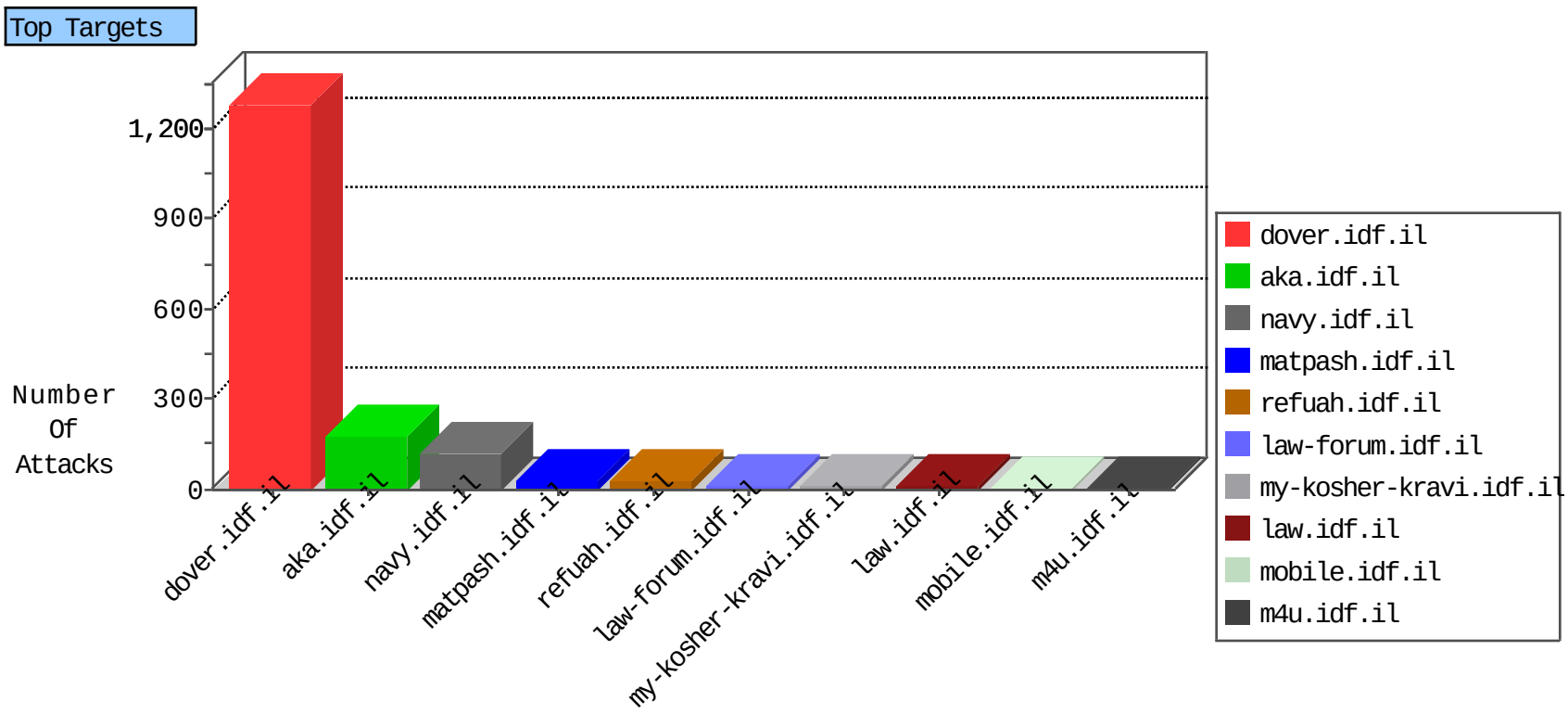
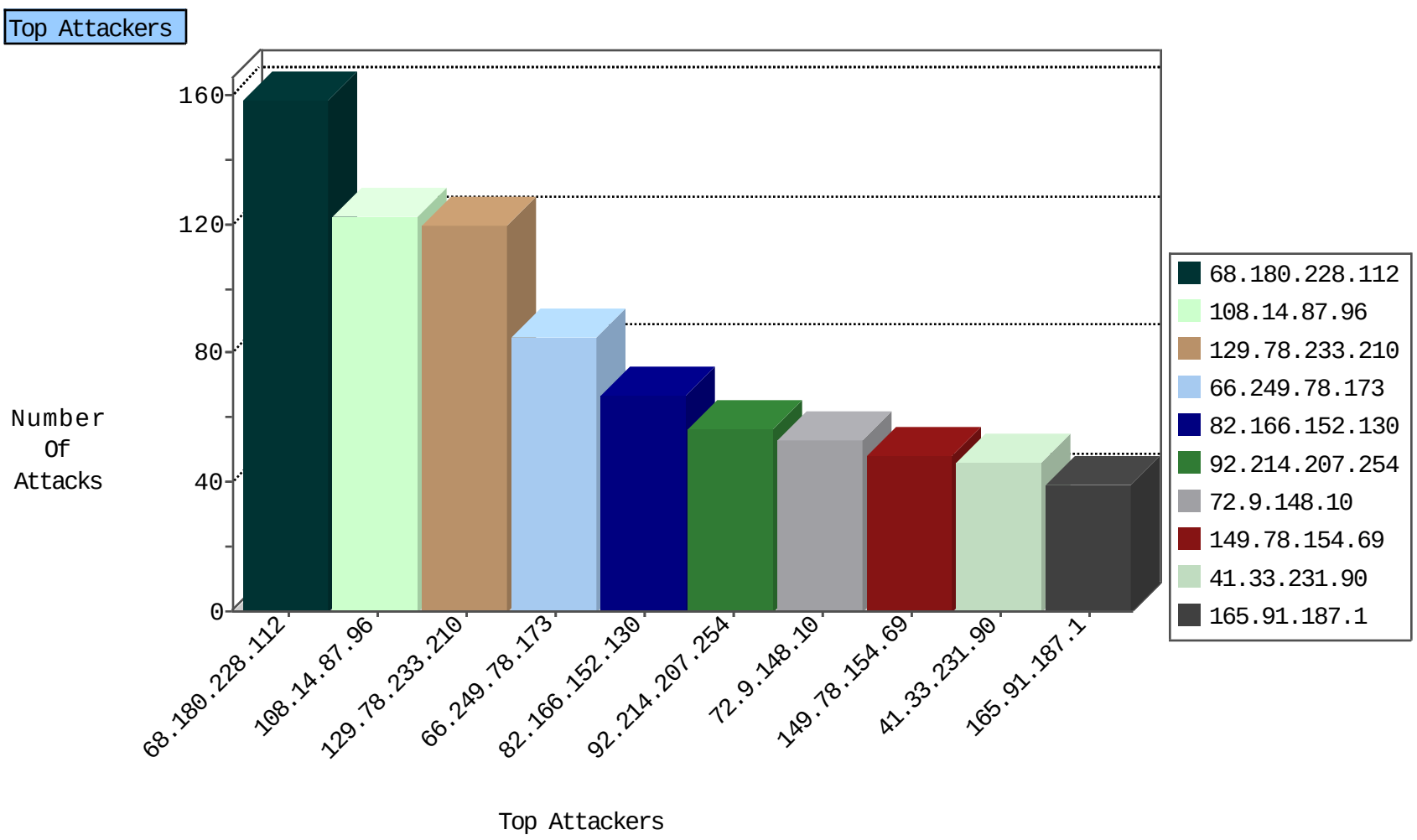
10-19-2015-06:04:02 to 10-19-2015-07:04:02

IDF Under Attack Daily Report





10-19-2015-06:04:02 to 10-19-2015-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.218.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
85.64.120.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
67.86.168.116	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
172.56.21.96	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
85.64.120.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
222.186.34.48	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.248.172.98	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.100	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-19-2015-06:04:02 to 10-19-2015-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-06:04:02 to 10-19-2015-07:04:02

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	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.168.30	147.237.0.200	Brazil	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
98.102.200.172	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
79.143.180.44	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.143.180.44	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.180	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.180	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.107.17.72	147.237.77.178	Seychelles	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.168.30	147.237.0.200	Brazil	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
98.102.200.172	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
98.102.200.172	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
79.143.180.44	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.180	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.180	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-19-2015-06:04:02 to 10-19-2015-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.14.87.96	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	123
129.78.233.210	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	120
92.214.207.254	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
165.91.187.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
37.142.190.17	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
46.19.85.175	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	28
37.26.149.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.100	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
172.56.21.96	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
79.182.218.144	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
80.179.13.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
84.109.152.101	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
85.64.125.155	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
70.199.105.196	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
75.166.199.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
46.19.86.250	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
184.38.206.174	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
79.177.151.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
76.218.200.134	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
2.54.3.43	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
67.86.168.116	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
46.19.85.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
79.181.15.55	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
79.181.177.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
1.47.232.123	Thailand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
157.55.39.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
176.12.136.157	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
79.178.139.201	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
162.243.62.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.24	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
65.30.171.129	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
2.52.144.249	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
66.249.64.178	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4

10-19-2015-06:04:02 to 10-19-2015-07:04:02

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	Distributed Suspicious Response Code	Block	143
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
82.166.152.130	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.152.130	Block	39
82.166.152.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	26
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	26
157.55.39.198	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	13
66.249.81.133	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve	Block	13
180.153.185.241	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/clientscripts/faq/faq.js%3fsiteversion	Block	13
65.55.210.65	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
217.12.204.134	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	13
87.69.127.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20956-he/dover.aspx×″×ž×©×™×›×•	Block	13
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/giyus/qanda/default.asp	None	13
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
94.159.191.0	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
207.46.13.190	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	13
78.128.92.202	Bulgaria	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	13
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
208.113.197.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149	Block	13

10-19-2015-06:04:02 to 10-19-2015-07:04:02