CaUMa - CATÁLOGO DE URLS MALICIOSAS

Paula Tavares e Rogerio Bastos

Ponto de Presença da RNP na Bahia, Universidade Federal da Bahia

CATÁLOGO DE URLS MALICIOSAS

RNP/CAIS

Rede Nacional de Ensino e Pesquisa possui o CAIS como CSIRT de coordenação, responsável pelo tratamento de incidentes, disseminação de boas práticas.

RNP/PoP-BA

O PoP-BA é responsável por operar os serviços da RNP na Bahia, atendendo as necessidades operacionais da rede Internet para instituições educacionais e de pesquisa.

CATÁLOGO DE URLS MALICIOSAS

CERT.Bahia

Grupo de resposta a incidentes de segurança da Bahia é responsável pelo tratamento de incidentes de segurança relacionados com a comunidade conectada a RNP na Bahia.

UFBA

Fundada em 1808 é a maior universidade da Bahia, conta com 112 cursos de graduação, possui campos em três cidades.
Atualmente é instituição abrigo do PoP-BA.

Phishing

- Utilização de meios digitais e engenharia social para obter dados pessoais, senhas ou informações financeiras da vítima.

- Através de:
  - Preenchimento de formulários
  - Acesso a links falsos
  - Download de malware

- Utilizando:
  - E-mail
  - SMS
  - Redes sociais

O Catálogo de Fraudes

Repositório de mensagens conhecidamente fraudulentas, alertando a comunidade sobre como se proteger desse tipo de ataque

Criado pelo CAIS em 2008, atualmente é mantido através de uma parceria CAIS e PoP-BA e UFBA

O catálogo possibilitou conhecer as características das fraudes e suas variações.

Atualmente uma segunda versão encontra-se em desenvolvimento.

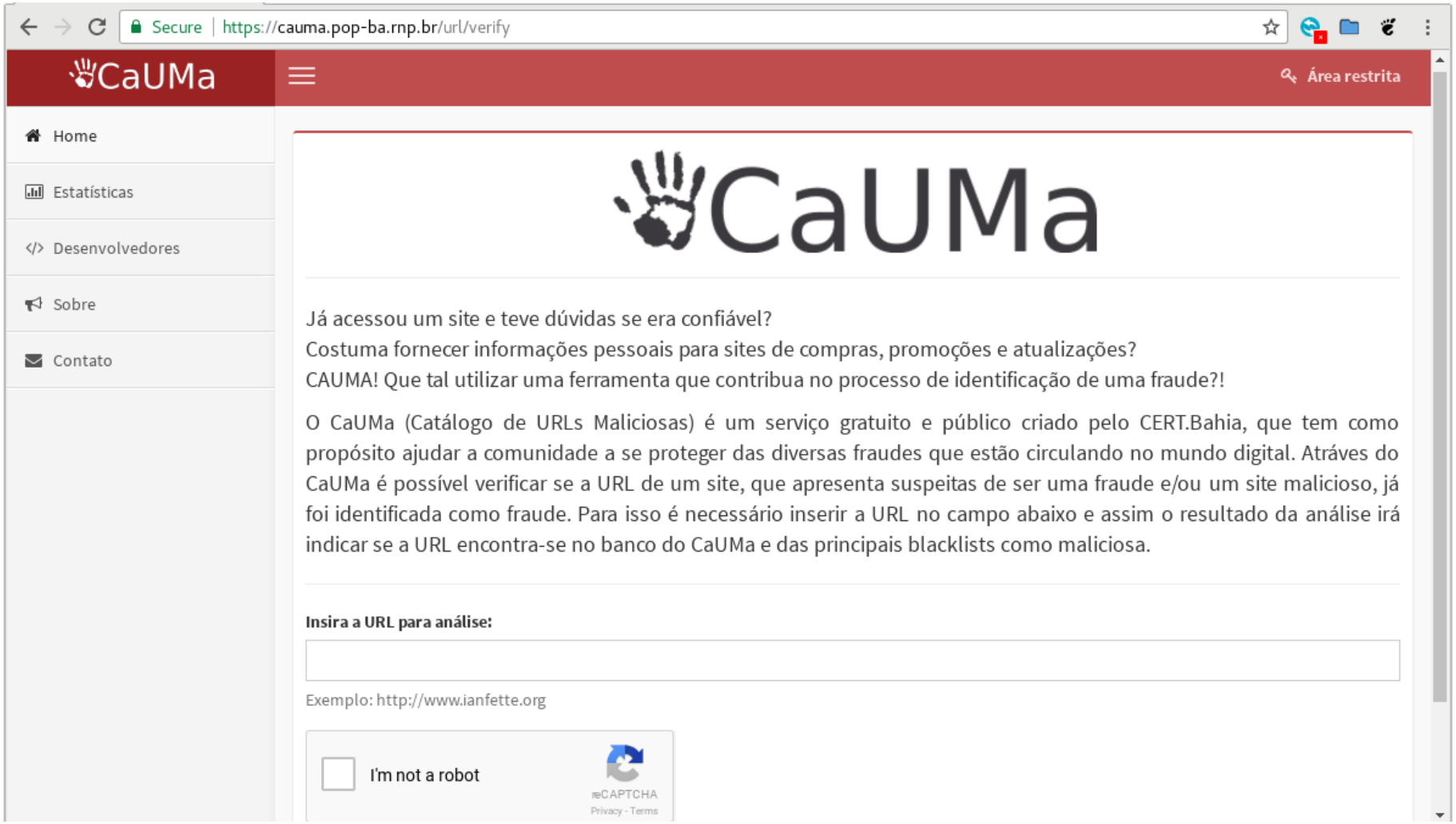
O Catálogo de URLs

Catálogo de URLs maliciosas criado inicialmente para alertar os usuários sobre as URLs contidas em fraudes brasileiras.

Serviço gratuito e público.

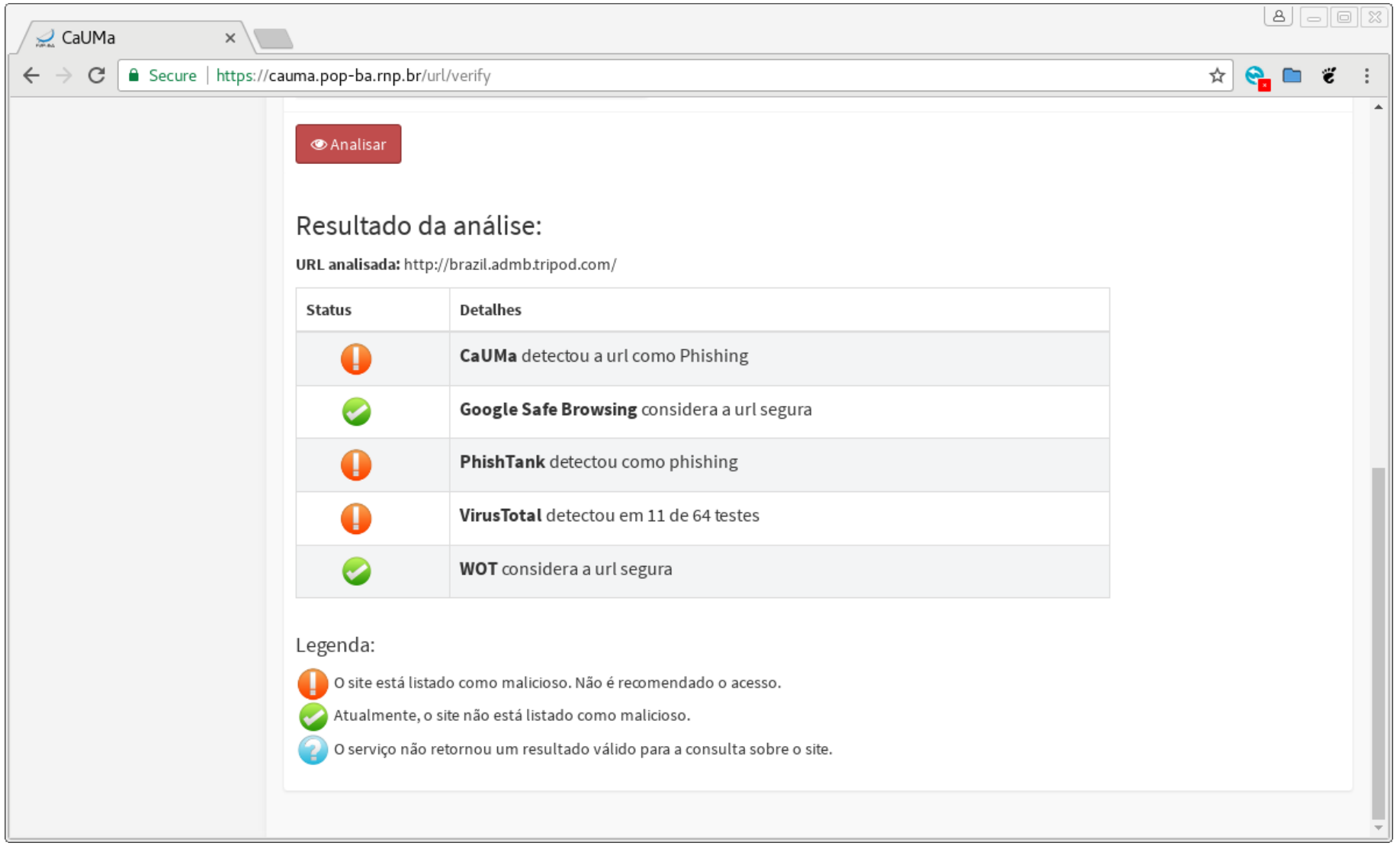
Lançado em 2015 no evento Encontro de Segurança em Informática do CERT.Bahia

O Catálogo de URLs



Fonte: https://cauma.pop-ba.rnp.br/

CATÁLOGO DE URLS MALICIOSAS



Fonte: https://cauma.pop-ba.rnp.br/

O Catálogo de URLs - Motivação

Cerca de 90% das fraudes registradas no Catálogo de Fraudes contêm URLs.

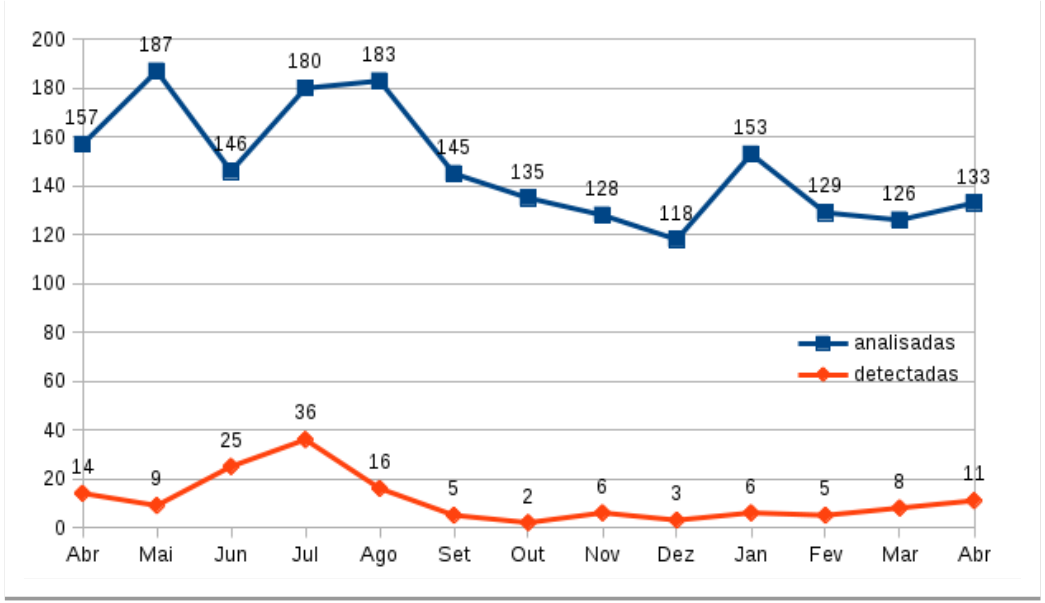
Alto índice de incidentes que ainda ocorrem através de mensagens de phishing

Serviços de reputação de URLs ou *blacklist* utilizados para alertar o acesso a URLs maliciosas que possuem algumas deficiências e oportunidades de melhorias:

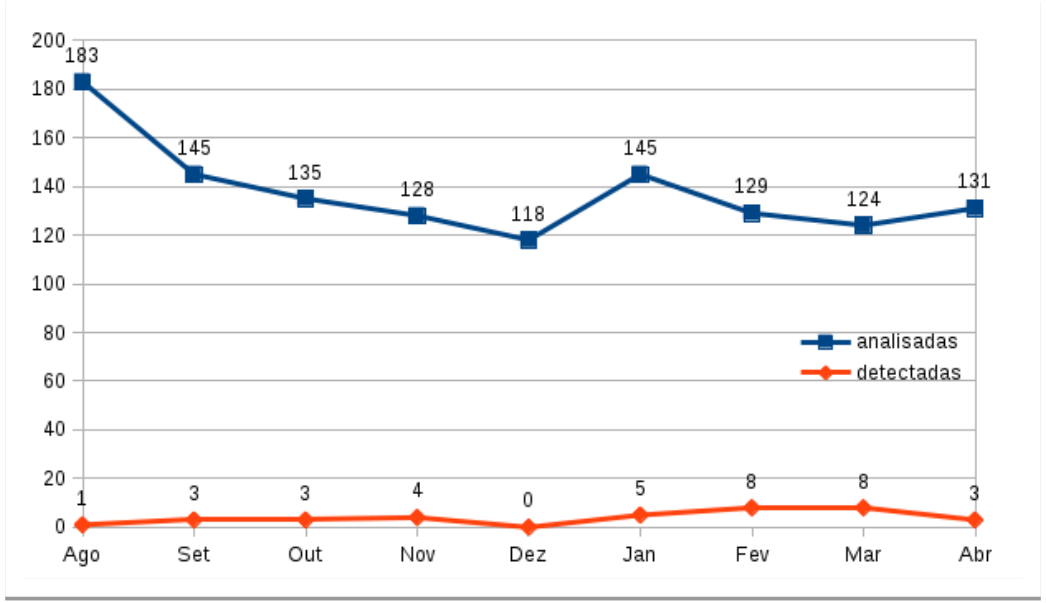
- Inconsistências e limite nas consultas através da API
- Baixa taxa de detecção das URLs maliciosas brasileiras na rede acadêmica

O Catálogo de URLs - Motivação

URLs encontradas no catálogo x URLs detectadas no Safebrowsing



URLs encontradas no catálogo x URLs detectadas no Phishtank



O Catálogo de URLs - Motivação

De 108 URLS no período de 02/05 á 17/05 (15 dias):

- Google Safebrowsing: identificou 5 (cinco)

- PhishTank: identificou 1 (uma)

CATÁLOGO DE URLS MALICIOSAS

URLs Catalogadas

129 / 3602

ONLINE / TOTAL

Fraudes por tipo

https://cauma.pop-ba.rnp.br/url/statistics

O Catálogo de URLs - Estatísticas

Domínios mais comuns

Domínio	Quantidade
com	727
br	183
net	45
org	40
pl	21
ru	20
co	18
info	12
me	12
lt	9

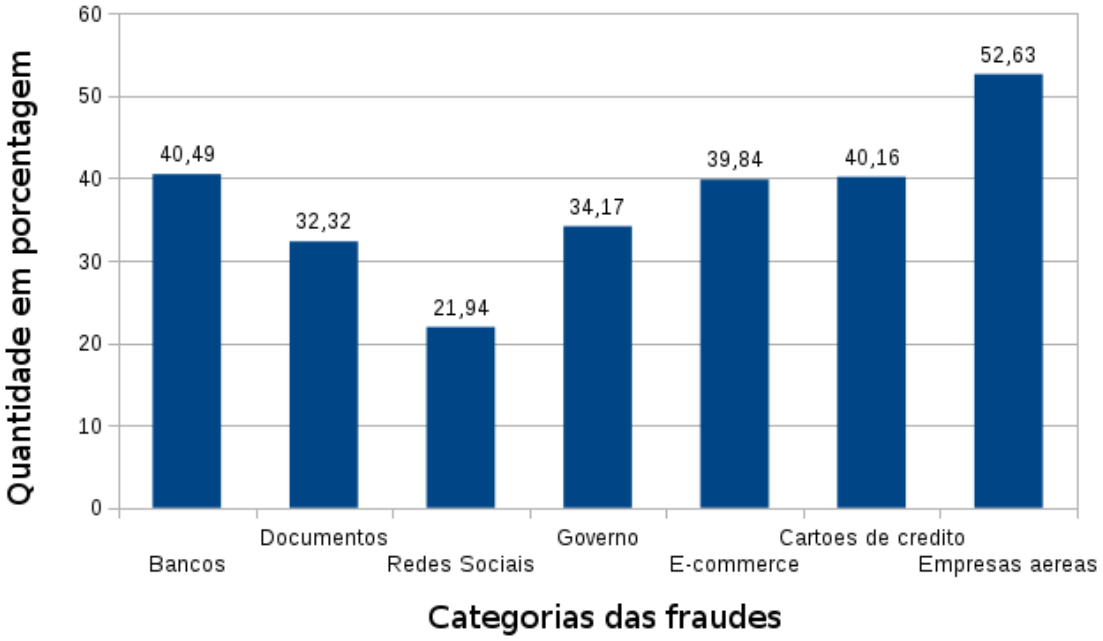
Domínios de primeiro nível (topo)

Domínio	Quantidade
com.br	170
googledrive.com	78
bitnamiapp.com	42
google.com	26
dropboxusercontent.com	21
tripod.com	18
formlogix.com	17
sugarsync.com	17
weebly.com	16
amazonaws.com	15

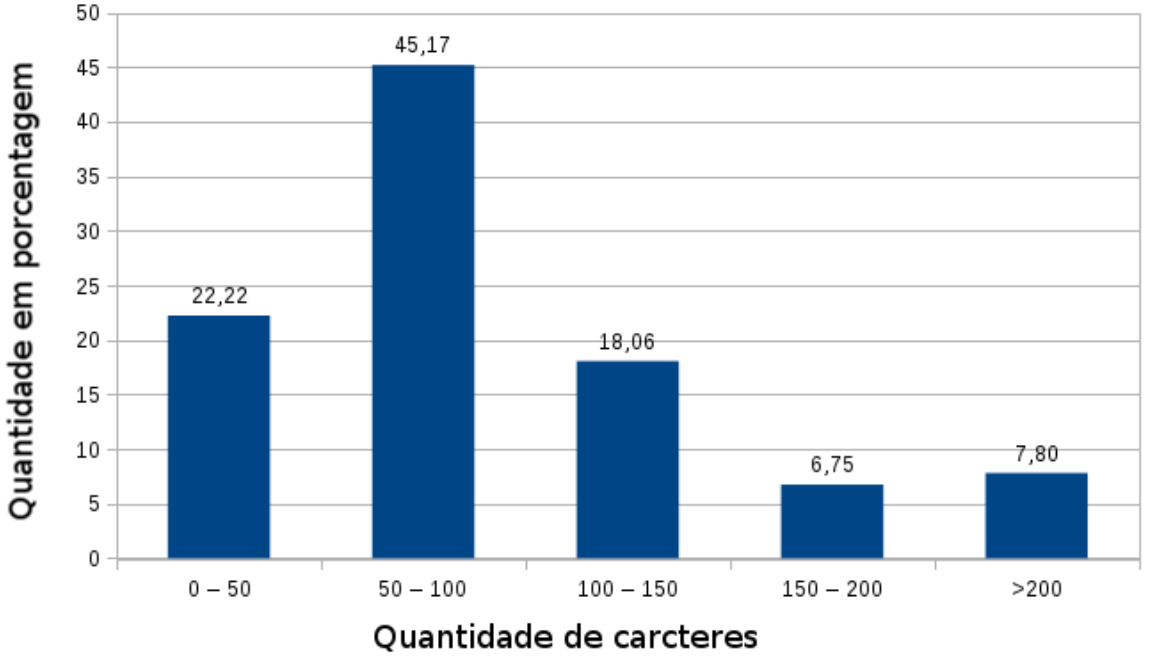
Domínios de até dois níveis

O Catálogo de URLs - Estatísticas

Nome de marcas e serviços na URL



Tamanho da URL



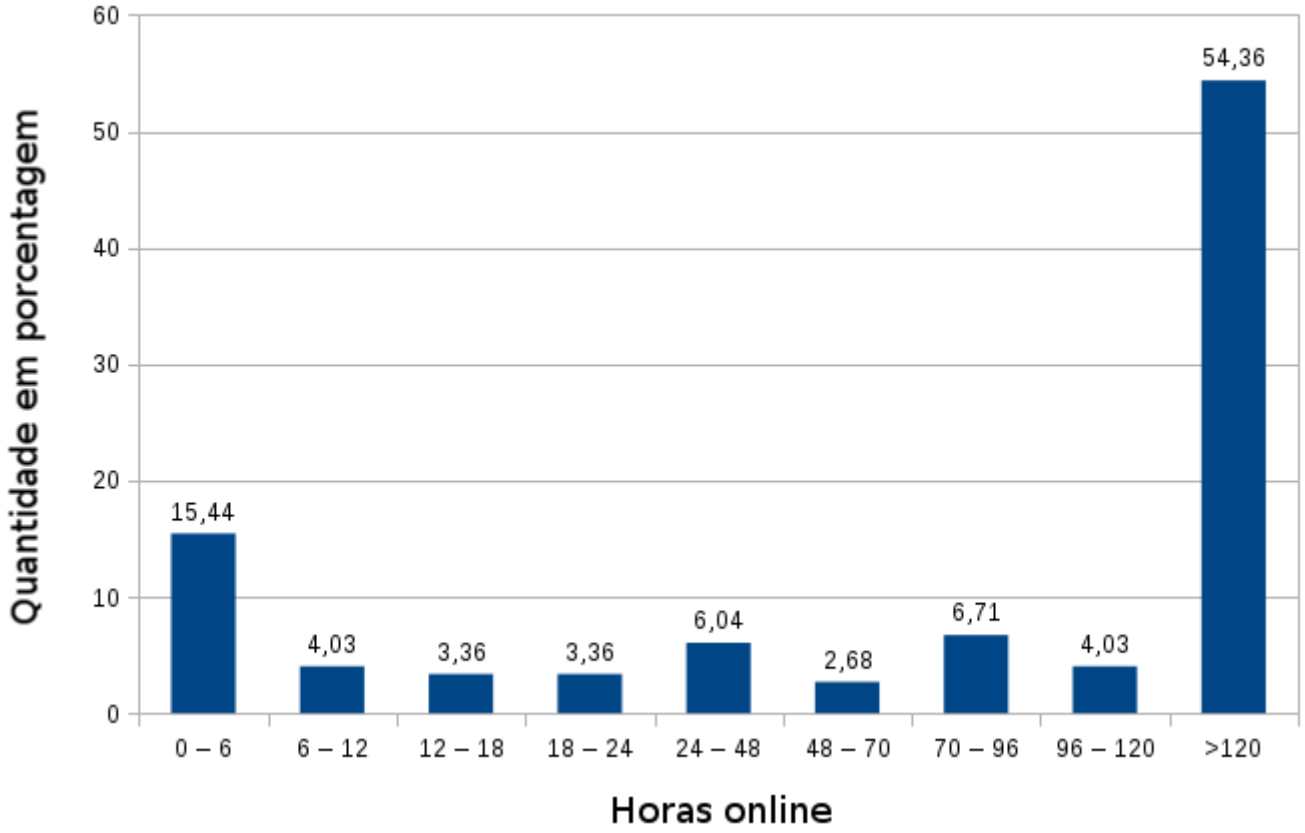
O Catálogo de URLs - Estatísticas

Tempo de vida do Phishing

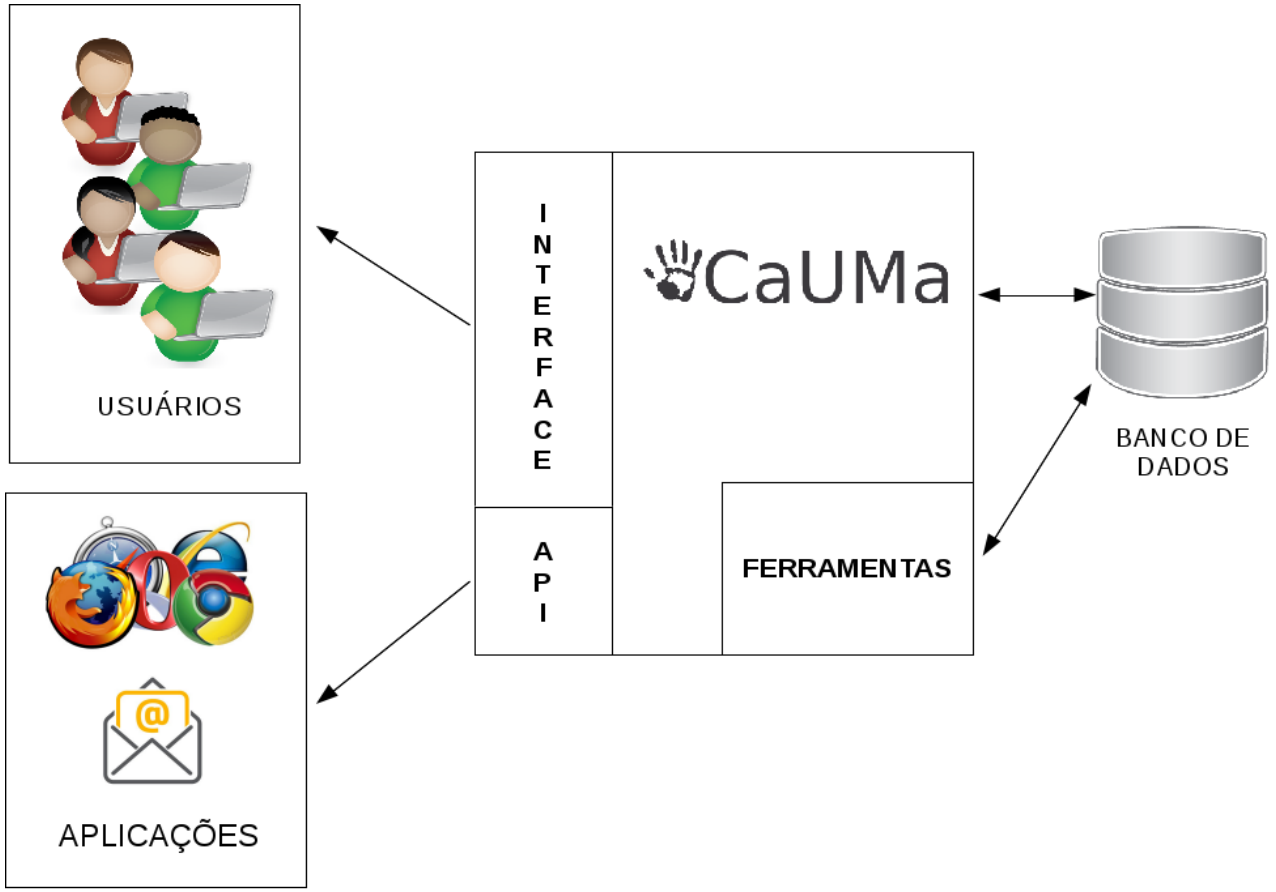
Artigo indicando como tempo de vida 48h - Sheng, S., An Empirical Analysis of Phishing Blacklists.(2009)

Notou-se diferença no tempo de vida das URLs brasileiras.Mais de 50% continuam disponível por um período igual ou superior a 5 dias.

A mesma URL pode ser detectada em mensagens fraudulentas diferentes.



O Catálogo de URLs - Arquitetura



Utilização

Através da busca direta na ferramenta

Utilização em complemento a outra blacklists através da API

O banco como base de conhecimento para desenvolvimento de pesquisas e de novos softwares e serviços relacionados a mitigação de phishing

Casos de uso

FURG – Plugin para Webmail Roundcube

Casos de uso

Desenvolvimento de projetos de pesquisa:

- Detecção de URLs maliciosas a partir de machine learning, UFBA, Lucas Ayres

Parcerias ainda em discussão

Conclusão

O aprimoramento nas técnicas para enganar o usuário quando se trata de mensagens maliciosas é notório e nem sempre o usuário está atento a essas questões, tornando necessário assim novos métodos de combate que não dependa apenas das boas práticas por parte do usuário.

Os serviços Catálogo de Fraudes e o CaUMa - Catálogo de URLs Maliciosas - além de alertar o usuário, cria uma base de conhecimento diariamente que pode servir como fonte para desenvolvimento de ferramentas de identificação, detecção e prevenção através do aprendizado de como essas fraudes se apresentam.

É valido considerar as particularidades de cada phishing que diferenciam-se, não somente de acordo com o grupo ao qual são direcionados como comunidade academica, empresas privadas, empresas públicas, como também de acordo com o país ao qual são enviados.

Trabalhos futuros

- Estabelecer parcerias com outras instituições
- Adicionar novas formas de captura de URLs
- Integração do CaUMa com os browsers
- Tornar a consulta mais inteligente :
  Inteligência artificial, desenvolvendo alguma heurística, usando outras informações como whois, expressão regular
- Desenvolvimento de plugins. ex.: cliente de e-mail Zimbra

Obrigada!

Paula Tavares
paulatavares@pop-ba.rnp.br