

# SANS ISC Free Software

RMLLSEC16 Rump Session



# SANS Internet Storm Center

- Created in 2001 to track the LiOn worm
- Today, sensors covers 500K IPs from 50 countries
- Data collection, analysis and warning system (like weather forecasts)
- Operated by volunteers ("handlers")



# Infocon



Date	Status	Reason
Jan 23 2015	Yellow	<a href="#">Adobe Flash Vulnerabilities</a>
Sep 26 2014	Yellow	<a href="#">Bash Shellshock</a>
Apr 08 2014	Yellow	<a href="#">OpenSSL Heartbleed</a>
Mar 16 2012	Yellow	<a href="#">MS12020 Windows RDP Vulnerability</a>
Sep 28 2010	Yellow	<a href="#">MS10070</a>
Jul 19 2010	Yellow	<a href="#">LNK Vulnerability in Windows</a>
Jul 13 2009	Yellow	<a href="#">MS Office Web Components ActiveX</a>
Oct 23 2008	Yellow	<a href="#">Microsoft RPC Patch MS08067</a>

# Data Collection

- SSH honeypots
- HTTP honeypots
- Web: 404 pages, CRL, HTTP headers
- DShield

# DShield Sensor

- SW: Modified version of Cowrie
- HW: Raspberry (or any other entry-level hardware)
- <https://github.com/DShield-ISC/dshield>

# DShield Client

- Collects src\_ip, src\_port\_, dst\_ip, dst\_port, proto, count
- Available for many<sup>(1)</sup> clients
- Easy to write your own client<sup>(2)</sup>  
(I wrote mine for OSSEC)

<sup>(1)</sup> <https://www.dshield.org/howto.html#clients>

<sup>(2)</sup> <https://www.dshield.org/specs.html>

# Top-20 Block List

<https://isc.sans.edu/block.txt>

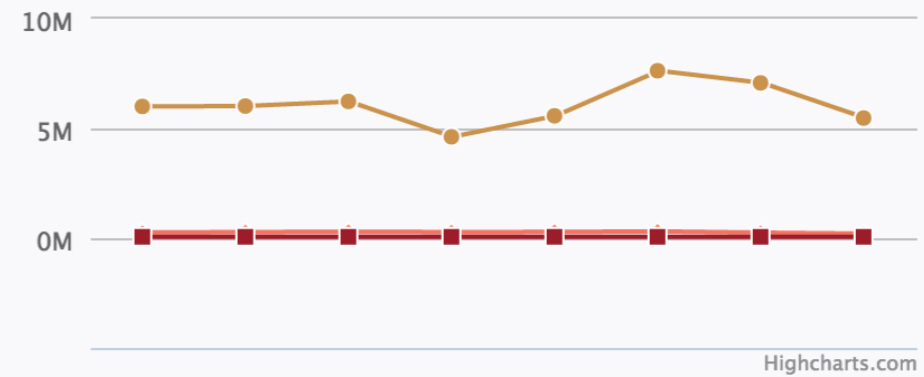
```
#
# DShield.org Recommended Block List
# (c) 2007 DShield.org
# some rights reserved. Details http://creativecommons.org/licenses/by-nc-sa/2.5/
# use on your own risk. No warranties implied.
# primary URL: http://feeds.dshield.org/block.txt
# PGP Sign.: http://feeds.dshield.org/block.txt.asc
#
# comments: info@dshield.org
# updated: Mon Jul 4 20:38:25 2016 UTC
#
# This list summarizes the top 20 attacking class C (/24) subnets
# over the last three days. The number of 'attacks' indicates the
# number of targets reporting scans from this subnet.
#
# Columns (tab delimited):
#
# (1) start of netblock
# (2) end of netblock
# (3) subnet (/24 for class C)
# (4) number of targets scanned
# (5) name of Network
# (6) Country
# (7) contact email address
#
# If a range is assigned to multiple users, the first one is listed.
#
Start      End      Netblock      Attacks Name      Country email
61.240.144.0 61.240.144.255 24      803      China United Telecommunications Corporation CN      ip_address@cnuninet.com
121.18.238.0 121.18.238.255 24      558      CHINA169-BACKBONE CNCGROUP China169 Backbone CN      abuse@cnc-noc.net
```

# Statistics

### Top 50 Offensive IPs Today

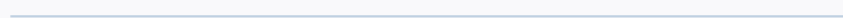


### Network Activity This Week

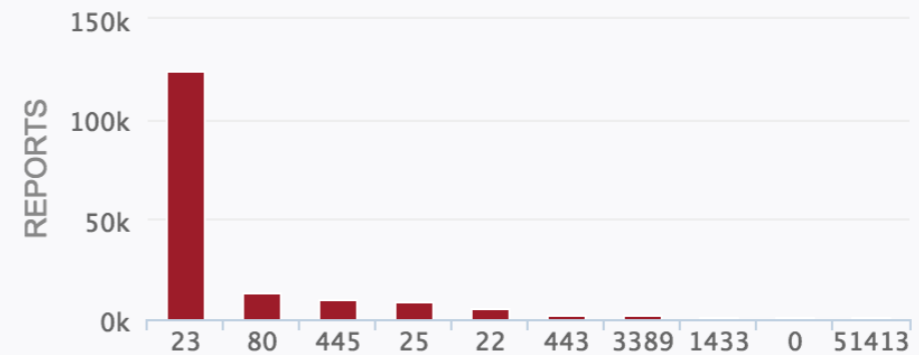


### Top 10 Offensive IPs Today

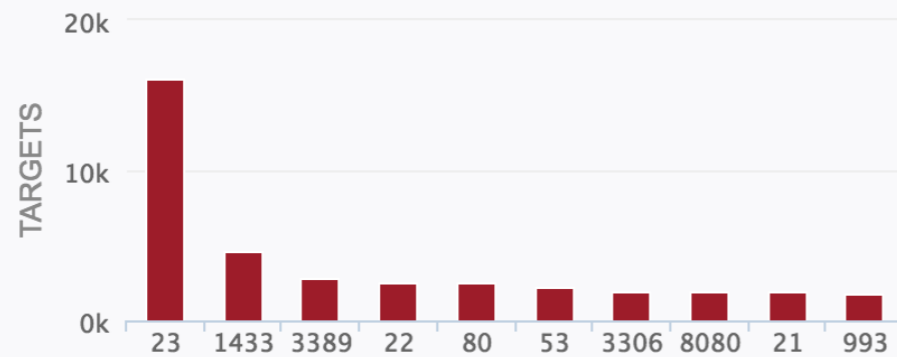
TARGET IPs



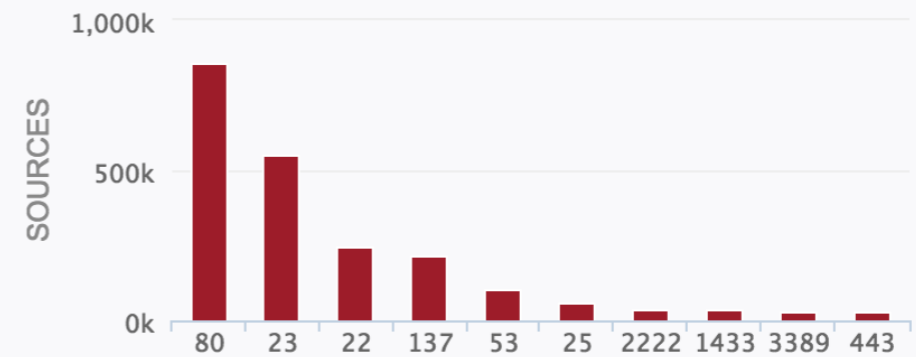
### Top 10 Ports Today by Unique Sources



### Top 10 Ports Today by Unique Targets



### Top 10 Ports Today by Total Activity






# API

<https://isc.sans.edu/api/>

```
# curl -L http://isc.sans.edu/api/ip/103.238.68.242
<?xml version="1.0" encoding="UTF-8"?>
<ip><number>103.238.68.242</number><count>4831</count><attacks>16</attacks><maxdate>2016-07-04</
maxdate><mindate>2015-10-30<
/mindate><updated>2016-07-04 11:03:51</updated><comment></comment><maxrisk></maxrisk><asabusecontact>tech@vnnic.vn</
asabusec
ontact><as>24088</as><asname><![CDATA[HANOITELECOM-AS-AP Hanoi Telecom Joint Stock Company - HCMC Branch,]]></
asname><ascoun
try>VN</ascountry><assize>4349</assize><network>103.238.68.0/24</
network><threatfeeds><blocklistde22><lastseen>2016-06-18</l
astseen><firstseen>2015-10-31</firstseen></blocklistde22><blocklistde25><lastseen>2016-07-04</
lastseen><firstseen>2016-02-11
</firstseen></blocklistde25><emergincompromised><lastseen>2015-12-03</lastseen><firstseen>2015-11-24</firstseen></
emergincom
promised><openbl_ssh><lastseen>2016-07-04</lastseen><firstseen>2016-01-04</firstseen></openbl_ssh></threatfeeds></ip>
```

# Color My Logs

```
Jul 4 06:41:41 vps2 kernel: [27458176.315340] [UFW ALLOW] IN= OUT=eth0 SRC=51.254.36.238
DST=213.186.33.99 LEN=73 TOS=0x00 PREC=0x00 TTL=64 ID=22910 DF PROTO=UDP SPT=42059 DPT=53 LEN=53
Jul 4 06:41:49 vps2 kernel: [27458183.365574] [UFW AUDIT] IN=eth0 OUT=
MAC=fa:16:3e:ce:ce:85:26:f3:8d:ea:3a:38:08:00 SRC=1.165.192.29 Network Name: HINET Data Communication Business Group,
PREC=0x00 TTL=45 ID=65125 DF PROTO=TCP SPT=34812 DPT=23 WINDOW= DShield received 5 reports from 2 targets about this IP address.
Jul 4 06:41:49 vps2 kernel: [27458183.365623] [UFW BLOCK] IN=eth0 Risk: 1
MAC=fa:16:3e:ce:ce:85:26:f3:8d:ea:3a:38:08:00 SRC=1.165.192.29 DST=51.254.36.238 LEN=52 TOS=0x00
PREC=0x00 TTL=45 ID=65125 DF PROTO=TCP SPT=34812 DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0
```



[Click here](#) to parse. (it can take a while for all the data to be returned. give it a minute)  
This page takes advantage of our [API](#). Use it for scripted submissions.

Summer  
2016  
14 Top  
Security  
Courses  
11 - 16 July

<https://isc.sans.edu>

<xmertens@isc.sans.edu>