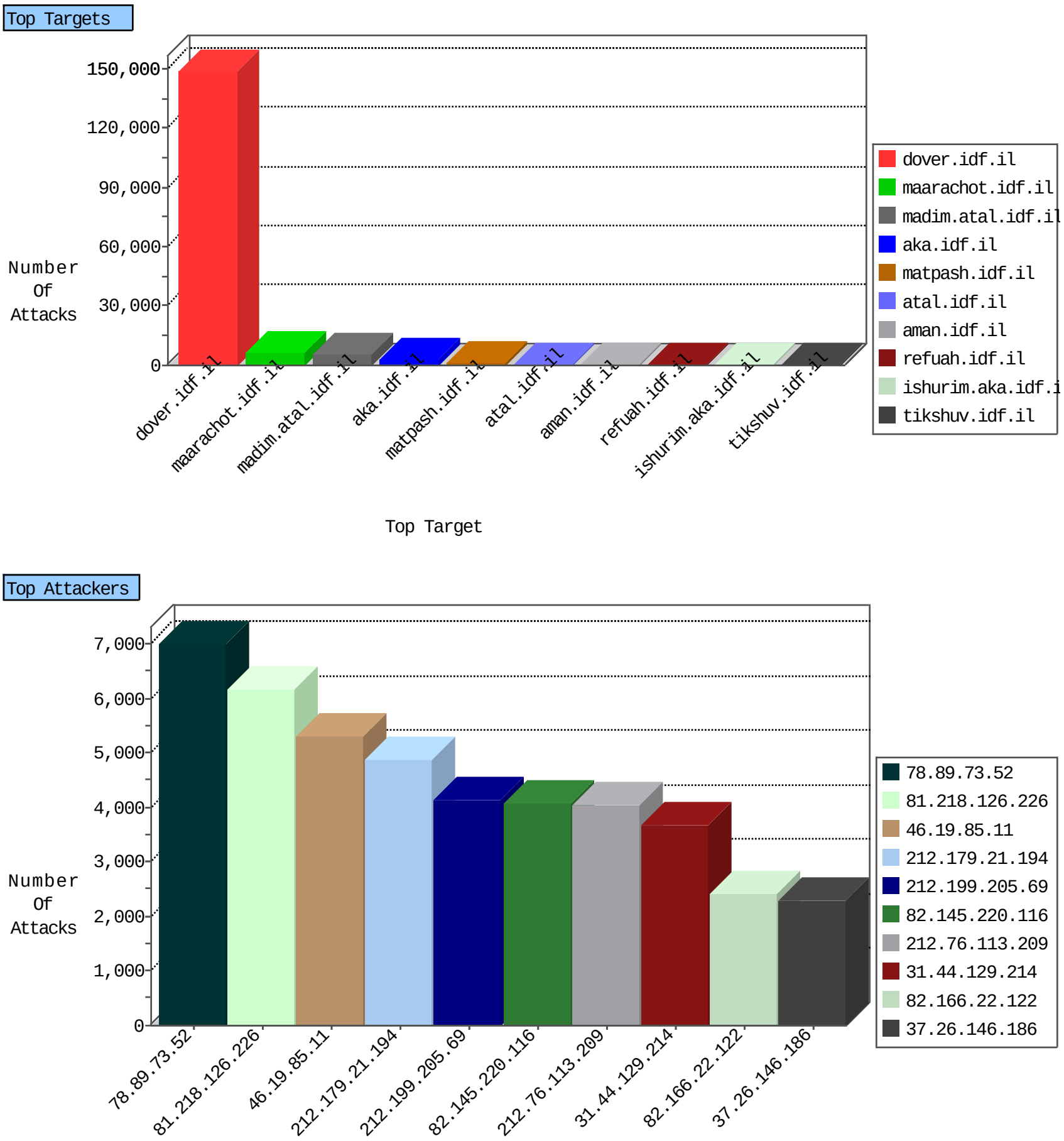
06-29-2015-00:00:02 to 06-30-2015-00:00:02

IDF Under Attack Daily Report



06-29-2015-00:00:02 to 06-30-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
81.218.126.226	Israel	147.237.77.170	maarachot.idf.il	TCP Scan (vertical)	drop	30791
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8600
66.249.93.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3076
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3022
176.12.136.161	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2665
212.25.82.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2525
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1922
105.200.80.137	Egypt	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	1549
66.249.73.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1379
82.166.22.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	995
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	854
109.66.113.204	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	853
66.249.73.217	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	610
5.28.167.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	596
79.183.208.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	575
109.67.236.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	500
31.13.167.176	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	374
84.109.17.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	355
193.188.65.156	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
213.57.47.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	285
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	279
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	271
176.12.149.161	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
89.139.2.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	243
87.68.48.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
84.108.118.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
213.57.13.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
80.12.39.140	France	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	215
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
62.0.53.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	179
176.12.141.181	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
77.125.247.47	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	165
176.12.138.254	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
79.183.142.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
37.142.139.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
220.181.108.105	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	148
79.177.14.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
109.186.42.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
94.159.210.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
89.139.63.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
2.54.134.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
77.125.154.116	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
46.120.25.116	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
109.253.156.221	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91

06-29-2015-00:00:02 to 06-30-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
124.173.120.119	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	33
213.139.53.108	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	22
213.8.245.50	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	16
213.8.245.58	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
46.116.226.50	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
109.67.183.102	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
198.52.155.201	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.14	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.228.174.183	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.199.224.24	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.34.11.29	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.228.174.183	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
93.173.183.103	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.139.53.101	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.213.19.186	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.77.151	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.54.63.192	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.161.216	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
181.171.205.135	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
192.116.166.66	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.255	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
31.168.28.169	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.116.121.45	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
176.13.14.75	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
2.52.24.8	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
192.116.197.84	Israel	147.237.72.166	aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	3
46.19.85.51	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.159.28	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
62.219.180.180	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.125.92.152	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.166	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.213.56.162	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
203.229.137.1	Korea, Republic of	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.86.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.230.59.170	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
192.116.177.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.173.231.205	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.251.15.80	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
95.86.107.166	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.177.32.60	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
194.90.15.61	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
77.126.63.168	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.186.185.174	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.143.161.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
80.246.136.107	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.116.197.84	Israel	147.237.76.86	navy.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	2
46.19.85.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

06-29-2015-00:00:02 to 06-30-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
37.8.121.122	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	278
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	61
182.50.130.49	Singapore	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	8
182.50.130.49	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
132.72.224.217	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
82.166.22.122	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	5
43.255.188.135	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
197.52.123.162	Egypt	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	3
50.57.139.99	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	3
43.255.188.135	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.135	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	3
105.200.80.137	Egypt	147.237.77.216	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
61.183.128.6	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	3
43.255.188.134	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.66	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
80.74.100.131	Israel	147.237.77.216	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
43.255.188.132	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
105.200.80.137	Egypt	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
176.12.140.244	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	SQL Injection - Select From	2
43.255.188.134	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
43.255.188.132	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.201	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
202.85.209.77	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
176.12.140.244	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
61.183.128.6	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
95.86.111.227	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
43.255.188.134	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
66.249.75.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2

06-29-2015-00:00:02 to 06-30-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
78.89.73.52	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7015
46.19.85.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5318
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4811
212.199.205.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4149
82.145.220.116	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4080
212.76.113.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4057
31.44.129.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3679
82.166.22.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2384
212.150.214.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1633
46.116.249.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1495
105.200.80.137	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1495
197.28.4.189	Tunisia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1466
81.218.97.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1439
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1429
141.0.12.228	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1416
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1088
95.86.120.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1081
82.145.220.223	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1045
200.82.57.235	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1006
89.187.221.1	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	989
37.26.147.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	950
79.182.209.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	871
95.86.109.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	862
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	857
200.53.156.225	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	824
79.178.98.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	812
2.54.137.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	780
45.219.202.5		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	768
109.64.54.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	762
164.138.124.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	740
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	737
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	736
192.115.83.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	732
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	722
46.19.86.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	674
38.64.174.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	673
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	661
95.86.71.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	611
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	562
149.88.197.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	547
37.26.147.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	534
79.182.15.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
185.26.182.32	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	496
2.54.132.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	480
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	479
82.80.68.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	471
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	465
66.249.73.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	456
193.104.77.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	456
85.250.114.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	430

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.146.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2230
176.13.9.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.9.30	Block	659
109.253.137.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	536
109.65.4.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	341
37.26.147.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
37.26.147.155	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.155	Block	270
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.110	Block	257
2.54.39.105	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.39.105	Block	243
80.246.136.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
185.32.178.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
2.54.42.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	139
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	137
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	127
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
188.166.86.38	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.166.86.38	Block	66
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
2.54.162.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
207.46.13.18	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.18	Block	48
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	46
176.12.138.159	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.138.159	Block	46
157.55.39.85	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.85	Block	46
54.187.55.213	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	38
157.55.39.11	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.11	Block	32
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
2.54.15.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
109.253.143.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.143.99	Block	21
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	20
207.46.13.144	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.144	Block	18
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
79.180.10.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
46.120.9.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	16
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.4.132.226	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.4.132.226	Block	15
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	14
79.180.49.153	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.180.49.153	Block	11
195.60.232.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
176.12.148.156	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	9
207.46.13.144	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	9
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	9
80.246.136.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	9
87.69.28.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	8
85.250.187.99	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	8
79.182.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
176.13.21.133	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
109.66.52.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/sachar/undefined	Block	8
2.54.30.189	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7