Projeto Honeypots Distribuídos

Émerson Salvadori Virti

emerson@tche.br

Roteiro

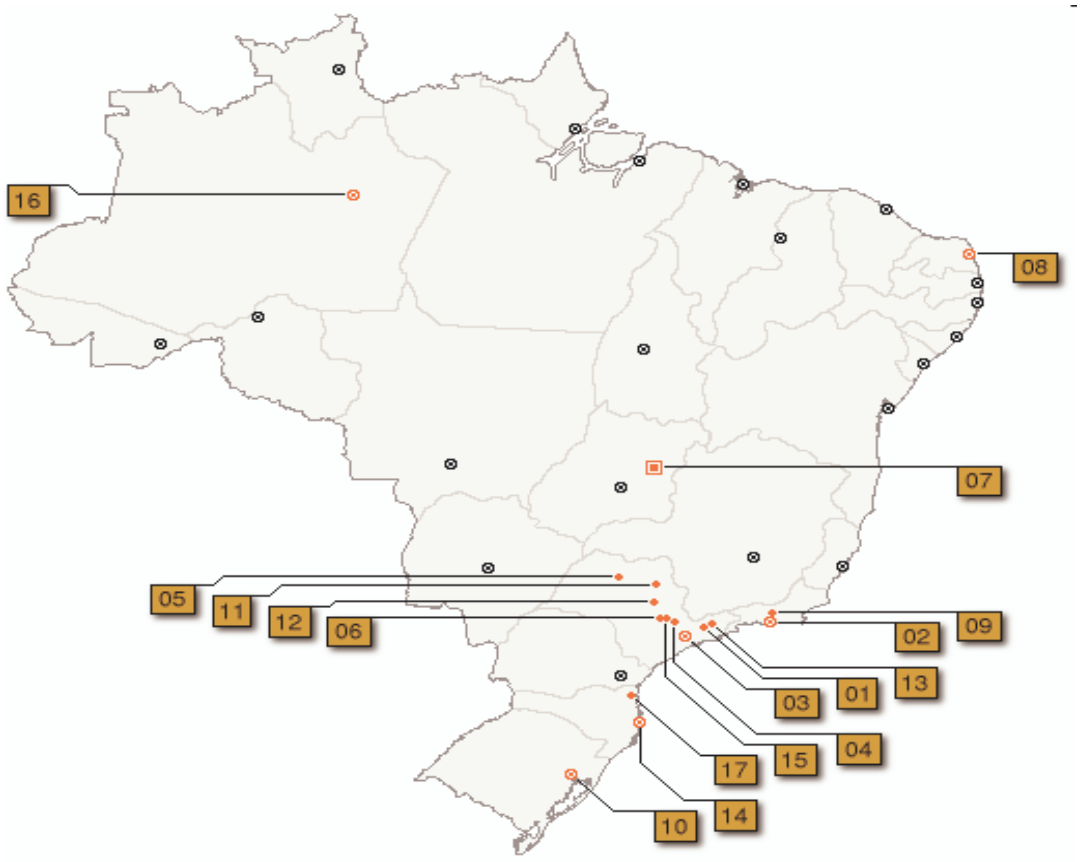
- Conceitos
- Apresentação do Consórcio Brasileiro de Honeypots
- Comparação das estatísticas do Consórcio através da observação de outros indicadores da Internet
- Análise das principais portas UDP acessadas
- Análise das principais portas TCP acessadas
- Conclusões
- Forma de inclusão no Consórcio
- Recomendações

Conceitos

- Honeypot

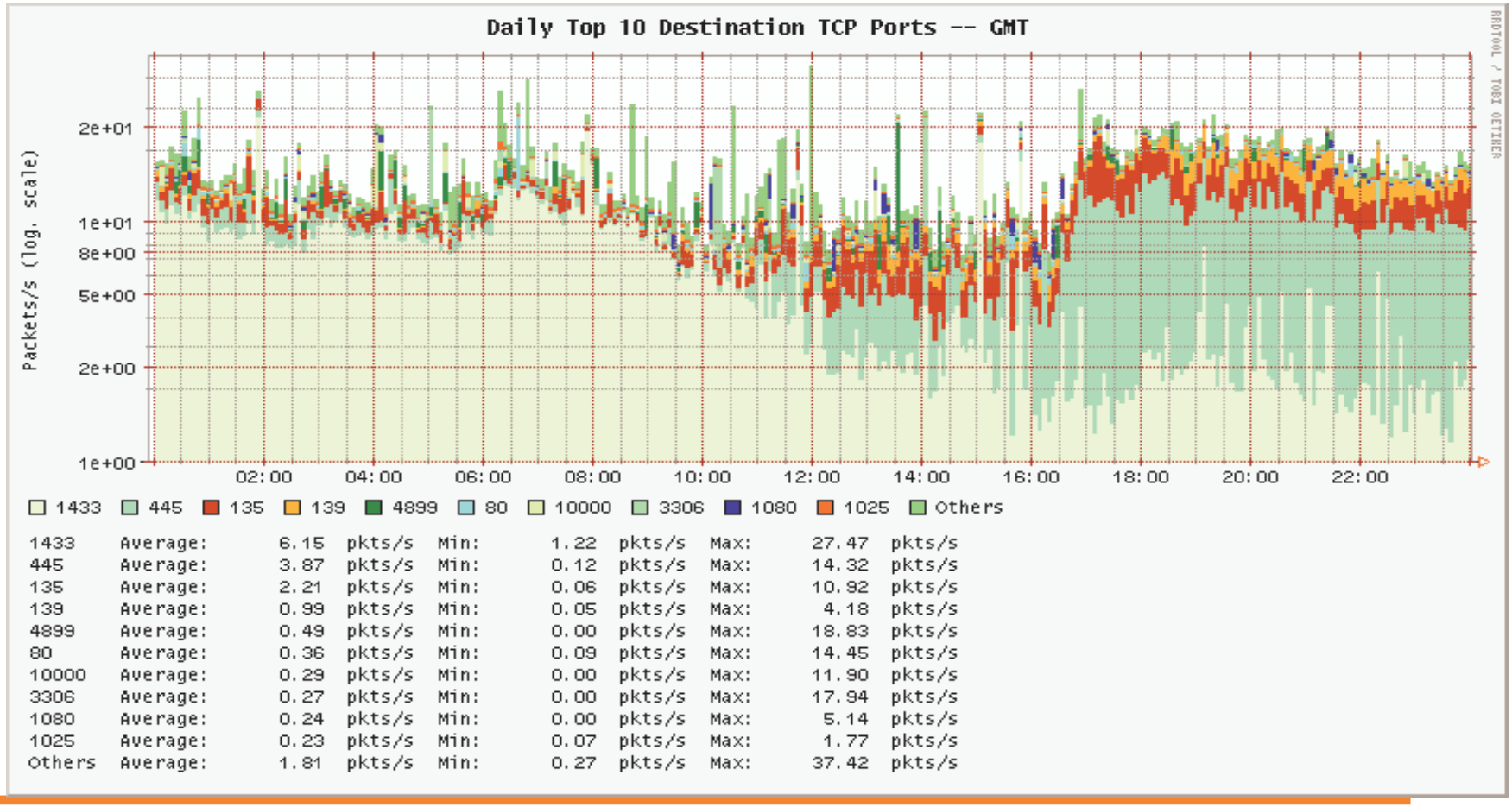
- Honeynet

Consórcio Brasileiro de Honeypots



Consórcio Brasileiro de Honeypots

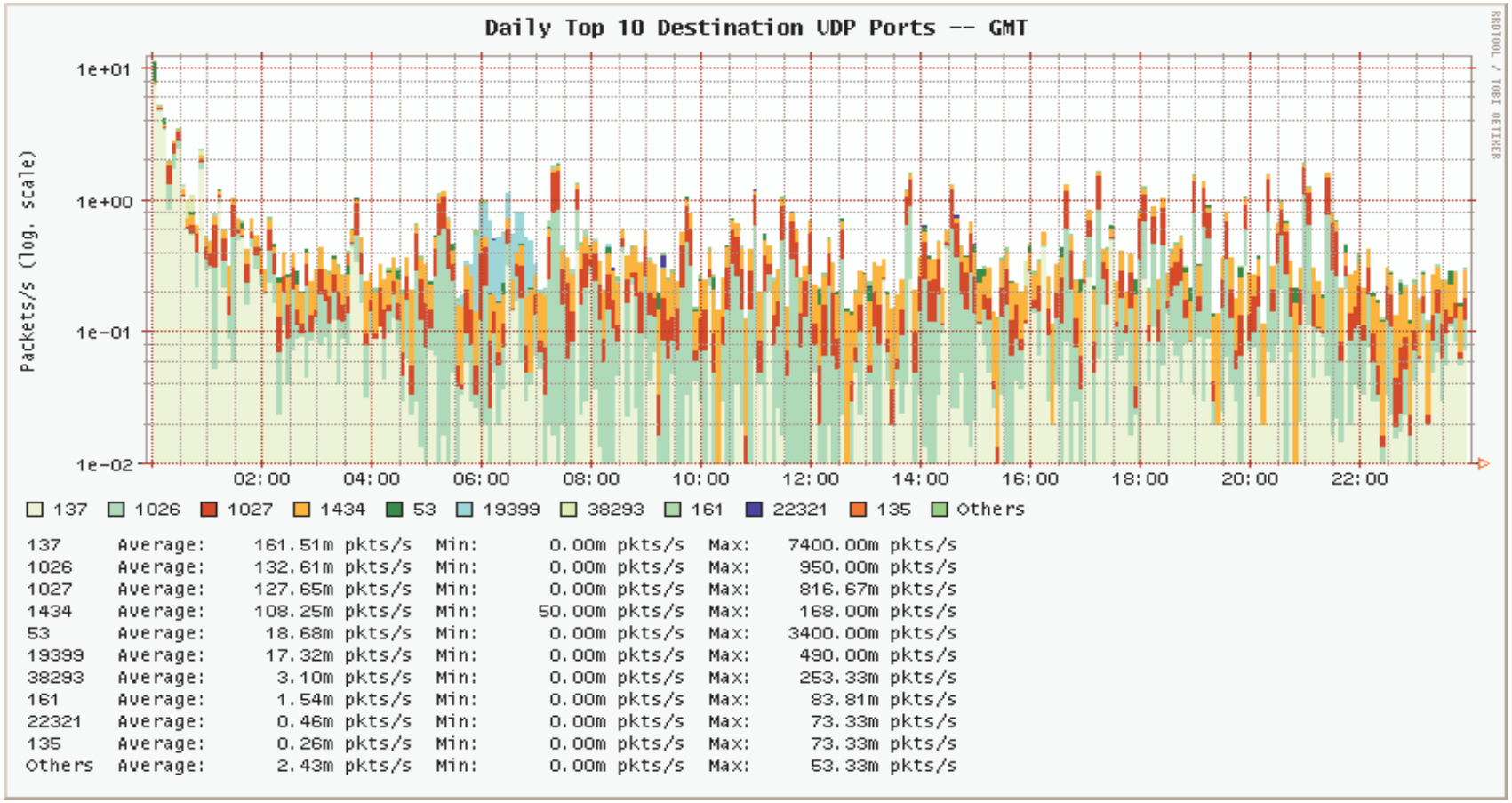
Portas TCP com Maior Número de Pacotes Trafegados



1433	Average:	6.15	pkts/s	Min:	1.22	pkts/s	Max:	27.47 pkts/s
445	Average:	3.87	pkts/s	Min:	0.12	pkts/s	Max:	14.32 pkts/s
135	Average:	2.21	pkts/s	Min:	0.06	pkts/s	Max:	10.92 pkts/s
139	Average:	0.99	pkts/s	Min:	0.05	pkts/s	Max:	4.18 pkts/s
4899	Average:	0.49	pkts/s	Min:	0.00	pkts/s	Max:	18.83 pkts/s
80	Average:	0.36	pkts/s	Min:	0.09	pkts/s	Max:	14.45 pkts/s
10000	Average:	0.29	pkts/s	Min:	0.00	pkts/s	Max:	11.90 pkts/s
3306	Average:	0.27	pkts/s	Min:	0.00	pkts/s	Max:	17.94 pkts/s
1080	Average:	0.24	pkts/s	Min:	0.00	pkts/s	Max:	5.14 pkts/s
1025	Average:	0.23	pkts/s	Min:	0.07	pkts/s	Max:	1.77 pkts/s
Others	Average:	1.81	pkts/s	Min:	0.27	pkts/s	Max:	37.42 pkts/s

Consórcio Brasileiro de Honeypots

Portas UDP com Maior Número de Pacotes Trafegados



137	Average:	161.51m pkts/s	Min:	0.00m pkts/s	Max:	7400.00m pkts/s
1026	Average:	132.61m pkts/s	Min:	0.00m pkts/s	Max:	950.00m pkts/s
1027	Average:	127.65m pkts/s	Min:	0.00m pkts/s	Max:	816.67m pkts/s
1434	Average:	108.25m pkts/s	Min:	50.00m pkts/s	Max:	168.00m pkts/s
53	Average:	18.68m pkts/s	Min:	0.00m pkts/s	Max:	3400.00m pkts/s
19399	Average:	17.32m pkts/s	Min:	0.00m pkts/s	Max:	490.00m pkts/s
38293	Average:	3.10m pkts/s	Min:	0.00m pkts/s	Max:	253.33m pkts/s
161	Average:	1.54m pkts/s	Min:	0.00m pkts/s	Max:	83.81m pkts/s
22321	Average:	0.46m pkts/s	Min:	0.00m pkts/s	Max:	73.33m pkts/s
135	Average:	0.26m pkts/s	Min:	0.00m pkts/s	Max:	73.33m pkts/s
Others	Average:	2.43m pkts/s	Min:	0.00m pkts/s	Max:	53.33m pkts/s

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

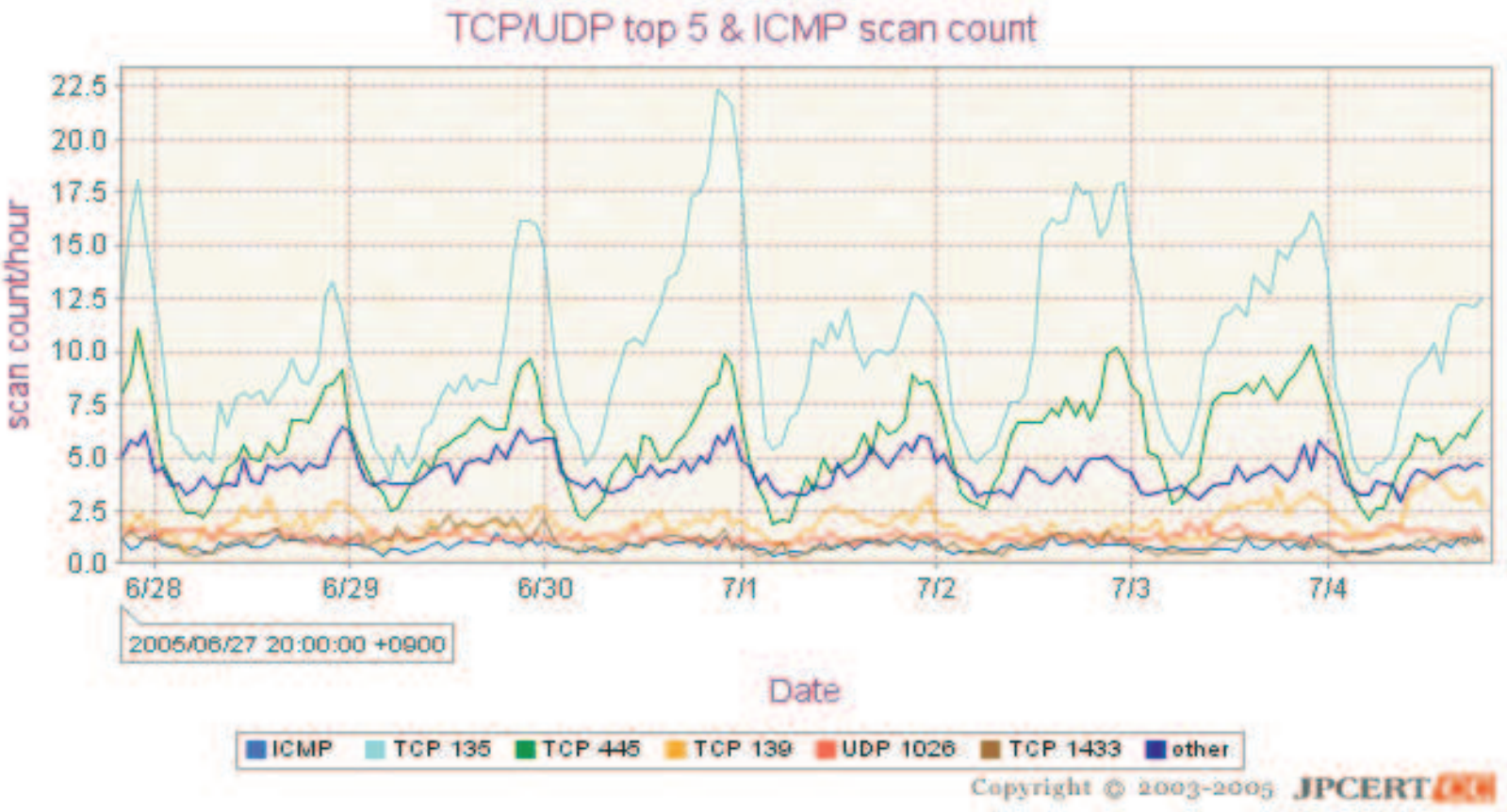
Service Name	Port Number	Explanation
microsoft-ds	445	Win2k+ Server Message Block
epmap	135	DCE endpoint resolution
---	1026	
halflife	27015	Half-Life Game Server
netbios-ssn	139	NETBIOS Session Service
eMule	4672	eMule / eDonkey P2P Software
gnutella-svc	6346	gnutella-svc
bittorrent	6881	Bit Torrent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

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, atulizada a cada 15 min, das top 5 portas scan

JPCERTCC

Japan Computer Emergency Response Team Coordination Center



Diferenças nas Estatisticas

- 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%

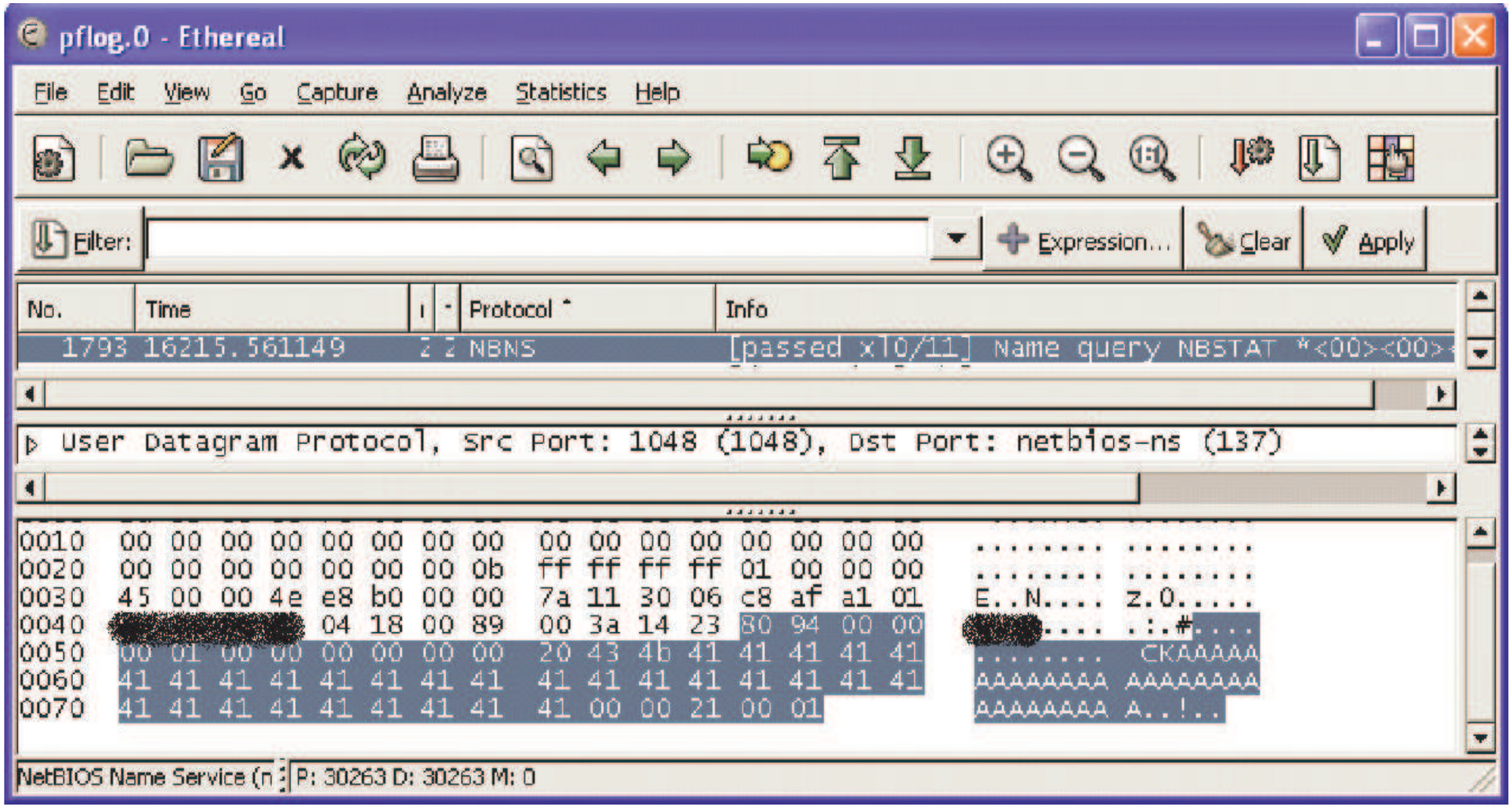
Portas com maior número de pacotes trafegados

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, Alcra 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



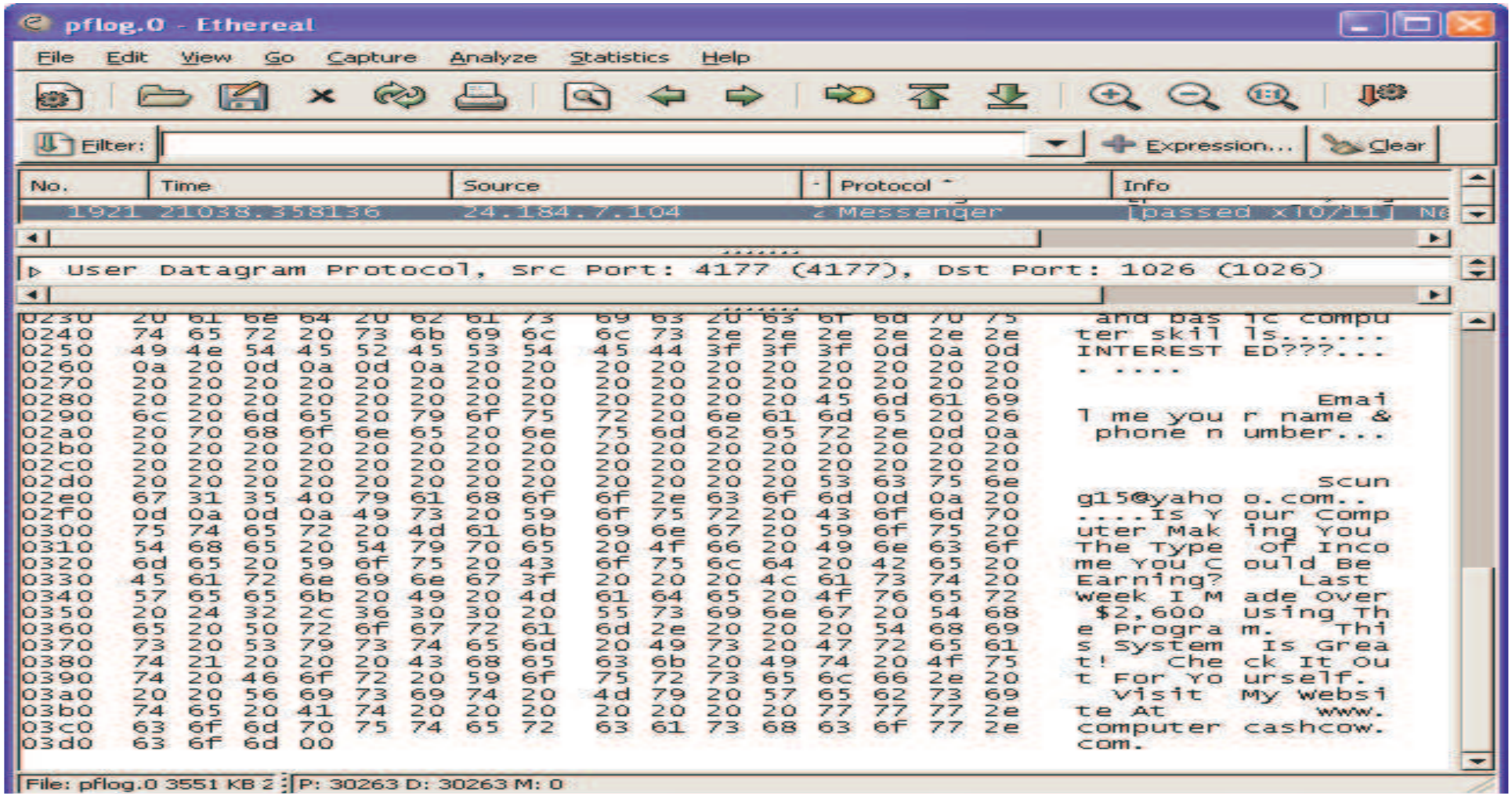
Portas com maior número de pacotes trafegados

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 Messeger
    - 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



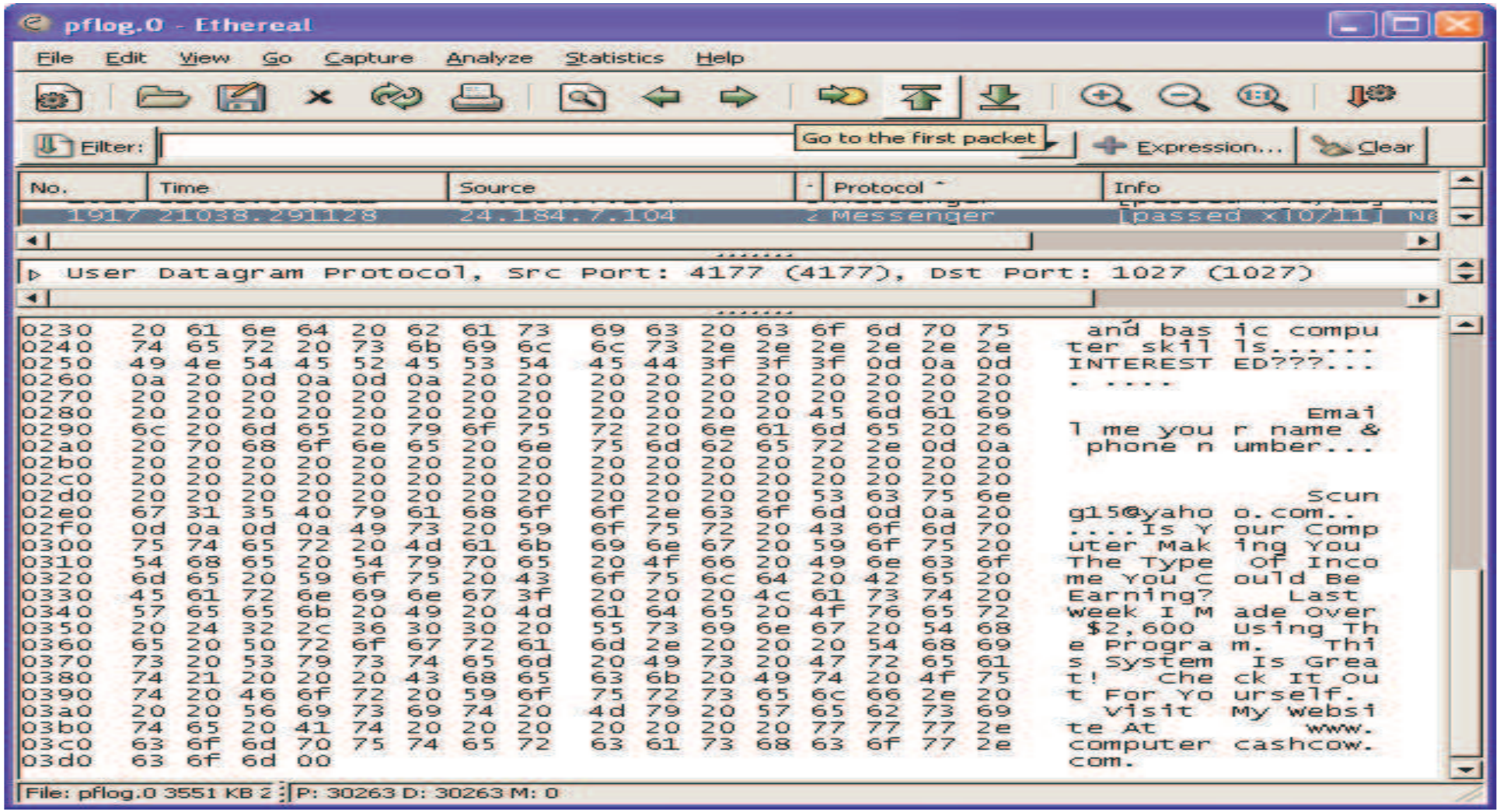
Portas com maior número de pacotes trafegados

1027/UDP

- Utilizado pelo ICQ – Instant Messanger
- 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



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)

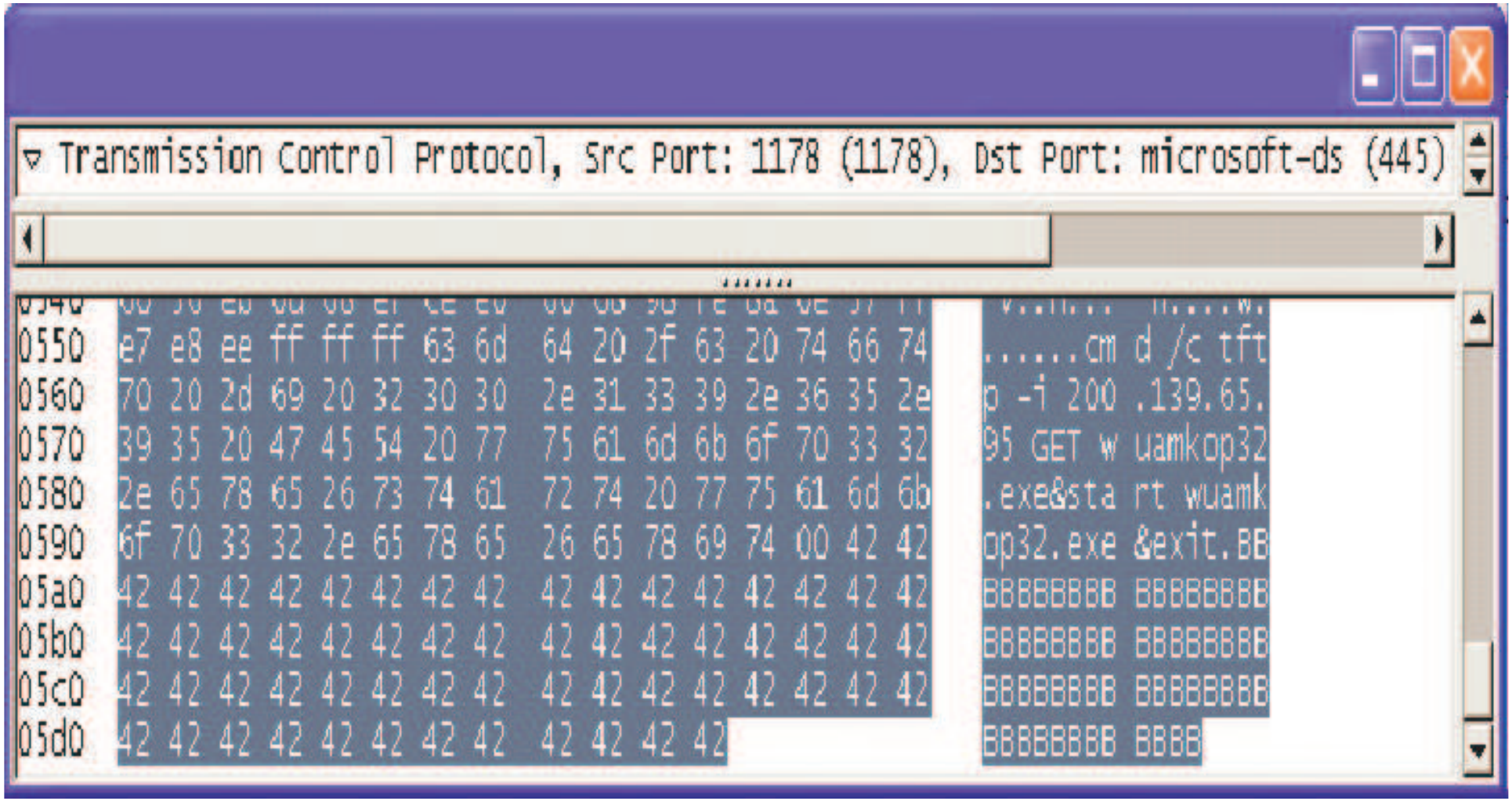
Portas com maior número de pacotes trafegados

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 rebootar.
- 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

- Vunerabilidades 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, tentanto 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

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

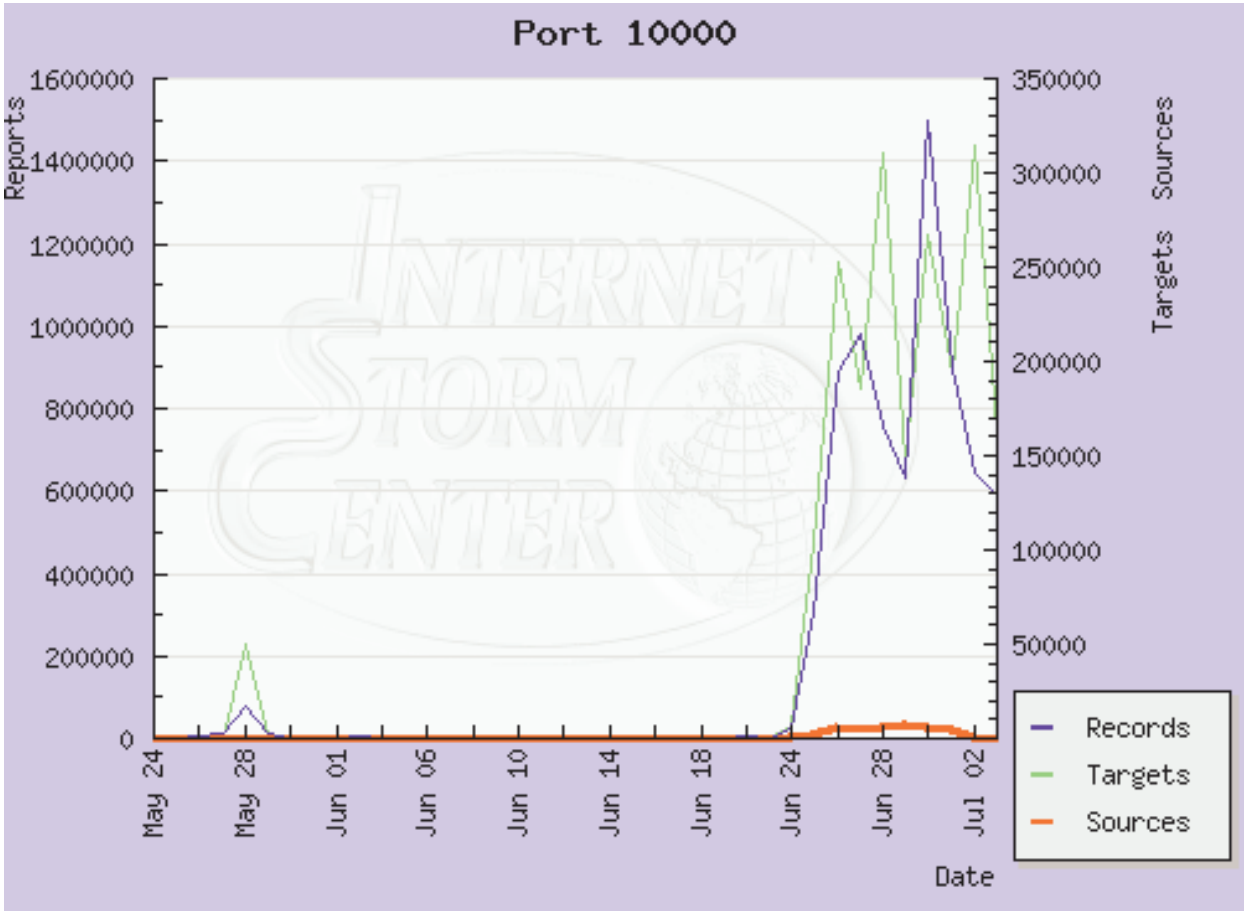
- Dia 22/06/2005 - descoberta de Buffer Overflow no VERITAS Backup Exec Remote Agent for Windows Servers

  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 regurança 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 pró-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

Participando do Consórcio Brasileiro de Honeypots

- Contatar com Klaus Jessen (CERT-BR)
  jessen@nic.br
- Necessidade de confiança
- Indicação
- Disponibilização dos logs por instituição
- Disponibilidade de tempo para atualizações nos honeypots
- Comprometimento com a confidencialidade
- Não necessita de recursos de hardware sofisticados

Perguntas ?

Emerson Virti

emerson@tche.br