Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) Comments on Request for Information for the .us Top Level Domain

Introduction

Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), appreciates this opportunity to comment on the Request for Information for the .US Top Level Domain (TLD). We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet, including the domain name ecosystem.

M^3AAWG is a technology-neutral global industry association. With more than 200 members worldwide, we are the largest such organization in the online community. We bring together stakeholders in a confidential trusted forum to develop best practices and cooperative approaches for fighting online abuse. As a working body, we focus on operational issues of Internet abuse including technology, industry collaboration and public policy. M^3AAWG works to fight online abuse caused by botnets, malware, spam, viruses, DoS attacks and other forms of online exploitation.

We commend the Department of Commerce for undertaking this initiative. M^3AAWG supports robust requirements for the .US TLD to address the growing scale of abuse that our members have experienced in recent years.

General Observations

DNS abuse is a significant and growing problem that calls for effective solutions. Ample research exists demonstrating that phishing, malware, and other forms of abuse continue to show a disturbing upward trend. In its 2024 study on *the Cybercrime Supply Chain,* Interisle Consulting Group concluded that cybercriminals have sharply increased their consumption of domain name resources for cyberattacks. Specifically, "(o)ver8.6 million unique domains were used in cyberattacks compared to 4.8 million last year – an 81% increase." Interisle also noted that "(o)ver 2.6 million domains used in cyberattacks were registered in bulk, a 106% increase compared to the previous year." These statistics highlight significant growth in the use of domain names for malicious activities, reflecting a concerning trend in cybercrime tactics.[1]

More troubling findings were reported by the CyberCrime Information Center in its most recent report of ccTLDs which listed the .US Registry in the top five of all ccTLDs experiencing the highest numbers of cybercrime domains during the period analyzed (Sept 2023- Aug 2024).[2] Preventing the registration of these domains and taking them down quickly should be a priority for the .US Registry.

The 2022 EU DNS Abuse Study commissioned by the European Commission similarly found that "malicious activities on the DNS have been a frequent and serious issue for years, affecting online security, causing harm to users and third parties, and thus undermining their trust in the Internet." The study concluded:

> *To date, the response to DNS abuse in terms of preventive and reactive measures includes a broad set of voluntary and prescriptive instruments ranging from technical measures and contractual clauses, to cooperation between DNS operators and competent authorities, and to regulatory actions. However, past initiatives are fragmented and, as data shows, have not yet resulted in a significant reduction of DNS abuse.*

As DNS abuse directly correlates with cybercrime, DNS abuse definitions adopted by the .US Registry should be consistent with the internationally recognized Convention on Cybercrime, which enumerates explicit definitions and categories of cybercrime. Moreover, the US should consider the Convention on Cybercrime's "Second Additional Protocol", which facilitates cooperation for domain name registrations.[3]

Specific Questions Posed by NTIA

***DNS Abuse*: NTIA is considering enhancing the SOW to include more rigorous requirements to prevent, mitigate, and disrupt malicious activity within usTLD, including "DNS Abuse," which has been recently defined in ICANN contracts as phishing, pharming, botnets, malware, and spam (when spam serves as a delivery mechanism for the foregoing abusive activities).**

[1] See: https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/673a102318cc943de2987231/1731858468631/CybercrimeSupplyChain2024.pdf

[2] https://www.cybercrimeinfocenter.org/cybercrime-activity-in-tlds-september-2023-august-2024

[3] https://www.coe.int/en/web/cybercrime/second-additional-protocol

M^{3}AAWG applauds the US government's interest in tackling online abuse and cybercrime.

M^{3}AAWG recommends that the Department of Commerce consider drawing from the best practices described in the M^{3}AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries Paper published last year. These were developed by M^{3}AAWG's technical experts to address the fundamental gap within the DNS community that exists for how registries and registrars can best operationally effectuate anti-abuse mechanisms specific to malicious or compromised domains. M^{3}AAWG recommends that this document guide the Department of Commerce in promoting a safer and more secure DNS ecosystem in the .US Registry.

***Third-party access to .us registration data, and registrant data privacy*: The current SOW requires the Contractor to "maintain a publicly accessible, accurate, and up-to-date registration (WHOIS) database for all usTLD registrations." At present, the registration information of .us registrants (e.g., name, email, physical address, and phone numbers) is published openly on the global Internet. NTIA has long supported access to .us registration data by legitimate parties who make legitimate requests. NTIA is exploring ways to enhance registrant data privacy within a registration data access system.**

While M^{3}AAWG understands and sympathizes with some of the legitimate concerns driving concerns related to privacy, M^{3}AAWG supports access to WHOIS data to the maximum extent possible to meet all legally permitted aims, including end users' legitimate interests in avoiding spam, scams, abuse, and phishing as necessary and proportionate. In the absence of clear federal privacy legislation and in light of the importance of functional WHOIS for anti-abuse actors and end users, M^{3}AAWG strongly supports unlimited, unencumbered access to .us WHOIS.

Based on our data and experience, most of the risk that .US faces comes not from harvesting of WHOIS data, but from inadvertently creating conditions that enable abuse of .us domains for phishing, spam, scams, and other online abuse and criminality. The availability of full .us domain registration data has positive impacts on domain abuse involving .us domains, as abusers tend to avoid public scrutiny enabled by data access. This "open source" model of policing has prevented .us from becoming known as a hotbed of abuse, as some other registries have. Having an open WHOIS that allows attribution leads to proactive mitigation efforts that stop abuse before it happens.

We respectfully suggest that the Department of Commerce refer to the APWG and M^{3}AAWG[4] reports on the impact of redactions of the WHOIS by other registries, as well as

[4] "ICANN, GDPR and WHOIS Users Survey" http://www.m3aawg.org/WhoisSurvey2018-10 and "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later" https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

the reports by Interisle Consulting[5]. Furthermore, having available registration data allows third parties to audit/verify that .us nexus requirements are being met.

Nexus Requirement: The usTLD is intended to serve the Internet community of the United States and does so through a United States nexus requirement. NTIA is exploring enhancing the enforcement of the nexus requirement.

M^{3}AAWG supports the robust verification of eligibility requirements.

There are multiple ways to enforce the .us nexus policy to ensure registrants meet the U.S. connection requirements, including automated verification processes to reduce abuse. M^{3}AAWG suggests that the Department be informed by the practices of other ccTLDs, such as those followed by EU ccTLDs, as documented by the DNS Research Federations Report. [6]

In addition, the .US TLD should be informed by the European Union's Cooperation Group's Guidelines on Domain Names and Registration Data published in September 2024, which describes a risk-based approach to verify the accuracy of WHOIS information. For example, it recommends that a "risk-based method approach" be adopted based on best practices, including taking account of the state of art of predictive algorithms techniques. The EU Guidelines also recommend that all registrations that present a "medium to high risk of malicious registration should undergo identity verification". In the case of domain names used for malicious purposes, the Guidelines state that prompt actions should be taken to remove or de-activate the domain names.

<u>Kids.us Statutory Obligation</u>: The Dot Kids Act of 2002 (the Act) is "[a]n act to facilitate the creation of a new, second-level Internet domain within the United States country code domain that will be a haven for material that promotes positive experiences for children and families using the Internet, provides a safe online environment for children, and helps to prevent children from being exposed to harmful material on the Internet, and for other purposes." NTIA is exploring how to identify and develop potential uses of the kids.us domain that are consistent with its objective of providing a safe space on the Internet for children.

M^{3}AAWG supports this proposal.

Multistakeholder consultation on usTLD policy: NTIA is considering requiring enhanced transparency and other adjustments to the current SOW requirement for multistakeholder community engagement in the management of the usTLD, including policy development.

[5] "WHOIS Contact Data Availability and Registrant Classification Study: A Study of the Effects of GDPR and ICANN Policy," https://www.interisle.net/ContactStudy2021.pdf

[6] See DNS Research Federation's Report- Why are European ccTLD abuse Rates so low? https://dnsrf.org/blog/habits-of-excellence--why-are-european-cctld-abuse-rates-so-low-/index.html

M^{3}AAWG recommends several improvements with regard to the following issues:

Modernization and Transparency

- Regular Contract and Policy Updates: Recommend frequent updates to the usTLD's Statement of Work to align with evolving threats and best practices in the DNS space.
- Increased Transparency: Achieve transparency in policy enforcement, such as publishing regular reports on abuse trends and enforcement actions.

Stakeholder Collaboration

- Coordination with Anti-Abuse Groups: Suggest formal partnerships with organizations like M^{3}AAWG to provide ongoing expertise in addressing abuse and emerging threats.
- Public-Private Collaboration: Recommend forming advisory groups with stakeholders from the tech, anti-abuse, and internet governance communities.
- Education and OutreachEnd-User Awareness**:** Adopt initiatives to educate .us domain registrants about security best practices and their responsibilities.
- Registrar Training: Launch training programs for registrars to recognize and mitigate abuse, guard against registrant account compromise, as well as to support compliance with security and privacy requirements.

***Security*: NTIA is considering updates and modernization of the current security commitments including cyber incident reporting.**

M^{3}AAWG supports this proposal and will be happy to provide expert input should NTIA request comments on this update.

Conclusion

We appreciate the opportunity to submit these comments and welcome further opportunities to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director
Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)
comments@m3aawg.org
P.O. Box 9125, Brea, CA 92822