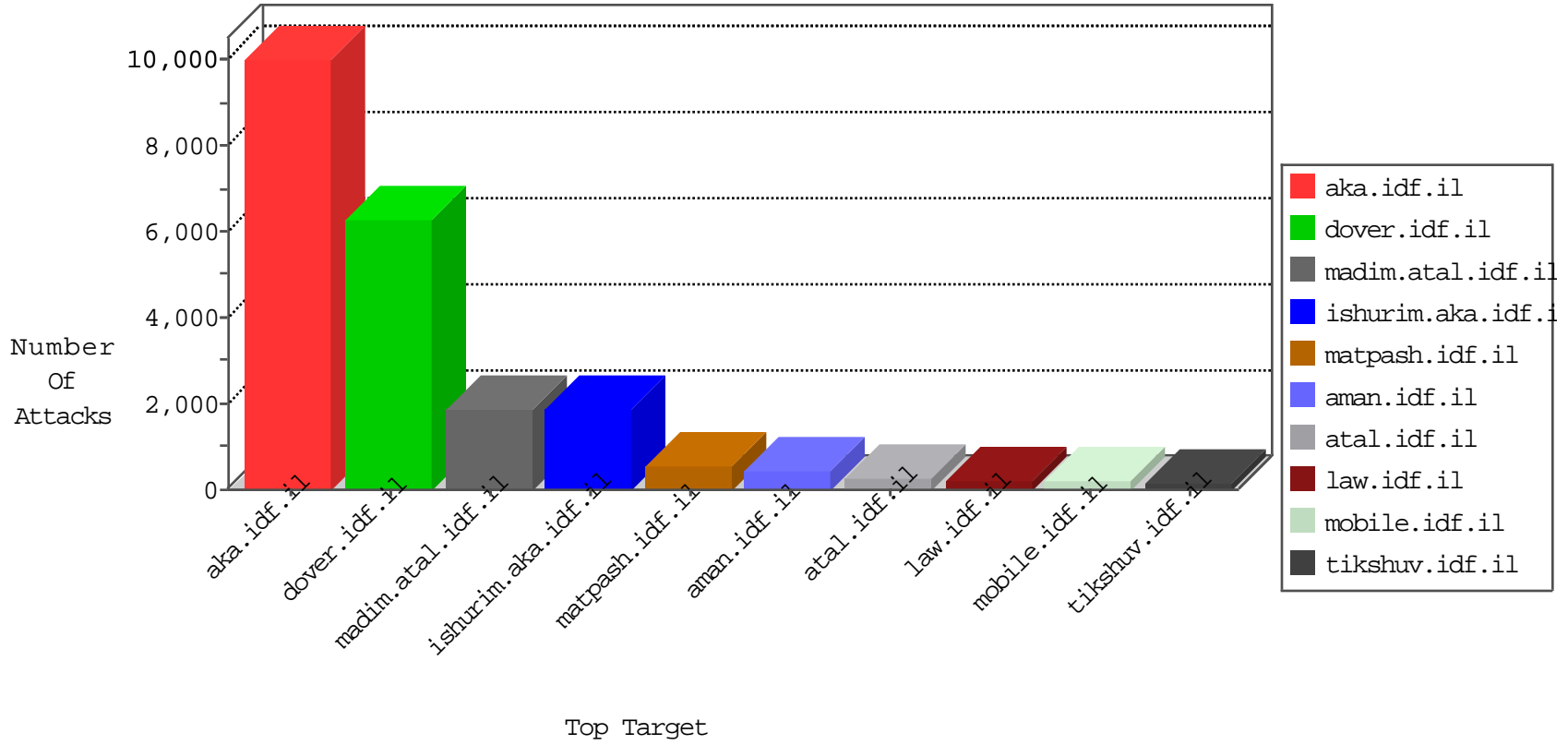


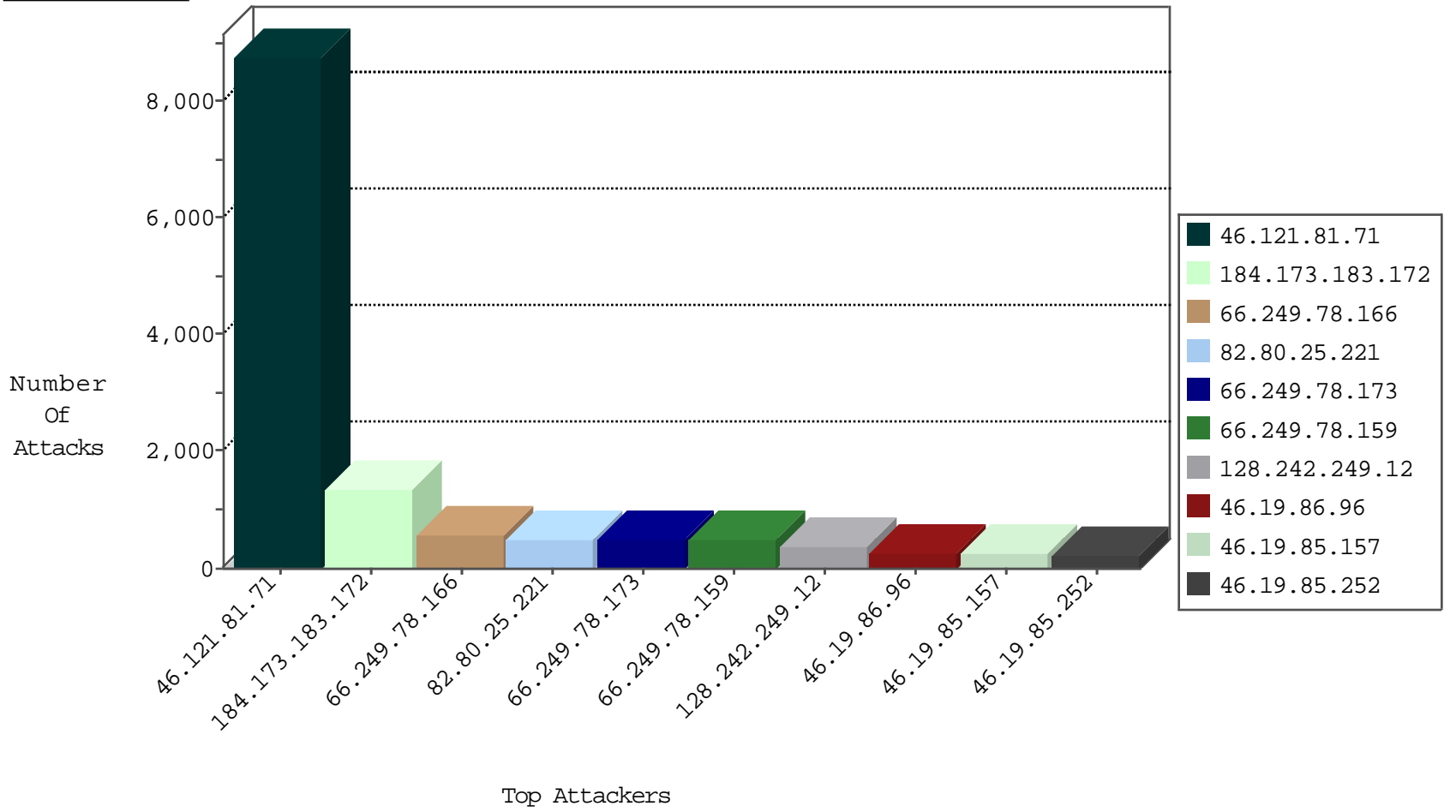
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	767
77.126.6.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	516
87.69.247.15	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	507
5.29.36.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	506
84.110.86.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	433
149.78.2.121	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	234
77.127.25.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
46.117.75.152	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	209
79.181.32.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	199
2.54.53.15	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
77.126.6.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	151
77.125.253.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
109.65.170.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
109.186.144.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.121.105.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
109.66.120.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
84.228.49.231	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
46.121.37.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	104
46.121.37.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.120.25.209	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
37.46.47.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	96
213.8.119.48	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.121.134.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
37.26.148.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
84.228.49.231	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	76
2.54.53.15	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	74
79.178.66.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
2.54.173.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
77.127.162.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
176.228.84.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
5.28.163.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
46.19.85.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	68
80.246.140.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
85.130.246.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
77.126.6.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	61
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
37.46.47.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	37
80.246.140.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	28
46.19.86.203	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	16
46.19.85.54	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	16
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
46.19.85.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	11
185.32.176.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	9
46.19.85.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	7
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
46.19.85.0	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	7
46.19.86.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	924
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	377
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	320
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	88
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	42
85.159.206.101	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	22
46.116.255.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	19
208.113.163.102	United States	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	16
174.122.238.122	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	16
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	12
66.41.172.99	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
77.127.242.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.171	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.126	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.108.109.174	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
121.215.2.244	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
24.139.45.132	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
175.44.61.28	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.116.85.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
18.239.0.155	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
92.241.42.139	Jordan	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
79.180.189.252	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
92.241.45.231	Jordan	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.194.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
37.26.147.201	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
208.113.163.102	United States	147.237.77.233	atal.idf.il	C071: HTTP: Access to - install.php	Block	3
85.25.103.119	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
174.122.238.122	United States	147.237.77.216	dover.idf.il	C071: HTTP: Access to - install.php	Block	3
178.217.187.39	Poland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
18.243.0.30	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
79.182.163.70	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	2

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	497
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	140
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
2.52.178.220	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
92.241.45.231	Jordan	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
92.241.42.139	Jordan	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
217.66.228.107	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
92.241.45.231	Jordan	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
92.241.42.139	Jordan	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
122.228.207.193	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
201.246.124.133	Chile	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	3
174.122.238.122	United States	147.237.77.216	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	3
208.113.163.102	United States	147.237.77.233	atal.idf.il	LOCAL_RULES - Request with the string install.php in it	3
201.246.124.133	Chile	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
2.52.145.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.35.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.162.228	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
79.141.170.7	Sweden	147.237.76.42	refuah.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
61.240.144.64	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
85.65.99.208	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
89.248.162.228	Netherlands	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
85.64.18.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.79.4	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.176	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
84.108.109.77	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
174.122.238.122	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP backup access	2
61.240.144.67	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.114	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.193	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.147	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
208.113.163.102	United States	147.237.77.233	atal.idf.il	SERVER-WEBAPP backup access	2
46.116.254.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.61.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.119.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.69.10	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
176.53.126.2	Turkey	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
89.138.235.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.247.122.15	Spain	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.181.118.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.52.170.215	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.53.126.2	Turkey	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
79.176.153.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
31.168.216.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.141.170.7	Sweden	147.237.77.176	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
85.65.177.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.121.81.71	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2566
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	388
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	336
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	328
176.67.106.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	132
37.8.69.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
104.131.40.8		147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	74
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
31.168.197.130	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	51
109.67.151.91	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	51
213.55.108.119	Ethiopia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
77.127.101.183	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
109.253.130.28	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.159.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.79.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.146.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
46.19.86.115	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
94.159.157.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
176.12.146.210	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.144.136	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.176	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	30
41.109.178.2	Algeria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.142.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.141.127	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.81.180	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	28
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
68.189.74.183	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.141.255	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.79.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
5.22.130.133	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
109.64.10.216	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	21
79.180.17.139	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
213.55.107.137	Ethiopia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
207.46.13.70	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
79.182.166.111	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
79.181.154.40	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
109.64.148.169	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
212.199.10.115	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.140.227	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.81.184	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	18
109.253.134.63	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.129.61	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
58.172.33.45	Australia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.186.10.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.149.140	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.157.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.81.71	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 46.121.81.71	Block	3447
46.121.81.71	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	2753
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.96	Block	246
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.157	Block	239
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	229
79.178.208.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	227
77.126.62.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	167
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.183	Block	149
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	116
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	116
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
149.88.108.175	United States	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73
66.249.78.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	72
2.54.61.130	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.61.130	Block	67
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	67
176.12.137.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	43
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	38
176.12.142.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	30
176.12.144.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
208.113.163.102	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	25
174.122.238.122	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	25
46.116.212.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	23
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	21
94.12.243.191	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 94.12.243.191	Block	16
77.125.243.151	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	15
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	15
149.88.124.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.88.124.89	Block	13
176.12.136.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
208.113.163.102	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 208.113.163.102	Block	13
174.122.238.122	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 174.122.238.122	Block	13
95.86.76.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
176.12.144.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
66.249.64.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	10
176.12.141.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
176.12.151.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
66.249.64.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	8
91.178.38.71	Belgium	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
79.177.152.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
176.12.141.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
176.12.137.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
176.12.143.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
66.249.75.13	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
91.178.38.71	Belgium	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 91.178.38.71	Block	6
17.142.152.63	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.63	Block	6
17.142.149.167	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.149.167	Block	6
85.65.74.247	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.65.74.247	Block	6
176.12.138.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6