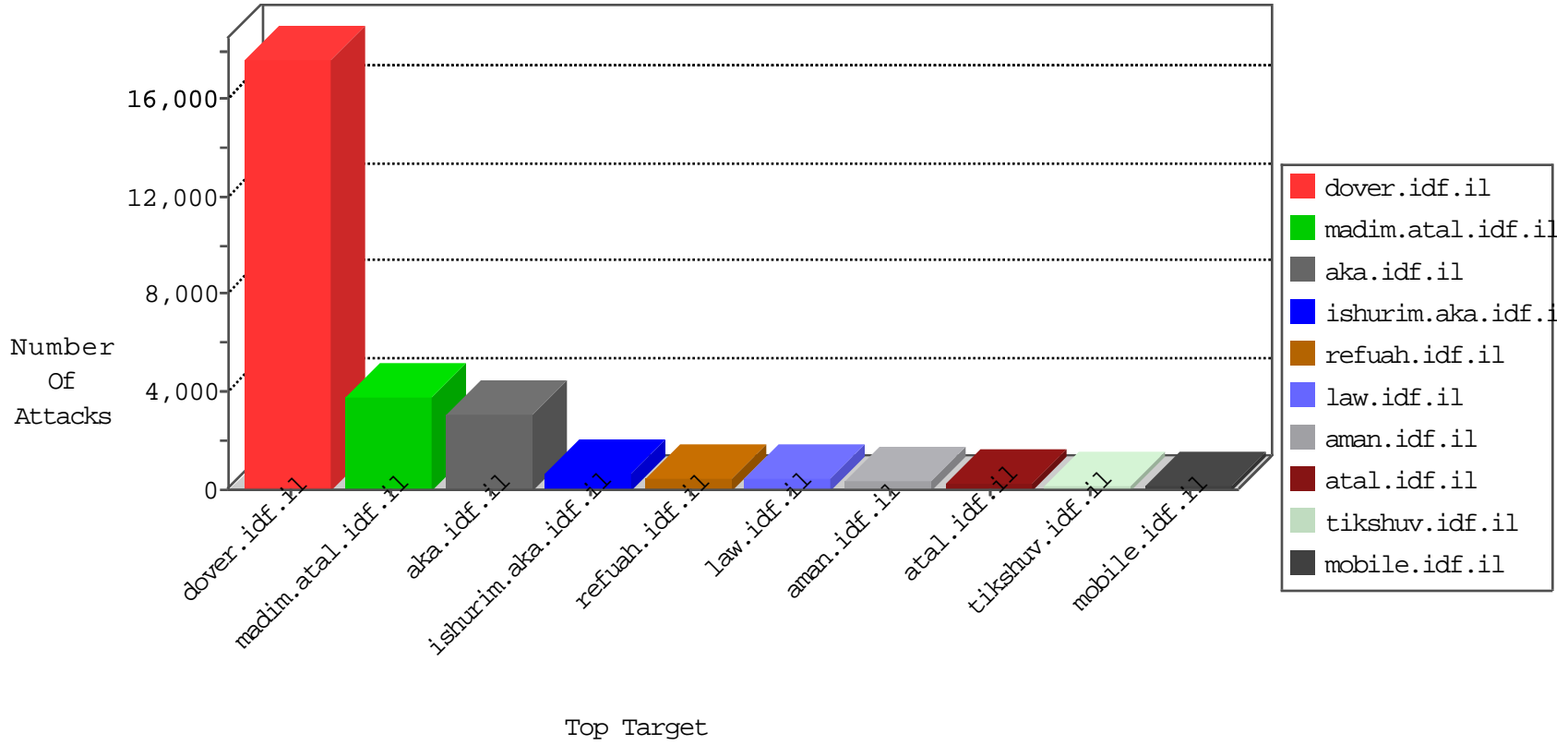


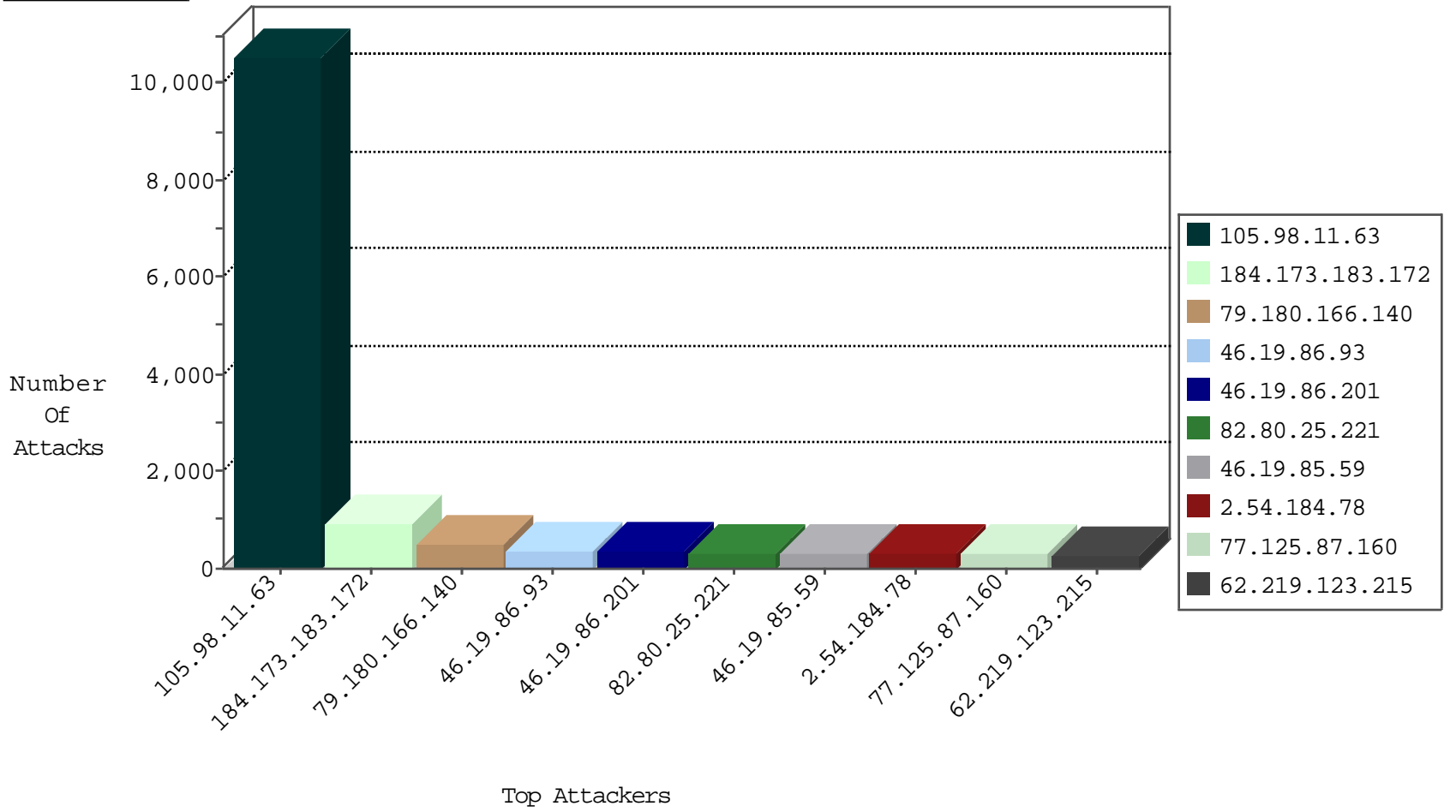
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.81.239	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	52039
54.148.136.55	United States	147.237.76.31	nakchal.idf.il	TCP handshake violation, first packet not syn	drop	11798
194.54.168.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1626
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	715
95.86.92.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	589
46.116.65.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	533
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	474
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	428
79.177.97.7	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	363
46.116.247.155	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	353
85.130.250.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	270
37.142.230.35	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	227
79.183.170.154	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	225
84.109.88.145	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	223
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
85.65.221.229	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
212.235.79.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
2.54.41.155	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
77.126.7.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
85.64.103.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
31.210.186.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
93.172.29.0	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
87.69.230.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
77.125.145.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
109.66.41.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
87.69.128.62	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
85.64.9.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
79.176.158.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
2.54.166.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
2.52.162.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
84.228.116.204	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
194.54.168.76	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
46.117.45.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
109.65.1.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
82.80.143.187	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
80.246.140.169	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
194.54.168.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
114.79.52.217	Indonesia	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
82.102.141.253	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	8
82.102.141.249	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	6
82.102.141.255	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
27.132.101.200	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	5
82.102.141.255	Israel	147.237.77.243	mobile.idf.il	Invalid TCP Flags	drop	4
189.177.109.30	Mexico	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
95.172.79.156	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3

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	919
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	285
62.219.123.215	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	275
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	138
65.49.70.90	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
79.176.111.102	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	23
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	21
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
82.166.190.11	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.116.238.242	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
46.19.85.214	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.116.162.176	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
89.139.42.245	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.166.190.10	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
85.65.144.251	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
146.148.56.75		147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
24.185.133.1	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.78.215.133	United States	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
194.90.169.2	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.251	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
212.235.18.186	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.158.139.101	United Kingdom	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
89.139.170.174	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
62.90.192.168	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
85.158.139.227	United Kingdom	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
212.199.10.114	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.0.17	m.ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3

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	280
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	111
54.186.204.9	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	23
80.246.141.35	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
46.19.86.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
91.227.71.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.64.118	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	3
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.76	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	3
5.28.135.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
2.54.42.206	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
79.180.33.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
54.186.204.9	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
87.69.247.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.123	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.161	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
54.186.204.9	United States	147.237.72.156	aman.idf.il	Tehila - Perl LWP with fake user agent	2
58.20.54.249	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.166	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
128.61.240.66	United States	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.121.106.239	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.110.209.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.132.102	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.7	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
122.228.207.76	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
109.64.194.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.118.11.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.152	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
79.180.14.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.230.93.27	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
54.186.204.9	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
84.108.46.136	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
54.186.204.9	United States	147.237.0.34	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	2
82.117.208.243		147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.166	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	5576
105.98.11.63	Algeria	147.237.77.216	dover.idf.il		drop	drop	4376
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	472
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	122
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	116
79.176.5.144	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	110
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	102
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
62.207.60.229	Netherlands	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	60
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
173.208.169.226	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	44
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	40
189.79.145.140	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.142.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.159.112	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.143.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
194.98.114.103	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.147.117	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.147.119	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
84.228.71.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
176.12.151.221	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.157.244	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.138.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.137.64	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
89.138.93.49	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	23
89.138.93.49	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
17.142.152.68	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
85.250.58.24	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
109.253.156.245	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	21
71.188.76.11	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	21
2.54.134.72	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.149.158	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
82.166.154.241	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	20
109.253.136.122	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
77.125.112.55	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.166.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.166.140	Block	513
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	349
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	339
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.59	Block	292
2.54.184.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.106	Block	228
46.120.147.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
5.22.130.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.150	Block	136
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
109.253.131.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
176.228.6.9	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.228.6.9	Block	85
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.211	Block	77
109.253.140.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
109.253.138.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
109.253.139.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.104	Block	64
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.217	Block	63
109.253.138.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.138.214	Block	59
109.253.157.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.11.63	Block	58
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
80.179.118.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	44
176.228.6.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
173.208.169.226	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 173.208.169.226	Block	43
109.253.145.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
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	41
109.253.144.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
109.253.142.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
109.253.146.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
80.246.136.192	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 010270D71C11AC3AD208FE704F5EDCAE3AD208000933003100380034003200310032003800360000012F00FF, Observed 010242C7250FAC3AD208FE423F67DAAE3AD208000933003100380034003200310032003800360000012F00FF	None	25
109.253.143.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
79.178.51.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	20
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	18
109.253.138.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
109.253.157.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
109.253.156.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
80.230.96.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	15
84.111.192.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
66.249.75.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	14
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	13
176.12.143.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
37.239.68.139	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gar/	Block	12
149.88.91.102	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
37.26.147.150	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
37.142.79.51	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	10
192.117.155.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
109.253.156.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9