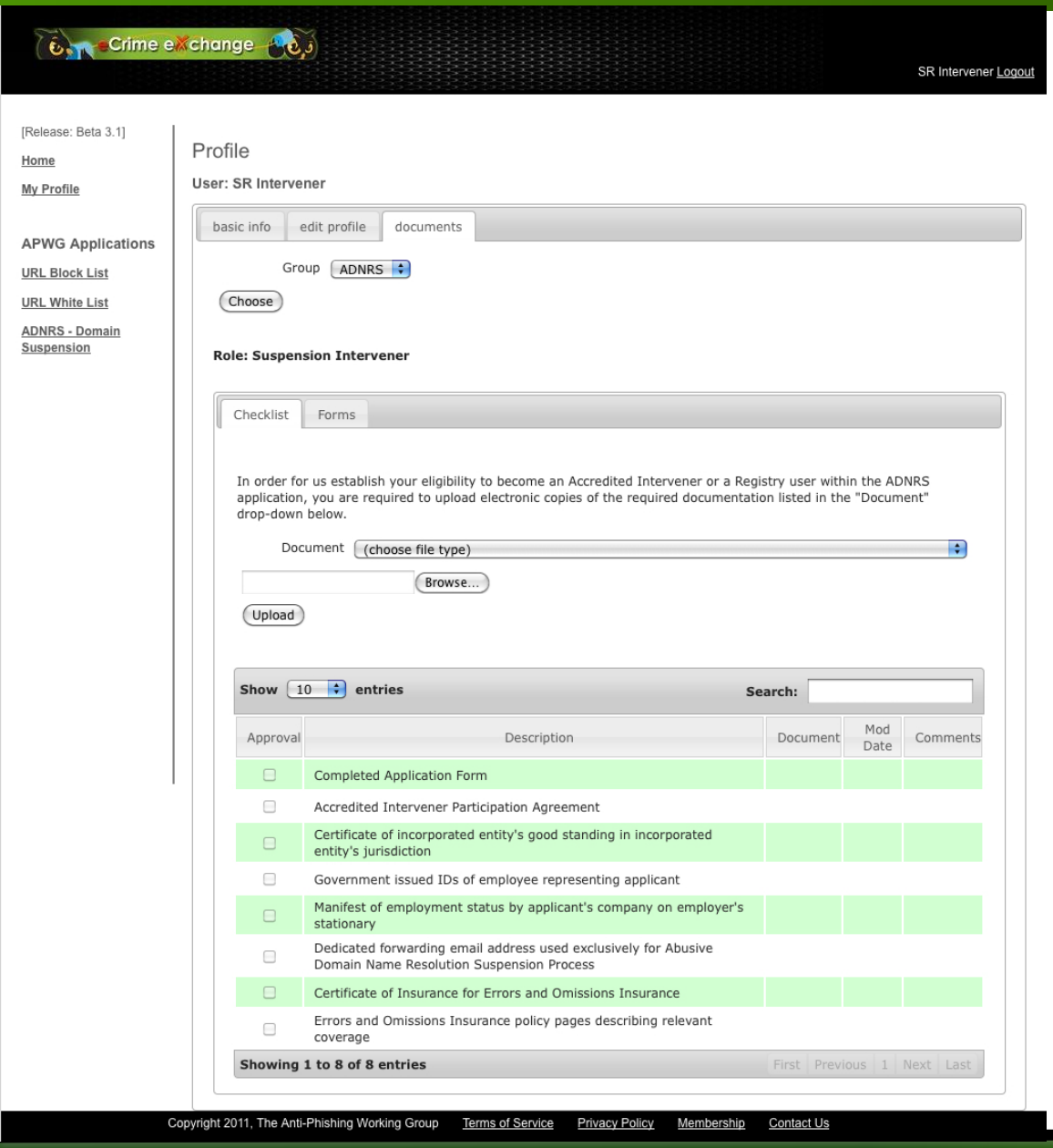


- Core application functions in place
  - Just added accreditation committee review component to vet applicants
- Working toward a Nov. 7 working Beta launch at APWG con-ference in San Diego
- Working with APWG members and research partners to bring ADNRS to operational tempo

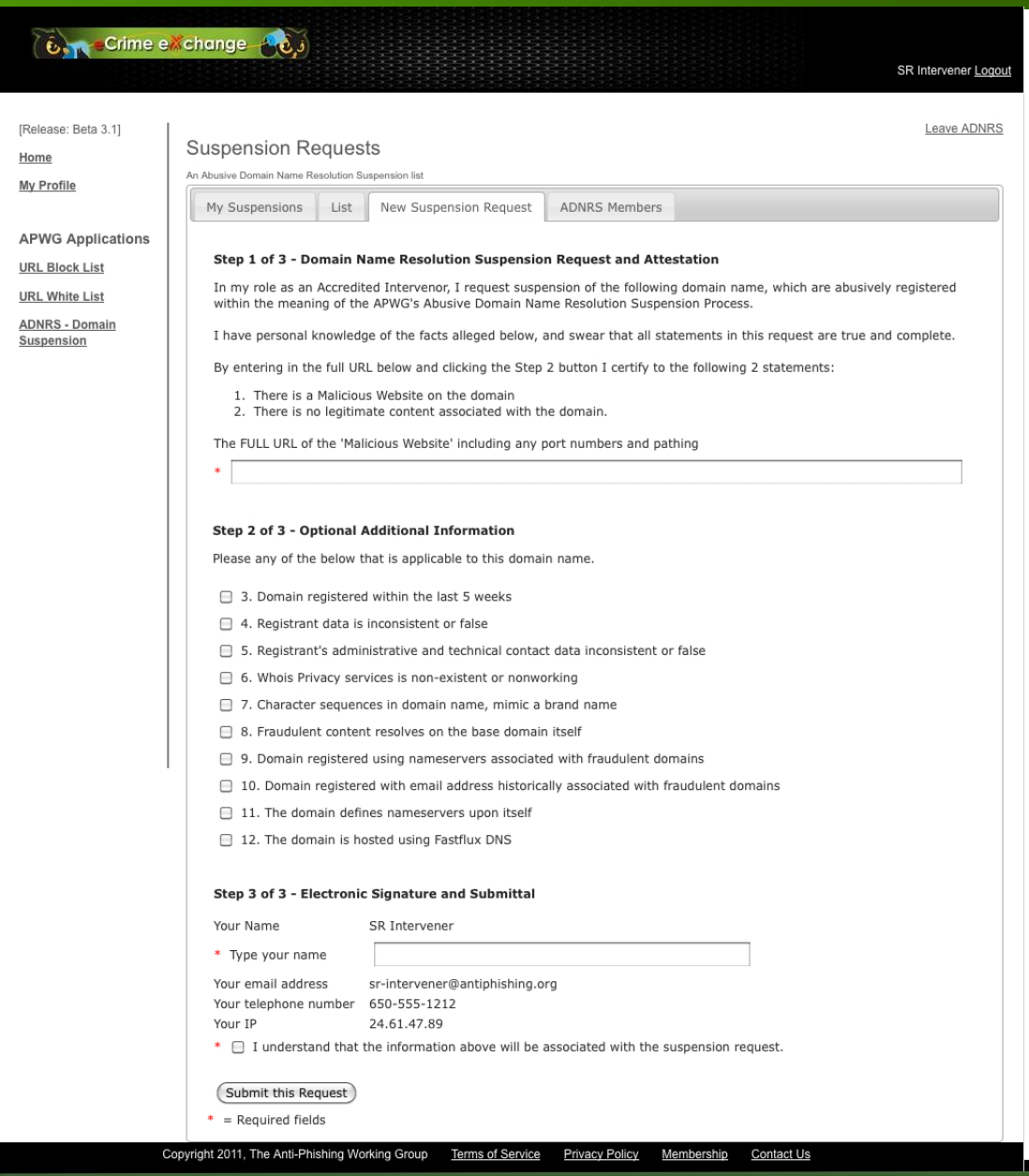
ADNRS Functional Overview

- Trusted Introducer scheme that gives Registries confidence the suspension requests are from party with history and capacity to examine and judge criminality of domain names
- Employs explicit criteria that can be tested by Registries before making a decision on suspension request
- Establishes formal, auditable communications channel between Accredited Intervener and Registry

Applicant View



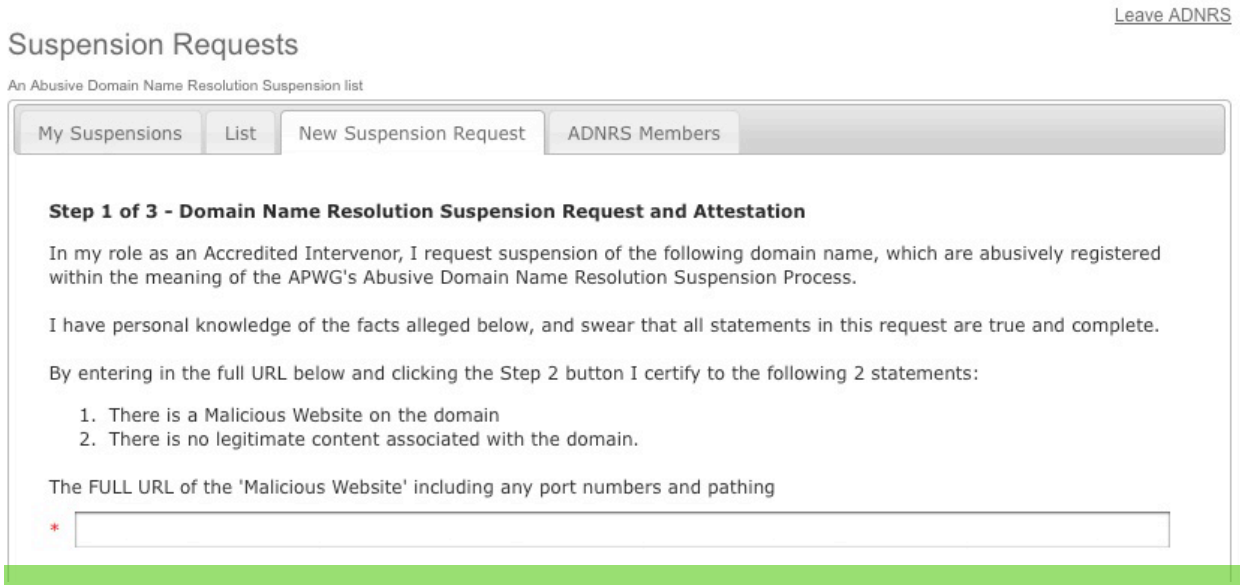
- Enrollment Manager (EM) vets applicant's qualifications and credential against criteria for participation
  - Proof of corporate standing
  - Applicant's employee credentials
  - Completed application
  - Completed user agreement
- Two ANDRS User Roles:
  - Accredited Intervener
  - Registry
- EM authenticates supporting documentation provided by the ADNRS applicants
- If successfully authenticated, EM ships completed application with data about applicant company's history and operational capacities to the Accreditation Committee for approval or rejection



Intervener View

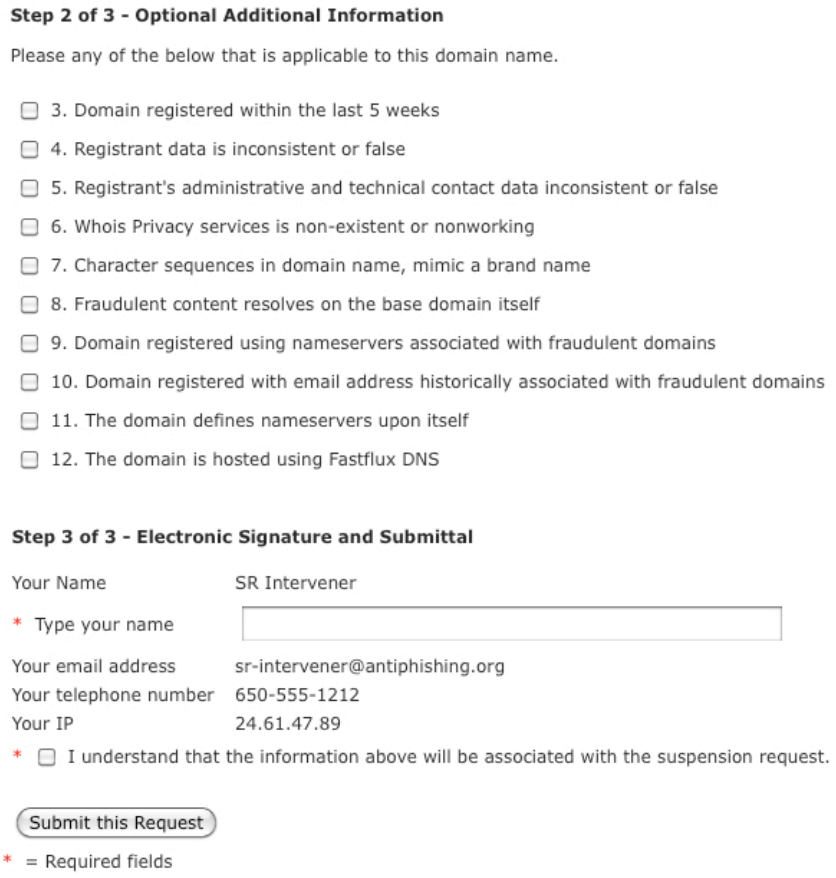
- ANDRS Process requires formal, signed attestations for suspension
- Attestation provides rich report data and manifests identity of the Intervener as a vetted and accredited reporter and responder
- Design architecture based around the central imperative: first, do no harm

Domain Name Resolution Suspension Request and Attestation



- **The Accredited Intervener attestation form requires, at minimum, the satisfaction of two primary criteria:**
  - ***Malicious content on the domain***
  - ***No legitimate content associated with the domain***

Domain Name Resolution Suspension Request and Attestation



Step 2 of 3 - Optional Additional Information

Please any of the below that is applicable to this domain name.

- [ ] 3. Domain registered within the last 5 weeks
- [ ] 4. Registrant data is inconsistent or false
- [ ] 5. Registrant's administrative and technical contact data inconsistent or false
- [ ] 6. Whois Privacy services is non-existent or nonworking
- [ ] 7. Character sequences in domain name, mimic a brand name
- [ ] 8. Fraudulent content resolves on the base domain itself
- [ ] 9. Domain registered using nameservers associated with fraudulent domains
- [ ] 10. Domain registered with email address historically associated with fraudulent domains
- [ ] 11. The domain defines nameservers upon itself
- [ ] 12. The domain is hosted using Fastflux DNS

Step 3 of 3 - Electronic Signature and Submittal

Your Name	SR Intervener
* Type your name	
Your email address	sr-intervener@antiphishing.org
Your telephone number	650-555-1212
Your IP	24.61.47.89

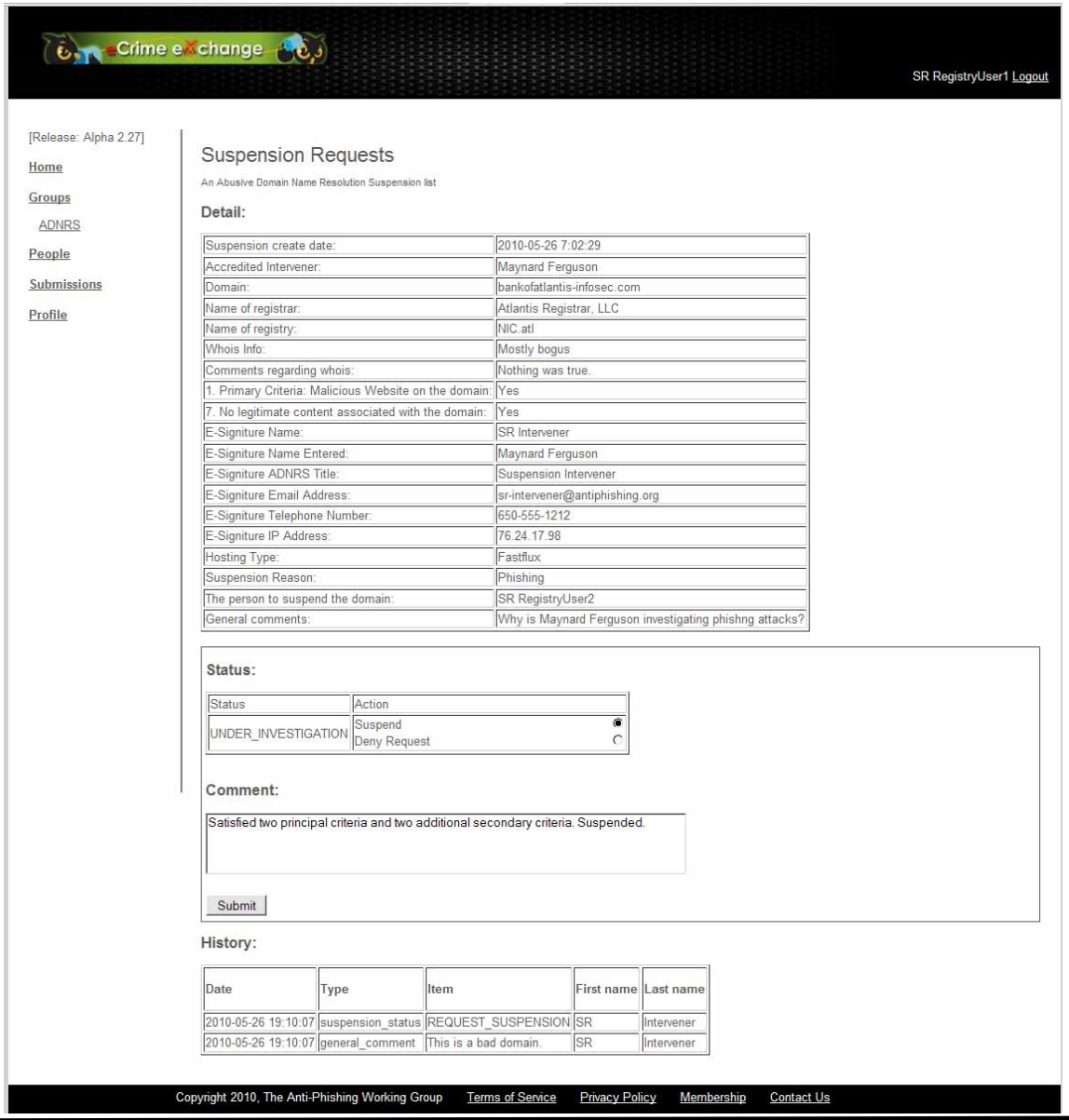
* [ ] I understand that the information above will be associated with the suspension request.

Submit this Request

* = Required fields

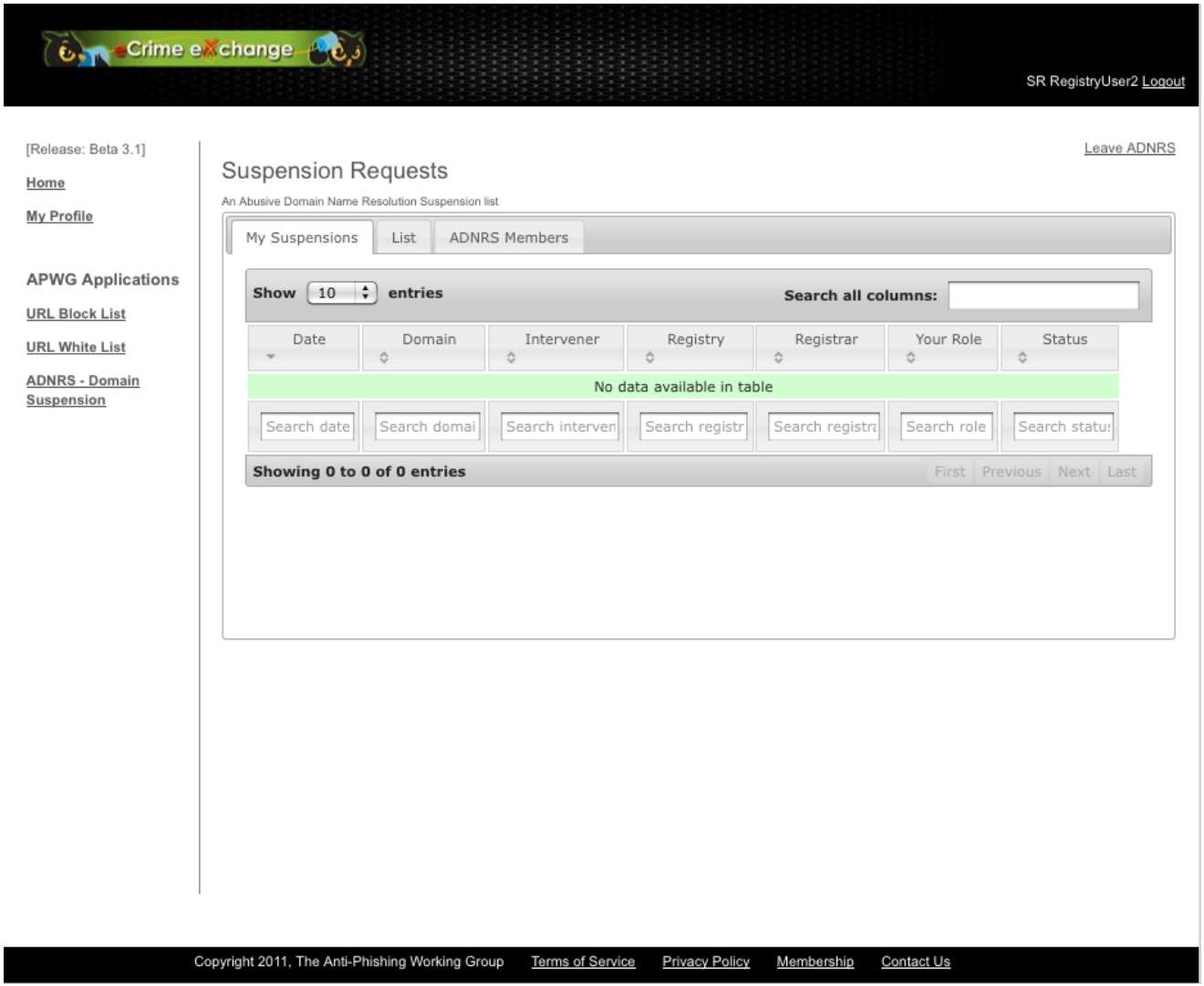
- **The Attestation provides additional characteristics of a domain name for the Registry to consider, besides the primary criteria**
- **To come: file loading mechanism for malware samples and screen shots**

Registry View



- Registry user notified that a suspension request is waiting at the eCX
- Reads the attestation and examines criteria cited in the submission
- Can reject, suspend or request more information from the Accredited Intervener

Registry View



- Registry user console tracks Resolution Suspension Requests
- ADNRS Process application archives each request in a recallable record with complete transaction and comment history
- Over time, records can yield insights into malicious domain registrations

New-Fashioned Domain Name Suspension Request Process

- Rigorous
- Routinizable
- Scalable
- Auditable

Join up for the Beta program today!

Contact: Peter Cassidy
pcassidy@apwg.org

Session 1- Latest Developments in the Fight Against DNS Abuse

Don Blumenthal
Public Interest Registry

Session 2 - Evolution of Domain Name Take-Downs

Titi Akinsamni
University of Witwatersrand
South Africa

One World

One Internet

Questions

ICANN

Dakar

SÉNÉGAL

N°42 23 - 28 October 2011

Thank You

ICANN

Dakar

SÉNÉGAL

N°42 23 - 28 October 2011