ICANN Registry Request Service

Ticket ID: U3T2D-1Y6S6
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2011-10-10 15:33:21
Print Date: 2011-10-10 15:40:59

Proposed Service

Name of Proposed Service:

Verisign Anti-Abuse Domain Use Policy

Technical description of Proposed Service:

Dealing with Malware

Abusive activity on the internet continues to rise, and public concern about the safety of the internet is clear. Verisign is aware that some reports have sought to portray the com/net TLDs as being at risk from maliciousness. All parts of the internet community are feeling the pressure to be more proactive in dealing with malicious activity. ICANN has recognized this and the new gTLD Applicant Guidebook requires new gTLDs to adopt a clear definition of rapid takedown or suspension systems that will be implemented. To address concerns over malware, Verisign is seeking to (i) provide a malware scanning service to assist registrars in identifying legitimate sites that have been infected and (ii) establish an anti-abuse policy to facilitate the takedown of abusive non-legitimate sites.

- *Malware Scanning Service*
  - *Registrants are often unknowing victims of malware exploits. Verisign has developed the capability to help identify malware in the zones managed by Verisign which, in turn, will help registrars by identifying malicious code hidden in their domain names. It is our intention to use this capability to identify malware on the internet and present the results to the registrars for action. This will be strictly optional and informational service to our registrars to allow them to address malware hidden in websites for the domain names they are managing.*
- *Facilitate takedown of malicious sites*
  - *Verisign's suspension system will contain the anti-abuse policy statement and a set of suspension procedures. The anti-abuse policy is comparable to other registry agreements, and Verisign will work with the registrars to develop a set of common suspension procedures to address non-legitimate abusive sites that effect the security and stability of the Internet.*

Anti-Abuse Policy

The new anti-abuse policy, would be implemented though a change to the .com. ,net and .name Registry Registrar Agreements and would allow the denial, cancellation or transfer of any registration or transaction or the placement of any domain name on registry lock, hold or similar status as necessary:

(a) to protect the integrity, security and stability of the DNS;

(b) to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental or quasi-governmental agency, or any dispute resolution process;
(c) to avoid any liability, civil or criminal, on the part of Verisign, as well as its affiliates, subsidiaries, officers, directors, and employees;
(d) per the terms of the registration agreement,
(e) to respond to or protect against any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the Internet),
(f) to comply with specifications adopted by any industry group generally recognized as authoritative with respect to the Internet (e.g., RFCs),
(g) to correct mistakes made by Verisign or any Registrar in connection with a domain name registration, or
(h) for the non-payment of fees to Verisign. Verisign also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute;

Malware Scanning Service

In connection with the adoption of the anti-abuse police, Verisign provide malware scanning for all .com, net and .name registrars pursuant to section 2.7 (b) of the proposed .com,.net .name Registry Agreements. This service will be optional allowing registrars to opt out of the service for .com, .net, and .name domain names under their management.
Section 2.7(b) provides:

If Registrar elects to allow Verisign to scan for malware, then in its registration agreement with each Registered Name Holder, Registrar shall also require such Registered Name Holder to acknowledge and agree that Verisign reserves the right for it or its agent to perform, in Verisign's unlimited and sole discretion, website scans or other views of websites for the purposes of, and only to the extent necessary to such purposes, detecting malware or as necessary protecting the integrity, security or stability of the registry; provided, Verisign will not disclose except to registrant and/or Registrar any data collected pursuant to a scan other than as permitted by applicable law, including applicable privacy and data protection laws, or pursuant to a court order.
Verisign defines malware as

"Malware" means any programming (code, scripts, active content, or other computer instruction or set of computer instructions) designed, or is intended, to (a) block access to, prevent the use or accessibility of, or alter, destroy or inhibit the use of, a computer, computer program, computer operations, computer services or computer network, by authorized users; (b) adversely affect, interrupt or disable the operation, security, or integrity of a computer, computer program, computer operations, computer services or computer network; (c) falsely purport to perform a useful function but which actually perform a destructive or harmful function or perform no useful function but consume significant computer, telecommunications or memory resources; (d) gain unauthorized access to or use of a computer, computer program, computer operations, computer

services or computer network; (e) alter, damage, destroy, monitor, collect or transmit information within a computer, computer program, computer operations, computer services or computer network without the authorization of the owner of the information; (f) usurp the normal operation of a computer, computer program, computer operations, computer services or computer network; or (g) other abusive behavior. Malware includes, without limitation, various forms of crimeware, dialers, disabling devices, dishonest adware, hijackware, scareware, slag code (logic bombs), rootkits, spyware, Trojan horses, viruses, web bugs, and worms.

Consultation

Please describe with specificity your consultations with the community, experts and or others. What were the quantity, nature and content of the consultations?:

See Below

a. If the registry is a sponsored TLD, what were the nature and content of these consultations with the sponsored TLD community?:

Not Applicable

b. Were consultations with gTLD registrars or the registrar constituency appropriate? Which registrars were consulted? What were the nature and content of the consultation?:

Verisign has worked with the Registrar community over the last six months in several aspects: piloting of the malware scanning service, participation in the piloting of the suspension procedures in our 'White Hat' initiative, and meetings to craft the language for the RRA updates. Following are the schedule of the events:

- *The first meeting was held with the Registrar constituency on March 7, 2011 to introduce the registrar community to the White Hat initiative and the malware scanning service.*
- *This was followed by two registrar meetings at the San Francisco ICANN meetings, where registrars were solicited for their input and participation in the pilots.*
- *Two additional registrar meetings were held a the Singapore ICANN meetings, to attempt to reach a broader distribution of registrars to participate in the pilots*
- *Three conference calls on July 21, 2011 to review the RRA red-lines with the registrars and gather their input. Based on this consultation, VeriSign revised the malware scanning to be an optional service.*
- *Three conference calls on October 5, 2011 to review the updates to the RRA based on the registrar feedback.*

As a result of these discussions, several registrars that have participated in either pilots or tests. The registrars involved in

the pilots and tests indicated the scans were very useful in identifying malicious code on their domains and would enhance data protection efforts.

c. Were consultations with other constituency groups appropriate? Which groups were consulted? What were the nature and content of these consultations?:

Verisign is a member of the Anti-Phishing Working Group (APWG), and has consulted with the staff on anti-abuse issues and mitigation practices. Verisign has also consulted with the IPC within APWG on domain suspension policy. The APWG is the global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types. The APWG also focuses on policy-related issues associated with the Domain Name System (DNS) to examine abuses of the DNS that may require remediation.

Verisign has been consulting with law enforcement, including agents from the U.S. Federal Bureau of Investigation who are responsible for investigating cybercrime. During the formulation of this registry policy proposal, Verisign engaged in a collaborative dialog with representative individuals from within the business, registrar, law enforcement and cyber security communities. The need to combat illegal domain name use is well-known and is not controversial.

d. Were consultations with end users appropriate? Which groups were consulted? What were the nature and content of these consultations?:

As a registry operator, Verisign did not consult with the registrants of .com/.net/.name domain names.

e. Who would endorse the introduction of this service? What were the nature and content of these consultations?:

Numerous registrars have expressed interest in Verisign's malware scanning service through the meetings, and conference calls reference above, and though the pilot program. They are interested in the identification and remediation support supplied by the registry to address the issues with malware in their domain names.

The NCFTA, a non-profit corporation, evolved from one of the nation's first High Tech Task Forces and, since 1997, has established an expansive alliance between subject matter experts (SMEs) in the public and private sectors. The NCFTA functions as a conduit between private industry, academia and law enforcement with a core mission to identify, mitigate and neutralize nationally and internationally-spawned cyber crimes. They have been involved in working on the anti-abuse program, and have indicated the intelligence shared within the program would be helpful in disrupting cyber crime.

Various Law enforcement personnel, around the globe, have asked us to mitigate domain name abuse, and have validated our approach to rapid suspension of malicious domain names.

The Anti-Phishing Working Group has also been supportive of the suspension service, and is engaged with Verisign in an interoperability pilot of the APWG and Verisign suspension services.

While Verisign cannot attest here that the above parties formally "endorse" this submission, we believe that the proposal is a welcome and constructive step forward to addressing pressing problems.

f. Who would object the introduction of this service? What were(or would be) the nature and content of these consultations?:

Parties who use domain names for abusive or illegal purposes, and parties who sell services to such abusers, may object to the new policy.

Registrants may be concerned about an improper takedown of a legitimate website. Verisign will be offering a protest procedure to support restoring a domain name to the zone.

Some registrars that have formal abuse policies and large abuse departments may be concerned the suspension system will require changes in their procedures. Verisign does not believe the new policy will substantially affect their current procedures. Verisign will be providing suspension requests into their current systems.

Registrars that do not have a 24x7 staff or formal abuse procedures may be concerned the anti-abuse suspension policy. There are provisions in the new procedures to provide the support these registrars need.

Registrants may be concerned about the impact of the service on their websites and Registrars also may be concerned about the impact of the malware scanning service on their customers. The malware scanning service will scan each domain once in a quarter, with a systems load comparable to a user accessing their website. Also, the malware scan is a virtual browser and does all analysis outside of the domains webserver.

Our continuing approach is to work with and through our registrars in a collaborative fashion. We believe that registrars share our view that organizations that are part of the infrastructure of the Internet (including registries, registrars, hosting providers, and ISPs) should all take reasonable steps to protect against online abuse and crime, in order to fulfill their obligations to protect the stability and security of the Internet.

Timeline

Please describe the timeline for implementation of the proposed new registry service:

In accordance with the provisions of section 6.1of the .com RRA/.net RRA/.name RRA the policy will take effect upon thirty (30) days notice to the .com/.net/.name registrars.

Business Description

Describe how the Proposed Service will be offered:

These services are offered as a two part solution to malware that threatens the security and stability of the Internet. The malware scanning service is offered to clean legitimate sites that have been unknowingly infected. The suspension service is offered to address non-legitimate sites that are abusing domain name services.

The malware scanning service will be implemented in the following steps:

- *Registrars will receive notice with a copy of the new RRA and a opt-out form*
- *Registrars that want to opt out of the service must sign and return the form to Verisign*

Note: we strongly encourage registrars to take advantage of this service to address malware in their zones. Verisign offers pilots to registrars to address their concerns about the impact of the service on their customers.

- *The scans will begin quarterly for the Verisign managed top level domains 30 days after the RRA notice*
- *Registrars will receive reports about infected sites (and remediation advice)*
- *This report is informational only*
- *No fee is assessed for this service*
- *Verisign has Tier 3 support for malware remediation if desired*

The suspension service will be implemented by working with registrars to implement the procedures in the appropriate timeframe. Registrars have different business models and processes, and there cannot be a one size fits all implementation plan. The common steps for the implementation will be as follows:

- *This set of procedures is only for those non-legitimate sites, legitimate sites that are infected will follow the malware scanning procedures.*
- *Law enforcement will have a formalized process for suspension requests*
- *Independent parties, with malware expertise, will be screening the suspension requests,*
- *Verisign will work with the registrars to develop the specific suspension procedures.*

Describe quality assurance plan or testing of Proposed Service:

Verisign has engaged Law Enforcement, Cyber Security SMEs, Government CERTS and Registrars in a pilot of the suspensions procedures, modifying them thru a number of test scenarios. This was has been completed in the US, to establish the baseline procedures.

Pilots with European Law Enforcement, Government CERTS and Registrars are planned, and other global test pilots will follow, to ensure global collaboration in the continuing development of the procedures.

Please list any relevant RFCs or White Papers on the proposed service and explain how those papers are relevant.:

Verisign is not aware of any relevant RFC or directly relevant White Papers.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

None.

What effect, if any, will the Proposed Service have on the reporting of data to ICANN:

None.

What effect, if any, will the Proposed Service have on the Whois?:

None.

Contract Amendments

Please describe or provide the necessary contractual amendments for the proposed service:

The Policy will be adopted pursuant to changes to Section 2.7 of the .com RRA/.net RRA/.name RRA.

Benefits of Service

Describe the benefits of the Proposed Service:

The benefits include:

o Enhancing coordination and cooperation among Verisign, law enforcement and registrars by providing an integrated response to criminal activities that utilize Verisign-managed TLDs and DNS infrastructure.

o Supporting registrars in protecting their registrants and domains by identifying potentially infected websites and providing remediation recommendations for malware to enhance prevention and combat cybercrime.

o Disrupting cyber-crime and other malicious use of the .com/.net DNS infrastructure, including malicious actors engaged in cyber-crime impacting Verisign customers, domains or infrastructure.

Competition

Do you believe your proposed new Registry Service would have any positive or negative effects on competition? If so, please explain.:

Verisign does not believe that the implementation of the policy will have a significant effect on competition.

Verisign will be offering a commercial malware service, thru a separate agreement, that will include more frequent scans of all their tlds. Such commercial service would compete with similar malware scanning products from commercial vendors.

How would you define the markets in which your proposed Registry Service would compete?:

Not applicable.

What companies/entities provide services or products that are similar in substance or effect to your proposed Registry Service?:

ICANN-accredited registrars are free to craft anti-abuse policies for inclusion in their Registrar-Registrant agreements. Those Registrar-Registrant agreements routinely forbid the illegal use of domain names, and often address many of the specific abusive practices.

Most other registries have relevant policies, including Afflias, Neustar and PIR.

In view of your status as a registry operator, would the introduction of your proposed Registry Service potentially impair the ability of other companies/entities that provide similar products or services to compete?:

Verisign does not believe that its proposed service would negatively impair the ability of other companies/entities that provide

similar services to compete.

Do you propose to work with a vendor or contractor to provide the proposed Registry Service? If so, what is the name of the vendor/contractor, and describe the nature of the services the vendor/contractor would provide.:

Verisign does not anticipate using any vendor or contractor to implement the proposed policy.

Have you communicated with any of the entities whose products or services might be affected by the introduction of your proposed Registry Service? If so, please describe the communications.:

See the prior sections of this application regarding consultations with third parties.

Do you have any documents that address the possible effects on competition of your proposed Registry Service? If so, please submit them with your application. (ICANN will keep the documents confidential).:

None.

Security and Stability

Does the proposed service alter the storage and input of Registry Data?:

No

Please explain how the proposed service will affect the throughput, response time, consistency or coherence of reponses to Internet servers or end systems:

Not applicable.

Have technical concerns been raised about the proposed service, and if so, how do you intend to address those concerns?:

Some Registrars have inquired about the load the malware scan will create on the web servers , where there are web servers hosting hundreds of names. The malware scanning service can be configured to either reduce or increase the rate of scanning based on the hosting solution. Verisign is offering pilot scans to test the configuration ensuring web servers will

not be impacted.

Other Issues

Are there any Intellectual Property considerations raised by the Proposed Service:

VeriSign is not aware of any intellectual property considerations.

Does the proposed service contain intellectual property exclusive to your gTLD registry?:

(1) Trademark or similar rights may exist or arise with respect to trade names or terminology used in connection with the proposed Service. (2) Copyright protection may exist or arise in connection with code written or materials created in connection with the proposed service. (3) Certain information or processes related to the service may be confidential to VeriSign and/or subject to trade secret protection.

List Disclaimers provided to potential customers regarding the Proposed Service:

VeriSign intends to include industry standard disclaimers, such as a disclaimer of all warranties, in the service agreement.

Any other relevant information to include with this request:

No