SAC 022
SSAC Advisory on Domain Name Front Running

An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)
October 2007

Executive Summary

This Advisory considers the opportunity for a party with some form of insider information to track an Internet user's preference for registering a domain name and preemptively register that name. SSAC likens this activity to front running in stock and commodities markets and calls this behavior *domain name front running*. In the domain name industry, insider information would be information gathered from the monitoring of one or more attempts by an Internet user to check the availability of a domain name.

When the domain name of interest for which an availability check is made is registered shortly after such a check, the individuals making the availability check may reasonably assume that the organization operating the web site or service they used to determine the availability of the name preemptively registered the name. Registrants have filed complaints with ICANN, registrars, and with Intellectual Property attorneys that suggest domain name front running incidents may have occurred. SSAC does not yet have any hard data to draw conclusions regarding the frequency (if any) of the occurrence of domain name front running.

SSAC acknowledges that a perception exists within the community that monitoring or spying is taking place when would-be registrants check the availability of a domain name. Much of the information presented before SSAC regarding domain name front running is anecdotal and incomplete. The information SSAC has reviewed allows us to observe that some part of the community believes monitoring practices that result in preemptive registration of domain names have occurred and that such practices are not acceptable. SSAC is concerned that, whether real or perceived, preemptive registration portrays an unfavorable image of the domain name industry. This Advisory is therefore a preliminary study and is intended to put the issue before the community for discussion and to solicit well-documented incidents, if any can be obtained.

In this Advisory, SSAC begins with a premise that *checking the availability of a domain name can be a sensitive act which may disclose an interest in or a value ascribed to a domain name*. SSAC suggests that any such domain name availability lookups should be performed with care. Our premise is that a registrant may ascribe a value to a domain name; that unintended or unauthorized disclosure, or disclosure of an availability check by a third party without notice may pose a security risk to the would-be registrant; and that availability checks may create opportunities for a party with access to availability check data to acquire a domain name at the expense of the party that performed an availability check, or to the benefit of the party that monitored the check. We attempt to assess these risks and suggest ways that information could be collected and used to engage in domain name front running activities.

SSAC observes that there does not appear to be a strong set of standards and practices to conclude whether monitoring availability checks is an acceptable or unacceptable practice. We conclude this Advisory with a call for public comment; specifically, we invite registrants, registrars and other parties who have information regarding possible domain name front running incident to report that incident to the committee with as much information as possible to assist SSAC in studying this matter further.

Introduction

This Advisory considers the opportunity for a party with some form of insider information to track an Internet user's preference for registering a domain name and preemptively register that name. This type of activity has been called domain name grabbing and preemptive registration in other contexts. SSAC compares this activity to front running in stock and commodities markets and thus calls this similar behavior *domain name front running*. In the domain name industry, insider information would be information gathered from the monitoring of one or more attempts by an Internet user to check the availability of a domain name.

Several possible incentives have been suggested to SSAC as motivations to engage in domain name front running. One possibility is that a domain name that is of interest to one or more Internet users has potential for domain name monetization[1]. A second possibility is that a domain of interest to an Internet user may have a commodity value in a secondary (resale) market; in particular, the domain name front runner might seek to sell the domain name registration to the party whose queries prompted the preemptive registration of that domain name.

Alternative explanations have also been suggested. Apparent instances of domain name front running may be mere coincidence or a consequence of domain name tasting[2]. Domain name tasting usually occurs during the 5 day Add Grace Period (AGP) so that the taster can cancel domain names deemed to be unprofitable before the AGP expires and recover the cost of registration. In any given month, over a million domain names can be tested for their potential to be profitable for monetization, and there is a reasonable chance that some of these names may coincide with names that have been subject to some form of a domain name availability check during that month.

Background

When the domain name of interest for which an availability check is made is registered shortly after such a check, the individuals making the availability check might (incorrectly) assume that the web site or service they used to determine the availability of the name preemptively registered the name. Registrants have filed complaints with ICANN, registrars, and with Intellectual Property attorneys that suggest domain name front running incidents may have occurred. At this time, SSAC has preliminary information from an intellectual property attorney regarding two alleged incidents of domain name front running. The attorney, however, has asked that SSAC refrain from disclosing the domain names and parties involved while the law firm continues to investigate these incidents. SSAC has also requested information from other sources who claim they have been victimized by domain name front running activities and is involved in ongoing discussions

[1] Domain Name Monetization is a practice whereby a set of pay-per-click (PPC) links and associated websites are automatically created for each domain name, each of the links generating an income to the domain registrant when users arrive at the website and click any of the links or associated websites.

[2] Domain Name Tasting is a practice where a party registers a domain name and tests to see whether a web site hosted using the name can attract traffic and earn revenue via advertising.

with other law firms; members of the registrar and registry communities; and security and domain name experts.

SSAC does not yet have any hard data to draw conclusions regarding the frequency (if any) of the occurrence of domain name front running. We do know that Internet users have filed complaints of suspected domain name front running incidents with registrars and ICANN. Some complainants offer (pre- and post-incident) WHOIS query results to support their claim. These data alone are often insufficient to determine whether the domain name was preemptively registered, how the data used to preemptively register this particular domain name were acquired, or whether this was an intentional or coincidental act.

Several factors contribute to difficulties SSAC and others have experienced when attempting to collect detailed information concerning these incidents. No strong set of standards and practices exists to conclude whether monitoring availability checks is an acceptable or unacceptable practice. To date, domain name front running complaints have been processed independently by the contacted parties, e.g., registrar and ICANN staff. No common reporting mechanism or agreed-upon characterization of what constitutes a domain name front running incident has been established by the community. Registrants who do not suspect abuse do not carefully document availability checks as they perform them, and are not familiar enough with the details of domain name registration to know what to document and report should they suspect that domain name front running has occurred. Registrants do not even know that they could be a target of domain name front running.

This Advisory defines and characterizes domain name front running using information collected from members of the registrar, registry and DNS communities, ICANN staff, and members of the community at large. These sources (or their organizations) have been contacted by registrants who have filed complaints regarding what they conclude to be a domain name front running incident. These sources (or their organizations) have investigated incidents that registrants claim to be characteristically similar to what SSAC defines here as domain name front running activities. Based on the currently available information, SSAC has developed a composite list of methods domain name front runners might employ to analyze DNS and WHOIS query data, identify domain names of interest, and preemptively register those domain names.

Domain Name Front running

During the latter half of the 19th century, certain settlers to what is now the southwestern region of the United States devised ways to preemptively file or *jump* a claim on a parcel of land prior to the official start of land runs established following the Indian Appropriation Act of 1889. Preemptive claim filing was also common during the North American Gold Rushes of this period. Settlers and miners who engaged in claim jumping shared several common characteristics: they had access to information (surveys, maps, geology reports), information holders (engineers, cartographers, territorial officials), or the land itself that allowed them to speculate and choose which land was most valuable;

they had advanced notice of a time when a claim would be filed for that land; and they had the means to filing the claim before another party could do so.

A practice known as front running was exposed long ago in the stock and commodities markets. Front running occurs when a broker fills an order for a security in his personal account based on trades or information disclosed by the broker's client (who is often privy to "insider" information) *prior* to filling his client's order. Front running trades are illegal under U.S. and other securities trading laws.

A domain name front running opportunity shares characteristics attributed to claim jumping and to front running trading as well. Domain name front runners, if such actors exist, exploit an opportunity to gather information, often in near real-time and from various sources; use that information to deduce whether a domain name is currently of interest to one or more parties; and preemptively register the domain name.

Methods of Monitoring and Identifying Domain Names of Interest

Registrants as well as interested parties in registrars, registries and staff at ICANN describe various opportunities for monitoring and identifying domain names of interest. SSAC has compiled this list to help the community appreciate the several means a front runner has at his disposal and to assess the risk that domain name front running poses. We include all the opportunities mentioned here; however, SSAC does not claim that any or all these methods are currently being used, or that this list is exhaustive, only that these represent plausible opportunities for gathering and monitoring domain names of interest to prospective registrants, and that these have been related to SSAC by parties who have anecdotal or partial information regarding a possible domain name front running incident.

Client software. Free- and shareware WHOIS client applications, Browser Helper Objects (BHOs), extensions, plug-ins and cookies are all essentially application software. Such applications can be programmed to record WHOIS queries, domain name queries, search engine arguments, etc. and relay these over covert connections – *back channels* – to the software developer or affiliated 3rd party of the developer. The query data could be used by the developer, an affiliate, or sold to a domain name front runner.

3rd Party WHOIS query portals. Any web server can host applications to perform WHOIS queries. Internet users may use such portals to check domain name availability. A party at any of these portals can use the query data directly or sell it to a domain name front runner.

Unauthorized executables. Email-delivered worms infect hundreds if not thousands of client computers daily. Malicious software delivered via email often includes trojan executables, programs that masquerade as legitimately installed applications or services but actually perform unauthorized and malicious activities. Trojan software can be programmed to collect URLs, DNS activity or keystrokes. End user (client) systems are not the sole targets of malicious code: inadequately secured DNS, web and other application servers may also be compromised by attackers, who then install trojan

software (e.g., "root kits") that can be programmed to monitor DNS, WHOIS and other system and user activities. The attacker can use the query data directly or sell it to a domain name front runner.

DNS operators. Some Internet users query the DNS rather than WHOIS services to determine whether a domain is in use, choosing to determine whether a domain name is available based on the receipt of a non-existent domain (NxD) response to a DNS query. This is generally a less accurate method than querying a registry or WHOIS, as a domain name can be registered, but is sometimes not published in the DNS. However, a party at any public DNS operator or a service provider who provides name service to subscribers can collect and use NxD data to register domain names in its own name or sell the NxD information to a domain name front runner.

Registrars (and resellers). Registrars perform domain name availability checks on behalf of customers and visitors to their registration portals. Many registrars use the EPP <check> command to query a domain name from one or more registries. Some registrars also offer proprietary application programming interfaces (APIs) to resellers, which extend the EPP <check> command to the reseller. These are intended uses. A party who is able to monitor EPP activity can collect and use the query data directly or sell it to a domain name front runner.

Name Spinners. When a prospective registrant checks the availability of a domain name (e.g., example.com) using a registrar's domain name availability checking service, that registrar may send an availability check for the second-level label (example) to COM and additionally to any other registries whose TLD labels they market (including ccTLDs). The registrar performs this cross-TLD availability check as a service to the registrant: e.g., if a prospective registrant asks whether example.com is available and it is not, the registrar is able to provide a list of TLDs under which the desired 2nd level label (example) *is* available. A party in this query chain can monitor and collect availability checks and sell the mined data to a domain name grabber.

Registries. Registries that receive checks for the availability of domain names in their TLDs can determine the list of names checked versus the list of names not yet registered, and make such a list available to domain name front runners.

Information leaks, social engineering. An employee may unintentionally or prematurely reveal a service mark, television or movie title, or product slogan his company intends to register as a domain name during a conversation in a public area, and a passer-by might speculatively register the name.

The number and variety of means and opportunities included in this list illustrate that domain name front running can be performed by many parties, using a wide variety of collection and monitoring techniques. Indeed, other entities (search engines, browser developers, ISPs) might conceivably engage in domain name front running if it was feasible and profitable. The existence of such means and opportunities, however, is not sufficient to conclude that any of these are being exploited. At this time, SSAC does not

have sufficient information to claim any of these opportunities are currently being exploited, but the committee continues to seek and solicit information related to suspected domain name front running incidents.

Coincidence

What appears to a prospective registrant as an intentional act may prove to be a coincidence. It is possible that two or more parties may become interested in a domain name a nearly the same time, especially if that domain name includes a popular instant messaging acronym (e.g., rofl., afaik, tyvm, bbiab, nvm) or suddenly popular phrase (e.g., "what *were* you thinking", "go ahead make my day"). The current volume of domain names tasted on a daily basis must also be considered; for example, an individual may imagine that a domain name is unique, but that name may have been previously registered, and previously registered names as well as permutations based on a key word in a domain name are commonly tasted. It is also worth noting that WHOIS services are not necessarily “real time”. A domain name may be registered at noon on a given day but WHOIS queries later that afternoon may still indicate that the domain is available.

Domain Name Front Running and Acceptable Conduct

An important question for the community to consider is "How do we characterize domain name front running?" SSAC makes several observations based on the methods and opportunities enumerated above.

1. Activities performed by software installed without authorization and consent (via viruses) and activities performed following unauthorized access to a computer system are considered to be illegal in certain jurisdictions. Domain name front running that is facilitated by such illegal activities might also be considered illegal activity.

2. Domain name mining activities performed by client software, browser helpers, or 3rd party WHOIS portals may be disclosed in the application's End User License Agreement (EULA) or at the developer's or operator's web site. In such circumstances, the user has been provided notice and has given consent. Even if the data collection were not disclosed, it is not clear whether this is universally considered to be an illegitimate act. Back channels themselves are topics of considerable debate: some security experts argue that if an application uses a back channel, the EULA must provide a truthful disclosure explaining what information will be collected and how it will be used and shared, while others would argue that such a disclosure is only needed if personal identifying information is collected.

3. Public DNS operators may be entitled to use or sell DNS utilization and logging information. Commonly, few agreements other than an Acceptable Use Policy (AUP) exist between operators and subscribers. AUPs may not disclose what types of logging and analysis activities the operator performs and how the operator will use log records. Service level agreements often exist between enterprise customers and service providers, but these typically focus on performance and availability metrics and may not address DNS and WHOIS data query collection, analysis or resale.

4. ICANN's Registrar Accreditation Agreement and Registry Agreements do not expressly prohibit registrars and registries from monitoring and collecting WHOIS query or domain name availability query data and either selling this information or using it directly. In the absence of an explicit prohibition, registrars might conclude that monitoring availability checks is appropriate behavior. A counter assertion can be made that having registrars monitor availability checks is inappropriate, that domain name front running is an unanticipated and undesirable consequence of the existing registration process, that "spying" on a customer (or a customer's customer) is unethical and violates a trust relationship between registrant and registrar (and between registrar and registry), and that such behavior undermines consumer confidence in the registration process and all those who participate.

5. Information leaks, social engineering and coincidence are outside the scope of any action that SSAC could recommend to ICANN and the community other than to suggest that checking the availability of domain names is one of many areas where individual discretion and a thoughtful appreciation for confidentiality is required.

These observations reveal several challenges we face as we study domain name front running. Based on currently available information, the various acts of collecting names of interest from DNS, WHOIS, domain name availability checks, and other resources to preemptively register a domain name may appear be unfair, improper and even criminal to registrants but none of these assertions have been established by fact, policy or law.

SSAC also observes that many domain name front running methods lie outside ICANN's influence and thus ICANN's policies may have limited effect (or no effect whatever if registrars and registries are not domain name front running participants).

Preliminary Findings

Of immediate concern to SSAC is *protection of industry image* for all parties to the domain name registration process and maintaining consumer confidence in the registration process. SSAC has sufficient information to observe that registrants *perceive* that parties affiliated with domain name registrations are participants in domain name front running but has no hard data to debunk or corroborate this perception. The perception of preemptive registration portrays an unfavorable image of the parties associated with the domain name registration process in specific, and of the domain name community in general. As such, SSAC feels obliged to study the matter further.

SSAC offers the following preliminary findings:

1. Checking the availability of a domain name can be a sensitive act which may disclose an interest in or a value ascribed to a domain name

2. Some potential registrants perceive that parties associated with the domain name registration process participate in domain name front running. SSAC believes that preventing this perception from evolving to accepted wisdom is an important consideration for the domain name community.

3. At this time, no Internet user has presented sufficient information to conclude that any party associated with the domain name registration process engages in domain name front running. Members of the SSAC have contacted attorneys who are studying cases of possible domain name front running activity and are involved in ongoing discussions with other law firms; members of the registrar and registry communities; and security and domain name experts.

4. No single process to handle domain name front running complaints exists today, thus the actual number (and even a reasonable estimate) of complaints reported is difficult to gather. The absence of a formal process also creates an information gap for a domain name tasting victim, who has no guidelines for the kinds of information that must be presented to corroborate a claim.

5. There does not appear to be a strong set of standards and practices to conclude whether monitoring domain name availability checks is an acceptable or unacceptable practice. Redressing domain name front running claims is left to the discretion of (primarily) the registrar, who may not have any credible reason to process such a complaint.

6. Even if formal policies or processes were to exist, it is possible to collect data to facilitate domain name front running from a variety of sources. This introduces considerable complexity and variability for anyone attempting to resolve the complaint (or design mitigation strategies). Moreover, a number of collection sources have no formal relationships with ICANN and are not obliged to comply with any policies prohibiting domain name front running. Thus, policy action alone will not mitigate domain name front running.

7. Various acts of collecting names of interest from DNS, WHOIS, domain name availability checks, and other resources to preemptively register a domain name may appear to be unfair, improper and even criminal to registrants but these conclusions are not necessarily established facts.

Call for Public Comment

SSAC believes that domain names are a highly speculated and potentially valuable commodity for monetization and sale. Further we believe that availability checking may have unanticipated consequences, depending on the methods a would-be registrant uses to perform such checks and the parties that the would-be registrant uses.

SSAC offers this Advisory as a vehicle for providing a context for public comment and discussion. SSAC invites individual users, registrants, registrars and other parties who have information regarding possible domain name front running incidents to report that incident to the committee with as much information as possible to assist SSAC in studying this matter further.

For each instance of suspected domain name front running, the type of information that would be most useful in studying the case includes but is not limited to:

- Method used to check domain name availability (e.g., web browser, application).
- Local access ISP.
- Provider or operator of the availability checking service.
- Dates and times when domain name availability checks were performed.
- Copy of the information returned (e.g., WHOIS query response) in the response to the availability check.
- Whether the domain name was reported as previously registered or never before registered in the response returned from the availability check.
- Copy of the information returned (e.g., WHOIS query response) indicating the name had been registered.
- Copies of any correspondence sent to or received from the registrant perceived to be a front runner.
- Correspondence with the registrar or availability checking service.
- Any information indicating a potential relationship between the availability checking service and the registrant that grabbed the name

Please submit incidents to the SSAC Fellow at SSAC-DNFR@ICANN.org.

Based on the information received, SSAC will either issue a subsequent report or give notice that insufficient information was collected to pursue the matter.

Call for Policy Consideration

SSAC suggests that the domain name community (including registries, registrars, registrants, civil society and academic study groups) examine the existing rules to determine if the practice of domain name front running is consistent with the core values of the community, and if not, to consider implementing measures (including new policies, regulations and codes) to restrict domain name front running It would be useful if other organizations such as the ccNSO, APTLD, LACTLD, RALOs, and others were able to conduct surveys of their members, and contribute to the SSAC analysis.

Acknowledgments

Information used to prepare this Advisory was collected by the SSAC Fellow from fellow SSAC members, ICANN legal counsel, ICANN registrar liaisons, and employees of registries and registrars who agreed to participate in the study. The following members of the ICANN community provided information that proved essential in composing the picture of domain name front running. The committee is grateful for their contribution of time and expertise.

Bruce Tonkin, Chief Technology Officer, Melbourne IT
Ross Rader, Director, Innovation & Research Company, Tucows
Steve Miholovich, Director of Product Marketing, Network Solutions
Tim Ruiz Vice President of Corporate Development and Policy, GoDaddy
Jay Westerdal, CEO and President, Name Intelligence
Jonathan Nevett, Vice President and Chief Policy Counsel, Network Solutions
Paul Stahura, President & COO, Demand Media