Background

- Concept floated at ICANN Costa Rica (March, 2012)
  - Rampant recidivism in domain abuse can be curbed
  - We need to work together

- Initial concept has evolved considerably
  - Daily volume of malware data doubled
  - Data feed idea became an API
  - API became a reputation system
  - SDF incorporated as a Canadian Non-Profit

- Official launch in January, 2014 … yeah!
About the Founders

Norm Ritchie
Domain Industry

The Canadian who holds the key to the Internet
It’s housed in two high-security facilities separated by the North American landmass.
The one authenticated map of the Internet.

Chris Davis
Cyber Security

Canadian to receive FBI award for uncovering massive botnet scheme
Some SDF Partners
What do Data Providers and Partners provide?

- Bad Guy Email Addresses
- ToS Breach Logs (Browser Fingerprint and Login IPs)
- Malware Data + Analysis
- Investigation Assistance
- Development Assistance
- Operational Assistance
Current Evolution

- Malware MD5 mapped to Domain Name + Category
  - Over 86M records
- Email Reputation Data
  - 7M+ records categorized
- Whois Data
  - 26M+ records categorized
- Browser Fingerprints
  - 315K collected
- ToS Violations logs
- Maltego Transforms
- Over 300M records in the Database
Coming Soon

- Postal Address Validation System - FREE
  - Dec, 2103 – Invite only Alpha
  - Jan, 2014 – Open Beta
- Phone Number Validation to follow
- Browser Fingerprint V2 Framework and Repository
- Registrar Rankings
Postal Address Validation

- Canada Post Partnership
- 150+ Countries
  - Last Name to Address Confidence Scoring
  - Multi-Format Fuzzy Logic
- UPS API approval for US addressing
- Google Maps API
- FREE!
Phone Number Validation

- Simple regex on current whois data = low fruit
- In the last 18 months, ~1.7 Million (gTLD) domains were registered with CC +1 and area codes that don't exist.
- Will publish findings
Browser Fingerprint DB

- Throwing away 300K current fingerprints at 94% unique
- New code is more accurate, better techniques
  - SDFPrint is a reversible 5 section hash
- Code is available now
Registrar Ranking

- Ranking based upon responsiveness to abuse complaints. NOT # of bad domains.
- Published record of turn around times on abuse complaints
- Apathetic and Malicious registrars will rise to the top
Synopsis of the API

- Validation scoring per data point for: Postal, Phone, Email
- Malicious reputation scoring per data point for: Email, Domain, IP, Postal, Phone, Fprint
- Simple or complex. JSON, XML, REST, CURL
- +details will present data after the score
query_string: "el27pupi@hotmail.com",
query_type: "email",
-
  -
    -
      description: "Malware - Registering or Supporting the distro or control of malware APT or botnet code",
      type: "Description",
      email: "el27pupi@hotmail.com",
      cat: 1
    -
      description: "Forum Activity - Email has been seen participating in black market forums - Hacking Carding etc",
      type: "Description",
      email: "el27pupi@hotmail.com",
      cat: 2
  -
    -
      description: "Generic Abuse - Email has been reported as abusive - Unverified",
      type: "Description",
      email: "el27pupi@hotmail.com",
      cat: 0
  -
    city: "Higuey",
    domain: "dark-conquer.com",
    create_date: "2012-09-02 00:00:00",
    country: "Dominican Republic",
    phone: "+1.8293577817",
    registrar: "FASTDOMAIN, INC.",
    name_servers: "NS1.GLOBAT.COM[NS2.GLOBAT.COM]",
    type: "Whois",
    email: "el27pupi@hotmail.com"
-
  -
    fingerprint: "4524ae6470fe950ca1652cb5d11c731",
    type: "BFP",
    email: "el27pupi@hotmail.com",
    f: 1200.88.36.330"
Summary

• Free Postal Address Validation API covering 150+ Countries – Jan 2014
• Email, IP, and Fprint reputation data
• ccTLD daily feeds starting Nov 1 2013
• Registrar reputation based on responsiveness
• This is a community effort! Always looking for more Partners!

www.thesecuredomain.org