The New gTLDs

Security by Design

White Paper

ISBN 978-0-9836249-8-1

2012/12/12

Context

The 'New gTLDs' (generic top-level domains) provide the Internet with its largest ever transformation. Security issues with previous and current gTLDs demonstrate that this change provides the potential for further deterioration of Internet security. However, with fresh ideas and collaboration between the security community and new registries, it is clear the new gTLDs can and will be more secure by design, and contribute to a safer Internet.

Aim

This white paper looks at the problems presented by domain abuse, what the new gTLD program is doing to address these issues and what other proactive measures can be taken by the industry.

Authors

Editor	Jart Armin
Contributors	Dr Bob Bruen, Steve Burn, Andrew Fields, Will Rogofsky, Bryn Thompson
Reviewers	Raoul Chiesa, Rod Rasmussen, Garth Bruen, Peter Kruse, Alexander Klimberg, Andrey Komarov

Feedback

We welcome any feedback relating to this white paper, and anticipate releasing new research on the topic of new gTLDs in 2013.

Web	http://newgtldsecurity.com
Email	contact@cyberdefcon.com
Editor	jart@cyberdefcon.com

ABOUT CYBERDEFCON

CyberDefcon is an independent organization dedicated to the pursuit of making the internet a safer place.

They provide clients and partners with the tools and information necessary to:

- Track down and resolve cybercrime
- Prevent loss of business through cyber alerts "before they happen"
- Militate against cyber attacks
- Manage risks and vulnerabilities

The CyberDefcon team is dedicated to making the internet more secure and to developing new technologies and techniques that give control back to website operators and service providers. They believe in encouraging a proactive and preventative approach to security.

Through its research outfits HostExploit and SiteVet, CyberDefcon plays an important role in engaging the cyber security community on issues of cybercriminal hosting. These research initiatives play a key part in collecting data on malicious activity around the web. This data is cross-verified with community partners and provided to clients in feeds, with a wide array of uses.

Web: http://cyberdefcon.com

Abstract

At the end of June 2012 there were more than 240 million domains registered across all Top- Level Domains (TLDs)[1]. Just a generation ago global connectivity on this scale seemed an unlikely achievement. Once-unfamiliar technologies are now embraced, absorbed and integrated into everyday life, and even seem commonplace in some of the remotest places on earth.

The domain industry has flourished in this time and yet remains an enterprise in its infancy. Changes to the Internet naming structure in 2013 provide an opportune juncture at which to map out a model for the future that meets the diverse needs of the industry.

Cybercriminal activity on the web reminds us that there are many obstacles to further industry growth. The rollout of the new gTLDs provides the opportunity for consensus on the approach to this challenge and much-needed standardization of procedures across the industry. As well, it provides the opportunity for new gTLDs to demonstrate a commitment to online security; with the immediate financial incentive of dramatically-reduced abuse costs. The result will be a trusted environment with minimal risk associated, which in itself will create the potential for real growth.

Registries can take the lead in demonstrating a commitment to online security and engender confidence and trust from the top down as the new gTLDs program begins to unfold.

This white paper looks at the current problems presented by domain abuse, what the new gTLD program is doing to address these issues and what other proactive measures can be taken by the industry.

1 http://www.verisigninc.com/en_US/why-verisign/research-trends/domain-name-industry-brief/

Contents

1. Introduction

1.1 Problem statement

It is an established fact that the backbone for the Internet as we know it was never designed with security in mind. As such, it has been in a constant state of retrospective revision; something cybercriminals have been quick to exploit to their advantage, through both technical vulnerabilities and lax procedures.

The new gTLD program presents several opportunities. While the overall aim is to introduce more competition and choice to customers, it is also a propitious time to ensure that the new gTLDs and their associated services are supported by greater security and infrastructural stability.

However, without appropriate preparation, it could potentially be another case of "retrospective revision".

The program will lead to increased diversity and competition in the domain market, with the knock-on effect of increased possibilities for phishing and cybersquatting techniques, in particular.

In addition, there is the potential for new domains to cause confusion: firstly, to consumers; secondly, to software which has been programmed to consider only current TLDs. Such software could be targeted by new malware.

With rates of malware infections already sky-high, any increase could further alienate Internet users. In June 2012, Google recorded almost 10,000 new malicious websites every day[2]. Kaspersky counted over one million new bad URLs per day over a 90 day period[3].

Whichever method of quantification is used, it is clear that cybercriminals can all too easily create chaos and havoc, and present an obstacle to future economic growth. The new gTLD program should be part of a solution to the problem, rather than another technological avenue for cybercriminals to attack.

So what are the major abuses and how will the new gTLD program help alleviate the problem?

2 http://googleonlinesecurity.blogspot.co.uk/2012/06/safe-browsing-protecting-web-users-for.html

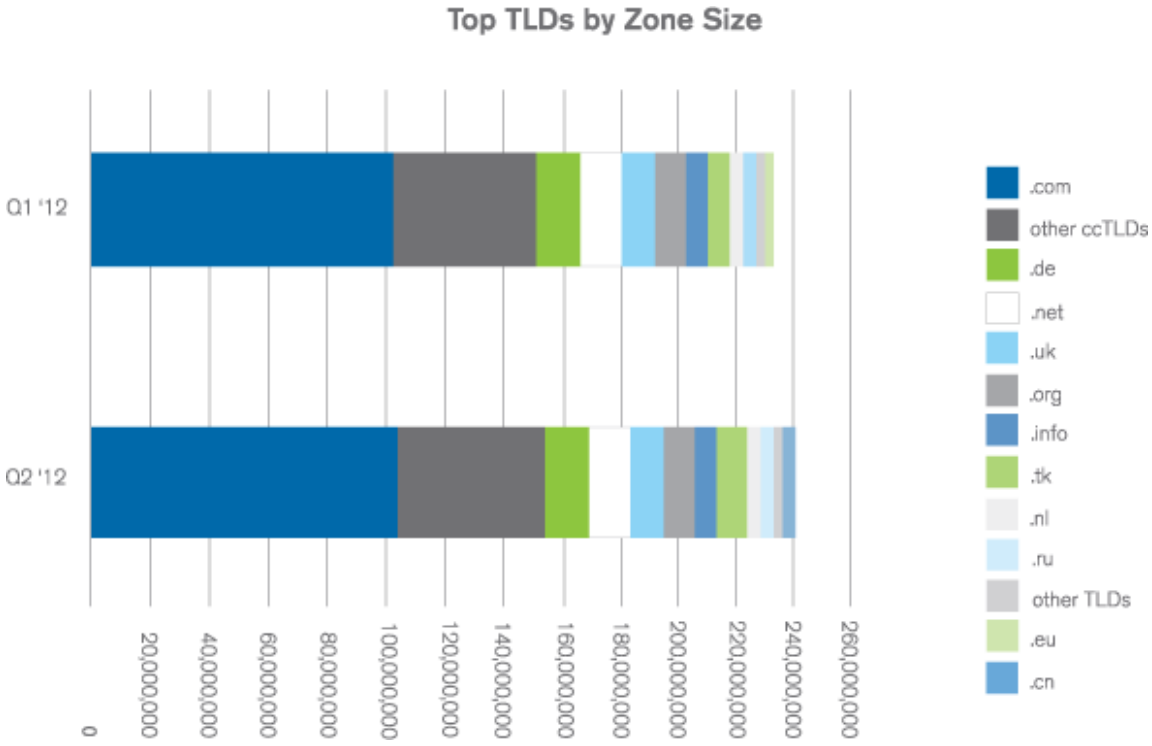
3 http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

1.2 New gTLDs under the microscope

There are currently 316 TLDs within the root zone, of which 22 are gTLDs. Of the 1,924 applications for new gTLDs now with ICANN, 1,173 are uncontested, 751 have more than one applicant and 652 are brand name applications (40% are listed on the Fortune 100, as 15 November 2012[4]).

With the arrival of hundreds of new gTLDs, there could soon be many new registrars selling domain names for the new dot extensions. Due to extra choice offered to consumers, it's expected that registrars specializing in "niche" markets of domains will appear, resulting in a higher density of registrars in the industry.

From a security perspective, will this be a positive or negative shift? Currently, the most familiar and largest of the gTLDs, *.com*, has a base size of 119.9 million domains[5], almost half the total number of all domains and an increase of 7.1 percent year-over-year.



Source: VeriSign

Considering the market share of *.com*, it may not seem surprising that it is a favored target of the cybercriminal. In fact, 90% of all malicious domain registrations were in just three TLDs: *.TK*, *.COM*, and *.IN*[6]. Mindful that the emergence of hundreds of new compliant gTLDs could add to this pool of malicious activity, security has been a priority from the outset of the program. All new gTLDs must comply to a number of features that will help prevent abuses and significantly reduce the number of malicious registrations through a vigorous registration process.

4 http://newgtlds.icann.org/en/program-status/statistics

5 http://www.verisigninc.com/en_US/why-verisign/research-trends/domain-name-industry-brief/

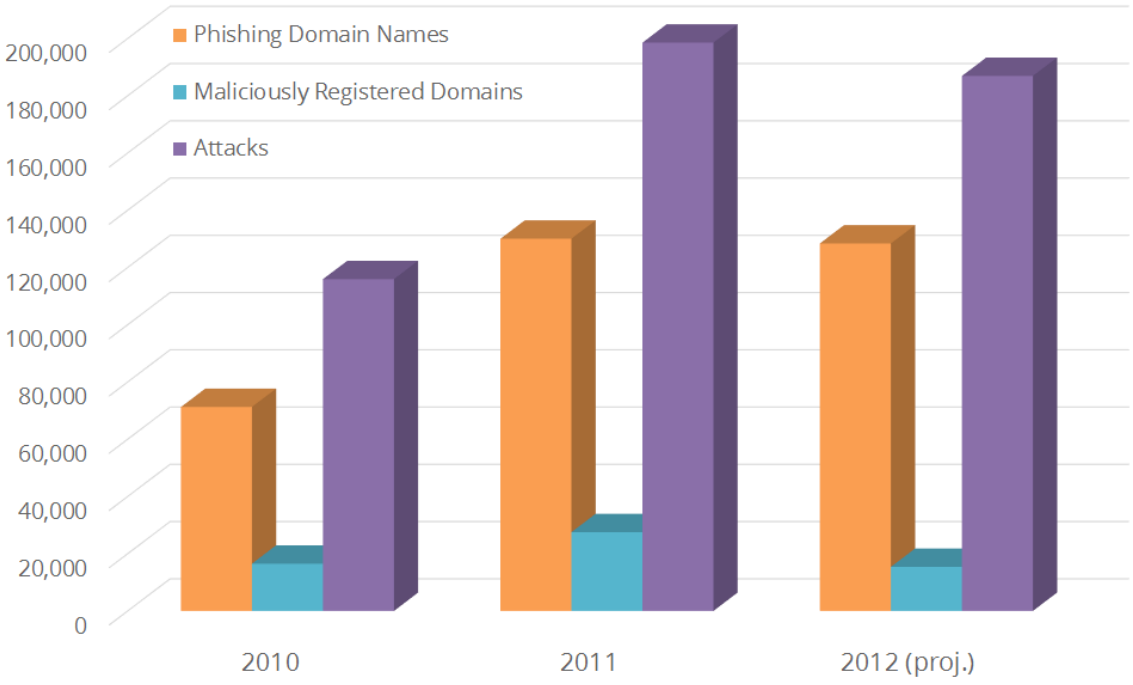
6 http://apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

2. The Problems

2.1 Cybercriminal abuse

Selected facts and figures:

- Around 9,500 to 10,000 new malicious domains per day[7] [8]
- 91,900,000 malicious URLS in 3 months June to Sept 2012[9]
- 2,700,000 malicious URLs per month (June)
- 300,000 malicious domains per month
- 7,712 new phishing-specific malicious domains, Jan–June 2012[10]
- 202 TLDs used for phishing



Source: APWG Global Phishing Survey 1H2012

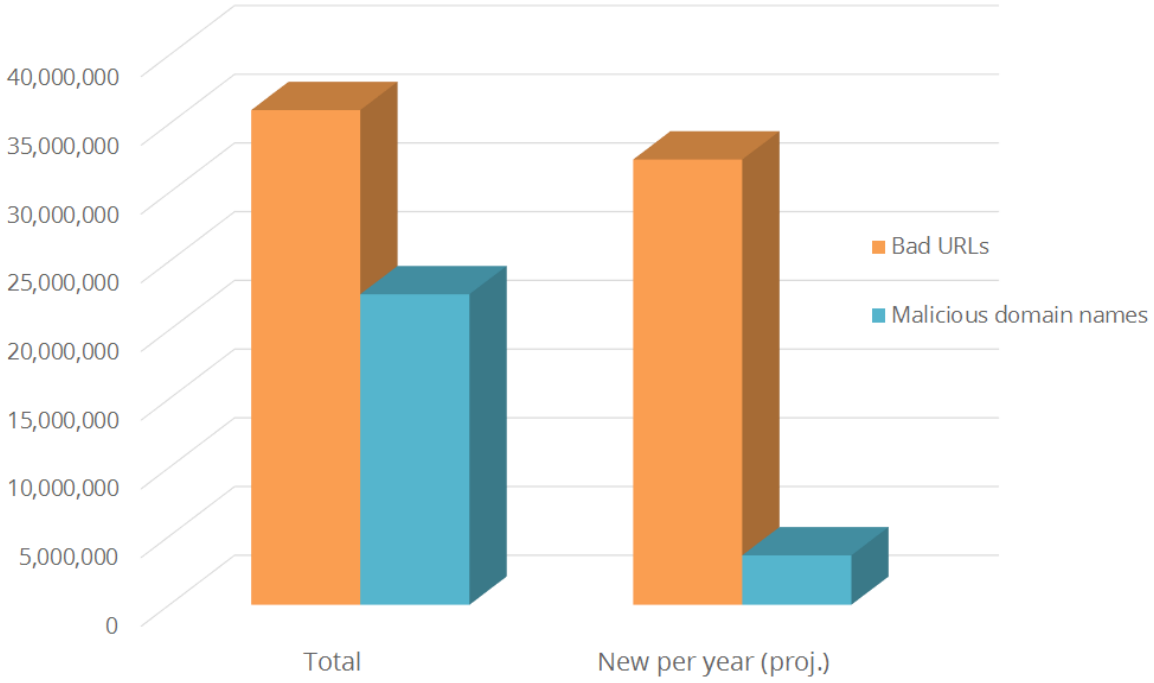
7 http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q2-2012.pdf
8 http://googleonlinesecurity.blogspot.co.uk/2012/06/safe-browsing-protecting-web-users-for.html
9 http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012
10 http://apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

There were 13,307 phishing attacks hosted on subdomain services in the first half of 2012, using 13,109 unique subdomains. Compare that to the 7,712 "regular" domain names registered by phishers in 1H2012.

"Subdomain registration services" are providers that give customers subdomain hosting accounts beneath a domain name that the provider owns. The domain name is effectively on the provider's own DNS space; the customer's hostname will look like this:

```
<anyone>.<service_provider_sld>.TLD
```

A logical conclusion is that phishers tend to favor subdomains as it allows for greater flexibility in forging "realistic-looking" URLs. The introduction of new gTLDs, provides a similar increase in options available. This is because users have come to typically only trust popular domain extensions, such as *.com* – thereby limiting the number of domains available to phishers. With the large range of new gTLDs – for example, .finance, .financial, .pay and others all related to payment services – users may be confused as to which extensions are more trustworthy.



Source: McAfee Quarterly Threat Report Q2 2012

A recent example of registries utilizing out-of-date systems was shown with the DNS hijacking and malicious redirection of critical .IE & .RO based domains, including Google and Yahoo[11] [12].

11 http://www.iedr.ie/docs/IEDR_Statement_F_issued_9_November_2012.pdf

12 http://www.securelist.com/en/blog?weblogid=208194028

Such attacks primarily rely on exploiting vulnerabilities in misconfigured and/or out-of-date software. The level of competition that potential registries face for the new gTLDs is expected to result in only those with the best records of security being accepted to offer new gTLDs, as laid out by ICANN guidelines. These inherently subjective guidelines are complementary to the more stringent registry requirements.

In turn, the registries are expected to require their registrars to follow the same standards in keeping systems up to date. In the longer term, potential innovative products or systems could be introduced by new gTLD registries that automatically enforce minimum software requirements on registrars' systems[13].

2.2 WHOIS accuracy

Providing WHOIS service is a central obligation of gTLD registries and registrars but the protocol used to retrieve data is decades old and the existing system is open to a number of abuses.

All registrants of gTLDs, registrars and registries, and a large part of the user community are affected by WHOIS in some way and yet, to date, there is no standard method for WHOIS data submission. Equally, display conventions vary with registries traditionally opting for a "thin" set of data based on collecting information on the domain name while registrars store data relating to the registrant as well.

The subject of WHOIS has continued to be a contentious issue over a number of years with its flaws and weaknesses brought into the limelight by several experts. For example, a report carried out by NORC at the University of Chicago for ICANN in January 2010, 'Study of the Accuracy of WHOIS Registrant Contact Information' found that "only 23% of (WHOIS) records were fully accurate"[14].

In March 2012, the WHOIS Review Team at ICANN recommended that all "unreachable" WHOIS registrations be reduced by 50 percent in one year[15].

2.3 Intellectual property abuse

One of the biggest threats to brand integrity comes from malicious cybersquatting and related abuses.

> *"'cybersquatting' occurs when a person other than the trademark holder registers the domain name of a well known trademark and then attempts to profit from this by either ransoming the domain name back to the trademark holder or by using the*

13 http://toronto45.icann.org/meetings/toronto2012/presentation-detecting-abuse-tld-aaron-young-15oct12-en.pdf

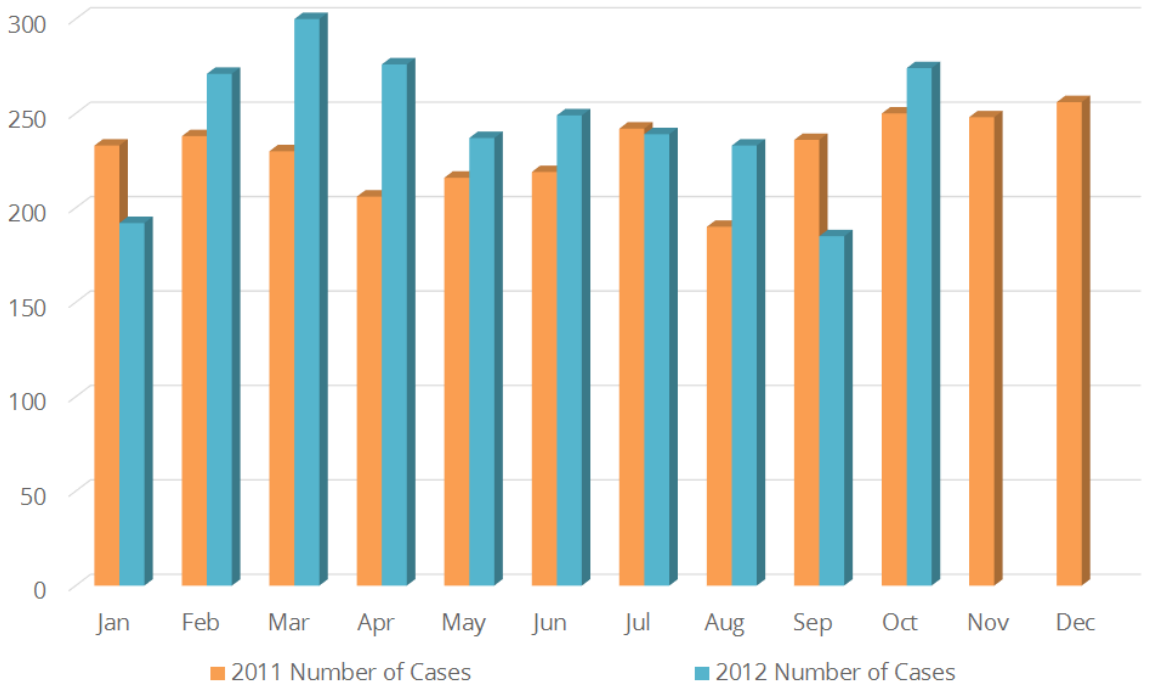
14 http://forum.icann.org/lists/whois-accuracy-study/pdfTNposvcgbS.pdf

15 http://www.icann.org/en/about/aoc-review/whois/reducing-unreachable-27jan12-en.htm

domain name to divert business from the trademark holder to the domain name holder" - DaimlerChrysler v. The Net Inc.[16]

The UDRP section at the Arbitration and Mediation Center at the World Intellectual Property Organizations (WIPO Center) has heard more than 22,500 cases relating to over 40,500 domain names (both generic and country code Top Level Domains gTLDs, ccTLDs) since its launch in 1999[17].

In 2011, trademark holders filed a record 2,764 cybersquatting cases covering 4,781 domain names. This corresponds to an increase of 2.5% and 9.4% over what had been the previous highs in 2010 and 2009.



Source: WIPO

As well, the WIPO Center has executed over 15,000 cases under Sunrise policies relating to registrations in the start-up phase of new domains.

The launch of hundreds of new gTLDs potentially increases the risk of cybersquatting. In anticipation a number of preventative measures have been applied to the new gTLD process in order to minimize the risk. New gTLDs will have to pass a rigorous application process and commit to a number of processes to ensure that TLD registration is compliant and assured.

One of the primary concerns has been over cybersquatting on new domains. Cybersquatting cases heard at WIPO show that many problems currently exist for domain owners, with big household brands particularly affected.

16 http://scholar.google.com/scholar_case?case=4716961749813728681

17 http://www.wipo.int/pressroom/en/articles/2012/article_0002.html

3. The New gTLD Program

The new gTLD Base Agreement with ICANN commits new registries to a number of actions that existing agreements do not have. These mandatory processes will form the basis for regular compliance-led audits and checks planned by ICANN[18].

In addition, all new gTLD contract winners will have demonstrated a high level of commitment to security before operations begin. The series of tests that each applicant must pass have been drafted to ensure that new gTLDs have the ability to engage in a program of 'security by design'. This is a new and welcome approach to ensuring conformity across the industry.

3.1 Problem-Solution overview

<table>
<tr><th colspan="2" rowspan="2">Problem</th><th colspan="3">New gTLD Solutions</th></tr>
<tr><th>Mandatory requirements</th><th>Additional registry mechanisms</th><th>Desired future innovations</th></tr>
<tr><td rowspan="3">Cybercriminal abuse</td><td>Phishing</td><td>DNSSEC</td><td colspan="2">Best practices</td></tr>
<tr><td>Malware</td><td>DNSSEC
IPv6</td><td>Enhanced abuse response</td><td>Domain add-ons</td></tr>
<tr><td>DNS hijacking</td><td></td><td>Enhanced registry systems</td><td>Automated minimum system enforcement</td></tr>
<tr><td rowspan="3">WHOIS</td><td>Accuracy</td><td>Thick WHOIS</td><td rowspan="3">Enhanced WHOIS standards</td><td rowspan="3">Internationalized protocol (IETF)</td></tr>
<tr><td>Auditing</td><td rowspan="2">Increased standardization</td></tr>
<tr><td>Access</td></tr>
<tr><td>Intellectual property abuse</td><td>Cybersquatting</td><td>TMCH
URS</td><td></td><td>Post-launch resolution process</td></tr>
</table>

18 http://newgtlds.icann.org/en/applicants/agb/base-agreement-specs-04jun12-en.pdf

3.2 Mandatory registry requirements

The introduction of a number of new mandatory undertakings at registry level ensures interoperability and compliance to standard specifications.

In the following sections, we examine specific parts of the new gTLD process and the anticipated effect on security issues. We examine the effect on the industry players – registries, registrars and webmasters or domain owners.

3.2.1 Domain Name System Security Extensions

Domain Name System Security Extensions (DNSSEC) at the zone level signs the root through the addition of an encrypted key and signature. This protects the DNS from attack by providing a validation path for look-up records and enables all the domains below the root to deploy DNSSEC and so complete a chain of trust. DNSSEC defends against DNS cache poisoning, redirects and spoofing. It is critical that DNSSEC is enabled at zone level.

After a slow start to DNSSEC signing, the majority of existing gTLDs are DNSSEC-enabled although only a third are fully "signed" according to ICANN's report dated 2012-11-24[19]. New gTLDs must sign their TLD zone files to enable DNSSEC.

For a guide to the benefits and associated risks of DNSSEC implementation, see Olaf M. Kolkman's RIPE presentation[20].

3.2.2 Rights and brand mechanisms

The introduction of a new Trademark Clearing House (TMCH) and the Uniform Rapid Suspension system (URS) is expected to prompt a reduction in Uniform Domain Name Dispute Resolution Policy (UDRP) cases (see Section 2.3 for case figures).

ICANN recently announced the selection of Deloitte and IBM to manage the new TMCH process. Deloitte Enterprise Risk Services will provide the Trademark Clearinghouse's authenticator/validator services[21]. The technical database administration services will be provided by IBM. It is expected that IPClearingHouse (CHIP) will be appointed to facilitate these services.

3.2.2.1 Trademark Clearinghouse

The Trademark Clearinghouse (TMCH) is designed to protect all brands from cybersquatting during the launch phase. The TMCH is intended as a place for use

19 http://stats.research.icann.org/dns/tld_report/

20 http://archive.apnic.net/meetings/19/docs/sigs/dns/dns-pres-kolkman-dnssec.pdf

21 http://icannwiki.com/index.php/Trademark_Clearinghouse

by all registries, registrars and industry players[22].

The TMCH will have two main functions:

- Validation Center for applications
- Data Center or Escrow services for data storage

There is still some debate on how these will operate without compromising on security, reliability or usability[23] but the TMCH is expected to prevent an increase in cybersquatting problems during the launch phase.

3.2.2.2 Uniform Rapid Suspension system

The Uniform Rapid Suspension (URS) system will expedite the suspension of domain names on clear-cut trademark infringement cases where there is no genuine contestable issue on the infringement or abuse that has taken place.

There were no initial candidates at ICANN's suggested price point of $300 - $500. A new RFI to identify a potential URS Service Provider was issued on September 24 2012[24].

3.2.3 A "thick" WHOIS

After prolonged debates on the issue of "thick" versus "thin" data at the registry, ICANN finally agreed that registries should comply with the same data requirements as registrars and all new gTLDs will be "thick" registries. See this CircleID article for a comparison of the two models[25], and why they are important.

The main thrust of the argument for improved data at the registry is to arrive at a greater consistency and accessibility of data. No longer will registries be able to define their own WHOIS output specifications and will be audited for compliance on a regular basis.

The issue is complicated somewhat by privacy laws that the agreement must not contradict – in particular, stringent European Union privacy laws relating to the period of time that registration details are stored for. ICANN is expected to allow European registries to opt out from these sections of the agreement to adhere with the local laws. See ICANN's *"Handling WHOIS Conflicts with Privacy Law"*[26] for further details.

However, the increased standardization of data will still bring its own benefits, regardless of the length of time that registrars store the data for. A standardized

22 http://newdomains.org/de/Implementation%20of%20the%20Trademark%20Clearinghouse%20(TMCH)
23 http://www.circleid.com/posts/20120828_trademark_clearinghouse_secure_reliable_usable_pick_any_two/
24 http://newgtlds.icann.org/en/applicants/urs
25 http://www.circleid.com/posts/how_a_new_gtld_should_choose_a_back_end_registry_system_part_3/
26 http://archive.icann.org/en/processes/icann-procedure-17jan08.htm

approach will help prevent registration abuses and aid legitimate forms of automation. Consistency of data enables analysis and measurement and allows for increased data quality at the registry, as all data is at hand.

A consistent response to WHOIS abuses can greatly reduce the problems and alleviate friction between law enforcement and industry players who have previously been unable to provide the answer to a simple request for full registrant/domain contact details.

3.2.4 IPv6

New gTLDs will be compatible to IPv6. The new registry operators will able to accept IPv6 addresses and have the facility to offer public IPv6 transport for at least two name servers including DNS and WHOIS.

IPv6 extends the outreach for unique public IP addresses. This can aid against a number of abuses where cybercriminals rely on hiding behind a shared IP address.

Additional IPv6 features that make it more secure than IPv4 include encryption "out of the box" (via IPsec), to help prevent session hijacking, and validation of the source address, to prevent IP spoofing used by attackers to falsify the origins of an attack or response testing of an intended target.

Further, IPv6 improves the chances of traffic reaching its end destination without being intercepted.

IPv6 as an essential requirement from the outset is a good example of *'security by design'*.

Support for IPv4 will continue.

See the June 2008 OECD report, *Economic Considerations in the Management of IPv4 and in the Deployment of IPv6*[27], for a detailed analysis of the advantages and disadvantages of IPv6 deployment.

3.2.5 Centralized Zone File Access

Access to TLD zone files is important to many entities, including researchers, academia and trademark protection organizations. Obtaining multiple zone files is not always easy, since each registry can provide its zone files in any format it chooses, with its own method of requesting access.

With an increase in the number of gTLDs, access could become even less consistent. For this reason, ICANN now requires that new gTLD registries provide zone files in a standard file format, and authenticate all requests through an

27 http://www.oecd.org/internet/interneteconomy/40605942.pdf

independent "Centralized Zone Data Access Provider"[28]. This more open approach to data access will result in a reduced barrier to further research.

3.3 Additional registry mechanisms

Further to new registry requirements, ICANN guidelines ensure that new gTLD registries will have established a positive record of security. As an extension to this approach, new gTLDs are expected to be supported by additional procedures, including:

3.3.1 Enhanced WHOIS

Compliance to a standard WHOIS data specification will contribute to a reduction in abuses, but in isolation it will not solve all the problems associated with WHOIS.

Here we suggest a range of additional processes to be adhered to in order to assist in improving data quality, security and customer service.

1. Carry out regular internal audits of WHOIS data for accuracy, treating it with the same importance as credit cards or other payment options.
2. Make WHOIS data as readily accessible as possible. Provide multiple query methods so that one-time or bulk queries are accounted for, as well as customers with a range of technical abilities.
3. Ensure each data field is completed and valid.
4. Filter registrations, using third party verification services if needed:
    - Check for properly formatted email addresses.
    - Check for integrity of addresses, phone numbers and mismatches of zip code (US) or equivalent.
5. Automate handling of bulk complaints of data inaccuracies (using third party services if needed).
6. Remediation of inaccurate WHOIS data, including takedown, if warranted.

Changes to WHOIS will bring positive advantages in reducing registration abuses via automation and monitoring of the due processes. This will also provide a platform for new technologies to emerge based on the new datasets.

3.3.2 Enhanced Abuse procedures

New gTLD registries are expected to demonstrate a commitment to resolving domain abuses and responding to cases in a timely fashion. Our suggestions include:

28 http://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf

- Proactive handling of abuse cases. By actively investigating abuses, rather than waiting for customers to report issues, service is improved to customers and load on the abuse department can be greatly reduced.
- Knowledgebase and automated responses to common issues. Customers reporting abuses should be able to do so clearly and promptly.
- Monitoring of common attack types.

See Sections 4.3 and 5.3 for registry and registrar abuse recommendions, respectively.

3.4 Future innovations

3.4.1 TMCH and URS

As this area develops there will be opportunity for innovative products to aid in the clearinghouse process. This could evolve around the search processes of the TMCH, in the validation of applications or in Escrow services and data storage.

Solutions are required for the post-launch TMCH phase. WIPO identified that the greatest risk from trademark abuse may well materialize *"after New gTLDs are delegated and become operational, in particular once any second-level domain name registrations become available*[29]*."* One method of tackling this would be through a Post-Delegation Dispute Resolution Procedure to settle objections and complaints outside of a court hearing.

3.4.2 WHOIS protocol

The ICANN-specified protocol RFC3912 has several shortcomings as identified by the Internet Engineering Task Force (IETF) Working Group on the Web Extensible Internet Registration Data Service[30].

In this document the IETF pinpoints several problem areas:

- WHOIS protocol has not been Internationalized
- It does not consistently support Internationalized Domain Name (IDN, described in [RFC5890])
- WHOIS has no query and response format
- WHOIS protocol does not support user authentication, access control for differentiated access

The IETF findings support the view that the WHOIS protocol requires updating in order to meet the evolving needs of the Internet community.

29 http://www.wipo.int/amc/en/domains/newgtld/

30 http://datatracker.ietf.org/doc/draft-zhou-weirds-dnrd-ap-object-inventory/?include_text=1

4. Registry Recommendations

The gTLD expansion represents significant opportunity to the registries awarded the new ICANN contracts, if historical growth can be used as a comparative guide[31]. For example, VeriSign – the .com registry – reported a 13 percent year over year revenue growth in Q3 2012[32]. Demand Media, selected as the technical registry operator for gTLD strings awarded to Donuts, invested heavily in new gTLDs ($18 million) in anticipation of strong market growth in the domain name industry and in support of the planned expansion.

The sum invested by each applicant provides some assurance that a new gTLD will not want a massive investment failure. Starting from a blank sheet is a good way to build a new business model based on a unique set of rules within a niche brand.

A new gTLD operator will already have shown its capability for providing a high level of competence, operational integrity and financial viability.

Mandatory measures aim to strengthen security at the zone level such as DNSSEC, IPv6 compatibility and new Trademark Protections (see Section 3.2.2.1) – instilling trust being an important element of registry business.

However, some issues remain a matter of contention, and a registry must be prepared to work closely with ICANN and registrars to resolve these. For example, who should be held accountable for malicious activity served on a network? Although the legal debate on this issue continues, both registries and registrars can work closely on security matters to help keep networks clean. Taking the lead will bring long term benefits through mutual trust and assurance that effective controls are in place.

31 http://www.demandmedia.com/blog/ahead-of-the-curve-in-gtlds/

32 https://investor.verisign.com/releaseDetail.cfm?releaseid=716434

4.1 General procedures

Spamming, phishing, malware, illicit pharmacy, etc., are all significant and enduring problems.

The Registry can, and should, take a lead role in actively encouraging Registrars to incorporate appropriate measures to tackle abuses through the legally binding Terms of Agreement.

Enhanced methods of reducing domain abuses:

1. Employ rate-limiting techniques to a known list of external open DNS resolvers, to avoid common DDoS attacks to internal DNS servers via DNS reflection.
2. Extend the Sunrise Launch Period from 30 to 60 days - this could include 30 days of advance notice on the Sunrise period.
3. Introduce a Trademark Post-Delegation Dispute Resolution Procedure (PDDRP).
4. Prohibit the transfer, deletion, or modification of DNS settings of a domain name for the life of the dispute.
5. Offer a Domain Protected Marks List (DPML) product for trademark protection.
6. A new Claims Plus product for trademark protection.
7. Make it a requirement of the registrar to report known instances of malicious activity or attempts to undermine security via a (monthly) report to the Registry.

Some Registry service providers have already proposed some of these measures for new gTLDs utilizing the newly formed TMCH. For example, Demand Media is supporting both a DPML and a Claims Plus product for their TLD applicants. The DPML is an optional service that will allow trademark holders to prevent registration of second level domains that contain their trademarked term across the TLDs that Demand Media supports. Demand Media will also utilize the TMCH in its support for a Claims Plus product which will build in alerts sent to the registrar and potential registrants that a domain they are searching for is in the TMCH.

For further DNS considerations, see McAfee's *Mining DNS for Malicious Domain Registrations* paper[33]. For DNSSEC deployment, see documentation for existing deployments, e.g. Verisign's deployment[34] and testing[35] plans.

33 http://www.mcafee.com/uk/resources/white-papers/wp-mining-dns-for-malicious-domain-regist.pdf
34 http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-deployment-02.txt
35 http://www.root-dnssec.org/wp-content/uploads/2010/06/draft-icann-dnssec-testing-01.txt

4.2 Contractual Compliance Audit program

At Toronto 45, ICANN proposed a three-year planned approach to a Contractual Compliance Audit program. The overall plan is due to be rolled out in 2013 and will apply all registries – new and retroactive.

Discussions continue on the Audit strategy but registries and registrars will be subject to a standard Auditing process in the future with additional audits also a possibility. The process is to ensure *"alignment and compliance by all contracted parties with their contractual obligations*[36]*."*

Registries should ensure they are ready to meet ICANN's regulations and objectives from the offset of their gTLD program, in advance of auditing.

4.3 Abuse procedures

In addition to the measures covered under 'Rights and Brand Protection', all complaints received at the Registry relating to domain names abuses, should be handled according to a dispute resolution process, which should be made easily accessible on its website with details of a single point of contact responsible for addressing the dispute resolution process.

Introduce a minimum set of requirements to apply as a result of receiving a verified complaint:

- Lock the domain within 24 hours of validation of the complaint
- Restrict all changes to the registration data, including transfer and deletion of the domain names
- Prohibit the transfer, deletion, or modification of DNS settings of the domain name for the life of the dispute
- Provide a timely response to abuse complaints concerning all names registered in the TLD through all registrars including those involving a reseller

For further recommendations, see StopBadware's *Best Practices for Web Hosting Providers*[37] and APWG's *Best Practices Recommendations*[38]

36 http://www.icann.org/en/resources/compliance
37 http://www.stopbadware.org/pdfs/best-practices-responding-to-badware-reports.pdf
38 http://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf

4.4 Application procedures

A rigorous process for Registrar application checking can prevent many abuses at the first hurdle, and therefore save abuse handling costs further down the line. Prevention of bogus registrations is a priority for all registries[39]. A top-down auditing approach provides additional assurance through to the end of the chain. Registries should encourage Registrars to enforce their policies further down, through to resellers and service providers.

- Verify that the primary email address for the Registrar is a valid business email address.
- Verify the applicant business is: active, valid, current in the Registration Agency records or equivalent.
- Verify current accreditation status and date of expiry.
- Verify that TLD data is consistent and correct at the TLD Registry level.
- Consider additional protections such as a two-stage registration process where a PIN is sent to a designated business postal address.

See Section 3.3.1 for WHOIS guidelines.

4.5 Registrar agreements

A new gTLD can contain its own terms and conditions. Use these to enforce restrictions on your registrars. For example:

- Encourage Registrars to educate resellers/service providers on Best Practices.
- Propose that Registrars introduce 'challenge response authentication' to verify the identity of the Registrant.
- Encourage Registrars to offer domains with additional protections for Registrants who may wish to opt for, for example, a per domain access model.
- Require that Registrars offer the option for notifications to Registrants be conveyed via additional methods to email such as telephone, fax, postal or courier services for additional protection.
- Annual/bi-annual review of agreement.

39 http://www.domainnamenews.com/legal-issues/false-registration-domains-leads-severe-criminal-punishment/6898

5. Registrar Recommendations

Registrars anticipate that the expansion in the number of new Top Level Domains will attract a great deal of interest and could lead to new sales and variable prices for specialized gTLDs. To prepare for this increased capacity many Registrars have begun to not only expand their technical infrastructure in breadth, but in scope as well. The increase in functionality and services is a direct result of the expansive mandatory protections built into the new gTLD program that Registrars must incorporate to sell these new gTLDs.

The benefits that a Registrar may anticipate as an effect of the mandatory security features and enhanced measures applied from the top level (registry) down include the following:

1. An assured standard of security and operational integrity.
2. An assured standard of financial integrity.
3. A higher standard for registration processing and assurance that registration data is accurate.
4. Standardization of abuse procedures and processes to expedite urgent matters and minimize false reports.

For Registrars, implementing higher levels of security can not only save the Registrar money but it can drive revenue by promoting the trust factor. A win for all involved.

A good example can be found in Demand Media's recent collaboration with CyberDefcon community partner HostExploit. Through the introduction of proactive measures to resolve Command & Control servers, and other areas of malicious activity, the security of its domain registration and web hosting platforms has been notably improved.

5.1 ICANN agreements

The Registrar's agreement between the Registrar and with ICANN sets the standard for a range of measures that aim to prohibit illegal or abusive activities.

A new Registrar Accreditation Agreement is reaching final consensus between

ICANN and interested parties, including the Registrar Stakeholder Group[40]. A number of measures are being incorporated into the new RAA which will require a greater involvement by registries and registrars. The following list has been agreed in principle[41].

1. Use of accredited privacy/proxy providers if required by ICANN.
2. Verifiable contact details on registrars and reseller's website.
3. Public display of corporate officers on registrar's website.
4. Public display of all related registrars on registrar website.
5. Notification to ICANN of changes to location, officers, ownership, or criminal convictions.
6. Registrars shall be legal entities in country of operation.
7. Resellers must be held accountable to the RAA.
8. Validation of WHOIS data.
9. Not to, knowingly or through gross negligence, allow the pursuit of criminal activity via the registration of domains or in the provision of a WHOIS service. In the case of receiving notice of such activity, the failure to apply appropriate solutions will prompt in termination of accreditation.
10. Registrar abuse point of contact to be clearly displayed on its website.
11. Process for amending RAA in the future.

5.2 Contractual Compliance Audit program

ICANN proposes a three-year planned approach to a Contractual Compliance Audit program. The overall plan is due to be rolled out in 2013.

Discussions continue on the Audit strategy but registries and registrars will be subject to a standard Auditing process in the future with additional audits also a possibility.

A major change under discussion which the security community is broadly in agreement on is for registrars to have a greater control over reseller compliance, which are only authorized within a registrar's own TLD[42].

5.3 Abuse procedures

Abuse procedures should be consistent with those of the Registry. See Section 4.3.

In addition, all complaints received at the Registrar relating to domain names

40 http://icannregistrars.org/calendar/announcements.php?utm_source=&utm_medium=&utm_campaign

41 https://community.icann.org/x/MQXPAQ

42 http://www.icann.org/en/resources/compliance

abuses should be handled according to a resolution process which should be made easily accessible on its website, with details of a single point-of-contact responsible for addressing dispute resolution.

5.4 General procedures

Registrars may be constrained by a number of factors, for example, operational size, and this may affect which additional recommendations can be introduced. Therefore, this can be considered a proactive 'wish list', but each point is worthy of serious consideration.

1. Make Terms and Conditions readily available in a "human readable" format, in addition to the full legal terms.
2. Investigate reports of illegal conduct (from law enforcement or otherwise).
3. Provide a standard system to track complaints in co-operation with the Registry.
4. Place limitations on domain proxy and privacy services.
5. State in the Reseller Agreement that resellers to be held accountable to all provisions of the RAA agreement.
6. Publish policies and procedures that define abusive activity.
7. Terminate accreditation for violations, e.g. cybersquatting.
8. Provide proper resourcing for all of the functions above.
9. Educate webmasters on how to prevent fast-flux botnets, double-flux botnets, and other related DNS-changing attacks. See Appendix 1, point 4.

A large number of DNS open resolvers are known to be misconfigured and remain vulnerable to multiple malicious activities[43], including the following:

- DNS cache poisoning attacks
- Denial of Service (DoS) or Distributed DoS (DDoS)
- Resource utilization attacks

To reduce abuses, DNS open resolvers, if present, should be checked and configured according to business need. A few simple changes to name server resolvers can prevent system abuses:

1. Permit queries and recursion only from trusted sources.
2. Perform randomization for UDP source port and transaction identifier.
3. Segregate authoritative and recursive resolvers.
4. Set the "Maximum Cache Length" and "Maximum Cache Size".

43 http://hostexploit.com/blog/14-reports/3540-familiar-hosts-a-open-resolvers.html

For further recommendations, see APWG's *Best Practices Recommendations*[44]. For a comparison of proactive detection methods, see ENISA's 2011 report[45]. For a technical overview relating to phishing detection, see the *Proactive Discovery of Phishing Related Domain Names*[46] manuscript from the University of Luxembourg. For DNS considerations, see McAfee's *Mining DNS for Malicious Domain Registrations* paper[47].

5.5 Application procedures

New gTLD registries should pass a strict code of conduct down to their registrars. One of the key components should be how to handle domain registrations.

By following these simple recommendations, the vast majority of fraudulent registrations can be avoided[48]:

- Check for properly formatted email addresses. (Many of the criminal registrations do not pass this test!)
- Check for integrity of addresses, phone numbers and mismatches of zip code (US) or equivalent. Common mismatches include: the entry of a city (town, village, etc.) listed as being in a state (province, territory, region, etc.) when it is not or a state listed in a country, when there is no such state in that country.
- Submit address parts of the registration record and the phone number to a verification service (all gTLDs could contribute financially to an agreed third party trusted service).
- Automate handling of bulk complaints of data inaccuracies (using third party services if needed).
- Retain data on previous suspended customers, and import similar data from law enforcement, in order to block malicious registrations.

5.6 Domain add-ons

The new gTLD program offers TLDs an opportunity to develop new markets and earn new revenues through a range of innovative 'state of the art' products, to fill the security gap that mandatory processes alone cannot fill.

Prospective domain owners can be enticed by unique anti-abuse products that distinguish one registrar from another; for example, domain malware scanning.

44 http://docs.apwg.org/reports/APWG_RegistrarBestPractices.pdf
45 http://www.enisa.europa.eu/activities/cert/support/proactive-detection
46 http://hal.archives-ouvertes.fr/docs/00/74/88/08/PDF/proactiveDiscoveryPhishing.pdf
47 http://www.mcafee.com/uk/resources/white-papers/wp-mining-dns-for-malicious-domain-regist.pdf
48 http://knujon.com/abuseddomainstudy.html

6. Registrant Recommendations

A top-down approach to security can provide major benefits to all industry players. By enforcing requirements and providing recommendations from registries to registrars all the way down to registrants, procedures become more simplified and familiar to customers.

In a new competitive market, driven by sales of new gTLDs, with domain add-ons becoming more common, it becomes even more important that registrants are informed clearly on the services they are taking out. Both registry and registrar can help by providing educational resources that new and existing applicants can access to find additional information on a number of subjects. These would aid the registrant to understand that:

- Verification measures are in place for security purposes.
- Accurate registration data is necessary and (should be) industry standard.
- Terms of Service provided include certain prohibited uses and abuses.
- Reselling is governed by certain conditions that mitigate malicious domain registrations and abuse of DNS.
- Enhanced opportunities available for resellers through added value services and domain name distribution supplies such as privacy protection, web hosting, and SSL certification.
- Opportunity for new innovative products throughout the domain name industry along the lines of malware scanning services, registration checking and compliance auditing to ICANN specification.

6.1 Security procedures

Note that procedures vary greatly depending on the nature of the registrant (i.e. individual, organization, reseller etc.).

To improve security, registrants should:

- Impose a password change policy. Periodically verify registration contact data.
- Proactively monitor domain name registration checking that data is consistent and that all points of entry are completed and verified.
- Ensure contact email address is verifiable, preferably a business email address and not from the registered domain name.
- Verify that all transfer attempts are intended.
- Check malware listing sites for webmasters – such as Google Safe Browsing – for the presence of owned domain names. Follow delisting guidelines if present.
- Mandatory security features at registry level is not an excuse for poor domain practises from webmasters. Domain owners should still remain vigilant at all times!

Registrants are advised to contact their registrar to see what additional security measures are available. For example, the registrar eNom offers an account validation feature that prevents unauthorized account access by requiring additional security questions, as well as notification and disabling functionality if there are attempts to log into your account. These strong security features in addition to unique and complex passwords are critical for registrant security.

Appendix 1

Best Practices Guide

This ***Best Practices Guide*** is intended as an aid for new gTLD Registries and Registrars and serves to provide a practical code that can reduce the risk and impact of cybercrime on its business and customers. It proposes to strengthen the terms of the Registrar Accreditation Agreement (RAA) with a number of additional measures.

1. **Respond quickly and appropriately to abuse reports and takedown requests.** Ensure the abuse team handles abuse reports from different parties – such as law enforcement, domain owners, cyber security community, general public – through multiple channels so that each department is independent.

   Have procedures in place with an action plan to enable a swift domain lock, suspension or termination. Work with downstream registrars and domain resellers to take direct action, when needed, to ensure that offending domains are suspended. Actuate suspension measures as detailed in the legally binding RAA for cases of contract violation.

2. **Be proactive and not just reactive in shutting domains down.** Do not rely solely on abuse reports and takedown requests. Use all data and tools at your disposal – public and corporate block lists, open source rulesets and spam lists are all widely available.

   Employ as many automated detection methods as possible of common exploits on your network. Use appliances such as IDS, IPS and WAF to detect and block exploits as high up the network chain as possible. Employ malware scanning on hosted accounts. When abuses are detected, manually investigate the case to determine if similar abuses may also be present, and how they could be prevented.

   For blocklists, see the Spamhaus DBL[49] and SURBL RBL[50]. For open-source

49 http://www.spamhaus.org/dbl/

50 http://www.surbl.org/

tools, see ClamAV[51] and YARA[52]. For rulesets, see Snort[53] and Emerging Threats[54]. For commercial abuse services, see NameSentry[55].

3. **Work closely with law enforcement and share fraudulent domain registration information.** Keep as much information on the registrant as possible, according to the WHOIS protocol employed and local privacy laws. It is good practice to keep information on the registrant separate from the publically available WHOIS information.

   If you suspect fraudulent or malicious activity on a domain, inform law enforcement and pass on details of the registrant, IP addresses, and modifications to the domain record, credit card information, name, address, email, company name, and all other available data. Don't wait for law enforcement to initiate contact!

   For example: for US, see IC3[56]; for UK, see ActionFraud[57].

4. **Reduce the registration of "fast-flux" domains.** Automatically-generated are utilized by botnets and cybercrime exploit kits. By making it much more difficult to frequently change the NS record of a domain, fast-flux domains can be almost entirely eradicated[58]. Examine existing customer data to see how often customers change NS and other DNS records, and enforce time limits on that basis. A good default is to not allow the NS record to be changed more than 5 times in any month. Impose either a hard limit, or raise a flag to investigate the account.

5. **Join industry groups and workshops.** By joining industry groups, your business can benefit from the shared experience of the group, and industry-leading research. With a groups and workshops focusing on specialist areas, there are a wide range of topics in which to engage, and use to improve your business processes. See:

   Anti-Phishing Working Group: an international association focused on unifying the global response to electronic crime – in particular, phishing – through development of data resources, data standards and systems for private and public sectors[59].

51 http://www.clamav.net/
52 http://code.google.com/p/yara-project/
53 http://snort.org/
54 http://www.emergingthreats.net/
55 http://architelos.com/services/namesentry/
56 http://www.ic3.gov
57 http://www.actionfraud.police.uk/report_fraud
58 http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf
59 http://www.antiphishing.org/

MAAWG: an organization that brings together the messaging industry to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations[60].

Center for Safe Internet Pharmacies (CSIP): a non-profit organization founded by leading internet industry participants – such as Google, Microsoft, Visa, Mastercard, eNom, GoDaddy – whose mission is to promote and encourage safe online pharmacies through education, enforcement, and information sharing[61].

6. **Reject domain registrations at your discretion.** Not all domain applications *have* to be accepted! Retain intelligent customer data to determine applications originating from previous customers, such as name, email, address, credit card information, IPs, etc. Integrate historic data from law enforcement, if available. When an application is received from a customer with a record of abuse, then deny the application and add the offender to a blocklist to prevent future registrations.
7. **Transmit the culture down the business chain.** You can be held responsible for the actions of your resellers; be proactive and give them advice on how they too can follow an approved code of practice.
8. **Engage with your customers.** Provide practical resources that educate and inform on the latest threats and vulnerabilities. This could be via third-party websites – such as national CERTs – or through a dedicated knowledgebase on your website.
9. **Ease the process of contacting you or making a complaint.** Determine a complaints procedure, details of which should be published on the company website. Open several channels of contact for your customers. Make sure the contact details are clearly available on the company website.

For phishing-specific recommendations, see the excellent APWG Registrar Best Practices[62]. For malware-specific recommendations, see StopBadware's *Best Practices for Web Hosting Providers*[63].

60 http://www.maawg.org/about_maawg
61 http://www.safemedsonline.org/who-we-are/members/
62 http://www.apwg.com/reports/APWG_RegistrarBestPractices.pdf
63 http://www.stopbadware.org/pdfs/best-practices-responding-to-badware-reports.pdf

Appendix 2

Glossary

Badware

Software that fundamentally disregards a user's choice on how his or her computer will be used. Types of badware are spyware, malware, or deceptive adware. Common examples of badware include free screensavers that surreptitiously generate advertisements, malicious web browser toolbars that take your browser to different pages than the ones you expect, and key logger programs that can transmit your personal data to malicious parties.

Cybersquatting

To knowingly register or manage a domain name that matches a known trademark, contains a known trademark or a variation of that trademark. The domain name can also be deliberately similar to a known trademark with the intention of causing confusion to the user.

DDoS (Distributed Denial of Service)

DDoS attacks or floods can be executed in a variety of ways. The desired effect is to interrupt the normal business of a web service. Attackers use the power of multiple computer systems, either via or a botnet or from number of users, to flood the system with multiple requests until it crashes. Another method to launch an attack is to amplify DNS requests via open resolvers which uses few resources to achieve its aim.

DNS (Domain Name System)

DNS associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. www.example.com, into IP addresses, e.g. 208.77.188.166, which networking equipment needs to deliver information. A DNS also stores other information such as the list of mail servers that accept email for a given domain, by providing a worldwide keyword-based redirection service.

DNS Security Extensions (DNSSEC)

A set of DNS extensions used to authenticate the origin at DNS level and check the integrity of DNS data. Implementation is required at registry level for the most effective protection.

Exploit

An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause irregular behavior to occur on computer software, hardware, or something electronic. This frequently includes such things as violently gaining control of a computer system or allowing privilege escalation or a denial of service attack.

gTLD

A generic top-level domain (gTLD) is one of the categories of top-level domains (TLDs) maintained by the Internet Assigned Numbers Authority (IANA) through the ICANN process. gTLDs are used in the Domain Name System of the Internet. The suffix at the end of a domain name determines the gTLD such as in the core group of generic top-level domains of .com, .info, .net, and .org domains. In addition, a set of restricted domains .biz, .name, and .pro are also considered generic; require proof of eligibility within set guidelines set. In 2013 the number of gTLDs will substantially expand through the new gTLD program.

IANA

The Internet Assigned Numbers Authority (IANA) performs the technical delegation of TLDs and address space and managing protocol parameter assignments under ICANN. IANA former responsibilities for IP address space assignment, protocol parameter assignment, domain name system management and root server system management are now performed by ICANN.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation with a world-wide responsibility for Internet Protocol (IP) address space allocation and generic (gTLD) and country code (ccTLD) Top Level Domain name system management. Other responsibilities include protocol identifier assignment and root server system management functions.

IDN

An Internationalized Domain Name is a domain name with one or more non-ASCII characters, to represent languages with non-Latin scripts such as Arabic, Hebrew, Chinese or Hindi.

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet[64].

64 http://www.ietf.org/about/

IP (Internet Protocol)

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering data packets from the source host to the destination host solely based on its address.

IPv4

Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP). Pv4 uses 32-bit (four-byte) addresses, which limits the address space to 4.3 billion possible unique addresses. However, some are reserved for special purposes such as private networks (18 million) or multicast addresses (270 million).

IPv6

Internet Protocol Version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 uses a 128-bit address, IPv6 address space supports about 2^128 addresses.

Phishing

Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is typically carried out using e-mail (where the communication appears to come from a trusted website) or an instant message, although phone contact has been used as well.

Registry

A registry operator generates the zone files which convert domain names to IP addresses. Domain name registries are, for example, VeriSign (for .com.), Afilias (for .info). Country code top-level domains (ccTLD) are delegated to national registries such Nominet in the United Kingdom, .co.UK, "Coordination Center for TLD .RU" for .RU and .РФ

Registrar

A domain name registrar is a company with the authority to register domain names, authorized by ICANN.

TMCH

The Trademark Clearinghouse is a database of trademarks that will be established by ICANN in order to enhance the protection of intellectual property on the Internet[65].

Trademark

A word, name, symbol or device applied in connection to goods that indicates the source of the goods and distinguishes them from others' goods.

65 http://icannwiki.com/index.php/Trademark_Clearinghouse

UDRP

The Uniform Domain Name Dispute Resolution Policy as approved and adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) on October 24 1999.

URS

The Uniform Rapid Suspension system was designed exclusively to provide trademark owners with a quick and a low-cost process to take down websites infringing on their intellectual property rights. The URSS was proposed by the trademark groups within ICANN in an endeavor to cut back the large number of trademark infringements, including cybersquatting[66].

WEIRDS

IETF Working Group on the Web Extensible Internet Registration Data Service protocol[67].

WHOIS

WHOIS contains details on registrant, administrative, billing and technical contact and is provided to registrars at the point of a domain name registration. WHOIS services are intended to provide free public access to information about the registrants.

WIRT

ICANN's WhoIs Review Team[68]

WIPO

The World Intellectual Property Organization (WIPO) is the United Nations agency dedicated to the use of intellectual property (patents, copyright, trademarks, designs, etc.) as a means of stimulating innovation and creativity. WIPO promotes the development and use of the international IP system through its services which includes domain name dispute resolution under procedures based on the Uniform Domain Name Dispute Resolution Policy (UDRP).

Zone File Access

A Zone File is a DNS configuration file that contains all DNS records for domain names under the relevant zone. gTLD registries hold the zone file for all domains registered under the gTLD. The method by which a zone file can be obtained is referred to as Zone File Access.

66 http://icannwiki.com/index.php/URS

67 http://datatracker.ietf.org/wg/weirds/

68 http://www.icann.org/en/groups/board/documents/briefing-materials-1-08nov12-en.pdf