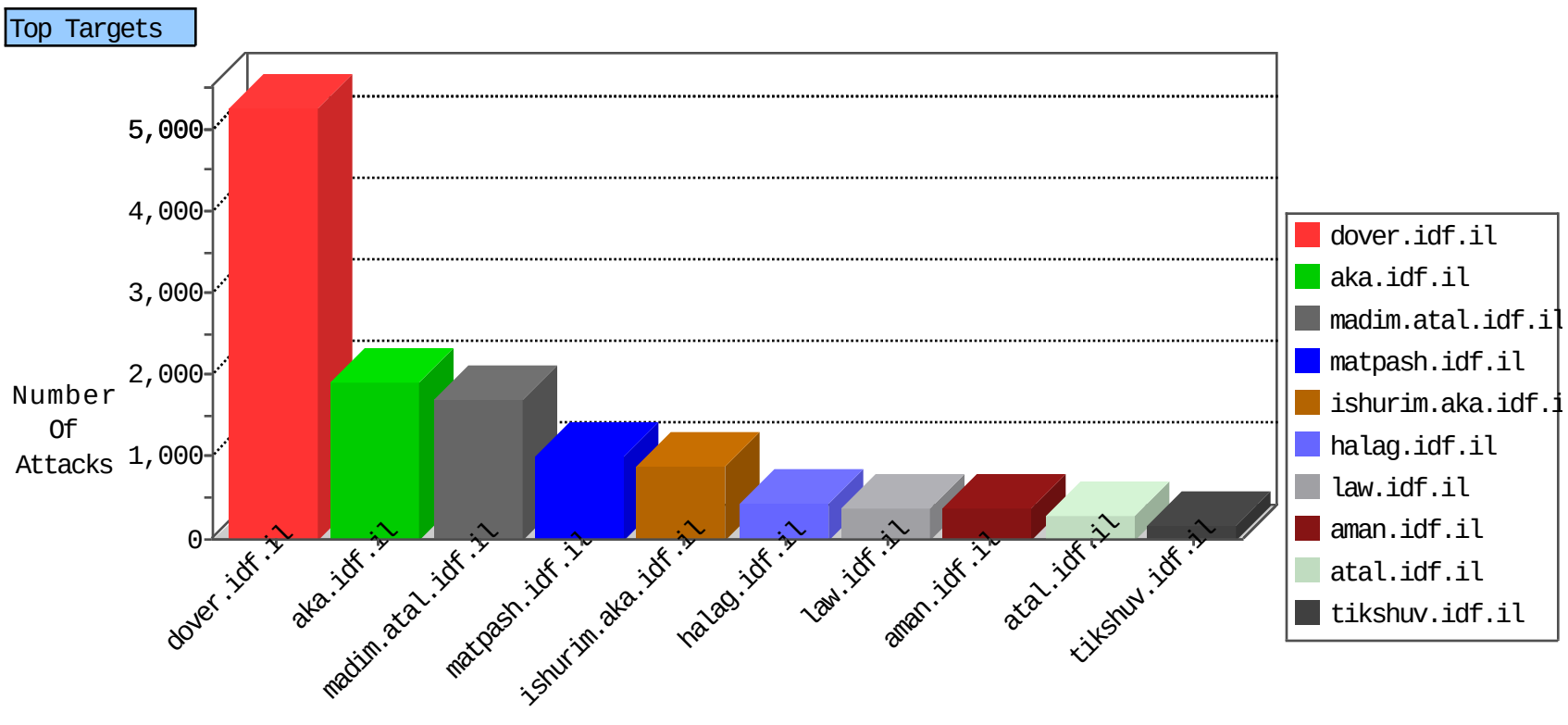
02-28-2015-00:00:09 to 03-01-2015-00:00:09

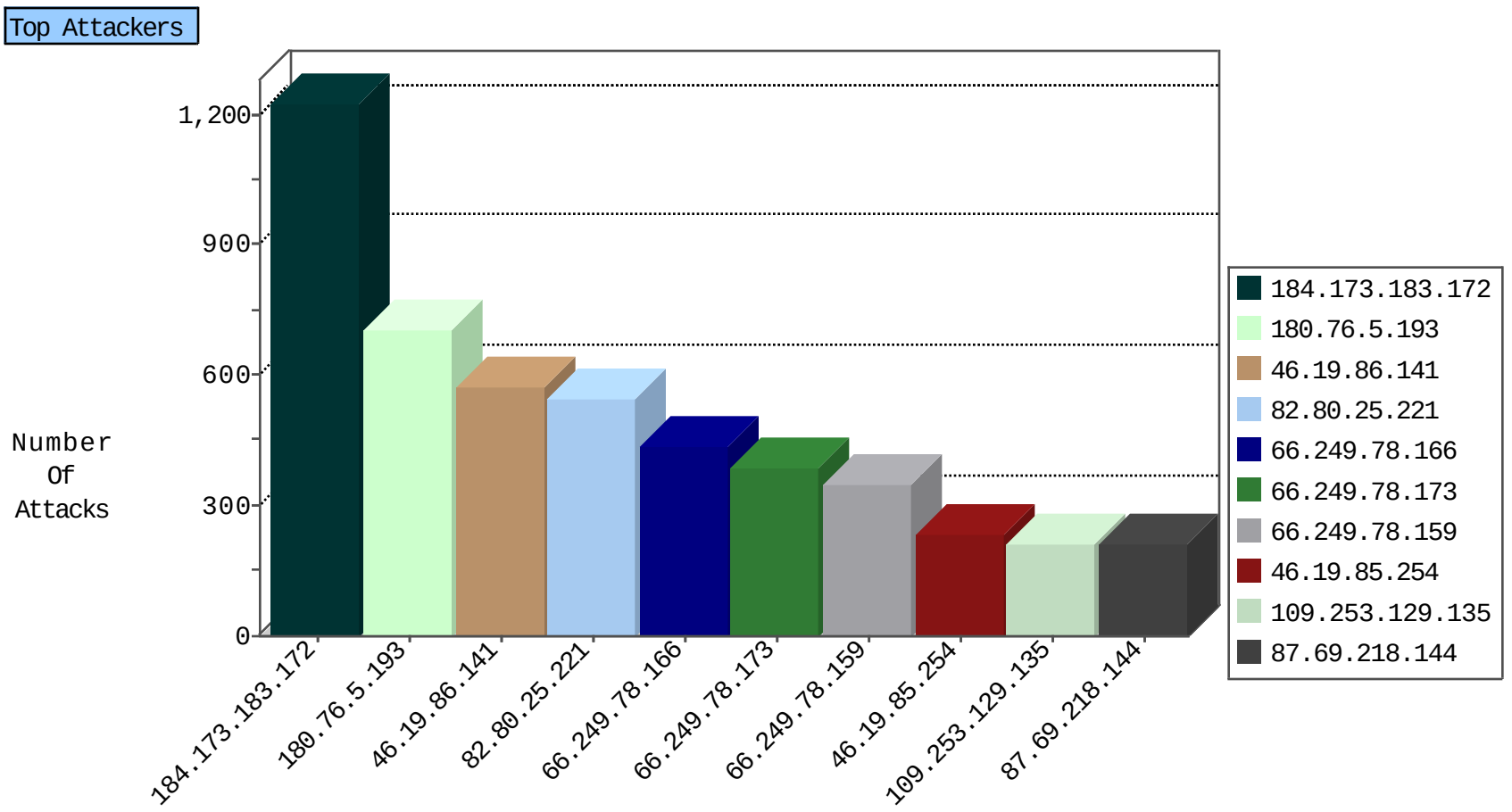
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-28-2015-00:00:09 to 03-01-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.196	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4081
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	589
109.64.21.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	458
84.228.12.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	359
89.139.63.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	290
84.229.196.15	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
46.120.73.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
85.64.125.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	185
94.159.189.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.180.166.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
84.94.93.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
84.229.157.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
79.176.17.158	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.183.35.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	114
84.95.134.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.116.1.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
109.65.171.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
37.26.146.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	87
85.64.79.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
80.246.137.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
2.54.143.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
46.120.73.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
46.19.86.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
109.160.218.72	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
80.246.137.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	56
46.19.85.72	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	26
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
41.140.5.105	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	10
79.181.170.252	Israel	147.237.77.170	maarachot.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	5
176.193.86.17	Russian Federation	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	4
46.19.85.242	Israel	147.237.77.170	maarachot.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	4
175.143.183.136	Malaysia	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
2.54.31.34	Israel	147.237.77.170	maarachot.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
220.231.161.177	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
84.108.106.206	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
46.19.85.66	Israel	147.237.77.170	maarachot.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
46.229.164.115	United States	147.237.77.74	law.idf.il	network flood IPv4 TCP-RST	drop	2
109.65.145.247	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
176.193.86.17	Russian Federation	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
125.88.17.156	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Http	drop	2
222.186.21.202	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
115.231.218.147	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
113.108.21.16	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Http	drop	2

02-28-2015-00:00:09 to 03-01-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	561
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	404
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	317
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	261
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	245
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	203
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	61
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	50
69.197.186.210	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
173.208.209.74	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	30
85.250.180.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	29
85.65.226.211	Israel	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	17
94.231.109.13	Denmark	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
37.142.233.235	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
158.58.168.211	Italy	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	11
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
94.231.109.13	Denmark	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	10
200.37.221.35	Peru	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
84.94.164.136	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
212.34.12.192	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.152	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.8.194.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
85.64.79.21	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	4
46.117.225.121	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
158.58.168.211	Italy	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
31.168.66.82	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
85.65.226.211	Israel	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.120	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
5.86.207.234	Italy	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3

02-28-2015-00:00:09 to 03-01-2015-00:00:09

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	429
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	142
192.35.222.17	United States	147.237.77.216	dover.idf.il	ET DOS SSL Bomb DoS Attempt	11
2.52.169.72	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
5.102.254.141	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
62.90.180.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.69.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
199.189.87.83	United States	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	4
58.20.54.249	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	3
122.228.207.193	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.23	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.179.102.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.24.171.223	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	2
122.228.207.199	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
109.64.10.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.242.52	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
79.181.18.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.147	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
213.57.185.151	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.129.110	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.147	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
84.108.86.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.106.150	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.46.193.114	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	2
122.228.207.193	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
5.29.130.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.233.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.16.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.119.52	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
199.189.87.83	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
122.228.207.199	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.23	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
80.179.204.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.199	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
115.231.218.147	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.52	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.39.174	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
80.74.124.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.160.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.174.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.180.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
85.65.42.102	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.23.91	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2

02-28-2015-00:00:09 to 03-01-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	398
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	346
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	312
92.132.135.94	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	196
109.66.56.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	102
176.193.86.17	Russian Federation	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	98
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	88
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
186.15.43.184	Costa Rica	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
168.235.197.26		147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	46
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
94.249.8.246	Jordan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
123.180.213.60	China	147.237.77.216	dover.idf.il	SAM rule	drop	drop	40
84.108.205.13	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	40
73.190.55.128	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
93.172.75.253	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	36
176.12.139.153	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.151.55	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.93.213	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.138.219	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.233.249.161	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
200.41.138.128	Argentina	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	29
31.210.187.179	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.141.190	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.151.45	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
50.62.135.148	United States	147.237.0.35	akaws.idf.il		drop	drop	24
176.12.140.154	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.134.108	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
37.26.147.138	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
94.231.109.13	Denmark	147.237.72.166	aka.idf.il	SAM rule	drop	drop	22
79.180.105.52	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
217.12.204.117	Ukraine	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	21
104.180.225.21		147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
176.12.151.179	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.93.219	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
77.126.175.152	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
109.253.145.96	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.88.187	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.146.161	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
79.180.29.218	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.131.2	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.93.216	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
199.30.24.226	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.19.85.134	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	17

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.141	Block	574
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	222
109.253.129.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	212
87.69.218.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	210
89.139.45.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
109.253.142.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
5.28.137.6	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	94
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73
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	40
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
109.253.143.50	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.143.50	Block	35
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	32
5.29.132.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.132.83	Block	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	30
109.65.193.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.193.66	Block	27
109.253.146.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	22
217.12.204.117	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	20
109.64.62.115	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.62.115	Block	18
85.250.12.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	18
46.229.164.99	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.99	Block	13
46.116.205.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	10
89.139.28.213	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	10
79.179.53.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
46.229.164.115	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.115	Block	10
46.229.164.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	9
149.78.253.72	United States	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.253.72	Block	9
176.67.100.91	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.67.100.91	Block	9
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	8
79.183.17.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
87.69.65.90	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	8
5.29.29.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
84.228.29.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
80.246.139.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	7
197.27.92.209	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.27.92.209	Block	7
79.180.190.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/giyus/general.aspx	Block	6
5.29.206.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.67.187.27	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.67.187.27	Block	5
79.180.113.234	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	4
87.69.219.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
94.159.236.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 94.159.236.219	Block	4
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	4
213.57.129.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
37.26.147.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
37.142.30.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
46.120.24.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	4