Criminal Abuse of Domain Names

Bulk Registration and Contact Information Access

Prepared by

Dave Piscitello and Dr. Colin Strutt

Interisle Consulting Group, LLC

17 October 2019

Executive Summary

Domain names that can be rapidly acquired, used in an attack, and abandoned before they can be traced are a critical resource for cybercriminals. Some attacks, including spam and ransomware campaigns and criminal infrastructure operation (e.g., "botnets"), benefit particularly from the ability to rapidly and cheaply acquire very large numbers of domain names—a tactic known as *bulk registration*. When cybercriminals can register hundreds or thousands of domain names in a matter of minutes, an attack can be widely distributed to make detection, blocking, and dismantling more difficult and prolonged.

Cybercrime investigation is always a race against the clock—the longer it takes to identify an attacker and block the attack, the more damage can be inflicted on more victims. Before the adoption by ICANN of a Temporary Specification ("Temp Spec") for handling domain name registration data in compliance with the European General Data Protection Regulation (GDPR), investigators had ready access to the contact information provided by domain name registrants ("Whois data"). This information, even when incomplete or inaccurate, facilitated rapid attack response both directly (when it correctly identified the attacker) and indirectly (by enabling "connect the dots" methods such as search-and-pivot).

The immediate effect of the Temp Spec since the GDPR took full effect on 25 May 2018 has been to severely limit access to domain name registrant contact information, most of which is now redacted by registries and registrars when they respond to Whois data queries. Although cybercrime investigators with proper authorization can petition a registry or registrar for the redacted information, this takes place on a glacial time scale compared to the "every second counts" imperative to limit the loss or harm caused by an attack.

The use of bulk registration to distribute attacks across hundreds or thousands of domain names in matters of minutes, coupled with the crippling of registration data access by the Temp Spec, presents cybercrime investigators with the dual impediments of harder-to-pursue criminal activity and harder-to-obtain information about the criminals.

For this report, Interisle researchers studied both aspects of this impediment:

- We studied samples of security events during which many thousands of domains were blocklisted in relatively short time frames.
- We identified registrars that offer bulk registration services and have large concentrations of blocklisted domains.
- We characterized the behavior of domain name registrants who engage in bulk registrations that are detected and blocklisted as criminal activities.
- We studied the way in which domain name registrants' use of privacy protection services or the redaction of Whois point-of-contact information inhibits or delays cybercrime investigation.

Our study confirms the hypothesis that cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domains for their attacks. The study identifies four specific registrars at which abusive registration activity appears to be concentrated. Our findings corroborate those of the 2017 ICANN report *Statistical Analysis of DNS Abuse in gTLDs* (SADAG).

Our study also confirms that ICANN's Temp Spec policy of redacting Whois point of contact information to comply with the GDPR significantly encumbers and delays cybercrime investigation. Working without

essential information, both real time and historical, investigators cannot make the necessary correlations to quickly and thoroughly map a criminal domain infrastructure or to attribute criminal activity to a perpetrator in time to prevent substantial harm to the victims of an attack.

Based on these findings, we make the following policy recommendations:

1. Validate domain name registration data.
2. Define "bulk registrant" as a new element of registration data for Whois.
3. Define an Acceptable Use Policy (AUP) that applies specifically to parties that register large numbers of domains.
4. Require registrants to apply for bulk registration services.
5. Distinguish domain names registered by legal entities from those registered by natural persons, classify parties that use bulk registration services as legal entities, and require unredacted access to the registration data of legal entities.
6. Maintain and publish a current list of validated bulk registrants.
7. Disallow registration transactions that involve large numbers of random-looking algorithmic domain names.
8. Disallow, for a period of one year, the re-registration of any bulk-registered domain name that has been used in a criminal cyberattack.
9. Provide the ICANN DAAR project with access to unredacted Whois data without rate limiting.

Implementing these recommendations will require the concerted and collaborative effort of every participant in the domain name registration system: ICANN, registries and registrars, government regulators, individual and institutional registrants, and cybercrime investigators. It may also require further study to establish thresholds and assess the effectiveness and feasibility of different implementation strategies.

We believe that committing to this effort is clearly within the scope of ICANN's obligation to operate "for the benefit of the Internet community as a whole" (see Bylaws, "Commitments"), which demands that it recognize a broad remit that extends to how a domain name (or other Internet identifier) is misused to point to or lure a user or application to content that is harmful, or to host content that is harmful.

Harmful content itself is not ICANN's concern; the way in which Internet identifiers are used to weaponize harmful content most certainly is.