September, 2018

TLDCON

Secure Domain Foundation

- 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 research and sharing data, intel and knowledge
    - Trust group
    - Data, Research, Analysis, Discussion
- Non-profit
  - Founded in 2014 as a Canadian non-profit corporation

SECUREDOMAIN FOUNDATION

DNS abuse mitigation

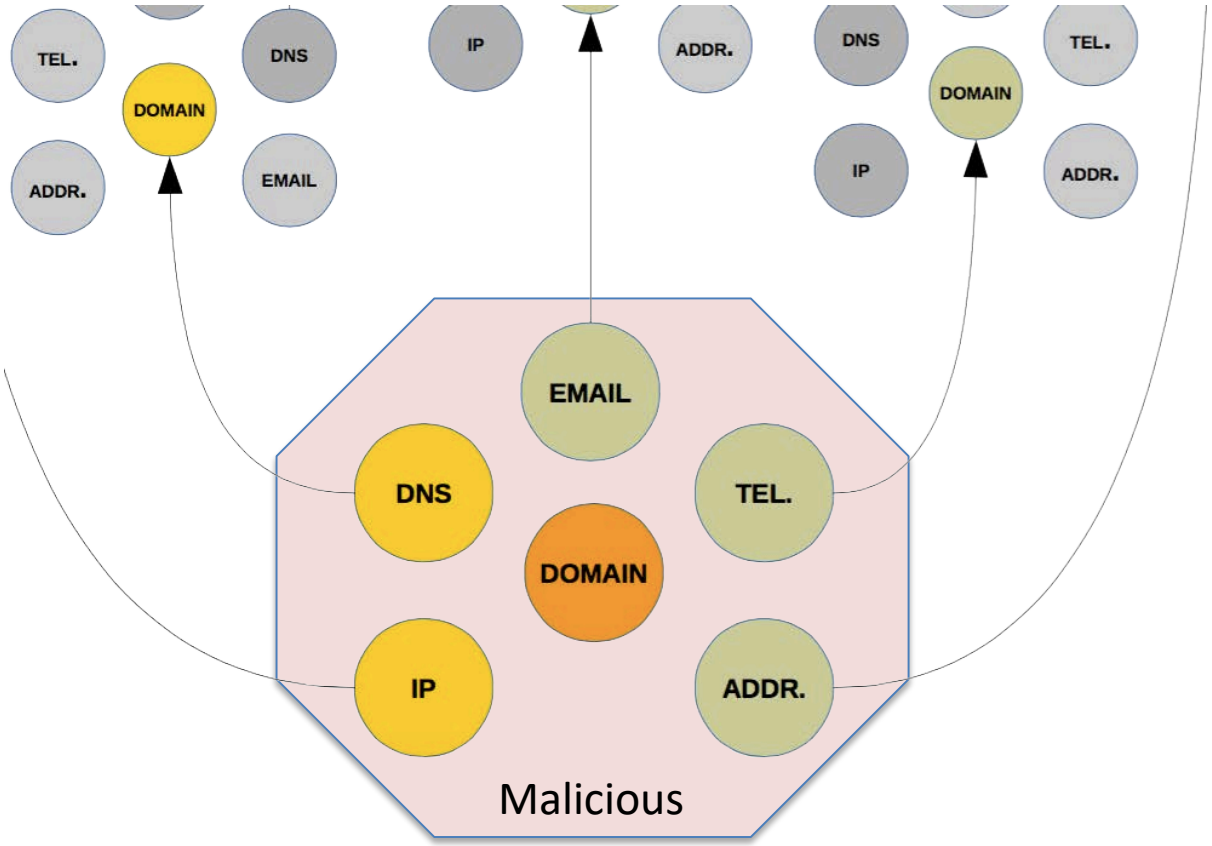
- Reactive
  - (Quickly) suspend domain names upon proof of maliciousness
- Proactive
  - Stop the bad guys from scaling their infrastructure
  - Common fake WHOIS data is still common data
  - Proactive abuse mitigation by registries and registrars is good for business
  - Share data through trusted third parties

SECUREDOMAIN FOUNDATION

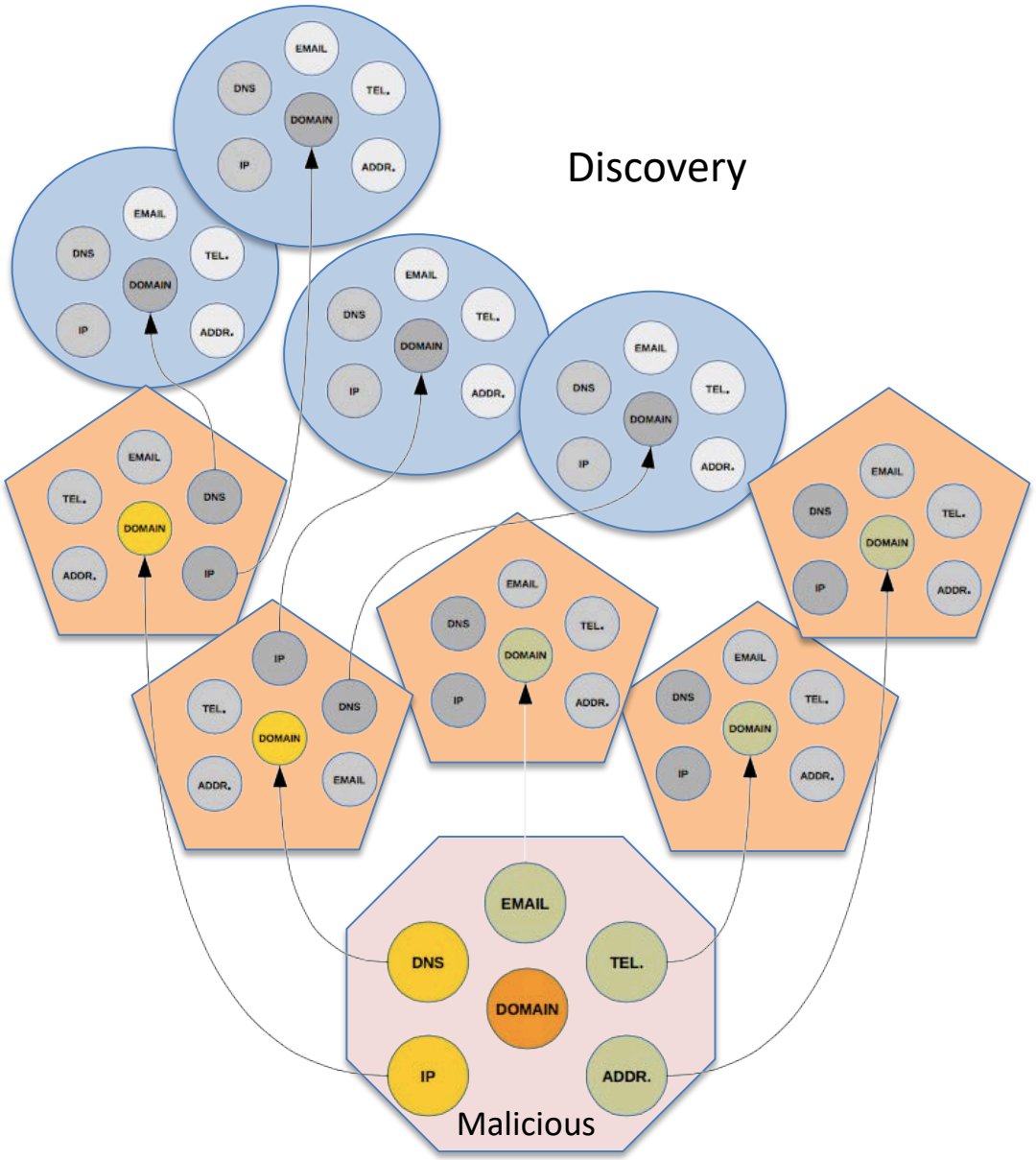
What can we infer from a malicious indicator?

- Given a:
  - Domain name
  - IP address
  - Email address

SECUREDOMAIN FOUNDATION



SECUREDOMAIN FOUNDATION



SECUREDOMAIN FOUNDATION

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)

SECUREDOMAIN FOUNDATION

Luminous

- A large, searchable repository of parsed whois data and malicious indicators
- Designed for
  - High Performance and Reliability
  - Scalability
  - Low operational needs
  - Very Flexible
- Query: CLI, API, Web interfaces
- Output: XML, JSON, Text

Luminous Data

- Whois since July 2013
  - 250M+ gTLD records
  - 120K-150K new registrations per day
- Historical Whois
  - 170M gTLD records
- Indicators of malicious activity
  - 80M unique indicators
    - 10K-100K being added per day

SECUREDOMAIN FOUNDATION

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.

SECUREDOMAIN FOUNDATION

What can you do?

- Share suspended domain name data
  - Domain names
  - Email addresses
  - IP addresses
- Use abuse desk orchestration
  - 10x productivity gain
- Expand Netoscope or SDF analysis across registries and registrars

Work together and automate

SECUREDOMAIN FOUNDATION

Interested in the SDF

- Sign up process?
  - Email us at register@securedomain.org
  - Agree to the SDF Data Sharing Agreement
  - Receive API key and portal login
  - Share Data!

SECUREDOMAIN FOUNDATION

Thank you

Norm Ritchie

norm@thesecuredomain.org

SECUREDOMAIN FOUNDATION