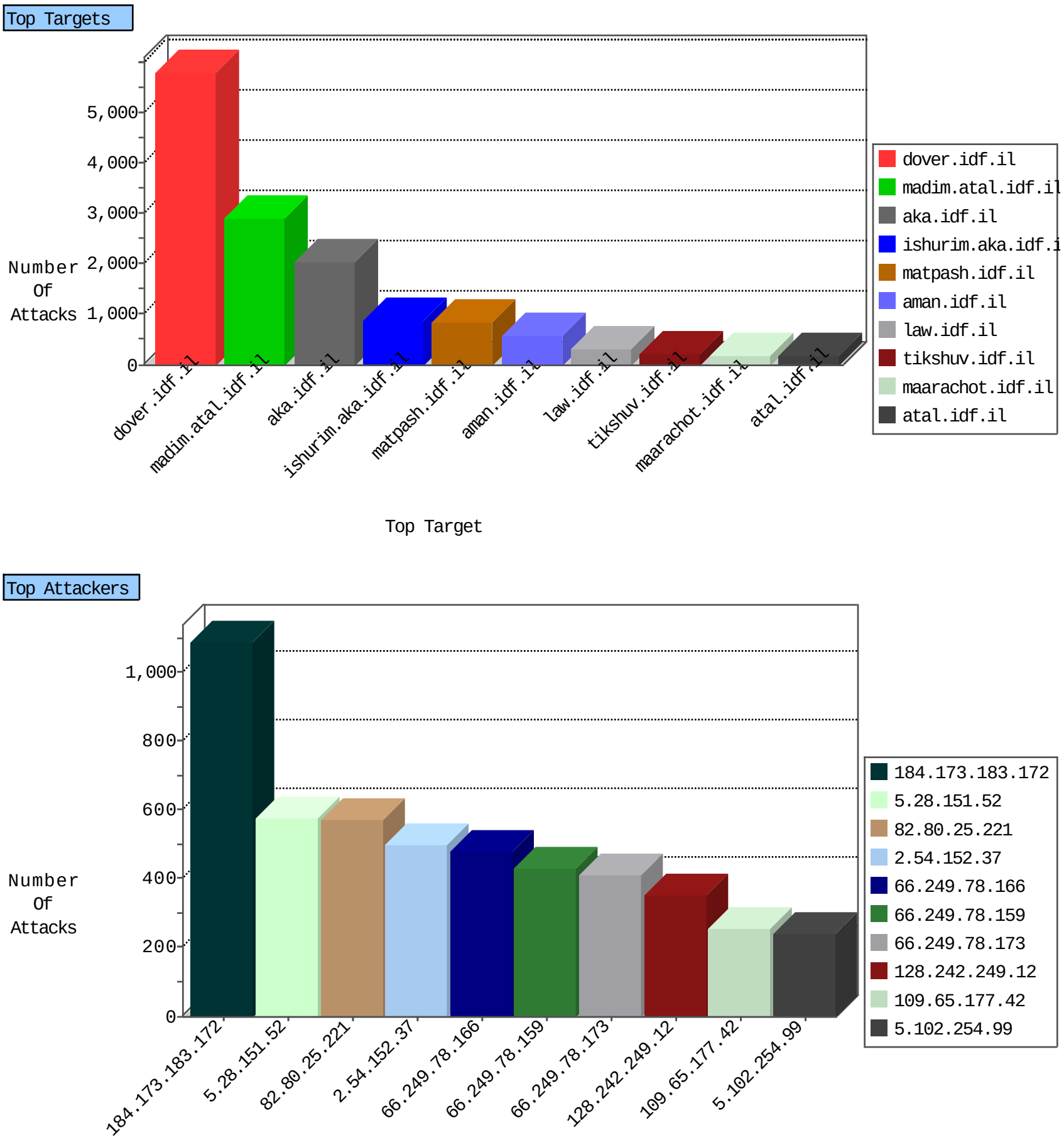
02-27-2015-00:00:00 to 02-28-2015-00:00:00

IDF Under Attack Daily Report



02-27-2015-00:00:00 to 02-28-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
185.13.194.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1773
66.249.78.60	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1286
198.24.178.242	United States	147.237.76.177	ncore.idf.il	TCP handshake violation, first packet not syn	drop	1180
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	819
2.54.4.47	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	447
213.57.199.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	388
109.66.120.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	355
77.126.75.80	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
46.116.102.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	305
79.183.114.42	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	234
85.65.203.72	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
84.108.61.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
89.138.225.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
89.139.180.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
87.68.153.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	123
79.177.131.79	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
87.69.180.145	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
84.228.179.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
109.66.117.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
84.228.161.80	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
84.109.80.185	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
79.181.148.86	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
109.160.241.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	75
2.54.131.171	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
2.54.161.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
85.65.213.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.182.129.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.116.111.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
46.116.102.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
79.181.170.252	Israel	147.237.77.170	maarachot.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	30
79.182.129.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	20
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
79.181.148.86	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	17
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	15
82.145.221.30	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
46.19.85.60	Israel	147.237.77.243	mobile.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
175.138.38.115	Malaysia	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	5
192.116.172.36	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
59.147.163.2	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
212.179.222.198	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
84.109.100.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2

02-27-2015-00:00:00 to 02-28-2015-00:00:00

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	684
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	354
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	238
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	168
37.130.227.133	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	44
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	32
104.155.13.140		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	12
104.155.13.140		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
128.39.142.20	Norway	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
212.34.12.127	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
41.35.228.122	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.182.51.126	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
89.187.142.208	Czech Republic	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
70.71.188.236	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.101.158.132	United States	147.237.77.19	law-forum.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	5
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	4
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
77.127.234.94	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
167.160.116.56		147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	3
78.175.135.166	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
173.185.253.118	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.64.235	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3

02-27-2015-00:00:00 to 02-28-2015-00:00:00

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	448
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
198.101.158.132	United States	147.237.77.19	law-forum.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	5
104.42.19.146		147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	4
84.94.18.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
37.187.250.73	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
115.231.218.147	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	3
104.42.19.146		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.23.59.161	France	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
213.57.168.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
42.121.64.180	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
93.172.186.188	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
2.52.15.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
58.20.54.249	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.228.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
109.253.130.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.109.96.215	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.37.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
94.53.216.105	Romania	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.64.191.241	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.53.216.105	Romania	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
109.64.191.241	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.53.216.105	Romania	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
87.69.165.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.152.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.53.216.105	Romania	147.237.77.74	law.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
94.23.59.161	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
77.127.78.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
94.23.59.161	France	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
176.12.143.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
213.57.72.127	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
85.65.177.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.147.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
84.109.97.37	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
80.74.124.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.235.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
37.142.58.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.147	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
109.66.8.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.53.216.105	Romania	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2

02-27-2015-00:00:00 to 02-28-2015-00:00:00

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	444
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	400
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	374
91.198.204.122	Denmark	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	226
198.103.167.20	Canada	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	141
113.200.26.199	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	104
62.201.203.85	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
137.95.1.11	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	83
149.78.165.247	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
5.239.229.143	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	68
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.141.9	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
108.27.92.243	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	46
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
80.179.78.115	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
168.63.200.167	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	32
79.180.31.244	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.144.215	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.157.234	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
149.78.100.58	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
149.78.32.97	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
66.249.64.92	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
157.55.39.160	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
84.228.49.131	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
207.46.13.118	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.129.107	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.133.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
46.19.85.156	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
98.103.165.210	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	24
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.179.147.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.253.147.204	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.147.219	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.160.225.74	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
210.186.142.62	Malaysia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.87.117.224	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	22
165.24.247.200	United States	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
82.81.128.71	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
149.78.43.148	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
92.241.39.124	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
176.12.148.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.137.229	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.150.11	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.148.55	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.28.151.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.151.52	Block	570
2.54.152.37	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.152.37	Block	501
109.65.177.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	257
5.102.254.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.102.254.99	Block	239
176.12.141.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
2.54.131.93	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.131.93	Block	187
109.253.133.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
176.12.144.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	125
80.246.136.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	110
109.66.20.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	102
176.12.139.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.149.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
176.12.139.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
80.246.137.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.137.225	Block	45
85.64.22.94	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.22.94	Block	44
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	38
176.12.146.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
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	32
176.12.141.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
176.12.143.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	25
176.12.141.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
85.64.38.5	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	23
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	22
83.130.111.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
80.246.137.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
176.12.137.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	10
79.177.207.83	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	9
109.67.54.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	9
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/giyus/general.aspx	Block	9
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/giyus/general.aspx	Block	8
109.253.144.218	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.144.218	Block	8
5.153.235.9	Sweden	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	8
149.78.158.94	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
79.181.33.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
109.67.28.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
176.12.150.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
84.108.227.128	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.227.128	Block	7
176.12.137.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
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
5.29.109.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
37.26.147.215	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.147.215	Block	6
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.120	Block	6
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	6
66.249.64.167	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
2.54.58.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
109.253.147.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6

02-27-2015-00:00:00 to 02-28-2015-00:00:00