THE

SECURE DOMAIN

FOUNDATION

What is the SDF?

- Many of the top security researchers volunteer their time
- Research users include Facebook, Google, MS, Trend, Kaspersky, etc..
- Update from ICANN .CR:
  - Changed Paths
  - Backend Data, DB, and API stable and actively in use.
  - Public front coming soon

The Issues, and our goal.

- Recidivism in abuse. Bad guys don't give up, they just become someone else's problem.
- Similar properties in bad actor registration
- No incentive for data sharing.
- If you share what you suspend, you can prevent others from inheriting that bad guy. If everyone shares abuse data, we all win.

What do we have today?

- 260+ Thousand bad actors actively being watched – Far more in historic data
- 25+ Million whois records over big tlds
- 5+ Million malware samples analyzed (domains, ips, etc) Growth rate of ~100K per day
- Integrated daily updates from all the public sources (emerging threats, alien vault, malware domains, etc)
- Exclusive Oriza Data

Oriza Data

- Private data sources – Sign NDA to know more

  In just 90 Days from known and verified bad actors:

- 2+ Million logins and account updates
- 96 Thousand new accounts created
- 163 Thousand browser fingerprints*
- Much much more... EG: bad guy XYZ logged in from this IP 14 minutes ago. He changed his account email from bob@bob.com to fred@fred.com, and his browser fingerprint is hash.
- Our unclassified data pool consists of tens of millions of accounts.

Use Cases

- Registrar can query about new registrations
- ccTLD/Registry can query for daily updates and notify their customers. Or run their historical data.
- DNS Providers/Sub Domain/Dynamic/Free DNS Can query new accounts
- Hosting providers can check their IP space, or query about new customers.
- Transactional sites can query about an active transaction.

What is the cost?

- The Secure Domain Foundation will never sell data, nor will it provide data for donation or any other financial consideration.
- This is FREE and it will remain so.
- Seriously it is free.

THE SECURE DOMAIN FOUNDATION

How Does it Work?

- JSON API – Query by:
  - Email
  - IP
  - Domain / including wild cards
  - Malware md5
  - Browser Fingerprint
  - Alias / Username (coming soon)
  - Name Server (coming soon)

QUESTIONS?

- Application Integration currently in dev:
  - CoCCA Registry
  - Maltego
  - CaseFile
  - Palantir
  - CIF (Collective Intelligence Framework)