Submitted May 19, 2009

Background

The Registry Internet Safety Group (RISG) is a global group of responsible Internet-related organizations whose mission is to facilitate dialogue, affect change, and promulgate best practices to address Internet identity theft, especially phishing and malware distribution. RISG is registry-focused, and includes organizations with significant experience related to the policy, legal, and operational challenges related to domain name security. The current membership includes registry operators Afilias (.INFO), NeuStar (.BIZ, .US), Nominet (.UK), The Public Interest Registry (.ORG), and SIDN (.NL); security firms Cyveillance, Internet Identity, McAfee, and Symantec; registrars GoDaddy.com, MarkMonitor, MelbourneIT, Network Solutions, and Oversee.net; and observers from law enforcement agencies.

RISG offers the following thoughts about "Potential for Malicious Conduct" to ICANN as it considers the issues of security and malicious uses of domain names as part of its New TLD process.

GENERAL PRINCIPLES AND APPROACHES

RISG's general approach is to create effective best practices that registries (and registrars) can adapt according to their needs and circumstances. We have taken this approach because:

A) Individual registries face widely varying types and levels of domain name abuse. Some registries do not experience some types of abuse at all, while others face very low levels.

B) It is important to understand the many different kinds of malicious uses of domain names. Each must be defined, measured, confirmed, and mitigated in separate ways.

C) A registry must meet the restrictions or requirements imposed by the jurisdiction(s) in which it is based or operates. ICANN-regulated TLDs must also comply with their ICANN contracts. RISG has researched how national and EU privacy laws prevent the sharing of certain kinds of registration and contact data relevant to domain names being used for malicious purposes. In another example, ICANN has recognized that gTLD registries and registrars may be prevented by local laws from fully complying with the provisions of ICANN contracts regarding personal data in WHOIS.

D) Registries legitimately have different business plans, and therefore different sales channels and registrant bases.
E) Registries (and registrars) can often choose different -- but effective -- ways to solve a particular problem.

These factors have indicated to us that specific policies or implementations often can't be applied well across TLDs. Rather, each TLD can shape policies and procedures according to its needs, and share ideas about what works.

The RISG's discussions of "security" generally include criminal issues such as phishing, malware distribution, and related problems. While laws vary by jurisdiction, we think that reasonable people can agree that theft and fraud are unlawful, and are of concern because they target multiple victims across the Internet-using public. Our group does not discuss cyber squatting and intellectual property infringement. We do not consider those to be security issues since they are civil disputes between individual parties and special dispute resolution processes exist to examine domain name disputes. We suggest that ICANN define security concerns clearly. ICANN's New TLD "Analysis of Public Comment" sometimes conflated "security" with intellectual property disputes between two parties. That makes the conversation about criminal behavior on the Internet, and its relations to the domain name system, sometimes confusing.

Our opinion is that no one party -- and no one type of entity -- can fight the problem of e-crime alone. Collaboration, data sharing, and education are effective and important.

It is our understanding that ICANN is focused on threats to the security and stability of the DNS itself, as well as making recommendations for DNS best practices such as using DNSSEC protocols and adopting smart practices for DNS caching on the Internet. We note that "threats to the security and stability of *the* DNS" may be very different issues from "malicious conduct *involving* the Domain Name System."

These are important distinctions. All of us want a safer Internet that can be trusted by users. The question is how to go about it, and what parties can help. We believe that ICANN is a very useful forum for parties to come together and pursue information exchange and education. The role of ICANN policy-making in addressing e-crime may be limited, but the many organizations and governments that participate in ICANN often have the ability to effectively pursue e-crime initiatives outside of ICANN and its policies.

Due to its nature and decision-making processes, ICANN may not best suited to create specific solutions to address the quickly evolving e-crime landscape. In general, prospective requirements or policies about domain names registration should give freedom to the parties on the ground to work out implementation details, and binding policy implementation details should be drafted by experts.

SPECIFIC ISSUES

ICANN asked the RISG four specific questions. These are questions about what might happen in the future. Of course, no one can predict the future accurately, especially when new variables are introduced. ICANN's New TLD program does introduce relevant new variables. What we offer below are observations about historical trends, and some topics that ICANN should consider.

Q1) "What, if any, trends have registries observed in the criminal activity that can be directly associated with increases in the overall number of domain names or with the addition of new generic top level domains (such as .cat, .jobs, .mobi, .tel, .travel)? What trends have you or your organization observed in the volume of illegal behavior or malicious conducts which are directly associated with increases in allocated domain names?"

It is difficult to predict how the security landscape will change, especially when considering variables such as how many TLDs may be introduced at once and by whom. We believe that the following trends should be taken into consideration prior to the launch of any new TLD.

ICANN's new TLD "Analysis of Public Comment" reported on certain concerns raised by third parties that new TLDs will offer criminals new resources to take advantage of, and will make abuse mitigation more difficult. As expressed on page 35, the concern that "the new [TLD] program will create a new wave of malicious activity, including spam and phishing", and on page 37, "Confusion at the second level. That is, expanding the number of TLDs will expand the number of locales at which abusers of the system could register second-level names intended to dupe end-users." Our related observations are:

A TLD may become more of a target for criminals once it becomes accepted by and known to end-users. Criminals also tend to migrate from TLD to TLD (and registrar to registrar) over time. The criminals move on as the affected registries and registrars become aware of problems and implement mitigation procedures. This already happens in the 200+ TLDs already in existence, and among the hundreds of ICANN-accredited registrars. We assume this pattern will continue.

It is logical that as a TLD grows and Web site usage in the TLD increases, that some of its domains will inevitably be compromised by criminals. The measurement of problems in a TLD should therefore take into account the overall size of the TLD. The APWG and ICANN's Fast-Flux Working Group have used such methods to see if problems are more pervasive in one TLD versus another.

As adoption of new TLDs gain acceptance on the Internet, criminal activities will keep evolving toward using these new TLDs. For example, recent organized phishing attacks against several major financial Institutions shows the use of multiple gTLD and ccTLD extensions, including .com to .mobi.

Q2) "In cases where urgent measures are needed to deal with malicious conduct involving the Domain Name System, what challenges exist? What measures can be employed by registries and registrars to speed response?"

Registries and registrars face a number of challenges regarding abuse mitigation. They include but are not limited to:

- Legal issues, such as varying privacy laws and government regulation and control. There are legal risks involved in identifying and suspending domain names, particularly in cases of false-positives.
- Some cases of alleged abuse or malicious behavior are difficult to identify and verify, thus increasing the complexity, cost, and risk of mitigation.
- Technical challenges, including obtaining, examining, and acting upon high-quality data. Some of those challenges are:
    - Need for data that is timely and in a format that can easily be shared with other interested parties. There is no standard data format as of yet. This is one area RISG is working to define.
    - Adoption of best practices which recommend retention policies for expired A-records often realized by long-cache TTL.
    - Registrant data is both dispersed as well as inaccurate.
- Costs. Security work is a cost center that impacts the bottom line. Assuming these costs is not business-critical for some registries and registrars, or is not given the same priority by others.

Q3) "As the current model of cooperative interaction between registry – registrar – security organizations and law enforcement - scales to become more global, what new processes will be needed to mitigate malicious conduct that utilize the Domain Name System?"

Cooperation and interaction between such parties is already global. We urge further voluntary data-sharing and cooperation between interested parties. The mitigation of “malicious conduct that utilizes the Domain Name System” seems largely beyond ICANN’s scope, as noted above.

There are criminals who operate across TLDs, such as phishing gangs and the creators of the Conficker worm, and responses against them can be coordinated across TLDs. It remains to be seen whether coordination in the DNS community can be scalable, and amongst TLDs may not be an appropriate in some situations. For example, Conficker was initially slowed by coordination amongst TLD operators, but Conficker’s creator then adopted a peer-to-peer communication model that bypassed the DNS community’s response efforts.

We suggest that ICANN, where appropriate, take steps to become aware of threats to the security and stability of the DNS itself as they develop, and to then inform and cooperate with relevant parties who can help prevent or mitigate such problems. New gTLDs have the potential to transform the organization of the DNS, and for this reason should be pursued in a cautious manner.

Q4) "What specific measures can be employed by ICANN as a corporation to mitigate any potential increase in malicious conduct that might arise solely from the additions of new gTLDs?"

Upon submission, new gTLD applications undergo an Applicant Review as part of the Initial Evaluation process, which includes an examination of the applicant’s technical, operational, financial, and service capabilities. As part of this Initial Evaluation, we recommend that ICANN also consider whether the applicant has sufficiently addressed abuse topics, including any proposed policies or anti-abuse procedures (based upon current best practices as defined by industry leaders). Applications that fail to include any mention of abuse should be referred to the Extended Evaluation process.

The ICANN compliance staff has a central role in ensuring that registrars respond to WHOIS complaints, and making sure that registrars are maintaining their WHOIS servers properly. The ICANN compliance staff should conduct regular reviews of all registrars’ compliance with WHOIS requirements, in accordance with existing agreements and consensus policies.