

Black and White Lists

How to use free data from the Internet Storm Center

Marcus H. Sachs
SANS Internet Storm Center
marc@sans.org



The Internet Storm Center

- SANS Internet Storm Center uses the DShield distributed incident detection technology
 - ISC database receives over ten million log lines daily from intrusion detection systems run by volunteers world-wide
- Thousands of system administrators send in additional observations and findings via email and the web
- Volunteer incident handlers analyze detected problems and anomalies, then post a daily diary of analysis
 - Analysis also feeds SANS research efforts
 - Direct feed to courseware, Top20 list, and weekly newsletters
- Service is free to the Internet community

Weather Forecasting

- SANS ISC analysis parallels weather analysis
 - Small sensors in as many places as possible
 - Sensors send raw information to multiple regional data collection points for early analysis and correlation
 - Regional collection feeds a national or global watch center
- Our sensors “see” tcp or udp flows, then we infer developing situations
 - We do not have a content monitoring capability

SANS ISC Statistics: Reports Submitted

Past 30 Days: 414,196,491 log lines

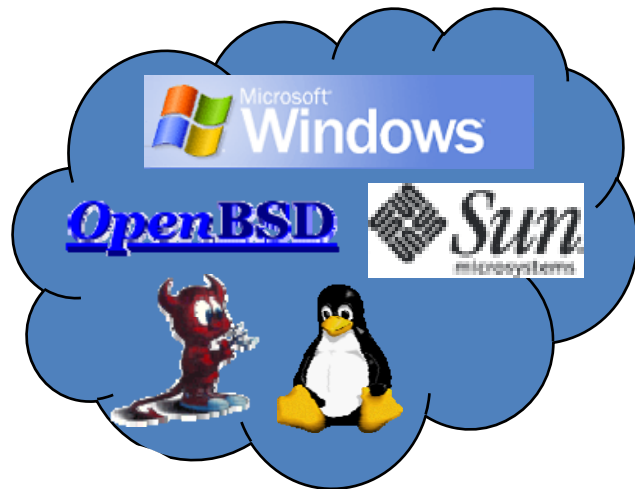
Past Seven Days: 95,558,962 log lines

Past 24 Hours: 11,906,713 log lines

All submitted by volunteer collectors!

The SANS ISC Process

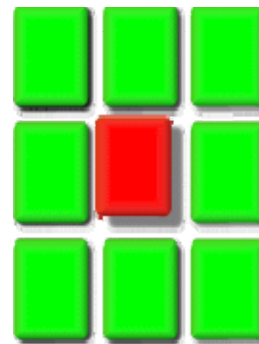
Data Collection



DShield Users



Analysis

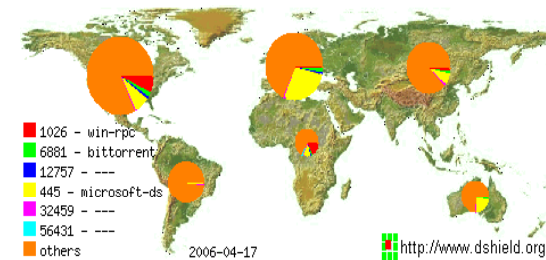


DShield.org

Dissemination

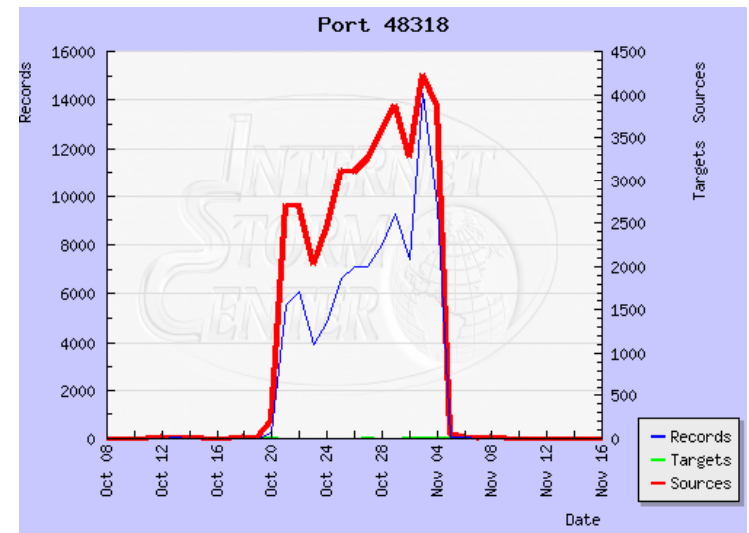


Service Name	Port Number	Activity Past Month	Explanation
microsoft-ds	445		Win2k+ Server Message Block
epmap	135		DCE endpoint resolution
---	20525		
netbios-ssn	139		NETBIOS Session Service
---	1026		
icq	1027		icq instant messenger
---	1025		
www	80		World Wide Web HTTP
domain	53		Domain Name Server
netbios-ns	137		NETBIOS Name Service



SANS ISC Services

- Sensor software for dozens of popular devices
- “Private” website and report generation capability for participants
- Fightback program with major ISPs
- Large incident database with preconfigured queries and search capabilities



Sensor Software

- SANS ISC provides client software for over 60 different devices
- Most popular hardware and software devices are included, such as
 - Linksys
 - Snort
 - SonicWall
 - Norton Personal Firewall
 - NetGear
 - ZoneAlarm
 - PortSentry
 - Windows Firewall
 - Cisco
 - Checkpoint
 - BlackIce
- Client software includes an installation program and directions for use
- If you have a device or software that is not supported we will write the code needed to build a sensor

Private Reporting and Analysis

- Each participant receives a custom view of the SANS ISC database
- Can compare own data with information from thousands of other sensors
- All submitted data is available for later retrieval and analysis
- Pre-generated data visualization templates make viewing past events very easy for most users

Sensor Report

DSshield - Your recent submissions 65.173.218.75 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://secure.dshield.org/myreports.php

User ID: 82436253
Total lines submitted on 2006-11-16:
 553

Nov-16-2006

source
 target
 targetport

Include 'Danger Levels': high medium low misconf.

Color Legend (Attack Severity based on Target Port):
High Medium Low Possible Firewall Misconfiguration

Not all ports are assigned a 'danger level'. Unassigned ports are represented by an empty white circle (○).

Currently showing lines 0 through 20

[Next Page](#)

Date	Time	Source	Source Port	Target	Target Port	Protocol	Danger
2006-11-16	12:02:32	204.016.208.135	13364	068.100.115.212	1027		○
2006-11-16	12:39:56	162.121.169.039	30391	068.100.115.212	1026		●
2006-11-16	12:46:25	202.097.238.203	42019	068.100.115.212	1027		○
2006-11-16	12:47:13	024.011.143.226	11656	068.100.115.212	1026		●
2006-11-16	12:47:14	024.076.240.035	3726	068.100.115.212	1027		○
2006-11-16	12:48:01	044.179.183.071	30391	068.100.115.212	1026		●
2006-11-16	12:48:35	221.208.208.091	49003	068.100.115.212	1026		●
2006-11-16	12:48:35	221.208.208.091	49003	068.100.115.212	1027		○

November 16th 2006 targetport Summary

45%

Port	Percentage
1026	45%
1027	26%
1025	20%
1031	3%
1035	3%
others	3%

Done secure.dshield.org Adblock

Fightback Capability

- Unique to the SANS ISC, participants can assist in locating and stopping the worst offenders
- Participating sites include their own IP address information in the submitted data
- By aggregating attack data, the SANS ISC can provide strong evidence to ISPs willing to stop abuse coming from their networks
- Feedback is returned to participants when an attacker is successfully stopped

Where Did That Attack Come From?

DSHield - IP Info 65.173.218.75 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://secure.dshield.org/ipinfo.php?ip=221.208.208.091&x=1&day=732996

IP Address: 221.208.208.91
HostName: 221.208.208.91

DSHield Profile:

Country:	CN
Contact E-mail:	abuse@cnc-noc.net
AS Number:	4837
AS Name:	CHINA169-Backbone
AS Contact:	abuse@cnc-noc.net
Total Records against IP:	225947
Number of targets:	1186
Date Range:	2006-11-03 to 2006-11-15
Comments:	

[request contact update](#)
[Queue Summary Update](#)
(Note: it will take up to 30min for the update to be effective.)

Top 10 Ports recently hit by this source:

Port	Attacks	Start	End
1026	121483	2006-10-16	2006-11-16
1027	110193	2006-10-16	2006-11-16

Last Fightback Sent: sent to abuse@cnc-noc.net on 2006-10-28 00:08:03
no reply received

Whois: [Querying whois.apnic.net]
[whois.apnic.net]
% [whois.apnic.net node-2]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

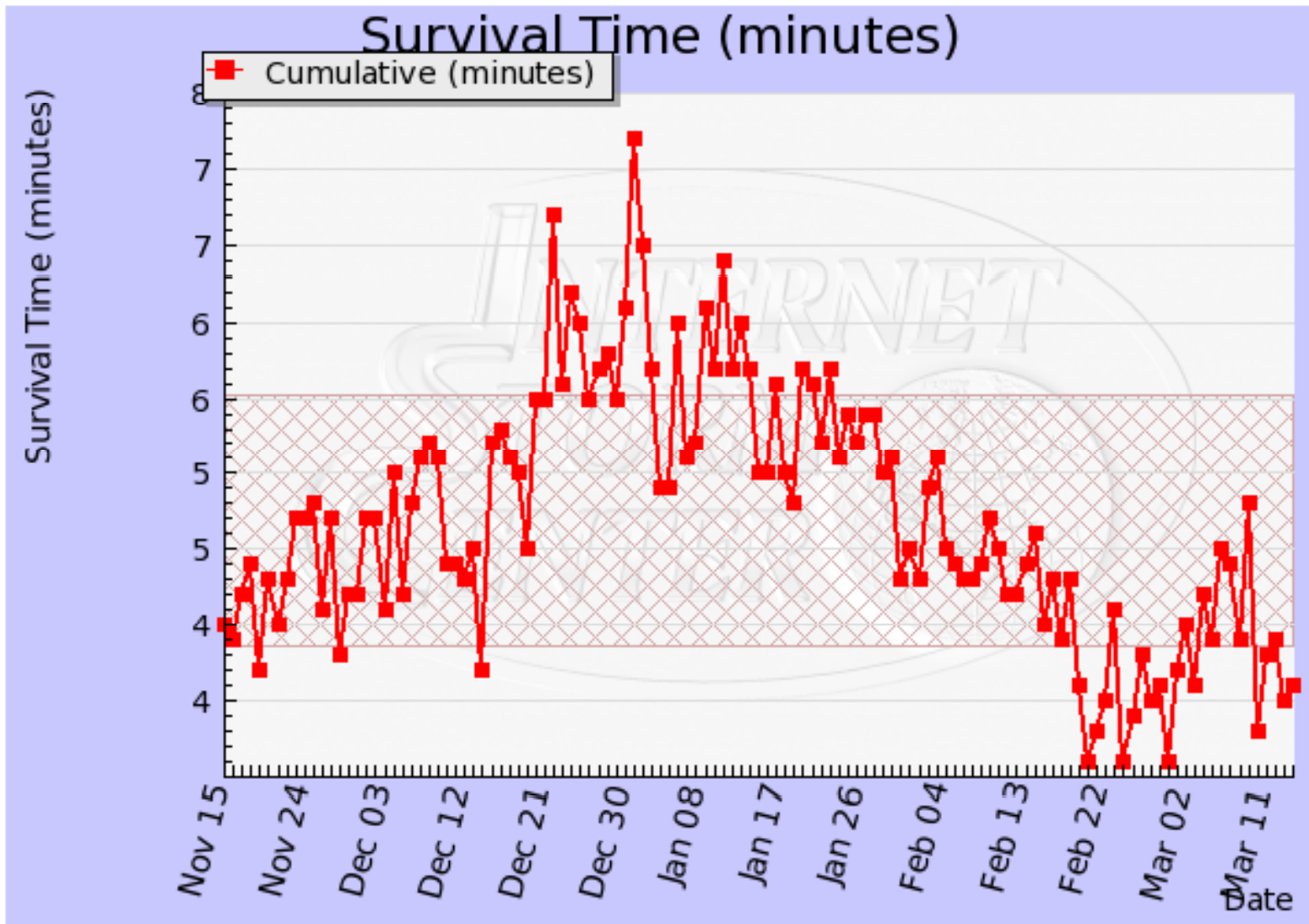
inetnum: 221.208.0.0 - 221.212.255.255
netname: CNCGROUP-HL
descr: CNCGROUP Heilongjiang Province Network
descr: China Network Communications Group Corporation
descr: No.156,Fu-Xing-Men-Nei Street,
descr: Beijing,100031

Done secure.dshield.org Adblock

SANS ISC Incident Database

- Data collected over the past few years are contained in a database that can be queried by any Internet user
- Some pre-configured queries include
 - Top ten offending sites
 - Top ten targeted ports
 - History of reported activity on any port
 - Summary information about any user-supplied IP address

Survival Time



Top Offending IP Addresses: A Simple Black List

Top 10 Source IPs

IP Address	Reports	Attacks	First Seen	Last Seen
203.094.243.191	870,031	99,232	2007-08-16	2008-03-15
202.101.235.100	156,813	96,277	2007-11-28	2008-03-15
080.168.118.014	135,724	93,724	2008-01-08	2008-03-14
210.188.206.242	180,170	119,119	2008-01-04	2008-03-15
202.099.011.099	107,107	107,107	2008-01-04	2008-03-15
218.064.237.219	107,107	107,107	2008-01-04	2008-03-15
058.242.042.235	107,107	107,107	2008-01-04	2008-03-15
202.109.178.203	107,107	107,107	2008-01-04	2008-03-15
210.212.130.229	107,107	107,107	2008-01-04	2008-03-15
061.181.255.106	107,107	107,107	2008-01-04	2008-03-15

IP Info (203.94.243.191)

IP Address (click for more detail):	203.94.243.191
Hostname:	203.94.243.191
Country:	IN
AS:	17813
AS Name:	MTNL-AP Mahanagar Telephone Nigam Ltd.
Reports:	870031
Targets:	99232
First Reported:	2007-08-16
Most Recent Report:	2008-03-15
Comment:	- none -

Early Warning

- Small group of volunteer incident handlers monitor sensor inputs
- When anomalies are detected, handlers convene an online conference to discuss and compare findings
- If a warning to the Internet community is needed, the SANS ISC handlers rely on SANS to get the word out rapidly
- Handlers continue to assess and provide guidance to users and administrators

An Invitation to Participate

- The SANS ISC's success is based on the active participation of thousands of users
- All Internet users, information analysis and sharing centers, and others willing to participate in a large distributed data collection and analysis project are invited to join
- Details are online at

<http://isc.sans.org>