Ataques Mais Comuns na Internet BR
Recomendações para Prevenção, Tratamento e Recuperação de Incidentes

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

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

Fórum de Segurança da BRISA
Brasília–DF
13 de abril de 2000

Ataques Mais Comuns na Internet BR
Recomendações para Prevenção, Tratamento e Recuperação de Incidentes

- Tratamento de Incidentes
- Legislação
- Vulnerabilidades / Estatísticas
- Deficiências mais comuns nos casos acompanhados
- Recomendações

NBSO—NIC BR Security Office

- Criado em junho de 1997
- Coordenado pelo GTS–CG
- Coordena as ações e provê informações para sites envolvidos em incidentes
- Não tem poder regulatório

NBSO—Forma de Operação

- Recebe notificações de incidentes de segurança
- Encaminha essas notificações para os responsáveis das redes envolvidas
- Correlaciona dados
- Mantém estatísticas sobre os incidentes reportados
- Se necessário, ajuda no site (dependendo da gravidade)

Como Proceder num Incidente

- denunciar scans / abusos
- incluir logs completos (timestamps, IP, etc)
- contactar
  - responsáveis pelo domínio / backbone
  - NBSO <nbso@nic.br>

Como Proceder numa Invasão

- não reinstalar de imediato a máquina
- preservar evidências
  - Não remover nenhum arquivo
  - fazer backup completo
- Verificar a integridade das demais máquinas

Como Proceder numa Invasão (cont)

- analisar as atividades suspeitas na máquina
  - analisar todas as conexões não autorizadas
  - arquivos inseridos ou modificados pelo invasor
  - backdoors / processos
  - contas criadas / utilizadas
- reinstalação segura
  - corrigir as vulnerabilidades detectadas durante a análise

Aspectos Legais

Legislação:

- Não há lei específica
  - Projeto de Lei 84, de 1999
  - Anteprojeto de Lei sobre armazenamento de logs
- Crimes previstos nas leis vigentes
  - Escuta telemática (sniffing)
  - Dano

Aspectos Legais (cont)

Evidências Válidas:

- Sniffers instalados
- Alterações no sistema (arquivos, processos, etc)
- Logs
- Análise do tráfego do invasor

Incidentes Reportados ao NBSO—1999

Mês	Usuário	DoS	Invasão	Web	Scan	Total
jan	5	7	14	22	67	204
fev	5	1	6	31	54	172
mar	7	5	12	19	60	203
abr	8	0	2	0	81	151
mai	10	1	7	2	57	145
jun	17	2	9	8	79	192
jul	26	0	10	14	110	208
ago	167	0	35	8	100	385
set	85	1	3	4	74	264
out	34	1	7	7	134	269
nov	148	1	14	18	182	418
dez	146	2	9	50	270	496
Total	658	21	128	183	1268	**3107**

Incidentes Reportados ao NBSO—2000 (janeiro a março)

Mês	Usuário	DoS	Invasão	Web	Scan	Total
jan	108	11	3	57	217	424
fev	78	8	11	80	270	509
mar	117	14	8	38	309	541
Total	303	33	22	175	796	**1474**

SPAM / Open Relay

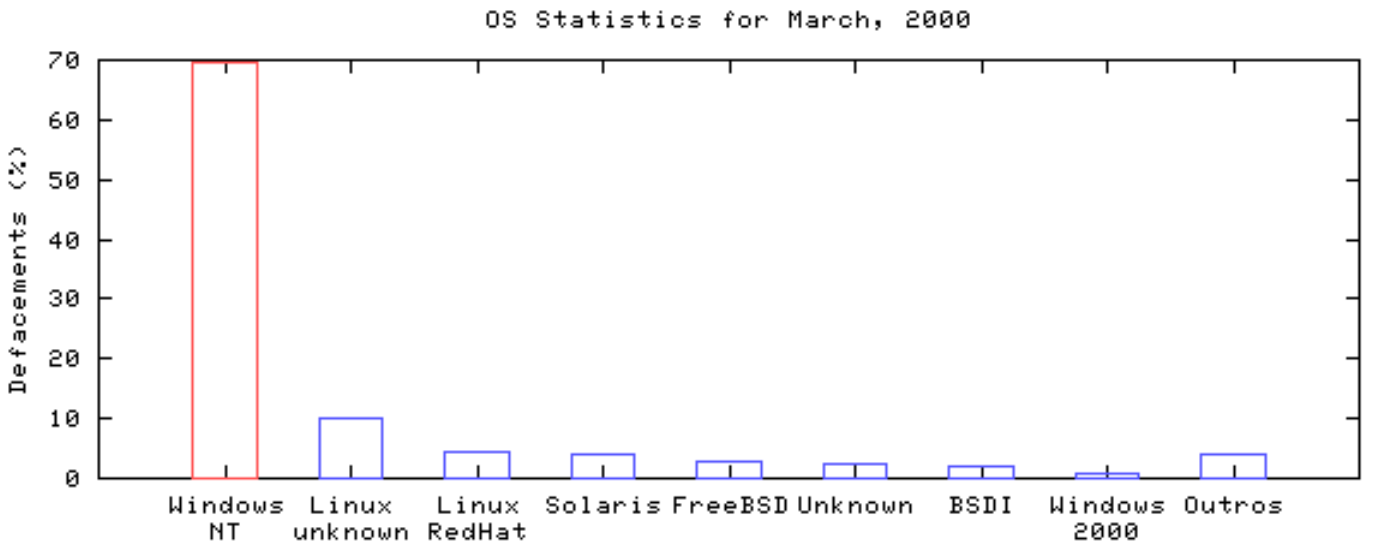
- Mail servers brasileiros com relay aberto

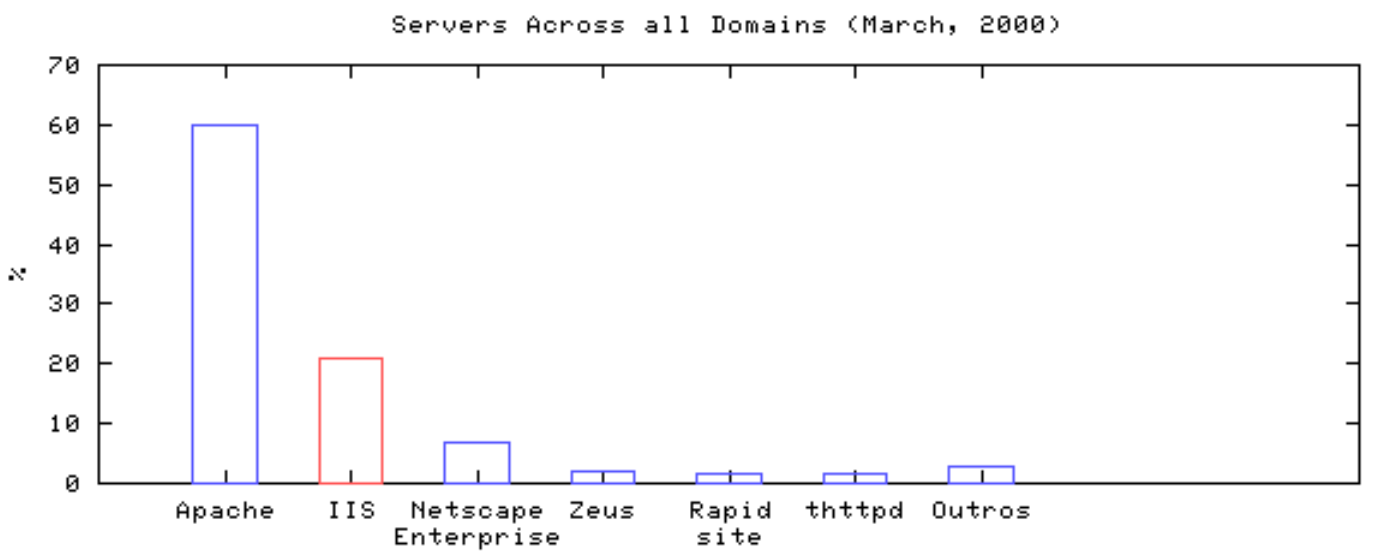
- Aprox. 15 reclamações de SPAM por dia
  (1100 nos primeiros 75 dias do ano)

- ORBS–Open Relay Behaviour-modification System
  - servidores com relay aberto: (bloco 200.128/9)
    * 878 em fevereiro/2000
    * 1019 em março/2000
    * 1329 em abril/2000

Vulnerabilidades mais Exploradas

- bind
- RPC (rpc.cmsd, rpc.statd, rpc.ttdbserverd)
- mountd
- amd
- IIS (FP extensions, RDS, ColdFusion, ODBC, etc)


OS Statistics for March, 2000
Defacements (%)
70
60
50
40
30
20
10
0
Windows NT
Linux unknown
Linux RedHat
Solaris
FreeBSD
Unknown
BSDI
Windows 2000
Outros


Servers Across all Domains (March, 2000)
%
70
60
50
40
30
20
10
0
Apache
IIS
Netscape Enterprise
Zeus
Rapid site
thttpd
Outros

DoS e DDoS

- floods (UDP, ICMP, SYN)
  - Amplificação de Broadcast (smurf)

- DDoS
  - Muitos sites na Internet hoje com baixa segurança
  - Mito: "Não tem nada de interessante em minha máquina para que alguém queira invadir"
  - egress filtering
  - cooperação do backbone
  - IPv6

DDoS—Efeito Colateral

```
03:22:28.868347 200.a.b.c.2608 > 134.50.37.238.59953: R 0:0(0) \
ack 1502205949 win 0

03:24:04.412266 200.a.b.c.2028 > 134.50.51.47.30686: R 0:0(0) \
ack 1179804064 win 0

03:24:45.190540 200.a.b.c.2813 > 134.50.83.181.54266: R 0:0(0) \
ack 1346973591 win 0

[...]

06:54:26.026078 200.a.b.c.2028 > 134.50.51.47.47070: R 0:0(0) \
ack 4287514625 win 0

06:56:21.250344 200.a.b.c.2813 > 134.50.83.53.23290: R 0:0(0) \
ack 1060973975 win 0

06:56:54.911255 200.a.b.c.2028 > 134.50.51.47.63454: R 0:0(0) \
ack 4276335617 win 0
```

Evidências Mais Comuns Após Uma Invasão

- rootkit (ps, netstat, ifconfig, ls, login, last, etc)
- sniffer
- backdoor / shell suid
- trojan de sshd / inetd / popd / fingerd / syslogd
- bots de IRC

Deficiências Graves nos Casos Acompanhados

- Uso de protocolos como pop, ftp, telnet, rlogin
  - Resistência à troca
- Ausência de sistema de log (syslogd)
- Análise de logs inexistente / ineficiente
- Falta de NTP

Deficiências Graves nos Casos Acompanhados (cont)

- Serviços desnecessários ou desconhecidos pelo administrador
- Tripwire com base de dados na própria máquina
- Falta de reclamações de ataques
- tcpwrappers como única forma de proteção
- Filtragem de pacotes inexistente / ineficiente

Equívocos

- “Estou usando criptografia nas conexões, isso é suficiente.”
  - senhas / dados guardados em clear text
  - SO com vulnerabilidades
- “Se acontecer alguma coisa é só baixar o backup.”
  - imagem da empresa
  - backup comprometido

Equívocos (cont)

- "Tenho uma consultoria que olha 'periodicamente' o site."
  - é necessário conhecer o tráfego de sua rede
  - analisar diariamente os logs
- "Conversei com ele, era apenas um garoto."
  - não houve arrependimento
  - site totalmente apagado

Equívocos (cont)

- "Conversei com o hacker, ele me ajudou a fazer a segurança do site. Agora está tudo bem."
  - mais backdoors instalados
  - nenhum log gerado

- "Ele invadiu o meu site e então eu o contratei para fazer a segurança."
  - utilizam scripts / exploits prontos
  - poucos conhecimentos técnicos
  - ética

Recomendações

- profissional dedicado à área de segurança
- aplicação de patches / atualização do sistema
- manter apenas serviços imprescindíveis
- filtragem de pacotes
- IDS
- log host centralizado

Recomendações (cont)

- uso de ssh, S/KEY
- pgp
- sincronização de relógio via NTP
- md5 / tripwire
- denunciar scans e tentativas de invasão
  Mito: "se eu reclamar muito vão achar que minha rede tem problemas" (ex: SPAWAR)

Recomendações (cont)

- manter logs por bastante tempo
- análise constante do tráfego da rede
- Adotar práticas anti-SPAM (fechar relay, etc)
- Implementar a RFC 2142: "Mailbox Names for Common Services, Roles and Functions"
  (aliases '`security`', '`abuse`', '`postmaster`', etc)
- Definição de Políticas (Segurança, Uso Aceitável, etc.)

URLs de Interesse

- COAST Hotlist: Computer Security, Law and Privacy
  `http://www.cerias.purdue.edu/coast/hotlist/`

- Global Incident Analysis Center
  `http://www.sans.org/giac.htm`

- Consensus Roadmap for Defeating Distributed Denial of Service Attacks
  `http://www.sans.org/ddos_roadmap.htm`

- Denial of Service (DoS) Attack Resources
  `http://www.denialinfo.com/`

- What is Egress Filtering and How Can I Implement It?
  `http://www.sans.org/infosecFAQ/egress.htm`

URLs de Interesse (cont)

- Counterpane Internet Security—Crypto Links
  `http://www.counterpane.com/hotlist.html`

- SecurityFocus
  `http://www.securityfocus.com`

- The Security Search Engine
  `http://www.securitysearch.net/`

- ATTRITION Mirrored Sites
  `http://www.attrition.org/mirror/attrition/`
  `http://www.attrition.org/mirror/attrition/stats.html`

- Technotronic Security Information
  `http://www.technotronic.com/`

URLs de Interesse (cont)

- Anti-Spam Recommendations for SMTP MTAs
  `ftp://ftp.unicamp.br/pub/RFC/rfc2505.txt.gz`

- Mailbox Names for Common Services, Roles and Functions
  `ftp://ftp.unicamp.br/pub/RFC/rfc2142.txt.gz`

- The Mail Abuse Prevention System
  `http://maps.vix.com`

- ORBS–Open Relay Behaviour-modification System
  `http://www.orbs.org`

URLs de Interesse (cont)

- The Network Abuse Clearinghouse
  `http://www.abuse.net`

- CAUCE, The Coalition Against Unsolicited Commercial Email
  `http://www.cauce.org`