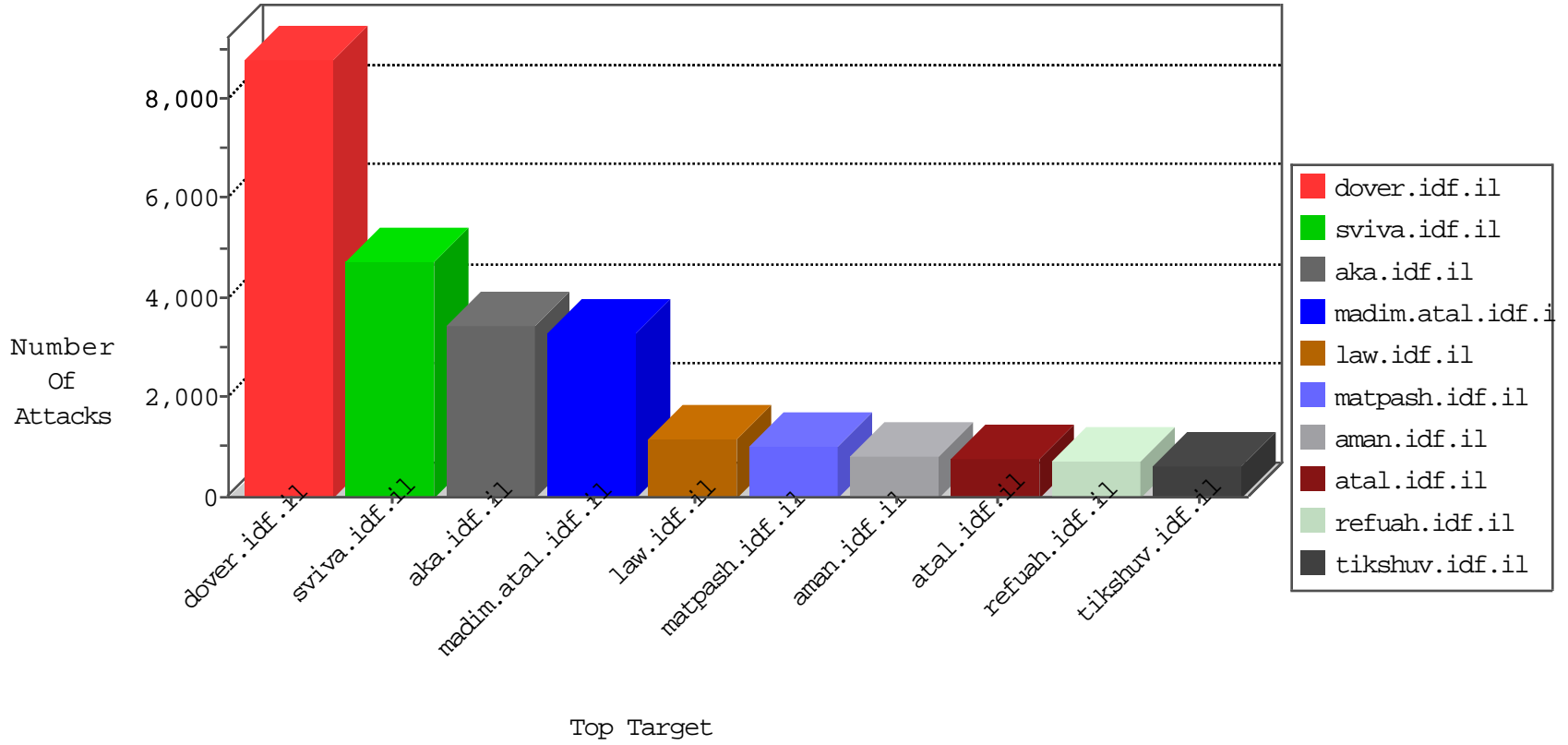


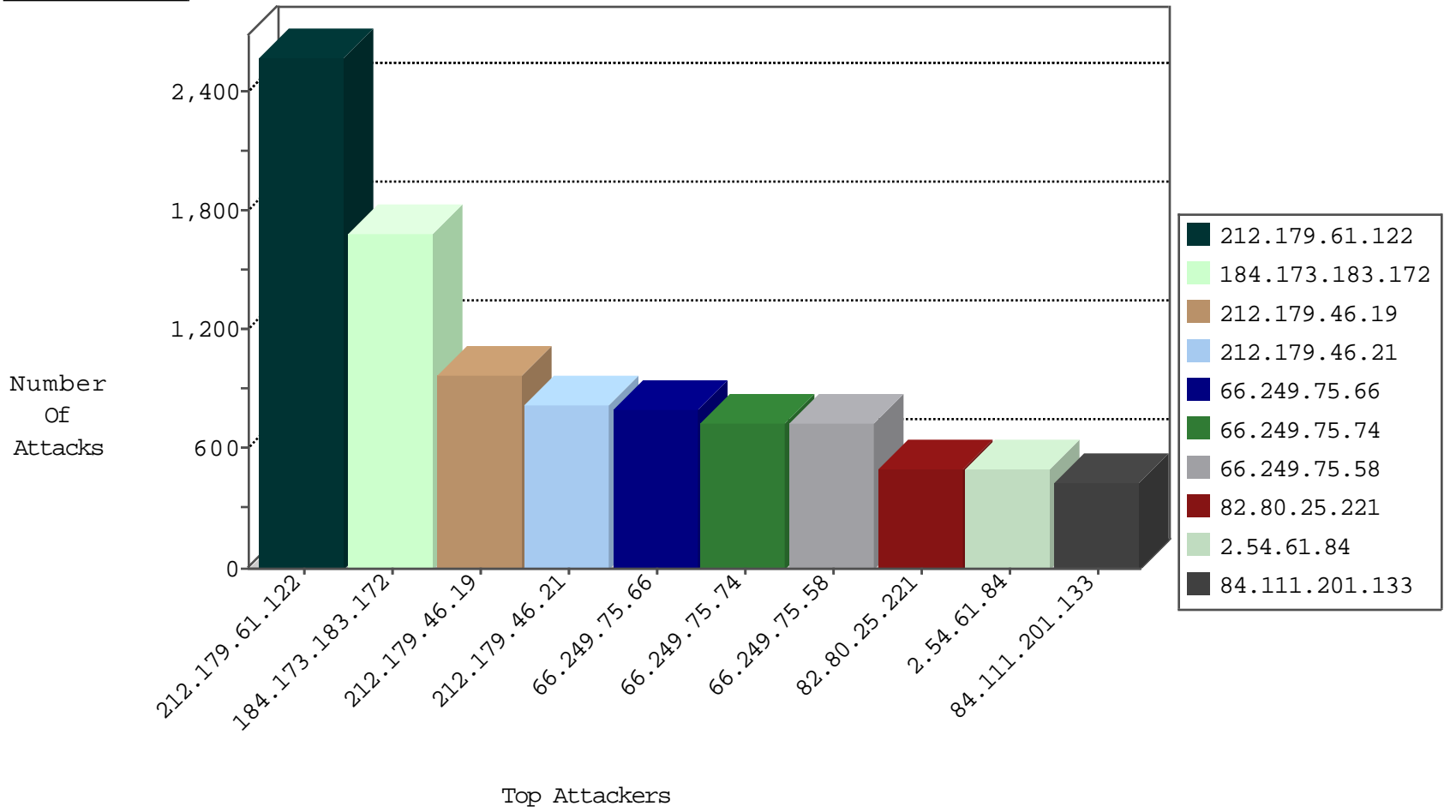
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	728
46.116.65.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	605
66.249.75.66	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	542
87.69.168.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	489
66.249.75.74	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	467
66.249.75.58	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	467
84.228.52.33	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	466
89.138.14.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	442
5.28.181.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	414
46.116.65.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	353
84.110.86.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	344
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	338
84.108.168.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	320
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	306
77.127.170.110	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	277
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	267
132.66.63.35	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	261
109.66.37.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
31.168.214.233	Israel	147.237.0.34	tikshuv.idf.il	HTTP-POST-Segmented-DoS	dest-reset	243
84.109.213.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	220
194.54.168.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	212
79.179.170.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	189
149.78.198.83	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	171
84.110.210.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
83.130.102.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
192.115.116.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	162
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	162
149.78.219.199	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
66.249.79.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	155
66.249.75.117	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	154
79.177.170.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	154
66.249.75.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	152
66.249.79.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	149
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	144
66.249.79.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	143
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	142
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	139
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	137
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	126
66.249.75.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	124
149.88.99.108	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	108
79.180.194.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
5.102.196.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	94
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	93

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	556
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	352
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	351
2.52.11.2	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	330
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	197
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	186
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	165
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	139
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	135
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	128
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	EgovRep_B-N	Block	100
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
62.0.101.97	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
212.29.202.206	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
130.211.249.104		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
130.211.249.104		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	9
87.69.152.39	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
66.91.181.154	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.52.25.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.10.112	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
192.99.82.245	Canada	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
149.88.99.108	United States	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	3
149.78.14.78	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
109.64.61.115	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

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	127
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	31
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
192.99.82.245	Canada	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	4
183.136.216.7	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.7	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
149.78.99.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.170	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
84.111.48.244	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.213	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.170	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.162	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.14	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
212.179.61.127	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
46.19.86.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.228	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
169.54.237.52	Switzerland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
89.138.76.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.120.128.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.8.162	Israel	147.237.76.31	nakchal.idf.il	OS-WINDOWS Microsoft Windows WebDAV propfind access	2
122.228.207.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.162	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
197.7.105.23	Tunisia	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	2
79.183.17.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.170	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.213	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
109.160.253.190	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.109.181.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
93.173.133.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.209.178	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
221.235.188.213	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.139	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
93.172.22.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.250.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.213	China	147.237.76.147	chimuch.aka.idf.il	ET SCAN Potential SSH Scan	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
46.19.86.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
130.211.249.104		147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
169.54.237.52	Switzerland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.122	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	2573
212.179.46.19	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	966
212.179.46.21	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	814
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	469
212.179.21.196	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	264
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	244
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	236
93.190.152.161	Europe	147.237.72.166	aka.idf.il	SAM rule	drop	drop	75
222.77.227.34	China	147.237.76.86	navy.idf.il	SAM rule	drop	drop	62
212.179.21.194	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	61
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
109.64.61.115	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	45
66.249.78.37	United States	147.237.77.234	halag.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
109.253.134.104	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
77.126.19.160	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.253.128.128	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
149.88.68.118	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
155.178.180.12	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	34
84.95.49.252	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	34
2.54.130.89	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
2.52.41.75	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	31
193.169.70.108	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	31
2.52.41.75	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	31
176.12.146.1	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
187.61.212.115	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.64	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.151.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
85.64.248.149	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
212.14.243.74	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	26
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
212.179.28.34	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
176.12.138.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
195.62.160.60	Italy	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
2.52.41.75	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	24
176.12.149.165	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.165.38	Netherlands	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
109.253.128.125	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
41.239.41.138	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
41.218.158.126	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
188.139.226.150	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
132.76.50.6	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
103.224.128.1	New Zealand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.159.124	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.61.84	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.61.84	Block	497
84.111.201.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	432
77.126.83.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	330
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.208	Block	319
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
89.139.38.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	207
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.210	Block	149
109.253.143.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	144
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
109.253.131.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
105.98.85.117	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.85.117	Block	96
105.98.85.117	Algeria	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	95
176.12.138.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	71
5.29.28.254	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.28.254	Block	64
109.253.130.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62
109.253.149.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	58
2.54.26.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
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	48
2.54.39.235	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.39.235	Block	45
109.253.142.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
173.208.169.226	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 173.208.169.226	Block	33
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	32
176.12.151.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
79.183.119.38	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	28
176.12.150.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
41.68.77.11	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	26
85.64.16.21	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	26
176.12.138.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
109.253.156.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
176.12.137.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	20
109.253.132.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	18
66.249.75.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	17
66.249.75.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	16
213.251.182.10	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	14
109.253.144.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	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	13
2.54.10.40	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.10.40	Block	12
41.68.77.11	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.68.77.11	Block	11
109.253.130.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
84.108.34.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
46.19.85.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
109.253.156.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
85.64.178.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.178.208	Block	9
81.218.0.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.0.130	Block	8
46.19.85.87	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	8
79.182.12.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
2.54.130.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8