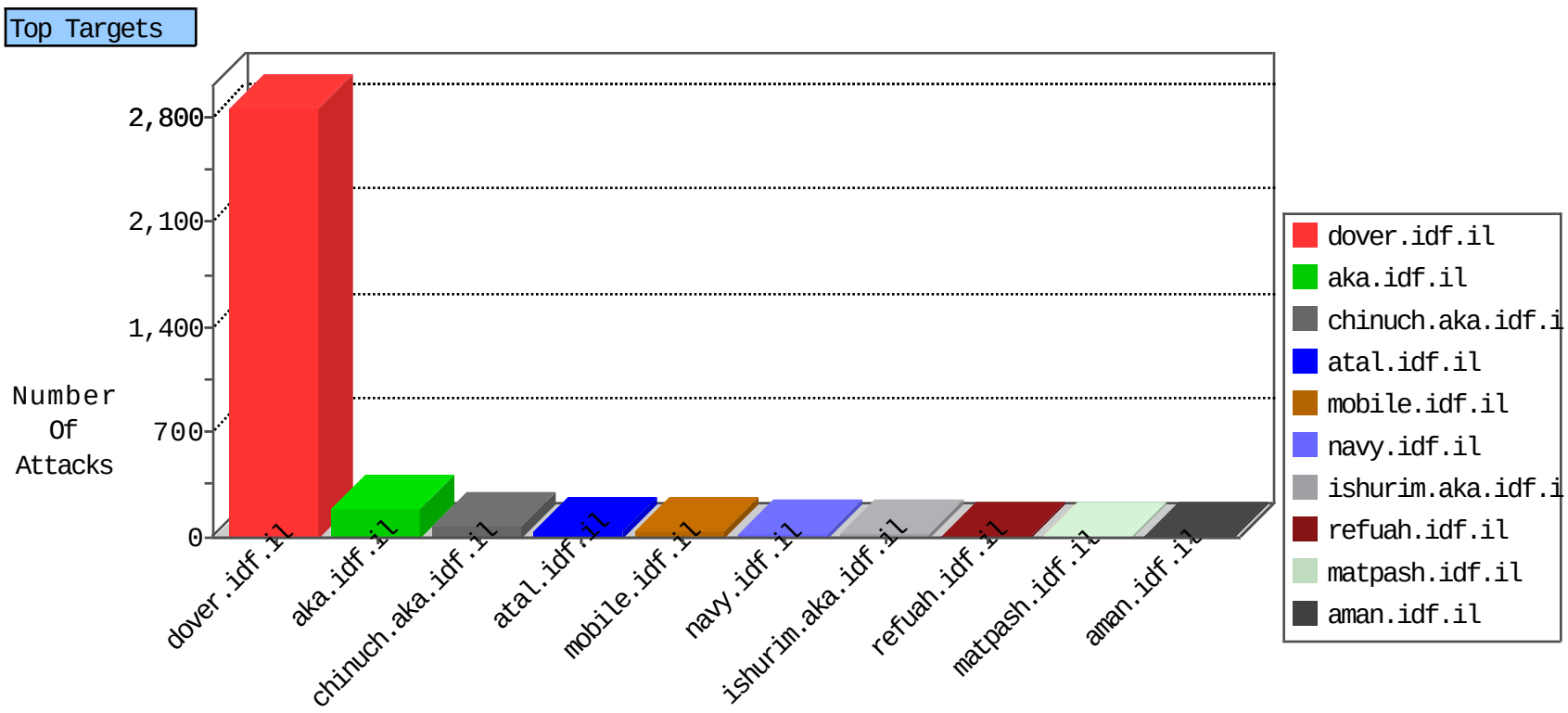
11-02-2015-01:04:04 to 11-02-2015-02:04:04

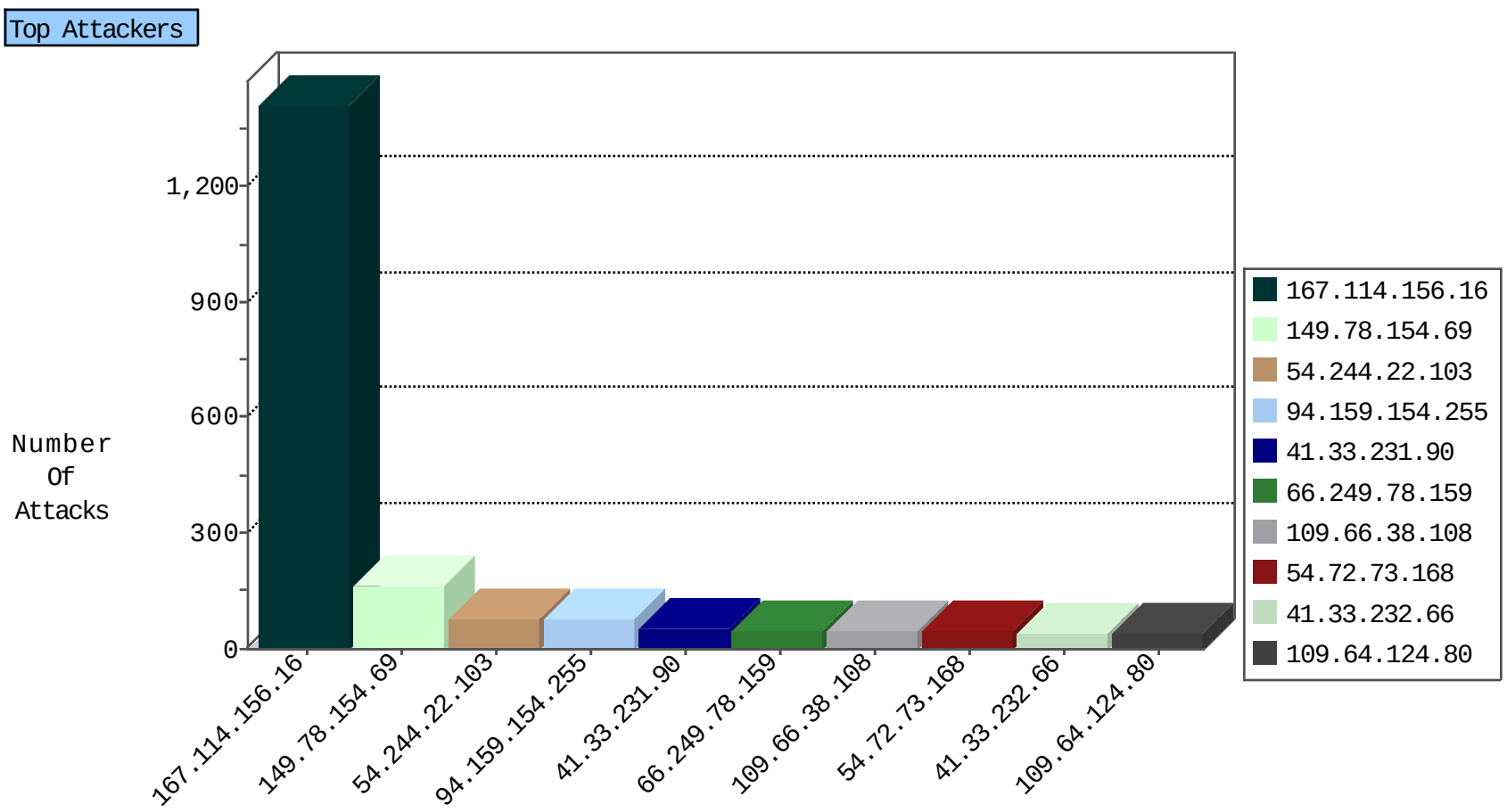
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-02-2015-01:04:04 to 11-02-2015-02:04:04

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	2455
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	615
108.46.12.18	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
85.64.57.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.183.229.69	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	13
85.250.197.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.73.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.86.99.147	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
95.86.99.147	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
51.36.102.169	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
178.64.216.24	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
84.108.145.253	Israel	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
94.159.154.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1

11-02-2015-01:04:04 to 11-02-2015-02:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.214.249.146	Romania	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-02-2015-01:04:04 to 11-02-2015-02:04:04

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
91.147.180.56	147.237.76.196	Saudi Arabia	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
91.147.180.56	147.237.76.196	Saudi Arabia	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
209.126.65.230	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
91.147.180.56	147.237.76.196	Saudi Arabia	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.65.230	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1

11-02-2015-01:04:04 to 11-02-2015-02:04:04

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.il	drop	First packet isn't SYN	drop	166
94.159.154.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
109.66.38.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
67.169.254.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.177.219.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	29
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.64.124.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.160.144.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
188.135.40.177	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
71.239.243.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.217.253.152	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.28.169.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
91.63.253.135	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
71.227.62.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
213.57.104.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.142.57.67	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
47.62.182.219	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.31.117.76	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
24.47.56.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.117.12.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
177.16.90.23	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
51.36.102.169	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.250.166.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
107.77.94.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.39	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
95.199.150.219	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
124.157.96.94	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

11-02-2015-01:04:04 to 11-02-2015-02:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	30
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
50.139.119.152	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
198.20.69.74	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
52.23.156.32	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	15
87.69.230.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	15
207.46.13.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/mainfs.asp	Block	15
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1923.pdf	Block	15
109.64.124.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
40.77.167.91	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	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
149.78.239.14	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	11

11-02-2015-01:04:04 to 11-02-2015-02:04:04