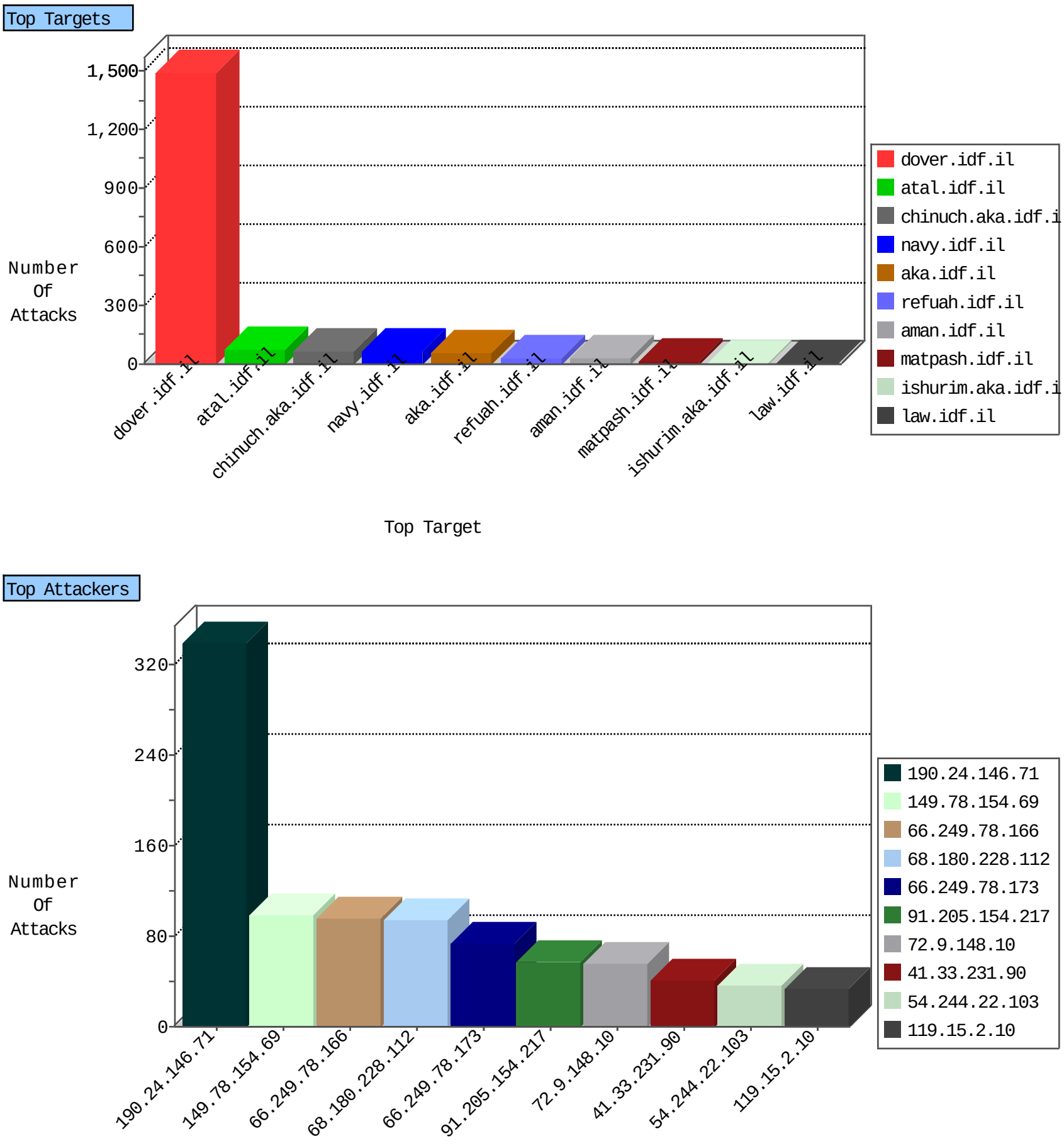
10-27-2015-02:04:06 to 10-27-2015-03:04:06

IDF Under Attack
Daily Report



10-27-2015-02:04:06 to 10-27-2015-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.77	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	154
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
119.15.2.10	New Zealand	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
45.63.1.137		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

10-27-2015-02:04:06 to 10-27-2015-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
103.21.58.191	India	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
209.15.196.171	Canada	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
179.7.78.2	Peru	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-27-2015-02:04:06 to 10-27-2015-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-27-2015-02:04:06 to 10-27-2015-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	339
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
91.205.154.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
2.54.62.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
119.15.2.10	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
77.126.209.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.38.183.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
69.123.223.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.27.173.104	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.142.200.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
24.190.235.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.239.128.30	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.239.0.30	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.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	10
79.180.4.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	9
174.115.118.58	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
220.255.97.210	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.145.222.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.228.61.209	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.144	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
220.255.146.30	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
83.130.101.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.25.61.154		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
76.30.12.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
203.127.96.201	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
124.158.17.98	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

10-27-2015-02:04:06 to 10-27-2015-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	84
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
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	56
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	28
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
157.55.39.13	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
41.239.128.30	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/	Block	14
207.46.13.35	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/opcontactus/opcontactus.aspx	Block	14
66.249.78.247	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
66.249.67.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/_layouts/authenticate.aspx	Block	14
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
207.46.13.82	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	14
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.144	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
68.180.230.244	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
5.102.194.28	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8853-he/refuah.aspx	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.142.68.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.165.15.241	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	14
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14

10-27-2015-02:04:06 to 10-27-2015-03:04:06