Apresentando a NSP-Security-BR

Pedro Bueno, GCIA
Guilherme Vênere , GCFA

GTS 01.05

NSP-SEC-BR

Missão:

Esforço voluntário que tem por missão promover a interação em tempo real entre provedores de redes (NSPs) e serviços (ISPs) no combate a ataques na Internet.

NSP-SEC-BR

Origem da lista NSP-SEC

— **Lista mantida por Hank Nussbacher e composta pelos principais provedores do mundo contando hoje com 600 inscritos**

— **Combate a ataques em tempo real através da troca de informações e obrigatoriedade de resposta.**

NSP-SEC-BR

Princípios da lista NSP-SEC

- **Troca de informações sobre máquinas comprometidas, ataques de negação de serviço, botnets e novas ameaças.**
- **Compromisso de respostas em tempo real às informações postadas na lista.**
- **Rígida política de participação.**

NSP-SEC-BR

Criação da lista NSP-SEC-BR

- **Sub-lista da NSP-SEC com os mesmos ideais e políticas.**
- **Solução imediata de casos envolvendo redes brasileiras.**
- **Compromissos assumidos entre os participantes:**
  - Confidencialidade
  - Resposta imediata aos casos reportados.
  - Obrigatoriedade de resposta.
  - Participação individual.
  - Colaboração e troca de informações e experiências.

Objetivos da lista NSP-SEC-BR

- **Combate a controladores Botnets (C&C)**
- **Combate a repositórios de malware**
  - artefatos@cais.rnp.br
- **Mitigação de ataques de DDoS**
- **Contenção de sistemas infectados e origem de contaminação dentro do seu ASN**
- **Combate a ataques de phishing**
  - phishing@cais.rnp.br
- **Alertas de dispositivos e sistemas comprometidos dentro do seu ASN**

NSP-SEC-BR

Composição da lista NSP-SEC-BR

- **Jun 2005: 13 membros (6 entidades);**
- **3 moderadores:**
  - Steve Gills (membro do Team Cymru)
  - Pedro Bueno (colaborador da equipe de segurança da BrasilTelecom)
  - Guilherme Vênere (membro do CAIS/RNP)

Benefícios da lista NSP-SEC-BR

- **Resposta imediata a casos envolvendo sua rede.**
- **Mitigação de ataques contra sua rede.**
- **Identificação de sistemas comprometidos na sua rede e que são origem de atividade maliciosa.**
- **Estabelecer rede de contatos responsivos.**

Algumas estatísticas interessantes...

- Botnets detectadas pelo CAIS : 141
- Botnets reportadas ao CAIS (rede RNP): 5
- Ataques DDoS lançados contra RNP : 5
- Ataques DDoS partindo da RNP : 16
- Tempo de resposta a um pedido de ajuda em DDoS:
  medio: 1 hora, menor: 14 minutos

(*) Fonte: CAIS/RNP – membro da NSP-SEC

Algumas estatísticas interessantes...

Incidentes de seguranca reportados ao CAIS (desde 01/01/2005):

TIPO	# de incidentes
Spam	10072
Virus	11970
Bots	2274
Proxy	33
Scanners	165
Defacements	3
Phishing	2

(*) estatísticas gentilmente cedidas pelo CAIS/RNP

Participação na lista NSP-SEC-BR!

2. Preencimento do formulário em:
   http://puck.nether.net/mailman/listinfo/nsp-security-br
3. Envio das Informações necessárias para se candidatar a participar da lista:
   Nome:
   E-mail:
   Fone:
   Fone (24hr):
   iNOC Phone:
   Empresa:
   ASNs responsável for:
   Descrição do Cargo:
   Internet security references (names & emails):
   PGP Key location:

nsp-security-br-owner@puck.nether.net

NSP-SEC-BR

Faça parte você também da lista NSP-SEC-BR!

- **Participe do mutirão de combate a ações maliciosas, faça a sua parte!**
- **Ajude a melhorar a imagem do Brasil**

NSP-SEC-BR:

http://puck.nether.net/mailman/listinfo/nsp-security-br

nsp-security-br-owner@puck.nether.net