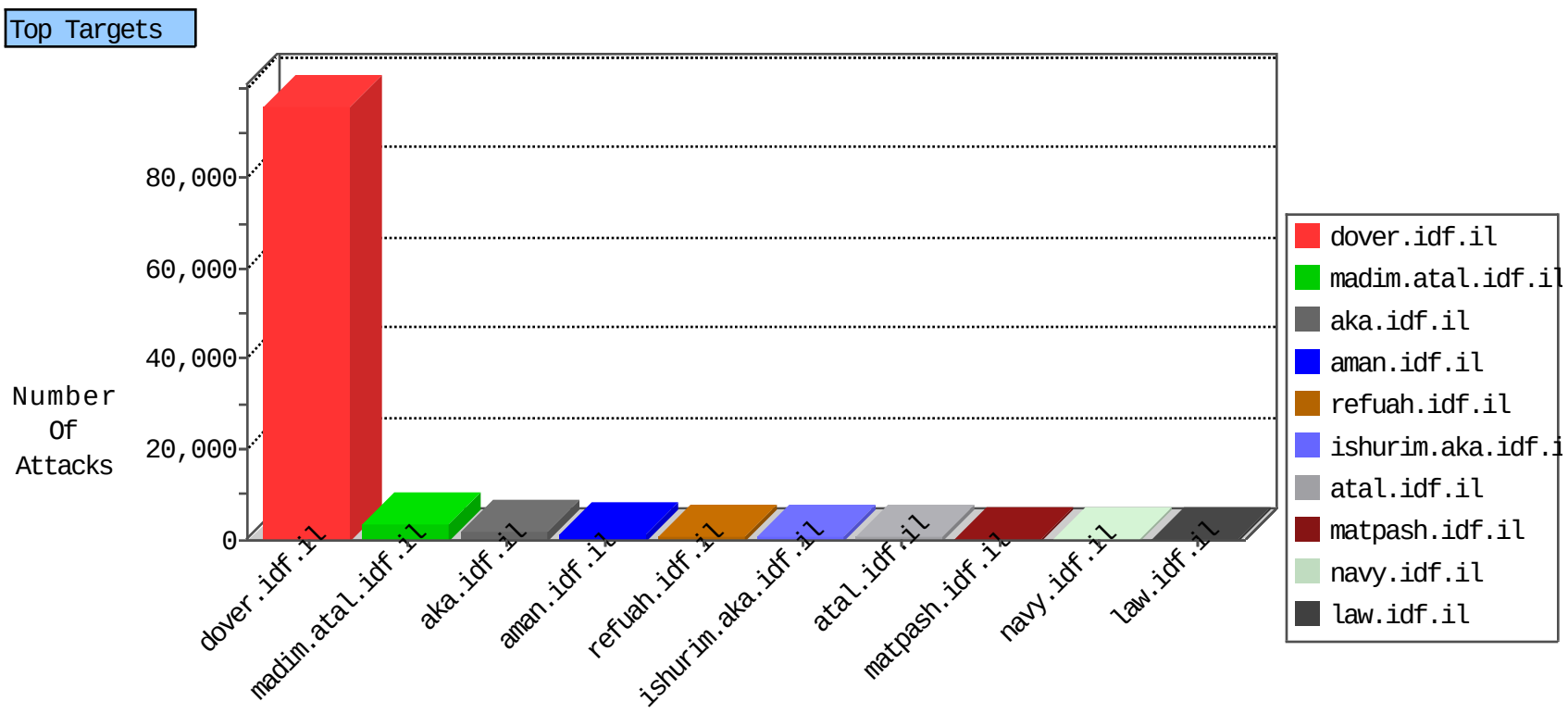
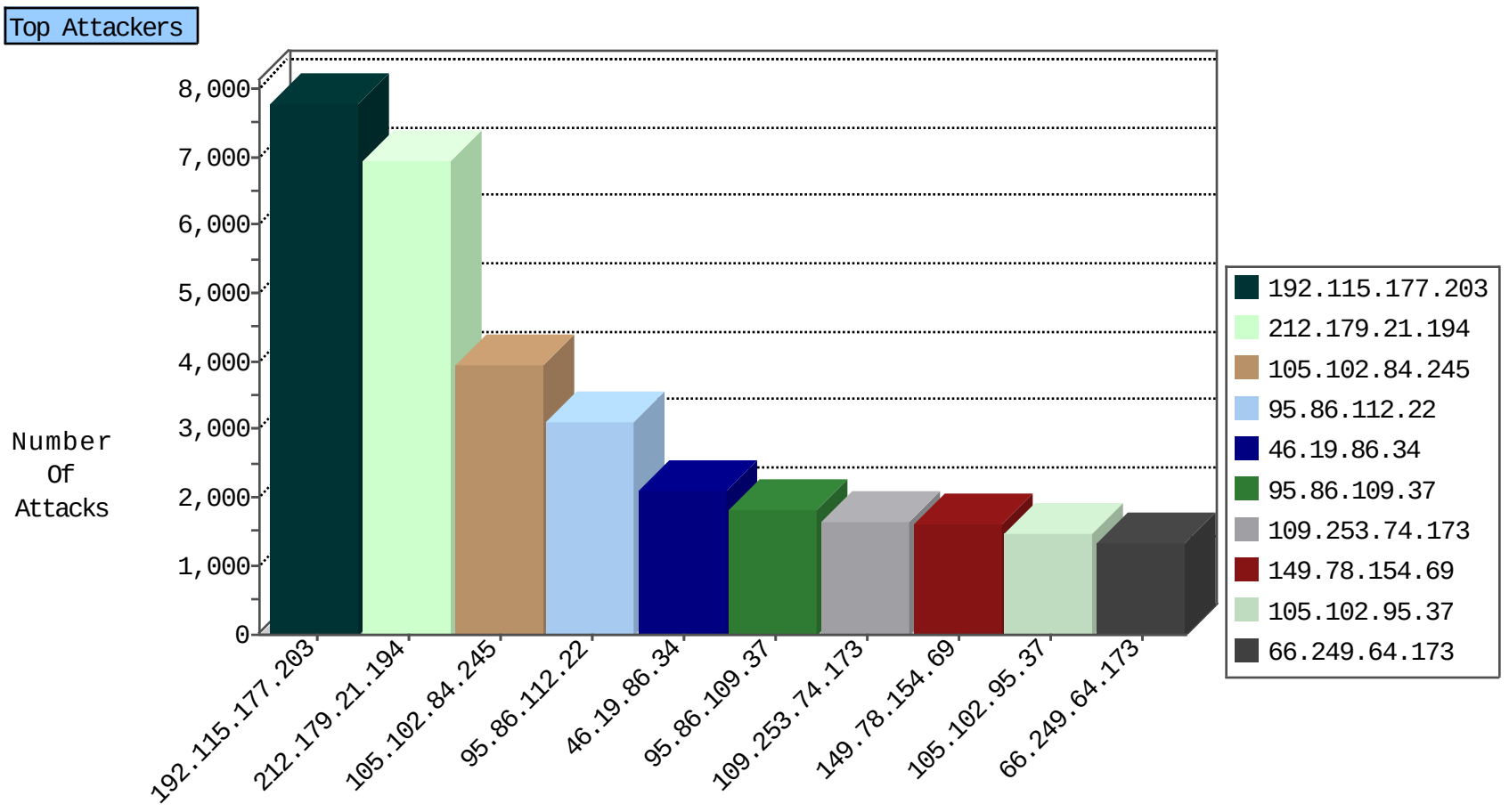
07-13-2015-00:00:09 to 07-14-2015-00:00:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-13-2015-00:00:09 to 07-14-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5367
220.181.108.162	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	4132
220.181.108.152	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2673
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1052
79.180.220.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	689
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	642
95.86.120.117	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	617
217.132.208.29	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	573
109.67.60.18	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	488
46.116.242.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	484
176.228.136.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	353
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	331
77.127.152.209	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	326
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	315
85.65.47.217	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	228
46.121.234.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
46.116.120.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
79.179.142.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
77.125.242.226	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	178
46.121.244.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
5.29.88.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
213.57.105.109	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	170
149.78.230.130	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
66.249.64.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	166
79.183.6.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
79.177.20.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
109.65.121.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
84.228.198.18	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
31.154.161.166	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
93.173.35.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
84.94.179.152	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
77.125.133.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
2.54.49.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	93
77.125.132.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
89.139.50.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
77.126.10.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
85.65.60.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	84
109.64.210.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.86.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	73
149.78.48.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72
79.182.51.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
85.250.102.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
185.32.178.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	63
84.109.101.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	37
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
5.22.129.149	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
46.19.86.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23

07-13-2015-00:00:09 to 07-14-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.218.97.114	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
46.116.242.154	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	25
77.127.152.209	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	18
82.166.22.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
79.183.6.21	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
93.173.24.236	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
46.116.149.99	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
213.139.53.40	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
109.186.185.174	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
87.69.20.153	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
132.72.134.183	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.178.107.32	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
81.218.97.45	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.180.186.20	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.67.183.244	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
104.237.157.164		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
62.90.72.41	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.64.97.182	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.177.20.81	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.186.104.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
82.102.141.254	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
112.111.189.65	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
109.186.7.187	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
193.108.195.249	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.64.249.42	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.178.216.140	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.73.250.17	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	4
46.19.85.120	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
222.84.0.31	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
190.186.103.110	Bolivia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.151.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.135	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.95.210.26	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
63.253.67.243	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.61.162	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.108.28	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.205	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.176.56.236	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.164.216	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.147.178	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.177.192	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.2.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.51	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.63.54	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.117.136.66	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.230.85.111	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-13-2015-00:00:09 to 07-14-2015-00:00:09

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	118
2.52.139.149	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	25
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
66.249.64.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
79.178.119.30	Israel	147.237.76.42	refuah.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
198.204.231.106	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
61.182.170.38	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	3
61.183.128.6	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
61.182.170.38	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
93.189.25.174	Austria	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
62.210.109.86	France	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
93.189.25.174	Austria	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.182.170.38	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.18	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.178	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
188.138.9.51	Germany	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
37.115.187.54	Ukraine	147.237.77.74	law.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	2
218.65.30.107	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.7	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
121.66.231.122	Korea, Republic of	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
5.189.137.95	Russian Federation	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.156.127	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.203.3.117	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
82.132.232.194	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	Taiwan	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
180.148.209.106	Bangladesh	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
45.63.107.220		147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
108.193.206.163	United States	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.121.242.208	France	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.65.30.107	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
74.118.90.37	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.17.72	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
58.211.5.189	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
199.101.186.236	United States	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1

07-13-2015-00:00:09 to 07-14-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
192.115.177.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7804
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6689
105.102.84.245	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3217
95.86.112.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3120
46.19.86.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2097
95.86.109.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1826
109.253.74.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1667
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1600
105.102.95.37	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1351
74.105.225.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1330
37.26.147.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1127
89.105.194.90	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1027
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	880
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	819
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	804
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	798
105.102.84.245	Algeria	147.237.77.216	dover.idf.i		drop	drop	613
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	605
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	585
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	571
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	564
77.125.165.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	548
46.121.202.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	486
5.102.254.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	440
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	429
46.121.198.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	417
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	372
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	370
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	360
8.37.225.2	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	356
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	353
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	352
196.213.190.113	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	345
2.54.27.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	344
192.114.105.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	336
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	321
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	281
2.52.142.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	278
37.60.45.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
46.120.28.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	249
66.249.64.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	244
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	243
5.102.254.200	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	234
66.249.83.161	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	231
66.249.64.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
141.0.15.25	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	221
66.249.83.155	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	218
91.199.69.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	216

07-13-2015-00:00:09 to 07-14-2015-00:00:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.40.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.40.230	Block	460
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.122	Block	456
176.13.13.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	360
109.64.123.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	230
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	226
109.253.140.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	222
77.125.105.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	206
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
46.19.86.200	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.200	Block	173
2.54.49.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	141
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	139
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	127
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
46.19.85.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
176.13.16.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
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
37.26.147.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.84	Block	35
2.54.43.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
149.78.50.244	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	23
31.186.228.30	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	18
31.168.114.146	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il//templates/homepage/homepage.aspx	Block	17
31.186.228.60	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
77.125.115.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	14
31.186.228.59	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
31.186.228.96	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
109.64.48.126	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
5.29.38.144	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	13
31.186.228.29	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
2.54.160.115	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.160.115	Block	11
84.94.26.175	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
2.54.40.230	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtHomePhone in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	10
31.186.228.32	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
2.54.38.1	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	10
31.186.228.58	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
46.120.158.163	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
176.13.19.217	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
176.13.19.217	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	Block	8
176.12.140.183	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
37.26.146.202	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
2.54.8.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
92.111.188.176	Netherlands	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	7
176.12.140.72	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
149.78.207.186	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
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	6
31.186.228.31	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6

07-13-2015-00:00:09 to 07-14-2015-00:00:09