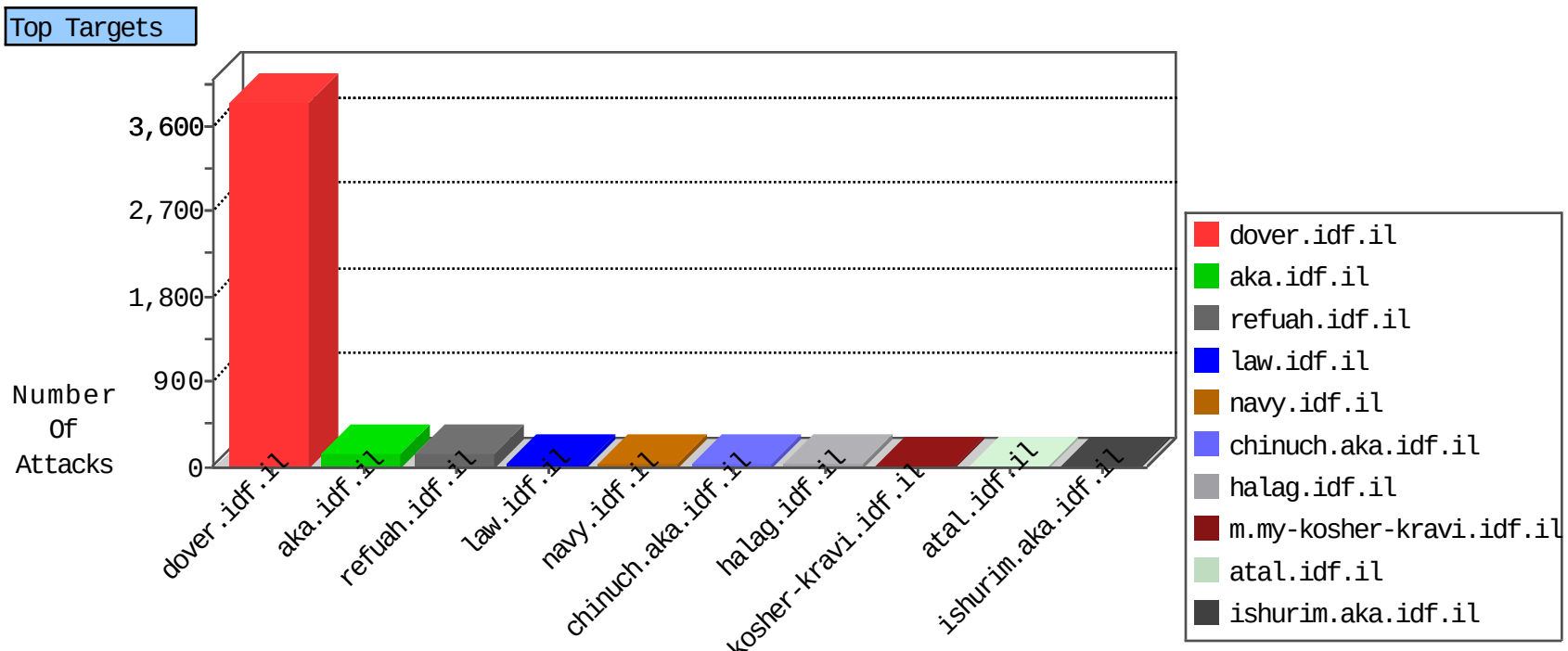
11-02-2015-02:04:04 to 11-02-2015-03:04:04

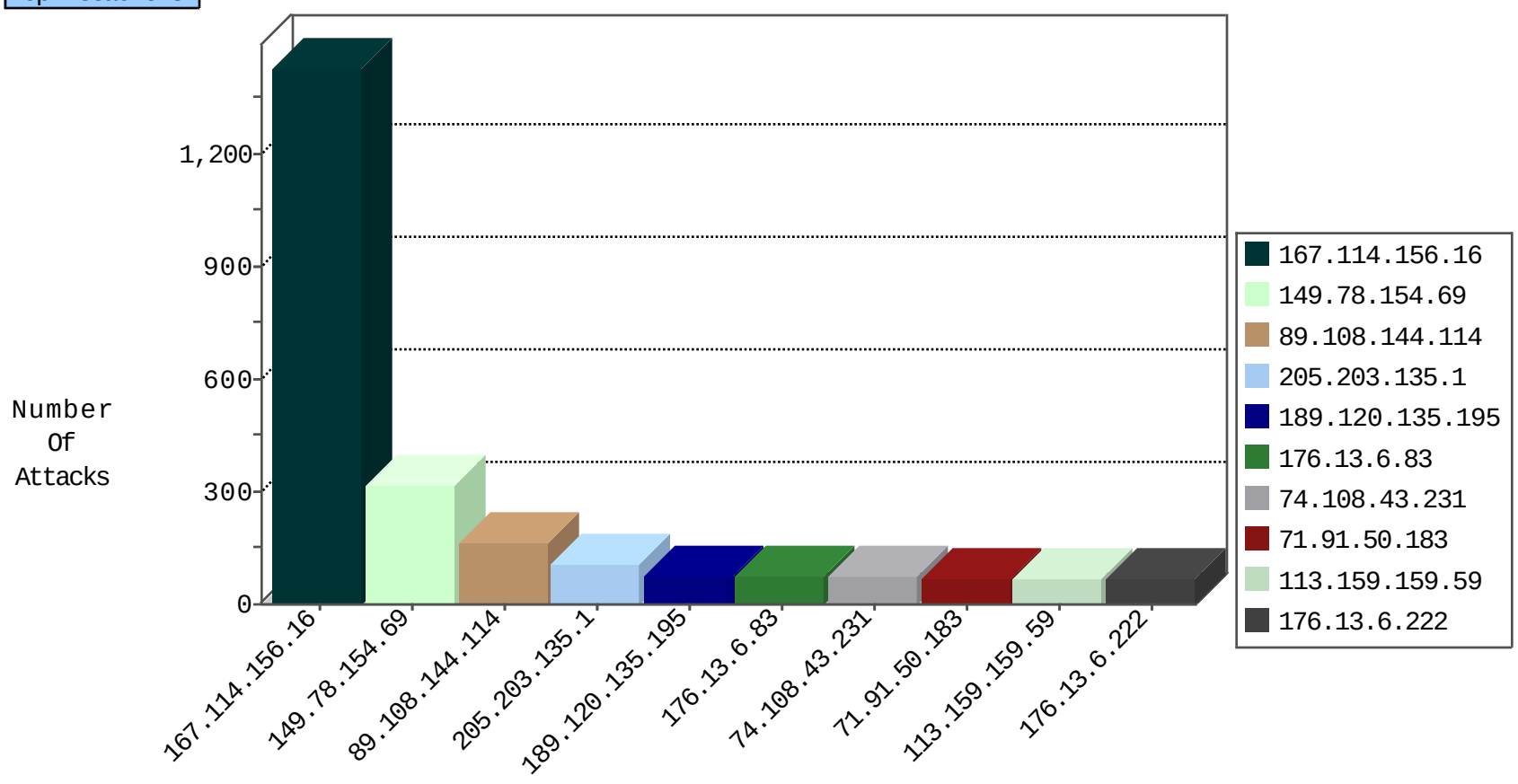
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-02-2015-02:04:04 to 11-02-2015-03:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2425
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	32
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
5.29.34.117	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
122.180.244.218	India	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-02-2015-02:04:04 to 11-02-2015-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-02-2015-02:04:04 to 11-02-2015-03:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
108.61.196.86	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.101	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.180	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.180	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.224.145.116	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
115.236.75.201	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
113.236.14.63	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
108.61.196.86	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
5.8.66.101	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.180	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.7.209.9	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
2.133.41.12	147.237.76.30	Kazakstan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.188.218.43	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.224.145.116	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
115.236.75.201	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

11-02-2015-02:04:04 to 11-02-2015-03:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	315
89.108.144.114	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	158
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	103
189.120.135.195	Brazil	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
74.108.43.231	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
176.13.6.83	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
71.91.50.183	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
113.159.159.59	Japan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
176.13.6.222	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	65
41.250.2.37	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
2.54.154.89	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
104.236.200.179		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
24.218.80.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
142.255.113.244	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
96.232.130.203	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
107.72.164.55	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
207.46.13.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
107.77.70.28	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
108.26.194.239	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
84.228.72.105	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
67.234.215.120	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
5.29.34.117	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
12.139.31.194	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
198.58.103.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
69.141.189.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.166	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
109.64.0.222	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
192.117.12.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
162.243.73.200	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.103.36	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
81.218.235.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
220.255.97.166	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
207.46.13.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.65.103	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
219.74.37.5	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
89.139.3.117	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
121.7.37.167	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
79.181.182.128	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-02-2015-02:04:04 to 11-02-2015-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
157.55.39.200	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/miluim/templates/inner.asp	Block	15
37.187.114.171	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /xmii/illuminator	Block	15
217.146.69.3	Estonia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	15
81.95.96.126	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	15
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1234-he/refuah.aspx	Block	15
107.20.255.148	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	15
66.249.75.60	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pds	Block	15
37.187.114.171	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /xmii/illuminator	Block	15
87.69.160.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.19.85.96	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
88.235.230.127	Turkey	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
54.210.135.33	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 54.210.135.33	Block	15
98.130.0.140	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
31.154.0.27	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
213.185.86.107	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	15
78.46.92.68	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	15
54.210.135.33	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-6859-en/patzar.aspx.	Block	15
104.236.200.179		147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/default.aspxdefault.aspx	Block	15

11-02-2015-02:04:04 to 11-02-2015-03:04:04