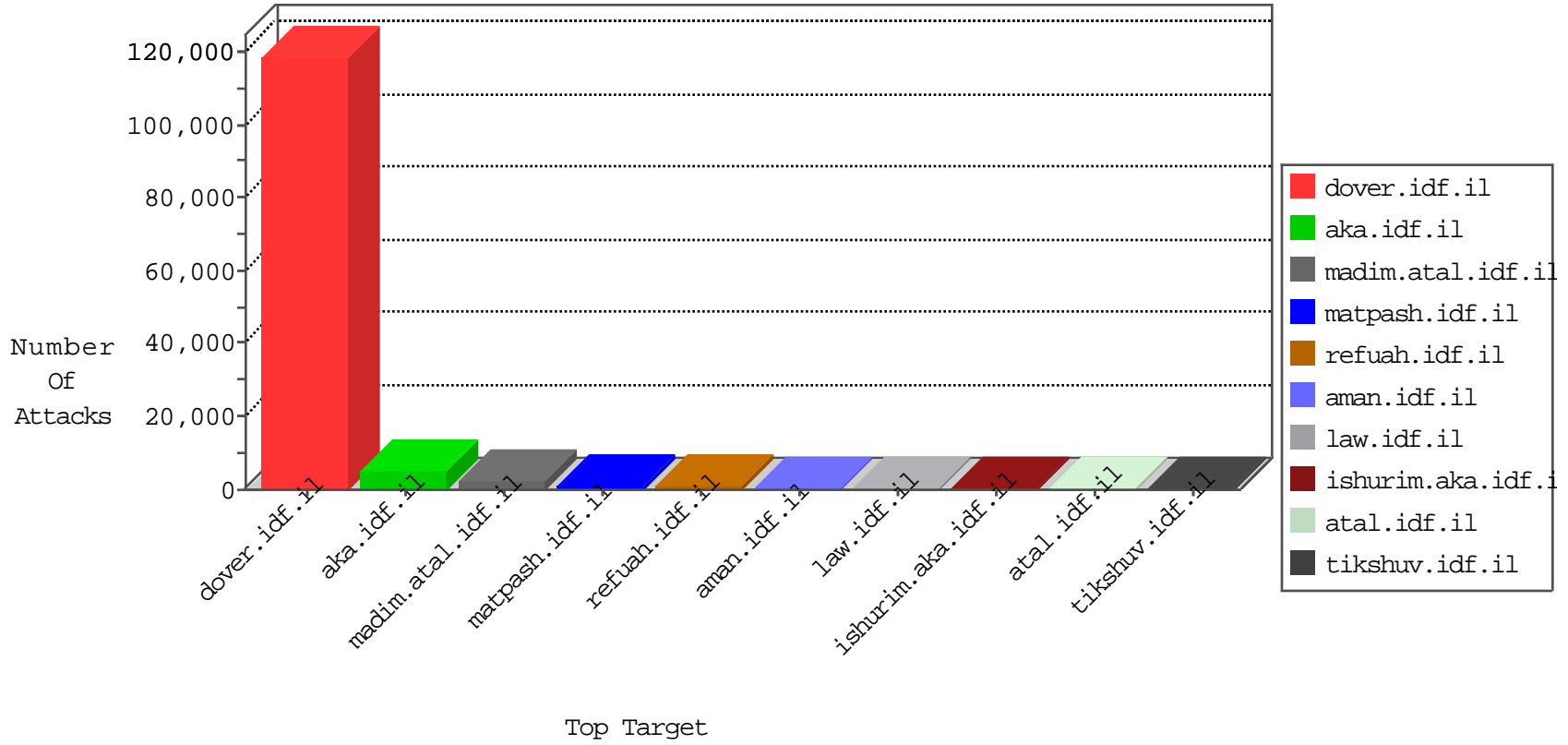


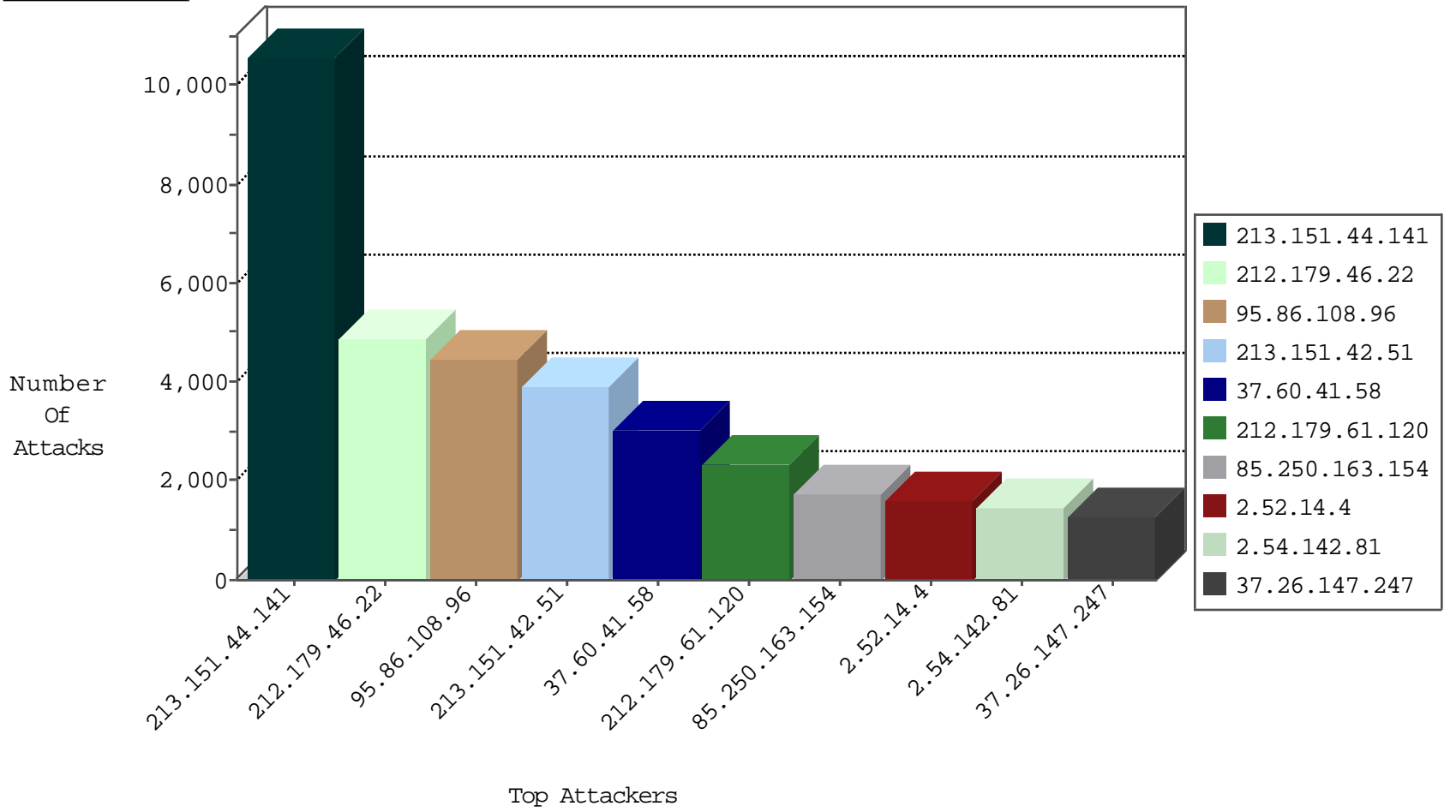
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.19.85.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5857
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5258
220.181.108.183	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2867
46.19.85.39	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2759
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	871
5.29.18.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	638
94.159.174.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	560
220.181.108.180	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	408
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	396
78.171.84.119	Turkey	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	315
220.181.108.185	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	304
79.181.101.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	265
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
220.181.108.114	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	219
109.64.141.50	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	215
85.65.194.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
77.126.218.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	185
79.181.192.3	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
220.181.108.182	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	155
213.151.46.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	149
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
213.151.36.114	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.166.145.239	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	125
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	123
220.181.108.156	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	120
109.65.3.149	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
199.190.46.75	Satellite Provider	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	113
46.116.113.188	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
46.116.142.147	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	103
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
185.32.178.107	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
109.65.52.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
109.67.147.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
87.69.188.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
149.78.37.250	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
80.246.136.142	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
176.12.144.212	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
80.246.137.49	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.150.125	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
80.12.35.30	France	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
185.32.178.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
46.19.86.23	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	81
46.121.62.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
109.186.6.6	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
213.57.32.176	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
89.139.171.44	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.159.42	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	566
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	514
212.185.61.12	Germany	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	212
212.185.61.12	Germany	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	209
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	137
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	118
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	114
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	87
138.134.192.10	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	25
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
107.167.185.113	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
107.167.185.113	United States	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
84.108.128.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
31.154.10.131	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
132.72.138.1	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
213.57.29.128	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
81.218.191.54	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
5.102.197.121	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	6
188.120.136.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
173.208.247.213	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.65.127.183	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
93.172.36.131	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
109.67.136.35	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
109.67.136.35	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In IDF

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.64.234	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	122
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	96
2.54.36.15	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	88
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	12
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	10
2.54.44.169	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER open_basedir PHP config option in uri	5
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER auto_prepend_file PHP config option in uri	5
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER safe_mode PHP config option in uri	5
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER disable_functions PHP config option in uri	5
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	5
160.176.170.188		147.237.77.216	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	5
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER suhosin.simulation PHP config option in uri	5
109.253.115.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
160.176.170.188		147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
27.74.130.34	Vietnam	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
78.129.148.77	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
194.90.167.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
84.111.38.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
79.180.19.213	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
160.176.170.188		147.237.77.216	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
138.134.192.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.254.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
160.176.170.188		147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt	2
176.195.248.171	Russian Federation	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
160.176.170.188		147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
79.179.65.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
160.176.170.188		147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
61.240.144.65	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
160.176.170.188		147.237.77.216	dover.idf.il	GPL WEB_SERVER global.asa access	2
37.142.65.248	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
144.0.0.60	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
27.74.130.34	Vietnam	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
78.129.148.77	United Kingdom	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
160.176.170.188		147.237.77.216	dover.idf.il	SERVER-WEBAPP Moveable Type unauthenticated remote command execution attempt	2
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
160.176.170.188		147.237.77.216	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 1	2
160.176.170.188		147.237.77.216	dover.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	2
212.143.110.33	Israel	147.237.72.166	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
79.182.68.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.234.73	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
213.151.44.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10580
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4851
95.86.108.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4471
213.151.42.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3900
37.60.41.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3014
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2313
85.250.163.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1731
2.52.14.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1593
2.54.142.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1480
37.26.147.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1282
2.52.164.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1240
212.76.112.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1212
95.86.94.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1210
172.56.10.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1062
37.142.4.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1006
212.143.127.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	942
82.166.164.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	904
77.125.150.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	895
209.88.198.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	880
81.218.71.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	845
80.74.107.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	762
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	729
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	728
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	722
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	708
85.250.165.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	672
84.228.46.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	612
5.29.135.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
85.115.58.180	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	484
2.54.134.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	475
46.19.86.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
82.145.220.76	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	429
46.19.86.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	423
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	422
62.219.13.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	396
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	384
82.145.223.30	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	372
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	371
91.220.22.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	366
79.179.31.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	363
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	350
199.190.46.143	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	342
2.54.182.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	338
132.70.33.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	337
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	337
2.54.20.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	328
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	326
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	324
95.86.64.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	318

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.138.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.138.209	Block	593
5.108.136.75	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.108.136.75	Block	358
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.56	Block	291
37.26.146.249	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.249	Block	210
2.54.150.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
176.12.149.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
185.32.178.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.89	Block	146
109.253.147.43	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.147.43	Block	142
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	139
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	121
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	90
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	88
79.177.34.140	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.34.140	Block	86
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	70
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	51
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
109.65.62.189	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	37
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	36
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	34
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	34
84.108.66.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	26
85.250.118.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	25
192.117.12.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	24
109.253.156.97	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.156.97	Block	23
176.12.150.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	21
212.179.61.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	20
79.176.200.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
85.130.226.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
84.111.7.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	18
84.108.4.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
2.54.18.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	16
149.78.186.175	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	15
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
95.86.68.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
212.143.147.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
109.67.166.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	13
89.139.9.145	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.9.145	Block	12
213.151.52.141	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
157.55.39.64	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.64	Block	12
95.86.127.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
195.160.240.11	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	11
85.65.161.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
207.46.13.25	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.25	Block	11
80.178.2.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
146.185.56.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
157.55.39.17	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.17	Block	9
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.213	Block	9