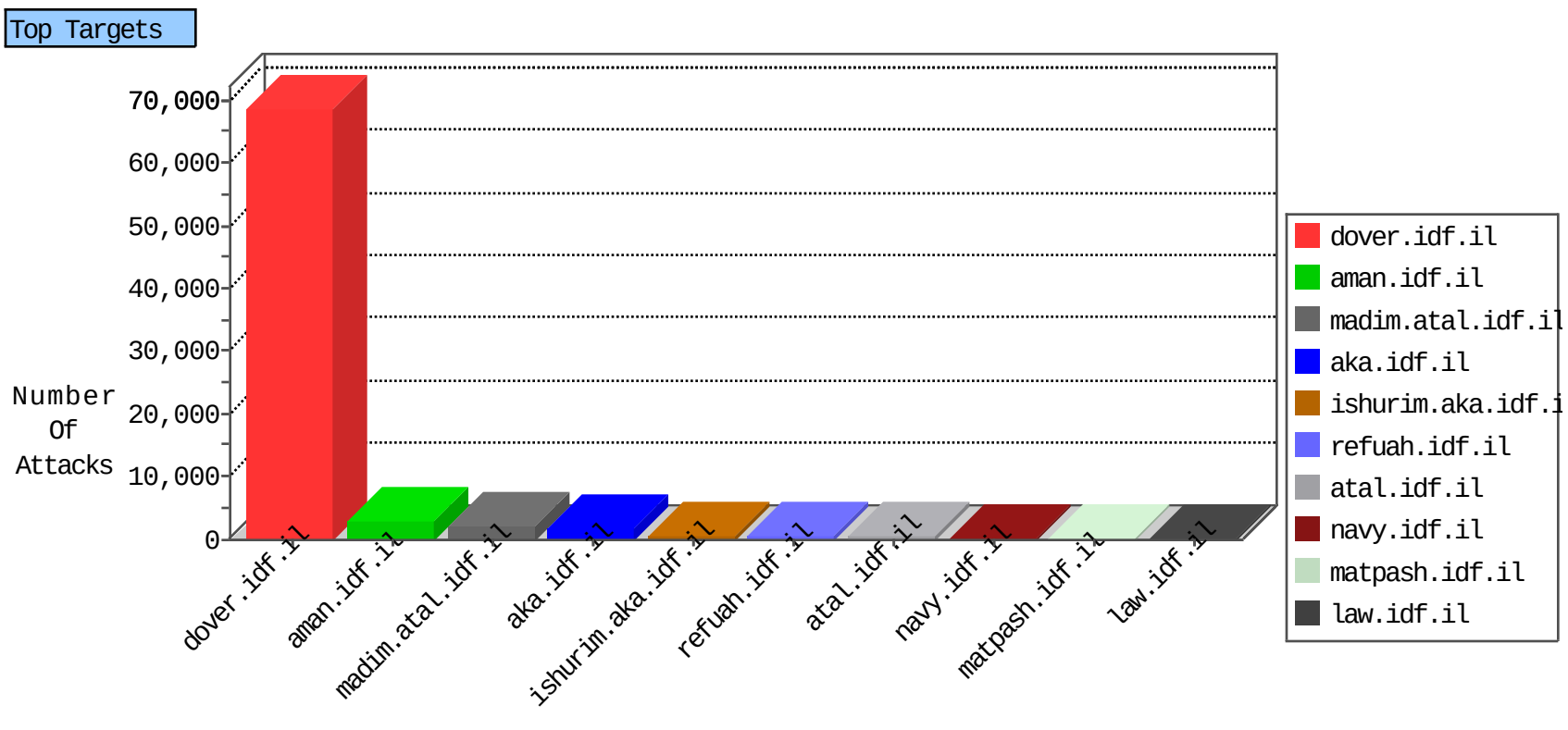
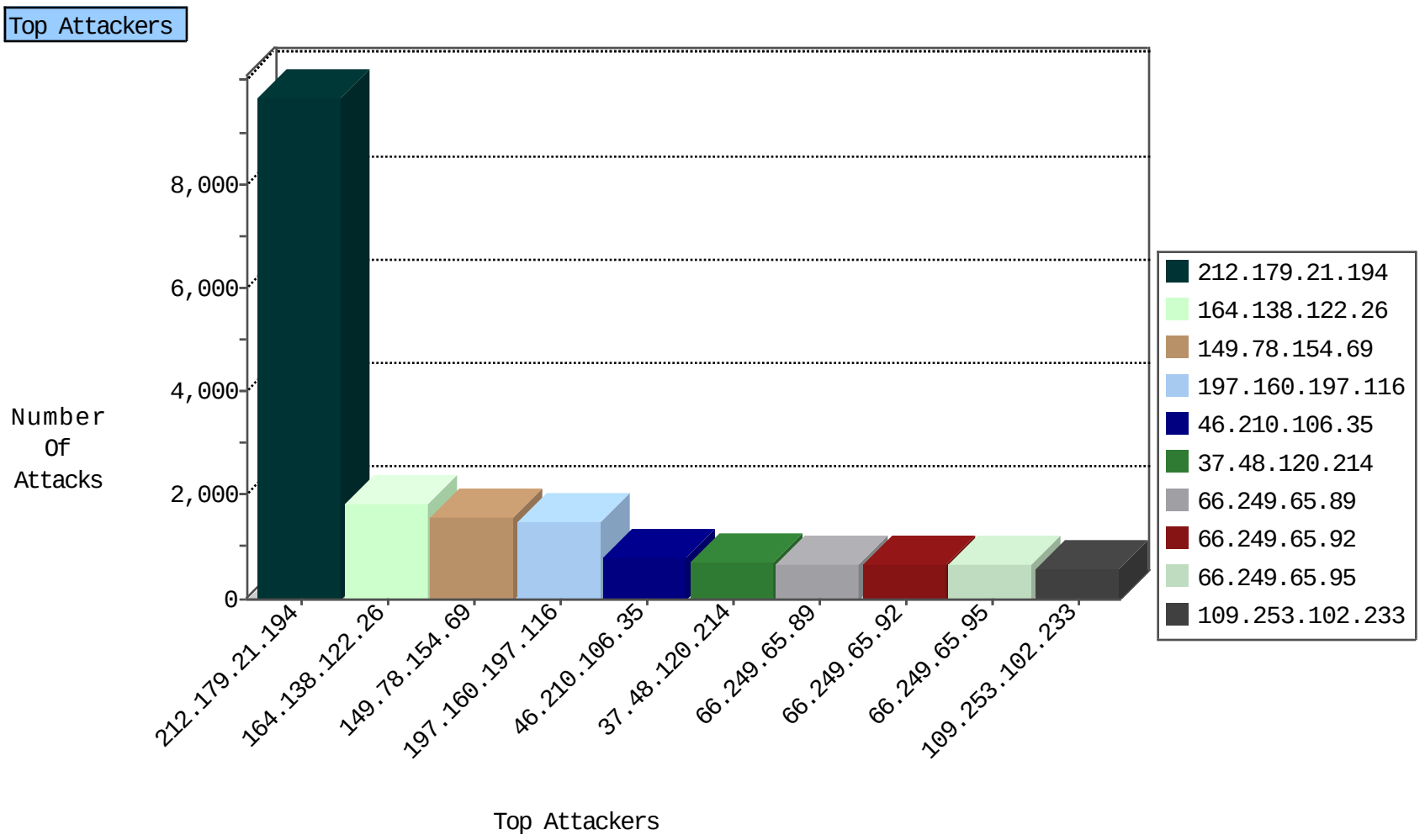
07-16-2015-00:00:04 to 07-17-2015-00:00:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-16-2015-00:00:04 to 07-17-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
192.198.151.43	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	14593
185.17.235.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6931
185.17.235.31	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6914
66.249.83.153	Israel	147.237.0.15	kosher-kravi.idf.i	TCP handshake violation, first packet not syn	drop	4915
66.249.67.27	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4811
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4664
52.28.175.49	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	4572
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4314
209.197.30.174	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2966
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	799
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	547
79.176.138.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	450
79.177.130.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	448
66.249.65.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	410
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	378
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	368
212.235.8.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	338
79.183.29.70	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	301
87.69.136.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	294
79.183.196.45	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
188.120.148.180	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
109.64.3.210	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
46.116.211.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	236
213.57.55.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
46.120.94.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
5.29.248.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
79.180.127.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
85.250.227.174	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	206
149.78.181.172	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	161
5.22.130.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
213.57.160.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
85.65.34.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
46.116.87.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	132
77.127.186.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
82.166.75.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
46.116.123.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
199.203.67.245	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
85.65.128.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
84.111.242.143	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
85.250.189.127	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
183.90.71.53	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	106
37.142.4.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
46.117.127.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
212.116.166.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	94
93.172.199.221	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.120.241.14	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
79.176.28.22	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
109.253.158.68	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81

07-16-2015-00:00:04 to 07-17-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.199.112.144	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
80.179.255.70	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
79.183.196.45	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
46.116.211.218	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
192.114.3.241	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
84.108.251.157	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
93.172.131.98	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.166.75.248	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.186.39.247	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
31.168.194.6	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.68.58.175	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
31.168.243.29	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.52.148.122	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.242.202.237	France	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.53	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
149.78.108.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
181.167.120.53	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
58.59.235.47	China	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
81.218.131.82	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
31.168.84.199	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.251	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.40	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.218	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.176.191.89	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.179.15.233	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.199.57.199	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.81.133	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.176.141.23	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
178.148.130.182		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.54	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.29.222.136	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
109.64.201.13	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.8.123.140	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.156.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.168.225	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.150.174.180	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
132.76.50.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
213.57.176.5	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
207.232.27.5	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.121.145.213	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
31.154.9.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.182.171.248	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.46.214.61	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

07-16-2015-00:00:04 to 07-17-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
99.48.176.9	United States	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	223
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	126
66.249.64.151	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	58
66.249.65.37	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	14
50.62.161.201	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	8
66.249.65.16	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
61.183.128.6	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	3
223.130.24.20	Australia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
221.203.3.117	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
46.118.119.63	Ukraine	147.237.77.74	law.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
62.212.73.138	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
176.58.123.82	United Kingdom	147.237.72.156	aman.idf.il	Tehila - Perl LWP with fake user agent	2
218.87.111.107	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	2
218.87.111.107	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
218.47.6.149	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
221.203.3.117	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
93.189.25.174	Austria	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
178.89.191.77	Kazakstan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
218.47.6.149	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
218.87.111.107	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.172	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
218.47.6.149	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
115.28.143.12	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.183.128.6	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
23.95.82.26	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
113.240.250.157	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.100	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
220.232.237.250	Hong Kong	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
64.34.216.214	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.55.121.17	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
162.246.18.136		147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.179.180.191	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.111.107	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
187.72.186.4	Brazil	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

07-16-2015-00:00:04 to 07-17-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9530
164.138.122.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1840
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1572
197.160.197.116	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1457
46.210.106.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	796
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	693
109.253.102.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	588
183.90.71.53	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	563
64.251.40.254	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	549
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	519
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	506
95.86.112.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	502
109.253.32.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	472
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	470
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	457
2.54.3.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	445
164.138.123.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	437
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	423
84.228.195.249	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	399
2.54.183.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
66.249.65.92	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	383
66.249.65.89	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	378
37.228.107.45	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	336
66.249.65.95	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	332
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	327
84.229.30.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
149.255.192.183	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	322
50.65.122.89	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	291
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	290
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
8.37.227.190	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	272
46.43.75.126	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
95.86.72.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	247
207.46.13.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	244
5.108.36.40	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	242
31.44.131.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	240
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
207.46.13.135	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208
68.180.228.176	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	207
95.86.68.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	205
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
1.38.22.231	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	191
79.178.3.192	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	183
188.165.15.193	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	175
46.19.85.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	174
79.183.127.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	169
66.249.65.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
205.203.135.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
66.249.65.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
66.249.65.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159

07-16-2015-00:00:04 to 07-17-2015-00:00:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.80.163.88	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.80.163.88	Block	438
46.117.26.179	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.26.179	Block	241
2.52.153.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	178
2.54.180.83	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.180.83	Block	166
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
2.52.8.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.8.148	Block	145
176.12.142.48	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.142.48	Block	136
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	118
2.52.23.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
2.54.58.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	93
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	79
109.66.113.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
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	44
84.228.153.87	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	27
167.114.64.100	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 167.114.64.100	Block	26
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	26
79.178.171.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/6_s3_	Block	24
197.160.197.116	Egypt	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 197.160.197.116	Block	20
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	20
197.160.197.116	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
188.165.15.193	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.193	Block	16
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	16
2.54.129.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	12
176.13.12.169	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.12.169	Block	10
115.78.235.170	Vietnam	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	10
85.250.148.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
189.208.88.3	Mexico	147.237.72.166	aka.idf.il	PHP Attempt	Block	9
79.183.217.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
109.66.7.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.116.77.60	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Parameter Type Violation on my-kosher-kravi.idf.il/templates/login/login.aspx parameter Master$ContentPlaceHolder1$password	Block	8
94.23.30.222	France	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 94.23.30.222	Block	8
176.13.12.169	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	8
213.57.106.115	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	8
176.13.16.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	7
84.132.43.116	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.132.43.116	Block	7
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
176.13.18.206	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
79.183.117.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
27.126.188.85	Hong Kong	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
212.150.174.180	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Parameter Type Violation on my-kosher-kravi.idf.il/templates/login/login.aspx parameter Master$ContentPlaceHolder1$password	Block	5
116.212.127.209	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
216.244.82.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main.asp/trackback/	Block	5
38.111.147.84	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	5
37.26.146.151	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il//categorytemplates/listchilddocuments/1152	Block	5
86.98.78.213	United Arab Emirates	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5

07-16-2015-00:00:04 to 07-17-2015-00:00:04