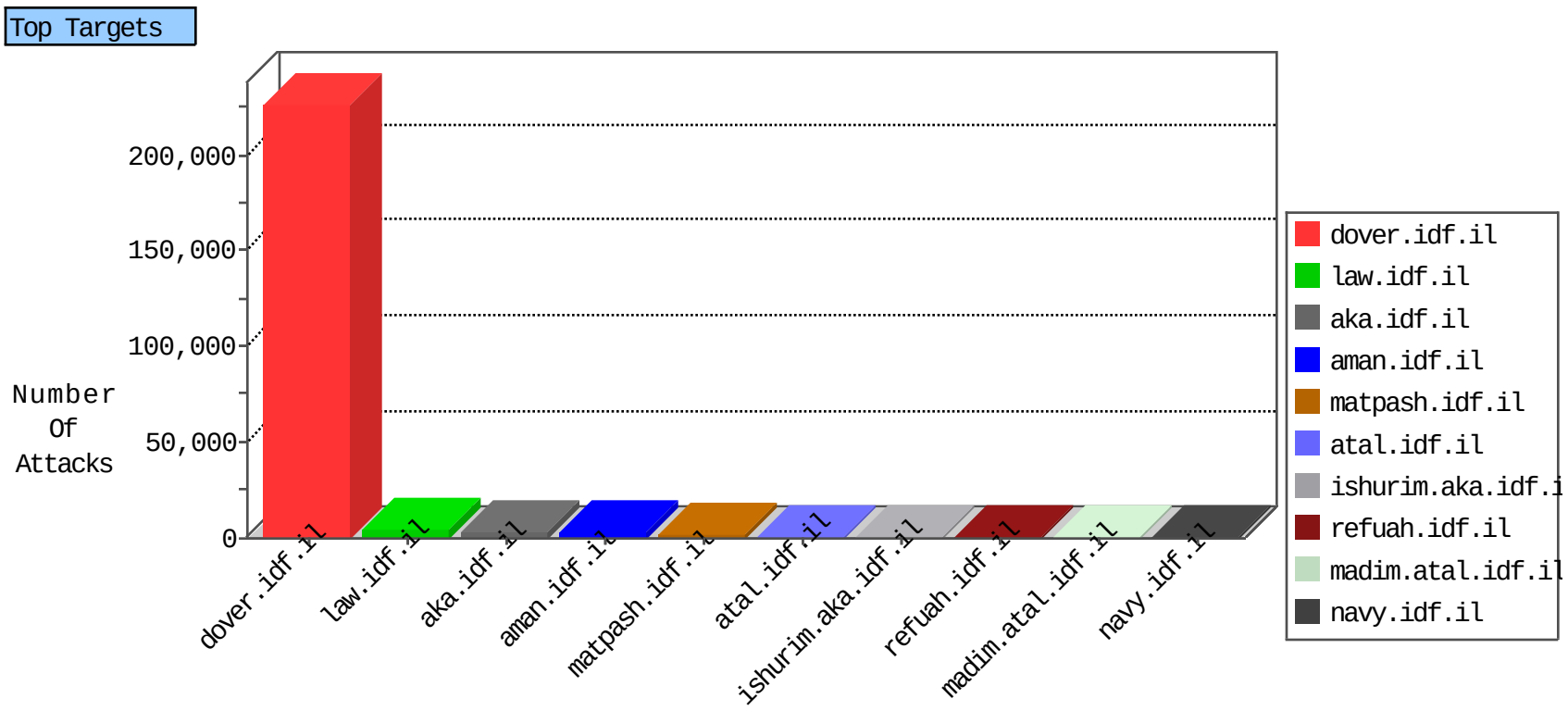
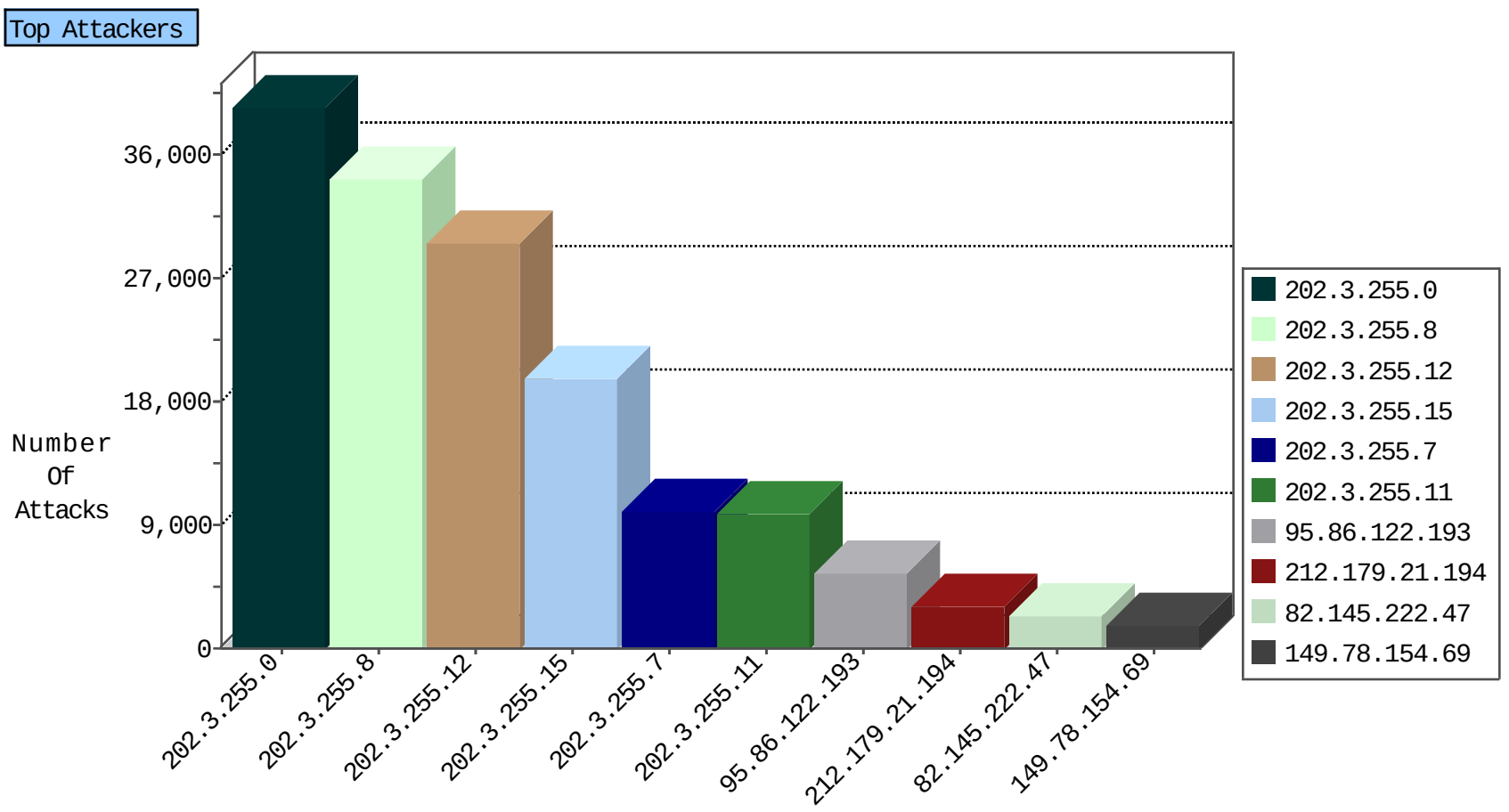
07-29-2015-00:00:06 to 07-30-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-29-2015-00:00:06 to 07-30-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
64.235.216.150	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	51149
41.232.33.53	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32376
66.249.93.164	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	19879
85.114.104.164	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14146
180.153.214.191	China	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	12141
176.223.85.154	Germany	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11762
188.165.15.94	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9992
66.249.67.67	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8096
50.251.213.11	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7057
80.94.146.53	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5984
144.76.26.177	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5517
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4122
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3657
129.64.11.39	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3643
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3077
79.180.186.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2764
87.69.2.131	Israel	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	2133
66.249.65.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1664
66.249.93.242	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1586
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	838
149.78.80.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	821
79.179.33.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	816
149.78.186.175	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	790
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	509
77.125.145.147	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	449
79.180.108.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
109.67.206.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	395
79.176.126.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	374
79.179.71.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	352
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	314
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
79.178.101.231	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	301
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	295
79.177.193.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	284
176.228.134.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
77.127.14.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
84.108.192.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	243
149.78.106.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	206
79.178.14.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
79.181.147.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
89.138.76.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
37.142.64.87	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
5.28.133.215	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
37.26.149.234	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
46.120.114.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
5.29.147.49	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
79.181.109.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
109.65.126.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
77.126.25.110	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
204.93.154.210	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174

07-29-2015-00:00:06 to 07-30-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
173.197.96.249	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	17
31.154.157.162	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
94.159.236.149	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.117.16.220	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.95.134.135	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
5.102.254.209	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
109.67.32.211	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.183.57.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.65.167.135	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.69.2.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
147.236.138.212	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
211.59.8.170	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
5.29.28.254	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.160.182.27	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.91	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
211.59.8.170	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
79.176.26.28	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
199.203.94.202	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
211.59.8.170	Korea, Republic of	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
50.48.42.219	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.155.228	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.117	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.181.249	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.248	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.125.214.76	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.222.238	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
62.219.164.245	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.199.9.194	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.90.165.71	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.61	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.217.7.128	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.143.48.42	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.177.198.193	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.52.175.182	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
73.133.126.26	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.142	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.117.220.107	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.228.144.189	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.210.251.69	France	147.237.72.166	aka.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	2
85.250.24.191	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.143.187.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.178.58.43	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.170	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.210.251.69	France	147.237.72.166	aka.idf.il	17031: HTTP: GetSimple CMS File Upload	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
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.17	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.178.180.166	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.116.237.174	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.166.22.141	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-29-2015-00:00:06 to 07-30-2015-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	35883
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	31149
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	26788
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	17894
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	9077
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	8954
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	99
172.56.19.237	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	88
5.196.82.41	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
79.183.132.7	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
45.114.11.44		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.44		147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	4
87.69.2.131	Israel	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	4
105.109.148.221	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	4
218.65.30.107	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.44		147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	4
218.65.30.107	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	3
82.166.22.217	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
45.114.11.44		147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	3
204.93.154.201	United States	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
218.65.30.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.76.176	test.ncore.idf.i	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
41.140.10.212	Morocco	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	3
61.183.128.6	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
62.74.9.60	Greece	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
191.240.116.92	Brazil	147.237.72.14	dover.idf.il(old	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.8.24	e.lifestyle.idf.	ET SCAN Potential SSH Scan	2
95.179.14.136	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.87	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.46		147.237.72.14	dover.idf.il(old	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.25	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
89.248.168.128	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
45.114.11.44		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
74.86.147.196	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
218.65.30.107	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.132	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
191.240.116.92	Brazil	147.237.0.19	madim.atal.idf.i	ET SCAN Potential SSH Scan	2
61.182.170.38	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
197.160.41.168	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
173.208.136.26	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
89.248.168.128	Netherlands	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2

07-29-2015-00:00:06 to 07-30-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.122.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5428
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3612
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3078
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2812
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2706
82.145.222.47	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2320
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1807
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1568
199.190.46.68	Satellite Provide	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1250
95.86.66.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1241
192.114.23.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1049
82.145.220.134	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	906
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	905
129.64.11.39	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	905
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	902
82.145.223.2	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	864
93.172.130.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	775
46.19.85.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	764
105.109.148.221	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	740
82.166.22.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	735
188.165.15.94	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	675
37.142.103.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	656
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	653
66.249.65.92	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	644
66.249.65.89	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	612
66.249.65.95	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	599
213.57.180.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	597
46.135.49.5	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	586
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	570
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	560
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	542
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	540
77.126.2.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	525
149.255.232.5	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	516
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
5.29.208.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	498
2.54.57.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	495
109.186.76.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	452
77.125.100.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	443
109.64.142.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	371
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	347
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
36.48.69.190	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	339
79.181.198.221	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	329
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
95.86.68.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	322
46.19.85.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
197.160.41.168	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	317
37.26.148.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.178.104.205	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.104.205	Block	409
45.35.20.204		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 45.35.20.204	Block	198
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	87
192.151.159.82	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	83
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	65
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	57
192.187.124.251	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	53
192.151.159.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	51
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.198.164	Block	51
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.98	Block	42
192.187.124.251	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	42
192.187.124.251	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	38
45.35.20.204		147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	36
192.151.159.82	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	34
192.151.159.82	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	33
192.151.159.82	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	33
193.201.224.126	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	32
192.187.124.251	United States	147.237.76.86	navy.idf.il	Distributed Admin Blocking	Block	30
192.151.159.82	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 192.151.159.82	Block	29
79.180.173.136	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.180.173.136	Block	28
84.228.116.220	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	28
192.187.124.251	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	27
46.121.220.209	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	26
188.143.232.13	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	26
192.187.124.251	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	25
192.187.124.251	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	25
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	22
65.208.151.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	22
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	22
188.165.15.94	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.94	Block	20
192.187.124.251	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	20
192.187.124.251	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	19
93.173.39.118	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	18
46.121.60.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
192.151.159.82	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	17
65.208.151.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	16
192.151.159.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	16
46.120.45.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
192.187.124.251	United States	147.237.0.15	kosher-kravi.idf.il	Distributed Admin Blocking	Block	15
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.178.3.17	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	14
65.208.151.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	14
79.178.3.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.181.147.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
192.187.124.251	United States	147.237.77.233	atal.idf.il	Distributed Admin Blocking	Block	14
65.208.151.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	14
79.181.52.207	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	14
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	12
46.120.160.160	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
198.204.245.202	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 198.204.245.202	Block	12