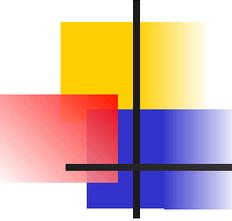


O Perfil da Segurança na Internet Através da Análise das Estatísticas do Consórcio Brasileiro de Honeypots

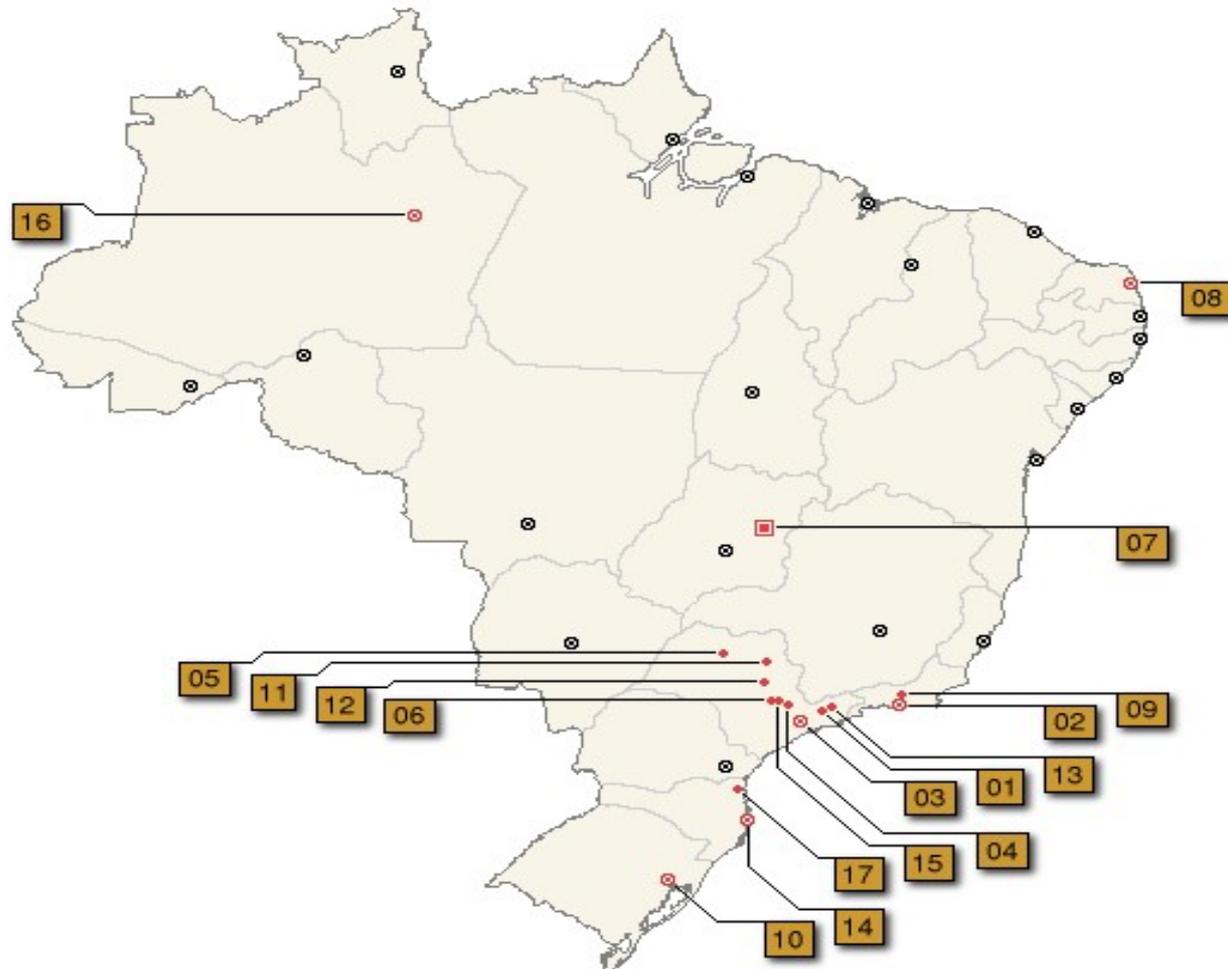
Émerson Salvadori Virti
Liane Tarouco
Leandro Márcio Bertholdo
CERT-RS/POP-RS



Roteiro

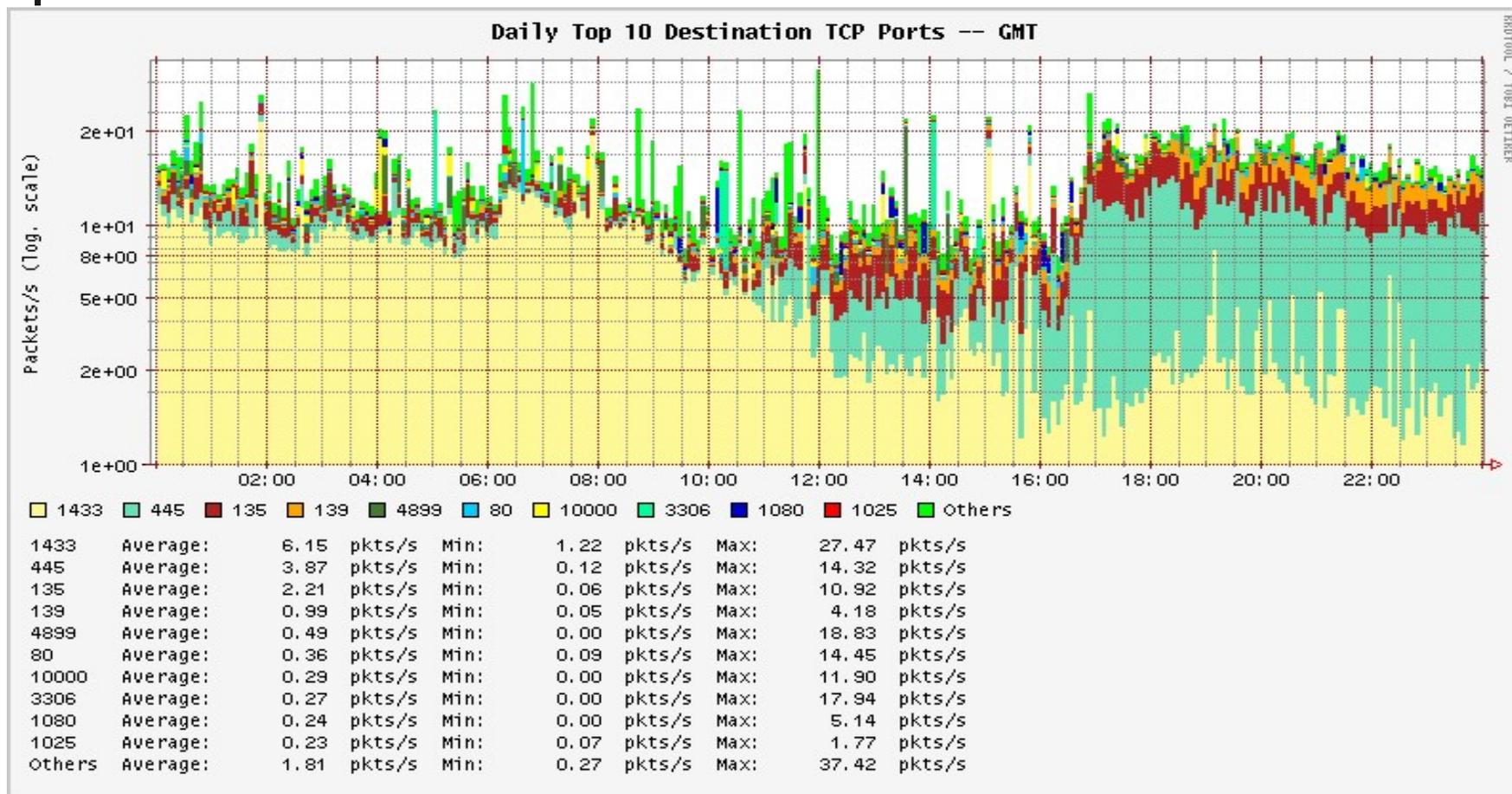
- Apresentação do Consórcio Brasileiro de Honeypots
- Comparação das estatísticas do Consórcio através da observação de outros indicadores da Internet
- Análise das principais portas UDP acessadas
- Análise das principais portas TCP acessadas
- Conclusões
- Recomendações

Consórcio Brasileiro de Honey Pots



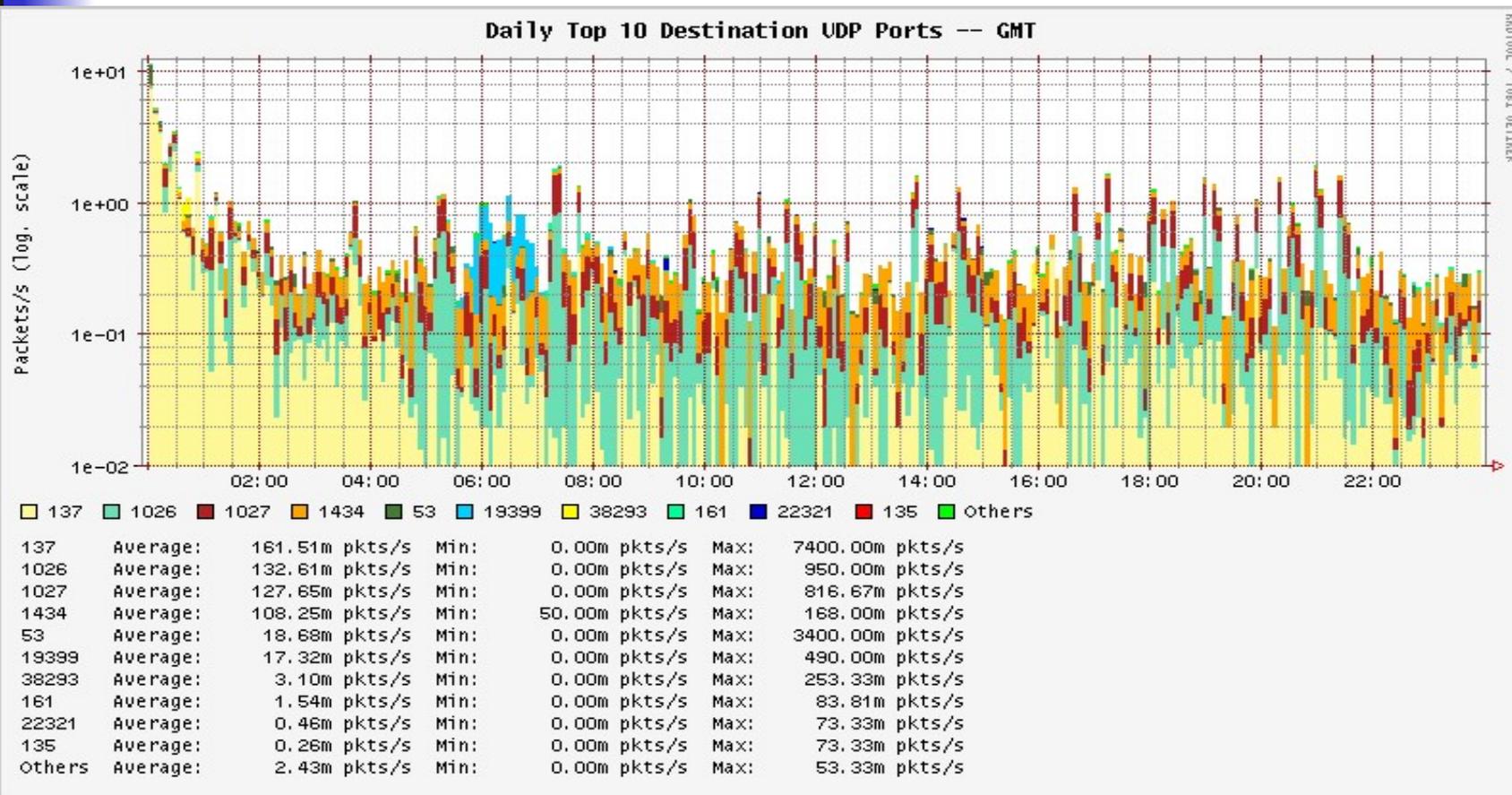
Consórcio Brasileiro de Honeypots

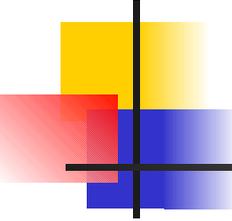
Portas TCP com Maior Número de Pacotes Trafegados



Consórcio Brasileiro de Honeydumps

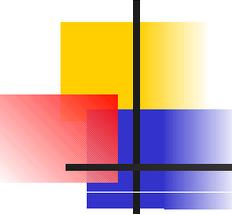
Portas UDP com Maior Número de Pacotes Trafegados





Dshield

- Distributed Intrusion Detection System
 - <http://www.dshield.org>
- Baseado no envio de logs de firewalls
- Pesquisa sobre as principais vulnerabilidades exploradas
- Fornecimentos de estatísticas em tempo real
 - Para cada porta
 - Top 10 portas

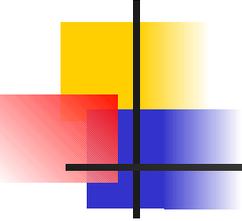


Dshield

Service Name	Port Number	Explanation
microsoft-ds	445	Win2k+ Server Message Block
epmap	135	DCE endpoint resolution
---	1026	
halflife	27015	Half-Life Game Server
netbios-ssn	139	NETBIOS Session Service
eMule	4672	eMule / eDonkey P2P Software
gnutella-svc	6346	gnutella-svc
bittorrent	6881	Bit Torrent P2P
domain	53	Domain Name Server
---	8956	

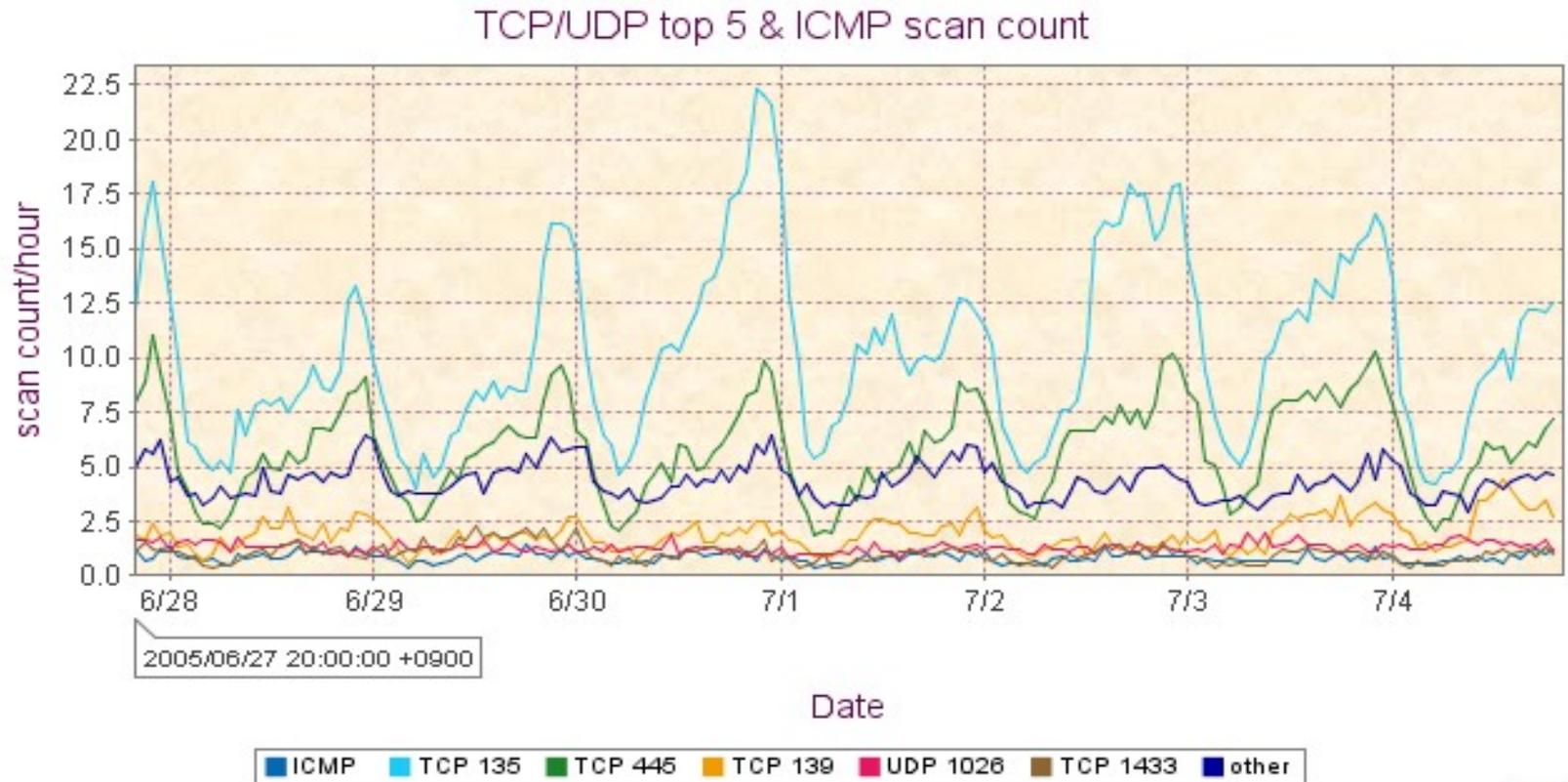
Dshield – 04/07/2005

JPCERTCC

- 
-
- Japan Computer Emergency Response Team Coordination Center
 - <http://www.jpCERT.or.jp/english>
 - Internet Scan Data Acquisition System: ISDAS – Distribuição de sensores no espaço da Internet japonesa
 - Publicação de uma lista, atualizada a cada 15 min, das top 5 portas scan

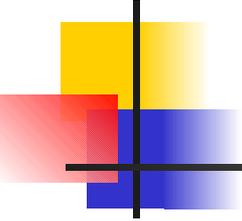
JPCERTCC

Japan Computer Emergency Response Team Coordination Center



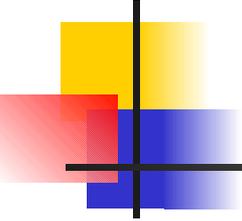
Copyright © 2003-2005 JPCERT

JPCERTCC – 04/07/2005



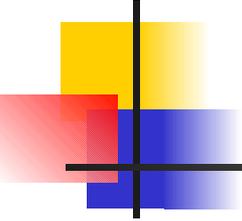
Diferenças nas Estatísticas

- Entre os integrantes do Consórcio
 - Worms geralmente fazem scans nas suas vizinhanças;
 - Diferentes espaços de endereçamento
 - Portas abertas e portas emuladas fazem aumentar o número de acessos
 - Filtros aplicados antes de chegar ao honeypot
- Entre Indicadores Mundiais
 - Diferentes espaços de endereçamento



Portas UDP com maior número de pacotes trafegados

- 137 – 28,15%
- 1026 – 23,11%
- 1027 – 18,86%
- 1434 – 3,25%
- 53 – 3,26%



Portas com maior número de pacotes trafegados

137/UDP

- Netbios Name Service – onde o Windows obtém informações referentes aos recursos oferecidos pelo host – nome do sistema, arquivos compartilhados, compartilhamento de impressoras.
- Geralmente scans para essa porta são resultado de alguns worms como o Blaster, Refaz, Alkra que exploram os arquivos compartilhados como forma de propagação.
- A seqüência "CKAA..." é utilizada para ser traduzida em um caracter "*" pelo servidor netbios-ns e verificar se existe arquivos compartilhados no ("C")

Portas com maior número de pacotes trafegados

137/UDP

pflog.0 - Ethereal

File Edit View Go Capture Analyze Statistics Help

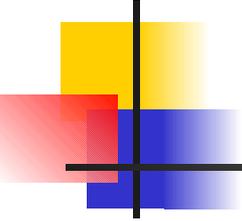
Filter: + Expression... Clear Apply

No.	Time	Protocol	Info
1793	16215.561149	2 2 NBNS	[passed x10/11] Name query NBSTAT *<00><00>

▶ User Datagram Protocol, src Port: 1048 (1048), dst Port: netbios-ns (137)

```
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0020  00 00 00 00 00 00 00 0b ff ff ff ff 01 00 00 00  .....
0030  45 00 00 4e e8 b0 00 00 7a 11 30 06 c8 af a1 01  E..N.... z.O.....
0040  [REDACTED] 04 18 00 89 00 3a 14 23 80 94 00 00  [REDACTED]... :.#....
0050  00 01 00 00 00 00 00 00 20 43 4b 41 41 41 41 41  ..... CKAAAAA
0060  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAA AAAAAAAAAA
0070  41 41 41 41 41 41 41 41 41 00 00 21 00 01  AAAAAAAAAA A..!..
```

NetBIOS Name Service (n) P: 30263 D: 30263 M: 0



Portas com maior número de pacotes trafegados

1026/UDP

- Utilizado pelo Serviço Mensageiro do Windows – Windows Messenger
 - Serviço destinado ao envio de simples mensagens para um ou mais usuários em uma LAN
 - Diferente do MSN Messenger
 - Presente nos Windows 2000 e XP
- Tipicamente, o tráfego destinado a essa porta é proveniente de spam para o Mensageiro do Windows

Portas com maior número de pacotes trafegados

1026/UDP

The screenshot shows the pflog.0 - Ethereal interface. The main display area shows a single packet (No. 1921) at time 21038.358136, source 24.184.7.104, protocol z Messenger, and info [passed x10/11]. Below this, the packet details are expanded to show a User Datagram Protocol (UDP) packet with Src Port: 4177 (4177) and Dst Port: 1026 (1026). The packet payload is displayed in hexadecimal and ASCII. The ASCII portion shows a promotional message for a computer system, including the text: "and basic computer skills... INTERESTED???... Email me your name & phone number... g15@yahoo.com... Is Your Computer Making You The Type of Income You Could Be Earning? Last week I made over \$2,600 Using This Program. This System is Great! Check it out for yourself. Visit My website At www.computer.cashcow.com."

No.	Time	Source	Protocol	Info
1921	21038.358136	24.184.7.104	z Messenger	[passed x10/11] Ne

User Datagram Protocol, Src Port: 4177 (4177), Dst Port: 1026 (1026)

```
0230 20 61 6e 64 20 62 61 73 69 63 20 63 6f 6d 70 75 and bas ic compu
0240 74 65 72 20 73 6b 69 6c 6c 73 2e 63 2e 2e 2e 2e ter skill ls.....
0250 49 4e 54 45 52 45 53 54 45 44 3f 3f 3f 0d 0a 0d INTEREST ED???...
0260 0a 20 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 . . . . .
0270 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0280 20 20 20 20 20 20 20 20 20 20 20 20 45 6d 61 69
0290 6c 20 6d 65 20 79 6f 75 72 20 6e 61 6d 65 20 26
02a0 20 70 68 6f 6e 65 20 6e 75 6d 62 65 72 2e 0d 0a
02b0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
02c0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
02d0 20 20 20 20 20 20 20 20 20 20 20 20 53 63 75 6e
02e0 67 31 35 40 79 61 68 6f 6f 2e 63 6f 6d 0d 0a 20
02f0 0d 0a 0d 0a 49 73 20 59 6f 75 72 20 43 6f 6d 70
0300 75 74 65 72 20 4d 61 6b 69 6e 67 20 59 6f 75 20
0310 54 68 65 20 54 79 70 65 20 4f 66 20 49 6e 63 6f
0320 6d 65 20 59 6f 75 20 43 6f 75 6c 64 20 42 65 20
0330 45 61 72 6e 69 6e 67 3f 20 20 20 4c 61 73 74 20
0340 57 65 65 6b 20 49 20 4d 61 64 65 20 4f 76 65 72
0350 20 24 32 2c 36 30 30 20 55 73 69 6e 67 20 54 68
0360 65 20 50 72 6f 67 72 61 6d 2e 20 20 20 54 68 69
0370 73 20 53 79 73 74 65 6d 20 49 73 20 47 72 65 61
0380 74 21 20 20 20 43 68 65 63 6b 20 49 74 20 4f 75
0390 74 20 46 6f 72 20 59 6f 75 72 73 65 6c 66 2e 20
03a0 20 20 56 69 73 69 74 20 4d 79 20 57 65 62 73 69
03b0 74 65 20 41 74 20 20 20 20 20 20 77 77 77 2e
03c0 63 6f 6d 70 75 74 65 72 63 61 73 68 63 6f 77 2e
03d0 63 6f 6d 00
```

File: pflog.0 3551 KB 2 P: 30263 D: 30263 M: 0

Portas com maior número de pacotes trafegados

1027/UDP

- Utilizado pelo ICQ – Instant Messenger
- Utilizado também pelo serviço do Windows Messenger
 - Quando o sistema tenta dar um bind na porta 1026/UDP se estiver ocupada, utiliza a próxima porta disponível (1027 e 1028) .
- Tipicamente, o tráfego destinado a essa porta é proveniente de spam para o Mensageiro do Windows

Portas com maior número de pacotes trafegados

1027/UDP

pflog.0 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Go to the first packet + Expression... Clear

No.	Time	Source	Protocol	Info
1917	21038.291128	24.184.7.104	z Messenger	[passed x10/11] Ne

User Datagram Protocol, Src Port: 4177 (4177), Dst Port: 1027 (1027)

No.	Time	Source	Destination	Length	Info												
0230	20	61	6e	64	20	62	61	73	69	63	20	63	6f	6d	70	75	and bas ic compu
0240	74	65	72	20	73	6b	69	6c	6c	73	2e	2e	2e	2e	2e	2e	ter skill ls.....
0250	49	4e	54	45	52	45	53	54	45	44	3f	3f	3f	0d	0a	0d	INTEREST ED???.
0260	0a	20	0d	0a	0d	0a	20	20	20	20	20	20	20	20	20	20
0270	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0280	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0290	6c	20	6d	65	20	79	6f	75	72	20	6e	61	6d	65	20	26	Email
02a0	20	70	68	6f	6e	65	20	6e	75	6d	62	65	72	2e	0d	0a	1 me you r name &
02b0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	phone n umber...
02c0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
02d0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
02e0	67	31	35	40	79	61	68	6f	6f	2e	63	6f	6d	0d	0a	20	Scun
02f0	0d	0a	0d	0a	49	73	20	59	6f	75	72	20	43	6f	6d	70	g15@yaho o.com..
0300	75	74	65	72	20	4d	61	6b	69	6e	67	20	59	6f	75	20Is Y our Comp
0310	54	68	65	20	54	79	70	65	20	4f	66	20	49	6e	63	6f	uter Mak ing You
0320	6d	65	20	59	6f	75	20	43	6f	75	6c	64	20	42	65	20	The Type of Inco
0330	45	61	72	6e	69	6e	67	3f	20	20	20	4c	61	73	74	20	me You C ould Be
0340	57	65	65	6b	20	49	20	4d	61	64	65	20	4f	76	65	72	Earning? Last
0350	20	24	32	2c	36	30	30	20	55	73	69	6e	67	20	54	68	week I M ade Over
0360	65	20	50	72	6f	67	72	61	6d	2e	20	20	20	54	68	69	\$2,600 Using Th
0370	73	20	53	79	73	74	65	6d	20	49	73	20	47	72	65	61	e Progra m. Thi
0380	74	21	20	20	20	43	68	65	63	6b	20	49	74	20	4f	75	s System is Grea
0390	74	20	46	6f	72	20	59	6f	75	72	73	65	6c	66	2e	20	t! Che ck It ou
03a0	20	20	56	69	73	69	74	20	4d	79	20	57	65	62	73	69	t For Yo urself.
03b0	74	65	20	41	74	20	20	20	20	20	20	20	77	77	77	2e	visit My websi
03c0	63	6f	6d	70	75	74	65	72	63	61	73	68	63	6f	77	2e	te At www.
03d0	63	6f	6d	00													computer cashcow.

File: pflog.0 3551 KB 2 | P: 30263 D: 30263 M: 0

Portas com maior número de pacotes trafegados

1434/UDP

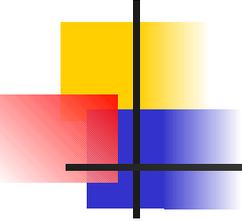
- Microsoft-SQL-Monitor
- Usado para monitorar os banco de dados MS - SQL
 - 10/07/2002 – Microsoft divulga patch para correção de erro no SQL
 - 25/01/2003 – Worm Slammer
 - 75 mil hosts em 30 min
- Atualmente, o worm spyBot e suas variantes.

Portas com maior número de pacotes trafegados

53/UDP

- Domain Name Service
- Vulnerabilidades no Bind
 - Bind 9 – FreeBSD 5.3 (CAN-2005-0034)
 - Queda do daemon named pelo envio de um pacote com conteúdo específico.
 - Bind 8.4.4 e 8.4.5 – (CAN-2005-0033)
 - Inoperabilidade do daemon através de overflow em determinada consulta.
 - Bind 4 e 8 – (CAN-2002-1219)
 - Múltiplas vulnerabilidades que possibilitam ao atacante executar código com privilégio do *uid* do named: tipicamente root

Portas TCP com maior número de pacotes trafegados



- 1433 – 37,73%
- 445 – 22,32%
- 135 – 11,09%
- 139 – 7,12%
- 80 – 3,45%
- 4899 – 2,93%
- 1080 – 2,27%
- 1025 – 1,69%
- 5554 – 1,03%
- 3306 – 0,95%

Portas com maior número de pacotes trafegados

1433/TCP

- Banco de Dados da Microsoft (Microsoft-SQL-Server)
- Clientes: Access, Excel, entre outros que são compatíveis com o ODBC
- Possibilidade de se habilitar SSL
(<http://support.microsoft.com/default.aspx?scid=/servicedesks/webcasts/wc042302/wcblurb042302.asp>)
- Scans para essa porta são muito comuns e, geralmente, procuram por banco de dados sem senha.
- MSSQL Hello Buffer Overflow attack
 - (CAN-2002-1123)

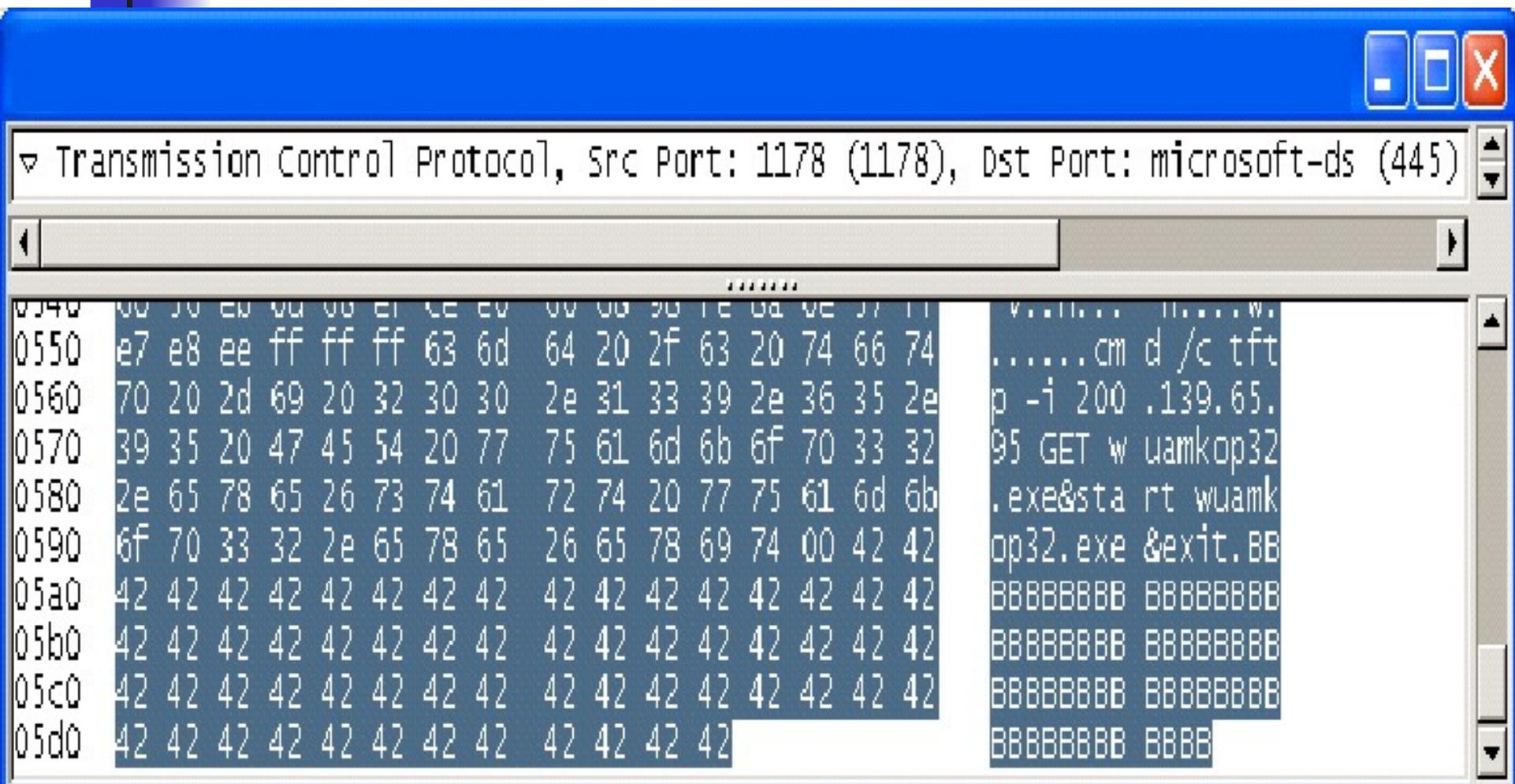
Portas com maior número de pacotes trafegados

445/TCP

- Microsoft Domain Service, Windows 2000/XP
– compartilhamento de arquivos e impressoras
- Pode ser habilitado SSL
- Junho/2005 (CAN-2005-0045)
 - Um servidor pode, em uma transação SMB (MS Server Message Block) maliciosa, causar overflow no cliente (Win2000) fazendo-o rebotar.
- Worms: SpyBot, Mytob@mm e Poxdar

Portas com maior número de pacotes trafegados

445/TCP



Portas com maior número de pacotes trafegados

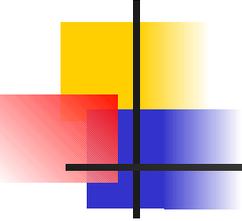
135/TCP

- Microsoft Remote Procedure call, também usado pelo SMB (Server Message Block) para compartilhamento de arquivos e impressoras
- Problemas comuns: usuário e senha sem criptografia, permissões erradas
- 2003 – worm MS.Blaster
 - Possibilidade de execução de código arbitrário através de Buffer Overrun. MS03-026
- 2004 – worm Welchia
- 2005 - Gaobot.gen, SpyBot, Poxdar, Mytob.AR@mm
- TODOS explorando a vulnerabilidade MS03-26

Portas com maior número de pacotes trafegados

139/TCP

- NetBIOS
 - 137 – TCP/UDP – Name Service
 - 138 – TCP/UDP – Datagram Service
 - 139 – TCP/UDP – Session Service
- Usado pelo SMB (Server Message Block) para compartilhamento de arquivos e impressoras no Windows
- Para o SMB pode ser habilitado o SSL.
- Também afetado pela vulnerabilidade MS03-026 (execução de código arbitrário)
- Vírus e worms que usam o compartilhamento de arquivos no Windows como forma de propagação



Portas com maior número de pacotes trafegados

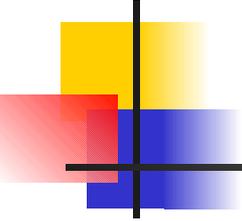
80/TCP

- Vulnerabilidades no servidor Web
- Ataques Relacionados
 - Defacement
 - Phishing
 - DoS
 - DDoS
 - SQL-Injection

Portas com maior número de pacotes trafegados

4899/TCP

- “Remote Administrator” para Windows
Windows 9x/ME/NT4.0/2000/XP/2003
 - Por padrão esse serviço não pede usuário, apenas senha.
 - O atacante pode ficar buscando acesso através de senhas fracas.



Portas com maior número de pacotes trafegados

1080/TCP

- Usado pelo Wingate
- Problemas comuns: configurações erradas de proxy
- Problemas de relay de spam
- Trojam: Webus, WinHole, SubSeven
- Worm: Bagle, Bugbear, Webus, Mydoom

Portas com maior número de pacotes trafegados

1025/TCP

- Primeira porta alocável dinamicamente
- Microsoft Remote Procedure Call (RPC) service.
- Trojans - criando Backdoors na porta 1025/TCP
 - Netspy, Maverick's, Matrix, Lala, Staprew

Portas com maior número de pacotes trafegados

5554/TCP

- Worm Sasser – Servidor FTP
- Scans para essa porta são provenientes de outros worms, assim como o Dabber, tentando explorar uma vulnerabilidade no servidor FTP do Sasser.

Portas com maior número de pacotes trafegados

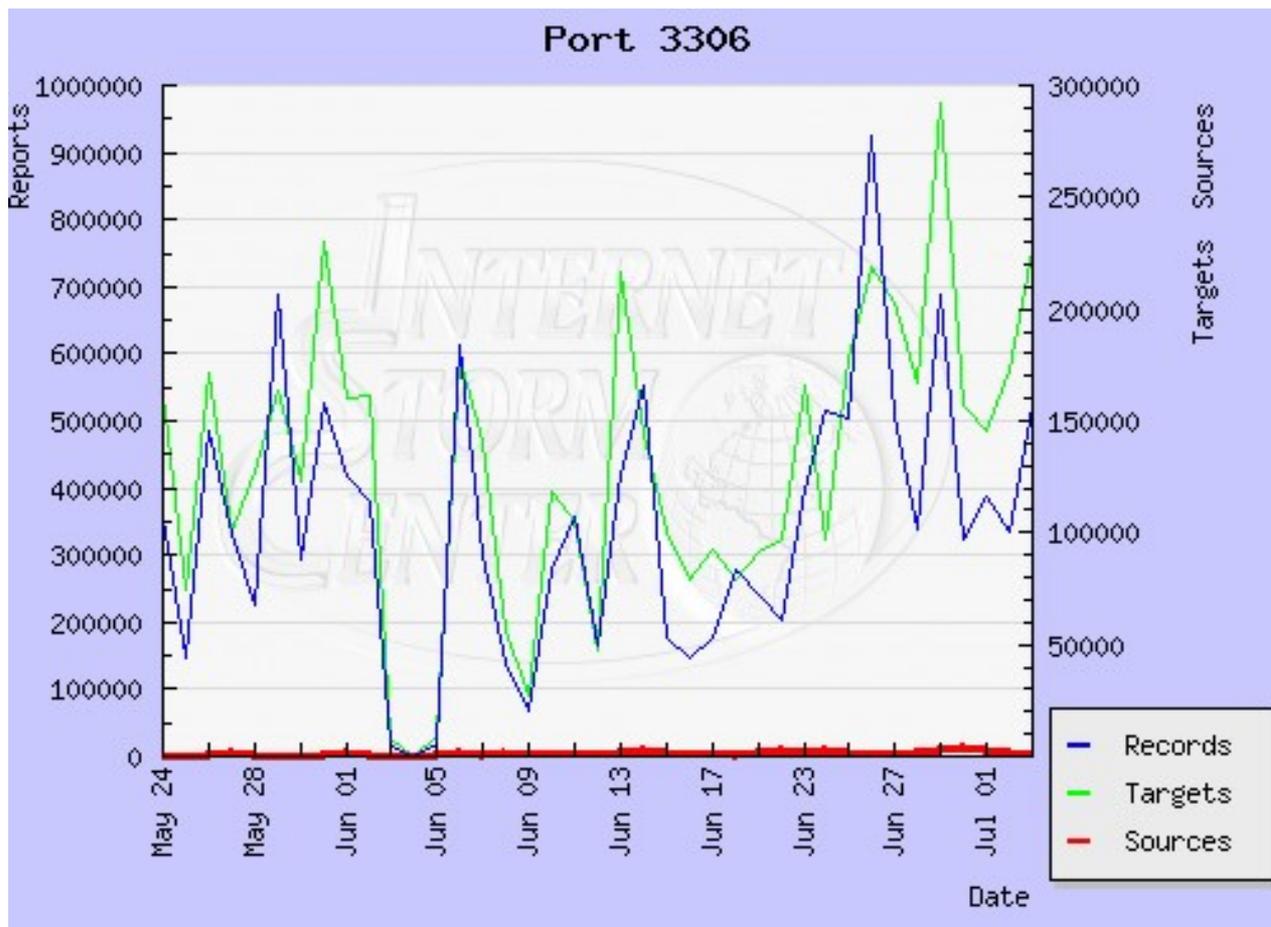
3306/TCP

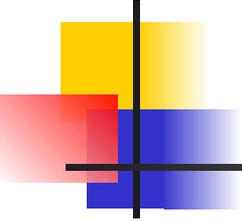
- Banco de Dados Mysql
- Tipos de Ataques
 - Busca por senhas fracas (mySQL Bot)
 - Overflow (25/05/2005)

http://www.frsirt.com/exploits/20050511.maxdb_webdbm_get_overflow.pm.phpBuffer

Portas com maior número de pacotes trafegados

3306/TCP





Outras portas TCP que apareceram nas TOP – 10 durante essa semana

- 25
 - 1,17%
 - Logs do dia 27/06/2005
- 10000
 - 4,7%
 - Logs do dia 27/06/2005

Portas com maior número de pacotes trafegados

25/TCP

- Porta SMTP (Simple Mail Transfer Protocol)
- Buscas por servidores de mail
 - Open relay
- Vulnerabilidades em clientes de mail como o Sendmail, Postfix, qmail, etc

Portas com maior número de pacotes trafegados

10000/TCP

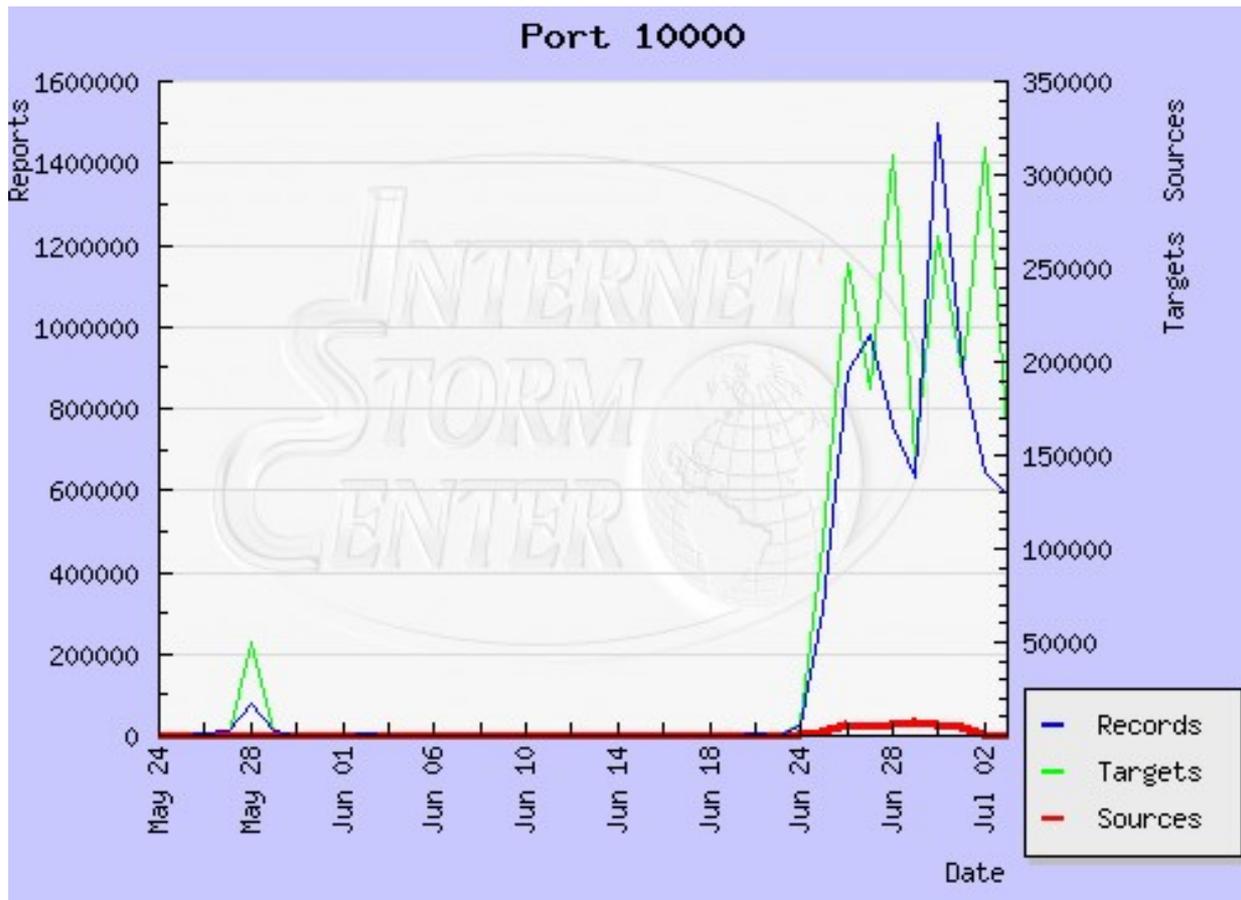
- Dia 22/06/2005 - descoberta de Buffer Overflow no VERITAS Backup Exec Remote Agent for Windows Servers

<http://support.veritas.com/docs/276604>

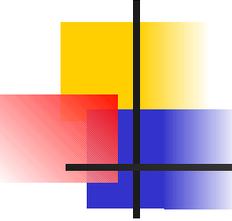
- No dia 27/06/2005 essa porta já aparecia como uma das 10 portas com maior número de pacotes trafegados nos honeypots do Consórcio

Portas com maior número de pacotes trafegados

10000/TCP

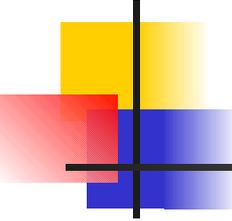


Dshield



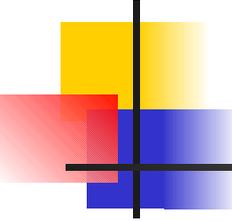
Conclusões

- Consórcio Brasileiro de Honeypots: uma ferramenta para a monitoração do estado da segurança no na Internet brasileira
 - Gráfico que mostrará variações abruptas no número de pacotes recebidos para dada porta
- Perfil da segurança na Internet
 - Rapidez na distribuição e uso de malwares
 - Exigência de uma equipe de segurança que tome mais providências pro-ativas que reativas



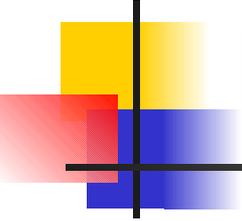
Recomendações

- Atualizações
- Atenção às novas vulnerabilidades
- Firewall
 - A grande quantidade de logs nas firewalls prejudica a segurança
- Logs do Consórcio Brasileiro de Honeypots



Agradecimentos

- Autores
 - Liane Tarouco
 - Leandro Bertholdo
- POP-RS/CERT-RS
 - Mell Fogliatto
 - Joao Ceron
 - Klaus Engelman
 - Andrey Andreoli
- CERT-BR
 - Klaus Steding-Jessen



Perguntas ?

Emerson Virti
emerson@tche.br