Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Recommendations for Preserving Investments in New Generic Top-Level Domains (gTLDs)

January 2018

The reference URL for this document: www.m3aawg.org/gTLDInvestments

1. Introduction

Over a thousand new generic Top-Level Domains (gTLDs) have been or are in the process of being created under ICANN's new gTLD program.[1] Each of those domains represents an investment of at least $185,000.[2] Unfortunately, those investments may dwindle until they become worthless due to two factors:

- Rampant domain name abuse in selecting new gTLDs
- The increasing perception that some new gTLDs would be little-missed even if they totally disappeared

Appropriate steps need to be taken now to protect:

- The gTLD program itself
- Operators of the most widely-abused new gTLDs
- Purchasers and users of domains registered in new gTLDs that are being abused
- Members of the internet community as a whole, who will otherwise be targeted with network abuse enabled by abused gTLDs

This document is written for current Registry operators and for companies interested in applying for new generic Top-Level Domains in the future. It outlines the risks observed by M³AAWG members and it also makes some recommendations which, if heeded, should help correct the problems some new gTLDs are facing.

2. Dot Com as a Comparative Baseline

Everything is relative. In the case of domain names, the de facto standard of care is defined by dot com as a normative baseline. While dot com establishes an implicit norm, it is generally believed to be perhaps the most important of all TLDs, as the following statistics demonstrate:

- Nine of the top ten Alexa[3] sites worldwide use a dot com TLD.[4]
- While there are hundreds of different TLDs, as of mid-summer 2015, nearly half (45.1%) of all second level domains were rooted in either .com or .net.[5]
- If the domain is omitted when entering a site's name in most web browsers' address bars, dot com is the default imputed TLD.[6]

[1] https://newgtlds.icann.org/en/program-status/statistics

[2] $185,000 is the application fee associated with applying for a new domain. Additional expenses are obviously associated with preparing the application and operating the new gTLD once obtained.

[3] http://www.alexa.com/topsites

[4] The exception? Wikipedia.org, coming in at number seven.

[5] http://www.verisign.com/assets/domain-name-report-september2015.pdf (133.5/296*100=45.1%)

[6] http://www-archive.mozilla.org/docs/end-user/domain-guessing.html

What this all means: dot com is a hugely popular success, is taken seriously by everyone, and is unquestionably too important to blocklist en masse. However, dot com domain names are also among the most widely abused domains on the internet.

For example, on a raw count basis, dot com domains are far and away the most commonly abused domains seen by SURBL, a popular domain name-based block listing service.[7] At the time this document was written, SURBL reported the following breakdown of domains listed in their blocklist:

Top-Level Domain*	Number of Blacklisted Domains by SURBL	Zone Size	Percentage of Zone
COM	512,012	130.6MM	0.39%
NET	99,912	15.0MM	0.66%
BIZ	61,699	2.1MM	2.94%
WIN	54,598	1.05MM	5.20%
ORG	54,589	10.4MM	0.52%

* [no other single TLD had more than 50,000 abused domains]

Similarly, dot com is the most frequently used phishing domain host, as reported in APWG (Anti-Phishing Working Group) phishing analyses.[8]

In considering the prevalence of dot com names in these abuse-related contexts, it is important to remember that dot com domains are also the most commonly used gTLD. Their misuse is at a scale proportionate to that TLD's overall market share. While it is true that there are a lot of abused dot com domains, there are also a lot of dot com domains, period.

3. New gTLDs and the Struggle for Success

The large number of new gTLDs that have recently been added—and will continue to be added for some time to come—represent a different proposition. These fledgling domains are not as well-established as dot com is. They are still striving to be taken seriously and struggling to succeed.

There are many ways that new gTLDs could potentially fail, including:

- Rejection by the marketplace (e.g., experiencing little or no demand)
- Unprofitability (many domains might be sold, but at such a low price that revenues do not exceed costs)
- Technical issues
- Association with abuse, with the result that some sites may refuse to accept traffic associated with that TLD

At least in the case of new gTLDs that have yet to enjoy widespread uptake, new gTLD owners may be tempted to employ aggressive marketing strategies in an effort to gain share. Market share is generally considered to be an excellent measure of overall gTLD success: a new gTLD that sells a considerable number of domains will generally be acclaimed as being more successful than gTLDs that sell only a comparative handful of domains.

[7] http://www.surbl.org/tld

[8] https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf, p. 10.

4. Competing on Price and the Race to the Bottom

Some new gTLD owners (largely those who believe that sales volumes are a crucial metric of success) may be tempted to compete on price, engaging in an unhealthy race to the bottom by offering to sell domain names at the absolute lowest possible prices. For example, at the time this was written, at least one registrar was offering domains in one new gTLD for just $0.40/year, with domains in additional new gTLDs being offered for less than a dollar per year.[9]

Selling domains at rock-bottom prices means that buying a domain name is a financially insignificant act. At $0.40/domain/year there is no real incentive (or available funds) for the gTLD operator to worry about abuse. And at $0.40/domain/year, there is also no reason for the domain registrant to care about their (effectively disposable) domain names.

Observation: While cheap domain name prices may result in increased sales, cheap prices may also lead to a perception of a TLD having low intrinsic value or of being a "bad online neighborhood."

Recommendation: Charge a price per domain that is high enough to send bottom-feeding domain name abusers elsewhere. In general, the higher the price selected per domain, the lower the level of abuse that particular TLD will experience. Whatever price is ultimately selected, at least avoid being one of the lowest-priced options available.

Setting a higher price not only makes a statement about the value of what is being sold (and discourages irresponsible use); it also ensures that if misuse does occur, sufficient funding will be available to tackle the problem.

5. Accountability and the Importance of Eliminating "Dark Corners"

Observation: Malicious actors flee from bright lights and close scrutiny. In the domain name ecosystem, bad guys attempt to avoid accountability for their abusive behaviors by obfuscating their identities behind private or proxy domain registrations.

When point-of-contact details are withheld, it is difficult to ensure that the details listed via WHOIS are "born accurate"—and will stay accurate over the lifetime of every domain.

Tolerating private or proxy registrations also means that the TLD operator is likely to have to deal with a greater number of legal demands to decloak private or proxy registrations or to at least provide the true registrant's actual contact information.

Recommendation: Transparency and accountability result in increased public confidence. Discouraging or forbidding private/proxy registrations, particularly for new gTLDs that are focused on corporations and business-related entities, will often be enough to send potential abusers elsewhere. Operators should know their customers and periodically validate all point-of-contact information provided.

6. Avoid Anonymous Payment Channels

Observation: Because normal financial operations (such as making payments with a credit card) result in additional, potentially attributable records, many malicious actors prefer anonymous payment channels (such as cash or various online alternative cryptographic currencies).

Recommendation: Do not accept payments made via anonymous payment channels. Require use of payment channels that facilitate validation of customer identities rather than facilitating anonymity.

[9] For current pricing details, see https://tld-list.com/ .

7. Do Not Use Resellers

Observation: While many resellers are potentially welcomed partners, some may be unsavory or less diligent at vetting customers than an actual ICANN-accredited registrar might be.

Recommendation: Avoid offering service via resellers.

8. Have (and Enforce!) Strong Terms of Service

Observation: Take the time to create strong terms of service with zero tolerance for online abuse. Ensure that maximum flexibility is retained to cure any breaches in the registration services agreement customers complete.

Recommendation: Registration services agreement should clearly spell out expectations for the customer and the channels that will be employed in the event a domain is being used for unlawful purposes. Strict terms of service send an important signal and may discourage many abusers from seeking domains in a gTLD in the first place.

9. Conclusion

Relatively simple measures—appropriate pricing; precluding anonymous points of contact and payment channels; declining to use resellers or using them within a strong Know-Your-Customer environment; insisting on strong terms of service; and enforcement of vetting the registration of trademarked names in all forms for banking institutions—will go far toward ensuring that the investment in a new gTLD will pay off, that abusers will go elsewhere, and that domains registered under the new gTLD will remain welcome everywhere.

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates to this paper.

M3AAWG1118