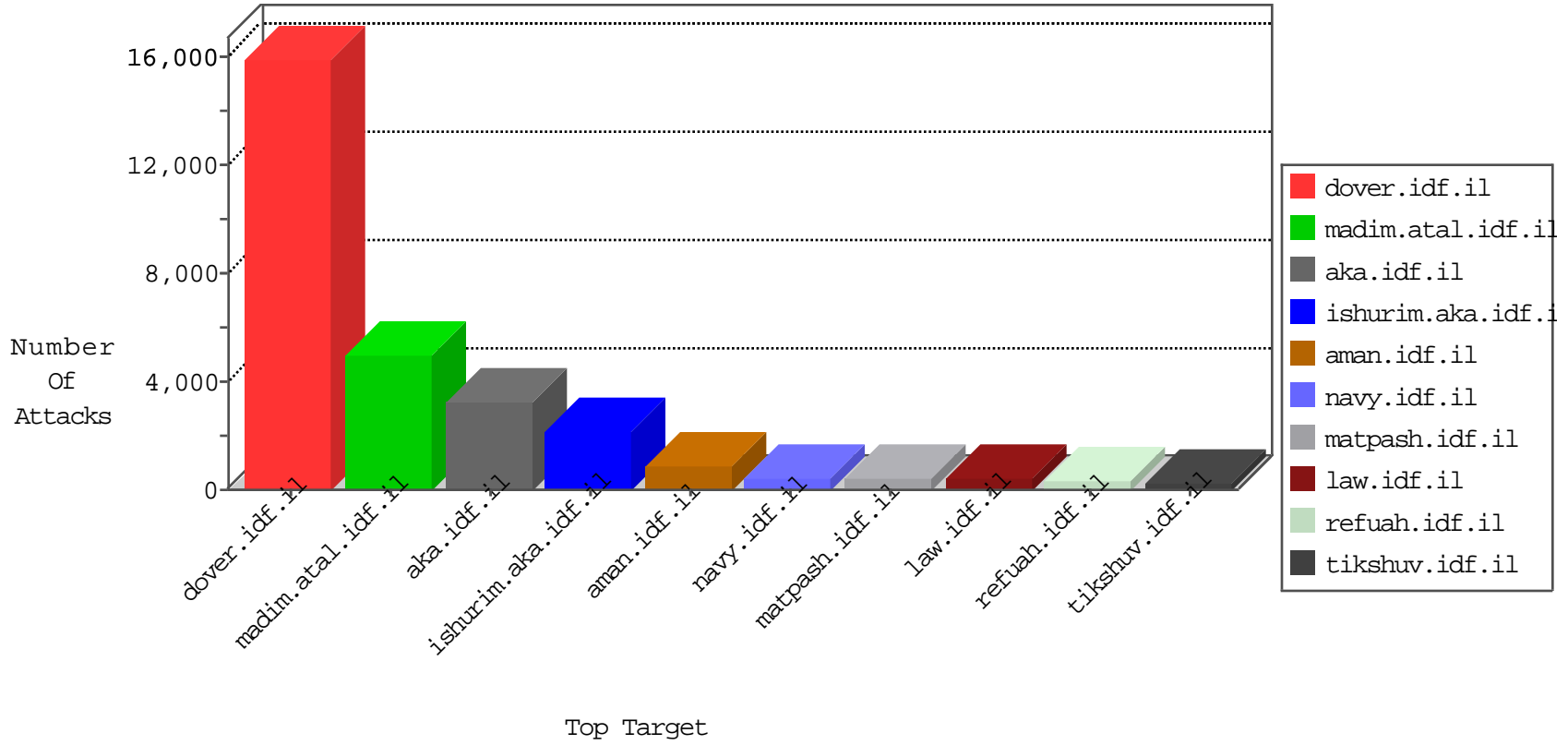


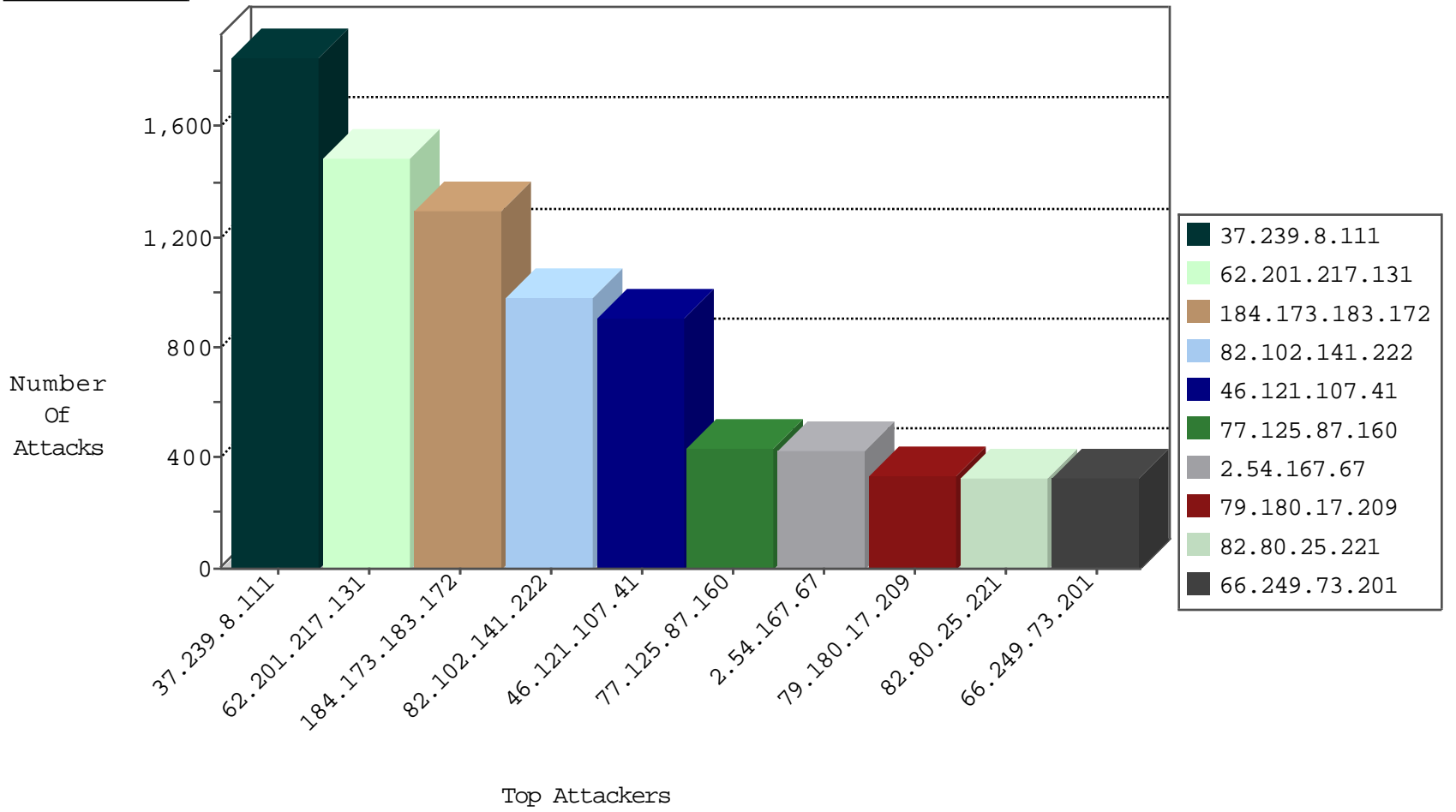
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	11955
66.249.64.171	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	9114
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6136
212.56.106.56	United Kingdom	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5788
66.249.75.237	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5673
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5456
66.249.78.29	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4878
178.191.163.54	Austria	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4335
84.202.157.229	Norway	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3622
66.249.69.66	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3449
66.249.93.245	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3403
95.132.4.189	Ukraine	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3104
66.249.78.51	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	2841
66.249.75.29	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2571
66.249.93.239	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2447
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	1625
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1446
66.249.93.242	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1413
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1365
109.65.8.116	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	981
66.249.64.96	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	933
66.249.78.15	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	919
173.252.113.113	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	787
66.249.78.204	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	697
77.125.222.246	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	648
46.117.190.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	411
89.138.194.107	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	407
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	342
85.130.184.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
82.102.141.222	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	292
109.186.145.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	289
5.28.173.201	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	283
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
94.159.237.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	215
77.127.183.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
31.168.84.241	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
212.150.171.253	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
66.249.81.209	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	178
207.232.36.210	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
85.64.12.225	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
77.126.66.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
62.128.35.129	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
109.160.244.80	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
5.29.190.100	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
37.26.148.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.183.134.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
84.109.180.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
77.126.165.162	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105

## 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	519
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	435
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	274
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	261
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	230
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	161
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	127
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
89.139.173.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	24
207.232.27.5	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
85.110.209.46	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
80.178.227.153	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
212.179.162.114	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
173.178.202.43	Canada	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
147.235.185.74	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.117	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
24.102.135.27	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
87.69.173.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.180.11.25	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.255.217	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
5.43.202.69	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.181.173.152	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
81.218.148.212	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.117.17.211	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.246.138.75	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.64.5.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
64.246.165.200	United States	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	4
193.169.70.101	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
87.68.157.75	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
80.98.71.112	Hungary	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.29	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.224	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.227	Israel	147.237.77.216	dover.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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	329
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	133
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 Ddos attack	69
122.228.207.193	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	5
109.64.155.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
122.228.207.193	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	4
46.117.165.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
64.79.85.205	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	3
122.228.207.193	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	3
212.143.99.62	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
212.129.52.90	France	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	3
91.199.69.254	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
122.228.207.193	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
122.228.207.193	China	147.237.76.198	e.ychalan.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.193	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
122.228.207.193	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.193	China	147.237.0.16	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
87.68.24.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.113.210	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
82.166.102.236	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	2
37.142.250.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.230.94.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.99	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.138.22	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.66.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.93.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
79.181.173.152	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
213.8.240.46	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
176.228.168.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
109.186.152.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.46.21	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
122.228.207.193	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
84.109.115.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
80.246.133.136	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
109.66.0.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.0.19	nadim.atal.idf.il	ET SCAN Potential SSH Scan	2
77.127.19.67	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
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	701
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	641
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	280
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	244
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
79.180.11.25	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	195
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	93
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
167.102.215.2	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
176.12.156.21	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
184.168.200.104	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	48
123.180.234.186	China	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	47
2.54.21.201	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	47
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
109.253.147.40	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.142.9	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
79.178.124.223	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.145.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.147.148	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.144.204	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.141.170	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.143.159	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.146.249	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
31.210.187.7	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	38
176.12.151.223	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.253.132.119	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.253.129.109	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.157.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.149.180	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
79.181.155.171	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.149.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.144.129	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.144.146	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
67.11.134.19	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.135.87	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.135.236	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
77.126.243.222	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
115.119.113.194	India	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
109.65.169.89	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
82.80.137.33	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
109.253.143.149	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.177.7.113	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
176.12.146.36	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.139.101	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
176.12.150.104	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.102	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.157.187	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30

02-12-2015-00:00:00 to 02-13-2015-00:00:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.107.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	910
82.102.141.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	760
2.54.167.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	427
62.201.217.131	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	345
79.180.17.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	337
176.12.140.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	230
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.239.8.111	Block	212
37.239.8.111	Iraq	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	211
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
46.19.85.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
176.12.149.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
109.253.139.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
176.12.151.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.151.25	Block	126
109.253.149.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
79.176.17.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
109.253.156.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	107
176.12.144.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.214	Block	86
176.12.141.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
2.54.48.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
176.12.144.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
37.26.147.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	46
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	46
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	46
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	39
109.253.138.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	36
93.172.152.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
176.12.136.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
176.12.141.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.157.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
109.253.136.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
77.125.78.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code Custom Temporary	Block	17
176.12.141.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	15
115.25.81.70	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	14
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.249	Block	13
176.12.141.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
176.12.143.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
213.151.57.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
176.12.143.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
85.64.178.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.178.208	Block	12
115.25.81.71	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	12
84.108.56.162	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 84.108.56.162	None	12
115.25.81.72	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	12
79.176.111.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
46.117.75.115	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.117.75.115	Block	12

02-12-2015-00:00:00 to 02-13-2015-00:00:00