Faculdades Integradas de Caratinga

TCC – Trabalho de conclusão de curso

ANÁLISE DE INVASÕES SOBRE HONEYPOTS DE BAIXA INTERATIVIDADE EM AMBIENTES LINUX

Gláucio Douglas Moreira

Orientador: Prof. Jacson Rodrigues Correia Silva

FIC

Caratinga, 10 de Dezembro de 2010

Sumário

Introdução

- Valor da Informação
- Tecnologia nova na computação
- Honeypots
    - Produção
    - Pesquisa
- Honeynets

Introdução (Cont.)

- Níveis de envolvimento
  - Baixa interatividade
  - Média interatividade
  - Alta interatividade
- Representatividade
  - Individual
  - Componente de uma Honeynet

Justificativa

- Carência de estudos na área.
- Grande demanda por profissionais no mercado
- Polêmica envolvida no assunto
- Investimentos em segurança no Brasil
- Necessidade e preocupação em segurança nas empresas

Objetivo Geral

- Analisar as invasões a Honeypots pela Internet em ambientes Linux de forma a levantar dados relevantes para a segurança em redes de computadores

Objetivos específicos

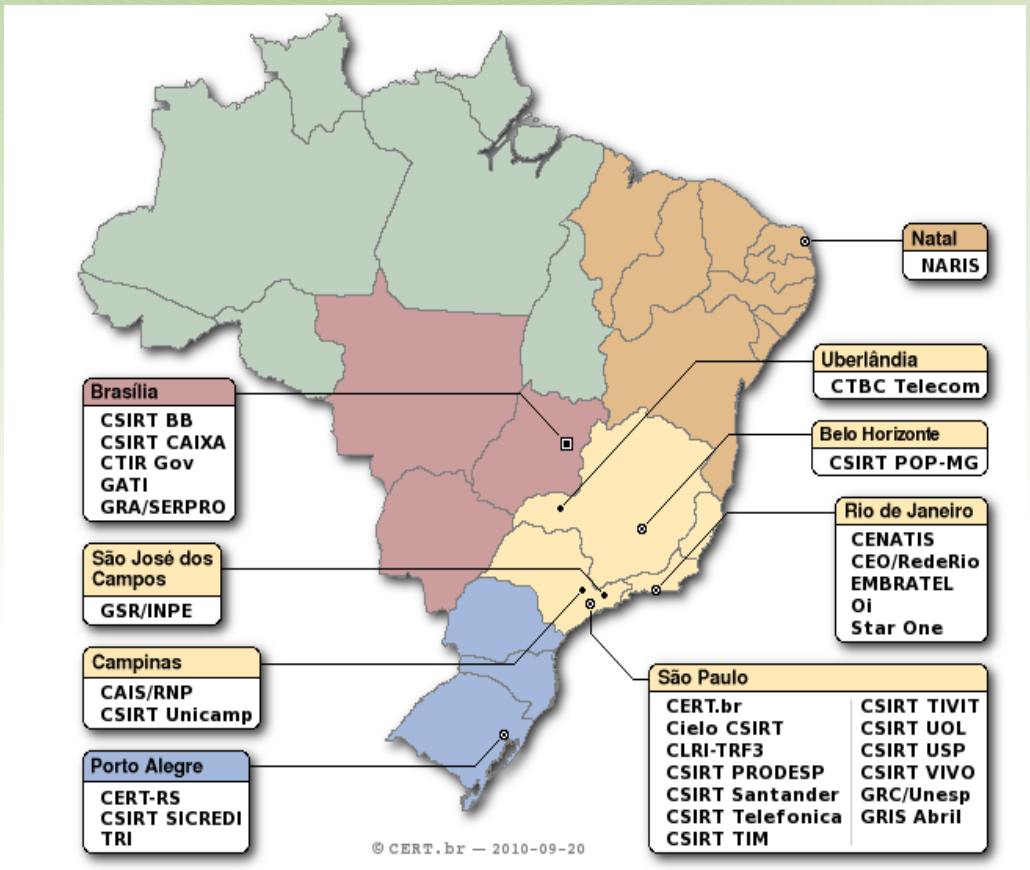
- Utilizar-se do ambiente Honeypot para obtenção de dados como:
  - IP de origem do ataque
  - Usuários e senhas mais utilizados
  - Data e hora do ataque, e as maiores reincidências
  - Comandos executados
  - Serviços mais comprometidos

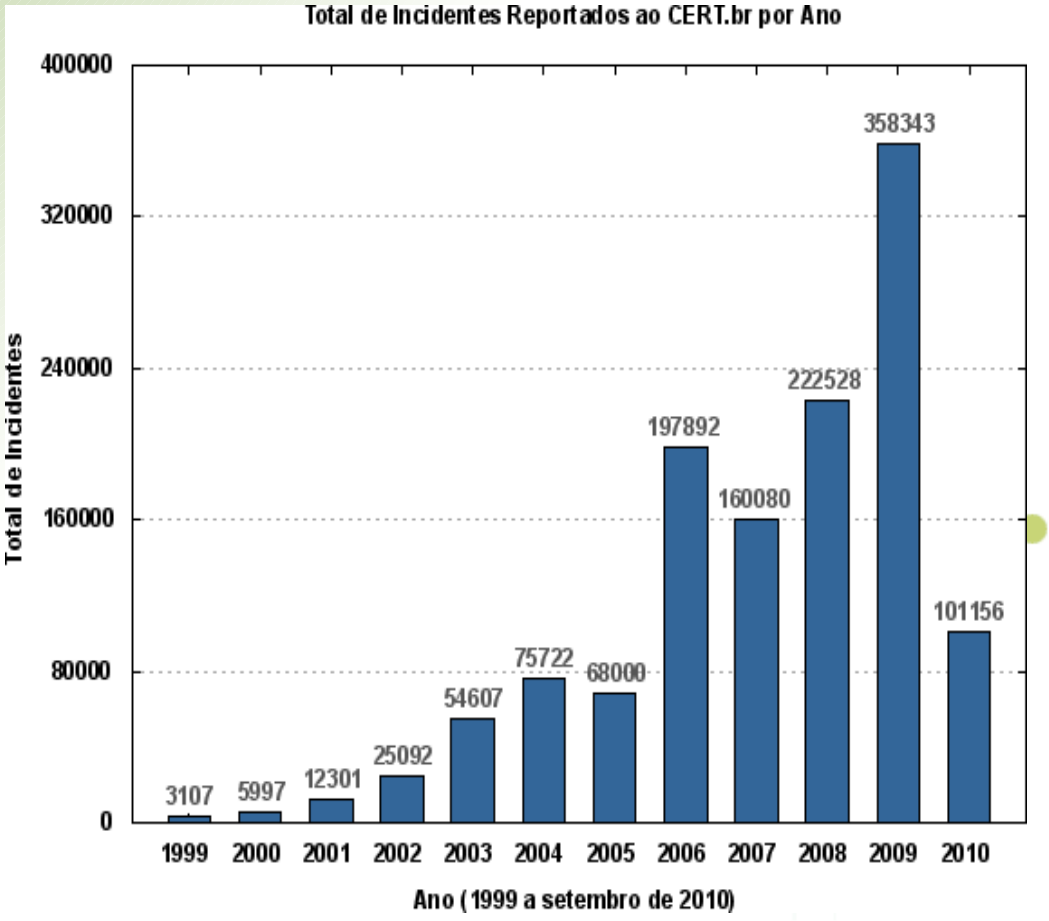
Referencial teórico

- Fakes-servers & Honeyperl
- Servidores falsos, com propósito de serem comprometidos. Fakes trabalhados:
  - squid
  - httpd
  - Telnet
  - echo
  - smtp
  - pop3
  - ftp

CERT.br e CSIRTs

- Tratamento de incidentes
- Treinamento e conscientização
- Análise das tendências de ataques



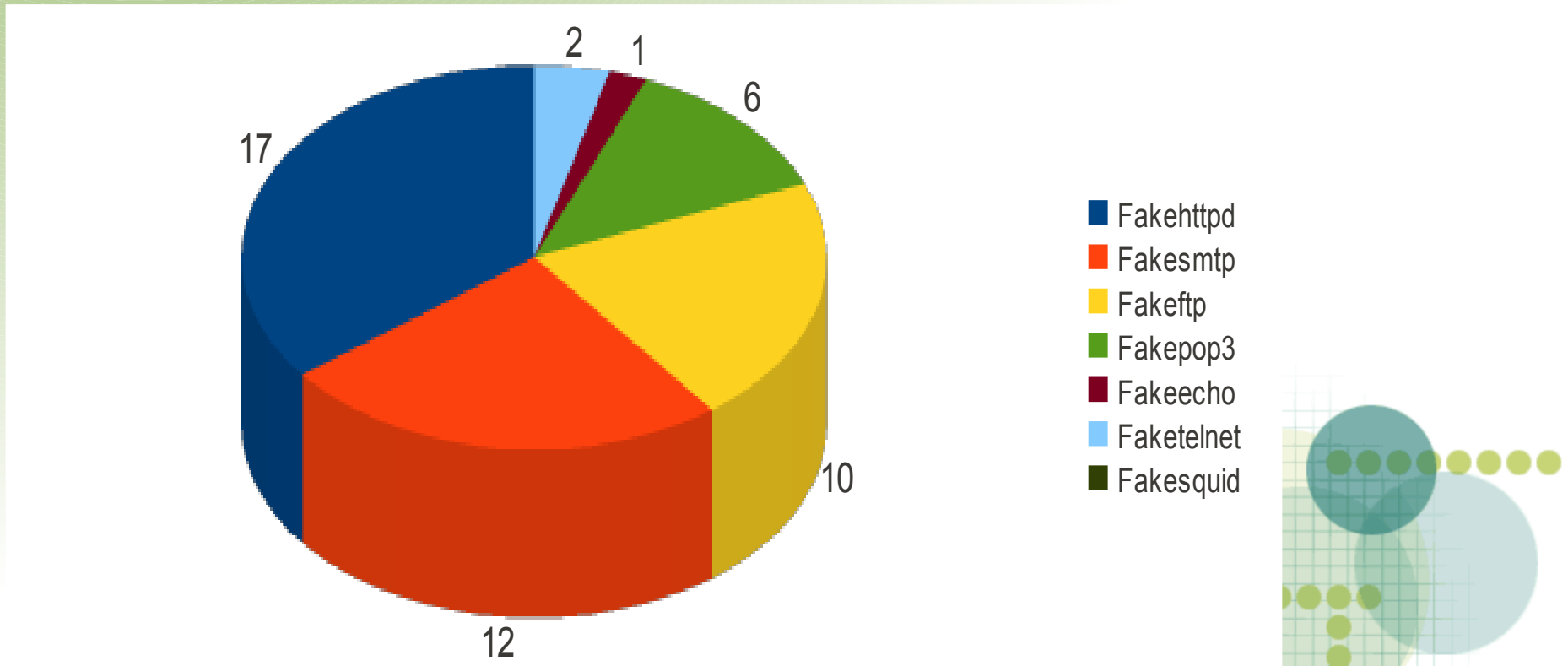


Metodologia

- Através da implantação de um Honeypot de baixa interação em ambiente Linux, conseguir levantar informações que revelam a real necessidade da aplicação de um Honeypot
- DNS Dinâmico
- Implantação da ferramenta Honeyperl
- Análise das informações em 44 dias

Resultados

- Serviços mais comprometidos
- Comprometimento por origens distintas



IP, País de origem, data e hora

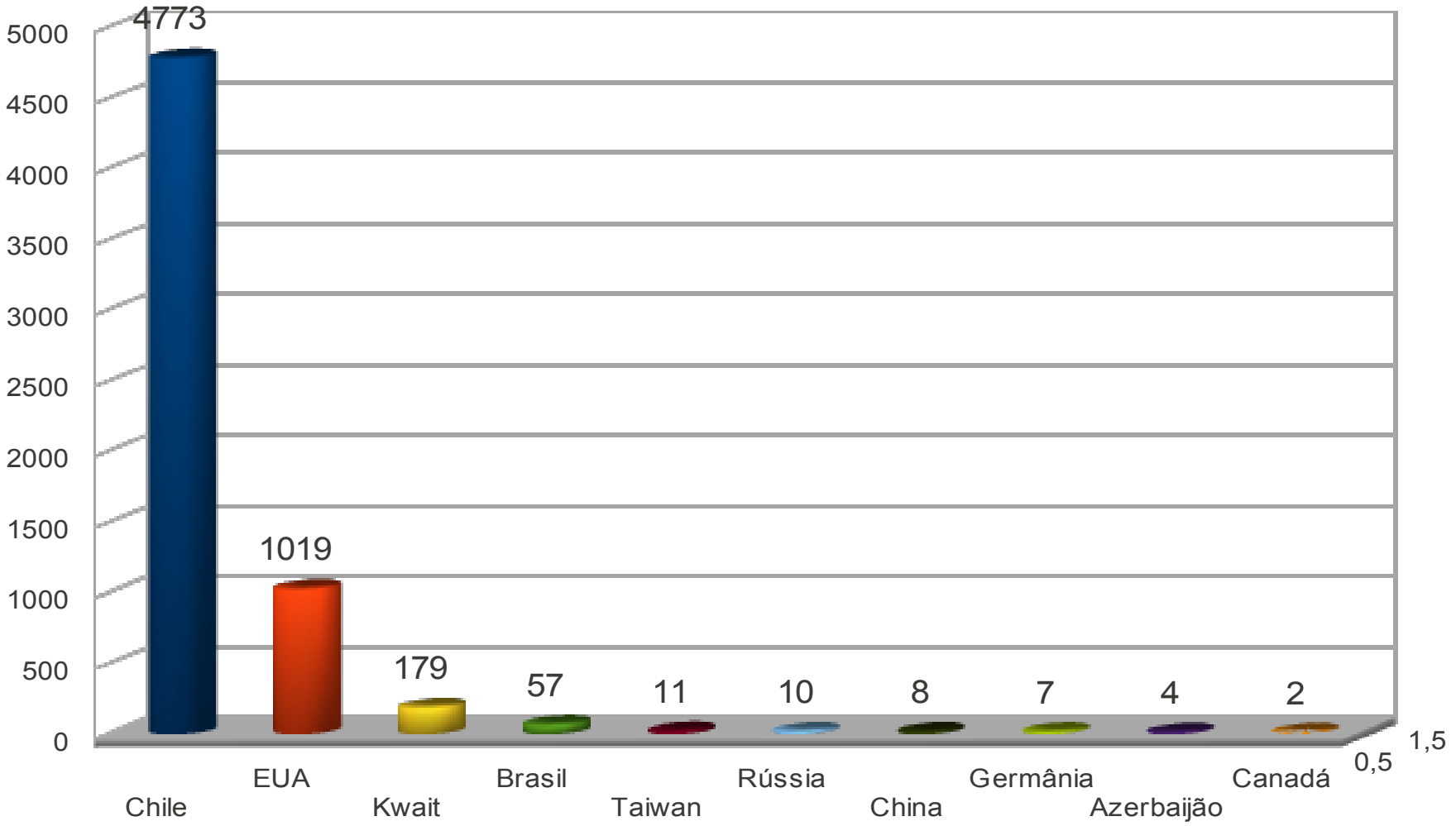
DATA/HORA	IP	PAÍS DE ORIGEM	NÚMERO DE ATAQUES
11/10/2010 16:00 às 17:00	114.45.50.191	República da Coréia	1
12/10/2010 a 13/10/2010 11:00 as 17:00	189.76.222.254	Brasil	26
13/10/2010 21:00 às 22:00	189.127.159.154	Brasil	14
13/10/2010 23:00:00	63.230.183.150	Estados Unidos	1
14/10/2010 07:00 às 08:00	118.168.142.195	Taiwan	1
15/10/2010 2:00 às 3:00	96.0.243.210	Estados Unidos	859
15/10/2010 a 20/10/2010 11:00 às 02:00	112.105.142.231	Taiwan	2
15/10/2010 00:00 às 01:00	187.63.198.185	Brasil	5

Usuários e senhas mais utilizados

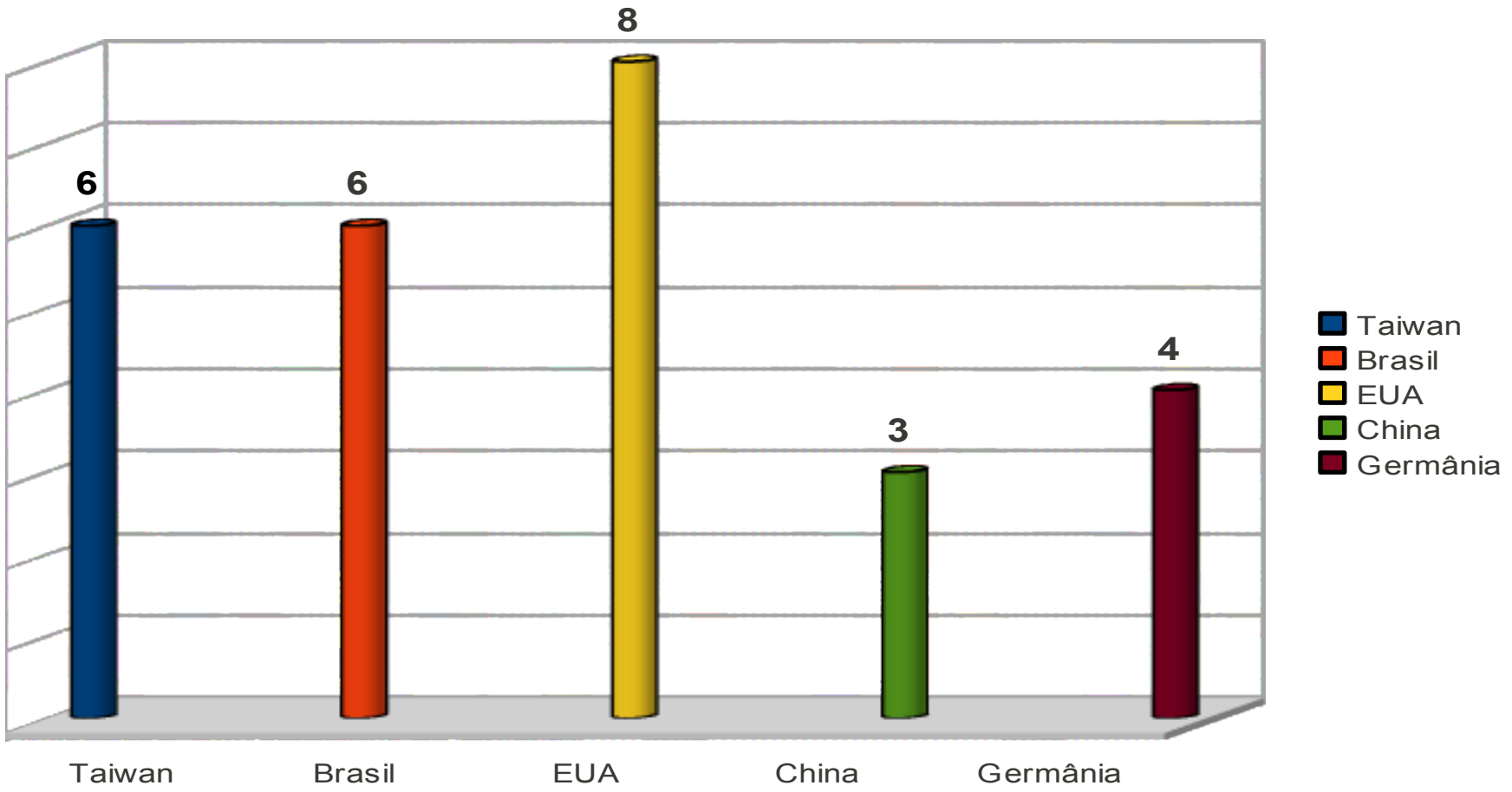
- Usuários e senhas eram intercalados. Atitude comum dos ataques ao Honeypot

IP	FAKE	USUÁRIOS	SENHAS
96.0.243.210	POP3	stanley,roob,milton,minim,tester,neal,solar,root,todd,stell,neil,pics,portal,timothy,victor,wear,rosimare,tomy,sasha,sanchez	test1234,passwd,qweasd.
118.175.66.120	POP3	root,admin,webmaster,user,web,www,administrator,oracle,sybase,informix,oracle8,lizdy,data,account,access,pwrchute,	1234

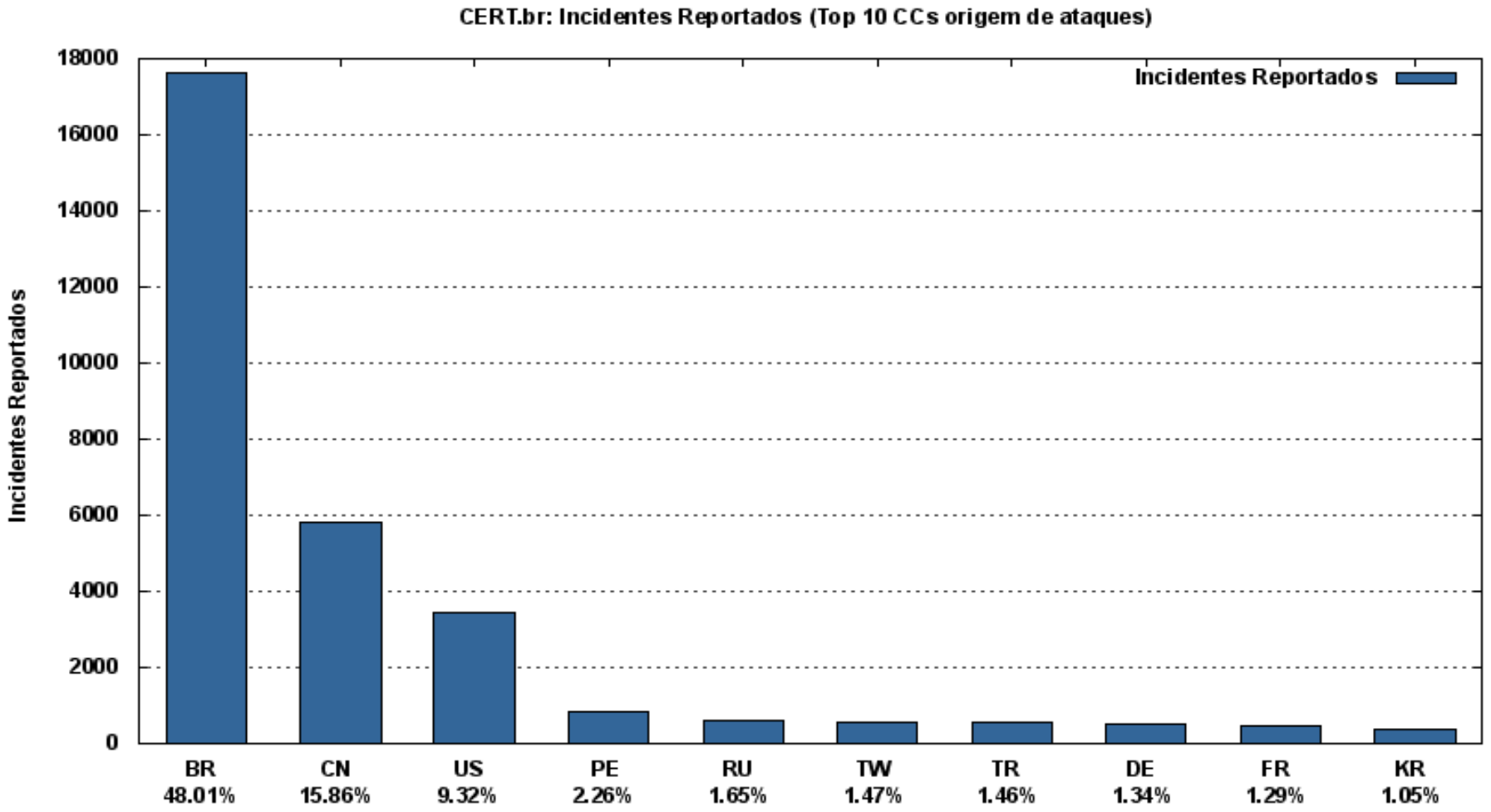
Ranking origem de ataques



Reincidência



Ranking 10 países CERT.br



Conclusão

- Grande demanda de estudos com novos métodos como Honeypot para segurança
- Honeypot não substitui as técnicas utilizadas por administradores de redes, e sim agrega valores
- A importância do Honeyperl no estudo sobre Honeypot
- Dados coletados servem de melhorias a diversas ferramentas
- Informações de segurança geradas para a empresa e/ou instituição envolvida

Trabalhos futuros

- Implementar um ambiente Honeypot & Honeynet para análise de segurança em instituições de ensino

- A instituição FIC ser um CSIRT, ou seja um ponto de presença do CERT.br

Referências Bibliográficas

ANDRUCIOLI, Alexandre Pinaffi. **Proposta e Avaliação de um Modelo Alternativo Baseado em Honeynets para Identificação de Ataques e Classificação de Atacantes na Internet**. Universidade Federal do Rio de Janeiro – COPPE/UFRJ. Tese de Mestrado apresentada em Abril de 2005.

The Honeynet Project: **Conheça seu inimigo – O projeto Honeynet**. Editora Makron Books, São Paulo, 2002.

LUIZ, Alberto. **Possibilidades de uso de Software livre como ferramentas de análise em investigações digitais**. Universidade Federal de Lavras – UFLA. Monografia apresentada em 10 de setembro de 2005.

RODRIGUES, Renato. **HONEYPOTS, Acompanhando os passos de uma invasão em tempo real**. Universidade Federal de Fortaleza – UNIFOR. Monografia apresentada em Novembro de 2004.

NETO, Urubatan., **Dominando Linux Firewalls Iptables**. 1ªed. Ciência Moderna Ltda, Rio de Janeiro – Brasil, 2004.

SOUZA, Tiago. **Honeypots – A segurança através do disfarce**. Universidade Federal do Rio de Janeiro – COPPE/UFRJ. Monografia apresentada em 9 de Agosto de 2005.

STATO, André. **LINUX Controle de Redes**, 1 ed. Visual Books Florianópolis-SC: Visual books 2009.

ULBRICH, Henrique César; VALLE, James Della. Universidade H4CK3R. 5a Ed. São Paulo: Digerati Books 2007