Perfil dos Ataques Atuais na Internet BR e Recomendações para o Aumento da Segurança de Sistemas Conectados à Internet

NIC BR Security Office

<nbso@nic.br>

http://www.nic.br/nbso.html

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

Brasília–DF
14 de abril de 2000

Perfil dos Ataques Atuais na Internet BR e Recomendações para o Aumento da Segurança de Sistemas Conectados à Internet

- Apresentações: CG, GTS, NBSO
- Forma de operação
- Tratamento de Incidentes
- Tipos de Ataque
- Vulnerabilidades / Estatísticas

Perfil dos Ataques Atuais na Internet BR e Recomendações para o Aumento da Segurança de Sistemas Conectados à Internet

- Invasões Acompanhadas
- Deficiências mais comuns nos casos acompanhados
- Criptografia
- Recomendações
- Referências

Comitê Gestor—CG

Criado por portaria interministerial MCT/MC 147, de 31 de maio de 1995.

- Recomendar padrões e ética de uso para a Internet no Brasil

- Atribuição de IPs e registro de domínio

CG—Estrutura

- Membros

- Grupos de Trabalho
  - GTS
  - GTER
  - GTRH

GTS

- Assessora o CG. Subgrupos:
  - SGTS-Backbones
  - SGTS-Provedores
- Desenvolve ferramentas, documentos e padrões organizacionais relacionados com a segurança da Internet/Br
- Recomendações para o Desenvolvimento e Operação da Internet/Br
  `http://www.cg.org.br/acoes/desenvolvimento.htm`

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/encaminha notificações de incidentes de segurança
  - denúncias de scans e abusos
  - logs completos (timestamps, IP, etc)
- Contatos
  - responsáveis pelo domínio / backbone
  - NBSO <nbso@nic.br>

NBSO—Forma de Operação (cont)

- Correlaciona dados
- Mantém estatísticas sobre os incidentes reportados
- Apoio Técnico

Tipos de Ataque

- Ataque a usuário final
- Denial of Service (DoS)
- Ataque a Servidor Web
- Scan
- Invasão

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**

Domínios que mais Reportam Incidentes

#	Exterior		Brasil	
	num	domínio	num	domínio
1	79	nasa.gov	1037	registro.br
2	37	llnl.gov	719	prodam.sp.gov.br
3	35	home.com	469	unicamp.br
4	31	ornl.gov	79	unitau.br
5	23	navy.mil	59	visanet.com.br
6	22	renater.fr	58	ufsc.br
7	20	fdic.gov	58	microlink.com.br
8	20	stanford.edu	55	brasilseg.com.br
9	19	chem.wisc.edu	41	nic.br
10	13	hotmail.com	29	netbank.com.br

Como Proceder numa Invasão

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

Como Proceder numa Invasão (cont)

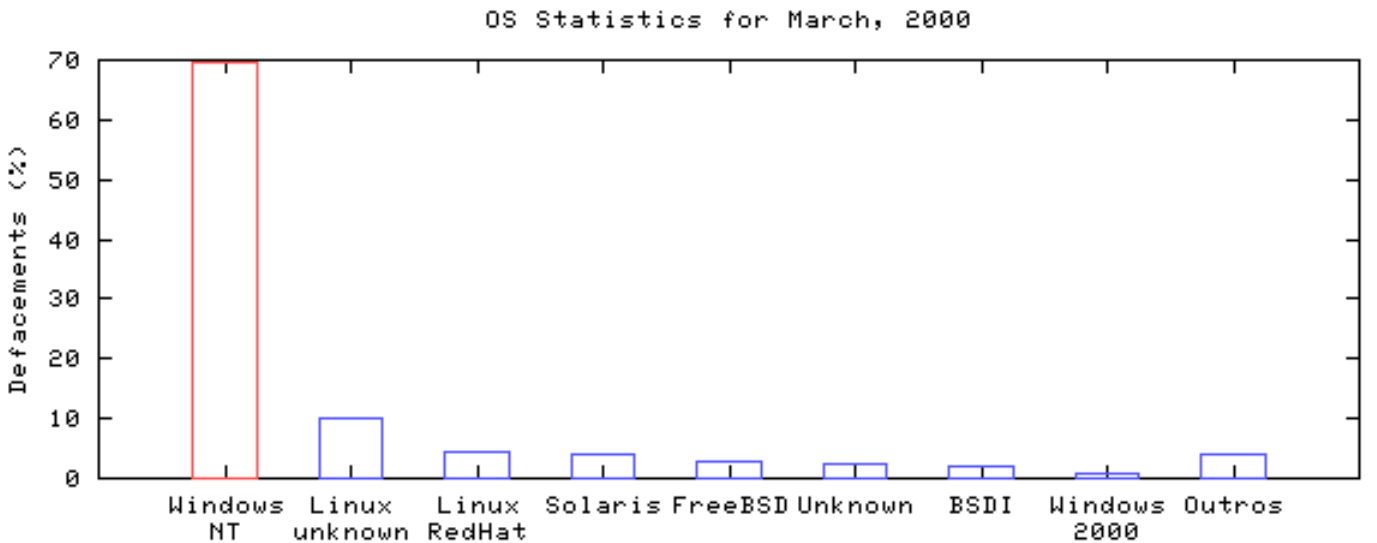
- analisar as atividades suspeitas na máquina
  - analisar todas as conexões não autorizadas
  - arquivos inseridos ou modificados pelo invasor
  - backdoors / processos
  - contas criadas / utilizadas
- reinstalação segura
  - corrigir as vulnerabilidades detectadas durante a análise

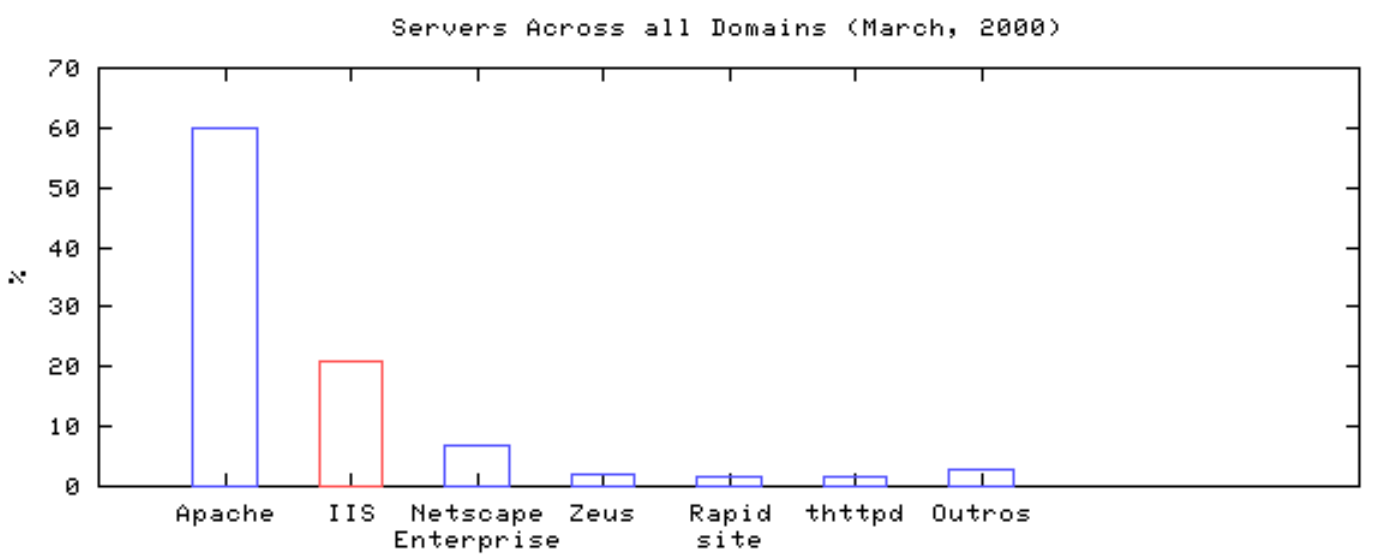
SPAM / Open Relay

- 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)

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

Vulnerabilidades mais Exploradas (cont)

ftp://ftp.technotronic.com/unix/

```
[DIR] Parent Directory
[DIR] aix-exploits . . . . . .  [Sep 18 08:58]
[DIR] bsd-exploits . . . . . .  [Apr 22 15:00]
[DIR] cgi-bin-exploits . . . . .  [Aug 18 18:03]
[DIR] digital-exploits . . . . .  [Apr 22 13:04]
[DIR] ftpd-exploits. . . . . .  [Sep 15 18:12]
[DIR] hp-ux-exploits . . . . . .  [Oct 14  1998]
[DIR] irix-exploits. . . . . .  [Jul  7 00:07]
[DIR] linux-exploits . . . . . .  [Oct  7 12:44]
[DIR] log-tools. . . . . .  [Jun 25 15:14]
[DIR] mail-exploits. . . . . .  [Jun 25 14:43]
[DIR] nameserver-exploits. . . .  [Aug  1 17:03]
[DIR] network-scanners . . . . .  [Oct  3 11:11]
[DIR] network-sniffers . . . . .  [Sep 22 13:45]
[DIR] packet-assembly. . . . . .  [Jul 20 18:14]
[DIR] passwd-crackers. . . . . .  [Dec  3  1998]
[DIR] sco-exploits . . . . . .  [Oct 13 08:20]
[DIR] security-tools . . . . . .  [Jul 26 08:20]
[DIR] solaris-exploits . . . . .  [Sep 28 22:50]
[DIR] sun-exploits . . . . . .  [May 24 23:24]
[DIR] tcp-exploits . . . . . .  [Apr 23 11:40]
[DIR] trojans. . . . . .  [Aug 19 10:16]
```

Casos Acompanhados—Exemplo 1

Instituição A

- obtiveram acesso privilegiado em diversas máquinas
- instalação de sniffer, capturando todos os pacotes de conexões telnet, ftp e smtp
- instalação de vários backdoors (que eram iniciados via rc)
- modificação do inetd e outros programas
- ftp dos mails da máquina para sites no exterior

Casos Acompanhados—Exemplo 2

Instituição B

- Invasores com acesso privilegiado em várias máquinas
- o telnetd foi substituído por um trojan, dando acesso privilegiado sem senha
- acessavam essas máquinas de dezenas de sites (Brasil e exterior)
- eram utilizadas como base para ataques a redes brasileiras, .gov, .com e .edu (EUA) além de outros países

Casos Acompanhados—Exemplo 2 (cont)

- contas próprias foram criadas no sistema
- registraram domínios informando as contas criadas como email de contato
- usavam as máquinas como repositório de dados e ferramentas
- registraram nomes no DNS

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
- tráfego de IRC (chat)

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
- Falta de reclamações de ataques
- 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 instituição
  - 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

Criptografia

- Algoritmos Públicos
  - Descritos na literatura
  - Analisados pela comunidade de criptografia
  - Segurança depende da chave usada
- Exportação pelos EUA
  - restrições de exportacao de criptografia forte
  - produtos aprovados podem ser quebrados pelo NSA?

Criptografia (cont)

- AES
  - algoritmo sucessor do DES
  - `http://csrc.nist.gov/encryption/aes/`
  - Finalistas: MARS, RC6, Rijndael, Serpent e Twofish
- OpenBSD (`http://www.openbsd.org`)
  - integração com criptografia
  - code auditing
  - sem restrições de exportação
  - seguro "por default"

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`