| Article/Volunteer | Observations | Hypothesis | Research | Findings | Possible recommendations & Champion |
|---|---|---|---|---|---|
| Article: Potential for Phishing in Sensitive-String Top-Level Domains<br>Volunteer: Laureen | Article considers what needs to happen for a phishing attempt to succeed and when and how prevention and mitigation can be effective.<br><br>Practical and easy to understand. Explains technical concepts in plain language. | Whether sensitive string gTLDS have a lower incidence of phishing due to restricted registration policies. | Primarily relies on APWG Global Phishing surveys.<br><br>Also looked at 300 most recent domains listed at Artists Against 419 (aa419.org) a repository of fraud sites, particularly advance fee frauds | Most phishing takes place on compromised domains (phisher has broken into registrant's web hosting) so registration restrictions (including those for sensitive string domains) don't matter under this scenario. pp. 12-14, 26<br><br>Other methods: malicious registrations [84% to chinese targets]; subdomain resellers [registries often provide free services including P/P services] ; and IP addresses. Pp10-11<br><br>Phisher can get benefit of "trusted" sensitive domain by simply creating URL string that appears to in the sensitive domain. Pp. 19-21<br><br>Phishing emails often hide their real destination domain name from user. Pp8-9.<br><br>Phishing generally small compared to # of domains in the world (mostly concentrated in legacy gTLDs and cc TLDs. pp. 10-11, 19-20 | Phishing does not appear to be any more or less prevalent proportionally in new gTLDs.<br><br>Pricing appeared to be a factor for attracting phishing in new xyz gTLD.<br><br>Malicious registrations can be reduced by controlling access to domain registrations via more stringent registration requirements and higher pricing.<br><br>gTLD operators should have and enforce terms of service and that allow suspension of the domain name for malicious actions, including phishing. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | .com contains 41.3% of domains and 58% of phishing domains (2H2014 data set). p.14<br><br>Expansion of gTLDs will likely not affect total amount of phishing. Will create new locations for phishing to take place. pp 15-16, 22, 26<br><br>New gTLD analysis: 26-29<br><br>Registration restrictions, pricing strategies (higher prices), and active mitigation deter phishing. Quick takedowns of phishing sites are essential. p.25 | |
| Article: Verizon 2016 Data Breach Investigations Report<br>Volunteer: Laureen | Data breaches continue to increase and evolve.<br><br>Not a primary source for our work but likely a good source of data and background for prevalence of data breaches and phishing in particular | Are new gTLDs more or less apt to be involved in the data breaches discussed in this report? | Data set of over 100,000 incidents<br><br>Many contributors (see p. 71) | Accommodation and Retail industries account for majority of data breaches (an incident that results in unauthorized disclosure of data) p.4<br><br>Actors in breaches primarily external p. 7<br><br>Primary motive is $$$ pp. 7-8<br><br>Phishing (w/attached malware) and point of sale attacks are common infiltration tools p.9 (Phishing focus pp. 17-19; PoS focus pp. 31-34) | Consider how Phishing and DoS attacks relate to consumer trust. If we opt to focus on these issues of domain abuse, the same person can include this report as a resource (perhaps Gao?) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Denial of Service attacks (DoS) con't to evolve (pp. 56-59)<br><br>Many different ways that bad actors can compromise credentials to infiltrate (figure 45 pg. 62) | |
| Source: ICANN Compliance web page<br><br>Volunteer: Laureen | On-line resource displaying variety of data maintained by ICANN K Compliance | Does ICANN Compliance compare complaint rates for legacy vs. new gTLDs? | | Data includes yearly reports on notices of breach, suspension, termination, or non-renewal; quarterly and annual reports; and summaries of outreach | Consider meeting with K compliance to ask about available data on new gTLDs. |
| Article: ICANN Contract Compliance 2015 Annual Report<br><br>Volunteer: Laureen | Yearly report summarizing ICANN Contract Compliance Activity<br><br>Notes huge increase from 2014 in gTLDs (+400 to +1100) and +1400 accredited registrars to 2100) | Has introduction of new gTLDs increased complaints? | ICANN Contract Compliance Data | Complaint count increased by 20% from prior year (increase in new gTLDs and registrars likely a factor)<br><br>Chief notes that while ICANN c/n be solution to problems of abuse and illegal activity, they can play a role in partnership with others in the Internet ecosystem.<br><br>In addition to handling complaints, Compliance performs audits; conducts outreach; and seeks to improve processes. Re: audits, review of potential risk of K'ed parties' non-compliance with various K provisions.<br><br>Launched initiative to improve knowledge of K compliance which included a video on how they can help w/domain name registration issues and a chart on what is a | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | contract compliance complaint (available in 8 languages)<br><br>Registrars: Abuse complaints: 438 (1%); WHOIS inacuracy (+75%); transfer (+14%)<br>Chart p. 8; description p.11<br><br>Registry: Abuse contact data (61) (small percentage of 2180 total); Zone file access (+31%); Registry Data Escrow (+21%)<br>Chart p. 8; description p.13<br><br>Formal notice activity included notices for publishing email POC for abuse reports;; maintain/publish records re: abuse reports; and publish on website procedure for receipt and tracking of abuse reports (all at approx. +4%) | |
| Article: ICANN Contract Compliance Dashboard Jan. 2016<br>Volunteer: Laureen | Monthly summary of ICANN Compliance complaint activity. | This report does not distinguish between legacy and new gTLDs (does Compliance have this data?) | Complaints filed with ICANN | For Registrars: top complaint topics involve WHOIS inaccuracy (68.2%) and transfers (20.5%) Abuse complaints relatively low (38 vs. +2000 for WHOIS inaccuracy and +600 for transfer)<br><br>For Registries: Zone file Access (61.9%) and Registry Data Escrow (12.6%)<br><br>Only 4 complaints re: Abuse Contact data | |

| | | | | | |
|---|---|---|---|---|---|
| Source: GAC Safeguard Advice in Communiques<br><br>Volunteer: Laureen | Governmental Advisory Committee issues formal written advice after every ICANN meetings. In response to new gTLD program, GAC issued safeguard advice on a variety of issues | Has GAC Safeguard advice enhanced consumer trust; had an impact on abuse? | GAC Communiques | Note: Although GAC issued many items of safeguard advice, ICANN did not accept all advice as given.<br><br>Beijing advice highlights:<br><br>Advice for all gTLDs<br>Reconsider decision to allow singular and plural versions of same string b/c could lead to consumer confusion<br><br>Require Registry operators to conduct WHOIS Verification and checks<br><br>Require Registry operators to ensure terms of use for registrants prohibit abusive activity (e.g. malware, botnets, phishing, piracy, infringement, fraud or deceptive activity, counterfeiting)<br><br>Require Registry Operators to conduct technical analysis to to asses whether domains in its gTLDs are being used to perpetuate security threats (e.g. pharming; phishing malware botnets)<br><br>Require registry operators to ensure a mechanism for making and handling complaints<br><br>Ensure real and immediate consequences for false WHOIS | We should add review of PICs for strings corresponding to highly regulated sectors to our data requests.<br><br>Brainstorm on how to measure impact of GAC safeguard advice.<br><br>Complicated b/c n/all advice implemented and n/ncess implemented as advised.<br><br>We should follow up on GAC gathered data on community applications and CPEs<br><br>LK can champion these issues. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | information and violation of requirement that domains should not be used for illegal purpose (including suspension of domain name)<br><br>For sensitive/regulated strings:<br><br>Registry operators to include in acceptable use policy that registrants comply with all applicable laws (including privacy and consumer protection)<br><br>Registry operators to require registrants that collect sensitive data (financial, health) to implement reasonable security measures<br><br>Registry Operators to require Registrants to have a single POC to report complaints or abuse.<br><br>Further Targeted Safeguards for domains associated with market sectors with clear and/or regulated entry requirements (financial, gambling, professional services: environmental, health and fitness, corporate identifiers and charity)<br><br>Registry operator to verify and validate credentials at time of registration; consult with authorities if in doubt; conduct | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | post registration checks to ensure continued compliance<br><br>Restricted Registration Policies<br><br>Registry operator should administer in transparent way; no undue preference to any registrar or registrants<br><br>For strings representing generic terms, exclusive registry access should serve a public purpose<br><br>Highlights of 2013 Buenos Aires Communique<br><br>Consider whether Public Interest Commitments fully implement safeguard advice<br><br>Recategorize .doctor as a highly regulated string to therefore ascribe these domains exclusively to legitimate medical practitioners (noting strong implications for consumer protection and consumer trust)<br><br>New Registry OPerators should be aware of importance of protecting children consistent with UN Convention on Rights of the Child<br><br>Highlights of 2014 Singapore Communique | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Concerns about outcomes of community applications<br><br>Reiterates advice that singular and plural of same string could cause consumer harm<br><br>Poses lengthy list of questions in appendix aimed at whether NGPC has fully implemented GAC safeguard advice (particularly verification/validation requirement; security checks) and concerns about proposed PIC Dispute Resolution Process<br><br>Highlights of London Communique<br><br>Asks for briefing on GAC concerns about implementation of safeguard advice re: verification of WHOIS information, verification/validation of credentials for regulated industries, security checks, PICDRP, and discrimination in restricted TLDs<br><br>Annex includes detailed discussion of where GAC thinks that NGPC has failed to fully implement its advice<br><br>Highlights of Los Angeles Communique | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Reiterates concerns with NGPC's failure to implement GAC advice on safeguards related to WHOIS, Security Risks, PICDRP, verification/validation of highly regulated strings, ensuring nondiscriminatory registration policies<br><br>Con't concerns about consistency of Community Priority Evaluation process<br><br>Subsequent Rounds<br>GAC advises that reviews of first round should be completed and finalized before policy for further gTLD rounds is developed.<br><br>Highlights of 2015 Singapore Communique<br><br>Regrets NGPC failure to adopt verification/validation requirement for strings associated with highly regulated industries.<br><br>Reiterates concerns re: length, complexity, and ambiguity of PICDRP. Seeks "fast track" for Law enforcement and gov't agencies. | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Highlights of 2015 Buenos Aires Communique<br><br>Asks NGPC to create a list of commended PICs related to verification/validation of credentials for domains in highly regulated sectors<br><br>Asks for method to assess number of abusive domain names within assessment of new gTLD program<br><br>Clarify acceptance or rejection of GAC advice with a straightforward scorecard<br><br>Highlights of Dublin Communique<br><br>Reiterates requests for 1) clear scorecard of accepted and rejected safeguard advice; 2) list of commended PICs re: verification/validation of credentials for domains in highly regulated sectors; and 3) harmonized methodology for reporting levels and persistence of abusive conduct (malware, botnets, phishing, piracy, infringement, fraud or deceptive activity, counterfeiting or other illegal activity) within new gTLDs<br><br>Reiterates concerns about CPEs and assessing public policy related | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | aspects of current gTLD program before launching new rounds Marrakech Communique Highlights<br><br>Focus on ensuring existing GAC safeguards maintained and improved.<br><br>Encourages review of PICs for strings corresponding to highly regulated sectors<br><br>Intends to gather data community applications and CPEs to contribute to CCT review. | |
| Assignment: CZDS-ZFA Passwords Reports<br>Volunteer:<br>Jamie | Monthly reports listing numbers of credentials with access to TLD zone files. TLD zone files contain the list of domain names that are registered and active for a given registry. Every new Registry is required to provide zone data files to approved requestors (e.g. law enforcement agents, IP attorneys, researchers) upon technical delegation | N/A | Spreadsheet of alphabetized listing of TLDs and number of passwords issued for access to zone files | Number of TLDs in May report with credentialed ZFA users: 993<br><br>Top 20 TLDs by number of credentialed ZFA users:<br><br>guru 1314<br>works 1312<br>technology 1311<br>voyage 1311<br>training 1309<br>today 1307<br>ventures 1307<br>vacations 1306 | Consider whether this data has any intrinsic significance. Data doesn't show what users found in ZF; only that they got permission to look. May be of interest only in conjunction with other data (e.g., level of reported abuse on a TLD). FInally, might be interesting to compare with comparable data for legacy TLDs. |

| | | | | | |
|---|---|---|---|---|---|
| | of its gTLD. The process used by many existing Registries is to create and execute a contract for every zone data request. By contrast, the process is streamlined by allowing requestors using the CZDS agree to standardized Terms and Conditions before submitting one or multiple requests, and Registries can simply approve or deny requests with one click. Registries can also save time by appointing ICANN to handle zone data file formatting and transfer (AXFR) instead of using internal resources. | | | watch 1306<br>tips 1305<br>villas 1305<br>vision 1305<br>support 1303<br>solutions 1302<br>systems 1302<br>viajes 1301<br>supplies 1300<br>tools 1300<br>supply 1299<br>solar 1295<br><br>Bottom 20:<br><br>mls 93<br>xn--w4rs40l 92<br>pro 85<br>warman 68<br>ally 57<br>shop 45<br>mlb 36<br>anquan 35<br>shouji 35<br>xihuan 35<br>yun 35<br>bnpparibas 16<br>gdn 16<br>voting 9<br>unicom 8<br>htc 7<br>xn--8y0a063a 7<br>shaw 6<br>xn--mxtq1m 6<br>xn--5tzm5g 5 | |

| | | | | | |
|---|---|---|---|---|---|
| Assignment: DNSSEC Deployment Report<br>Volunteer:<br>Jamie | Website with graphical and spreadsheet depiction of TLDs that are DNSSEC-signed in the root and that are signed allowing for signing of SLDs. While number of signed TLDs is high, number of signed SLDs remains low. | Contractual requirement on registries to sign TLDs has accelerated deployment of DNSSEC at top level but not at second level | Data set of signed TLDs and SLDs. | 87% of TLDs (1160/1327) are signed; only 3% of SLDs are signed;<br><br>number of signed TLDs on 10/13: <200;<br>number of signed TLDs as of 3 June 2016: 1160 | Consider why DNSSEC adoption by registrants is so low and whether higher adoption would have positive impact on trust. |
| Assignment: TLD DNSSEC Report | Similar to report above, graphical depiction of DNSSEC deployment and list of signed TLDs as of 4 June 2016. Also lists TLDs that have not been signed (mostly ccTLDs) | Contractual requirement on registries to sign TLDs has accelerated deployment of DNSSEC at top level but not at second level | Data set of signed TLDs | Summary:<br>● 1327 TLDs in the root zone in total<br>● 1169 TLDs are signed;<br>● 1160 TLDs have trust anchors published as DS records in the root zone | Contractual requirement to deploy DNSSEC has had or could have positive impact on consumer trust. |
| Assignment: Deployment Guide: DNSSEC for Internet Service Providers (ISPs)<br>Volunteer:<br>Jamie | Published as part of ISOC's Deploy360 Programme, this is a high level piece encouraging ISPs to deploy DNSSEC in their networks with short description of deployment requirements. | ISOC Deploy360 programme has had a positive impact on ISP adoption of DNSSEC | More of a blog than a research program | None; advocacy piece | Research whether third parties like ISOC have had a positive impact on DNSSEC deployment |
| Assignment: CloudFlare: How DNSSEC works<br>Volunteer:<br>Jamie | Vendor webpage describing how DNSSEC works. | Availability of DNSSEC products and services will increase deployment at second level. | Narrative on how DNSSEC works. | None. Narrative description on DNSSEC. | Research whether availability of vendor products and services have had a positive impact on DNSSEC deployment |
| Assignment: DNSSEC- What it is and why is it important?<br>Volunteer: | ICANN staff created webpage describing DNSSEC in Q&A format. Page is archived as document was drafted | Does the availability of information on DNSSEC increase deployment | Q&A on how DNSSEC works. Out of date. | None. Q&A on DNSSEC. | |

| | | | | | |
|---|---|---|---|---|---|
| Jamie | before root was signed in 2010. Needs to be updated. | | | | |
| Assignment: ICANN Registry Agreements<br>Volunteer:<br>Carlton Samuels | The Base agreement formally covers in seven (7) articles the intentions and expectations from the delegation and operation of the gTLD, inclusive of the understandings, obligations and mutual covenants of ICANN and the registry operator. It also specifies and frames the process by which amendments to contract, the services and redress of grievances are addressed. | Where lies the responsibilities for safeguards, trust and consumer protections? | ICANN deems itself the capacity to execute and maintain the agreement; Registry Operator warrants it is competent to operate the registry per agreement; will only provide approved services and will follow all the rules and policies specified for provisioning registry services | The narrative is that by virtue of it being subject to public comment, the base agreement is developed by the community.<br><br>Amendments are purely bilateral, between ICANN and the RySG. The community may comment but has no standing otherwise.<br><br>The base contract is for ten (10) years, renewable.<br><br>The burden of technical acceptance of tld - and the extent and possibility of use - is solely that of the registry operator.<br><br>Services provisioned must be approved and in keeping with consensus policies. Any variation in service must be approved prior to launch or change.<br><br>Price changes must be notified to ICANN and registrars. [New policy will change that!]<br><br>Registry fee consists of 2 parts; fixed and transaction level fee. | Specification 6 & 7 outlines several safeguards pertinent to consumer trust and consumer confidence and protection; availability, abuse mitigation, name collision; minimum RPMs'<br><br>Specification 11 frames the PICs for registry<br><br>Maybe 3rd Party Liability for some actions might actually assist in enforcing the rules. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Registry operator must escrow registration data and with approved provider.<br><br>Registry operator must provide registration data publication services to specifications.<br><br>Mediation and arbitration are preferred modes for dispute resolution and ICANN's liability is strictly limited.<br><br>Some aspects of the contract, notably SLAs, PICs and clauses derived of consensus policies, are ring fenced from both arbitration or mediation.<br><br>Registry operator is obliged to indemnify and defend ICANN "and its directors, officers, employees, and agents" from all third-party suits, liabilities, costs, damages.<br><br>Registry is obliged to report specific data every month in a specified format<br><br>The amendment process is well defined:<br>It can only be initiated by ICANN or the RySG and may not be invoked more than once per year. | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | If deadlocked or stalemated, mediation is invoked by either party. If mediation fails, then arbitration.<br><br>Assuming agreement, the proposed amendment is published for public comment and all registries notified.<br><br>The public comment period must last a minimum of 30 days and is extensible.<br><br>At the end of the public comment period, the working party consider and adjudicate comments. Thereafter a final proposal is provided all registry operators and it is put to the vote of the ICANN board.<br><br>Assuming approval all around, the proposal[s] become effective 60 days after legal notice is served on all registry operators.<br><br>[Specifications 6, 7, 10 and 11 refer safeguards and trust matters.] | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Assignment:<br>Afilias Anti Abuse Policy<br>Volunteer:<br>Carlton Samuels | Policy is pursuant to the Registry-Registrar Agreement (RRA) and is intended to address all matters that Afilias considers "creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general."<br><br>Afilias recognizes a veritable smorgasbord of abuse factors, from spam thru fast flux hosting and child pornography to illegal access to computers and networks. | What is their experience in identifying domain abuse and how successful have they been in curbing them by the penalties exacted? | What has been the impact of new gTLDs on domain abuse and could any be traced to the new specs; Specs 6,7, 11. | TBD; Need domain abuse figures reported, action taken and impact. | Consider Afilias list of domain abuse factors as baseline and see what reporting mechanisms there are in their RRA for comparative analysis. |
| Assignment:<br>.RICH Anti Abuse Policy<br>Volunteer:<br>Carlton Samuels | i-REGISTRY is operator of the .rich TLD. The abuse policy is integral to their RRA. They broadly outline how the operator will respond to abuse which covers "general aspects of anti-abuse, acceptable use and rapid takedown and applies to registrars and registrants."<br><br>It identifies and share as common with Afilias their listed abuse factors but in response will engage in proactive screening, | Does the .rich domain abuse reports show any major comparable variations from that of Afilias and if so, in what specific areas?<br><br>What is the impact of Spec 6,7, 11, if at all? | The .rich Domain Abuse Report & how the PICs have performed. | TBD | Are new gTLDs experiencing domain abuse at a higher level than legacy TLD?<br><br>What is the nature of such abuse, if any?<br><br>Are the Safeguards in Specs 6,7 and 11 of any impact? |

| | | | | | |
|---|---|---|---|---|---|
| | inclusive of WHOIS records, expedited response to law enforcement requests.<br><br>i-REGISTRY also enumerate the abuse reports by type they will generate. | | | | |
| Assignment:<br>ICANN Global Consumer Research Report 2015<br>Volunteer:<br>Carlton Samuels<br>(Topics 2 &3) | The survey commissioned by ICANN aims to measure consumer awareness, choice and trust in the DNS in general and the new gTLDs in particular. The methodology adopted makes a distinction between end users and registrants; end user experience is reported here. An update is expected soon.<br><br>Visitation is the measure of awareness. | What is the level of awareness of consumers for the DNS and specifically, the new gTLDS?<br><br>Is trust and confidence in the DNS impacting end user behaviour? | Sample size 6,144 18+ year-olds in 24 countries on all continents.<br><br>Survey conducted online. | 46 percent reported awareness of at least one new gTLD<br>- 65 percent of those who are aware reporting they have also visited a new gTLD.<br>- .EMAIL and .LINK led in awareness and visitation of new gTLDs.<br><br>In comparison:<br>- 79% were aware of the legacy domains COM, NET, and ORG especially.<br>- 71% have visited those<br><br>Domains with an implied purpose and functional associations were the ones most recalled. | Only those already online has opinions!<br><br>74% percent are familiar with malware, phishing or stolen credentials.<br>Only 37% were aware of cybersquatting<br><br>What is the level of awareness of the safeguards or any of the domain anti abuse policies embedded in RRAs |
| Assignment:<br>SAC041-<br>Recommendation to prohibit use of redirection and synthesized responses by new TLDs<br>Volunteer:<br>Carlton Samuels | SSAC asserts that DNS redirection and synthesized DNS responses erode the trust relationships and present opportunities for malicious attacks, thusly undermining the stability and security of the DNS | Harmful and contrary messaging can be introduced in the error resolution process via an iterative resolver with capability to modify a response from an | Several respected researchers have reported the possibility of harmful outcomes from so-called | Wildcarding can spoof messages from authorized sources in a conversation. This could be exploited for cause, resulting in instability in the DNS resulting in an erosion of trust and decrease in the security of the system.<br><br>Existing services, such as email and spam filters are adversely affected | "Synthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which |

| | | | | | |
|---|---|---|---|---|---|
| | | authoritative source | wildcarding processes. Coming on a service request by an operator, this was further studied by a [RTS] Evaluation Panel and affirmed. | and can fail, resulting in economic harm to consumers and users of these systems. | the operator may have little control or influence.” |
| Assignment:<br>SSAC Advisory on Registrant Protection - Best Practices for Securing Security and Stability in the Credential Management Lifecycle<br><br>Volunteer:<br>Carlton Samuels | Credential management has been tapped as the source of many recent breaches of security. SSAC outlines the best practice for registries and registrars to enhance the security of domain names and the operating support systems pertaining with improved credential management. | The security of domain names and the systems that are used to provision them is maintained if certain practices are adopted and adhered to. | | Reporting of security breaches at registries and registrars must be instituted and established as part of ICANN compliance framework<br><br>The notice is contractually obliged and must include detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response<br><br>Stronger authentication practices must be encouraged in future Registrar - Registry Accreditation Agreements, inclusive of multi-factor authentication<br><br>ICANN should facilitate training of registries and registrar personnel in the best practices enumerated in collaboration with other | Determine the status of implementation, if any of SSAC Advisory. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | interested parties in the Internet ecosystem and with coverage of specific topics. | |
| Trust in the Internet Survey 2016<br>by<br>nccgroup and IDG Research Services | (Not a primary source for our work). This discussion paper gives a snapshot of consumers' current attitudes to the new gTLDs. research suggests that online security is an increasingly important part of "brand perception" | Regardless of the domain, most consumers are not highly confident with the new names. But there is variation between the trust levels of different names. '.brand' – domains that are brand specific such as .hsbc – and '.bank' engender the most trust. | Survey was fielded by IDG Research Services from Oct 16 2015 to Oct 22 2015. The results were collected through an online questionnaire . 5,000 people from the US and 5,000 people from the UK were surveyed. | Last year's survey suggested that there was a strong appetite for verification amid the flurry of new gTLDs.<br>This year's survey reinforces this view. Over 40% said that they don't feel enough is currently being done to protect their data. | => the ball is currently in businesses' court: The new gTLDs provide a significant opportunity for businesses to use them to differentiate and protect their brand – to secure the way their customers see them. |
| The NameSENTRY Abuse Report | | | | | |
| Techniques to Break the Botnet Attack | Technical Paper about Internet Relay Chat (IRC) protocol | A bot is a program that runs on an end-system performing tasks automatically. A botnet is typically seen as a | | Denial of Service (DoS) and then Distributed Denial of Service (DDoS) were implemented in these bots. A survey shows 90.4% of total emails were spam in June 2009. Among all spam, 83.2% was sent through botnets. | DNS Based Detection Technique<br>The bots use DNS queries in order to locate the C&C server hosted by the Dynamic DNS provider. Monitoring the traffic and the DNS makes it |

| | | | | | |
|---|---|---|---|---|---|
| | | network of bots that use computing resources for a malicious end. The botnet is generally controlled by a single entity called as botmaster. Botnets infect new machines using techniques common to most classes of malware, they are distinguished by their use of command and control (C&C) server. The master computer sends instruction to its bots through a command and control (C&C) server, which passes commands from the botmaster to bots, and sends stolen information from | | | pretty easy to detect the botnet and DNS traffic irregularity. This is most famous and easy technique to botnet detection but it will be tough to detect recent advanced botnet through this technique.<br>DNS Failure Graph<br>DNS Failures method is the simplest and yet efficient method for detecting the attackers network.DNS failure are rare to occure in any network,but in attackers network the graph of DNS failure rises while generating new malicious websites. This become a way through which the attackers network can be traced. This method studies the DNS faliure graph to detect the attackers network. |

| | | | | | |
|---|---|---|---|---|---|
| | | bots to their master. | | | |
| ISTR 20: Internet Security Threat Report | Symantec´s yearly report | All type of threats. Relevance of DNS specific threats: Section on WEB THREATS (pp.31-45) Poodle, ShellShock, and Heartbleed | | The total number of sites found with malware has virtually halved since 2013. | |
| Secure Domain Foundation, The Cost of Doing Nothing: The Business Case for Proactive Anti-Abuse<br><br>Volunteer: Drew Bagley | Survey of registrars about their anti-abuse practices and costs<br><br>Can potentially use as a primary source to illustrate wide interpretation of 2013 RAA as well as business/legal incentives for anti-abuse efforts connected to consumer safeguards and trust | Whether there is a business case for proactive anti-abuse | Surveyed registrars comprising a cumulative total of 35 million registered domain names. | Registrars differ from one another in how they interpret their responsibilities under 3.18 and 3.7.8 of the RAA 2013. Increased abuse complaints drive up costs for registrars. Proactive anti-abuse, detecting abuse before a complaint has been filed, can save money. Reputation matters for some registrars because of increased competition. Therefore, resources are spent responding to publicized complaints. | Look into how divergent methods of WHOIS verification and reasonable investigation requirements vary for new gTLD registrars. Determine if there is a direct correlation between varying interpretations of safeguards and prevalence of abuse as well as effect on public trust. |
| Amplified DDoS Attacks: The current biggest threat against the Internet<br><br>Volunteer: Drew Bagley | Brief overview of recent distributed denial of service attacks and interview with experts on how to mitigate future attacks | DDoS is a big threat that can be mitigated if ISPs adopted BCP38, thereby validating IP address sources | Interview cybersecurity experts | There is no valid reason for network operators to accept traffic from spoofed IP addresses (IP addresses that do not match up with the numbers in their source range). | Determine whether new gTLD operators (registries) have been affected by DDoS attacks |

| | | | | | |
|---|---|---|---|---|---|
| | Likely not a primary resource for purposes of the CCT Review | | | | |
| DNS Pharming: Someone's poisoned the water hole!<br><br>Volunteer: Drew Bagley | Article written in 2005, providing an overview of DNS cache poisoning<br><br>Likely not a primary resource for purposes of the CCT Review | Techniques for efficient DNS querying lead to reliance on DNS cache which can be corrupted to route users to malicious IP addresses. | | DNS cache poisoning on a local machine or DNS resolver can lead an Internet user to navigate to an attacker's website instead of the website to which the user intended to navigate. This may be done through pharming, by luring a user to click on a link in an email that leads the victim's machine to query the attacker's name server which then overwrites the local DNS cache with false IP addresses for legitimate domain names. | Determine whether there are any DNS cache poisoning issues unique to new gTLDs. Determine whether DNSSEC adopted has mitigated this. |
| WHOIS Accuracy Reporting System (ARS)<br><br>Volunteer: Drew Bagley | Website for the WHOIS Accuracy Reporting System reports<br><br>New report coming out in June 2016 - could be used as a primary source | Whether WHOIS data of registered domain names used valid syntax and whether information was operationally valid | | Phase 2 report indicates that, as of 2015, 97% of domain names were operating under the rules of the 2009 RAA due in part to grandfathering of already-registered domain names or already-accredited registrars.<br><br>There does not appear to be a significant different in the 2009 RAA-based accuracy of new gTLD WHOIS data over legacy new gTLD data. | Should determine if there is any correlation between WHOIS accuracy and DNS abuse and consumer trust |
| IETF- RFC List<br><br>Volunteer: Drew Bagley | Still assessing | | | | |
| DNS Stability, Security, and Resiliency | Could be used as a primary source | | | | https://www.icann.org/en/system/files/files/dns-s |

| | | | | | |
|---|---|---|---|---|---|
| Volunteer: Drew Bagley | Excellent overview of threats to the DNS system but mostly applicable to DNSSEC adoption issues for purposes of the CCT Review | | | | ymposium-25oct12-en.pdf |
| Registration Abuse Policies Working Group Final Report<br><br>Volunteer: Drew Bagley | Could be used as source article<br><br>Analysis of variations in registration abuse policies | | | | Research on registrar abuse policies should be informed by this report |
| SAC 025: SSAC Advisory on Fast Flux Hosting and DNS<br><br>Volunteer: Drew Bagley | | | | There are patterns of fast flux hosting related domain names | Is fast flux hosting more or less prevalent in new gTLDs? |
| Article/Volunteer | Observations | Hypothesis | Research | Findings | Possible recommendations & Champion |
| Article : Search Engine Poisoning (SEP)<br><br>Volunteer : David | SEP is common practice amongst hackers. The goal is to make use of search engine results to draw users to sites that contain malware.<br>Popular Search Engine results are manipulated or the malicious site may appear as a sponsored link. The popular sites are infected by XXS (Cross Site Scripting) | Are new gTLDs more subject to SEP as the TLD may in itself be a keyword? | | The hacker selects URLs taken from domains that rank high in search engine.<br>The bad actor creates a huge number of URLs containing targeted keywords.<br>The target keywords become associated with these URLs.<br>These are then included in forums, user comments or reviews and leading a server delivering the malware. This is XXS (Cross Site Scripting). The attacker is not taking over the website. | Assess whether new gTLDs are more vulnerable to SEP attacks than legacy ones?<br>Assess whether specific new gTLDs being targeted?<br>What solutions have been offered if any by new gTLD registries?<br>Are search engines "avoiding" certain TLDs?<br>Consider the improvements which can |

| | | | | | |
|---|---|---|---|---|---|
| | They become intermediaries that redirect unsuspecting users to malicious sites.<br>It is a DNS abuse though not sure how easy to quantify.. | | | The poisoned results get high ranking for the target keywords given the high ranking domains in the first place + large amount of references in these URLs.<br>Significant economic consequences on targeted companies: brand damage, loss of customers, decreased rankings. | be made by search engines to return more sanitized references to consumers. |
| Article : Spoofing Attack : IP, DNS & ARP<br><br>Volunteer : David | Spoofing attacks are when a malicious party impersonates another device or user on a network in order to launch attacks (malware and viruses)<br>It is a DNS abuse though not sure how easy to quantify.. | Are new gTLDs any more subject to Spoofing attacks than legacy gTLDs?<br><br>Can a user trust the domain name has not had its underlying DNS spoofed?<br><br>Internet Users want to be assured that when they type in a certain domain name that they go to the right domain name and that the DNS has not been hijacked. | | 3 of the most common types of Spoofing attacks are :<br>- Via IP<br>- Via ARP<br>- Via DNS<br>DNS Servers Spoofing attacks are executed by modifying the DNS server in order to reroute a specific domain name to a different IP address | Consider the vulnerability of new gTLDs regarding Spoofing attacks and the impact on companies and on consumers.<br><br>Which new gTLD registries are offering additional protection and if so how?<br><br>If so to what extent successful? |
| Article : fTLD Enhanced Security | fTLD Registry Services offer for .bank and .insurance enhanced trust | Are the security requirements listed by fTLD | fTLD Registry Services, LLC provides a | fTLD Registry Services, LLC offers solution to protect Domain Names and the servers associated against | Study if it is feasible to implement mandatory higher security |

| | | | | | |
|---|---|---|---|---|---|
| Volunteer : David | Should such enhanced trust, it it works, not be extended across all new gTLDs? | enough to limit DNS abuse? Would it be feasible to oblige all (which?) Registries to ensure a higher level of security? | detailed list of Security Requirements. Consider these and other TLDs that may provide (eg .TRUST) | different types of attack including spoofing, phishing and other malicious activities. p.2 | requirements to prevent more DNS abuse? Identify and review other new gTLD registries that have put in place enhanced security.<br><br>Consider the tenability of a position of prohibiting Proxy/Privacy Registration Services.<br><br>Consider the recommendations of the WHOIS Review Team. |
| Article : Frequently Asked Questions: Name Collision Occurrence Management Framework for Registries<br><br>Volunteer : David | This occurs when a TLD is being used in an internal network. A query for that internal TLD could end up in the public DNS | Did the Name Collision Occurrence Management Framework work? What examples can be identified showing name collisions were avoided? | Review Report on effectiveness from ICANN? Review reports on effectiveness of not or other comments from Registries | No findings from the ICANN FAQs, need to assess usefulness from objective sources. | Identify any ICANN or Registry reports on effectiveness of the Framework and issues avoided as well as what could be improved in the future. |
| Assignment: The Curse of the URL Shorteners: How Safe Are They?<br>Volunteer: Fabro Steibel | URL<br>Shortening services like bit.ly Google and<br>Microsoft are popular. | identify the effectiveness of security measures put in place by the various URL shortening services | we attempt to create shortened URLs to create a shortened link to any infected | This limited experiment shows that URL shortening services have a long way to go before<br>Internet users can trust them to deliver safe links. About half of the most popular URL | URL shortening services Are a threat. They can improve and provide a safer web experience for their users. Can we measure how well they are doing? |

| | | | | | |
|---|---|---|---|---|---|
| | Credible sources, like ISC SANS, show that URL shortening services, when compromised, can provide a mechanism for malicious hackers to infect unsuspecting visitors.<br><br>Criminals use these services to bypass Google's Safe Browsing service, which is used by popular browsers.<br><br>URL shortening services have partnered with security companies to identify malicious URLs and websites. Some of them even use the SURBL blacklists to identify if someone has tried to link to a malicious website. | Do URL shortening services have any kind of security measures in place? How effective are these security measures? | domain(stage 1) or malicious full URL (stage 2). Data, feb/2010 | shortening services seem to be somewhat effective at blocking access to well known malicious URLs that can be found on blacklists.<br><br>It seems that popular services like bit.ly, which do try to use blacklists in order to prevent malicious hackers from using their services and pointing to bad websites, can still be easily fooled by chaining together shortened URLs created by another service. | Note: research was from 2010. We probably would need to repeat the test to consider the results valid, |
| Assignment: SYMANTEC INTELLIGENCE REPORT NOVEMBER 2015 Volunteer: Fabro Steibel | Symantec report on Targeted Attacks & Phishing, Vulnerabilities, Malware, Mobile & Social Media, and Spam<br><br>Ps: read with https://www.symantec.com/security-center/threat-report | None. It is a descriptive analysis of evolution of Internet threats, with no mention to gTLDs | comprehensive source of Internet, which is made up of more than 57.6 million attack sensors and records in over 157 countries | Public Administration was the most targeted sector<br><br>Organizations with 251-500 employees were most likely to be targeted by malicious email<br><br>In terms of targeted attacks in general, the Finance, Insurance, & Real Estate sector was the most targeted | Probably, the most targeted gTLD threats are public administration, large organizations, finance, insurance and real state. |

| | | | | | |
|---|---|---|---|---|---|
| Assignment:<br>Redirecting DNS for Ads and Profit<br>Volunteer: Fabro Steibel<br><br>ps: | Error traffic monetization solutions leverage the context provided by ISP customer traffic in order to rewrite protocol error messages to valid responses, redirecting<br>users toWeb servers that show advertisements or search results hopefully of interest to the user.<br><br>Security researchers have exploited<br>cross-site scripting vulnerabilities in two providers' ad<br>servers to demonstrate fairly sophisticated phishing and cookie theft attacks | We also observe a more aggressive form of DNSdriven traffic manipulation, search-engine proxying. | analysis of the redirection pages collected between Jan/2010 and May/11, the location and content of the ad servers, and the marketing material provided by the companies involved. | One monetization vendor reroutes all user search queries to Bing, Yahoo, and (sometimes) Google via proxy servers controlled or rovided by Paxfire. profits of 1–3 USD per customer per year<br><br>Most monetization<br>occurs in Italy (40%), the US (33%), Brazil (33%),<br>Argentina (27%), Germany (25%), and Austria (20%).<br>The UK (18%), Canada (15%), and Spain (12%) occupy<br>the medium range. ISPs in Australia, Belgium,<br>Finland, France, Israel, Lithuania, New Zealand, Norway,<br>Poland, Russia, Sweden, and Switzerland do not<br>commonly use DNS error monetization: these countries have wildcarding adoption rates below 10%. | It suggest that ICANN wants to fight redirecting DNS. There , is a possibility of end user threats in redirecting DNS, that is not document in the article. However, considering that up to 1/3 of traffic is redirected In some major countries, there is a possible urge to tackle the issue. Note: this is not a gTLD particular issue, it refers to all web traffic |
| From .academy to .zone:<br>An Analysis of the New TLD Land Rush | new TLDs have resulted in a burst of defensive registrations as companies aggressively defend their trademarks to<br>avoid consumer confusion.<br><br>Data from latest monthly registry reports | This paper analyzes the types of domain registrations in the new TLDs to determine registrant behavior in the brave new world of naming abundance. We also examine | We gather DNS, Web, and WHOIS data for each new domain, and combine this with cost structure data from ICANN, the registries, | We find that only<br>15% of domains in the new TLDs show characteristics consistent with primary registrations, while the rest are promotional, speculative, or defensive in nature; indeed, 16% of domains with NS<br>records do not even resolve yet, and 32% are parked. Our financial analysis suggests only half of the registries have earned enough to | The paper concludes that the new gTLDs have<br>yet to provide value to the Internet community in the same way as<br>legacy TLDs. |

| | | | | | |
|---|---|---|---|---|---|
| | on January 31, 2015, which altogether totals 502 new TLDs.<br><br>We have focused our analysis on why registrants spend money on domains in the new TLD program.<br><br>We differentiate public and private TLDs by checking public information about the start of general availability<br><br>we focus on domains that reached general availability (GA) before our February 3, 2015<br><br>We gathered pricing data for domains in the new gTLDs from a wide range of registrars<br><br>We also compare new domain registrations with URIBL, a publicly available domain blacklist, to see how the blacklist rate compares between old and new TLDs | the cost structures and monetization models for the new TLDs to identify which registries are profitable. | and domain registrars to estimate the total cost of the new TLD program | cover their application fees, and 10% of current registries likely never will solely from registration revenue.<br><br>351,457 xyz domains (46% of xyz) remain unused and display a standard Network Solutions registration page when visited in a Web browser.<br><br>Overall, the introduction of the new TLDs had only minimal impact in the rate of registration of the old TLDs<br><br>*Content Category* — *Results*<br>No DNS 567,390 15.6%<br>HTTP Error 362,727 10.0%<br>Parked 1,161,892 31.9%<br>Unused 504,928 13.9%<br>Free 432,323 11.9%<br>Defensive Redirect 236,380 6.5%<br>Content 372,569 10.2%<br>**Total** 3,638,209 100.0%<br><br>Registrants purchase domain names from a registrar and pay a yearly fee to keep them, yet a large fraction of domains in the new gTLDs do not even resolve. | |

| | | | | | |
|---|---|---|---|---|---|
| Assignment: Best Practices to Address Online and Mobile Threats<br>Volunteer: Fabro | This report provides readers with a plain language description of the threats facing businesses, network providers and consumers in the online and mobile threat environment, and suggest best practices for industry and governments to address these threats<br><br>Malware and Botnets, Phishing and Social Engineering, Internet Protocol and Domain Name System Exploits, Mobile, VoIP, and Telephony Threats, Hosting & Cloud | This is a descriptive study, with general best practices | none | Domain name registries in both the generic Top Level Domain (gTLD) and country code Top Level Domain (ccTLD) spaces, as well as the registrars they do business with, should implement and closely oversee 'Know Your Customer' programs to prevent abuse of domain assignment. That will allow them to determine if and when they should avoid conducting business with a registry, a registrar, a reseller or a privacy/proxy service provider.<br><br>For privacy/proxy services, there is an urgent need for accreditation programs to be implemented and enforced. This will clarify the rules and processes for handling requests to relay, pass communications to the underlying customer, and reveal, disclosing the customer's identity. This applies to all privacy and proxy services, regardless of whether they operate in the gTLD space or the ccTLD space and regardless of whether they are owned, managed or operated by a registry or a registrar. | They suggest registrars to implement accreditation programs |
| | | | | | |
| Assignment: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Volunteer: Calvin | | | | | |
| Assignment: WHOIS Accuracy Reporting System (ARS) Volunteer: Calvin | | | | | |
| Assignment: About the DNS Seal Project Volunteer: Calvin | | | | | |
| Assignment: WHOIS Primer | | | | | |
| Assignment:SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook Volunteer: Calvin | | | | | |
| Assignment:Measuring the DNS Volunteer: Zuck | Article discusses potential methodology for developing metrics around DNS health. More appropriate for SSRT and the Health Index effort. | | | | |
| | | | | | |
| | | | | | |