www.glesec.com
GLESEC
Your Global e-security Partner

MONTHLY SECURITY REPORT

PREPARED FOR: METROBANK

DECEMBER 2012

ABOUT THIS REPORT

The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the systems under contract. The information generated by these systems is then aggregated, correlated and analyzed. The more complete the set of systems under contract the more accurate and complete the results will be. The report is organized to provide an executive summary with recommendations (as necessary or applicable) followed by more detailed information.

Index

1. About this report

We at GLESEC believe information security is a holistic and dynamic process. This process requires on-going research and follow up. Holistic since no single “device” can provide the security necessary for an organization. Technology alone cannot provide the security necessary, but people that understand the operations and information generated by the security devices are a key to proper security. The process is dynamic since due to the nature of Internet security given the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase of malware, phishing, organized crime, and hacktivism is the very cause of this of information security exposure phenomena.

2. Confidentiality

GLESEC considers the confidentiality of client’s information as a trade-secret. The information in this context is classified as:

a) Client name and contact information
b) System architecture, configuration, access methods and access control
c) Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

3. Executive Summary

This report corresponds to the period from DECEMBER 1, 2012 to DECEMBER 31, 2012

Based on the information gathered from the DefensePro during this period 13,350 attacks on METROBANK, 207 of which were considered critical were all stopped by the Radware DefensePro 508. During the previous period, 14,878 attacks on METROBANK, 34 of which were considered critical were all stopped by the Radware DefensePro 508. The overall quantity of attacks were similar to the previous period although the critical attacks had a important gain.

GLESEC discovered a large number of Brute Force Web, DNS, and SMB attacks. TCP, Web, UDP, and SIP Scanning attempts were also frequent. The Scanning attempts were highly concentrated with origins in Asia, specifically from China. Intrusion Rules, Anti Scanning, Signature and Cracking Protection assisted in preventing attacks directed at server and network level. GLESEC discovered attacks directed at well-known port numbers: 1433 (microsoft-sql-server), 23 (telnet), 3306 (mysql), 22 (ssh), 5060 (sip), 3389 (rdp/ms wbt server), 8080 (http-alt), 5900 (vnc), 80 (http), 445 (microsoft-ds), 443 (https), and 53 (dns) in order of frequency.

Flood attacks such as HTTP Page Flood, Network Flood utilizing IPv4 UDP attacks were observed this period. Rate Limiting, Behavioral DoS, DoS Protection and Signature Protection assisted in mitigating these attack vectors.

Some Packet Anomalies are being observed, triggering the device to block anomalous traffic. This is caused by attacks or evasion tactics directed at the firewall in order to bypass its function and scan the internal network or in order to collapse the underlying network infrastructure, this can also be caused by applications that do not adhere to RFC standards.

4. Recommendations

GLESEC recommends for METROBANK to review the following Critical Controls: 3, 4, 5, 6 in response to Brute Forcing (Cracking Protection) and Scanning (Anti Scanning) attempts viewed in this period. Specifically adding a Vulnerability Management Service coupled with a METROBANK remediation policy would significantly decrease the attack surface, avoiding script-kiddies and automated attacks such as those observed originating from China.

GLESEC also suggests reviewing the SIP infrastructure as it is attacked consistently from month to month.

GLESEC also recommends METROBANK utilize the **Twenty Critical Security Controls for Effective Cyber Defense** that were formulated as a joint effort from the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. These are readily available from SANS and GLESEC has included the links to the information below:

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response Capability
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

GLESEC offers many services and products that would assist in securing METROBANK to a greater degree. Some of our services are included in the section that follows. If interested in additional information about our offerings please contact info@glesec.com

5. Scope of this Report

The systems/services under this contract include:

Risk and Application	Countermeasures	GLESEC Services	Contracted
External layer security	Firewall	MSS-FW	No
External Layer Security	**Intrusion Prevention, DoS, NBA, Zero Day**	**MSS-APS**	**Yes**
Application Layer Security	**Application Firewall**	**MSS-APS**	**Yes**
Vulnerability Management	Vulnerability Management	MSS-VM	No
Internal Layered Security	End-Point Security	MSS-EPS	No
Centralized Alerting, Reporting and Intelligence	SIEM	MSS-SIEM	No
External and Internal Layer – Basic Infrastructure	DNS and IPAM	MSS-DNS	No
High Availability	Load Balancers – Links	SSP	No
High Availability	Load Balancers - Servers	SSP	No

GLESEC Services:

MSS: Managed Security Service (full outsourcing)

SSP: Security Support Program (systems management and support)

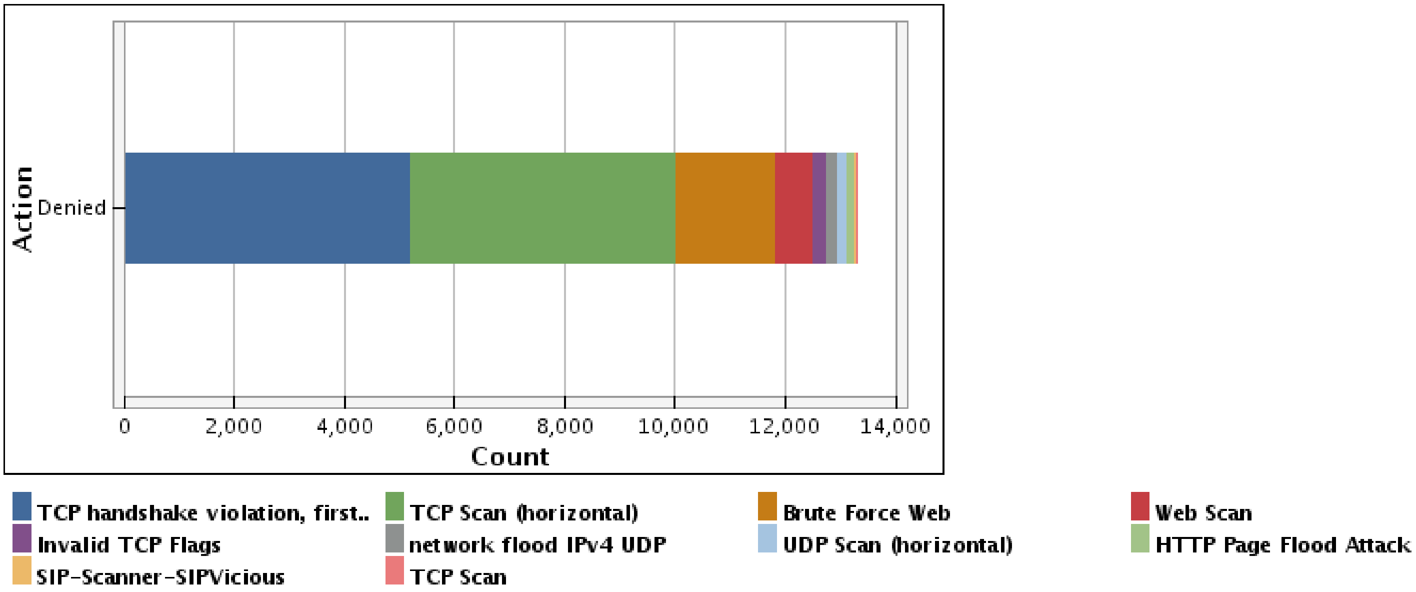
METROBANK Systems: Radware DefensePro 508

METROBANK Systems: Radware AppWall

6. Detailed Security Report

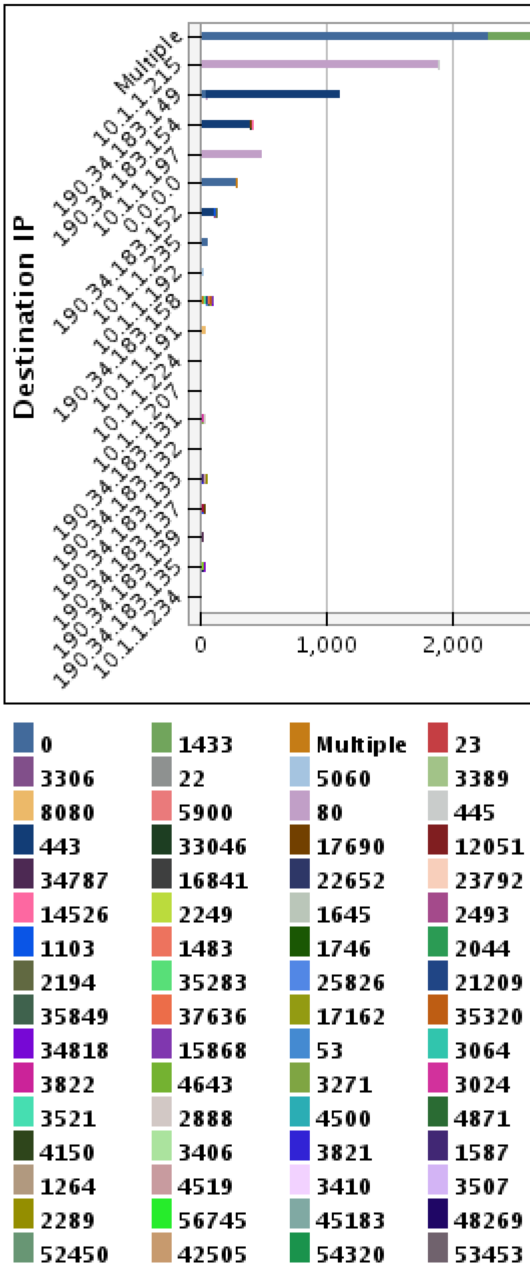
Graph: Attacks Allowed and Denied

This report provides the count of total allowed and denied attacks along with network security rule.



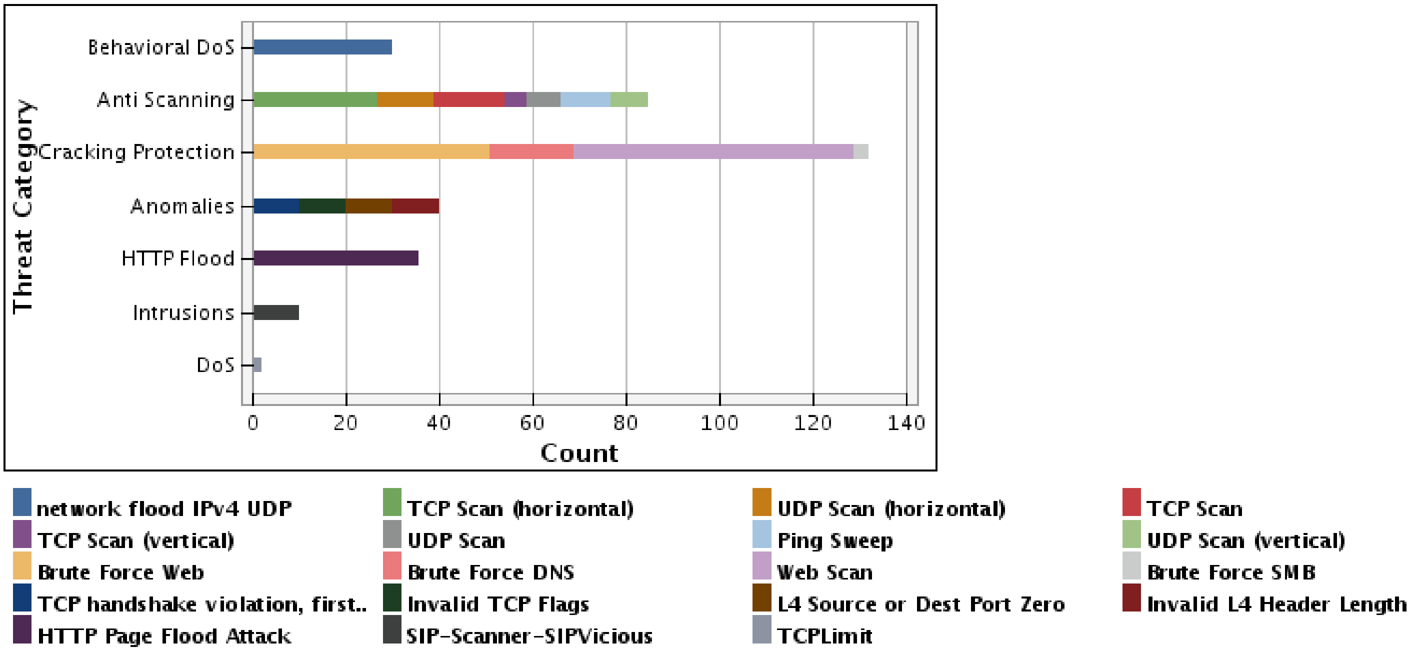
Graph: Attacks by Destination and Port

This report provides information on the total number of attacks that were attempted on which target device and port and for how many times, along with the attack name, network security rule.



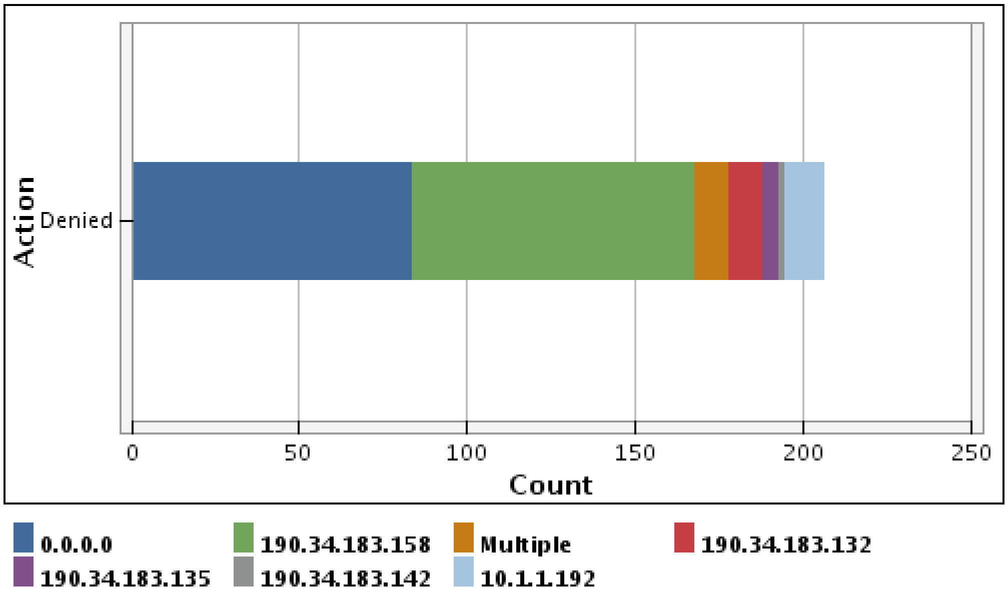
Graph: Attacks By Threat Category

This report lists the attacks per Attack Category, listing the attack name, network security rule.



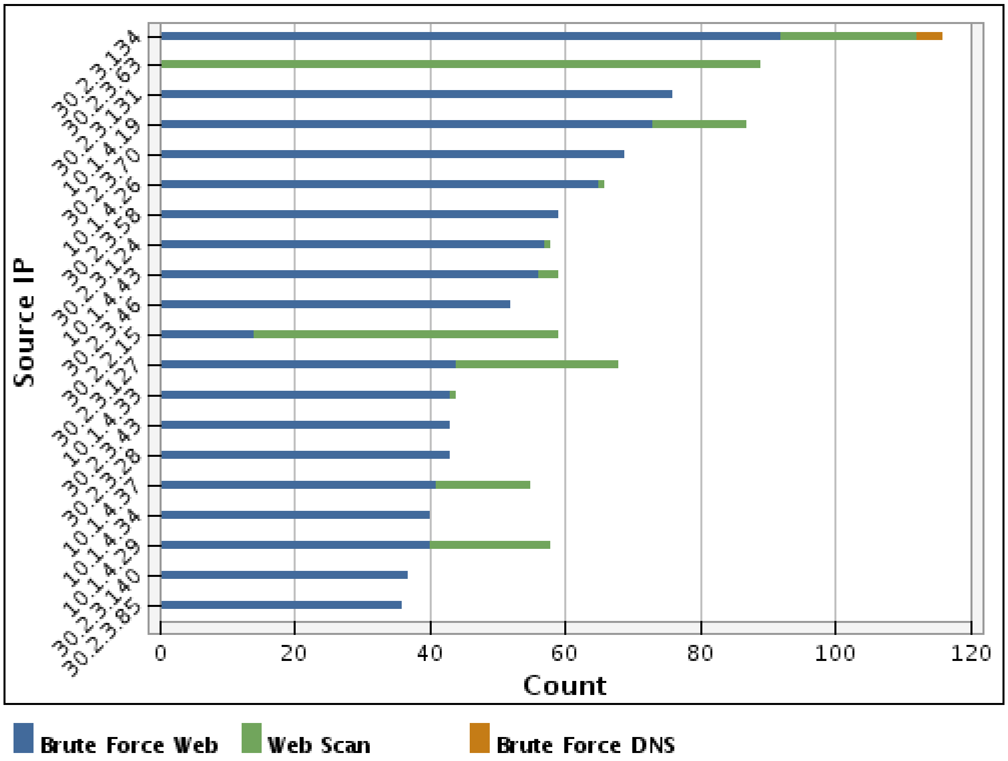
Graph: Critical Attacks

This report provides Critical Attacks information, which includes the destination on which the attack was targeted, the source from where the critical attack originated, port, attack name, network security rule along with the number of times the attack was launched.



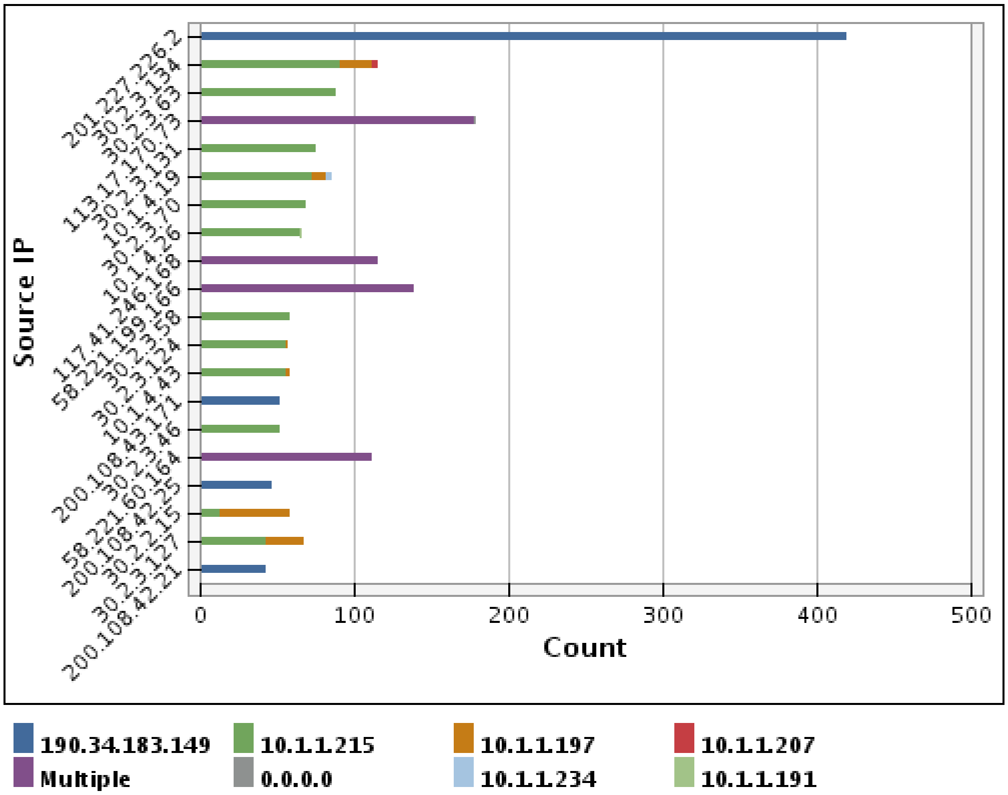
Graph: Internal Attacks by Sources

You can view information on the attacks, the internal source that was responsible for the attack, attack name, network security rule along with the total number of times the attack was launched.



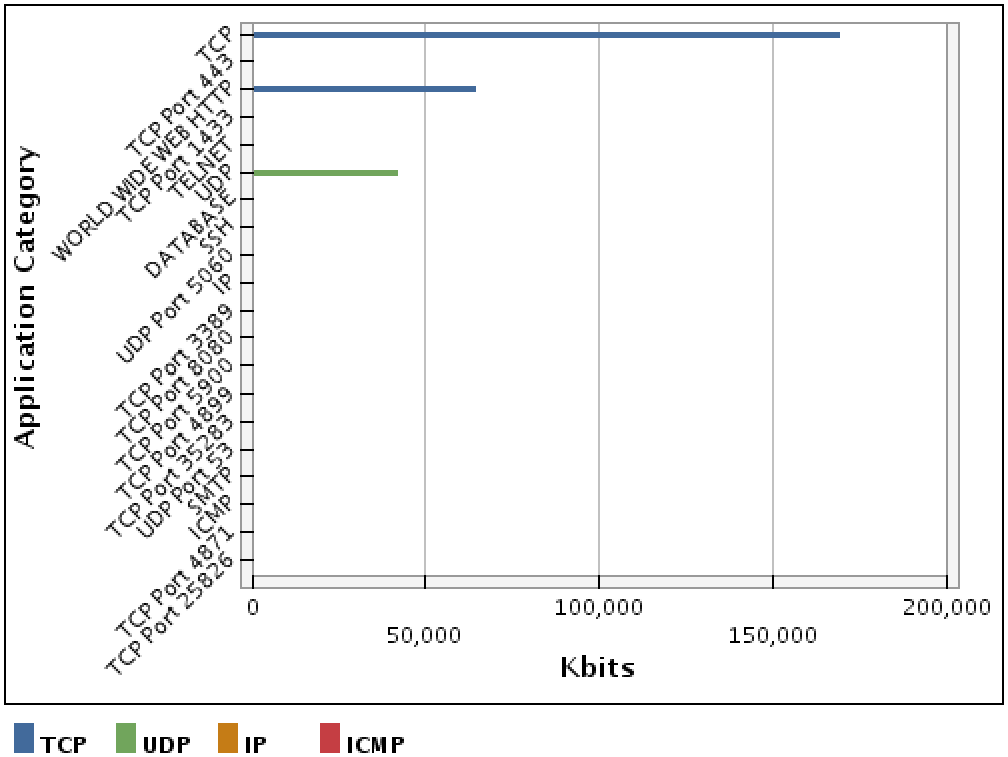
Graph: Top Attack Sources Blocked

This report provides information on the top sources that were blocked on the DP IPS and from where the attacks had originated. This report also shows the destination on which the attack was targeted, its destination port along with the network security rule.



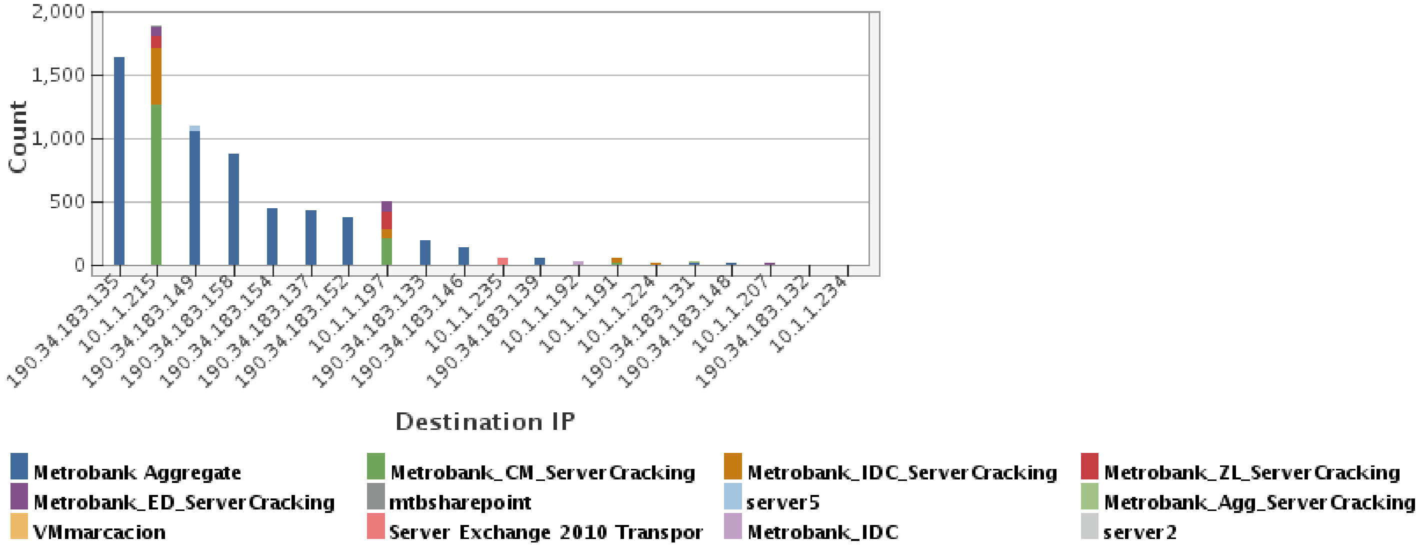
Graph: Top Attacked Applications

This report provides information on the most popular protocol families (or application categories) like web (http, https), e-mail (smtp, pop3)... and their respective child protocols. It also shows the port used by the protocol, the network security rule and the details of number of hits for each protocol family (or application category).



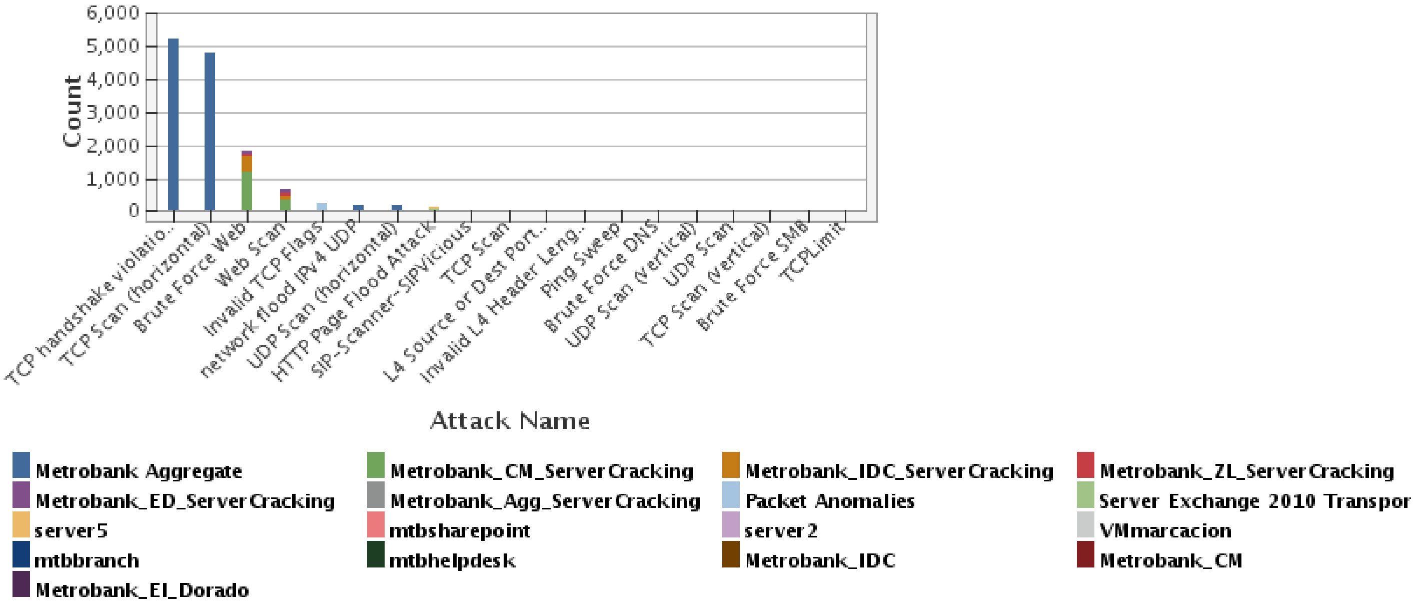
Graph: Top Attacked Destinations

This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



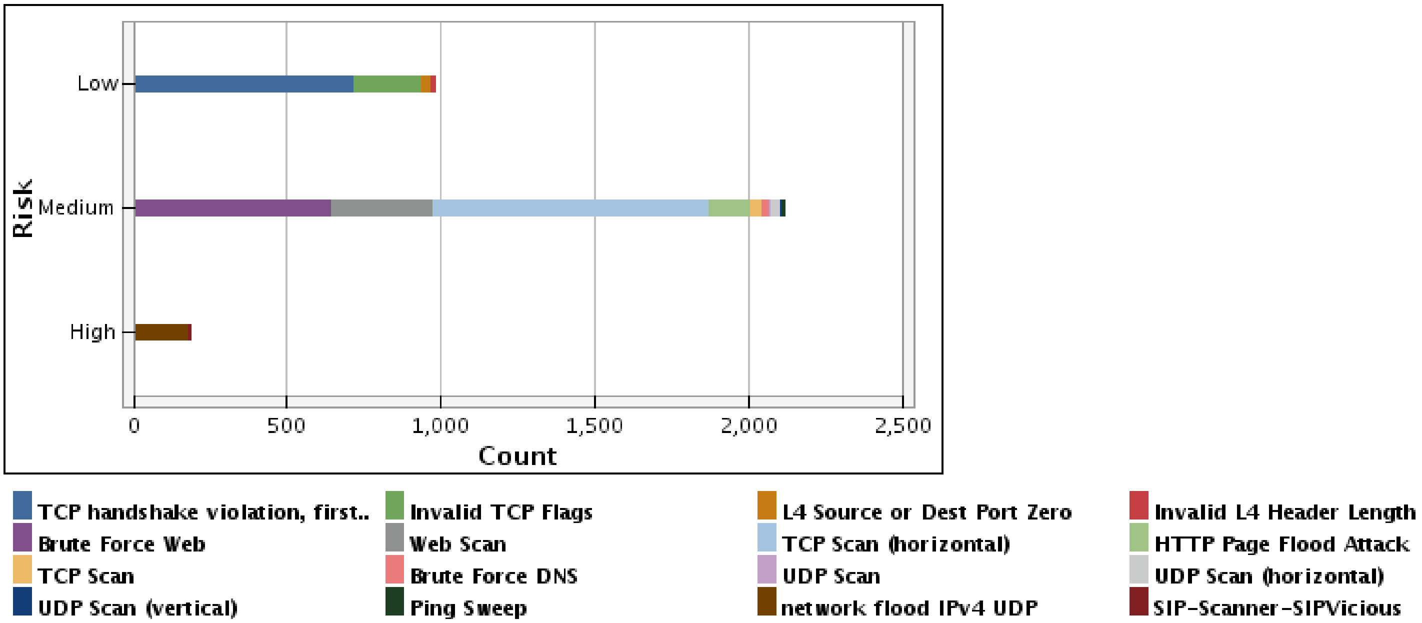
Graph: Top Attacks

This report provides information on the total number of top attacks attempted, the attack name, network security rule and the total number of attacks that triggered with this combination.



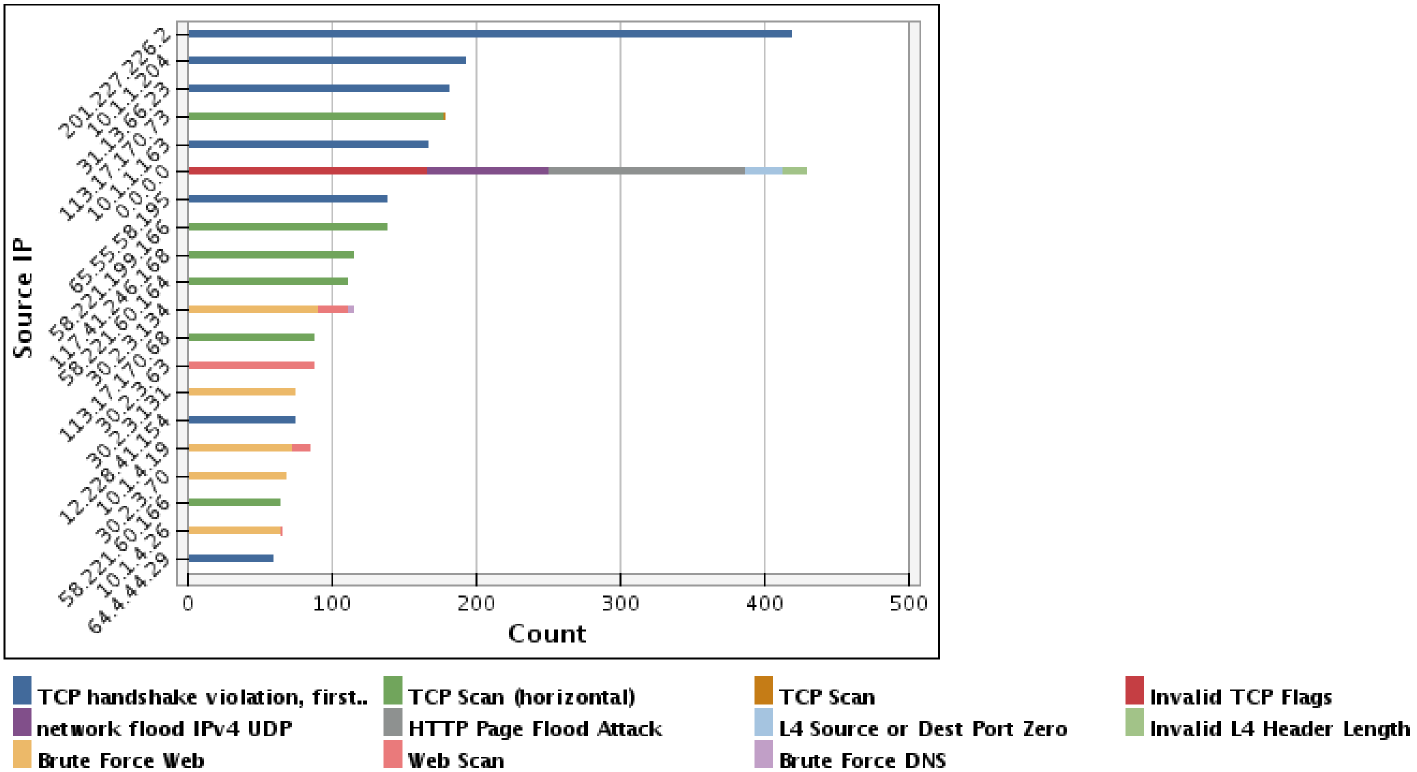
Graph: Top Attacks Blocked By Risk

This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack, attack name, source, destination, the destination port, network security rules are shown.



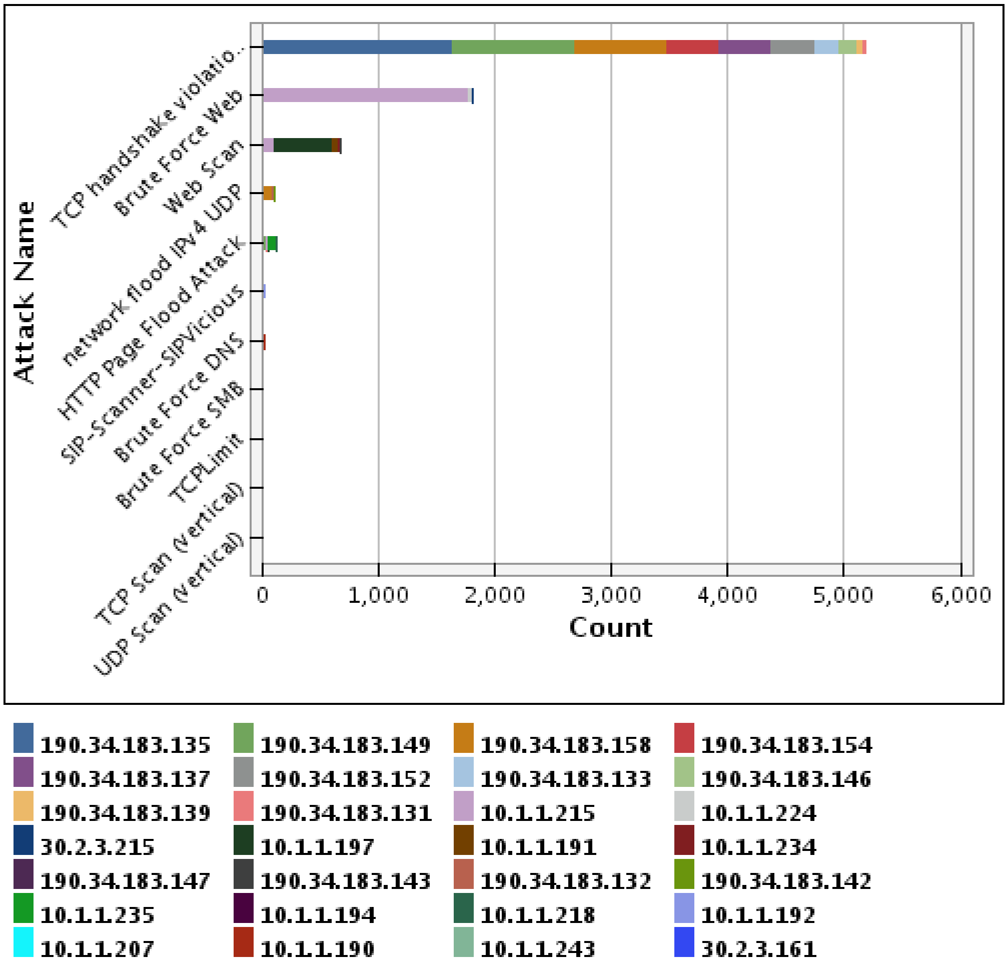
Graph: Top Attacks by Source

This report provides information on the top attacks attempted, categorized by attacks for each source that was the source of attacks along with the attack name, network security rule and the number of attacks that triggered with this combination.



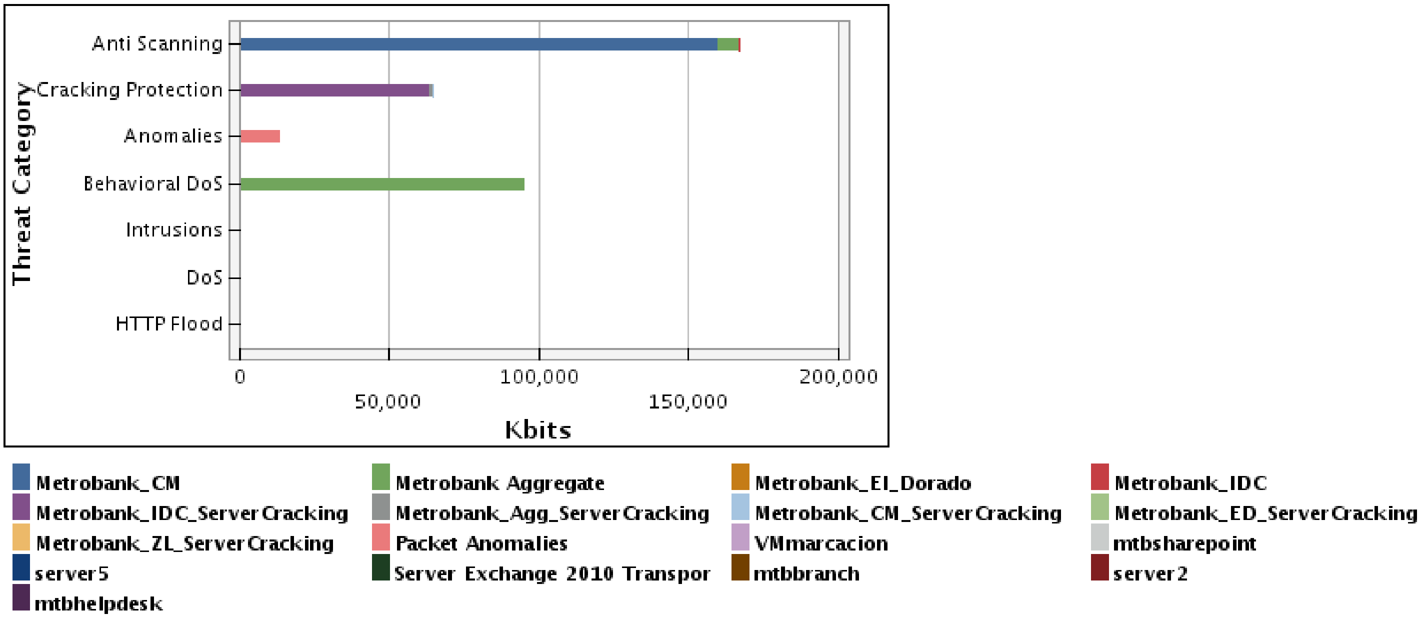
Graph: Top Destinations by Attack

This report provides information on the attacks attempted for the most number of times on the destination protected system IPs along with the network security rule.



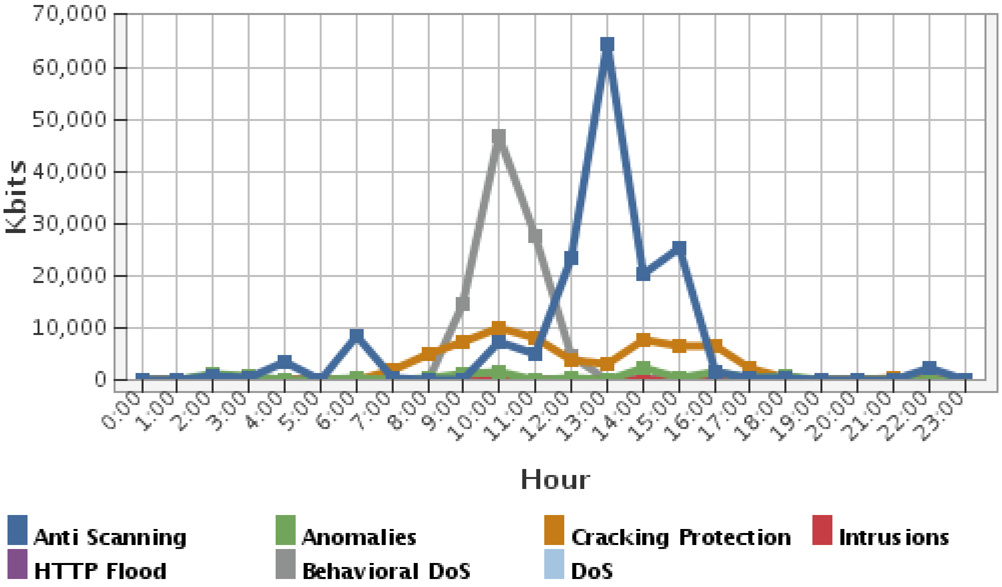
Graph: Attack Categories by Bandwidth

This report shows the attack categories based on the BW of the attacks sharing the same category including Packets and Bits (Kbits). This report also shows the network security rule for each of the attack categories.



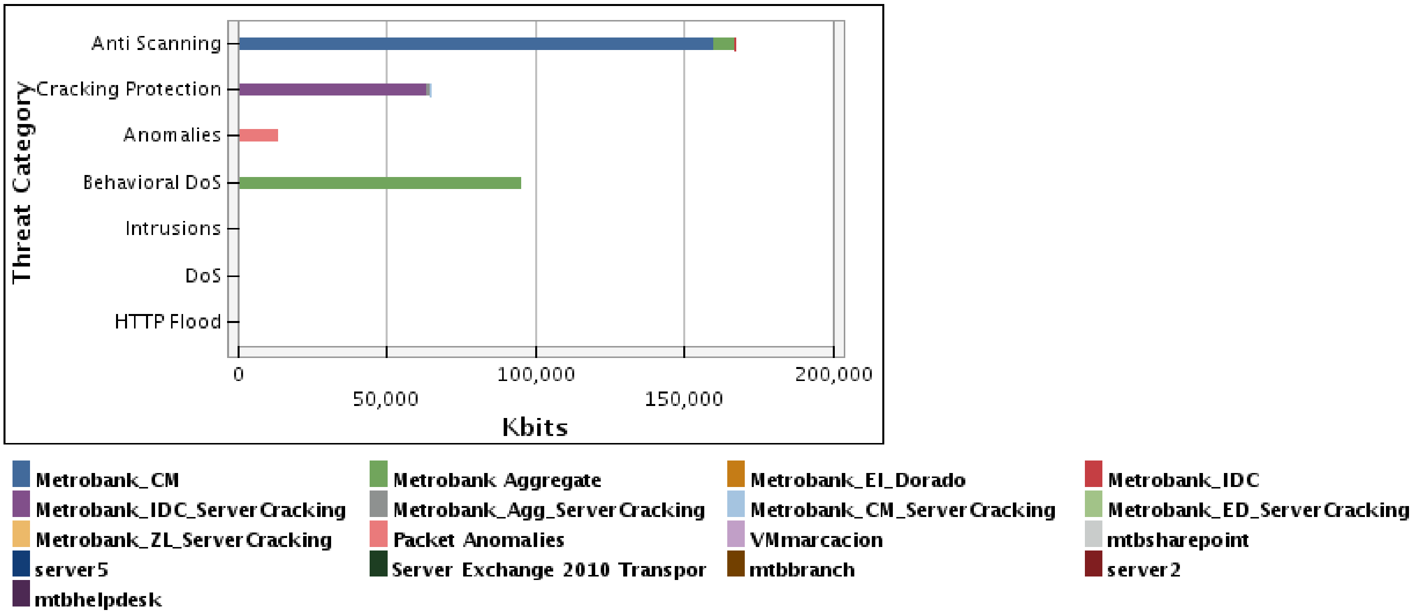
Graph: Bandwidth by Threat Category by Hour of Day

This report shows the most bandwidth (BW) consuming threat categories based on the bandwidth (BW) of the attacks sharing the same threat category including Packets and Bits (Kbits) for each hour of day. This report also shows the network security rule and threat categories.



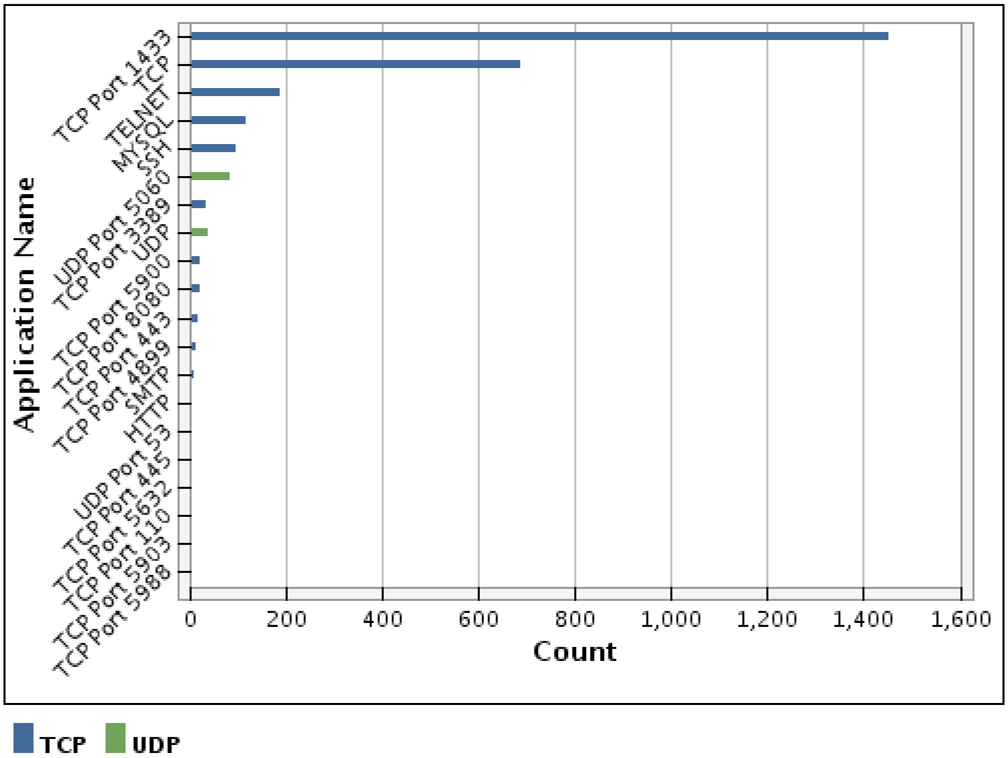
Graph: Top Attacks by Bandwidth

This report shows the most bandwidth (BW) consuming attacks based on the BW of the attack including Packets and Bits (Kbits). This report also shows the network security rule and for each attack.



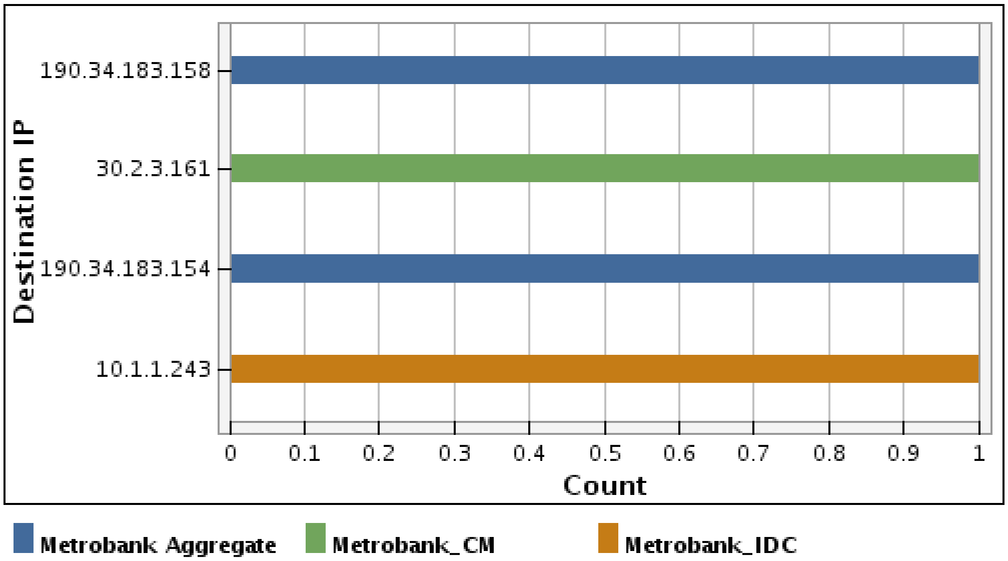
Graph: Top Probed Applications

This report shows historical view of the TOP probed L4 ports (mapped to L7 application name) that were being scanned along with the network security rule.



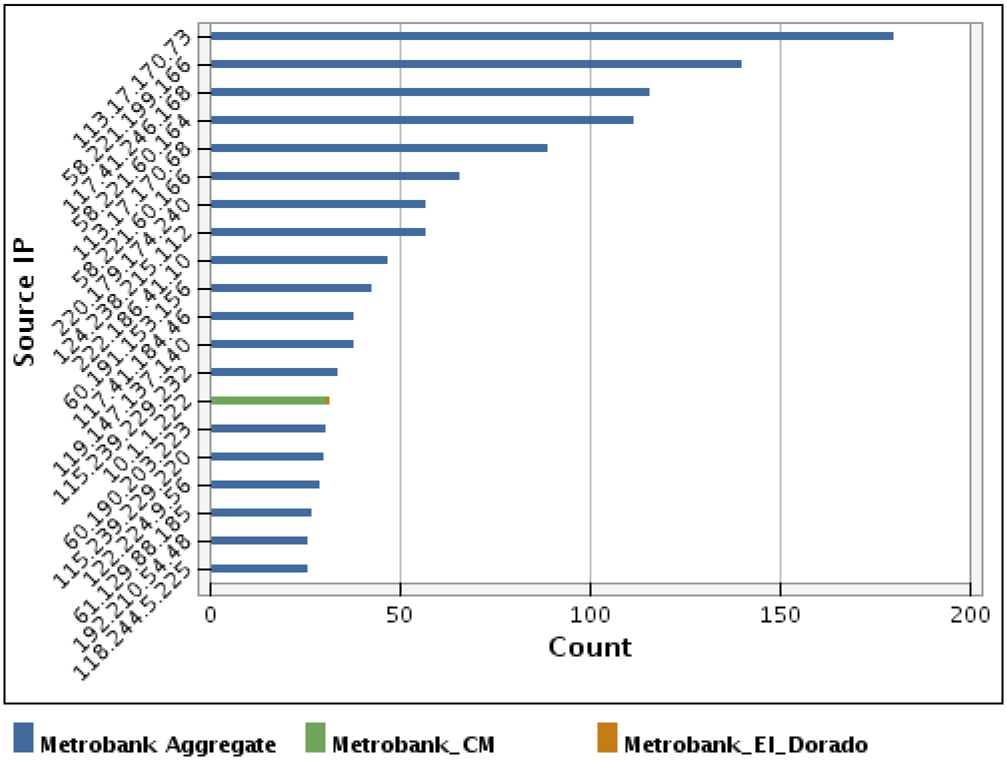
Graph: Top Probed IP Addresses

This report shows historical view of the TOP probed IP addresses that were being scanned along with the network security rule.



Graph: Top Scanners (Source IP Addressed)

This report shows historical view of the TOP source IP addresses that have scanned the network by network scanning activities along with the network security rule.



NOTE: See Appendix 1 – Top Scanners (Source IP Addressed) (WHOIS Information)

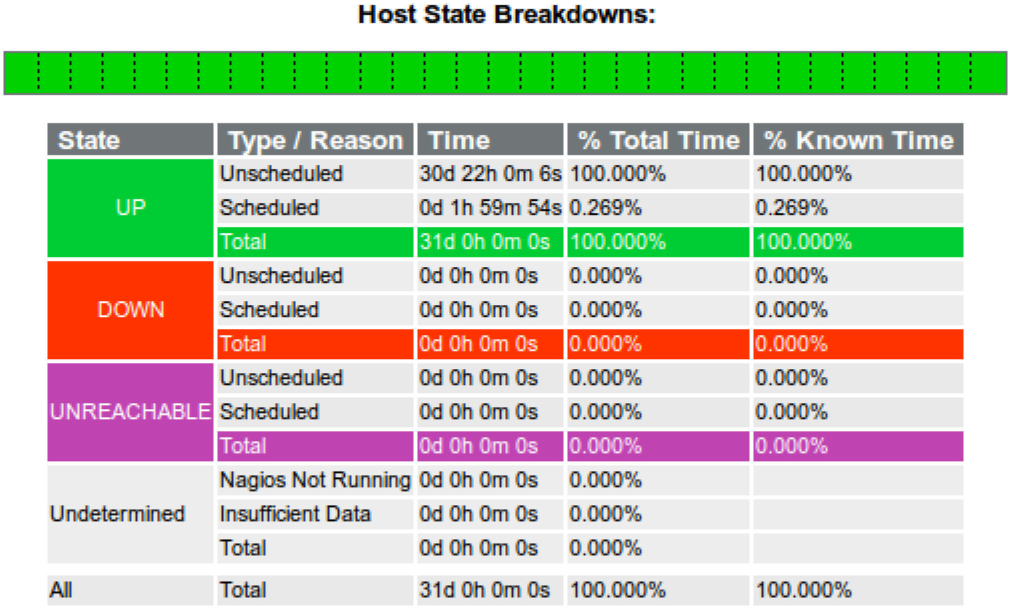
7. Detailed Security Operations Systems Report

This section of the report represents the activities performed by GLESEC’s Global Operations Center. These include:

a) Monitoring of system availability

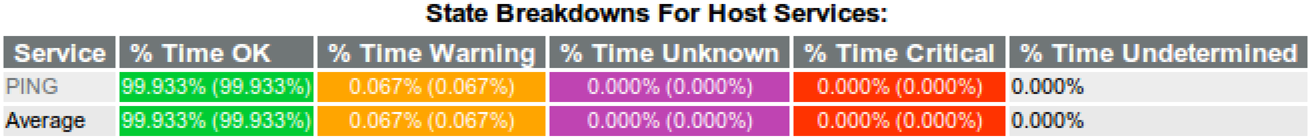
METROBANK DefensePro Availability:

The DefensePro was considered up and available 100% of time of time during this report period.



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 22h 0m 6s	100.000%	100.000%
	Scheduled	0d 1h 59m 54s	0.269%	0.269%
	Total	31d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 0h 0m 0s	100.000%	100.000%



State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.933% (99.933%)	0.067% (0.067%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	99.933% (99.933%)	0.067% (0.067%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

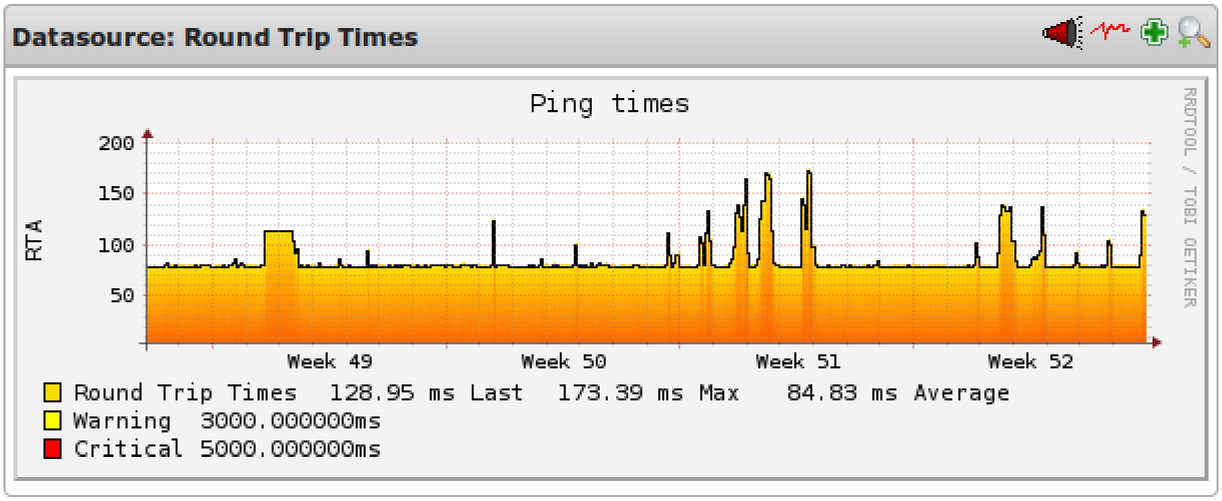
b) Monitoring system performance

METROBANK DefensePro Host Performance:

Round trip ping times averaged 84.83 ms from the GLESEC GOC to METROBANK with 0% average packet loss

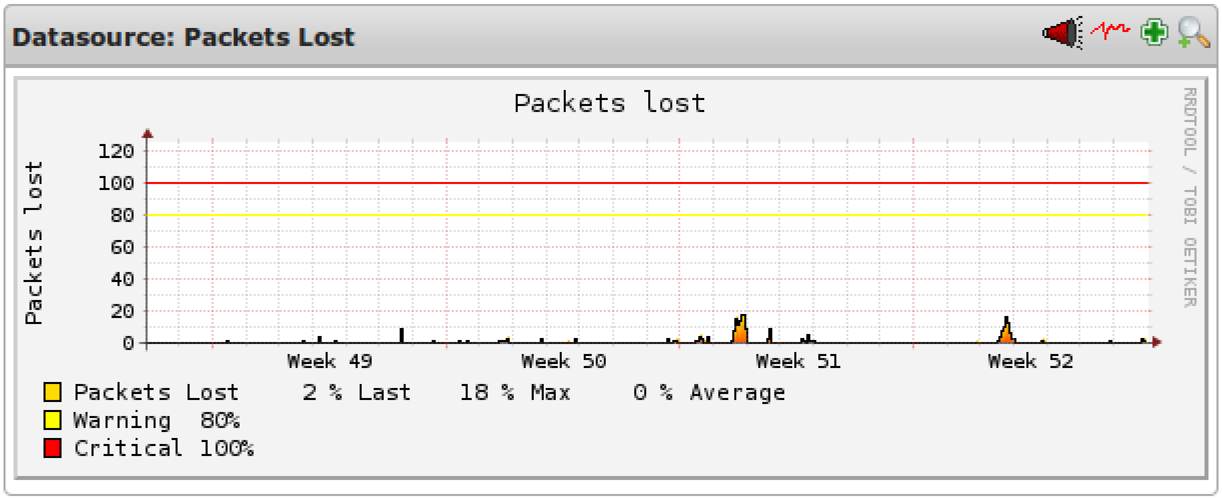
Host: MetroBank DefensePro 508 **Service:** Host Perfdata

Custom time range 01.12.12 0:00 - 31.12.12 0:00



Datasource: Round Trip Times

```
🟨 Round Trip Times   128.95 ms Last   173.39 ms Max    84.83 ms Average
🟨 Warning  3000.000000ms
🟥 Critical 5000.000000ms
```



Datasource: Packets Lost

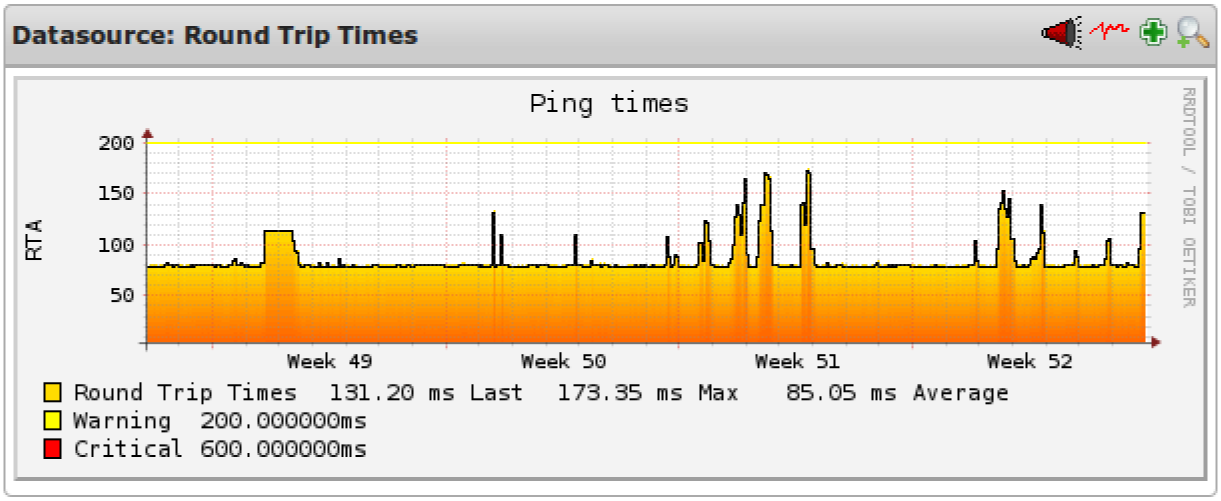
```
🟨 Packets Lost    2 % Last    18 % Max     0 % Average
🟨 Warning  80%
🟥 Critical 100%
```

METROBANK DefensePro Ping Performance:

Round trip ping times averaged 73.67 ms from the GLESEC GOC to METROBANK with 0% average packet loss

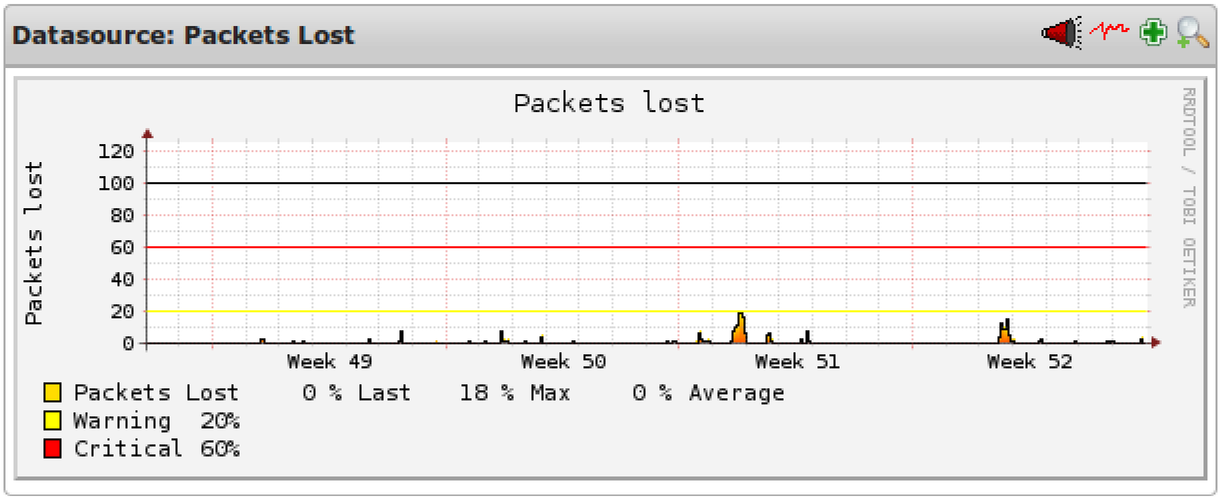
Host: MetroBank DefensePro 508 **Service:** PING

Custom time range 01.12.12 0:00 - 31.12.12 0:00



Datasource: Round Trip Times

🟨 Round Trip Times 131.20 ms Last 173.35 ms Max 85.05 ms Average
🟨 Warning 200.000000ms
🟥 Critical 600.000000ms



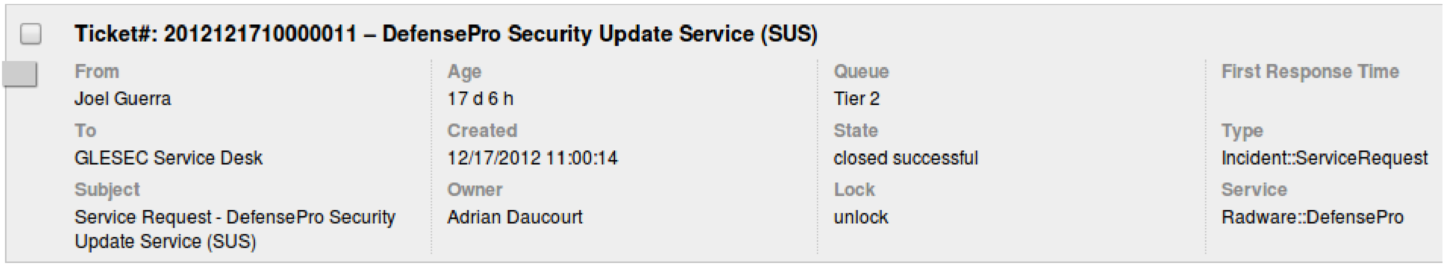
Datasource: Packets Lost

🟨 Packets Lost 0 % Last 18 % Max 0 % Average
🟨 Warning 20%
🟥 Critical 60%

c) Change management procedures

METROBANK Change Management: N/A

One request for this period was opened to verify that automatic updates for the Radware Security Update Service were successfully applied.



□ **Ticket#: 2012121710000011 – DefensePro Security Update Service (SUS)**

From	Age	Queue	First Response Time
Joel Guerra	17 d 6 h	Tier 2	
To	Created	State	Type
GLESEC Service Desk	12/17/2012 11:00:14	closed successful	Incident::ServiceRequest
Subject	Owner	Lock	Service
Service Request - DefensePro Security Update Service (SUS)	Adrian Daucourt	unlock	Radware::DefensePro

d) Incident Response procedures

METROBANK Incident Report: N/A

8. Appendix 1 - Top Scanners (Source IP Addressed) WHOIS Information

This section provides additional WHOIS detail for the **Graph: Top Scanners (Source IP Addressed)**

```
inetnum:      113.16.0.0 - 113.17.255.255
netname:      CHINANET-GX
descr:      CHINANET GUANGXI PROVINCE NETWORK
descr:      China Telecom
descr:      No.31,jingrong street
descr:      Beijing 100032
country:     CN
admin-c:     CH93-AP
tech-c:     CR766-AP
status:     ALLOCATED PORTABLE
changed:      hm-changed@apnic.net 20080918
mnt-by:      APNIC-HM
mnt-lower:    MAINT-CHINANET-GX
source:      APNIC
role:       CHINANET GUANGXI
address:      No.35,Minzhu Road,Nanning 530015
country:     CN
phone:      +86-771-2815987
fax-no:     +86-771-2839278
e-mail:     hostmaster@gx163.net
admin-c:     CR76-AP
tech-c:     BD37-AP
nic-hdl:     CR766-AP
notify:     hostmaster@gx163.net
mnt-by:      MAINT-CHINANET-GX
changed:      hostmaster@gx163.net 20021024
source:      APNIC
changed:      hm-changed@apnic.net 20111114
person:      Chinanet Hostmaster
nic-hdl:     CH93-AP
e-mail:     anti-spam@ns.chinanet.cn.net
address:      No.31 ,jingrong street,beijing
address:      100032
phone:      +86-10-58501724
fax-no:     +86-10-58501724
country:     CN
changed:      dingsy@cndata.com 20070416
mnt-by:      MAINT-CHINANET
source:      APNIC
```

```
inetnum:      113.16.0.0 - 113.17.255.255
netname:      CHINANET-GX
descr:      CHINANET GUANGXI PROVINCE NETWORK
descr:      China Telecom
descr:      No.31,jingrong street
descr:      Beijing 100032
country:     CN
```

```
admin-c:       CH93-AP
tech-c:        CR766-AP
status:        ALLOCATED PORTABLE
changed:       hm-changed@apnic.net 20080918
mnt-by:        APNIC-HM
mnt-lower:     MAINT-CHINANET-GX
source:        APNIC
role:          CHINANET GUANGXI
address:       No.35,Minzhu Road,Nanning 530015
country:       CN
phone:         +86-771-2815987
fax-no:        +86-771-2839278
e-mail:        hostmaster@gx163.net
admin-c:       CR76-AP
tech-c:        BD37-AP
nic-hdl:       CR766-AP
notify:        hostmaster@gx163.net
mnt-by:        MAINT-CHINANET-GX
changed:       hostmaster@gx163.net 20021024
source:        APNIC
changed:       hm-changed@apnic.net 20111114
person:        Chinanet Hostmaster
nic-hdl:       CH93-AP
e-mail:        anti-spam@ns.chinanet.cn.net
address:       No.31 ,jingrong street,beijing
address:       100032
phone:         +86-10-58501724
fax-no:        +86-10-58501724
country:       CN
changed:       dingsy@cndata.com 20070416
mnt-by:        MAINT-CHINANET
source:        APNIC

inetnum:       115.239.228.0 - 115.239.231.255
netname:       NINBO-LANZHONG-LTD
country:       CN
descr:         Ninbo Lanzhong Network Ltd
descr:
admin-c:       TD222-AP
tech-c:        CS64-AP
status:        ASSIGNED NON-PORTABLE
changed:       auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:        MAINT-CN-CHINANET-ZJ-SX
source:        APNIC
role:          CHINANET-ZJ Shaoxing
address:       No.9 Sima Road,Shaoxing,Zhejiang.312000
country:       CN
phone:         +86-575-5136199
fax-no:        +86-575-5114449
e-mail:        anti-spam@mail.sxptt.zj.cn
admin-c:       CH109-AP
```

```
tech-c:        CH109-AP
nic-hdl:       CS64-AP
mnt-by:         MAINT-CHINANET-ZJ
changed:         master@dcb.hz.zj.cn 20031204
source:         APNIC
changed:         hm-changed@apnic.net 20111114
person:         Taichun Du
nic-hdl:       TD222-AP
e-mail:        anti-spam@mail.sxptt.zj.cn
address:        Shaoxing,Zhejiang.Postcode:312000
phone:          +86-574-88311333
country:        CN
changed:         auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:         MAINT-CN-CHINANET-ZJ-SX
source:         APNIC

inetnum:        115.239.228.0 - 115.239.231.255
netname:         NINBO-LANZHONG-LTD
country:        CN
descr:         Ninbo Lanzhong Network Ltd
descr:
admin-c:         TD222-AP
tech-c:        CS64-AP
status:        ASSIGNED NON-PORTABLE
changed:         auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:         MAINT-CN-CHINANET-ZJ-SX
source:         APNIC
role:         CHINANET-ZJ Shaoxing
address:        No.9 Sima Road,Shaoxing,Zhejiang.312000
country:        CN
phone:          +86-575-5136199
fax-no:        +86-575-5114449
e-mail:        anti-spam@mail.sxptt.zj.cn
admin-c:         CH109-AP
tech-c:        CH109-AP
nic-hdl:       CS64-AP
mnt-by:         MAINT-CHINANET-ZJ
changed:         master@dcb.hz.zj.cn 20031204
source:         APNIC
changed:         hm-changed@apnic.net 20111114
person:         Taichun Du
nic-hdl:       TD222-AP
e-mail:        anti-spam@mail.sxptt.zj.cn
address:        Shaoxing,Zhejiang.Postcode:312000
phone:          +86-574-88311333
country:        CN
changed:         auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:         MAINT-CN-CHINANET-ZJ-SX
source:         APNIC
```

```
inetnum:       117.40.0.0 - 117.43.255.255
netname:      CHINANET-JX
descr:        CHINANET Jiangxi province network
descr:        China Telecom
descr:        No.31,jingrong street
descr:        Beijing 100032
country:       CN
admin-c:        CH93-AP
tech-c:       JN113-AP
status:       ALLOCATED PORTABLE
mnt-by:        APNIC-HM
mnt-lower:      MAINT-IP-WWF
mnt-routes:     MAINT-IP-WWF
changed:        hm-changed@apnic.net 20070912
source:        APNIC
role:       JXDCB NET
address:        DATA COMMUNICATION BUREAY
address:        NO.39,YANJIANG NORTH ROAD,NANCHANG,JIANGXI
country:       CN
phone:         +86 791 6730586
fax-no:       +86 791 6707755
e-mail:       hostmaster@public1.nc.jx.cn
admin-c:        XY1-AP
tech-c:       WZ1-CN
tech-c:       WW49-AP
nic-hdl:      JN113-AP
notify:       hostmaster@public1.nc.jx.cn
mnt-by:        MAINT-IP-WWF
changed:        hm-changed@apnic.net 20020812
source:        APNIC
changed:        hm-changed@apnic.net 20111114
person:        Chinanet Hostmaster
nic-hdl:      CH93-AP
e-mail:       anti-spam@ns.chinanet.cn.net
address:        No.31 ,jingrong street,beijing
address:        100032
phone:         +86-10-58501724
fax-no:       +86-10-58501724
country:       CN
changed:        dingsy@cndata.com 20070416
mnt-by:        MAINT-CHINANET
source:        APNIC

inetnum:       117.40.0.0 - 117.43.255.255
netname:      CHINANET-JX
descr:        CHINANET Jiangxi province network
descr:        China Telecom
descr:        No.31,jingrong street
descr:        Beijing 100032
country:       CN
admin-c:        CH93-AP
```

```
tech-c:        JN113-AP
status:        ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:       MAINT-IP-WWF
mnt-routes:      MAINT-IP-WWF
changed:         hm-changed@apnic.net 20070912
source:         APNIC
role:          JXDCB NET
address:        DATA COMMUNICATION BUREAY
address:        NO.39,YANJIANG NORTH ROAD,NANCHANG,JIANGXI
country:        CN
phone:          +86 791 6730586
fax-no:        +86 791 6707755
e-mail:        hostmaster@public1.nc.jx.cn
admin-c:        XY1-AP
tech-c:        WZ1-CN
tech-c:        WW49-AP
nic-hdl:       JN113-AP
notify:        hostmaster@public1.nc.jx.cn
mnt-by:         MAINT-IP-WWF
changed:         hm-changed@apnic.net 20020812
source:         APNIC
changed:         hm-changed@apnic.net 20111114
person:         Chinanet Hostmaster
nic-hdl:       CH93-AP
e-mail:        anti-spam@ns.chinanet.cn.net
address:        No.31 ,jingrong street,beijing
address:        100032
phone:          +86-10-58501724
fax-no:        +86-10-58501724
country:        CN
changed:         dingsy@cndata.com 20070416
mnt-by:         MAINT-CHINANET
source:         APNIC

inetnum:         118.244.0.0 - 118.244.255.255
netname:         TVNET
descr:         Beijing Time-vision Telecommunication
descr:         Technical,Ltd
descr:         No.18 Xibahe Dongli,
descr:         Chaoyang District,Beijing,China
country:        CN
admin-c:        JY1241-AP
tech-c:        JY1241-AP
mnt-by:         MAINT-CNNIC-AP
mnt-irt:       IRT-CNNIC-CN
changed:         ipas@cnnic.cn 20091220
status:        ALLOCATED NON-PORTABLE
source:         APNIC
route:         118.244.0.0/16
descr:         CNC Group CHINA169 Sichuan Province network
```

```
descr:          Addresses from CNNIC(BBnet)
country:        CN
origin:         AS4837
mnt-by:         MAINT-CNCGROUP-RR
changed:        abuse@cnc-noc.net 20080321
source:         APNIC
person:         Justin Yang
address:        No.18 Xibahe Dongli,Chaoyang District ,Beijing P.R.C.
country:        CN
phone:          +86-10-65661862
fax-no:         +86-10-65661862-243
e-mail:         superxi@bj.datadragon.net
nic-hdl:        JY1241-AP
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.net.cn 20070404
source:         APNIC

inetnum:        119.144.0.0 - 119.147.255.255
netname:        CHINANET-GD
descr:          CHINANET Guangdong province network
descr:          Data Communication Division
descr:          China Telecom
country:        CN
admin-c:        CH93-AP
tech-c:         IC83-AP
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20080207
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CHINANET-GD
mnt-routes:     MAINT-CHINANET-GD
source:         APNIC
person:         Chinanet Hostmaster
nic-hdl:        CH93-AP
e-mail:         anti-spam@ns.chinanet.cn.net
address:        No.31 ,jingrong street,beijing
address:        100032
phone:          +86-10-58501724
fax-no:         +86-10-58501724
country:        CN
changed:        dingsy@cndata.com 20070416
mnt-by:         MAINT-CHINANET
source:         APNIC
person:         IPMASTER CHINANET-GD
nic-hdl:        IC83-AP
e-mail:         ipadm@189.cn
address:        NO.1,RO.DONGYUANHENG,YUEXIUNAN,GUANGZHOU
phone:          +86-20-83877223
fax-no:         +86-20-83877223
country:        CN
changed:        ipadm@189.cn 20110418
mnt-by:         MAINT-CHINANET-GD
```

```
abuse-mailbox:  abuse_gdnoc@189.cn
source:         APNIC

inetnum:        122.224.9.0 - 122.224.9.255
netname:        NINBO-LANZHONG-LTD
country:        CN
descr:          Ninbo Lanzhong Network Ltd
descr:
admin-c:        TD231-AP
tech-c:         CS64-AP
status:         ASSIGNED NON-PORTABLE
changed:        auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:         MAINT-CN-CHINANET-ZJ-SX
source:         APNIC
role:           CHINANET-ZJ Shaoxing
address:        No.9 Sima Road,Shaoxing,Zhejiang.312000
country:        CN
phone:          +86-575-5136199
fax-no:         +86-575-5114449
e-mail:         anti-spam@mail.sxptt.zj.cn
admin-c:        CH109-AP
tech-c:         CH109-AP
nic-hdl:        CS64-AP
mnt-by:         MAINT-CHINANET-ZJ
changed:        master@dcb.hz.zj.cn 20031204
source:         APNIC
changed:        hm-changed@apnic.net 20111114
person:         Taichun Du
nic-hdl:        TD231-AP
e-mail:         anti-spam@mail.sxptt.zj.cn
address:        Shaoxing,Zhejiang.Postcode:312000
phone:          +86-574-88311333
country:        CN
changed:        auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:         MAINT-CN-CHINANET-ZJ-SX
source:         APNIC

inetnum:        124.236.0.0 - 124.239.255.255
netname:        CHINANET-HE
descr:          CHINANET hebei province network
descr:          China Telecom
descr:          No.31,jingrong street
descr:          Beijing 100032
country:        CN
admin-c:        BR3-AP
tech-c:         CH93-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CHINANET-HE
mnt-routes:     MAINT-CHINANET-HE
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20060725
```

```
source:        APNIC
person:        Bin Ren
nic-hdl:       BR3-AP
e-mail:        hostmaster@hbtele.com
address:       NO.69 KunLun avenue, Shijiazhuang 050000 China
phone:         +86-311-85211771
fax-no:        +86-311-85202145
country:       CN
changed:       renbin@hbtele.com 20060606
mnt-by:        MAINT-CHINANET-HE
source:        APNIC
person:        Chinanet Hostmaster
nic-hdl:       CH93-AP
e-mail:        anti-spam@ns.chinanet.cn.net
address:       No.31 ,jingrong street,beijing
address:       100032
phone:         +86-10-58501724
fax-no:        +86-10-58501724
country:       CN
changed:       dingsy@cndata.com 20070416
mnt-by:        MAINT-CHINANET
source:        APNIC
```

NetRange: 192.210.48.0 - 192.210.63.255

```
CIDR:          192.210.48.0/20
OriginAS:      AS40676
NetName:       PSYCHZ-NETWORKS
NetHandle:     NET-192-210-48-0-1
Parent:        NET-192-0-0-0-0
NetType:       Direct Allocation
RegDate:       2012-09-27
Updated:       2012-09-27
Ref:           http://whois.arin.net/rest/net/NET-192-210-48-0-1
OrgName:       Psychz Networks
OrgId:         PSL-86
City:          Walnut
StateProv:     CA
PostalCode:    91789
Country:       US
RegDate:       2008-02-20
Updated:       2012-11-19
Ref:           http://whois.arin.net/rest/org/PSL-86
ReferralServer: rwhois://rwhois.psychz.net:4321
OrgAbuseHandle: NOC3077-ARIN
OrgAbuseName:   NOC
OrgAbusePhone:  +1-626-549-2801
OrgAbuseEmail:  noc@psychz.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/NOC3077-ARIN
OrgNOCHandle: NOC3077-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-626-549-2801
```

```
OrgNOCEmail:  noc@psychz.net
OrgNOCRef:    http://whois.arin.net/rest/poc/NOC3077-ARIN
OrgTechHandle: NOC3077-ARIN
OrgTechName:   NOC
OrgTechPhone:  +1-626-549-2801
OrgTechEmail:  noc@psychz.net
OrgTechRef:    http://whois.arin.net/rest/poc/NOC3077-ARIN
Found a referral to rwhois.psychz.net:4321.
autharea=192.210.54.0/24
xautharea=192.210.54.0/24
network:Class-Name:network
network:Auth-Area:192.210.54.0/24
network:ID:NET-12816.192.210.54.32/27
network:Network-Name:192.210.54.32/27
network:IP-Network:192.210.54.32/27
network:IP-Network-Block:192.210.54.32 - 192.210.54.63
network:Org-Name:vpsks
network:Street-Address:中国辽宁省沈阳市
network:City: 沈阳市
network:State:辽宁省
network:Postal-Code:110000
network:Country-Code:CN
network:Tech-Contact:MAINT-12816.192.210.54.32/27
network:Created:20121102000012000
network:Updated:20121102000012000
network:Updated-By:abuse@psychz.net
contact:POC-Name:Network Administrator
contact:POC-Email:abuse@psychz.net
contact:POC-Phone:
contact:Tech-Name:Network Administrator
contact:Tech-Email:abuse@psychz.net
contact:Tech-Phone:
```

inetnum: 220.178.0.0 - 220.180.255.255

```
netname:        CHINANET-AH
country:        CN
descr:          CHINANET anhui province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
admin-c:        CH93-AP
tech-c:         AT318-AP
status:         ALLOCATED non-PORTABLE
changed:        wanglinlin2@anhuitelecom.com 20060317
mnt-by:         MAINT-CHINANET
source:         APNIC
role:           ANHUI TELECOM
address:        305 Changjiang West Road
address:        Hefei Anhui China
country:        CN
phone:          +86 0551 5185089
```

```
fax-no:         +86 0551 5185500
e-mail:         wanglinlin2@anhuitelecom.com
admin-c:          LW604-AP
tech-c:         LW604-AP
nic-hdl:        AT318-AP
notify:         wanglinlin2@anhuitelecom.com
mnt-by:          MAINT-CHINANET-AH
changed:          wanglinlin2@anhuitelecom.com 20060323
source:         APNIC
changed:          hm-changed@apnic.net 20111114
person:          Chinanet Hostmaster
nic-hdl:        CH93-AP
e-mail:         anti-spam@ns.chinanet.cn.net
address:          No.31 ,jingrong street,beijing
address:          100032
phone:           +86-10-58501724
fax-no:         +86-10-58501724
country:         CN
changed:          dingsy@cndata.com 20070416
mnt-by:          MAINT-CHINANET
source:         APNIC
```

```
inetnum:        222.184.0.0 - 222.191.255.255
netname:          CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
country:         CN
admin-c:          CH93-AP
tech-c:         CJ186-AP
mnt-by:          APNIC-HM
mnt-lower:        MAINT-CHINANET-JS
mnt-routes:       MAINT-CHINANET-JS
changed:          hm-changed@apnic.net 20040223
status:         ALLOCATED PORTABLE
source:         APNIC
role:          CHINANET JIANGSU
address:          260 Zhongyang Road,Nanjing 210037
country:         CN
phone:           +86-25-86588231
phone:           +86-25-86588745
fax-no:         +86-25-86588104
e-mail:         ip@jsinfo.net
admin-c:          CH360-AP
tech-c:         CS306-AP
tech-c:         CN142-AP
nic-hdl:        CJ186-AP
notify:         ip@jsinfo.net
mnt-by:          MAINT-CHINANET-JS
changed:          dns@jsinfo.net 20090831
```

```
changed:        ip@jsinfo.net 20090831
changed:        hm-changed@apnic.net 20090901
source:         APNIC
changed:        hm-changed@apnic.net 20111114
person:         Chinanet Hostmaster
nic-hdl:        CH93-AP
e-mail:         anti-spam@ns.chinanet.cn.net
address:        No.31 ,jingrong street,beijing
address:        100032
phone:          +86-10-58501724
fax-no:         +86-10-58501724
country:        CN
changed:        dingsy@cndata.com 20070416
mnt-by:         MAINT-CHINANET
source:         APNIC

inetnum:        58.221.199.160 - 58.221.199.175
netname:        NANTONG-LANZHOUZHONGHESOFT-CORP
descr:          Nantong Lanzhou Zhonghe Soft CORP
descr:          Nantong City
descr:          Jiangsu Province
country:        CN
admin-c:        CH448-AP
tech-c:         CH448-AP
changed:        ip@jsinfo.net 20090602
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-CHINANET-JS
mnt-lower:      MAINT-CHINANET-JS-NT
source:         APNIC
person:         chinanet-js-nt hostmaster
address:        No.88,Huancheng South Road,Nantong 226001
country:        CN
phone:          +86-513-5518003
fax-no:         +86-513-5521614
e-mail:         ntip@pub.nt.jsinfo.net
nic-hdl:        CH448-AP
mnt-by:         MAINT-CHINANET-JS-NT
changed:        ip@jsinfo.net 20021211
source:         APNIC

inetnum:        58.208.0.0 - 58.223.255.255
netname:        CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
country:        CN
admin-c:        CH93-AP
tech-c:         CJ186-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CHINANET-JS
```

```
mnt-routes:     MAINT-CHINANET-JS
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20050624
source:         APNIC
role:           CHINANET JIANGSU
address:        260 Zhongyang Road,Nanjing 210037
country:        CN
phone:          +86-25-86588231
phone:          +86-25-86588745
fax-no:         +86-25-86588104
e-mail:         ip@jsinfo.net
admin-c:        CH360-AP
tech-c:         CS306-AP
tech-c:         CN142-AP
nic-hdl:        CJ186-AP
notify:         ip@jsinfo.net
mnt-by:         MAINT-CHINANET-JS
changed:        dns@jsinfo.net 20090831
changed:        ip@jsinfo.net 20090831
changed:        hm-changed@apnic.net 20090901
source:         APNIC
changed:        hm-changed@apnic.net 20111114
person:         Chinanet Hostmaster
nic-hdl:        CH93-AP
e-mail:         anti-spam@ns.chinanet.cn.net
address:        No.31 ,jingrong street,beijing
address:        100032
phone:          +86-10-58501724
fax-no:         +86-10-58501724
country:        CN
changed:        dingsy@cndata.com 20070416
mnt-by:         MAINT-CHINANET
source:         APNIC

inetnum:        58.208.0.0 - 58.223.255.255
netname:        CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
country:        CN
admin-c:        CH93-AP
tech-c:         CJ186-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CHINANET-JS
mnt-routes:     MAINT-CHINANET-JS
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20050624
source:         APNIC
role:           CHINANET JIANGSU
address:        260 Zhongyang Road,Nanjing 210037
```

```
country:      CN
phone:        +86-25-86588231
phone:        +86-25-86588745
fax-no:       +86-25-86588104
e-mail:       ip@jsinfo.net
admin-c:      CH360-AP
tech-c:       CS306-AP
tech-c:       CN142-AP
nic-hdl:      CJ186-AP
notify:       ip@jsinfo.net
mnt-by:       MAINT-CHINANET-JS
changed:      dns@jsinfo.net 20090831
changed:      ip@jsinfo.net 20090831
changed:      hm-changed@apnic.net 20090901
source:       APNIC
changed:      hm-changed@apnic.net 20111114
person:       Chinanet Hostmaster
nic-hdl:      CH93-AP
e-mail:       anti-spam@ns.chinanet.cn.net
address:      No.31 ,jingrong street,beijing
address:      100032
phone:        +86-10-58501724
fax-no:       +86-10-58501724
country:      CN
changed:      dingsy@cndata.com 20070416
mnt-by:       MAINT-CHINANET
source:       APNIC
```

inetnum: 60.190.203.0 - 60.190.203.255

```
netname:      NINBO-LANZHONG-LTD
country:      CN
descr:        Ninbo Lanzhong Network Ltd
descr:
admin-c:      TD202-AP
tech-c:       CS64-AP
status:       ASSIGNED NON-PORTABLE
changed:      auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:       MAINT-CN-CHINANET-ZJ-SX
source:       APNIC
role:         CHINANET-ZJ Shaoxing
address:      No.9 Sima Road,Shaoxing,Zhejiang.312000
country:      CN
phone:        +86-575-5136199
fax-no:       +86-575-5114449
e-mail:       anti-spam@mail.sxptt.zj.cn
admin-c:      CH109-AP
tech-c:       CH109-AP
nic-hdl:      CS64-AP
mnt-by:       MAINT-CHINANET-ZJ
changed:      master@dcb.hz.zj.cn 20031204
source:       APNIC
```

```
changed:       hm-changed@apnic.net 20111114
person:        Taichun Du
nic-hdl:       TD202-AP
e-mail:        anti-spam@mail.sxptt.zj.cn
address:       Shaoxing,Zhejiang.Postcode:312000
phone:         +86-574-88311333
country:       CN
changed:       auto-dbm@dcb.hz.zj.cn 20100105
mnt-by:        MAINT-CN-CHINANET-ZJ-SX
source:        APNIC

inetnum:       60.191.153.152 - 60.191.153.159
netname:       WENLING-XINGYU-NETBAR
country:       CN
descr:         WenLing XingYu Netbar
descr:
admin-c:       QZ811-AP
tech-c:        CT24-AP
status:        ASSIGNED NON-PORTABLE
changed:       auto-dbm@dcb.hz.zj.cn 20100513
mnt-by:        MAINT-CN-CHINANET-ZJ-TZ
source:        APNIC
role:          CHINANET-ZJ Taizhou
address:       No.668 Shifu Street,Jiaojiang,Taizhou,Zhejiang.318000
country:       CN
phone:         +86-576-8680619
fax-no:        +86-576-8680613
e-mail:        anti-spam@mail.tzptt.zj.cn
admin-c:       CH111-AP
tech-c:        CH111-AP
nic-hdl:       CT24-AP
mnt-by:        MAINT-CHINANET-ZJ
changed:       master@dcb.hz.zj.cn 20031204
source:        APNIC
changed:       hm-changed@apnic.net 20111114
person:        QingQin Zhu
nic-hdl:       QZ811-AP
e-mail:        anti-spam@mail.tzptt.zj.cn
address:       Youdianyu, Zheguo,Wenling,Zhejiang.Postcode:317500
phone:         +86-576-86440107
country:       CN
changed:       auto-dbm@dcb.hz.zj.cn 20100513
mnt-by:        MAINT-CN-CHINANET-ZJ-TZ
source:        APNIC

inetnum:       61.128.0.0 - 61.129.255.255
netname:       CHINANET-CN
descr:         Data Communication Division
descr:         China Telecom
country:       CN
admin-c:       CH93-AP
```

```
tech-c:         CH93-AP
mnt-by:          APNIC-HM
mnt-lower:        MAINT-CHINANET
changed:          hostmaster@apnic.net 20000113
status:         ALLOCATED PORTABLE
source:          APNIC
person:          Chinanet Hostmaster
nic-hdl:        CH93-AP
e-mail:         anti-spam@ns.chinanet.cn.net
address:         No.31 ,jingrong street,beijing
address:         100032
phone:           +86-10-58501724
fax-no:         +86-10-58501724
country:         CN
changed:          dingsy@cndata.com 20070416
mnt-by:          MAINT-CHINANET
source:          APNIC
```