Anti-Abuse Policy

The following policy (“.berlin Anti-Abuse Policy") is announced pursuant to the Registry-Registrar-Agreement (“RRA”) and is effective upon thirty days' notice by dotBERLIN GmbH & Co. KG (“Registry”) to Registrars. Abusive use(s) of .berlin domain names should not be tolerated.

The policy includes the general aspects of anti-abuse, acceptable use and rapid takedown and applies to registrars and registrants of .berlin domain names and defines how the Registry will proceed if abuses that are reported to the Registry. The policy does not replace the Uniform Dispute Resolution Policy (UDRP) or Uniform Rapid Suspension (URS) or other proceedings for disputes.

The Registry intends that no domain name in the .berlin gTLD shall be used in a manner (acceptable use) which, infringes any other third party’s rights, is in breach with any applicable laws, government rules or requirements or for the purposes of undertaking any illegal or fraudulent actions, including spam or phishing activities. Failure to comply with the above provisions may result in the suspension or termination of the domain name registration by the Registry.

The Registry, together with the Registry-Service-Provider, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the .berlin namespace. The specific measures include, but are not limited to an Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse, committing to rapid identification and resolution of abuse (rapid takedown), including suspensions, ensuring completeness of WHOIS information at the time of registration, publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

Abusive activities during the operation of a gTLD registry system can be categorized as follows:

- Abusive registrations of names under a gTLD.
- Abusive use of a domain name under that gTLD („Malicious Use“)
- Abuse of the registration processes, the technical interfaces, infrastructure of the Registry systems and the DNS network itself.

With respect to the first (and also parts of the second) category, ICANN’s “RAP” WG (Registration Abuse Policies Working Group) has produced an illustrative categorization of known abuses in their “Registration Abuse Policies Working Group Final Report” (http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf, dated 29 May 2010). The anti-abuse measures of the .berlin gTLD registry largely follow the RAPWG’s recommendations for the individual abuse scenarios. More details on the individual countermeasures are included below.

Furthermore, the proposed registry also takes into consideration the ICANN Security and Stability Advisory Committee’s document “SAC 048” (“SSAC Comment on Orphan Glue Records in the Draft

Applicant Guidebook") as well as "SAC 023" ("Is the WHOIS Service a Source for email Addresses for Spammers?").

General Provisions against Abuse under the .berlin gTLD

Legal Safeguards

To meet the requirements of ICANN to a community-based designation of the application, the registrant must use a .berlin domain name in an economic, cultural, social or any other meaningful connection to the City of Berlin.

This designation of .berlin to the .berlin Community will be enforced by specific language in the Registry-Registrar-Agreement that holds gTLD Registrars responsible to include the restrictions as outlined above in respective agreements with their gTLD registrants.

The Registry will, from time to time in its sole discretion or upon evidence or advice manually conduct continuing or recurring audits of domain names registered to ensure continued compliance with these requirements. Failure to comply will result in a notice providing 20-days to comply. Non-compliance following such a notice period may result in take-down of the relevant domain name, at the discretion of the Registry.

WHOIS Accuracy Measures

In parallel to auditing .berlin domain names for compliance with the eligibility requirements as outlined in 2.1, any such domain names will simultaneously also be checked for the accuracy of their WHOIS data.

Abuse Contact and Abuse Handling Provisions

The .berlin registry operator will establish and publish a single abuse point of contact on its website. This contact is responsible for addressing matters requiring expedited attention and for providing a timely response to abuse complaints concerning all names registered in the .berlin, through all registrars of record, including those involving a reseller.

The contact information for the abuse contact will consist of:

- an email address
- a phone number
- the postal address of the abuse contact (offices of the Registry)

Communication submitted to the abuse contact will be handled as follows:

- review inbound communication for new abuse requests and/or ongoing cases
- treat remaining communication such as spam or non-applicable requests (e.g. for domains in other TLDs) appropriately, e.g. by discarding or rejecting it
- identify registrar of respective domain

- provide a preliminary response to the request's originator
- approach registrar of record with the abuse case
- track abuse handling measures of registrar
- respond to originator with the outcome

Confirming receipt of communication and forwarding third-party communication is regularly handled during business hours, but after 24 hours at the latest. The initial time frame for the registrar of record to complete its abuse handling measures is 72 hours. Exceptionally and only at a registrar's request this can be extended by another 24 hours. Details will be specified in the Registrar Accreditation Agreement.

Potential Registration Abuse Categories and Countermeasures

As outlined above ICANN's RAPWG has identified a number of potential abuse categories (see chapter 5 of their document). These correspond to the first bullet point of the potential abuses of a Registry as listed in section 1 above ("Abusive Registrations"). The proposed registry system addresses these individual categories as follows:

Cybersquatting

Abuses from cybersquatting cases in the proposed .berlin will be addressed by using ICANN's existing and well know Uniform Dispute Resolution Process ("UDRP"). However, registry staff will also closely follow developments regarding Rights Protection Mechanisms within ICANN and will investigate potential paths towards adoption of such processes once they are clearly defined for the .berlin registry space.

Front-Running

Even though the RAPWG does not recommend any specific action regarding this issue, the proposed registry will a) treat all logfiles and any other information that reflects user interests in a particular domain name as confidential. Such data and log information will only be available to staff with actual operational requirements to access those files, and b) will include a respective provision in the gTLD's registrar accreditation agreement.

Gripe Sites; Deceptive and Offensive Domain Names

The gTLD registry will – in accordance with its contract with the City of BERLIN – develop best practices to restrict the registration of offensive strings. Additionally, it is believed that the existing UDRP, in addition to court decisions (which the registry will obviously be bound by) provides sufficient, independent action against such potentially abusive names.

Fake Renewal Notices

The registry will not, in line with the RAPWG's recommendations, implement any specific countermeasure within its registry systems and services. As the registry is required to provide

accurate and complete WHOIS information for all domain names (which is believed to be the information source for such notices) it is not feasible to implement such measures at this level. It is understood that ICANN continually monitors this issue and will take necessary countermeasures against registrars associated with such practices.

The registry will, however, post warnings on their website about any clearly fraudulent (and clearly illegal) renewal and expiration notices of which its staff becomes aware and will take legal measures against registrars performing such illegal, fraudulent acts.

Name Spinning

This is considered to be a practice employed mainly by registrars in a legitimate way to offer users more choice and/or alternatives should their desired name already be taken. As such, it is believed that it is within the registrar's responsibility to use those techniques in a considered manner. In reality it is not possible for the registry to differentiate between a legitimate domain name request, say one manually entered by a user, and a domain name request that was "spun" by the registrar.

In the event that such name spinning practices could lead to trademark infringements on a domain name, the UDRP allows for appropriate action to be taken against the holder of such a name. This follows the RAPWG's recommendation.

Pay-Per-Click

In agreement with the RAPWG's position, this is considered to be an indirect and purely web related issue that does not have a direct relationship to the registration of domain names. In most cases, pay-per-click is a legitimate revenue source for domain name owners and web site operators. Any potential misuse of such practices must be out of scope for the Registry and again any trademark cases are expected to be brought using the UDRP.

Traffic Diversion

In accordance with the RAPWG's position, this is again a web related issue and no specific countermeasures have been implemented within the registry's operations.

Domain Kiting / Tasting

In order to prevent mass domain kiting / tasting (as it was observable in gTLD and ccTLD registries), the Registry will implement the "Add Grace Period Limits Policy" (http://www.icann.org/en/tlds/agp-policy-17dec08-en.htm), which efficiently removes the financial advantage of domain kiting / tasting and hence significantly reduces the volume of such registrations. All registrars will obviously be treated identically in this respect with no exemptions from that policy.

Abusive Use of a Domain Name

Corresponding to the second bullet in the list above ("Abusive Use"), the RAPWG has also provided an analysis in their Final Report. The Registry will apply a policy as outlined below:

Anti-Abuse Policy for gTLD

The intention of .berlin's Abuse Policy is to take action against the use of a domain name in conjunction with illegal, malicious, fraudulent or otherwise harmful activities on the Internet. Such activities comprise:

- Spam: Spam is generally defined as bulk unsolicited e-mail, but can also occur in instant messaging or mobile environments. Spam may be sent from domains, and spam is used to advertise Web sites.
- Phishing: Phishing is a website fraudulently presenting itself as a trusted site – often as a bank website – in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).
- Pharming: Pharming is a redirection of Internet users to fraudulent websites, predominantly achieved by techniques like DNS hijacking or poisoning.
- Deliberate distribution of Malware: Malware is a piece of software that without the users' consent infiltrates their system to harm it or e.g. use it for bot net activities. Examples are viruses, worms, Trojans or key logger.
- Malicious Fast-Flux hosting: Malicious Fast-Flux hosting is a DNS-based component of bot net activities in particular, to e.g. disguise the location on the Internet of these activities and to harden them against discovery and defense.

Any incoming communication about a potential abuse will be handled according to section 3 of the response to this policy. Experts at the Registry Operator will then assess whether there is indeed an abuse at hand in conjunction with a gTLD domain name and of what kind it is. Subsequently the best method to tackle the issue will be derived from the initial assessment.

The main differences are a) whether the domain name has specifically been registered to commit the malicious activity or if this activity exploits a legitimate use of the domain name and its registrant is fully unaware of it, i.e. its website has been hacked – and b) whether there is a need for immediate action (domain is locked and removed from the delegation) or not (domain is locked only).

The Registry will keep records and track metrics regarding abuse and abuse reports. These will include:

- Number of abuse reports received by the Registry's abuse point of contact described above;
- Number of cases and domains referred to registrars for resolution;
- Number of cases and domains where the Registry took direct action;
- Resolution times;
- Number of domains in the gTLD that have been blacklisted by major anti-spam blocklist providers, and;
- Phishing site uptimes in the gTLD.

Handling of URS Requests

The registry Operator's handling of Uniform Rapid Suspension (URS) requests is specified in detail in section 1.3 of the response to question #29.

Registry Interfaces Abuse

The registry will employ the following countermeasures to protect against abuses of the registry systems and the DNS network itself:

WHOIS data harvesting

WHOIS access is a critical and vital service provided by any gTLD registry and the Registry will obviously comply with ICANN's requirements for WHOIS access.

However, as indicated in the SSAC's document "Is the WHOIS Service a Source for email Addresses for Spammers?", WHOIS abuse can be considered to be one of the primary means to generate email address lists for the purposes of sending unsolicited email, in particular the practice of mass harvesting information from the WHOIS. It is also believed that the WHOIS is the main source of data for generating fake renewal notices. To protect against harvesting of registration data (and particularly, email addresses), the registry will employ the following countermeasures:

- WHOIS query rate limits: All access to whois data will be query rate limited on a per-IP-address basis (for IPv4) and a per-prefix basis (for IPv6), with a daily limit of 25 WHOIS queries per IP address⁄prefix. Once this limit is reached, the WHOIS server responds with a relevant notification message instead of the standard WHOIS answer (The query limits may be reviewed and adapted by the Registry operator from time to time). IP-Ranges of accredited registrars (and other IP-ranges, eg. ICANN itself, UDRP and URS service providers etc) will be excluded from those rate limiting measures. This will allow legitimate usage of the service while at the same time make it very difficult to harvest data on a large scale.
- Email⁄Phone⁄Fax privacy: The EPP implementation of the "contact" object provides a mechanism that allows a registrar to define whether or not the "email", "phone", and "fax" fields of the contact object shall be publicly disclosed (i.e. "contact:disclose" element). The registry will set these fields to "do not disclose" by default, however, registrars can modify this setting via the normal EPP command stream. When a flag for a certain field is set to "do not disclose", the respective field will be omitted from anonymous WHOIS outputs, providing a minimum level of privacy to registrants. To allow for various business processes, IP Ranges of accredited registrars (and other IP-ranges as needed, eg. ICANN itself, UDRP and URS service providers) will still need to see the full data set, including those fields marked as "do not disclose".
- WHOIS monitoring: The WHOIS service will be monitored in order to identify unusual activity on the interface

The countermeasures above provide a well-balanced compromise between the requirements to provide access to WHOIS data and the basic data protection rights of registrants. More information about the WHOIS service provided by the registry is contained in response to Question 26.

EPP Interface Abuse

As described in the answers to the SRS, EPP and security questions (Question 24, 25 and 30, respectively), the EPP interfaces of the Registry are heavily firewalled, are only accessible from IP-ranges of accredited registrars and are protected by EPP authentication mechanisms. As such, abuse of those interfaces (such as DDoS, brute-force attacks against username/password combinations etc) can only be performed from networks of parties with which the Registry Operator has a legal agreement. Additionally, EPP interfaces are rate-limited at the network layer.

On top of the outlined technical means, usage figures beyond any regular and meaningful traffic patterns that are ongoing or recurring will be investigated by the Registry Operator. A lack of a decent explanation for such non-regular registrar behaviour on the EPP interface might lead to sanctions such as service degradation, interruption or even termination to the extent possible it is provided for in the Registrar Accreditation Agreement.

DNS Interface Abuse

Public nameservers, hidden masters and the signing infrastructure is configured and firewalled so that they allow NOTIFYs and UPDATEs from the required addresses only. In order to prevent zone walking and load peaks, zone transfers from the DNS infrastructure are disabled.

Management and removal of orphan glue records

It is understood, that in line with the SSAC's comments in http://www.icann.org/en/committees/security/sac048.pdf, glue records have a vital function in the correct and normal operation of the DNS but that they can also be used for malicious purposes.

In order to prevent such malicious usage, the registry performs glue record management in accordance with the following policy:

- Provisioning of host objects with glue: In line with the EPP RFCs, glue record ("internal") host objects can only be provisioned when the superordinate (parent) domain name exists in the registry. Host objects that are not under the TLD managed by the registry ("external hosts") can never have A or AAAA records
- Deletion of domain with subordinate glue record hosts: When a domain name transitions from a "REGISTERED" to a "REDEMPTION" status (for example, via the EPP "delete domain" command, or via expiration), the domain name itself is removed from the DNS, however any glue records under the deleted domain are kept in the zone temporarily. Other registrars who are affected by a potential impact on DNS service due to the upcoming removal of the host from their domains are notified via the EPP message queue.
- Subsequently, when the domain name transitions from a "REDEMPTION" to a "PENDING DELETE" status, the glue records under the affected domain name are revoked from the DNS, but still exist in the SRS database.

- In the last step of the deletion process (transition from “PENDING DELETE” to “AVAILABLE”), the glue record host objects are deleted together with the domain and are also removed from any other domain name in the registry that still uses those hosts.
- This policy effectively prevents misuse of orphan glue records in the registry since the status of a host object always follows the status of the superordinate domain. As a result glue records can never exist for domains that are not in the registry database. Additionally, keeping the glue records in the zone during the redemption period together with notification to Registrars significantly reduces the risk of other domains being impacted and reduces the effort required by a registrar in the event that the domain is subsequently restored.

However, in addition to this procedural policy outlined above, the registry operator will also act on documented evidence that glue records are present and used in connection with malicious activity by subsequently removing such glue records manually.

Contacts

All reports of abuse should be sent to abuse@nic.berlin.

Any complaints regarding inaccurate WHOIS information or should be addressed to the sponsoring registrar of that domain. Complaints may also be sent to whois@nic.berlin.