
Honeynet.BR

Desenvolvimento e Implantação de um Sistema para Avaliação de Atividades Hostis na Internet Brasileira

Honeynet.BR Team

<http://www.lac.inpe.br/security/honeynet/>

honeynt-team@lac.inpe.br

Instituto Nacional de Pesquisas Espaciais – INPE

NIC BR Security Office – NBSO/CG-I.br

Roteiro

- Histórico e Conceitos
- O Projeto HoneyNet.BR
 - Topologia
 - Contenção e Captura de Tráfego
 - Geração de Alertas e Sumários
- Resultados e Conclusões

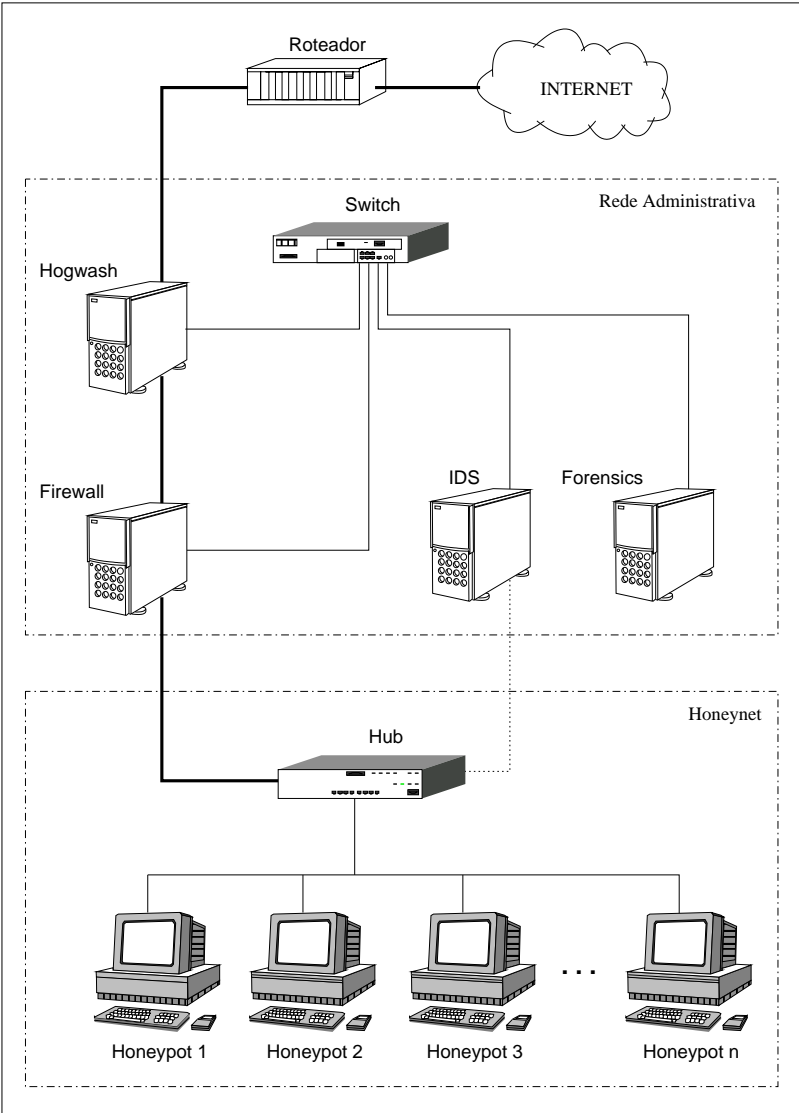
Histórico e Conceitos

- 1988: “*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*

O Projeto Honeynet.BR

- Acompanhamento de atividades hostis na Internet BR
- Desenvolvimento de ferramentas próprias
- Dezembro/2001: fase de projeto
- Março/2002: entrada em operação
- Junho/2002: ingresso na *Honeynet Research Alliance*

Topologia



Contenção de Tráfego de Saída

- Regras de saída do *Firewall*
 - *Egress filtering*
 - Serviços vulneráveis / não usuais
- Normalização do tráfego
- Bloqueio por conteúdo
- Limitação de banda
- Alteração dinâmica de regras de filtragem
 - `sessionlimit`

Captura de Tráfego

- *Firewall*
 - Mecanismo de *logging* do pf
- IDS
 - Interface sem endereço IP
- Formato `tcpdump`
- Rotação e compressão periódica

Geração de Alertas

- Tráfego de saída
 - Indica uma máquina comprometida
- Comandos de *shell*
 - *shell* modificada envia *logs* para outra máquina
- Sensibilidade é configurável
- Alertas podem ser enviados por *email*, *pager* ou celular

Sumários

- Gerados diariamente
- Estatísticas
 - Total de pacotes capturados
 - Percentual por protocolo
 - *Hosts* e portas que mais receberam e geraram tráfego, etc
- Alertas de `snort`
- Tráfego de entrada

Resultados

- Invasões
 - Vulnerabilidades mais exploradas
 - * wu-ftpd
 - * OpenSSH
 - * SSL/Apache
 - Conversação entre os invasores (IRC)
- DoS
 - UDP, ICMP fragmentado
 - Distribuído e controlado via IRC (`kaiten`)

Resultados (cont.)

- *Worms*
 - Nimda, Code Red, etc
 - MS SQL *Worm*
 - SSL/Apache *Worm* (slapper e variantes)
- SPAM
 - Procura por *open proxies* e *relay* aberto
 - “*pop-up*” SPAM (135/UDP)

Resultados (cont.)

- Análise de ferramentas capturadas
 - Novas assinaturas para o `chkrootkit`
- “*Know Your Enemy – A Profile: Romanian Blackhat Community*”
- Primeira captura do Slapper-B
 - Alerta ISS
 - “*Scan of the Month*” de novembro

Resultados (cont.)

Origem dos <i>scans</i> (IPs por país)										
1	2	3	4	5	6	7	8	9	10	Total
US	KR	BR	FR	CN	DE	TW	RO	IT	JP	
265	170	150	126	108	102	94	84	81	48	1748

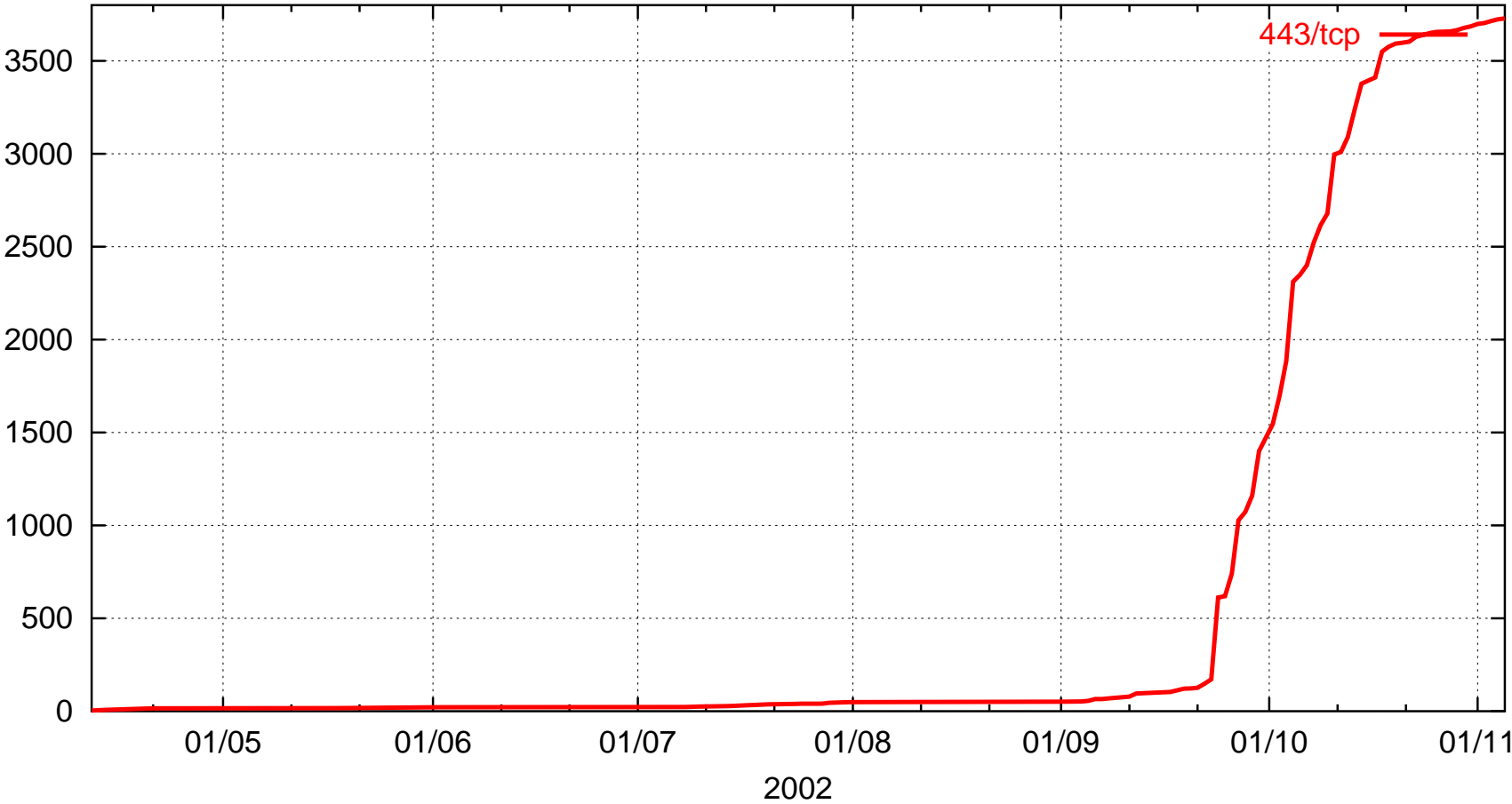
Origem dos <i>exploits</i> lançados (IPs por país)										
1	2	3	4	5	6	7	8	9	10	Total
US	KR	TW	CN	PL	JP	BR	IT	IN	CL	
38	21	17	13	9	9	8	7	4	4	167

Acesso a <i>backdoors</i> (IPs por país)										
1	2	3	4	5	6	7	8	9	10	Total
RO	TW	BR	KR	US	JP	CA	CN	PL	PE	
71	16	14	8	8	7	4	3	2	1	140

Dados de março a novembro de 2002

Resultados (cont.)

Evolução do Slapper Worm



Conclusões

- Grande ferramenta para coleta de artefatos e avaliação de atividade hostil
- Cooperação entre a comunidade de segurança é essencial
- Mudança no perfil dos atacantes
 - Uso de criptografia para acesso às máquinas comprometidas
- Necessidade de novos mecanismos de monitoração

Referências

- **Projeto HoneyNet.BR**

<http://www.lac.inpe.br/security/honeynet/>

- ***The HoneyNet Project***

<http://project.honeynet.org/>

- ***HoneyNet Research Alliance***

<http://project.honeynet.org/alliance/>

- ***Scan of the Month Challenge***

<http://project.honeynet.org/scans/>