



Daily Intrusion Prevention System Statistics



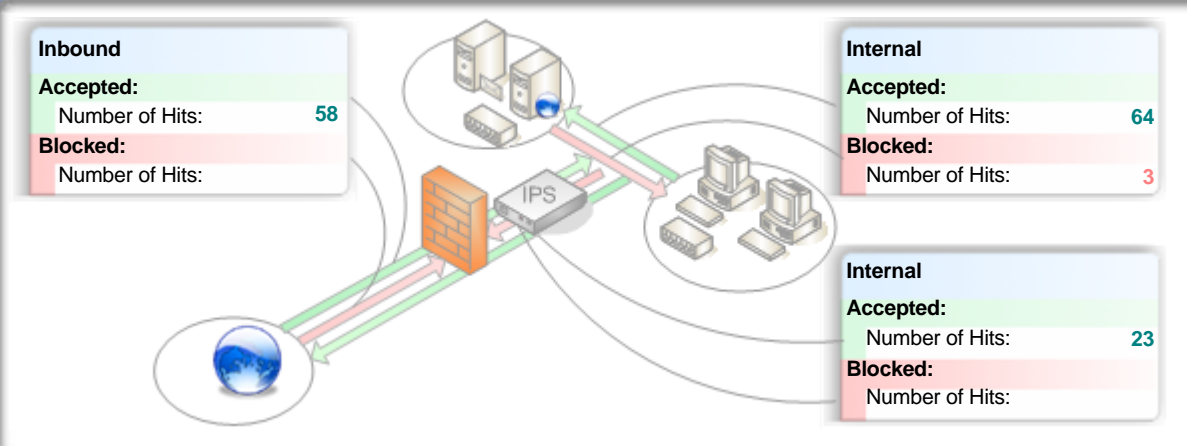
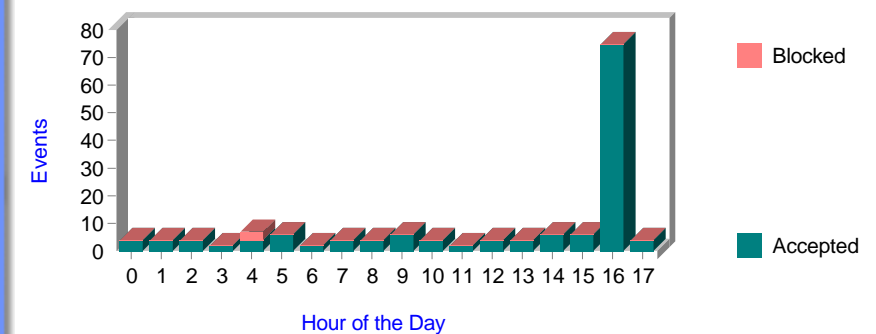
Sunday April 17, 2005



IPS - Computers Targeted by and Sending Potential Threats

| Top Computer Targetted | | Number of Computers |
|-------------------------------------|--|---------------------|
| Internal Target of Internal Threats | d7.DATASET(192.168.0.201) | 1 |
| Internal Target of Inbound Threats | 192.168.0.92 | 2 |
| External Target of Outbound Threats | host4-17.pool8537.interbusiness.it(85.37.17.4) | 2 |
| Top Source Computer | | Number of Computers |
| Internal Source of Internal Threats | BOUZIGUES(192.168.0.52) | 1 |
| External Source of Inbound Threats | messenger.hotmail.com(207.46.104.20) | 53 |
| Internal Source of Outbound Threats | 192.168.0.92 | 1 |

IPS Filtered Traffic - Hourly Activity



IPS Filtered Traffic - Flux

| | Accepted | Blocked | Total |
|----------|----------|---------|-------|
| Inbound | 58 | 0 | 58 |
| Outbound | 23 | 0 | 23 |
| Internal | 64 | 3 | 67 |

IPS - Top 5 Potential Threats

| Short Description | Severity | Events |
|----------------------------------|----------|------------|
| SMB.DCERPC.Registry.OpenHKLM.139 | 1 | 64 |
| edonkey | 1 | 48 |
| invalid_param | 1 | 10 |
| invalid_pointer | 1 | 10 |
| msn | 1 | 10 |
| Total Top 5 Attacks | | 142 |

IPS - Top 5 Services Targeted by Potential Threats

| | Accepted | Blocked | Total |
|------------------------------|-----------|-----------|------------|
| 139 | 67 | 0 | 67 |
| 53 | 23 | 0 | 23 |
| 3843 | 10 | 0 | 10 |
| 3007 | 2 | 0 | 2 |
| 3008 | 2 | 0 | 2 |
| Total Top 5 Services: | 14 | 23 | 104 |

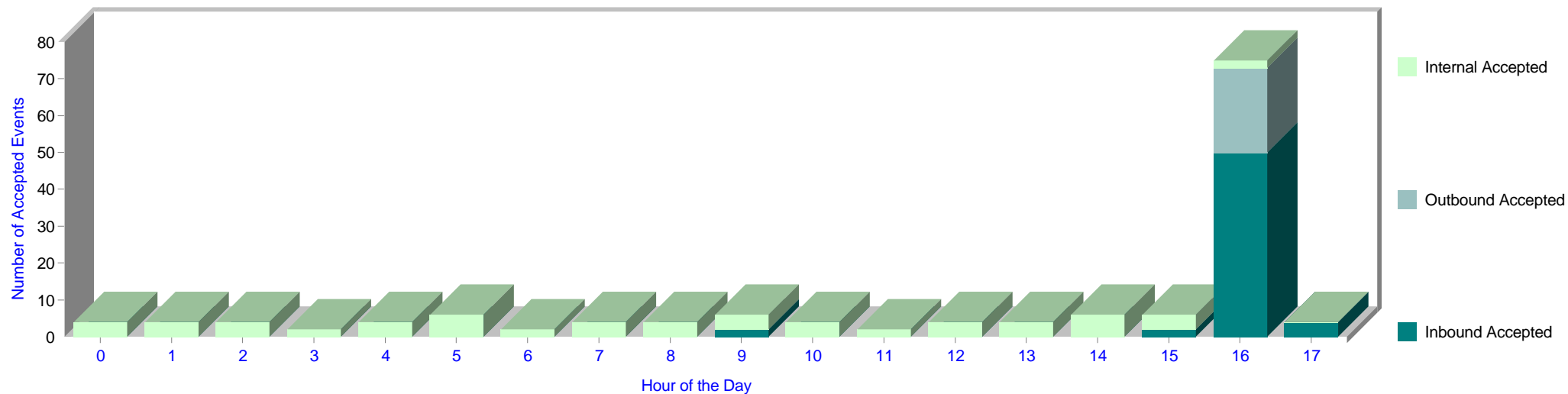


Events by Hour of the Day - Graph

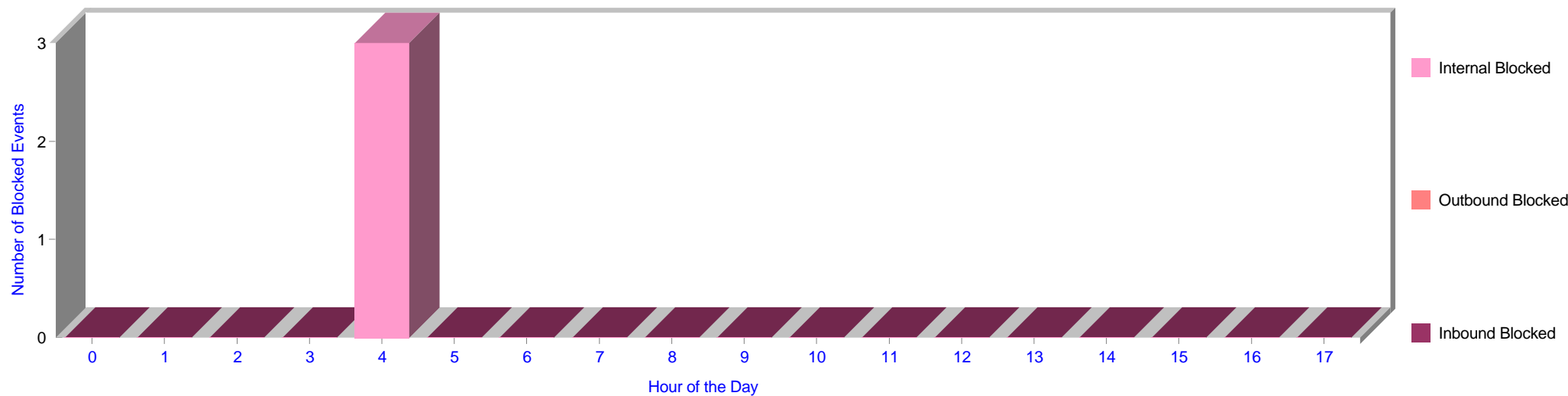
Sunday April 17, 2005



Accepted Traffic



Blocked Traffic





Events by Hour of the Day - Data

Sunday April 17, 2005







| Hour | Inbound | | Outbound | | Internal | | Total Hits | | Total |
|--|-----------|---------|-----------|---------|-----------|----------|------------|----------|------------|
| | Accepted | Blocked | Accepted | Blocked | Accepted | Blocked | Accepted | Blocked | |
| 00:00 | | | | | 4 | | 4 | | 4 |
| 01:00 | | | | | 4 | | 4 | | 4 |
| 02:00 | | | | | 4 | | 4 | | 4 |
| 03:00 | | | | | 2 | | 2 | | 2 |
| 04:00 | | | | | 4 | 3 | 4 | 3 | 7 |
| 05:00 | | | | | 6 | | 6 | | 6 |
| 06:00 | | | | | 2 | | 2 | | 2 |
| 07:00 | | | | | 4 | | 4 | | 4 |
| 08:00 | | | | | 4 | | 4 | | 4 |
| 09:00 | 2 | | | | 4 | | 6 | | 6 |
| 10:00 | | | | | 4 | | 4 | | 4 |
| 11:00 | | | | | 2 | | 2 | | 2 |
| 12:00 | | | | | 4 | | 4 | | 4 |
| 13:00 | | | | | 4 | | 4 | | 4 |
| 14:00 | | | | | 6 | | 6 | | 6 |
| 15:00 | 2 | | | | 4 | | 6 | | 6 |
| 16:00 | 50 | | 23 | | 2 | | 75 | | 75 |
| 17:00 | 4 | | | | | | 4 | | 4 |
| Total for Sunday April 17, 2005 | 58 | | 23 | | 64 | 3 | 145 | 3 | 148 |



Top 5 Internal Computer(s) Targeted by the Top 5 Internal Threats

Sunday April 17, 2005



| Internal Computer Targeted | Threat Category | Potential Threat Description | Number of Potential Threats |
|--|---|---|--|
|   d7.DATASET(192.168.0.201) |  netbios | SMB.DCERPC.Registry.OpenHKLM.139 SMB.DCERPC.SamrEnumerateAliasesInDomain.139 |  67 64 3 |
| Total for the above list: | | | 67 |



Top 5 Internal Computer(s) Targeted by the Top 5 Inbound Threats

Sunday April 17, 2005



| Internal Computer Targeted | Threat Category | Potential Threat Description | Number of Potential Threats |
|----------------------------------|-----------------|------------------------------|-----------------------------|
| 192.168.0.92 | p2p | edonkey | 56 |
| | im | msn | 48 |
| BOUZIGUES(192.168.0.52) | | | 8 |
| | im | msn | 2 |
| Total for the above list: | | | 58 |



Top 5 External Computer(s) Targeted by the Top 5 Outbound Threats

Sunday April 17, 2005



| External Computer Targeted | Threat Category | Potential Threat Description | Number of Potential Threats |
|--|-----------------|------------------------------|-----------------------------|
| | | | |
| host4-17.pool8537.interbusiness.it(85.37.17.4) | dns_decoder | invalid_pointer | 12 |
| | | invalid_param | 8 |
| | | invalid_param | 4 |
| host5-17.pool8537.interbusiness.it(85.37.17.5) | dns_decoder | invalid_param | 11 |
| | | invalid_opcode | 6 |
| | | invalid_opcode | 3 |
| | | invalid_pointer | 2 |
| Total for the above list: | | | 23 |



Top 5 Internal Computer(s) Sending the Top 5 Internal Threats

Sunday April 17, 2005



| Internal Computer Sending Threats | Threat Category | Potential Threat Description | Number of Potential Threats |
|-----------------------------------|-----------------|---|-----------------------------|
| BOUZIGUES(192.168.0.52) | netbios | | |
| | | SMB.DCERPC.Registry.OpenHKLM.139 | 64 |
| | | SMB.DCERPC.SamrEnumerateAliasesInDomain.139 | 3 |
| Total for the above list: | | | 67 |



Top 5 External Computer(s) Sending the Top 5 Inbound Threats

Sunday April 17, 2005



| External Computer Sending Threats | Threat Category | Potential Threat Description | Number of Potential Threats |
|--|-----------------|------------------------------|-----------------------------|
| | | | |
| messenger.hotmail.com(207.46.104.20) | im | msn | 5 |
| ns20286.ovh.NET(213.251.133.129) | p2p | edonkey | 2 |
| 0x503e1df8.bynxx8.adsl-dhcp.tele.dk(80.62.29.248) | p2p | edonkey | 1 |
| 131.Red-81-36-215.pooles.rima-tde.NET(81.36.215.131) | p2p | edonkey | 1 |
| 205-177-3-3.btnaccess.NET(205.177.3.3) | p2p | edonkey | 1 |
| Total for the above list: | | | 10 |



Top 5 Internal Computer(s) Sending the Top 5 Outbound Threats

Sunday April 17, 2005



| Internal Computer Sending Threats | Threat Category | Potential Threat Description | Number of Potential Threats |
|-----------------------------------|-----------------|------------------------------|-----------------------------|
| | | | |
| 192.168.0.92 | dns_decoder | invalid_param | 23 |
| | | invalid_pointer | 10 |
| | | invalid_opcode | 3 |
| Total for the above list: | | | 23 |



Top 5 External Computers with the Top 5 Inbound Threat Detailed Results

Sunday April 17, 2005



| External Computer Sending Threats | Internal Target Computer | Service | Threat Category | Potential Threat Description | Action | Number of Threats |
|---|--------------------------|---------|-----------------|------------------------------|----------|-------------------|
| messenger.hotmail.com(207.46.104.20) | 192.168.0.92 | 3007 | im | msn | Accepted | 2 |
| | 192.168.0.92 | 3225 | | msn | Accepted | 1 |
| | 192.168.0.92 | 4413 | | msn | Accepted | 1 |
| | BOUZIGUES(192.168.0.52) | 1600 | | msn | Accepted | 1 |
| ns20286.ovh.NET(213.251.133.129) | | | | | | 2 |
| | 192.168.0.92 | 3746 | p2p | edonkey | Accepted | 1 |
| | 192.168.0.92 | 3844 | | edonkey | Accepted | 1 |
| 0x503e1df8.bynxx8.adsl-dhcp.tele.dk(80.62.29.248) | | | | | | 1 |
| | 192.168.0.92 | 4060 | p2p | edonkey | Accepted | 1 |
| 131.Red-81-36-215.pooles.rima-tde.NET(81.36.215.131) | | | | | | 1 |
| | 192.168.0.92 | 4321 | p2p | edonkey | Accepted | 1 |
| 205-177-3-3.btnaccess.NET(205.177.3.3) | | | | | | 1 |
| | 192.168.0.92 | 3843 | p2p | edonkey | Accepted | 1 |
| Total for the above list: | | | | | | 10 |



Top 5 Internal Computers with the Top 5 Outbound Threat Detailed Results

Sunday April 17, 2005



| Internal Computer Sending Threats | External Target Computer | Service | Threat Category | Potential Threat Description | Action | Number of Threats |
|-----------------------------------|--|---------|-----------------|------------------------------|----------|-------------------|
| 192.168.0.92 | | | | | | 23 |
| | host4-17.pool8537.interbusiness.it(85.37.17.4) | 53 | dns_decoder | invalid_pointer | Accepted | 8 |
| | host5-17.pool8537.interbusiness.it(85.37.17.5) | 53 | | invalid_param | Accepted | 6 |
| | host4-17.pool8537.interbusiness.it(85.37.17.4) | 53 | | invalid_param | Accepted | 4 |
| | host5-17.pool8537.interbusiness.it(85.37.17.5) | 53 | | invalid_opcode | Accepted | 3 |
| | host5-17.pool8537.interbusiness.it(85.37.17.5) | 53 | | invalid_pointer | Accepted | 2 |
| Total for the above list: | | | | | | 23 |



Top 5 Internal Computers with the Top 5 Internal Threat Detailed Results

Sunday April 17, 2005



| Internal Computer Sending Threats | Internal Target Computer | Service | Threat Category | Potential Threat Description | Action | Number of Threats |
|-----------------------------------|---------------------------|---------|-----------------|---|----------|-------------------|
| | | | | | | |
| BOUZIGUES(192.168.0.52) | | | | | | 67 |
| | d7.DATASET(192.168.0.201) | 139 | netbios | SMB.DCERPC.Registry.OpenHKLM.139 | Accepted | 64 |
| | d7.DATASET(192.168.0.201) | 139 | | SMB.DCERPC.SamrEnumerateAliasesInDomain.139 | Blocked | 3 |
| Total for the above list: | | | | | | 67 |

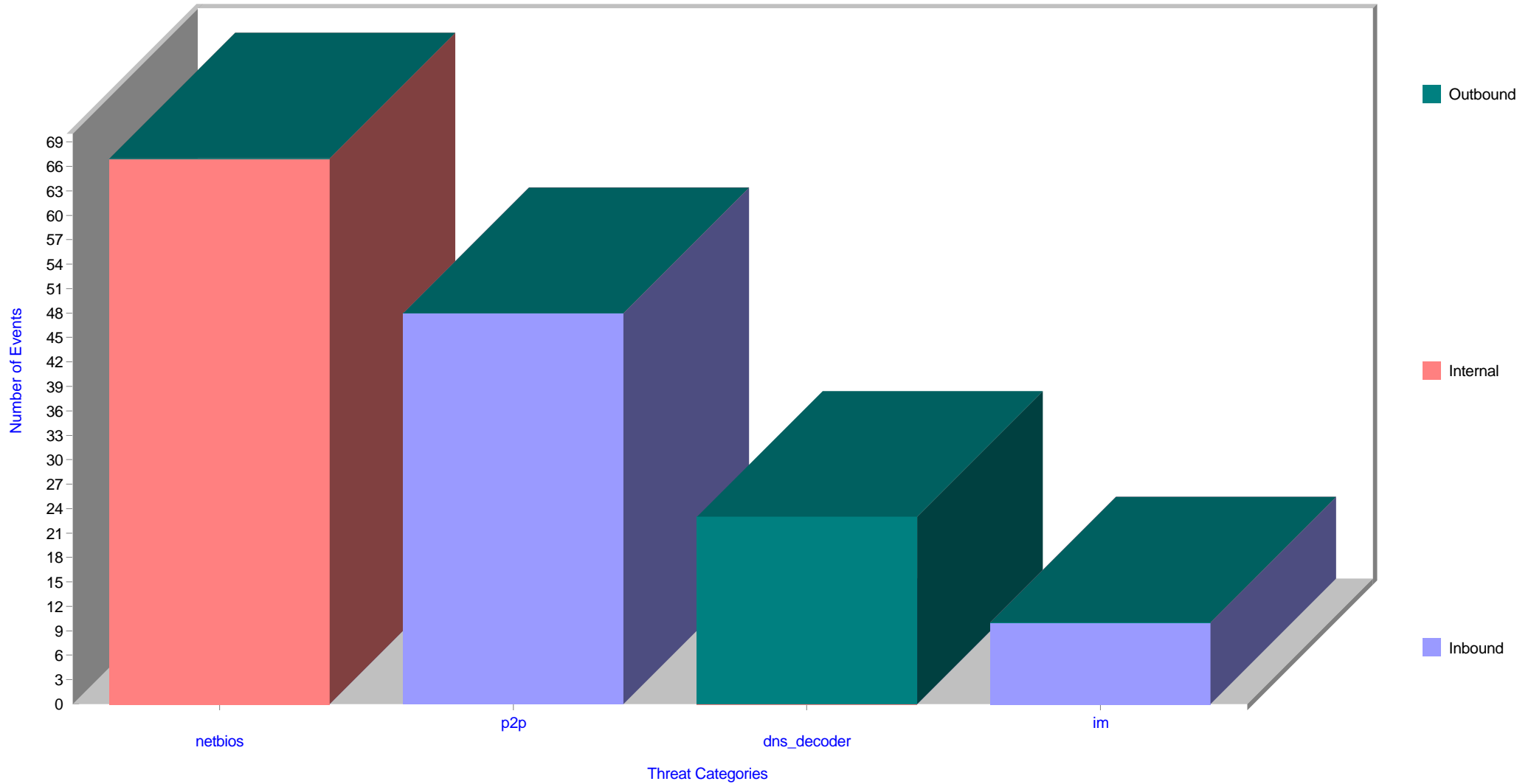


IPS Potential Threat Categories Detected - Graph

Sunday April 17, 2005



Top 5 Threat Categories Detected Sorted by the Total Number of Potential Threats.





Top 5 Threat Categories Detected with their Top 5 Threats

Sunday April 17, 2005



| Threat Category | Signature | Potential Threat Description | Inbound | Internal | Outbound | Total Threats |
|----------------------------------|--------------|---|-----------|-----------|-----------|---------------|
| | | | | | | |
| netbios | | | | 67 | | 67 |
| | FGT102039613 | SMB.DCERPC.Registry.OpenHKLM.139 | | 64 | | 64 |
| | FGT102039618 | SMB.DCERPC.SamrEnumerateAliasesInDomain.139 | | 3 | | 3 |
| p2p | | | 48 | | | 48 |
| | FGT109051907 | edonkey | 48 | | | 48 |
| dns_decoder | | | | | 23 | 23 |
| | FGT8912898 | invalid_pointer | | | 10 | 10 |
| | FGT8912909 | invalid_param | | | 10 | 10 |
| | FGT8912906 | invalid_opcode | | | 3 | 3 |
| im | | | 10 | | | 10 |
| | FGT108855298 | msn | 10 | | | 10 |
| Total for the above list: | | | 58 | 67 | 23 | 148 |