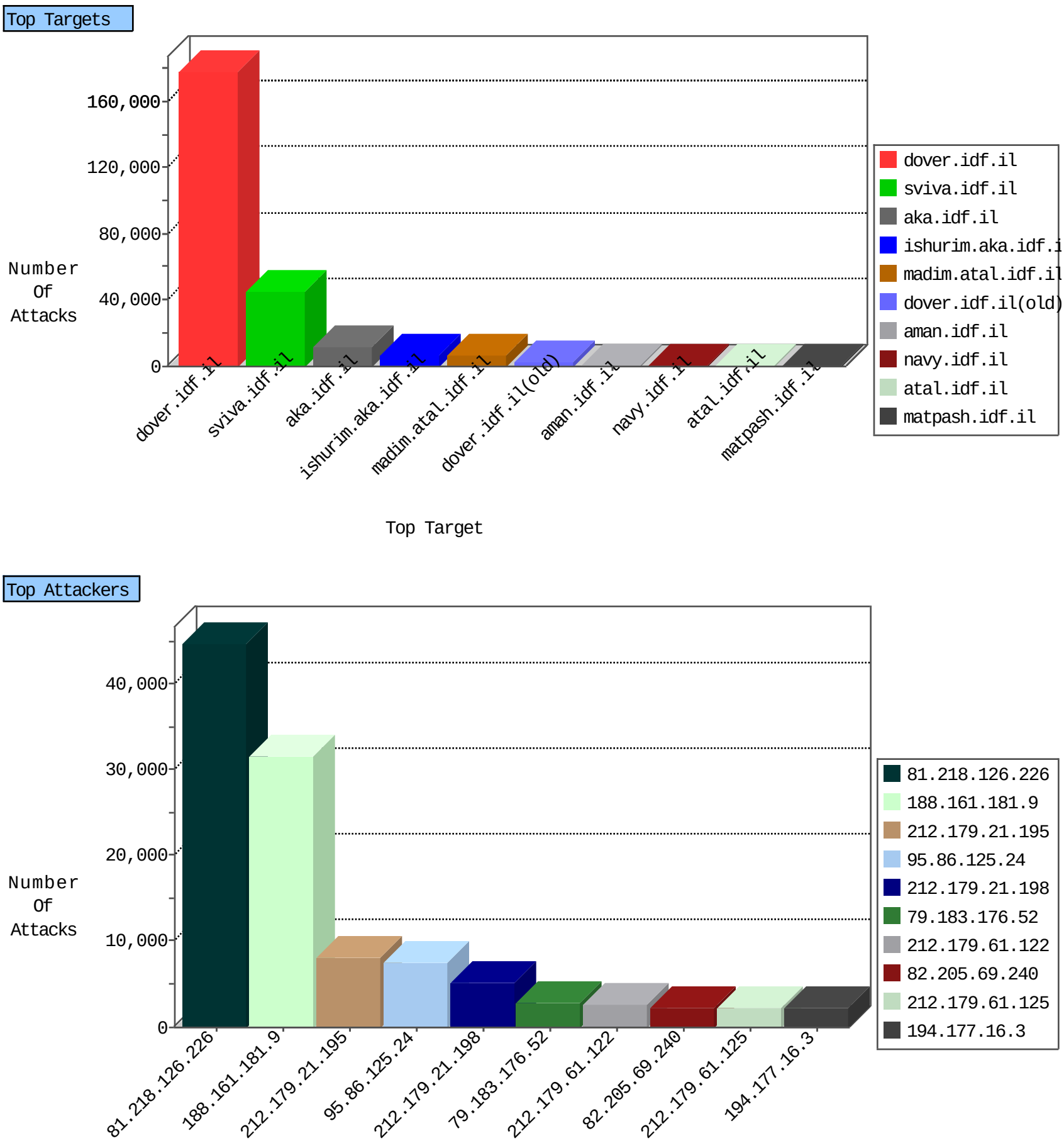
11-13-2014-00:00:06 to 11-14-2014-00:00:06

IDF Under Attack Daily Report



11-13-2014-00:00:06 to 11-14-2014-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.160.251.227	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6475
193.68.41.17	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3279
212.179.61.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3174
66.249.69.105	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	2732
5.28.169.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2542
5.43.203.176	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2502
46.32.210.219	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2002
81.218.126.226	Israel	147.237.77.235	sviva.idf.il	TCP Scan (vertical)	drop	1691
66.249.91.66	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	744
79.178.171.226	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	543
82.205.69.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	413
197.30.73.142	Tunisia	147.237.77.234	halag.idf.il	TCP Scan (vertical)	drop	371
37.26.146.171	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
132.64.67.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	285
66.249.78.115	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	199
80.246.138.220	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
94.159.185.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	127
98.125.153.51	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	115
82.102.141.195	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	94
212.25.105.125	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	91
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	89
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	85
109.253.158.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	82
212.117.143.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	82
82.166.212.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
77.125.148.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	63
5.29.38.167	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	63
81.218.126.226	Israel	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	62
93.173.130.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
46.121.239.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	40
197.119.195.4	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	39
95.179.37.211	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
85.250.69.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
82.102.141.254	Israel	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	24
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
62.207.60.228	Netherlands	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	23
46.19.86.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
82.145.218.27	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
46.19.86.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.178.153.128	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.179.18.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
82.102.141.194	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid TCP Flags	drop	18
80.246.139.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
82.102.141.201	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	17
208.84.104.19	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
109.160.157.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
109.253.129.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
81.218.126.226	Israel	147.237.77.235	sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	14
176.12.156.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
87.68.147.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12

11-13-2014-00:00:06 to 11-14-2014-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	95
87.69.122.71	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
183.49.17.105	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
91.235.168.194	Sweden	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	7
105.225.7.23	South Africa	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.34.12.119	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.12.221	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
194.140.248.20	Hungary	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
184.168.193.42	United States	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	4
82.102.141.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
2.54.12.16	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
87.69.214.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
50.63.196.46	United States	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	4
41.199.2.241	Egypt	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	3
91.235.168.194	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
132.170.162.28	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.59.66	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.28.188.157	Israel	147.237.72.14	dover.idf.il(old	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.151.52.38	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
46.19.86.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.180.68	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.232.97	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.190.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.69.132.120	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
128.235.234.93	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
76.219.183.30	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.75.252.112	Germany	147.237.72.14	dover.idf.il(old	C041: HTTP: Access to - index.php?option=com_jce	Block	2
111.67.22.10	Australia	147.237.72.14	dover.idf.il(old	C041: HTTP: Access to - index.php?option=com_jce	Block	2
46.120.245.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.159.182.160	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.153	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.102.194.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.206	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
142.4.4.174	United States	147.237.72.14	dover.idf.il(old	C041: HTTP: Access to - index.php?option=com_jce	Block	2
213.6.177.116	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
50.63.202.30	United States	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	2
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	Block_Level_70_100	Block	2
96.242.55.54	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
209.134.142.193	United States	147.237.72.14	dover.idf.il(old	C041: HTTP: Access to - index.php?option=com_jce	Block	2
120.43.30.53	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
85.181.91.251	Germany	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.95.88.100	Israel	147.237.76.86	navy.idf.il	C066: HTTP: .conf Access	Block	2
213.57.108.4	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.177.176	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

11-13-2014-00:00:06 to 11-14-2014-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	90
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	85
82.102.141.201	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	60
2.54.36.5	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	18
85.65.239.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
76.95.231.86	United States	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
197.30.73.142	Tunisia	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
37.26.147.185	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
187.40.45.232	Brazil	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
91.236.75.11	Poland	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
85.64.51.68	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.110.15	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.103.64.112	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.186.181.203	Israel	147.237.77.74	law.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	2
192.126.120.49	United States	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
212.235.89.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.44.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.91.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.59.249	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.168.183.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.2.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.125.71.200	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
109.64.177.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.180	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.251.235	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.254.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	2
121.125.71.200	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
87.69.211.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
85.250.19.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.95.88.100	Israel	147.237.76.86	navy.idf.il	SQL Injection - Paranoid	2
91.236.75.11	Poland	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
59.106.108.116	Japan	147.237.72.14	dover.idf.il(old)	Tehila - Perl LWP with fake user agent	2
85.64.215.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.229.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.137.111	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.7.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.210.187.107	Israel	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
149.78.116.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.102.141.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.146.142	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.146.122.183	Vietnam	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
77.126.2.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.103.64.112	United States	147.237.72.14	dover.idf.il(old)	Tehila - Perl LWP with fake user agent	2
81.218.100.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.235.55.247	Israel	147.237.72.14	dover.idf.il(old)	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	2
46.19.85.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.230.74.149	Israel	147.237.72.14	dover.idf.il(old)	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	2

11-13-2014-00:00:06 to 11-14-2014-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.126.226	Israel	147.237.77.235	sviva.idf.i	Invalid ACK number	Bad TCP sequence	monitor	39714
188.161.181.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	illegal header format detected: Illegal start li in request	Block HTTP Non Compliant	monitor	10447
212.179.21.195	Israel	147.237.77.216	dover.idf.i		drop	drop	8140
95.86.125.24	Israel	147.237.77.216	dover.idf.i		drop	drop	7601
212.179.21.198	Israel	147.237.77.216	dover.idf.i		drop	drop	5260
79.183.176.52	Israel	147.237.77.216	dover.idf.i		drop	drop	2755
212.179.61.122	Israel	147.237.77.216	dover.idf.i		drop	drop	2687
82.205.69.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i		drop	drop	2225
212.179.61.125	Israel	147.237.77.216	dover.idf.i		drop	drop	2224
194.177.16.3	Israel	147.237.77.216	dover.idf.i		drop	drop	2194
79.180.141.23	Israel	147.237.77.216	dover.idf.i		drop	drop	2168
188.120.148.108	Israel	147.237.77.216	dover.idf.i		drop	drop	1999
212.179.61.127	Israel	147.237.77.216	dover.idf.i		drop	drop	1953
197.205.220.237	Algeria	147.237.77.216	dover.idf.i		drop	drop	1940
212.179.21.194	Israel	147.237.77.216	dover.idf.i		drop	drop	1766
46.19.86.160	Israel	147.237.77.216	dover.idf.i		drop	drop	1545
41.33.231.86	Egypt	147.237.77.216	dover.idf.i		drop	drop	1502
193.68.41.17	Hungary	147.237.77.216	dover.idf.i		drop	drop	1487
212.179.21.196	Israel	147.237.77.216	dover.idf.i		drop	drop	1341
95.86.84.23	Israel	147.237.77.216	dover.idf.i		drop	drop	1131
208.115.113.89	United States	147.237.77.216	dover.idf.i		drop	drop	1123
54.72.0.55	United States	147.237.77.216	dover.idf.i		drop	drop	948
54.72.73.168	United States	147.237.77.216	dover.idf.i		drop	drop	923
2.54.170.130	Israel	147.237.77.216	dover.idf.i		drop	drop	895
212.179.46.19	Israel	147.237.77.216	dover.idf.i		drop	drop	852
188.161.181.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i		drop	drop	820
37.142.79.112	Israel	147.237.77.216	dover.idf.i		drop	drop	793
213.184.43.211	Estonia	147.237.77.216	dover.idf.i		drop	drop	789
208.115.111.73	United States	147.237.77.216	dover.idf.i		drop	drop	777
212.179.46.21	Israel	147.237.77.216	dover.idf.i		drop	drop	772
41.199.2.241	Egypt	147.237.77.216	dover.idf.i		drop	drop	732
46.19.85.55	Israel	147.237.77.216	dover.idf.i		drop	drop	730
81.218.126.226	Israel	147.237.77.235	sviva.idf.i	command injection detected in request: 'ping'	Command Injection	monitor	677
193.43.245.250	Israel	147.237.77.216	dover.idf.i		drop	drop	649
193.43.246.250	Israel	147.237.77.216	dover.idf.i		drop	drop	648
66.249.78.158	United States	147.237.77.216	dover.idf.i		drop	drop	610
41.33.232.65	Egypt	147.237.77.216	dover.idf.i		drop	drop	586
65.49.68.195	United States	147.237.77.216	dover.idf.i		drop	drop	574
91.235.168.194	Sweden	147.237.77.216	dover.idf.i		drop	drop	568
178.162.199.102	Germany	147.237.72.166	aka.idf.il		drop	drop	560
66.249.78.172	United States	147.237.77.216	dover.idf.i		drop	drop	540
50.87.144.145	United States	147.237.77.216	dover.idf.i		drop	drop	524
77.127.154.35	Israel	147.237.77.216	dover.idf.i		drop	drop	518
81.218.126.226	Israel	147.237.77.235	sviva.idf.i	command injection detected in URL: 'ping'	Command Injection	monitor	502
217.169.229.157	Netherlands	147.237.77.216	dover.idf.i		drop	drop	498
68.180.228.121	United States	147.237.77.216	dover.idf.i		drop	drop	496
31.210.187.115	Israel	147.237.77.216	dover.idf.i		drop	drop	490
2.54.21.158	Israel	147.237.77.216	dover.idf.i		drop	drop	487
46.19.85.224	Israel	147.237.77.216	dover.idf.i		drop	drop	484
95.86.75.211	Israel	147.237.77.216	dover.idf.i		drop	drop	455

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.161.181.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Malformed URL from 188.161.181.9	Block	10320
188.161.181.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 188.161.181.9	Block	9970
109.253.133.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.133.67	Block	611
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	416
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.213	Block	396
109.253.159.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	349
2.54.137.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	323
109.253.137.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	314
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
82.102.141.212	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.141.212	Block	290
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	282
37.26.146.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	274
2.54.157.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
109.253.133.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	247
66.249.78.101	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.101	Block	229
10.110.110.38		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	207
66.249.78.94	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.94	Block	199
80.246.138.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
176.12.139.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.74	Block	187
82.102.141.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
66.249.78.108	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.108	Block	177
185.32.179.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
84.109.12.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	169
37.26.148.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
2.54.43.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
87.69.136.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	141
79.176.165.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
80.246.140.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
176.12.148.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
79.177.199.150	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.199.150	Block	107
176.12.150.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
80.246.139.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.138.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
80.246.138.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
149.78.166.10	United States	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	70
207.46.13.46	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	68
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	60
84.108.20.61	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	51
5.29.53.88	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	48
87.68.251.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/glyus	Block	48
85.64.228.146	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	48
46.116.155.64	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	47
176.12.139.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
80.246.139.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
79.180.142.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	42
213.57.225.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	39
66.249.69.204	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.204	Block	38
84.94.24.15	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	37
87.69.122.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	35