

Forum on DNS Abuse

Nii Narku Quaynor
Moderator

24 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**



Session 1- Latest Developments in the Fight Against DNS Abuse

Pierre Danjineau
INFOCOM



Session 1- Latest Developments in the Fight Against DNS Abuse

Lanre Ajaya
Pinet Informatics



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**



Session 1- Latest Developments in the Fight Against DNS Abuse

Frederick Gaudreau
Surete du Quebec





F
RANCOPOL

Réseau international francophone de formation policière



"On the Internet, nobody knows you're a dog."

« 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/120A/0018/09

FAIT A ABIDJAN LE 22 SEPTEMBRE 2009

L'ACCUSE

Nom :

Prénoms :

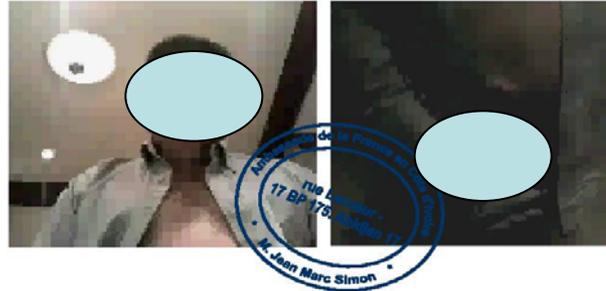
Age :

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-cnccc/20090326-fra.htm>



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



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



Questions

One World

One Internet



Dakar
SÉNÉGAL
N°42 🇸🇳 23 - 28 October 2011

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



Session 2 - Evolution of Domain Name Take-Downs

Michael Moran
INTERPOL



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



Unifying the
Global Response
to Cybercrime

Purpose of ANDRS Program

- The **ANDRS 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 Registries 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

[Release: Beta 3.1] [Leave ADNRS](#)

[Home](#)
[My Profile](#)

APWG Applications
[URL Block List](#)
[URL White List](#)
[ADNRS - Domain Suspension](#)

Suspension Requests
An Abusive Domain Name Resolution Suspension list

[My Suspensions](#) | [List](#) | [Forms](#) | [ADNRS Members](#) | [Invitations](#) | [Committee](#)

Users email address:

Role:

Company: [Add new Company](#)

SR EnrollMgr [Logout](#)

Copyright 2011, The Anti-Phishing Working Group [Terms of Service](#) [Privacy Policy](#) [Membership](#) [Contact Us](#)

- Core application functions in place
 - Just added accreditation committee review component to vet applicants
- Working toward a Nov. 7 working Beta launch at APWG conference 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 ANDRS 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

[Release: Beta 3.1]

[Home](#)[My Profile](#)

APWG Applications

[URL Block List](#)[URL White List](#)[ADNRS - Domain Suspension](#)

Profile

User: SR Intervener

basic info | edit profile | documents

Group: **ADNRS**[Choose](#)

Role: Suspension Intervener

Checklist | Forms

In order for us establish your eligibility to become an Accredited Intervener or a Registry user within the ADNRS application, you are required to upload electronic copies of the required documentation listed in the "Document" drop-down below.

Document: (choose file type)

 [Browse...](#)[Upload](#)

Show 10 entries

Search:

Approval	Description	Document	Mod Date	Comments
<input type="checkbox"/>	Completed Application Form			
<input type="checkbox"/>	Accredited Intervener Participation Agreement			
<input type="checkbox"/>	Certificate of incorporated entity's good standing in incorporated entity's jurisdiction			
<input type="checkbox"/>	Government issued IDs of employee representing applicant			
<input type="checkbox"/>	Manifest of employment status by applicant's company on employer's stationary			
<input type="checkbox"/>	Dedicated forwarding email address used exclusively for Abusive Domain Name Resolution Suspension Process			
<input type="checkbox"/>	Certificate of Insurance for Errors and Omissions Insurance			
<input type="checkbox"/>	Errors and Omissions Insurance policy pages describing relevant coverage			

Showing 1 to 8 of 8 entries

[First](#) [Previous](#) 1 [Next](#) [Last](#)

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

[Release: Beta 3.1]

[Leave ADNRS](#)[Home](#)[My Profile](#)

APWG Applications

[URL Block List](#)[URL White List](#)[ADNRS - Domain Suspension](#)

Suspension Requests

An Abusive Domain Name Resolution Suspension list

My Suspensions List New Suspension Request ADNRS Members

Step 1 of 3 - Domain Name Resolution Suspension Request and Attestation

In my role as an Accredited Intervener, I request suspension of the following domain name, which are abusively registered within the meaning of the APWG's Abusive Domain Name Resolution Suspension Process.

I have personal knowledge of the facts alleged below, and swear that all statements in this request are true and complete.

By entering in the full URL below and clicking the Step 2 button I certify to the following 2 statements:

1. There is a Malicious Website on the domain
2. There is no legitimate content associated with the domain.

The FULL URL of the 'Malicious Website' including any port numbers and pathing

*

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.

* = Required fields

Domain Name Resolution Suspension Request and Attestation

[Leave ADNRS](#)

Suspension Requests

An Abusive Domain Name Resolution Suspension list

My Suspensions List New Suspension Request ADNRS Members

Step 1 of 3 - Domain Name Resolution Suspension Request and Attestation

In my role as an Accredited Intervener, I request suspension of the following domain name, which are abusively registered within the meaning of the APWG's Abusive Domain Name Resolution Suspension Process.

I have personal knowledge of the facts alleged below, and swear that all statements in this request are true and complete.

By entering in the full URL below and clicking the Step 2 button I certify to the following 2 statements:

1. There is a Malicious Website on the domain
2. There is no legitimate content associated with the domain.

The FULL URL of the 'Malicious Website' including any port numbers and pathing

*

- 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

Crime eXchange
SR RegistryUser1 Logout

[Release: Alpha 2.27]

[Home](#)
[Groups](#)
[ADNRS](#)
[People](#)
[Submissions](#)
[Profile](#)

Suspension Requests

An Abusive Domain Name Resolution Suspension list

Detail:

Suspension create date:	2010-05-26 7:02:29
Accredited Intervener:	Maynard Ferguson
Domain:	bankofatlantis-infosec.com
Name of registrar:	Atlantis Registrar, LLC
Name of registry:	NIC.atl
Whois Info:	Mostly bogus
Comments regarding whois:	Nothing was true.
1. Primary Criteria: Malicious Website on the domain:	Yes
7. No legitimate content associated with the domain:	Yes
E-Signature Name:	SR Intervener
E-Signature Name Entered:	Maynard Ferguson
E-Signature ADNRS Title:	Suspension Intervener
E-Signature Email Address:	sr-intervener@antiphishing.org
E-Signature Telephone Number:	650-555-1212
E-Signature IP Address:	76.24.17.98
Hosting Type:	Fastflux
Suspension Reason:	Phishing
The person to suspend the domain:	SR RegistryUser2
General comments:	Why is Maynard Ferguson investigating phishing attacks?

Status:

Status	Action
UNDER_INVESTIGATION	Suspend <input checked="" type="radio"/>
	Deny Request <input type="radio"/>

Comment:

Satisfied two principal criteria and two additional secondary criteria. Suspended.

History:

Date	Type	Item	First name	Last name
2010-05-26 19:10:07	suspension_status	REQUEST_SUSPENSION	SR	Intervener
2010-05-26 19:10:07	general_comment	This is a bad domain.	SR	Intervener

Copyright 2010, The Anti-Phishing Working Group [Terms of Service](#) [Privacy Policy](#) [Membership](#) [Contact Us](#)

- 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

The screenshot displays the 'Registry View' interface for 'Suspension Requests'. At the top left is the 'Crime eXchange' logo. The user is logged in as 'SR RegistryUser2' with a 'Logout' link. The page title is 'Suspension Requests' and it is described as 'An Abusive Domain Name Resolution Suspension list'. There are tabs for 'My Suspensions', 'List', and 'ADNRS Members'. The 'List' tab is active, showing a table with columns: Date, Domain, Intervener, Registry, Registrar, Your Role, and Status. The table is currently empty, displaying 'No data available in table'. There are search filters for each column and a 'Show 10 entries' dropdown. The footer contains copyright information for 2011, The Anti-Phishing Working Group, and links to Terms of Service, Privacy Policy, Membership, and Contact Us.

- 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



Questions

One World

One Internet



Dakar
SÉNÉGAL
N°42 🇸🇳 23 - 28 October 2011

Thank You

