M3AAWG 62nd General Meeting | Canada, Toronto | October 2024

Lightning Talks

Fighting Phishing and DNS Hijacking on a National Level

Cristine Hoepers, Ph.D.

October 10th, 2024

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Cristine Hoepers, Ph.D.

General Manager

CERT.br/NIC.br

Bachelor in Computer Science

Ph.D. in Applied Computing

Background in System & Network Administration

SEI-Authorized CERT Instructor

Mary Litynski Award Recipient, 2020

FIRST Hall of Fame, 2024

cert.br Computer Emergency Response Team Brazil

National CSIRT of Last Resort

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

SEI Partner Network

Creation:

August/1996: CGI.br publishes a report with a proposed model for incident management for the country[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report's recommendations[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The National Internet Registry (NIR)

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Phishing Landing Pages – Jan-Sep/2024 stats

6411 landing pages in total

- Breakdown by brands
  - **4664** Brazilian brands
  - **1747** International brands
- Breakdown by hosting country (IP allocation) – Top 5

US	**4426**	**BR**	**660**
CA	**513**	**DE**	**327**
PT	**76**		

Network resources involved

- **47** Country Codes (IP allocation)
- **265** Autonomous Systems
  - Top **15** are Clouds / CDNs
    - account for **82%** of pages
- **3417** IP addresses
  - Some are repeat offenders
  - Some host multiple campaigns

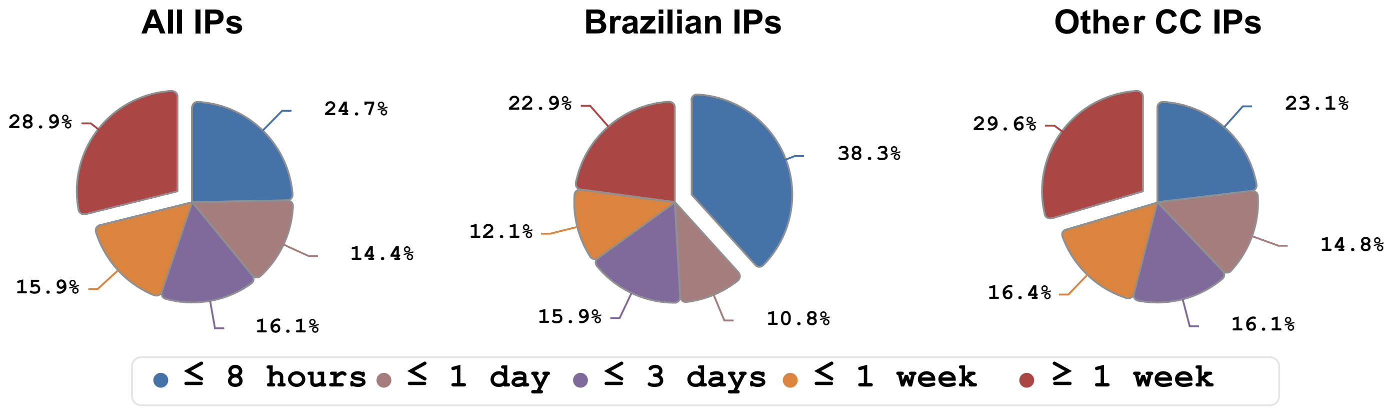
Source: https://stats.cert.br/phishing/

Phishing Landing Pages – Uptimes by IP Allocation

- Top **15** ASes are Clouds / CDNs – account for 82% of pages
  - **2** Brazilian-based
  - **10** US-based
  - **1** each: CA, CY, PT

Phishing Landing Pages - January-September 2024

Uptimes - IP addressess alocatted to Brazil vs. other Countries



Source: CERT.br — https://stats.cert.br/phishing/ — by Highcharts.com

Challenges Reporting Phishing Landing Pages

- Brands are Brazilian, texts are in Portuguese and lures have a local context – poorly understood by tools and foreign analysts
- Techniques used by the criminals require “tweaks” from analysts
  - geolocation / geofencing
    - need to use proxies in Brazil or verify the filesystem
  - only visible in smartphones
    - need to use browser accessibility configurations or real smartphones
  - pharming
    - need to know the victim domain and change the computer or browser configuration
      (alternatively use `curl -s -H "Host: <victim>" URL`)

Phishing Enabled by DNS Hijacking: Impersonation of Recursive Resolvers + Impersonation of Authoritative DNS Servers

“When a small office or home office (SOHO) router is compromised, the DNS settings for the recursive resolver are changed so that requests are sent to a “rogue” DNS server controlled by the attackers. This rogue DNS server impersonates the Authoritative Server of the domain being hijacked and behaves as a regular recursive for other domains.
Examples of these types of attacks include the DNSChanger and GhostDNS botnet attacks.”

Source: ICANN DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG) Final Report
https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report
https://www.team-cymru.com/post/ghostdnsbusters

Challenges Reporting the Rogue DNS Servers

- Cloud services, in general
  - do not have policies or playbooks that cover this type of attack
  - do not have abuse desk staff with DNS training or query tools like dig/whois
    - verifying the report requires querying for the impersonated brand
    - comparing with legitimate DNS delegation/information
- Domains being hijacked are well known in Brazil
  - but not known in other countries
  - a few exceptions

Improving Cooperation with National CERTs

- Try to provide a way to be contacted for troubleshooting
  - new types of abuse and attacks will not be covered by playbooks
  - CERTs can provide additional context and help reduce abuse
    - but we need to reach an analyst to explain technical details
- Participate in different communities and try to create trusted relationships
  - FIRST, TF-CSIRT, APCERT, LAC-CSIRTs, to name a few
- Provide means for trusted contacts to report abuse / exchange IoCs
  - MISP, APIs, etc.

Contact

For additional questions, please email:

<cristine@cert.br>