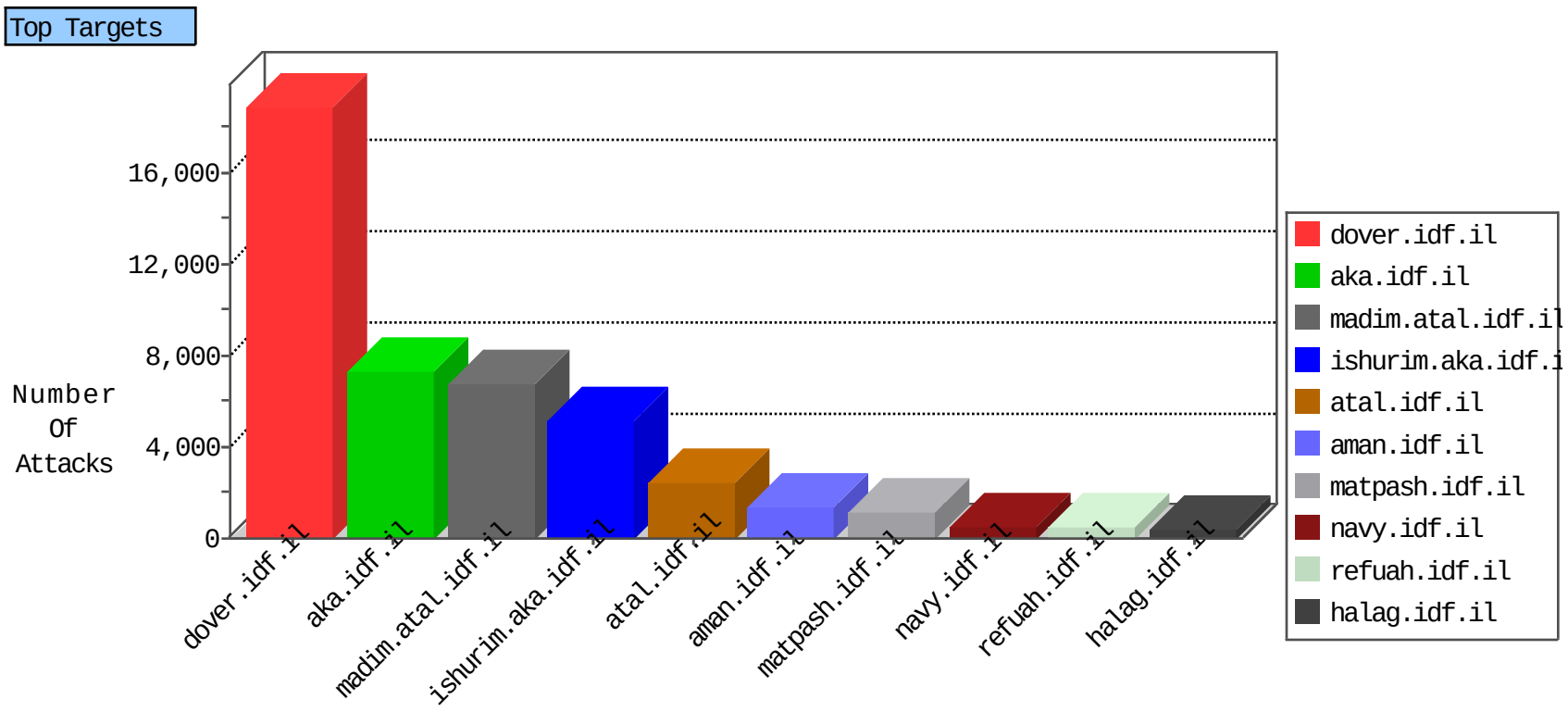
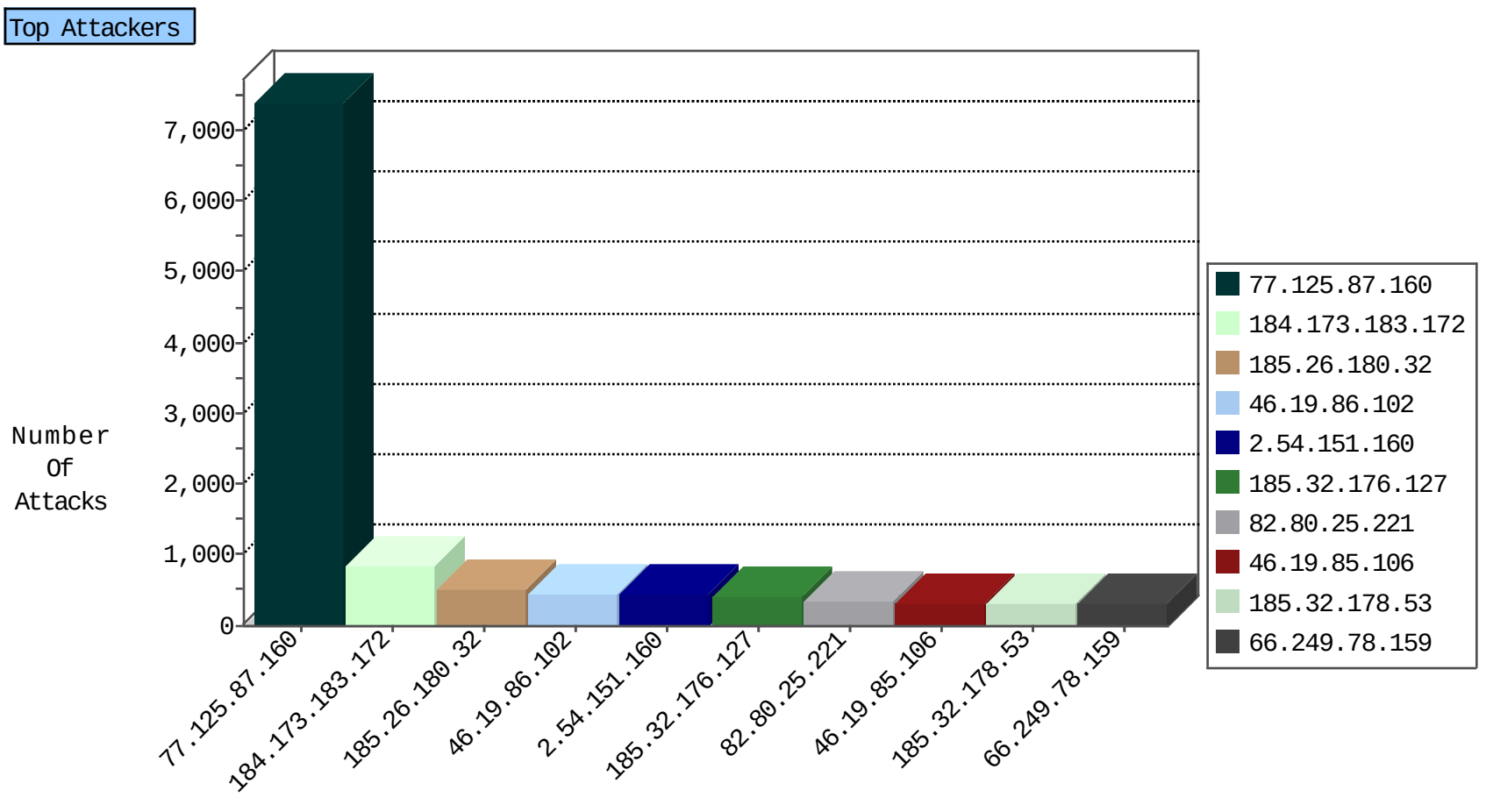
03-09-2015-00:00:04 to 03-10-2015-00:00:04

IDF Under Attack Daily Report





03-09-2015-00:00:04 to 03-10-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
134.134.139.78	United States	147.237.72.167	ishurim.aka.idf.i	TCP handshake violation, first packet not syn	drop	50197
85.65.245.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1563
5.29.179.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1472
109.67.212.167	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1147
87.68.9.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	442
79.180.50.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	422
212.68.154.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	334
109.253.158.20	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	273
109.253.128.105	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	266
109.253.157.23	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	249
109.65.170.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
93.172.175.166	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	238
85.64.72.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
77.127.25.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
212.76.103.9	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	198
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
109.253.139.54	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	185
62.219.163.84	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
87.69.135.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	173
149.78.227.62	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	165
93.172.60.64	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
77.127.101.55	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
46.19.86.39	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	152
5.29.7.197	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	139
46.117.131.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
109.253.136.222	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	127
81.218.85.170	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	123
79.178.17.244	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	120
2.54.61.163	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	119
46.117.122.97	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
199.203.172.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
82.102.141.249	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	99
109.253.129.228	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
2.54.45.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
2.54.51.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
37.142.87.98	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.13.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
80.246.139.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
109.253.157.239	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
84.109.49.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
2.54.25.129	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
46.120.166.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
84.94.63.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
85.64.218.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
79.180.100.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
85.250.32.107	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
2.54.13.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	75
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.85.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	74

03-09-2015-00:00:04 to 03-10-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	4493
77.125.87.160	Israel	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	1983
77.125.87.160	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	640
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	435
77.125.87.160	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	292
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	244
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	139
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	136
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	123
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	109
85.64.219.113	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	96
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	93
91.200.12.26	Ukraine	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
77.127.242.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	29
185.22.224.96	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	18
108.168.219.174	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
108.168.219.174	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
138.134.102.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
2.54.30.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
46.116.255.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
5.29.174.197	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	7
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	7
213.133.100.37	Germany	147.237.77.121	e.navy.idf.il	DVRep_P-N_40-59	Permit	6
138.134.102.16	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.35	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
68.174.240.245	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	6
78.46.173.58	Germany	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.180	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
93.172.34.244	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.69.206.198	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.154	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
46.19.85.169	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.219	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.4	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5

03-09-2015-00:00:04 to 03-10-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	344
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	112
2.52.155.235	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
46.19.86.181	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	5
77.126.232.107	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
85.64.145.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.28	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	4
213.6.234.24	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL Injection - Select From	3
82.165.24.123	Germany	147.237.77.74	law.idf.il	SQL Injection - Select From	3
2.54.165.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
79.176.43.230	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	3
46.19.86.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.160.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.120	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
115.231.218.23	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.189.239	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
212.179.61.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
176.53.126.2	Turkey	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
176.53.126.2	Turkey	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
31.168.77.253	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.11.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.53.126.2	Turkey	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
213.251.182.10	France	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
87.68.80.214	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.52.22.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.33.122	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
109.186.24.74	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.39.86.39	France	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.23	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
66.102.6.202	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
149.88.69.180	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.23	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
54.83.174.70	United States	147.237.72.167	ishurim.aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
176.53.126.2	Turkey	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.23	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
94.188.158.91	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
213.251.182.10	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.118.48.248	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
213.251.182.10	France	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
66.249.78.21	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
176.53.126.2	Turkey	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2

03-09-2015-00:00:04 to 03-10-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.32	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	516
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	264
216.52.215.232	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	242
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	218
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	214
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	212
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	186
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	168
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	103
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	86
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
66.249.75.200	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
38.111.147.86	United States	147.237.76.42	refuah.idf.il		drop	drop	70
66.249.75.184	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
66.249.75.216	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
81.218.148.177	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	61
173.254.199.136	United States	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	60
173.254.199.136	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	60
84.95.252.59	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
176.12.150.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
110.85.234.57	China	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	51
212.117.143.250	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
109.253.141.231	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.137.154	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
80.230.89.243	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	47
79.183.50.135	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
176.12.145.100	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.140.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.137.236	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.137.207	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
79.178.115.18	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
176.12.143.108	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
79.179.138.150	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
132.65.44.83	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.253.144.151	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
84.95.58.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
176.12.137.87	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.138.8	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.151.122	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.138.117	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.150.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.144.186	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
79.176.10.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
109.253.143.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.140.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
82.80.58.78	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
62.90.100.202	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	454
2.54.151.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	434
185.32.176.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	419
185.32.178.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	324
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	278
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	263
185.32.176.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	248
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	232
80.246.141.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	201
176.12.148.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	181
2.52.149.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	173
2.54.148.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
80.246.139.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	143
80.246.141.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	132
109.253.139.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	121
176.12.148.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
79.176.51.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
2.54.20.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
2.54.55.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	114
109.253.128.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	88
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	88
109.253.145.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	81
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	78
176.12.143.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	76
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	75
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
109.253.144.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73
2.52.149.79	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.149.79	Block	72
87.69.141.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
2.54.177.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
109.253.137.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.134.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.134.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
109.253.149.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
109.253.146.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
109.253.137.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
2.54.26.165	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.26.165	Block	50
109.253.158.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
80.246.139.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
109.253.157.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
109.253.157.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
109.253.141.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
176.12.145.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.132	Block	39
109.253.136.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
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	37
37.26.146.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
46.19.86.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35