Domain Name System Abuse

The McCarthy Institute IP-Con
Sandra Day O'Conner College of Law at
Arizona State University

Lori Schulman
Senior Director, Internet Policy
March 17, 2022

What is Domain Name System (DNS) Abuse?

- EU Commission Study (published 1/31/22)
  - Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.
- ICANN Specification 11 of Registry Agreement
  - …Malware, botnets, phishing, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law…
- DNS Abuse Framework (voluntary effort)
  - Malware, Botnets, Phishing, Pharming, SPAM (when delivering the previous 4).
- Proposed by ICANN's Business Constituency
  - ...distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law…

Registries and Registrars Hold the Keys to the Kingdom

- Registrars and Registries (RRs) are now the only parties who can reliably access contact data in a timely manner (e.g., in minutes or hours). http://www.interisle.net/PhishingLandscape2020.pdf
- Uncertain legal landscape puts undue pressure on RRs
- IPR owners have lost a key tool for self help

Brand Owners Play a Key Role in Fighting Abuse

Brand owners have an obligation to monitor their intellectual property and act on illegal activities

- Educate employees (or volunteers or customers) to spot and report infringement
- Engage third party vendors with sophisticated screening technology
- Investigate and report suspected abuse to vendors, platforms, payment providers registrars, registries and law enforcement as appropriate
- Take affirmative actions to stop the abuse – notice, negotiation, legal action
- Collaboration with RRs, law enforcement and cybersecurity researchers

Challenges in Detecting, Reporting and Mitigation of Abusive Practices

Lack of access to registration data

Exponential nature of the harm and the ease at which it may be repeated

Lack of transparency regarding 3rd party mitigation policies

Reducing DNS Abuse More Effectively

Better Reporting and compliance

- Include intellectual property statistics in industry reports
- Publish intellectual property policies and report on effectiveness
- Adhere to contractual obligations including RA Spec 11

Finding an acceptable level of risk tolerance for data sharing

- Create more legal certainty regarding the appropriate balance between individual privacy and the need to combat illegal activity
- Acknowledge shared risks

Collaborate with intellectual property owners on a consistent basis

- Acknowledge common goals to keep DNS trusted and safe
- Cyber hygiene – know your customer
- Invest in predictive technologies and fair policies for implementation

Ongoing Efforts to Address the Questions

- EU Legislative Response with regard to Cybersecurity (NIS2)
- US DRUGS Act
- Launch of DNS Abuse Institute
- Internet and Jurisdiction Policy Network
- ICANN Contracted Party House Working Group
- Publicly and Privately Commissioned Studies
- Internet Governance Forum (IGF)
  - Dynamic Coalition on Data and Trust
  - Dynamic Coalition on Internet Safety, Security, Stability

Proposed European Solution for Registration Data - NIS2.0

- Currently under negotiation – Trilogue stage (Parliament, Council, Commission)
- Focused on cybersecurity to reduce inconsistencies; promote collective, coordinated action
- Requires collection of accurate, accessible WHOIS data with minimum require of domain name, date of registration, registrant data
  - Legal Person's names, addresses, emails, telephone numbers publicly available
  - Individual Person's name, surname, and email address
- Information provided to Legitimate Access Seekers
  - How broad will the definition be?

Proposed U.S Solution – DRUGS Act
Domain Reform for Unlawful DruG Sellers (HR 6352, S3399)

- Relates to domain names or websites facilitating the illegal sale of drugs.
- Based on “trusted notifier” model (NTIA/Opioids Program)
- US based registrars and registries must lock the domain within 24 hours of notification.
- Domain must be suspended within 7 days of notification (subject to appeal)
- Trusted Notifiers = FDA, DOJ, AGs, Boards of Pharmacy, FDA/DEA partners
- Fines and imprisonment for noncompliance

Information courtesy of Alliance for Safe Online Pharmacies (ASOP).

Wish List for Fighting DNS Abuse

- Domain name industry collaborative efforts that include intellectual property interests on a consistent basis
- Full compliance with ICANN's Public Interest Commitments and other contractual obligations
- Meaningful voluntary practices to supplement contractual obligations
- Stop fighting data wars!
- Legislation as necessary

lschulman@inta.org