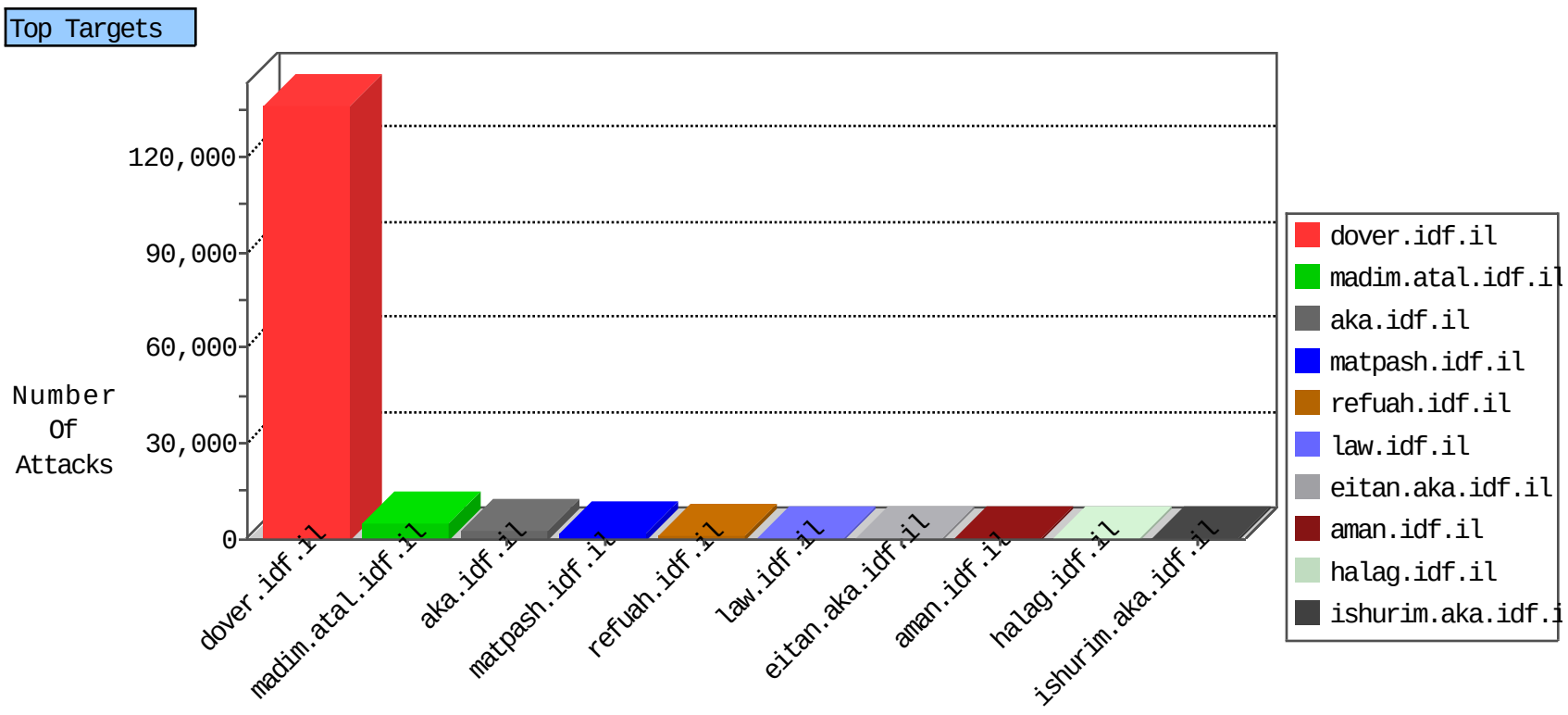
06-21-2015-00:00:01 to 06-22-2015-00:00:01

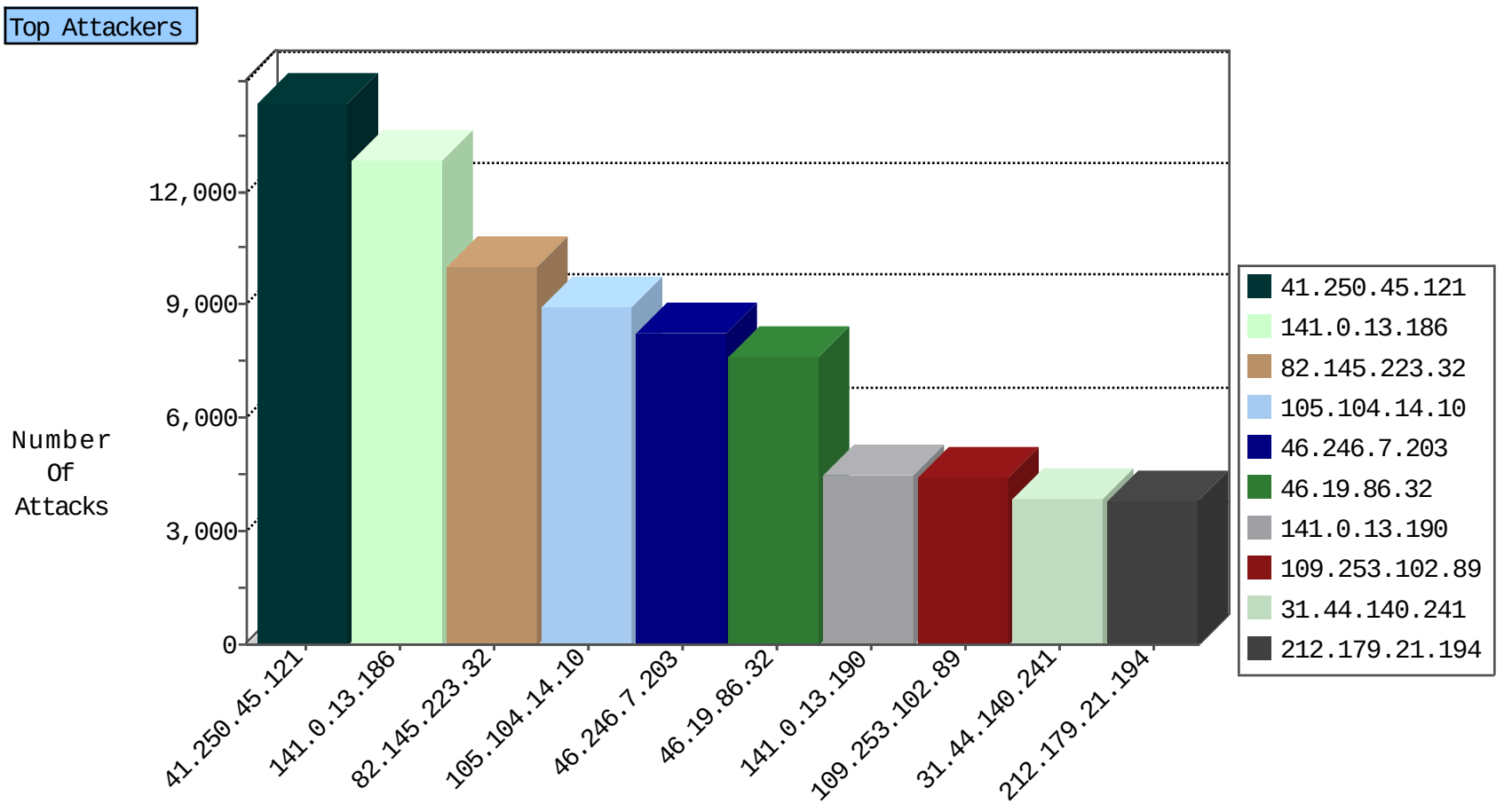
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

06-21-2015-00:00:01 to 06-22-2015-00:00:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
141.0.13.186	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23784
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3850
79.176.14.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2741
194.90.99.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2703
141.0.13.190	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1484
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	716
66.249.64.156	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	617
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	536
85.64.79.228	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	527
76.164.214.83	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	493
84.94.191.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	470
46.19.86.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	441
79.179.152.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	387
109.66.198.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	373
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	341
84.109.90.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	335
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	329
37.142.104.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	304
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	286
79.179.32.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
220.181.108.85	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	237
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
84.94.104.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	215
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
87.68.215.168	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	213
109.160.135.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
82.81.240.47	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
149.78.44.187	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	136
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
66.249.64.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	128
220.255.145.145	Singapore	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	125
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
37.187.157.108	France	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	118
79.180.99.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
5.29.117.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
213.57.228.45	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
79.182.208.146	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
84.108.109.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	97
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	97
84.109.127.56	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
109.253.146.227	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
82.102.141.250	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
5.29.33.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
109.253.146.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
85.65.145.55	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
2.54.154.140	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	82

06-21-2015-00:00:01 to 06-22-2015-00:00:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1005
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	360
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	344
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	237
184.173.183.172	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	138
138.134.192.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	29
81.218.251.250	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
178.234.239.198	Russian Federation	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
191.213.176.242	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
147.235.185.74	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
185.71.140.76		147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
207.232.41.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	6
62.0.42.2	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
89.138.195.157	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
222.84.4.160	China	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
212.179.150.17	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4
185.71.140.76		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
94.230.86.195	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	7610: IP Reputation	Block	4
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4

06-21-2015-00:00:01 to 06-22-2015-00:00:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.19.85.227	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	124
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	94
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
43.255.188.131	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
61.183.128.6	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.16	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
192.3.108.133	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
46.101.48.216	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.130	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.158	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.8.46	e.chinuch.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
66.249.78.174	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.133	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.21	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.133	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
184.154.207.42	United States	147.237.0.34	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.188.133	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2

06-21-2015-00:00:01 to 06-22-2015-00:00:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.250.45.121	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14239
141.0.13.186	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12700
82.145.223.32	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9997
105.104.14.10	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8913
46.246.7.203	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8264
46.19.86.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7418
141.0.13.190	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4435
109.253.102.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4414
31.44.140.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3847
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3584
2.54.147.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2540
79.182.202.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1778
164.138.114.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1551
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1243
85.250.140.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1027
46.19.85.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	973
193.28.155.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	874
178.62.202.236	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	868
79.183.116.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	791
95.86.70.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	622
95.86.116.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	505
212.199.11.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	504
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	496
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	469
50.118.172.147	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	463
37.26.147.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	462
46.19.86.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	453
200.81.38.157	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	412
37.8.49.42	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	395
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	370
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	361
84.228.201.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	359
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	351
109.42.0.4	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	349
213.151.42.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	342
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	323
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	321
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
188.165.15.95	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	302
2.54.26.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	298
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	294
212.235.69.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	291
212.76.112.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	286
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
84.94.32.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.114.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1404
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	477
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	451
109.253.133.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	423
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	418
193.106.54.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	406
185.32.178.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	305
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	226
2.54.131.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	210
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	157
176.12.150.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.213	Block	153
5.29.202.44	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.202.44	Block	145
185.32.178.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	141
5.29.83.134	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 5.29.83.134	Block	137
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
109.253.139.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.139.59	Block	105
31.168.143.10	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 31.168.143.10	Block	98
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	90
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	89
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	89
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	81
95.175.35.73	Israel	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	69
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
2.54.139.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	68
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
109.66.18.25	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 109.66.18.25	Block	56
109.253.132.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
176.12.145.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
37.8.60.99	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	51
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	51
176.12.137.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
176.12.148.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
37.26.147.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
37.142.114.52	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected , Observed ********** ********** ********** *	None	24
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
80.246.130.185	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 80.246.130.185	Block	18
176.12.137.168	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	17
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
2.54.164.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	15
46.19.85.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15