Luminous:
Bringing Big(ger) Data to the Fight

Norm Ritchie
Drew Bagley

ICANN Helsinki
June, 2016
Secure Domain Foundation

• Non-profit
  – Founded in 2014

• Proactive mitigation of malicious domains used for cybercrime
  – A clearinghouse for intel on malicious domains
    • Malicious domains and numbers
    • Bad Actor indicators (email, IP, name servers, addresses)
  – A forum for sharing data, intel and knowledge
    • Trust group
    • Data, Research, Analysis, Discussion
Some Use Cases

• Registrars and Hosts
  – Does this account owner have a reputation for malicious activity?

• Registries
  – What domains in my TLD were reported as malicious today?

• Security Analysts
  – What other domains are associated with this {domain, email, IP, NS, phone}

• Researchers
  – Statistics for policy decisions (empirical data)
Proactive Use Case

Potential Registrants

Filter Through

Proactive Pre-Screening

-Whois Verification
-Check for association with known domain abuse

Filter Through

Ongoing Screening

-Whois Verification
-Check for association with known domain abuse

Fewer abuse complaints = money saved

Secure Domain Foundation
What can we infer from a malicious indicator?

• Given a:
  – Domain name
  – IP address
  – Email address
Malicious Discovery

Discovery
A Simple Concept But ...

• There is a LOT of data
• There is a LOT of data churn
• Success breeds a LOT of queries
• Searches need to be fuzzy
• Implementation can be operationally intensive
Introducing Luminous

• A large, searchable repository of parsed whois data and malicious indicators

• Designed for
  – High Performance and Reliability
  – Scalability
  – Low(er) operational needs
  – Very Flexible

• Query: CLI, API, Web interfaces

• Output: XML, JSON, Text
Luminous Data

• Whois since July 2014
  – 80M gTLD records
  – 120K-150K new registrations per day

• Historical Whois
  – 170M gTLD records

• Indicators of malicious activity
  – 7M unique indicators
    • 10K-100K being added per day
Indicator Classification

- ADWARE: Resource is known for Adware Activity
- ANTIVIRUS: Resource is known to spread fake anti-virus software.
- SUSPICIOUS: Resource is known for general suspicious activity.
- BOTNET: Resource is a known host for a bot-net frame-work.
- COMPROMISED: Resource has been compromised previously.
- FRAUD: Resource is known for financial fraud activity.
- MALICIOUS: Malicious activity / Bullet proof hosting
- MALWARE: Resource is known for spreading malware
- PHISHING: Resource is known for phishing activity.
- SPAM: Resource is known for spam activity.
- RISKWARE: Resource is known for spreading risky ware and hacking tools.
- PHARMACY: Resource is a online pharmacy
- WHITELIST: Resource is white-listed.
- SUSPENDED: Resource has been suspended by a registrar previously.
Current breakdown

- MALICIOUS: 27620
- ADWARE: 47865
- ANTIVIRUS: 8576
- BOTNET: 1114
- COMPROMISED: 357
- FRAUD: 76795
- RISKWARE: 1512
- MALWARE: 2+ M
- PHISHING: 2+ M
- SUSPICIOUS: 1+ M
Example Commands

- **whois**
  - Performs whois queries either out of archive or directly from the server. Can accept a valid top-level-domain, domain or a suffix.

- **whois-server**
  - Simply returns the whois server for a domain.

- **whois-ref**
  - Matches and returns a set of domains from a given e-mail address or telephone number.

- **flags**
  - Queries the database for flags associated with the provided entity. Can query on IP, domain, top-level domain, suffix or email address.

- **export**
  - Export utility using xml template.

- **resolve**
  - Resolve utility, resolves a domain to an IP address including history.

- **resolve-ref**
  - Reverse resolve utility, traverses the database to match on IP-address or a domain.
Example Commands

- **dns**
  - Displays the NS data of a domain including historical

- **dns-ref**
  - Retrieves domains based on a given NS or domain name.

- **asn**
  - Retrieves the AS number of an IP address.

- **asn-ref**
  - Retrieves IP addresses based on a given AS number or other IP address

- **mx**
  - Mail server utility, retrieves any mail servers if connected to a domain.

- **mx-ref**
  - Mail server reference search utility. Returns any domains connected to a mail server or other given domain.

- **report**
  - Report utility. Uses either an internal or an external XML template to provide a semantic report.
Example Output

```xml
<?xml version="1.0"?>
<query>
  <domain>securedomain.org</domain>
  <server></server>
  <date>
    <created>02-19-2002 14:04:43</created>
    <updated>01-25-2016 00:18:17</updated>
    <expires>01-01-1970 00:00:00</expires>
  </date>
  <registrar />
  <reseller />
  <owner>
    <name>The Secure Domain Foundation</name>
    <contact>Norm Ritchie</contact>
    <email>
      <value>admin@thesecuredomain.org</value>
      <host>thesecuredomain.org</host>
      <user>admin</user>
      <domain>thesecuredomain.org</domain>
    </email>
  </owner>
  <phone>
    <value>1 (613) 821-5888</value>
    <country_code>1</country_code>
    <area_code>613</area_code>
    <subscriber>8215888</subscriber>
    <country>CA</country>
    <region>Ontario</region>
  </phone>
  <address>
    <value>7082 Bush Dr Ottawa 08 K4P1M7 CA</value>
    <street>7082 Bush Dr</street>
    <city>Ottawa</city>
    <region>08</region>
    <postal_code>K4P1M7</postal_code>
    <country>CA</country>
    <latitude>45.416667</latitude>
    <longitude>-75.7</longitude>
  </address>
</query>
```

...
Next Up

• Beta available now
  – early adopters
    • Thanks CoCCA!

• Near term
  – Member submissions and vetting
  – Deletion and removal
  – Watch list
  – Batch
  – Ongoing:
    • New/More whois and indicator data
Sign Up Process

- Email us at register@securedomain.org
- Sign the SDF Data Sharing Agreement
- Receive API key and portal login
- Share Data!
Luminous API

Signup available: Now

Price: Free

Interested?
register@securedomain.org

Norm Ritchie – norm@securedomain.org
Drew Bagley – drew@securedomain.org