

nic.br egi.br

registro.br

COMBATE AO REGISTRO FRAUDULENTO DE DOMÍNIOS
GTS-30 | 07/12/2017

COMBATE AO REGISTRO FRAUDULENTO DE DOMÍNIOS

Rubens Kühl
NIC.br

registro.br nic.br cgi.br

Apple (ajuda-icloud.com.br)

← → ↻ Not secure ajuda-icloud.com.br

Apps Telefone Sistema Adminis Whois Scanner NIC/SRF Wiki SRF/PJ SRF/PF Beta INPI Comunic.br Coredump Coredump-ADM Infoplex - Busqu SociosBrasil.com Wayback Machin

iCloud [Buscar Meu iPhone](#)



Buscar iPhone

ID Apple

Senha

[Iniciar Sessão...](#)

[Esqueceu o ID Apple ou a Senha?](#)

[Instruções de Configuração](#)

Ponto Frio (ofertadireta-pontofrio.com.br)

ofertadireta-pontofrio.com.br/promocoes.php?id=OtghD-Elp3gh

Apps Telefone Sistema Adminis Whois Scanner NIC/SRF Wiki SRF/PJ SRF/PF Beta INPI Comunic.br Coredump Coredump-ADM Infoplex - Busqu SociosBrasil.com Wayback Machin

Confira as vantagens que o Pontofrio traz para você!

pontofrio.com

ATÉ 10% DE DESCONTO* NAS COMPRAS EM 1X NO CARTÃO DE CRÉDITO
*Válido somente para produtos vendidos e entregues pelo Pontofrio.com.br



Panela Elétrica de Arroz Philco PH5 Visor Glass - Preto - Panelas Elétricas...

Os melhores eletroportáteis com o menor...

De R\$ 89,90

POR R\$ 45.00

Clique e confira



Grill Mondial Redondo Smart Grill G-04 - Grill no PontoFrio.com ...

Grill Mondial Redondo Smart Grill G-04 c...

De R\$ 119,90

POR R\$ 60.00

Clique e confira



Multiprocessador Philco All in One Citrus 800W - Preto - Processador de Alime...

Promoções e preços baixos você só e...

De R\$ 149,90

POR R\$ 75.00

Clique e confira



Fritadeira Air Fryer Mondial AF-03 - Preta - Fritadeiras no PontoFrio.com ...

Fritadeira Air Fryer Mondial AF-03 - P...



Faqueiro Tramontina em Inox Copacabana com Estojo de Madeira - 76 Peças - At...

Faqueiro Tramontina Copacabana Inox c/ E...



Panela de Pressão Tramontina Malaga - 4,5 L - Panelas de Pressão no PontoFr...

Panela de Pressão Tramontina Malaga - 4...

Santander (atualizacao-app-seguro.com.br)

← → ↻ atualizacao-app-seguro.com.br ☆ :
Apps Telefone Sistema Adminis Jr Whois Scanner NIC/SRF Wiki SRF/PJ SRF/PF Jr Beta INPI Jr Comunic.br Jr Coredump Jr Coredump-ADM Infoplex - Busqu SocioBrasil.com Wayback Machin

 Santander



 Pessoa Física  

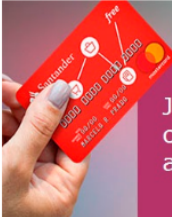
Internet Banking Como Acessar ▾

▼ Pessoa Física ▶ Pessoa Jurídica

[Acesse sua conta](#)




Quero

-  Um cartão de crédito
-  Abrir uma conta
-  Baixar o App Santander



Já pensou em ter um cartão de crédito livre de anuidade?

Resolva On-line e facilite seu dia a dia

-  Fatura de cartão
-  Baixar o App Way
-  Boletos

Americanas (americanas-oficiais.com.br)

americanas-oficiais.com.br/Produtos/www.americanas.com/Smart-TV-LED-55-Samsung-Full-HD-com-Convertor-Digital-Wi-Fi-Miracast-WiDi-2-USB-3-HDMI-25.html

Apps Telefone Sistema Adminis Whois Scanner NIC/SRF Wiki SRF/PJ SRF/PF Beta INPI Comunic.br Coredump Coredump-ADM

tele vendas 24h atendimento meus pedidos minha conta loja mais próxima cartão americanas.com

Seu Barato O maior outlet da internet

americanas.com

a maior loja. os menores preços.

buscar



olá, faça seu login ou cadastre-se



minha cesta 0 item

compre por departamento

oferta do dia

tv e home theater > tv > tv led

Smart TV LED 55" Samsung Full HD com Conversor Digital Wi-Fi Miracast WiDi 2 USB 3 HDMI (código do produto: 126644670)

DES
CON
TAÇO

DES
CON
TAÇO

zoom
passe o mouse



SP

R\$ 3.999,00 - (desconto de 60%)

R\$ 1.399,00

Promoção válida apenas para pagamento via BOLETO

• **R\$ 1.399,00** (60% de desconto) **Avista** no Boleto

produto em estoque
vendido e entregue por americanas.com

comprar

Oneclick

frete e prazo:

CEP -

calcular

não sei meu CEP

lista casamento

recomendar

informações do produto

informações técnicas

avaliação dos clientes

garantia estendida

manual de instruções

informações do produto

pesquise uma característica



Smart TV LED 55" Samsung Full HD com Conversor Digital Wi-Fi Miracast WiDi 2 USB 3 HDMI

CONTRATO DO REGISTRO.br

CLÁUSULA TERCEIRA: DOS DADOS CADASTRAIS

I. O REQUERENTE deverá fornecer seus dados pessoais, solicitados nos campos de preenchimento obrigatório do site do REGISTRO.br, de forma que reflitam sempre os seus dados reais e válidos;

CLÁUSULA QUARTA: DAS OBRIGAÇÕES DO REQUERENTE

O REQUERENTE do registro de domínio e usuário da base de dados do REGISTRO.br se obriga a:

I. **Escolher** adequadamente **o nome do domínio** a ser registrado, ciente de que **não poderá ser registrado** nome que desrespeite a legislação em vigor, que **induza terceiros a erro**, que viole direitos de terceiros, que represente conceitos predefinidos na rede Internet, que conceitue palavras de baixo calão ou abusivas, que simbolize siglas de Estados, Ministérios, dentre outras vedações;

V. **Fornecer e manter somente dados verdadeiros, atualizados e completos**, declarando-se ciente de que a utilização de dados falsos, inválidos, incorretos ou de terceiros, são de sua inteira responsabilidade, **podendo acarretar a rescisão do presente CONTRATO** e, conseqüentemente, o cancelamento automático do domínio registrado, e, ainda, caracterizar a prática de ato ilícito, sujeitando-o as penalidade previstas em lei;

VI. **Utilizar adequadamente e somente para fins lícitos o domínio a ser registrado**, não praticando quaisquer atos que violem a legislação e regulamentos em vigor;

IX. **Apresentar documentos** e atualizar dados **quando solicitado pelo REGISTRO.br**

O QUE CONSTITUI UM REGISTRO FRAUDULENTO

Uso do nome de domínio para colaborar numa tentativa de enganar usuários

Dados falsos de registro

Uso de domínios descartáveis

Possíveis ações:

- **Pedido de documentos**
- **Pedido de documentos e assinatura de termo de responsabilidade**
- **Congelamento imediato**



COMO ERA EM 2016

Relatos recebidos via abuse ou hostmaster@registro.br

Filtros (expressões regulares) em cima do feed de registro de novos domínios

Relatos recebidos via rede de contatos, incluindo listas de discussão

COMO FICOU EM 2017 (1º semestre)

Relatos recebidos via abuse ou hostmaster@registro.br

Filtros (expressões regulares) em cima do *feed* de registro de novos domínios

Relatos recebidos via rede de contatos, incluindo listas de discussão

Processamento de *feeds* gratuitos de informação

- **OpenPhish**
- **PhishTank**
- **ShadowServers Compromised Website**
- **Malware Patrol**
- **[Fornecedor não identificável devido a *NDA*]**

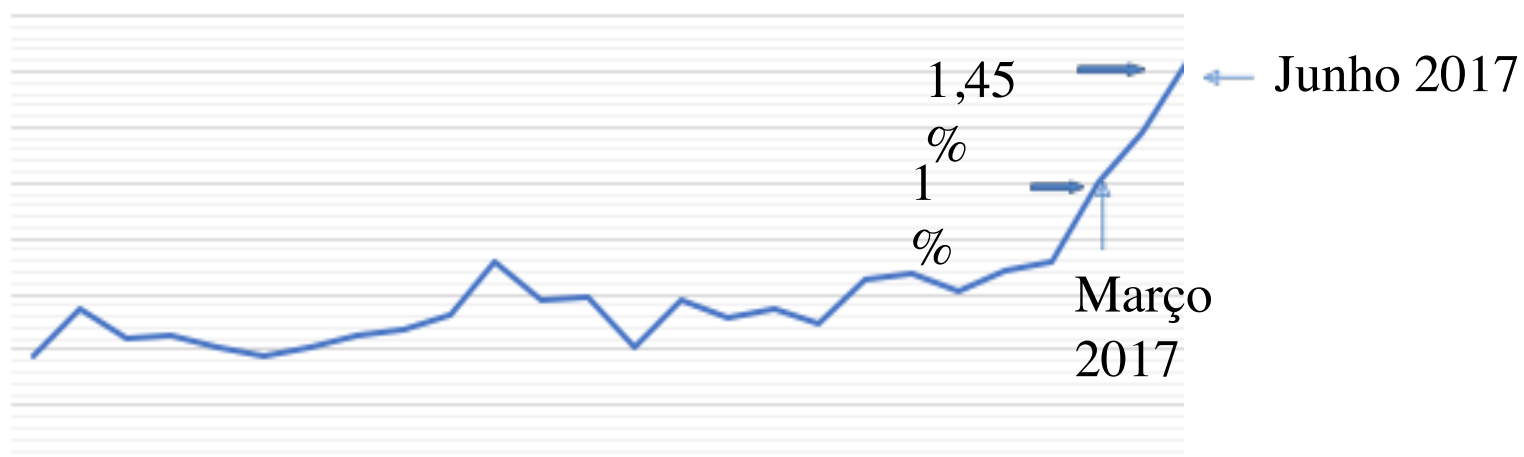
(Quais são mais efetivos ?)



ACÇÃO E REACÇÃO



O QUE ACONTECEU NO *CHARGEBACK*



FRAUDE DE REGISTRO DE DOMÍNIO x FRAUDE DE MEIO DE PAGAMENTO

Mais correlacionados do que se imaginava

Há correlação nos dois sentidos

Coordenação desses dois fatores não apenas diminui volume, melhora também tempo de detecção e ação

REFORÇOS



NOVAS FERRAMENTAS



RESULTADO



HORIZONTE 2018

Migração de ferramentas internas de e-mail para aplicação Web

Investigação de novos *feeds* (problema: baixo ROI incremental)

Incorporação de técnicas de *scoring* da experiência humana em algoritmos

Utilização de padrões de *queries* DNS como indicador

Machine Learning, talvez ?

Run, Fraudster, Run!



Obrigado!
<https://registro.br>

 rubens@registro.br

nic.br egi.br

www.nic.br | www.cgi.br