nic chile

SOMOS EL PUNTO CL

DNS Abuse

ccTLD News Session #2

Guillermo Lama

CISO - Nic Chile

glama@nic.cl

Previous situation

- NIC Chile has a Local Dispute Resolution Policy based on arbitration and also a requirement of accuracy in registration data (article 17).
- Except for that, NIC Chile only suspended domain accused of DNS abuse when ordered by a Chilean court.
- Almost all abuse reports were about compromised websites, not to abusive registrations
- We forwarded abuse reports to the domain contacts, and to the web hosting provider, in case the contacts were not responding
- Main drawback:
    - Long Response time not effective for cyberattacks targeting to perform malicious acts in the first hours of deployment

Facing DNS Abuse

- Starting in 2020, we started seeing an increasing number of abusive registrations
- The pandemic encouraged the migration of many businesses to the online world, with crime activity also increasing there
- Increase in suspicious cases detected and reported by the national CSIRT

Change of Policy in 2020

Responding to the changing threat environment, in 2020 the terms and conditions for the .CL domain were changed to allow for the suspension of a domain when there is evidence of it being used for phishing, distributing malware or spam as a vector for malicious activities.

Article 6 (2020) gives authority to NIC Chile to suspend domains used for DNS abuse

In addition, the existing Article 17 allows NIC Chile to delete domains with inaccurate registration data that is not corrected when requested

Takedown request analysis

- Analize if the report refers to a hacked website, where the domain name holder is a victim, or to a domain name registered for malicious purposes.
  - In the first case, try to alert the registrant or their web hosting provider.
  - In the second case, continue with the protocol.

Domain Suspension Checklist

Criteria:

- Identify if domain was created for one of the specific types of abuse
- Registration Date and Time
- Check for similar domain names already registered
- Domain contact information
- Confirm Registrar used to register

Collecting Evidence

- Analyze evidence provided and collect additional evidence
  - E-mail headers
  - Website Screenshots
  - Downloadable Malware or similar
  - Problem: malicious web pages may have been designed to look different when viewed from different platforms

    Android, Windows, MacOS, Linux

    Browsers
  - Mail servers used, in case of phishing

Decision

- Decision is made by a committee that includes technical and legal staff. In case it decides it is a case of DNS abuse:
  - Domain name suspension
  - Register date and time of suspension
  - Register operator that suspended the domain
  - Inform domain contact of suspension

Classification and Actions taken

- 2476 request received from different sources, containing duplicates:
    - 710 unique cases:
        - 640 were hacked sites with phishing content, not DNS abuse → report to domain contacts and to hosting company
        - 70 domains suspended:
            - 35 with invalid registration data → suspended and eventually deleted after data was not corrected
            - 35 cases deemed to be DNS abuse → proceed to domain suspension

Trending scam methods

- Smishing (sending malicious URLs via SMS)
- Typosquatting - May be malicious (phishing) or opportunistic (clickbait)
- Redirecting of shortened URLs

Further Steps

- Custom system enhancements for takedown requests management
- Continuous suspension protocol review
- Working on pattern detection to speed up analysis of cases
- Implement DNS Abuse status dashboard