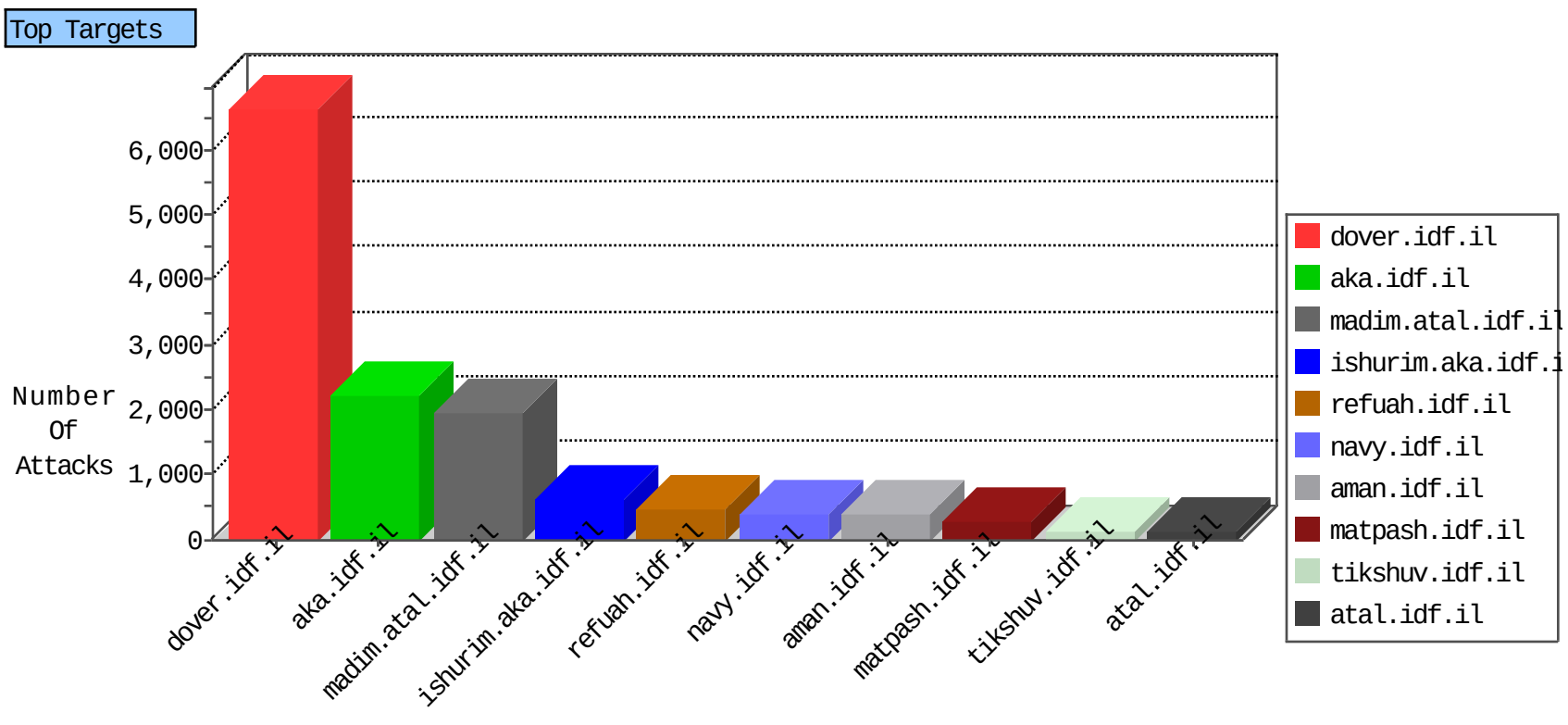
03-17-2015-00:00:08 to 03-18-2015-00:00:08

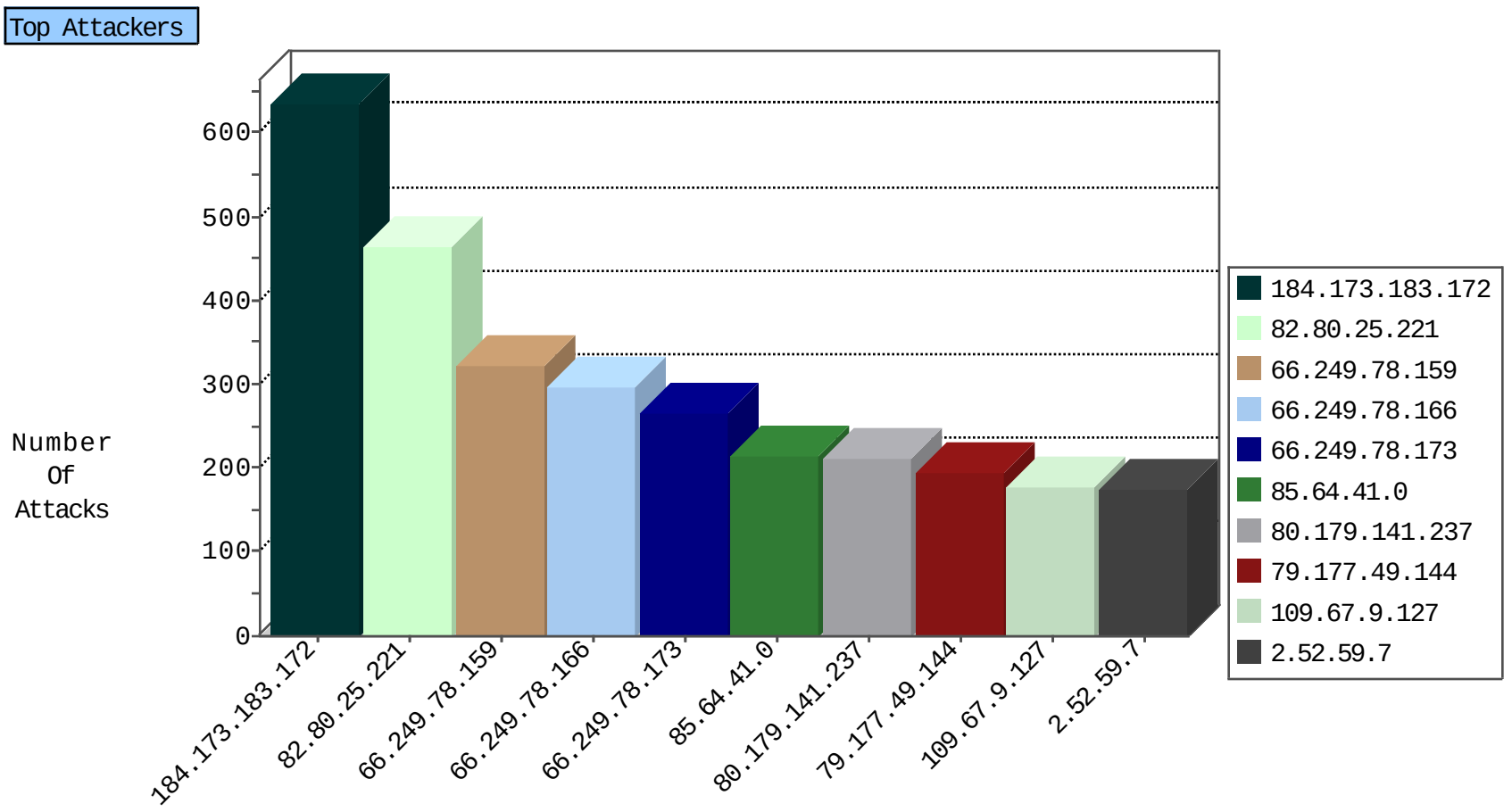
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-17-2015-00:00:08 to 03-18-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2577
80.179.141.237	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	1103
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	444
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	367
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	305
80.179.141.237	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
85.250.88.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
37.239.68.112	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	178
5.29.6.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
77.125.208.12	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
109.253.159.59	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
176.12.146.236	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	127
176.12.146.236	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
46.121.56.51	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
176.12.149.9	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	76
84.111.115.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
85.250.108.127	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
176.12.149.9	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
84.109.75.62	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64
82.102.141.251	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	42
168.235.197.166		147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	27
82.102.141.251	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	26
85.250.108.127	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	20
93.173.185.35	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	19
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	15
82.102.141.253	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	13
82.102.141.250	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	8
212.143.139.219	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	7
89.139.173.221	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	6
82.102.141.251	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	5
182.214.51.65	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	3
42.98.84.156	Hong Kong	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
61.166.189.69	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
85.18.173.109	Italy	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	2
222.186.58.177	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
202.157.226.24	Japan	147.237.76.39	mobile.meitav.idf.i	Block_Udp_All_Nets	drop	2
117.21.176.17	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
112.118.7.232	Hong Kong	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.40	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
218.227.218.92	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
189.10.55.48	Brazil	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
54.76.44.111	United States	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Https	drop	1
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
113.108.21.16	China	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1
71.6.216.46	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

03-17-2015-00:00:08 to 03-18-2015-00:00:08

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	636
79.177.49.144	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	196
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	144
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	94
27.153.208.142	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
86.85.14.46	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
86.85.14.46	Netherlands	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
212.34.12.182	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
77.127.246.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
212.34.12.182	Jordan	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
211.124.49.60	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
79.178.117.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
180.76.5.193	China	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	7
37.142.217.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.43.93.111	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
41.33.231.88	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
95.86.67.233	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
211.124.49.60	Japan	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
68.83.107.253	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
109.67.137.148	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
79.176.36.218	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
88.241.45.185	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
87.68.60.231	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.225.26	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
84.94.173.251	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	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
173.220.55.236	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	3
212.150.174.186	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
85.65.6.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
75.97.34.172	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.121.114.227	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.205.81.115	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.43.93.111	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
176.228.190.5	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
93.104.0.91	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

03-17-2015-00:00:08 to 03-18-2015-00:00:08

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	387
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	132
46.19.86.77	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	43
46.210.114.60	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
79.180.154.19	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	37
212.143.139.219	Israel	147.237.76.86	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	21
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
115.231.218.147	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
87.68.249.75	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
218.24.171.223	China	147.237.77.227	e.hamaz.idf.il	GPL SCAN nmap TCP	2
66.249.78.165	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
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
188.165.15.231	France	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
84.111.200.57	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
74.82.198.10	Canada	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
212.179.61.120	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
2.54.176.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.154	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
59.46.193.114	China	147.237.77.227	e.hamaz.idf.il	GPL SCAN nmap TCP	2
213.204.127.33	Lebanon	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
128.61.240.66	United States	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.6	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.147	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
79.180.39.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.147	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
176.12.144.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.204	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.24.171.223	China	147.237.76.44	e.refuah.idf.il	GPL SCAN nmap TCP	2
207.46.13.133	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.158	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
89.248.162.228	Netherlands	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
5.28.187.16	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.114	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
74.82.198.10	Canada	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.248.162.228	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
59.46.193.114	China	147.237.76.44	e.refuah.idf.il	GPL SCAN nmap TCP	2
74.82.198.10	Canada	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
115.231.218.147	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
37.26.147.205	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.52.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.161.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.107.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.193	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.26.11.118	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1

03-17-2015-00:00:08 to 03-18-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	224
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	192
79.228.107.245	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	156
188.120.148.183	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	87
2.54.36.157	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	62
2.52.59.7	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	58
2.52.59.7	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	57
188.120.148.183	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	55
2.52.59.7	Israel	147.237.76.42	refuah.idf.il	Invalid sequence number	Bad TCP sequence	monitor	55
85.237.234.151	Slovakia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
176.12.144.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
157.55.39.95	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.146.13	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
87.68.91.146	Israel	147.237.0.19	madim.atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	33
176.12.136.226	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.149.158	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.140.189	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	30
207.241.226.144	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	28
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
132.3.21.79	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
31.13.162.33	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	26
31.186.228.27	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	26
31.186.228.91	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	25
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
46.244.94.61	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
31.186.228.90	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
188.120.148.250	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	24
176.12.138.182	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
176.12.146.32	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.94	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	22
176.12.136.142	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
5.22.129.168	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
31.186.228.24	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	22
207.46.13.121	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
31.186.228.89	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	21
79.161.20.58	Norway	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	21
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	20
5.22.129.168	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	19
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	18
46.19.86.77	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	18
109.253.141.213	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
2.54.58.212	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
2.54.58.212	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.176.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	173
109.67.9.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
109.253.135.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	132
85.64.41.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	130
194.90.229.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	121
176.12.137.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	108
80.178.2.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	90
85.64.41.0	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.64.41.0	Block	83
176.12.149.239	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.149.239	Block	75
109.253.143.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
176.12.143.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
46.19.86.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	67
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	66
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	64
176.12.141.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	64
109.253.159.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.159.59	Block	62
109.253.157.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
37.140.188.30	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.140.188.30	Block	51
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	50
176.12.143.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	46
109.253.145.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
109.253.157.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
176.12.146.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
176.12.138.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	39
176.12.141.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
176.12.139.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
109.253.83.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
176.12.149.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
109.253.137.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
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	20
149.78.28.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	19
46.120.80.57	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	16
176.12.150.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
176.12.144.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
176.12.148.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
176.12.144.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
188.165.15.200	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.200	Block	13
37.142.46.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	12
82.81.193.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	11
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
176.12.142.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
109.253.144.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
109.64.68.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
109.253.158.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
17.142.144.105	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.144.105	Block	9
17.142.149.254	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.149.254	Block	9