CoCCA Panopticon | Domain Security Initiative

Assumptions - Registry side

- Malicious domain-related activity is often the result of compromised hosting, not malicious registrations.
- Registries can block or flag for manual approval suspicious registrations, dga domains, URL hijacks (typo squatting) etc.
- Registries have no capacity to prevent a registrant from creating subordinate domains
- Response by the ccTLD manager to activity in subordinate hosts will be after the fact

Assumptions - Registrar side

- Limited internal capacity or incentive to actively monitor and respond to domain related security issues

- Concerns forwarded to registrars only by a ccTLD manager may result in delays in notifying domain contacts - or often no action on the part of the registrar

Assumptions - Registrant side

- Domain contacts have the highest incentive to remedy any issues.
- It is beneficial to advise malicious actors that their use of the name space is being monitored.
- The ccTLD policy matrix and commercial environment allows direct registry to registrant communications - when such communication is in the interest of addressing security issues.

Initiative objectives

- Provide ccTLD managers with current and verified data on domain related security issues;
- Send security notices from the ccTLD manager directly to domain contacts using a credentialed RDAP user
- Quick resolution of security issues and reducing a possible administrative burden on registrars
- Provide tools that can be used without any development effort or expense on the part of the ccTLD manager

Key Features

- *Does not* utilise zone files, GDPR compliant and does *not* require development effort on the part of the ccTLD manager
- Will work with any registry platform and / or RDAP server
- Tested with the open source https://reddog.mx RDAP server

Components

- a public data collection and validation component - a repository hosted by CoCCA (no domain contact information is collected or stored in this database).

- a stand-alone GDPR compliant java application (Arke) hosted by the ccTLD manager that connects to both the relevant ccTLD repository data (made available daily) and, if available, an RDAP server to get additional data and send notices to domain contacts.

Process 1

- Automate the daily collection and normalisation of malicious Uniform Resource Identifiers (URIs) for small and medium sized ccTLDs from multiple threat intelligence feeds.
- Analyse URI host names to distinguish between domains registered in the ccTLD registry and subordinate domains created by domain contacts.
- Query the applicable TLD DNS servers to see if the domain is delegated and active (nxdomain).
- Query the Quad 9 filtered recursive DNS service to see if a domain is blocked by Quad 9.

Process 2

- Using a commercial randomised IP proxy service, test each reported URI from 2 different geo located sources for their http and https status.
- Query the Google Web Risk API to see if the URI has been flagged by google as an active threat.
- Query the tranco list for the ranking of popular domains with identifiers.

Process 3

- If the TLD is RDAP enabled, connect with a credentialed user and look for create date, EPP status and other useful data that may be redacted in WHOIS.
- If zones are available, Panopticon can search for URL hijacking (typo squatting) activity.
- Analyse the collected data and provide a daily report to ccTLD manager.
- If the ccTLD registry system is RDAP enabled, a locally hosted app (Arke) can send an email to domain contacts if a domain has appeared in reputable abuse feeds and the indicator(s) have been validated by CoCCA in the past 24 hours.

Why RDAP?

- WHOIS services are not helpful: server output often differs, rate limiting is common, required data is often redacted.

- RDAP: easy integration via an existing industry standard API

- ccTLD managers retain full control of personal and commercially sensitive data

Panopticon and GDPR - 1

CoCCA collects, normalises and does and analyses of the data from abuse feeds (and if available, RDAP data) and provides a small database file to the ccTLD manager with the daily report.

ccTLD manager can run a small app (Arke) provided by CoCCA. Arke has a small json config file that contains the following:

- the location of a daily records.sql provided by CoCCA
- the location of tld zone file in bind format
- the URL and credentials for the ccTLD RDAP server, and
- the location of an email template in xml format

Panopticon and GDPR - 2

Arke will “fill in the blanks” of the data set with personal or commercially sensitive data in the possession of the ccTLD manager but missing from the data provided by CoCCA and:

- send the emails to domain contacts

- provide the ccTLD manager with a list of high risk / possible malicious registrations (typo squat or dga domains) that have not yet appeared in any of the feeds

CoCCA

THANK YOU

For more information https://panopticon.coccaregistry.org