Registration Abuse Policies Working Group – Definitions
Version 31 March 2009

ABUSE

Original proposal:
Malicious or wrongful use causing harm or potential harm to registrants and Internet users.

Variations suggested on the RAP WG Conference Call (30 March) and Adobe Connect:

a) Malicious or *illegal* use causing harm to registrants and Internet users
b) Malicious or *fraudulent* use causing harm or potential harm to registrants and Internet users
c) Malicious or *fraudulent* use causing harm or *intended* harm to registrants and Internet users
d) Conduct which uses a domain name or IP address to cause harm or potential harm *to any third party*
e) Malicious or *fraudulent* use causing harm or *undue* harm to registrants and Internet users
f) To treat in a harmful, injurious or offensive way
g) *Conduct with no legitimate use or purpose which uses a domain name or IP address to cause* harm or potential harm *to any third party*
h) Malicious or wrongful use causing harm or potential harm to *third parties*
i) Malicious or wrongful use causing harm or potential harm to *the Internet Community*
j) *An activity that imposes negative (economic or other) effects upon another party*

k) Misuse is an action that causes actual harm, is the predicate to such harm, is illegal or illegitimate, or is otherwise considered contrary to intention and design of a stated legitimate purpose, if such purpose is disclosed. (from the Whois Draft Working Definitions prepared by the GNSO drafting team)

Questions raised: How to judge intent? Should intent be part of the definition of abuse? How do you deal with conduct / technologies that are not malicious by nature, but become abusive in the way they are being used (intent) e.g. fast flux? Should a definition include who is targeted by the abuse? How do you qualify harm or potential harm? How can harm be further defined?

Category: Pre-registration abuse

Type	Definition	Primary Target	Legitimate use (Y/N)	Requires DNS System[1] (Y/N)	RAPWG scope (Y/N)?
Malware/botnet control	Pre-designation of domain names to control malware (e.g. Conficker example).	Consumers			
Name spinning	Automated tools used to create domain permutations.	Consumers			

Category: Registration abuse

Type	Definition	Primary Target	Legitimate use (Y/N)	Requires DNS System (Y/N)	RAPWG scope (Y/N)?
Cybersquatting	Trademark (or variation) in domain name. Domain bought/owned for the purpose of reselling or use in malicious activity.	Brand owners			
Mass/automated registration abuse	Automated tools used to register bulk domains.	Brand owners/con-sumers			
False WHOIS	Registrations using false/incorrect contact information.	Trademark owners/con-sumers			
Domain Front Running	Domain name front running is the practice whereby a domain name registrar uses insider information (such as from availability searches) to register domains .By registering the domains, the registrar locks out other potential registrars from selling the domain to a	Registrants			

[1] Does this type of abuse require the domain name system (i.e. registering a domain name) or could it also function without it e.g. by using IP resolution?

	customer.				
Inappropriate use of WHOIS	Using WhoIs information for mass marketing purposes and solicitations	Consumers			

Category: Post-registration abuse

Type	Definition	Primary Target	Legitimate use (Y/N)	Requires DNS System (Y/N)	RAPWG scope (Y/N)?
Phishing	Web sites purporting to be a trusted brand in order to acquire sensitive in formation from consumers (e.g. online banking credentials, email passwords).	Consumers			
Phishing emails	Emails distributed to direct victims to phishing websites or to gather sensitive information from consumers.	Consumers			
Malware websites	Web sites used to deploy malware.	Consumers			
Malware emails	Care - not usually new domains (simply use free ISP services) but some utilise specific domains, depicting the brand.	Consumers			
Pharming	Redirecting internet users to malicious sites to capture sensitive information.	Consumers			
419/Lottery/Domain names/scam emails	Care - not usually new domains (simply use free ISP services) but some utilise specific domains, depicting the brand.	Consumers			
Spam	Domain used to send out unsolicited emails in bulk.	Consumers			
Pay-per-click	Use of trademark in domain to draw traffic to site containing paid placement advertising.	Brand owner			
Traffic Diversion	Use of brands in visible text, hidden text, meta tags and title to manipulate	Brand owner			

	search engine rankings and divert traffic.				
Offensive	Website containing adult and/or pornographic content using trademark within domain.	Brand owner			
Domain kiting	Abuse of the five-day grace period to register, delete and immediately re-registering domains with the end result of having the domain registered without ever actually paying for it.	Registry			
Domain tasting	Registrant using the Add Grace Period at the beginning of the registration to test the marketability of the domain	Registry			
Gripe/Commentary Site	Complaint/forum site with trademark in domain name.	Brand owner			
Command & Control domains/botnets	Control of infected machines to facilitate malicious behaviour , providing scalability.	Consumers			
Fast Flux	DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.	Consumers			
Counterfeit	Web sites used to sell counterfeit goods.	Consumers			
False affiliation	Website that is falsely purporting to be an affiliate of brand.	Consumers			
Unauthorized or improper use of brand/logo in website	Unauthorized or improper use of brand/logo in website.	Brand owner			
Gripe/Commentary Site	Complaint/forum site; site may use branding such as logo and/or discuss proprietary information.	Brand owner			
Offensive	Website containing adult and/or	Consumers			

	pornographic content using trademark within content of site.				

Category: Domain name use abuse

Type	Definition	Primary Target	Legitimate use (Y/N)	Requires DNS System (Y/N)	RAPWG scope (Y/N)?
Fake renewal notices	Correspondence sent to registrants from fake registrar in order to claim renewal fees.	Registrants			
Domain phishing	Phishing targeting registrants for domain name service credentials to hijack domains (could be malware too).	Registrants			
Renewal/transfer abuse	Registrar targeted by third-party purporting to be registrant in order to amend/transfer domain.	Registrar			