APWG

APWG Malicious Domain Suspension Process
Application Briefing Memo

A governed process for suspending maliciously registered domains securely, prudently, and with manageable scale

The APWG Malicious Domain Suspension (AMDoS) system enables specially accredited Interveners to submit suspected malicious domain names for investigation and suspension by Sponsoring Registrars and Top-Level Domain Registries.

Closely allied with governance bodies and corporate operational directorates responsible for brand integrity and remote channel security, the APWG was able to navigate the security and legal challenges that domain suspensions need to address in the development of its AMDoS application.

AMDoS orders and systematizes suspension requests through a formal process that ensures the credibility of malicious domain reporters and integrity of their suspension requests – and speeds them on their way to the Registrars of record.

APWG vets malicious domain reporters (Accredited Interveners) with the vigor and diligence required for a responder with such potent authority.

Although the AMDoS process safe-guards against error, it still affords quick action in the suspension of a malicious site, matching cybercrime's speed.

The AMDoS process application manages suspension requests through a formal, auditable process that:

1. Establishes common criteria for defining malevolent domain names eligible for suspension.

2. Examines and confirms *bona fides* of Accredited Interveners regarding their institution's capacity to judge consistently the character of a domain name against set criteria;

3. Provides an auditable platform for submission of suspension requests by Accredited Interveners that formalizes communications between them and Sponsor Registrars and Registries;

4. Presents Attestations from known parties to Registrars and Registries for voluntarily judgment based on clearly articulated and verifiable testimony describing a violation of a Terms of Service Agreement.

Accredited Interveners

The AMDoS security process begins with vetting of our Accredited Interveners. The accreditation process for Interveners of AMDoS is stringent. APWG vets each applicant, intervener via an extensive application process. Applicant interveners, are subject to an expert committee review for accreditation before they can access the AMDoS application.

In order to be considered for application as an Accredited Intervener, applicants are stepped through a pre-screening process to establish the applicant institution's eligibility.

After the initial beta period, candidates will be required to be a member in good-standing of APWG and must work for an enterprise elevant to the management and investigation of cybercrime. A request for application is made to our Enrollment Manager, who then determines a candidates eligibility for enrollment.

Accredited Interveners are fully vetted employees of vetted APWG member organizations

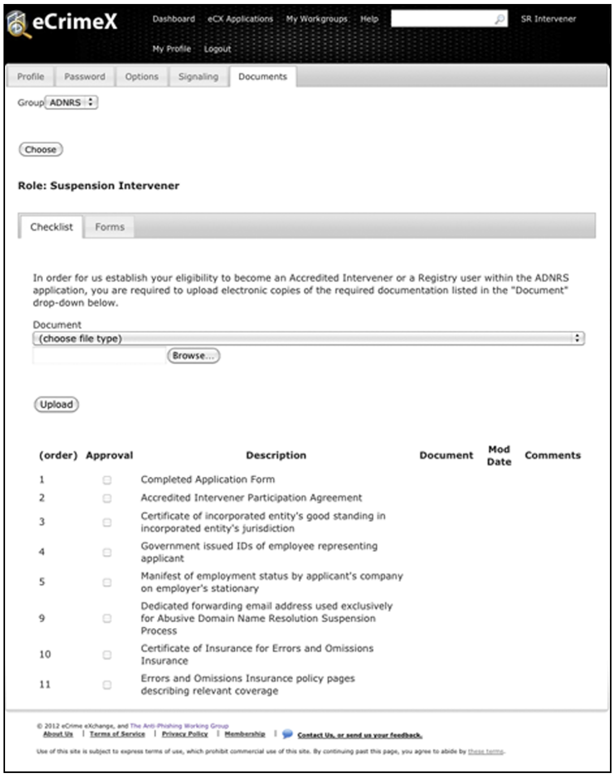
Once a candidate has passed this pre-screening process, they must complete a formal application [Figure 1] and provide proof of valid incorporation and other documentation, which the AMDoS Accreditation Committee reviews. Once the candidate satisfies these requirements, their application is put to a committee vote.

The AMDoS committee is made up of the top-level APWG officers and members from a number of industrial and civil sectors that engage cybercrime as a daily management assignment.

Registrar & Registry Users

Likewise, Registrars and Registry Users are stepped through an application process to confirm *bona fides* of the applicant and NOC/SOC level of correspondence and commensurate authority within the enterprise.

Once the AMDoS Enrollment Manager admits an intervener or registry applicant to the AMDoS, their institutions will have access to the AMDoS user console and be able to complete a *Domain Name Resolution Suspension Request and Attestation* [Figure 2] (if an intervener) and (if a Registry User) access and manage those suspension requests records on the AMDoS console relating to their domain spaces.



Role: Suspension Intervener

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)

(order)	Approval	Description	Document	Mod Date	Comments
1	□	Completed Application Form			
2	□	Accredited Intervener Participation Agreement			
3	□	Certificate of incorporated entity's good standing in incorporated entity's jurisdiction			
4	□	Government issued IDs of employee representing applicant			
5	□	Manifest of employment status by applicant's company on employer's stationary			
9	□	Dedicated forwarding email address used exclusively for Abusive Domain Name Resolution Suspension Process			
10	□	Certificate of Insurance for Errors and Omissions Insurance			
11	□	Errors and Omissions Insurance policy pages describing relevant coverage			

© 2012 eCrime eXchange, and The Anti-Phishing Working Group
About Us | Terms of Service | Privacy Policy | Membership | Contact Us, or send us your feedback.
Use of this site is subject to express terms of use, which prohibit commercial use of this site. By continuing past this page, you agree to abide by these terms.

Figure 1

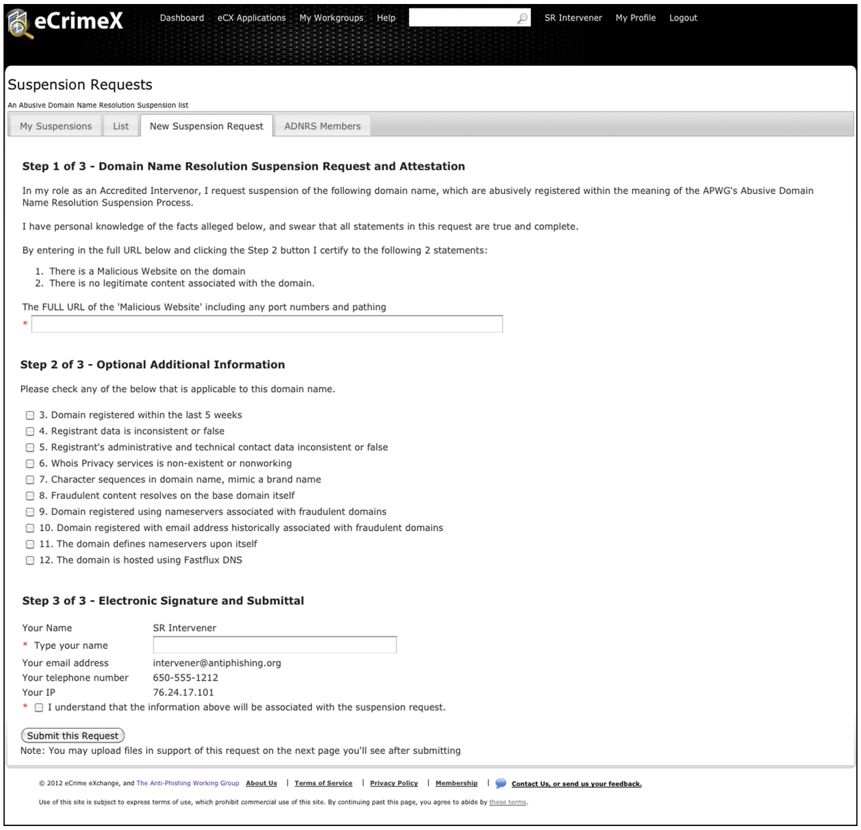
For more information about how to become an Accredited Intervener, please visit our web site: www.ecrimex.net

In Place Of Ad Hoc Correspondence, a Governed and Auditable Process

When an Accredited Intervener creates a new Suspension Request by supplying the required information via the *Domain Name Resolution Suspension Request and Attestation* page [Figure 2] in AMDoS, the system populates the new suspension request with the data from a domain name WHOIS data query, if they can be retrieved.

After being signed and submitted, the AMDoS system allows the Accredited Intervener to upload supporting documents such as screenshots and attach them to the attestation.

AMDoS automatically distributes the request and attestation to the relevant Registry based on the Top-Level Domain (TLD) identified in the request. (If a Registry User from the TLD is enrolled on AMDoS, it will be forwarded to that user; if not, AMDoS will perform a look-up in GNSO data and forward a notification of interest by an Accredited Intervener to the Registry's Technical Contact email address notifying the Registry a suspension request has been filed on a domain name in its TLD space.)



Suspension Requests

An Abusive Domain Name Resolution Suspension list

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

In my role as an Accredited Intervenor, 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 check 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	intervener@antiphishing.org
Your telephone number	650-555-1212
Your IP	76.24.17.101

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

Note: You may upload files in support of this request on the next page you'll see after submitting

© 2012 eCrime eXchange, and The Anti-Phishing Working Group

Use of this site is subject to express terms of use, which prohibit commercial use of this site. By continuing past this page, you agree to abide by these terms.

Figure 2

Thereafter, the Accredited Intervener can track the progress of the request from the *My Suspensions* list, and determine if a domain name has previously been reported by searching the list of all Suspension Items in the system.

Registry Users automatically see Attestations assigned to their TLDs in their own *My Suspensions* list.

With a click on the record, the Accredited Intervener's personnel can assign Team Members to manage the record or to advance the processing of the suspension request and attestation.