DNS ABUSE

SOME FINDINGS FROM CCT RT

BACKGROUND

- Prior to the approval of the New gTLD Program, ICANN invited feedback from the cybersecurity community on DNS abuse and the risks posed from the expansion in the DNS name space. The community identified the following areas of concern:
- Feedback came from groups such as the Anti-Phishing Working Group (APWG), Registry Internet Safety Group (RISG), the Security and Stability Advisory Community (SSAC), Computer Emergency Response Teams (CERTs), the banking/financial and wider Internet security communities.

THE SAFEGUARDS

- **Nine (9)** were recommended on **community feedback**
  - Vet registry operators
  - Require Domain Name System Security Extension (DNSSEC) deployment
  - Prohibit “wildcarding”
  - Encourage removal of “orphaned glue” records
  - Require “Thick” WHOIS records
  - Centralize Zone File access
  - Document registry- and registrar-level abuse contacts and policies
  - Provide an expedited registry security request process
  - Create a draft framework for a high security zone verification program

ARE SAFEGUARDS EFFECTIVE?

- CCT RT examined the safeguards "*safeguards using available implementation and compliance data*" and "*commissioned a **quantitative DNS abuse study** to provide insight into the relationship, if any, that may exist between levels of abuse and implemented safeguards in the new gTLD name space*."
- A preparatory report by ICANN revealed challenges to adhering to a single definition of "DNS abuse"
  - Abuse is in the eye of the beholder and/or jurisdiction
  - Lack of data in areas where abuse is alleged
  - Lack of comparative data on abuse in Legacy vs. nGTLDs
- Some **outfits** had data and insight

WHAT WE KNOW IS MIXED!

- **Spamhaus** consistently ranks new gTLDs amongst its list of "*The 10 Most Abused Top-Level Domains*" based on the ratio of the number of domain names associated with abuse versus the number of domain names seen in a zone
- **Architelos** and the Anti-Phishing Working Group named ***.com*** the TLD with the largest number of domain names associated with abuse
- **Phishlabs** found that phishing sites in ngTLD zones have increased 1000% since 2016
- Variety of registration rules and safeguards in the hundreds of gTLDs delegated makes it difficult for definitive distinctions in abuse rates for legacy vs. ngTLDs

STUDY METHODOLOGY

- Examined *zone files, Whois records, and 11 distinct domain name blacklist feeds* to calculate rates of technical DNS abuse from **1 January 2014 through the end of 31 December 2016**
- Abuse associated with privacy and proxy services
- Geographic locations associated with abusive activities
- Abuse levels distinguished by “maliciously registered” versus “compromised” domains
- An inferential statistical analysis on the effects of security indicators and the structural properties of ngTLDs

STUDY RESULTS I

- New gTLDs **did not** increase the total amount of abuse in the gTLD space
- Safeguards alone do not guarantee a lower rate of abuse in each new gTLD compared to legacy gTLDs
- Factors such as registration restrictions, price, and registrar-specific practices seem more likely to affect abuse rates
- Abuse is migrating to new gTLDS
  - In the last quarter of 2016, 56.9 of every 10,000 legacy gTLD domain names were on spam blacklists whereas the rate for new gTLD domain names was 526.6 domain names per 10,000 registrations

STUDY RESULTS II

- **Compromised** domain names more likely source of phishing and malware rather than **malicious registrations** in legacy gTLDs than new gTLDS
- Abuse is not universal
- ***.top, .wang, .win, .loan, and .xyz*** are the source of highest malware in new gTLDs
  - Since the end of 2015, the .top TLD has had the highest rate of abusive registrations for all legacy and new gTLDs
  - Domain selling price was a common factor in these new gTLDS
- Malicious registrations have increased in new gTLDs

STUDY RESULTS III

- Abuse is not random
  - Registry business models in terms of restrictions and price are indicators
  - Specific registrars can be identified

RECOMMENDATIONS

- **Rec#1: Amend existing Registry Agreements or in negotiations** of new Registry Agreements with subsequent rounds of new gTLDs include provisions in the agreements to provide incentives, including financial incentives, to registries, especially open registries, to adopt proactive anti-abuse measures

- **Rec#2**: Negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars for technical DNS abuse

- **Rec#3**: Study the relationship between specific registry operators, registrars and DNS abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives, publish findings and make the data available for outside researchers