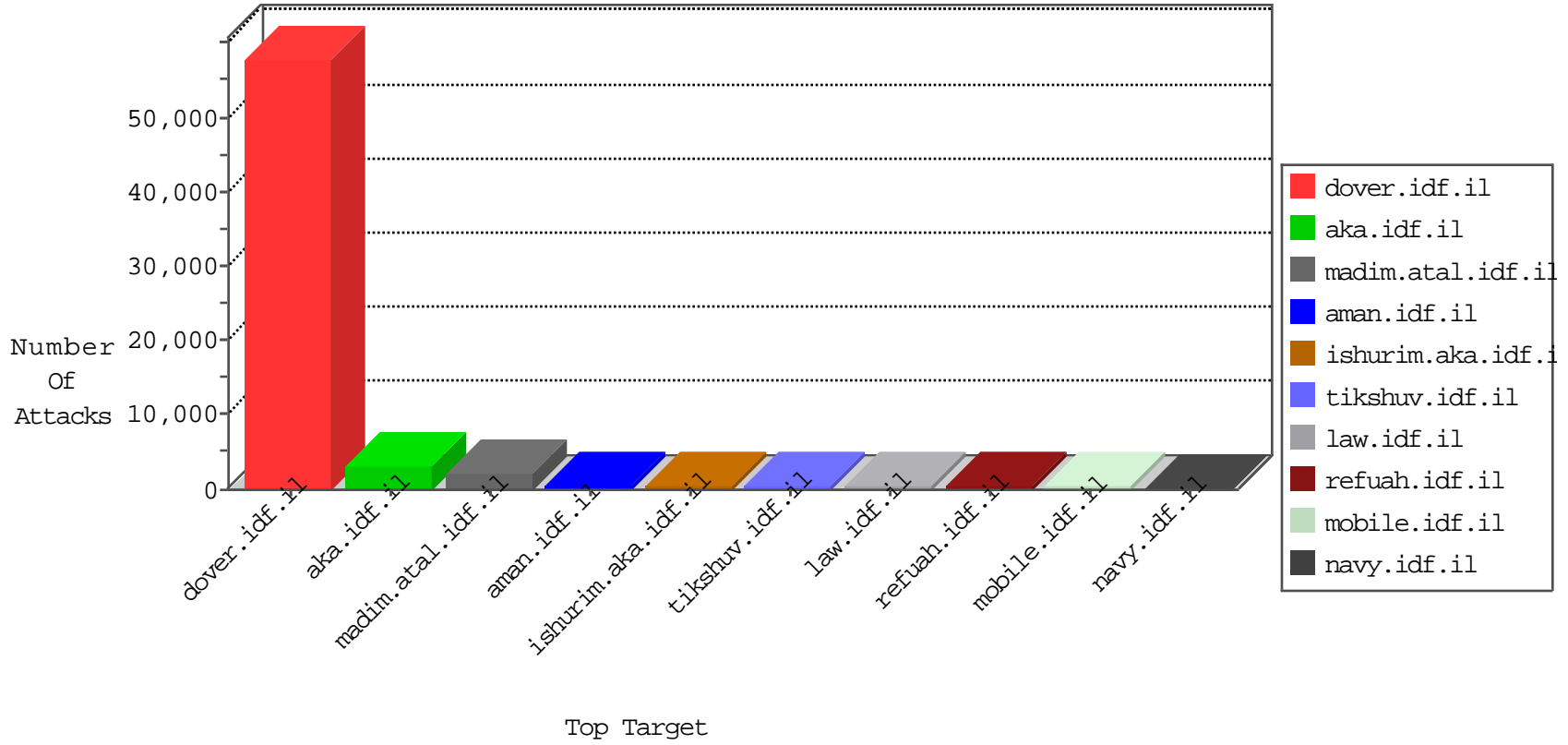


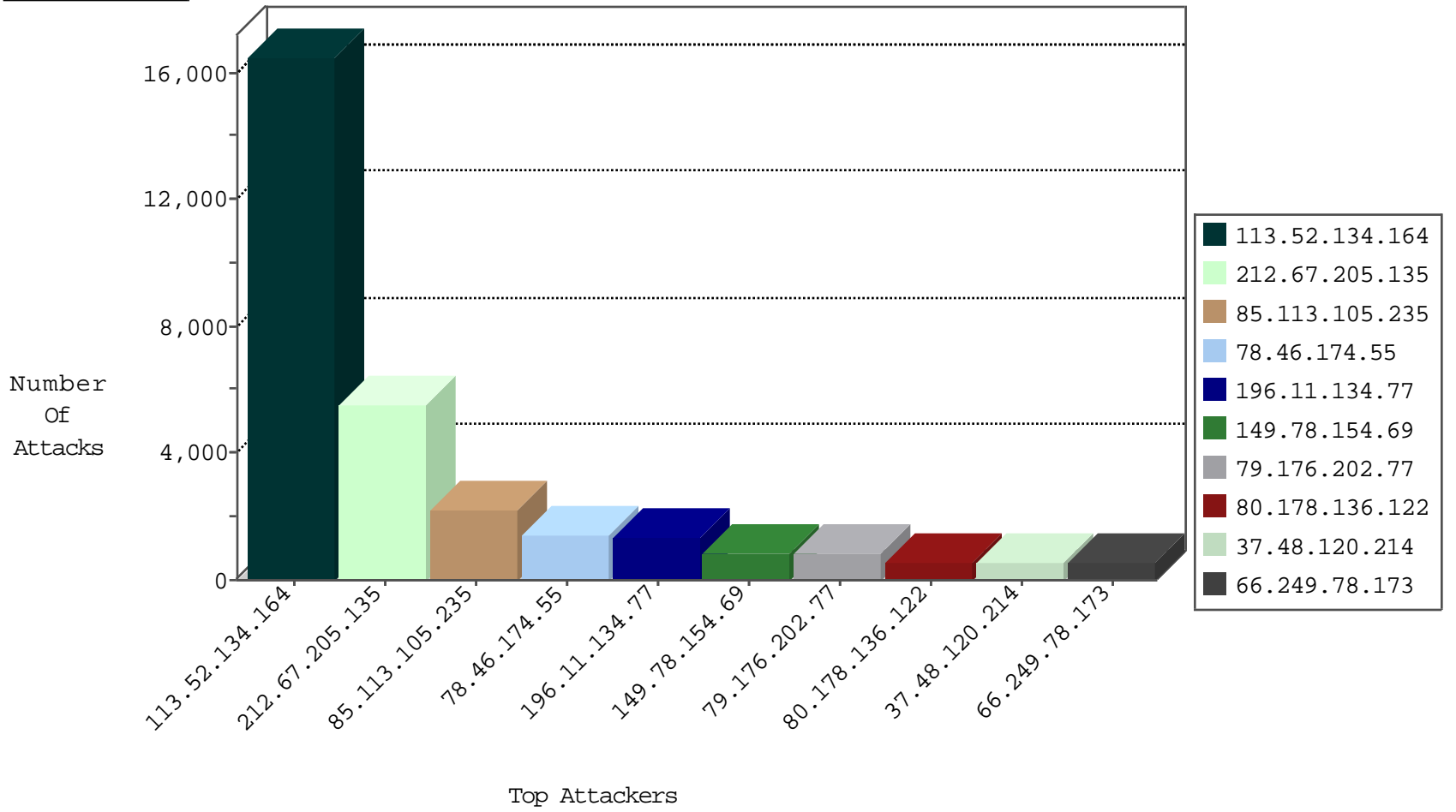
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	149870
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	71472
220.181.108.102	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	47021
195.191.148.7	Bulgaria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36227
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	31486
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30004
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	21540
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20002
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	17746
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16524
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	16124
220.181.108.119	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	14507
66.249.78.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13780
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	13682
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	11794
220.181.108.185	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	11007
84.158.4.118	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9884
66.249.78.242	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9049
220.181.108.88	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	8561
66.249.78.211	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	8096
220.181.108.176	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	7939
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7641
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6907
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	6873
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6646
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6161
66.249.78.47	Israel	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	6016
66.249.78.254	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5117
66.249.65.65	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4835
95.91.227.135	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4643
173.76.13.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4399
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3252
220.181.108.170	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3163
66.249.83.188	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2540
66.249.64.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2247
77.126.61.14	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2216
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1912
66.249.67.139	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1660
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1383
79.179.167.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1229
220.181.108.117	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	998
195.191.148.7	Bulgaria	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	995
220.181.108.187	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	733
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.il	block-sp-trafl	drop	604
5.29.18.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	586
85.64.125.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	481
84.110.85.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	456
77.127.14.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	420
95.86.68.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	398
79.183.233.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	133
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	127
185.33.168.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	EgovRep_B-N_70-99	Block	110
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	97
195.191.148.7	Bulgaria	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	55
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	43
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	31
203.151.234.15	Thailand	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	30
125.79.138.185	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	30
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
66.249.79.253	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.116.150.130	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
66.249.79.229	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
2.54.9.206	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
79.182.102.134	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
66.249.79.241	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
79.177.8.165	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
125.227.255.30	Taiwan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
84.228.14.148	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
37.26.146.155	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
109.186.35.100	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	8
46.121.82.80	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
37.142.176.49	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
85.250.202.224	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
121.146.93.228	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
84.228.228.146	Bulgaria	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	7
86.12.190.4	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	7
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
109.65.28.142	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
84.228.117.24	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
79.176.113.145	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	5
212.35.64.194	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
105.51.127.117	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN Vega Web Application Scan	1104
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	133
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL Injection - Select From	99
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	98
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	87
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	86
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	86
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	86
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	6
85.113.105.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	6
212.86.219.134	Germany	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
91.148.192.64	Netherlands	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	4
176.12.138.2	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.79.55	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
221.235.189.245	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
183.136.216.3	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
221.235.189.245	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	3
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
62.221.99.118	Moldova, Republic of	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.78.254	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
79.143.87.178	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
221.235.189.245	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
144.0.0.60	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
121.88.5.177	Korea, Republic of	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.217	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
221.235.189.245	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.3	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
59.46.193.114	China	147.237.76.199	e.nakchal.idf.il	GPL SCAN nmap TCP	2
66.249.67.159	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
128.199.167.194	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
66.249.79.241	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.52.134.164	Hong Kong	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9381
196.11.134.77	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1334
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	852
79.176.202.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	829
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	548
80.178.136.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	518
95.86.116.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	442
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	438
66.249.83.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	395
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	372
5.28.136.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	353
66.249.83.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
66.249.83.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	331
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	326
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	296
84.158.4.118	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	261
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	255
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	247
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	236
109.253.141.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
109.67.117.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	210
91.8.72.80	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	205
149.78.213.207	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	197
203.116.187.1	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	196
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	179
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	176
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	168
109.65.1.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	163
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	149
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	148
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	141
213.247.64.14	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	140
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
5.29.67.155	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	137
66.249.81.242	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	134
66.102.8.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	130
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
66.102.8.178	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
38.99.190.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
66.249.81.245	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
66.249.78.234	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	118
79.183.124.219	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111
83.221.154.225	Denmark	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
66.249.64.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	107
66.249.64.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	106
79.180.148.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
84.228.244.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
89.186.174.69	Denmark	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	102

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	530
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	401
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	401
109.253.147.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.147.130	Block	353
176.12.138.2	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.138.2	Block	334
2.54.31.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	242
84.111.158.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	232
37.26.147.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
84.108.49.9	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.108.49.9	Block	188
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.180	Block	151
2.54.175.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.175.46	Block	128
176.12.150.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
109.253.134.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
70.148.148.66	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	51
109.253.140.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
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
79.182.182.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	22
66.249.78.228	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.228	Block	20
66.249.78.240	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.240	Block	19
66.249.78.173	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	18
109.66.36.61	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	16
66.249.78.166	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	16
95.86.110.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
66.249.78.159	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
157.55.39.65	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.65	Block	13
206.221.181.195	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 206.221.181.195	Block	13
207.46.13.127	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
66.249.78.234	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	11
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	11
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
157.55.39.215	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
87.68.85.188	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatenakatqantity.aspx	Block	9
189.102.143.70	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
5.102.254.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
84.111.84.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
79.180.135.143	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.135.143	Block	7
157.55.39.86	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.86	Block	7
109.253.112.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	6
207.46.13.42	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.42	Block	6
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/templates/getfile/	Block	6
157.55.39.43	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.43	Block	6
5.29.230.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	6
71.135.107.39	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.176.230.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
66.249.73.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.73.209	Block	5
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	5