Honeypots Um Projeto Pró-ativo em Segurança de Redes

Marita Maestrelli **marita@cbpf.br**
Fernando Spencer **spencer@cbpf.br**

2006

Prefácio

Hoje necessitamos da segurança virtual tanto quanto da segurança física. A computação está em nosso dia a dia e a conexão com a Internet é essencial para a comunicação pessoal e profissional.
Várias propostas são lançadas para prover segurança na Internet, como máquinas configuradas com sistemas de análise de fluxo para identificação de tráfego malicioso e possível bloqueio, máquinas com listas de acesso a determinados serviços, e no nosso caso, máquinas rodando sistemas simulados para conseguir o maior número de informações para identificação de intrusos e assim evitá-los em nossos sistemas reais.
Esta nota técnica descreve um projeto Nacional de HoneyPots, ou seja, máquinas em diversos ponto da Internet Brasileira coletando informações sobre procedimentos que atrapalham o fluxo de tráfego em nossas redes.

Índice

1. Histórico

Cronológico dos Projetos de Honeypots e Honeynets:

- 1989: "*The Cuckoo's Egg*"
- 1992: "*An Evening with Berferd*"
- 1998: *Deception Toolkit* (DTK)
- 1999: *The Honeynet Project*

– Rede projetada para ser comprometida

– Utilizada para observar o comportamento dos invasores

- 2002: *Honeynet Research Alliance*
- 2002: Honeynet.BR

- Acompanhamento de atividades hostis na Internet BR

- 2003: Consórcio Brasileiro de Honeypots

- Criado em setembro de 2003, sob a coordenação do Dr. Antonio Montes (CENPRA/MCT), Cristine Hoepers e Klaus Steding-Jessen (CERT.BR/CGIBR).

Consórcio Brasileiro de Honeypots

Em setembro de 2003 foi criado o Projeto de Honeypots Distribuídos com o objetivo principal de aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro.

Atualmente conta com 34 instituições participando com pelos menos um ponto em diversos estados brasileiros. A localização desses pontos pode ser observada na figura 1.

A página do Projeto e a fonte da figura 1 e da Tabela 1 pode ser acessada através de: http://www.honeypots-alliance.org.br/

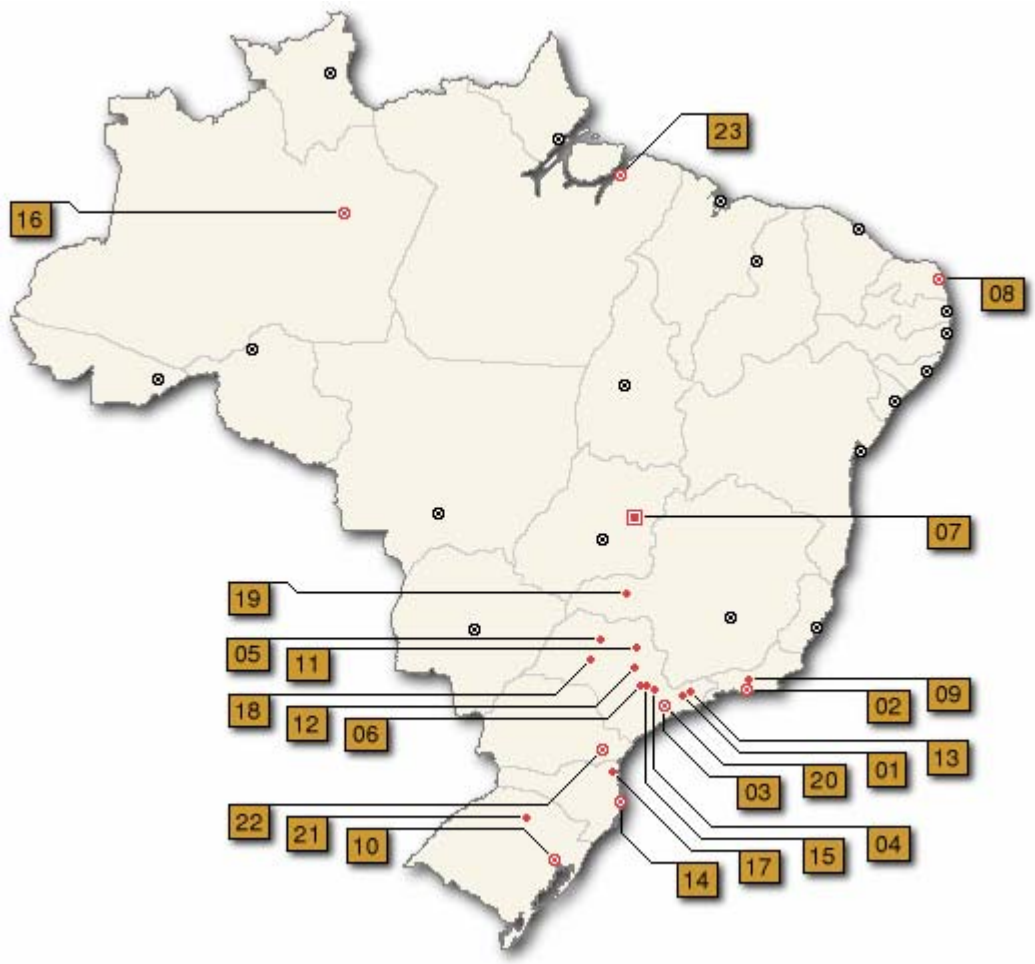

Figura 1 – Localização dos Honeypots no território brasileiro

Na Tabela 1 estão listadas as Instituições que fazem parte da aliança com seu respectivo número relacionado na figura 1.

O CBPF e a RedeRio participam do Projeto desde outubro de 2003 e são pioneiras no Rio de Janeiro, além de incentivar e ajudar as demais instituições do estado. Atualmente conta com 4 (quatro) *hosts* no projeto.

- Únicas máquinas da SUN (4) no projeto, 1 modelo Sparc 4, 1 modelo Sparc 5, 1 modelo Ultra 1, e 1 modelo Ultra 2;
- Os quatro honeypots iniciaram em: 1º. – outubro de 2003, 2º. – março de 2004, 3º. – agosto de 2004 e 4º. – julho de 2005;

Tabela 1 – Instituições que fazem parte da Aliança

#	Cidades	Instituições
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, HP Brasil, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministério da Justiça, TCU, UNB LabRedes
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR
23	Belém	UFPA

2. Introdução

Situação Atual da Internet:

- Crescente número de computadores conectados com disponibilidade de banda larga
- Descuido nas configurações de vários desses computadores
- A informação é disponibilizada com facilidade
- Grande quantidade de informações potencialmente maliciosas
- Necessidade de mecanismos para coibir ou diminuir o tráfego malicioso

Na busca de soluções surgiu o Projeto de Honeypots Distribuídos, com finalidades bem determinadas:

- Implantar uma rede distribuída de honeypots de baixa interatividade (*Honeyd*), buscando cobrir a maior parte do espaço de endereços IP da Internet no Brasil;
- Montar um sistema de análise de dados que permita o estudo de correlações e tendências de ataques;
- Atuar conjuntamente com Grupos de Resposta a Incidentes de Segurança de Computadores (CSIRTs) na difusão destas informações.

3. Honeypots e Honeynets

3.1. HoneyPots

São recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades.

São implementados de maneira que todo o tráfego destinado a eles seja anômalo ou malicioso, minimizando os falsos-positivos.

São classificados de duas maneiras:

- **Honeypots de Baixa Interatividade**

Os sistemas e serviços de rede são emulados e o sistema REAL é inacessível.

São relativamente seguros e podem ser usados como monitoramento em redes de produção.

- **Honeypots de Alta Interatividade**

Os serviços de rede são legítimos e o atacante pode assumir o controle do honeypot.

Proporcionam coleta de inteligência, análise de tendências,novas vulnerabilidades, captura de ferramentas, etc.

A tabela a seguir mostra uma comparação entre os dois tipos de Honeypots:

Baixa Interatividade	**Alta Interatividade**
Emulam sistemas e serviços	**Executam as versões reais**
Simples.Fácil gerenciamento	**Cuidados na instalação e configuração. Coleta de artefatos**
Atacante não tem controle	**Pode ter controle total**
Ações limitadas, captura de tráfego e malware	**Captura de mais informações, incluindo ferramentas e comandos**
Difíceis de iludir atacantes avançados/determinados	**Difícil de distinguir de um sistema de produção**

3.2. HoneyNets

São redes compostas de uma sub-rede de administração e de uma sub-rede de honeypots.

"Honeynets são ferramentas de pesquisa que consistem de uma rede projetada especificamente para ser comprometida, com mecanismos de controle que impedem que esta rede seja usada como base para lançar ataques contra outras redes." Cristine H., Klaus S.-J., A. Montes

As Honeynets podem ser de dois tipos:

- **Honeynets Reais**

Em uma *honeynet* real os dispositivos que a compõem, incluindo os *honeypots*, mecanismos de contenção, de alerta e de coleta de informações, são físicos.

Para exemplificar, uma *honeynet* real poderia ser composta pelos seguintes dispositivos:

- diversos computadores, um para cada *honeypot*. Cada *honeypot* com um sistema operacional, aplicações e serviços reais instalados;
- um computador com um *firewall* instalado, atuando como mecanismo de contenção e de coleta de dados;
- um computador com um IDS instalado, atuando como mecanismo de geração de alertas e de coleta de dados;
- um computador atuando como repositório dos dados coletados;

- *hubs*/*switches* e roteador (se necessário) para fornecer a infra-estrutura de rede da *honeynet*.

As vantagens deste tipo são: baixo custo por dispositivo; mais tolerante a falhas (ambiente é distribuído), e os atacantes interagem com ambientes reais.

As principais desvantagens são: manutenção mais difícil e trabalhosa; necessidade de mais espaço físico para os equipamentos, e custo total tende a ser mais elevado.

- **Honeynets Virtuais**

Uma *honeynet* virtual baseia-se na idéia de ter todos os componentes de uma *honeynet* implementados em um número reduzido de dispositivos físicos. Para isto, normalmente é utilizado um único computador com um sistema operacional instalado, que serve de base para a execução de um *software* de virtualização, como o *VMware* (*Virtual Infrastructure Software*) ou o *UML* (*User Mode Linux*). Os *softwares* de virtualização permitem executar diversos sistemas operacionais com aplicações e serviços instalados, ao mesmo tempo.

As vantagens das *honeynets* virtuais são: manutenção mais simples; necessidade de menor espaço físico para os equipamentos, e custo final tende a ser mais baixo.

As principais desvantagens são: alto custo por dispositivo, pois são necessários equipamentos mais robustos; pouco tolerante a falhas (muitos componentes concentrados em um único ponto); o *software* de virtualização pode limitar o *hardware* e sistemas operacionais utilizados; o atacante pode obter acesso a outras partes do sistema, pois tudo compartilha os recursos de um mesmo dispositivo (no caso da categoria de auto-contenção), e possibilidade do atacante descobrir que está interagindo com um ambiente virtual.

4. Projeto HoneyPots Distribuídos

- Rede de Honeypots de baixa interatividade com o objetivo de cobrir o maior número de AS da Internet brasileira.
- Implantado em diversas redes de produção no Brasil, atualmente conta com 44 hps e aproximadamente 10000 ips.
- Utiliza o aplicativo *honeyd* para emular diferentes sistemas operacionais e serviços de rede.
- Logging centralizado.

- Capacidade de detecção de incidentes (complementa os SDI).
- Permite levantar tendências de ataques, coletar artefatos, correlacionar eventos, no ciberespaço brasileiro.
- Apoio à atuação de grupos de resposta a incidentes de segurança.

Configuração de um HoneyPot de baixa interatividade:

- Sistema real: openBSD com firewall e kernell compacto;
- Simulador: honeyd
- Proxy ARP: arpd
- Programas para registrar as atividades: *listeners*
- Geração de logs diários enviados para um servidor central

A figura a seguir é uma representação simbólica de um Honeypot no CBPF:

- **Sistema OpenBSD**
- ***honeyd***
- ***arpd***
- **Estação Sun Sparc**

- **Sistema OpenBSD** – é um sistema operacional livre da família UNIX, multiplataforma. Suas vantagens mais enfatizadas são: padronização, portabilidade, correção e segurança.
- **Honeyd** – é um programa que cria hosts virtuais em uma rede. Os hosts podem ser configurados como executando serviços arbitrários e podem ser adaptados paracendo rodar em certos sistemas operacionais. Honeyd habilita um único host com múltiplos endereços.
- **Arpd** – é um programa que escuta pedidos ARP e responde por endereços IP não alocados. Utilizando ARPD em conjunto com HONEYD é possível povoar o espaço de endereço não alocado em uma rede de produção com honeypots virtuias.
- **Estação SUN Sparc** – máquina com arquitetura robusta e estável.

5. Resultados – Estatísticas

Os demonstrativos a seguir foram elaborados só com os daods dos HoneyPots do CBPF.

A Figura 1 mostra a porcentagem de cada protocolo(TPC, UDP e ICMP) dos pacotes que trafegam nos Honeypots.

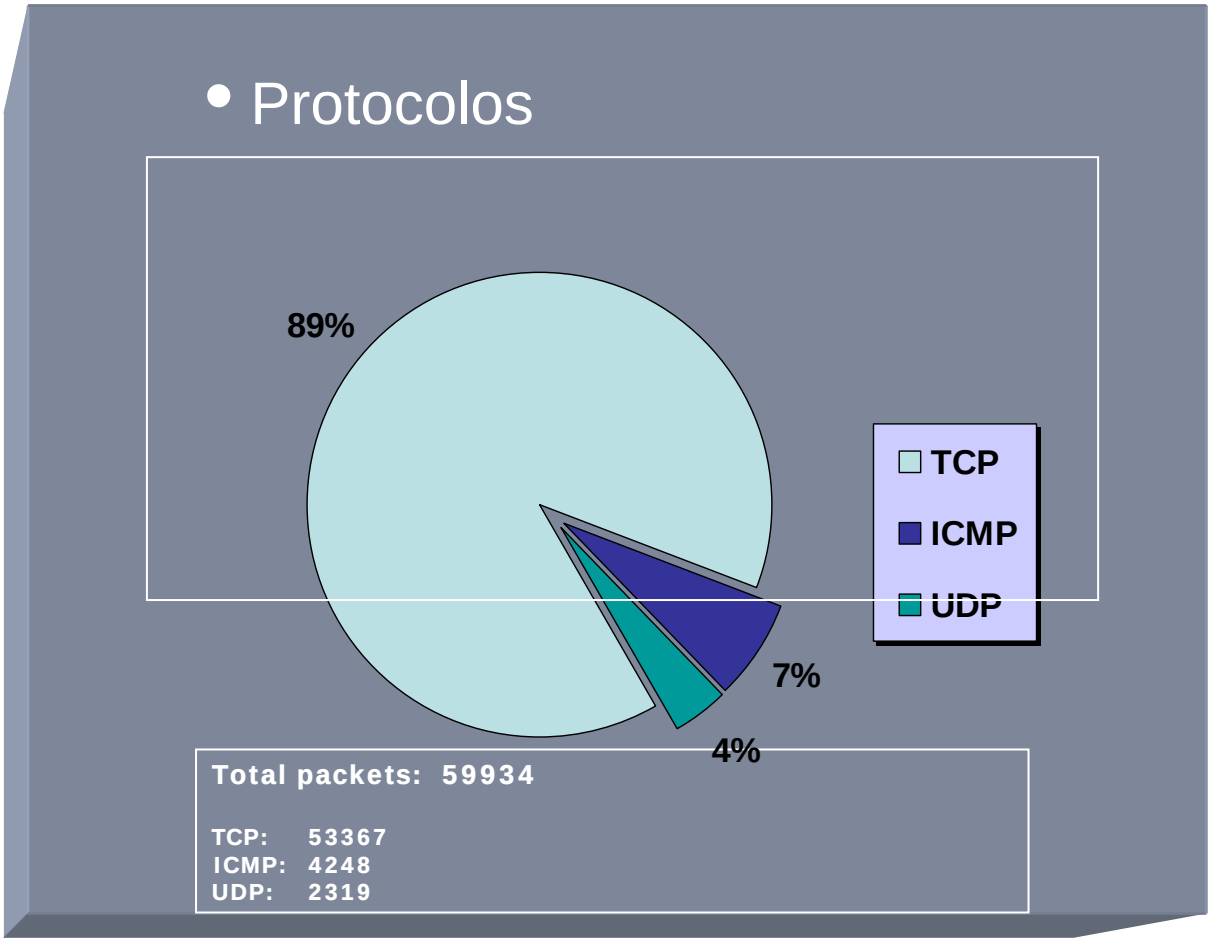

Figura 1 – Protocolos dos pacotes nos Honeypots

A Figura 2 mostra os países com mais incidentes de máquinas realizando atividades maliciosas em nossos Honeypots.

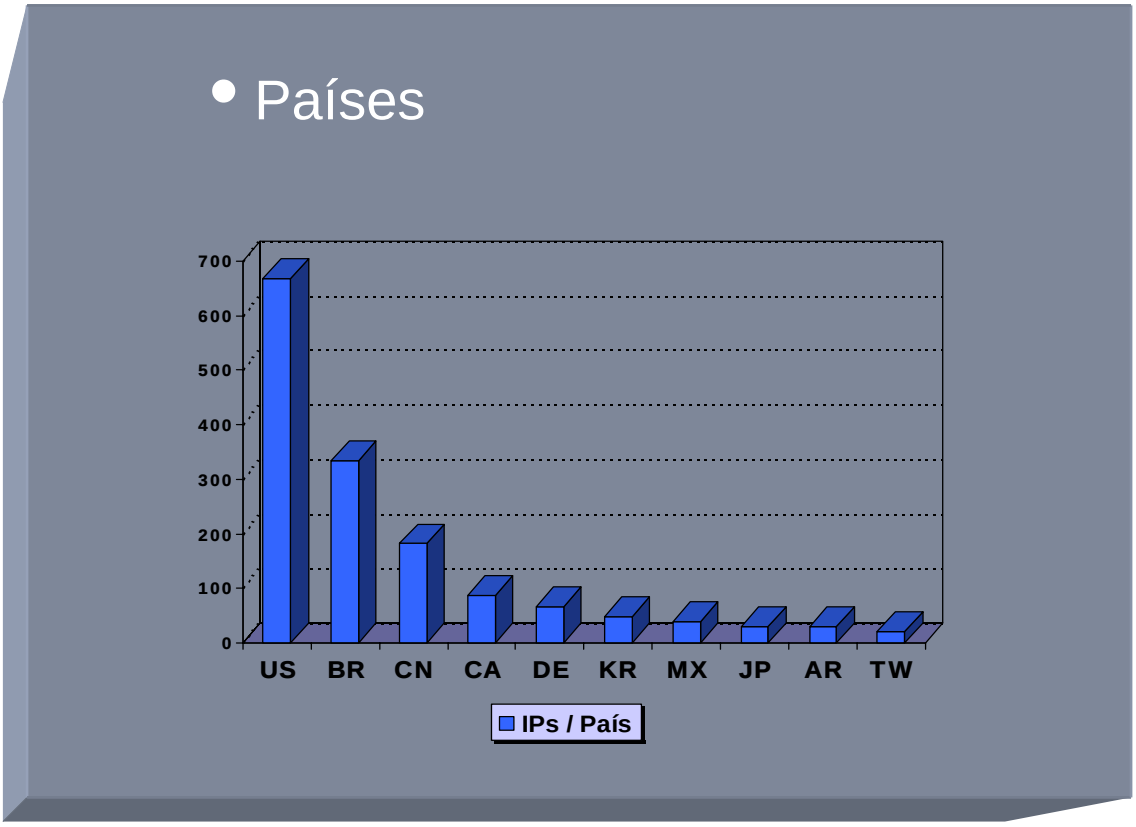

Figura 2 – Quantidade de hosts por países que mais atacam os Honeypots

A Figura 3 mostra a incidência dos ataques em relação aos sistemas operacionais.

Figura 3 – Hosts atacantes por Sistema operacional

A Figura 4 mostra as portas TCP mais atacadas nos nossos Honeypots. Cabe lembrar que a incidência em determinada porta retrata uma vulnerabilidade em evidência de determinado serviço.

A porta TCP 4899 é para o serviço de "*Remote Administrator*" para Windows, Windows 9x/ME/NT4.0/2000/XP/2003; Por padrão esse serviço não pede usuário, apenas senha, e o atacante pode ficar buscando acesso através de senhas fracas.

A porta TCP 135 é Microsoft Remote Procedure call, também usado pelo SMB (Server Message Block) para compartilhamento de arquivos e impressoras;

- Problemas comuns: usuário e senha sem criptografia, permissões erradas
- Em 2003 – worm MS.Blaster, com possibilidade de execução de código arbitrário através de Buffer Overrun. A Figura 4.1 mostra a evolução desse Worm no ano de 2004.
- Em 2004 – worm Welchia
- Em 2005 - Gaobot.gen, SpyBot, Poxdar, Mytob.AR@mm

TODOS exploravam a vulnerabilidade MS03-26

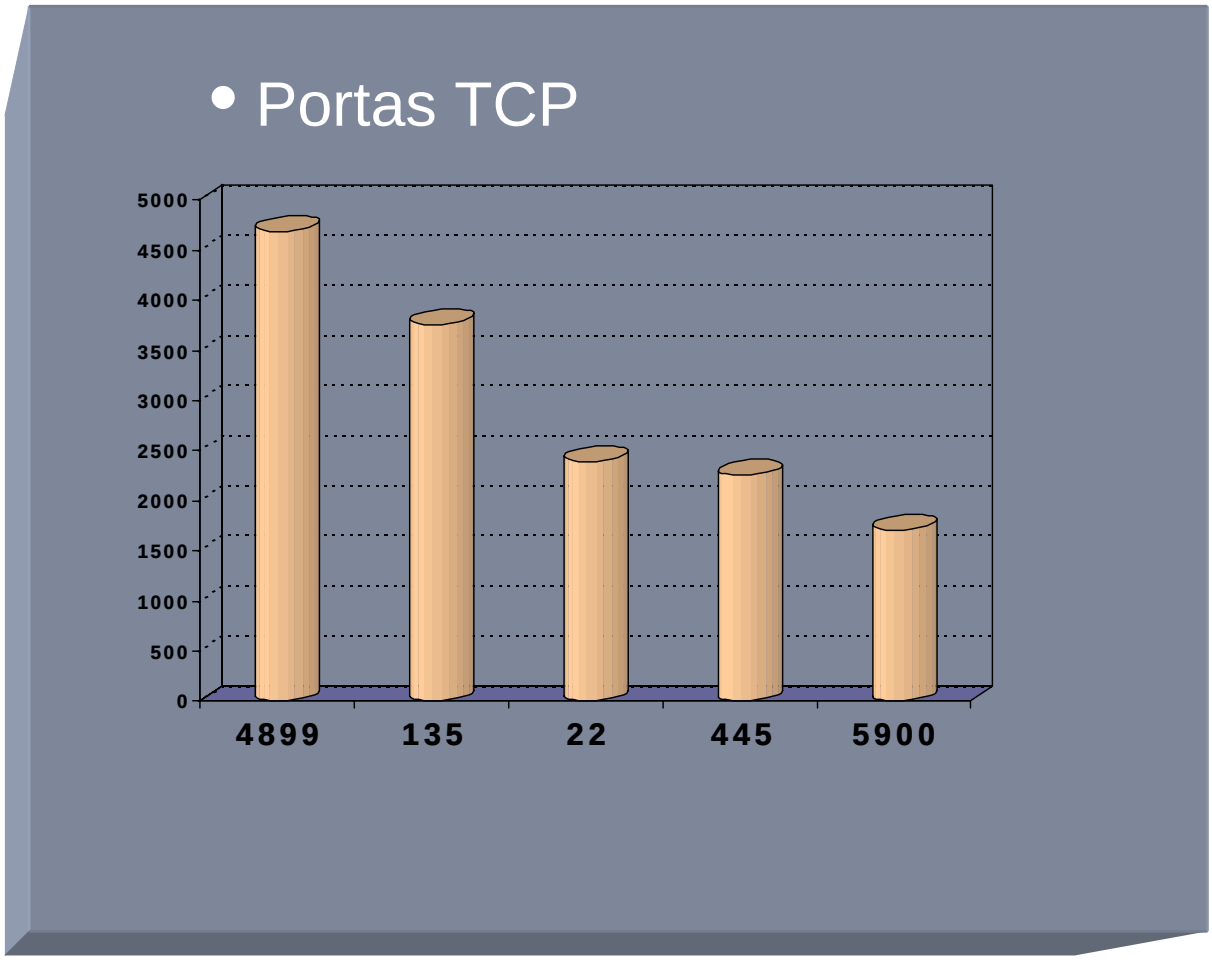

Figura 4 – Portas TCP mais atacadas

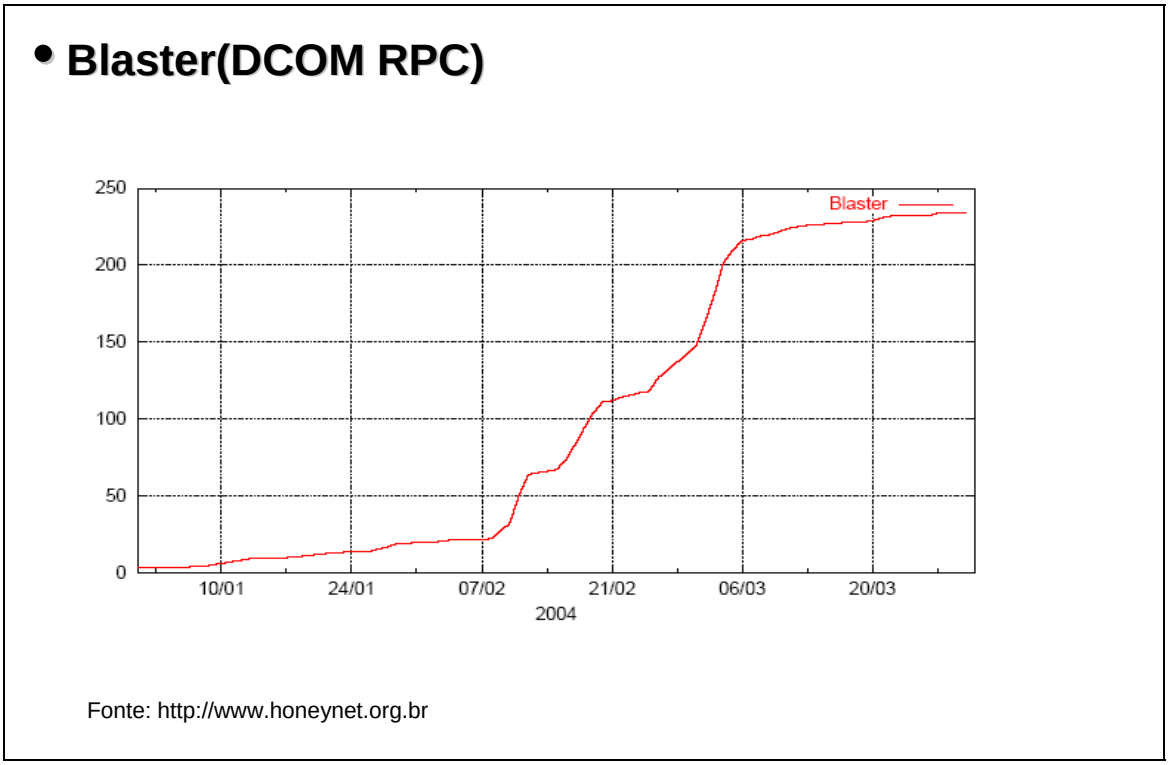

Figura 4.1 – Crescimento do Worm Blaster nos meses de jan a mar/2004

A Figura 5 mostra as portas UDP com maior incidência de ataque.

A porta UDP 53 é o serviço de DNS - Domain Name Service
- Vulnerabilidades no Bind(servidor de DNS):

- Bind 9 – FreeBSD 5.3 (CAN-2005-0034)

Queda do daemon named pelo envio de um pacote com conteúdo específico.

- Bind 8.4.4 e 8.4.5 – (CAN-2005-0033)

Inoperabilidade do daemon através de overflow em determinada consulta.

- Bind 4 e 8 – (CAN-2002-1219)

Múltiplas vulnerabilidades que possibilitam ao atacante executar código com privilégio do uid do named: tipicamente root

A porta UDP 1026 é utilizada pelo Serviço Mensageiro do Windows – Windows Messenger; É um serviço destinado ao envio de simples mensagens para um ou mais usuários em uma LAN.
Tipicamente, o tráfego destinado a essa porta é proveniente de spam para o Mensageiro do Windows.

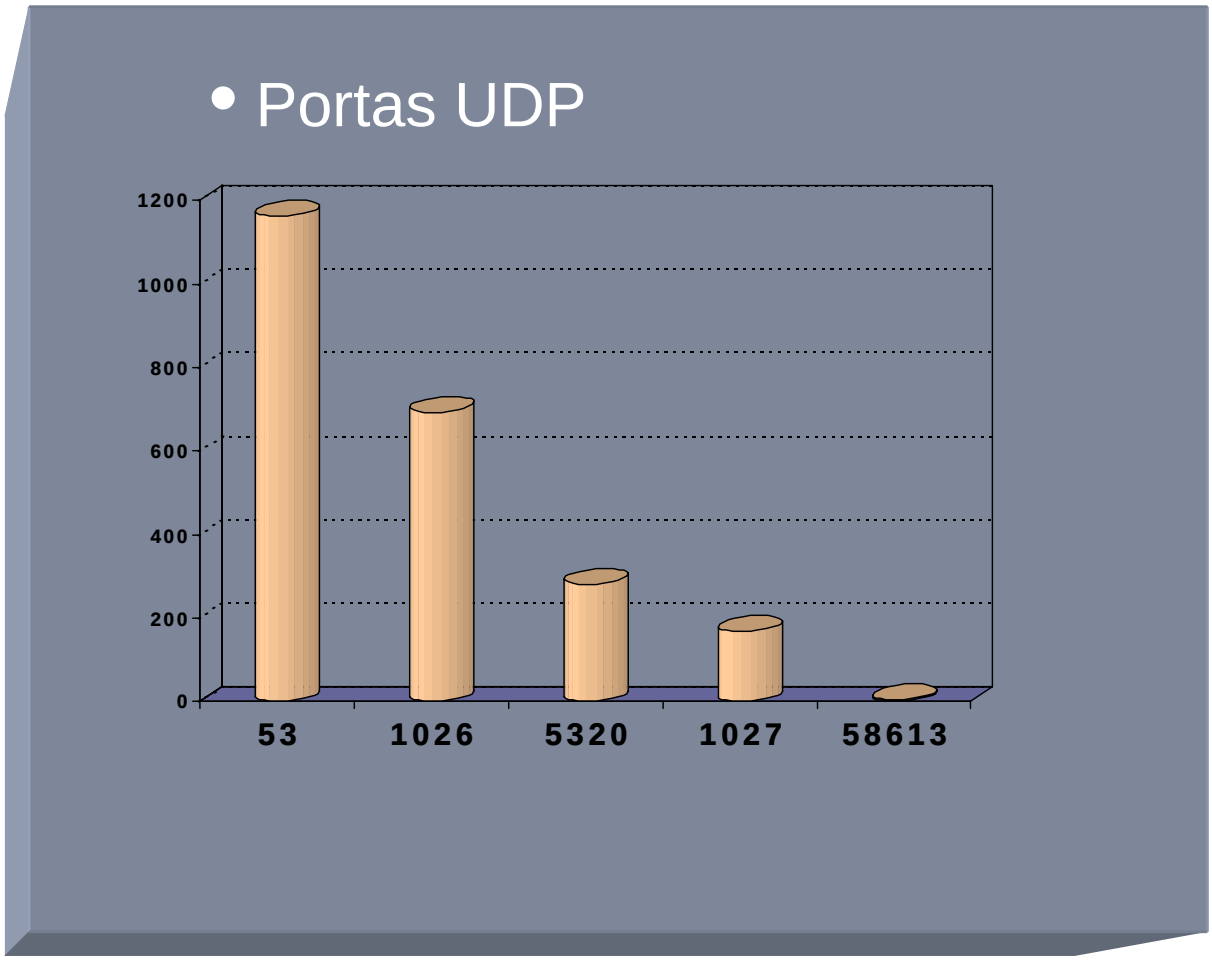

Figura 5 – portas UDP com maior incidência de pacotes

6. Conclusão:

O Consórcio Brasileiro de Honeypots é uma ferramenta para a monitoração do estado da segurança na Internet brasileira.

Ele proporciona a descoberta de atividades maliciosas antes de elas serem anunciadas e/ou publicadas.

Como exemplo, citamos o problema com a porta 5000, no dia 17/05/2004 que foi uma varredura em massa, procurando máquinas atacadas através de uma vulnerabilidade no windows XP(MS04-011). O exploit chamava-se LSASS. Com o início da atividade nos Honeypots pode-se evitar que a atividade tomasse proporções gigantescas na Internet brasileira.

Os participantes do Consórcio tem a facilidade de corrigirem seus sistemas rapidamente, pois a identificação de máquinas contaminadas e/ou vulneráveis em sua rede é descoberta logo no início devido a tendência dos worms em varrer as redes vizinhas.

Diversos trabalhos a nível de pós-graduação estão sendo feitos com o estudo de HoneyPots, além de teses de mestrado e doutorado.

7. Referências:

[1] http://project.honeynet.org/alliance/

[2] http://www.honeynet.org.br/

[3] http://www.honeypots-alliance.org.br/

[4] http://www.cert.br/