Resposta a Incidentes de Segurança

NIC BR Security Office
nbso@nic.br
http://www.nic.br/nbso.html

Cristine Hoepers
cristine@nic.br
Klaus Steding-Jessen
jessen@nic.br

SSI 2000
São José dos Campos
25 de outubro de 2000

Notas:

Notas:

Resposta a Incidentes de Segurança

- Como não responder a um incidente (exemplos)
- Contactando Sites
- Fases do Processo
- Interação entre Grupos de Segurança (GS)
- Equívocos

Notas:

Exemplo 1

```
Regra "Default Block SubSeven 2.1/2.2 Trojan"
bloqueada (d1sac,27374).
Conexão TCP de entrada
Endereço, serviço local é (d1sac,27374)
Endereço, serviço remoto é
(foo15069.foobar.com.br,1906)
O nome do processo é "N/A"
```

Notas:

Exemplo 1 (cont)

```
Olá!

    O IP mencionado abaixo, não pertence à
foobar.com.br.

Atenciosamente,
Suporte Foobar
```

Notas:

Exemplo 1 (cont)

```
Caro Internauta,

Verifique se está digitando corretamente seu login
sem @foobar.com.br e a sua senha correta, e sem
nenhum espaço entre as letras.

Atenciosamente
Suporte Foobar
```

Notas:

Exemplo 1 (cont)

```
Caro Internauta

Informamos que este problemas já foi solucionado.
Por Favor, envie - nos um novo e - mail se o
problema persitir com a mensagem de erro.

Atenciosamente,
Suporte Foobar
```

Notas:

Exemplo 2

```
Aug 25 13:05:35 inode named[679]: unapproved query
from [a.b.217.131].4828 for "version.bind"

--

Date            : 2000-08-25
Time (GMT)      : 15:28:01
Attack Type     : DNS port probe
Intruder IP     : a.b.217.131
Intruder Name   : gateway.foo.net
Port            : port=53
Victim IP       : 198.144.206.5

--

2000-08-25 00:07:32 a.b.217.131 4307 198.123.1.0 53
2000-08-25 00:07:32 a.b.217.131 4308 198.123.1.1 53
```

Notas:

Exemplo 2 (cont)

```
Date: Sat, 26 Aug 2000 13:20:50 -0300

Um de nossos profissionais instalou um scanner
(pscan) no gateway de nosso sistema a nossa
revelia e sua máquina foi uma das verificadas.
Esta ação foi descoberta logo depois pelo
responsável de nossa rede e o profissional já
foi punido pela demissão.

Gostaria mais uma vez de nos desculpar pela
inconveniência tendo a mais completa certeza de
que fato semelhante não tornará a ocorrer.

Atenciosamente,

Diretoria Foo Development Ltda.
```

Notas:

Exemplo 2 (cont)

```
Name:    hippie.foo.net
Address:  a.b.217.136

Aug 27 06:55:19 router 92117: list 101 denied tcp
    a.b.217.136(4156) -> x.y.192.1(53), 1 packet

Aug 27 06:55:19 router 92118: list 101 denied tcp
    a.b.217.136(4157) -> x.y.192.2(53), 1 packet

Aug 27 06:56:04 router 92591: list 101 denied tcp
    a.b.217.136(4365) -> x.y.192.210(53), 1 packet

Aug 27 06:56:04 router 92592: list 101 denied tcp
    a.b.217.136(4366) -> x.y.192.211(53), 1 packet
```

Notas:

Exemplo 2 (cont)

```
Date: Tue, 29 Aug 2000 01:49:08 -0300

Prezados Senhores,

o scanner usado era na verdade parte de uma
ferramenta que esta sendo desenvolvida por nos
para a analise de top level domains a ser usada
em meu outro cargo.

O responsavel pelo problema foi um programador que
era justamente o encarregado pelo desenvolvimento
do processo de stealth mode das requisicoes syn
e udp.

A explicacao dada foi a de estar desenvolvendo uma
nova ferramenta para "spoofar" pacotes "conection
oriented" como o TCP, porisso testa-lo na porta 53.

Atenciosamente,
Fulano
Diretor de Tecnologia Foo Development LTDA
```

Notas:

Exemplo 3

```
Date: Wed, 13 Sep 2000 11:45:12 -0300 (GMT+3)
From: Operacao-FoobazNet <operacao@foobaz.com.br>
To: Klaus Steding-Jessen <jessen@nic.br>
Cc: "Trower, Kris" <trower@more.net>, nbso@nic.br
Subject: Re: MOREnet Security Event 01-02252

    Estavamos no meio de uma reunião durante essa
    hora.

    Com certeza, é spoof.

    Ou um portscan sensível demais.

    done, Ciclano, Ciclano@foobaz.com.br.
```

Notas:

Exemplo 4

```
From: "denuncia@barbaz.com.br"
       <denuncia@barbaz.com.br>
To: jessen@nic.br
Subject: Re:Re: Spam Abuse From www.gata.tsx.org
Date: Thu, 20 Apr 2000 16:01:13 -0300 (BRT)


Dear Klaus,

Thank's for your message about a BO attack.  Our
company will verify this case in high priority! You
can read our policy on
http://www.barbaz.com.br/foo.htm

Beltrano
Customer Electronic Service BARBAZ-Brasil
```

Notas:

Exemplo 4 (cont)

```
From: "denuncia@barbaz.com.br"
       <denuncia@barbaz.com.br>
To: jessen@nic.br
Subject: Re: Abuse!  Suspicious Activity!!!
Date: Sat, 27 May 2000 10:52:39 -0300 (BRT)

Dear User,

Thank's for your message about a SPAM message.  Our
company will verify this case in high priority! You
can read our policy on
http://www.barbaz.com.br/foo.htm

Sincerely,

Fulano
BARBAZ Customer Service
```

Notas:

Exemplo 4 (cont)

```
From: Ciclano@barbaz.com.br
To: jessen@nic.br
Subject: Re: Hacker Report
Date: Mon, 24 Jul 2000 09:19:10 -0300 (BRT)


Por ocasiao do meu casamento, estarei fora ate dia
30/07.
Atenciosamente,
Ciclano
```

Notas:

Exemplo 4 (cont)

```
From: "denuncia@barbaz.com.br"
       <denuncia@barbaz.com.br>
To: jessen@nic.br
Subject: Re:Re: PLEASE TAKE OF THIS HACKER HERE
Date: Tue, 15 Aug 2000 17:59:42 -0300 (BRT)


Dear Webmaster,

Thank's for your message about a BO attack and
Spam.  Our company will verify this case in
high priority!  You can read our policy on
http://www.barbaz.com.br/foo.htm

Best regards,

Beltrano
Customer Electronic Service - BARBAZ Brasil
```

Notas:

Exemplo 5

```
To: nbso@nic.br
From: Mail Administrator <postmaster@foobar.com.br>
Subject: Message rejected by mailing list -
         postmaster@foobar.com.br
Date: Sat, 1 Jul 2000 18:45:42 -0300

Your message to this group has been rejected.
```

Notas:

Exemplo 6

```
From: MDaemon@foobar.foobaz
Subject: Mailing list listing
To: nbso@nic.br


LIST command recognized

If the remainder of this message is blank then all
the lists hosted by this server are set to hide
userlist information.
```

Notas:

Contactando Sites

- Notificação de um Incidente
  - enviar email para:
    - RFC 2142 (‘`security`’, ‘`abuse`’)
    - contatos do domínio/SOA
    - GS de todas as redes envolvidas
    - NBSO
  - logs com horário e timezone

Notas:

Contactando Sites (cont)

- Resposta a um Incidente:
  - Enviar email para:
    - Todos a quem a reclamação foi enviada originalmente
    - GS de sua rede / empresa / instituição
    - NBSO
  - Informar as ações tomadas

Notas:

Fases do Processo

- Atividades Prévias
- Investigando o Incidente
  - Usuário Final
  - Servidor
- Recuperação

Notas:

Atividades Prévias

- Profissional/equipe dedicada à segurança
- Definição de políticas:
  segurança, uso aceitável, etc.
- Implementar a RFC 2142:
  '`security`', '`abuse`', '`postmaster`', etc.
- Manter contatos do domínio e SOA atualizados

Notas:

Atividades Prévias (cont)

- DNS reverso
- Sincronização de relógio via NTP
- Log host centralizado
- Manter logs por bastante tempo

Notas:

Atividades Prévias (cont)

- Cópia dos binários em CDROM/floppy
- MD5 / tripwire
- Sistema com patches/atualizado
- Manter apenas serviços imprescindíveis
- IDS / firewall

Notas:

Investigando o Incidente

- Usuário final / dialup
- Servidor

Notas:

Investigando o Incidente – Usuário Final

- Contactar o usuário
- Seguir a AUP
- Se originou invasão/crime:
  - guardar logs e dados pessoais
  - liberar os dados pessoais mediante mandado judicial
- Informar atitudes tomadas

Notas:

Investigando o Incidente – Servidor

- Não desligar ou rebootar a máquina
  - no máximo retirar da rede
- Procurar por evidências de invasão
  - rootkit (ps, netstat, ifconfig, ls, login, last, etc)
  - sniffer / bots de IRC
  - backdoor / shell suid
  - trojan de sshd / inetd / popd / fingerd / syslogd
  - módulos de kernel (LKMs)

Notas:

Investigando o Incidente – Servidor (cont)

- Procurar por logs que apontem para outras redes
  - contactar todas as redes envolvidas
  - enviar os logs relacionados
- Analisar o tráfego
- Repetir o procedimento nos outros servidores

Notas:

Recuperação

- Avaliar impacto/causas do incidente
- Reavaliar a segurança do site
- Criar estratégia de Recuperação
- Reinstalação segura
- manter:
  - logs da invasão / binários modificados

Notas:

Interação entre Grupos de Segurança

- Escopo de atuação
- União de Esforços
- Troca de informações
- Cruzamento de informações
- Descobertas de novos métodos

Notas:

Equívocos

- "Se acontecer alguma coisa é só baixar o backup."
  - imagem da empresa/instituição
  - backup comprometido
- "Tenho uma consultoria que olha 'periodicamente' o site."
  - é necessário conhecer o tráfego de sua rede
  - analisar diariamente os logs

Notas:

Equívocos (cont)

- "Conversei com ele, era apenas um garoto."
  - não houve arrependimento
  - site totalmente apagado
- "Ele invadiu o meu site e agora é o responsável pela segurança."
  - ocultam atividades de hacking
  - utilizam scripts / exploits prontos
  - poucos conhecimentos técnicos
  - ética

Notas:

Equívocos (cont)

```
From: "Script Kiddie" <kiddie@hotmail.com>
To: webmaster@<dominio>
Subject: HACKERS e o seu site
Date: Tue, 05 Sep 2000 03:45:11 GMT

Atencao, o server no qual o host
http://www.<dominio> esta hospedado esta vulneravel
a ataques de hackers (inclusive o grupo no qual
faço parte "m3u GrUp0 d3 H4cK1nG", alterou a
sua HP a pouco tempo).

Sou cosultor de segurança e espero que tomem
providencias.

Para maiores informaçoes, favor contatar:
"Script Kiddie" (KIDDIE) <kiddie@hotmail.com>
```

Notas:

Equívocos (cont)

```
From: "Script Kiddie" <kiddie@hotmail.com>
To: info@<dominio>
Subject: INVASAO ao site www.<dominio>
Date: Sat, 16 Sep 2000 05:56:01 GMT

O site possui varios erros de configuracao, os
erros estao sendo explorados por hackers do
grupo m3u GrUp0 d3 H4cK1nG (grupo no qual
pertenco).

Sou consultor de seguranca, autor da "Coluna
Lammer", membro do m3u GrUp0 d3 H4cK1nG, entre
outros.

Caso estejam interessados em corrigir os furos,
favor entrar em contato. Caso nao respondam esse
mail, irei alterar o site novamente (para
demonstrar as vulnerabilidades).

Abracos ...
"Script Kiddie" (KIDDIE)
<kiddie@hotmail.com> - m3u GrUp0 d3 H4cK1nG Team
```

Notas:

URLs de Interesse

- NIC BR Security Office
  http://www.nic.br/nbso.html
- Sites de referência
  http://www.nic.br/links.html

Notas: