Mitigating threats associated with your TLD
Moving from passive, complaints-based action to pro-active measures

**Primary Goal**: To identify and take action against domains that may violate the TLD’s Acceptable Use Policy or that have otherwise been flagged by third parties as potentially harmful.

**Secondary Goal**: Identify and share information on other domains registered by those individuals for closer inspection. Privacy concerns? We only share data with the secure domain foundation that is publicly available under CoCCA WHOIS / RDDS policy. The Secure Domain Foundation connects as a “CERT” client type and able to query by EPP (read only) and dedicated WHOIS query.

**Our First Attempt** – Contracted a reputable security company to do periodic scanning of the websites of domains in the registry. Outcome? Expensive and not overly useful...

- Most AUP violations / criminal activity is in lower level domains created by Registrants - names that do not appear in the registry and were not scanned, very few “hits”. No “drill-down” on the data. Difficult to extract and store information locally.

- People are generally less than thrilled about having their websites scanned. Detection may be overly intrusive and may impact web applications and/or disrupt services provided to end users -as well as invite angry emails from systems administrators.
Current Attempt – Compare domains (and hosts, contacts, emails) in the registry against databases that contain data that identifies potentially harmful host names or actors.

More useful, it identifies subordinate domains not in the registry (baddomain.domain.tld) and has none of the side effects of active scanning.

Configuration Procedure? Simple...

Configure CoCCA to connect to an external DB, via an API and continuously “walk through” registry records (domain / email / name servers) and look for a match, if one is found, import the data and make it part of the domains history.

CoCCA can be configured to automatically email and/or send SMS to Administrators, Registrars, Registrants or CERT’s and automatically lock (or suspend) the domain when there is a match.

Future versions will allow users to configure the automated actions based on reputation variables - severity of the issue, number of reports, sources of the data etc.

Automation allows operators of even the smallest ccTLD’s with limited human or technical resources to take pro-active measures to identify and react to threats that are associated with domains in their TLDs.
<table>
<thead>
<tr>
<th>Username / API Key</th>
<th>External Verification System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cocca</td>
<td>CHIP</td>
<td>CHIP verify</td>
</tr>
<tr>
<td>4199b068b94716a347e4aa866f5ab504</td>
<td>SECURE_DOMAINS</td>
<td>Secure Test</td>
</tr>
</tbody>
</table>

Edit Record (Secure Test) Cancel

Verification Type

API Key

Description

Host

Port

Save
Easy to configure actions and notifications... will be expanded on in future versions.

Links to any other databases that have an API will be incorporated in future builds as resources allow. CoCCA is “neutral” we just make it easy for users to connect.
CoCCA will ...

- store all unique reports it finds and associate them with the domains history
- automatically “clear” domains if issues are resolved
- allow drill-down for all domains registered using the same email or hosts
- send notices to admins if a new domain is registered by an individual who is listed as a contact for a domain that has been flagged.

For more information - garth.miller@cocca.org.nz