February 27, 2018

Dear Mr. Hedlund:

The undersigned global businesses and their customers depend upon the continuing security, stability and resiliency of the Internet, and thus have significant interests in domain name industry issues and outcomes. We are amongst the leaders in working to protect the interests of customers and those of the broader Internet from domain name system (DNS) abuse, in various ways. As long standing participants in ICANN- and industry-related conversations and policymaking, we are contacting you with our concerns about serious harm occurring to Internet users, and a request for action that we believe would serve the interests of the broader community.

Under your direction, ICANN's Compliance team has broadened the various forms of feedback it seeks from the broader community. This is much appreciated. Accordingly, we write with concerns that you and your department are in a position to help resolve.

We commend ICANN for orienting its policymaking function towards a more data- and fact-based approach. This orientation of course depends on the availability of data and reports that provide an accurate view of the DNS and the impact of DNS abuse on stakeholders. While there is more data that needs to be collected and analyzed, it's gratifying to see that ICANN Org is now in a better position to use and publish more widely available and reliable data to better evaluate DNS harm to users and more effectively exercise its responsibilities to help remedy ongoing harms.

Specifically, ICANN and the community now have at their disposal published data--namely, the Statistical Analysis of DNS Abuse in gTLDs (SADAG) report and the ongoing Domain Abuse Activity Reporting (DAAR) System regarding rates of abuse in the DNS. These rates are regrettably showing stark increases and serious concentrations of abuse across legacy and new gTLDs, registries and registrars, and in the proliferation of spam, malware, phishing and other harms. For example, according to the Domain Abuse Activity Reporting (DAAR) System report:

- the 25 most exploited TLDs account for 95% of the abuse complaints submitted to DAAR.
- Five TLDs alone are responsible for more than half of abuse complaints.

Additionally, according to the SADAG report[1]:

- The number of abused phishing domains in legacy gTLDs is mainly driven by the .com gTLD and at the end of 2016 represents 82.5% (15,795 of 19,157) of all abused legacy gTLD domains considered in this study. (pp.10-11)
- …the five new gTLDs suffering from the highest concentrations of domain names used in phishing attacks listed on the APWG domain blacklist in the last quarter of 2016 collectively owned 58.7% of all blacklisted domains in all new gTLDs. (p.11)
- …we observe as many as 182 and 111 abused .work and .xyz domains, respectively. The results indicate that the majority of .work domains were registered by the same person. 150 domains were registered on the same day using the same registrant information, the same registrar, and the domain names were composed of similar strings. Note that only 150 abused

[1] The SADAG report relies on data from SpamHaus, the Anti-Phishing Working Group (APWG), StopBadware, SURBL, the Secure Domain Foundation (SDF) and CleanMX.

domains, blacklisted in the third quarter of 2015, influenced the security reputation of all new gTLDs. (pp.11-12)

- ...the overwhelming majority of malware domains, which were categorized as compromised, belong to one of four new gTLDs: .win, .loan, .top, and .link (77.1%, which represents 19,261 out of 24,987 domains). (p.13)

Troublingly, there also is a clear problem with one particular contracted party:

- We find distinctive common patterns in domain name registration further suggesting malicious registrations. For example, we find 9,376 .link domains of which 9,256 were created in the first quarter of 2016 and 9,253 were registered with Alpnames Limited registrar. (pp.13-14)
- …for 37.09% of the abused new gTLD domains reported by StopBadware, the sponsoring registrar is located in Gibraltar. Almost 195 abused new gTLD domains per 10,000 located in Gibraltar are abusive. (p.19) (Note: Alpnames is located in Gibraltar.)
- …we find that the abuse is driven by a single registrar: Alpnames Limited. For example, during the study period this registrar has acted as the sponsoring registrar for 53.97% (59,044) of the new gTLD domains that have been blacklisted by Spamhaus. (p.19)
- [Figure 31] shows one registrar, Alpnames Limited, having a high volume of abusive new gTLD domains reported by both Spamhaus and SURBL. (p.19)

You'll agree these are troublesome statistics, and are antithetical to a secure and stable DNS administered by ICANN.

We are alarmed at the levels of DNS abuse among a few contracted parties, and would appreciate further information about how ICANN Compliance is using available data to proactively address the abusive activity amongst this subset of contracted parties in order to improve the situation before it further deteriorates. Also, can ICANN provide any details as to whether the higher rates of abuse (as documented above by parties that appear not to be the subject of enforcement notices) correlates to specific breaches of the RA and RAA by the relevant contracted parties[2]? Are there specific hurdles that Compliance perceives that inhibit enforcement activity against such contracted parties? Has ICANN prioritized its attention to compliance matters relating to such parties and does it have sufficient resources to handle them before they reach a new stage of criticality?

Specifically, is Compliance more assertively applying Specification 11(3)(b) of the Registry Agreement, compelling offending registry operators to disclose actions taken against security threats? How is ICANN's Consumer Safeguards effort playing a stronger role in determining new areas for compliance action?

Not only do we look forward to hearing the details of ICANN Org's comprehensive actions in this area, we seek, as an immediate and urgent matter, compliance action on the worst offenders in current ICANN reports.

We also would like to know additional ways in which the undersigned parties could support ICANN in this broad endeavor. If helpful to develop steps forward, we welcome an in-person meeting with you, other relevant ICANN Org executives, and your staff.

[2] https://features.icann.org/compliance/enforcement-notices We note that none of the parties named in the SADAG report appear to be the subject of currently documented Compliance actions.

Over the long term, we suggest development of a data-driven roadmap for compliance based on key information and statistics. We encourage Compliance to consult with the wider community to help shape this data-driven roadmap, and we look forward to offering our further input.

Thank you for your attention to this letter. Please direct your reply to The Independent Compliance Working Party, c/o Fabricio Vayra at fvayra@perkinscoie.com.

Sincerely,

Adobe Systems, Inc.
DomainTools
eBay Inc.
Facebook, Inc.
Microsoft Corporation
Time Warner Inc.