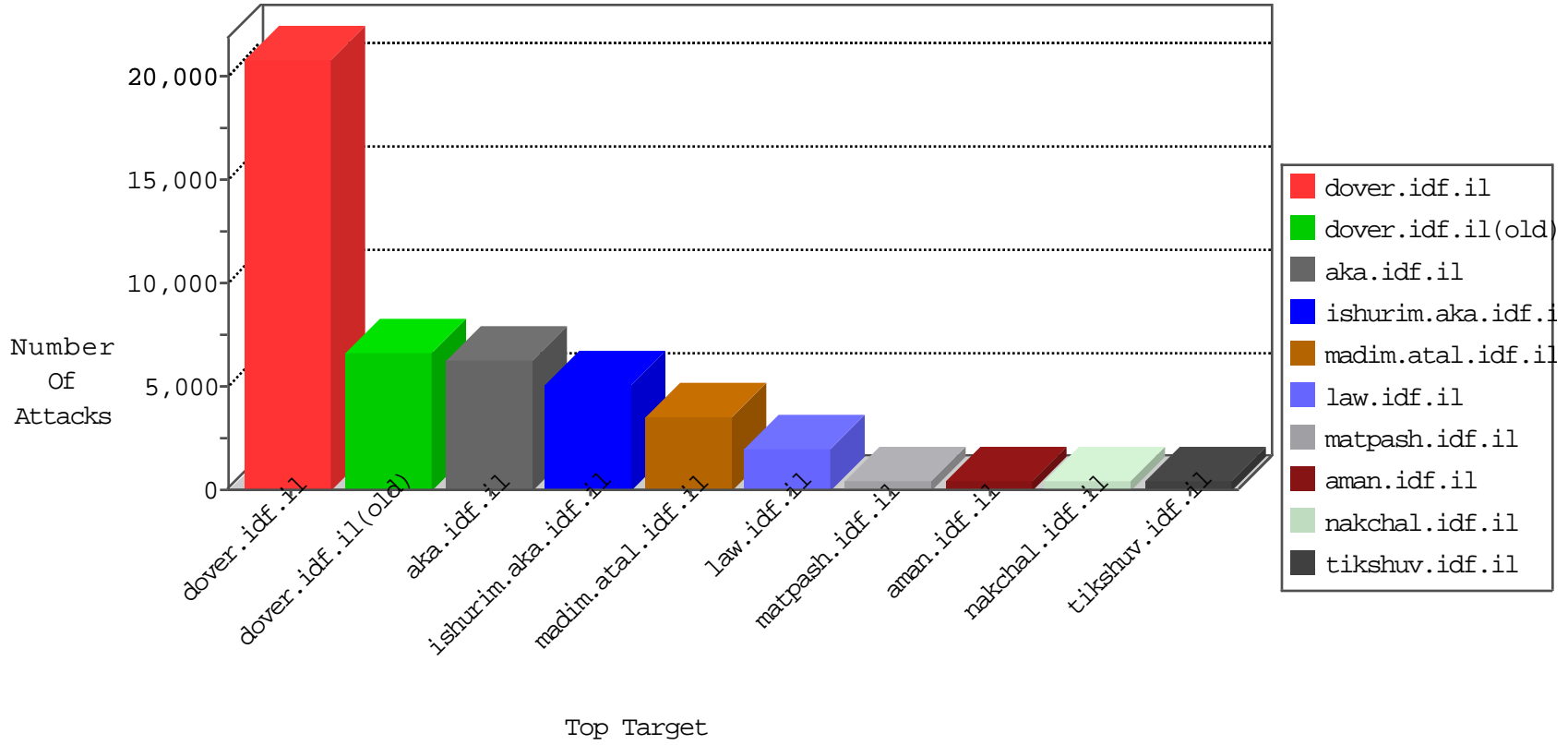


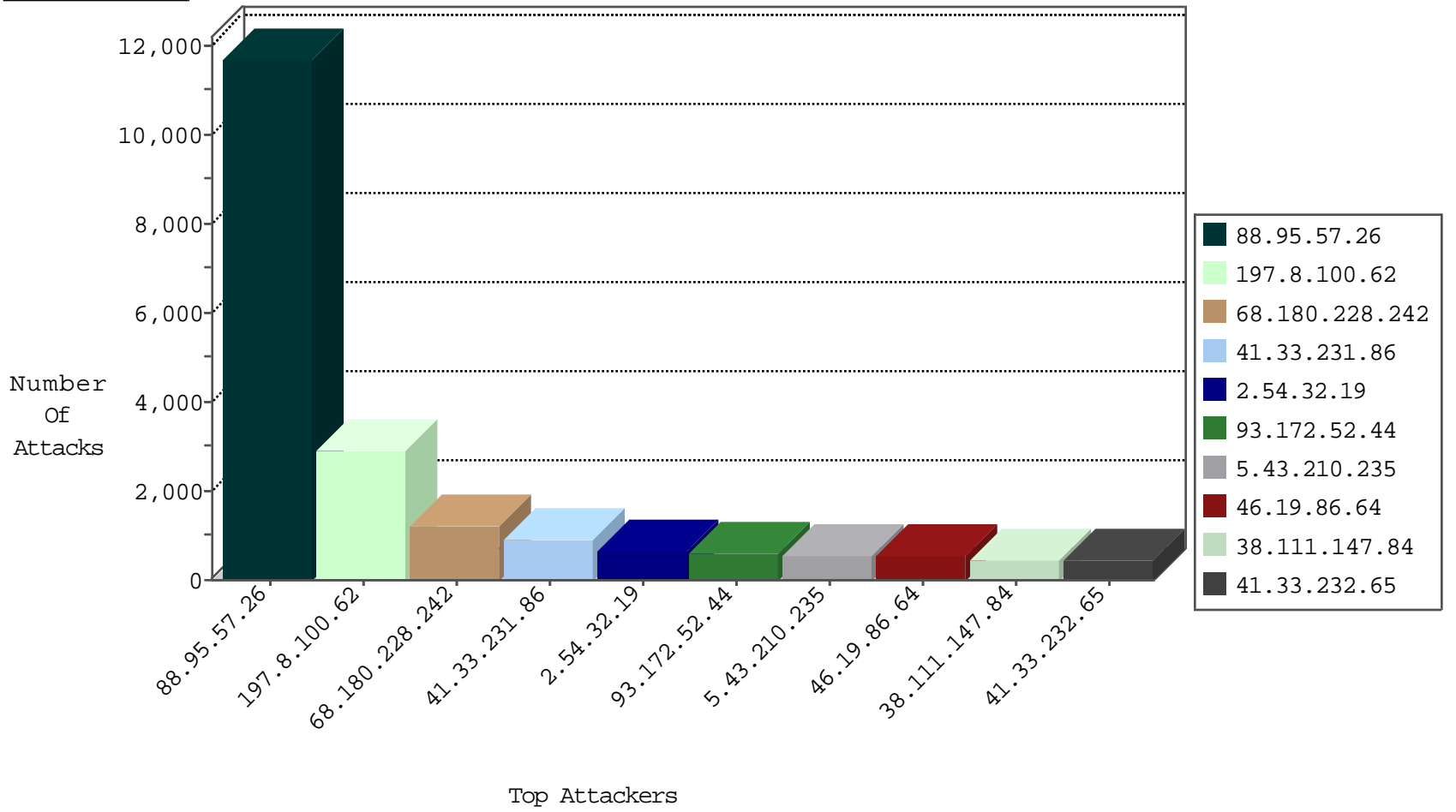
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
88.95.57.26	Norway	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	31546
212.150.112.130	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	363
2.54.130.126	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	94
213.57.198.27	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	81
37.26.147.254	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
46.19.86.215	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
2.54.46.215	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
82.102.141.208	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
82.102.141.214	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	65
82.80.79.50	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	63
82.102.141.200	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	30
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	27
82.102.141.193	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	26
193.109.199.151	United Kingdom	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
82.102.141.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	16
197.8.100.62	Tunisia	147.237.77.216	dover.idf.il	UDS-GET-Limit	drop	13
82.102.141.201	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	12
82.102.141.214	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	11
82.102.141.200	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	11
82.102.141.208	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	9
82.102.141.248	Israel	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	9
82.102.141.217	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	9
82.102.141.193	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	9
82.102.141.217	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	9
82.102.141.199	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	9
82.102.141.217	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	9
197.8.180.19	Tunisia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	8
82.102.141.249	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	8
82.102.141.193	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
81.218.183.91	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	7
125.64.35.67	China	147.237.76.86	navy.idf.il	TCP Scan (vertical)	drop	7
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	7
82.102.141.200	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	7
195.200.205.79	Israel	147.237.72.166	aka.idf.il	Anomaly-IP-bad-frag-bits	drop	7
82.102.141.202	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	7
188.15.230.90	Italy	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
62.210.244.74	France	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
82.102.141.201	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	6
82.102.141.255	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
82.102.141.213	Israel	147.237.77.243	mobile.idf.il	Invalid TCP Flags	drop	6
125.64.35.68	China	147.237.76.86	navy.idf.il	TCP Scan (vertical)	drop	6
82.102.141.213	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
82.102.141.255	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
82.102.141.218	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
82.102.141.251	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
82.102.141.215	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
94.176.148.28	Romania	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.96	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	101
66.249.78.15	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	96
66.249.78.22	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	90
120.24.64.253	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	89
66.249.78.89	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	87
66.249.78.29	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	82
66.249.78.82	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	49
27.153.204.157	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	35
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	32
62.90.243.139	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	27
85.250.53.200	Israel	147.237.72.166	aka.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	24
79.180.104.23	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	24
68.180.228.118	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	18
77.125.92.58	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	17
212.179.61.126	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	16
62.219.113.188	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	14
188.165.15.84	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	14
87.68.86.237	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	12
192.115.177.202	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.115.177.203	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
66.249.78.118	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	12
66.249.78.125	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	10
82.80.168.133	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	10
66.249.64.135	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	10
188.165.15.181	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
95.86.114.84	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
188.165.15.98	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
66.249.78.111	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
85.65.86.93	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
188.165.15.87	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
77.125.86.159	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
192.118.11.124	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
188.165.15.26	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
188.165.15.160	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
82.102.172.158	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
66.249.64.131	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
93.39.151.180	Italy	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
109.64.204.74	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
188.165.15.97	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
188.165.15.240	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
46.19.85.200	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
207.232.36.85	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
79.178.151.39	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
207.46.13.108	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6
81.218.251.249	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.57.63.30	Israel	147.237.77.216	dover.idf.il	17056: TLS: OpenSSL Invalid Session Ticket Denial-of-Service Vulnerability (ONLY enable under DoS attack)	Permit	6
37.26.147.201	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6
87.68.63.163	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	5
84.228.144.206	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.235	sviva.idf.il	Block_Level_70_100	Block	5

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	344
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	150
46.19.85.228	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	70
46.19.86.63	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
213.151.47.159	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	36
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Admin login page scan - Havij	23
5.39.219.26	Netherlands	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	20
85.250.188.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	11
80.230.4.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	10
37.142.152.219	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	7
82.80.198.164	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	7
107.167.110.60	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	5
176.228.182.148	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
77.127.68.101	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
94.159.217.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
202.77.120.66	Indonesia	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
202.77.120.66	Indonesia	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
82.205.18.196	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	3
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	3
212.68.144.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
202.77.120.66	Indonesia	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.19.86.210	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.116	United Kingdom	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
188.120.152.136	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.151.39.216	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
79.182.105.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
202.77.120.66	Indonesia	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
85.64.42.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.198.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.228.152.22	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.211	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.240.170	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.141.225.10	Korea, Republic of	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
213.57.37.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.196.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.170.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
74.208.155.85	United States	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
61.174.50.251	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
202.77.120.66	Indonesia	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
80.246.137.219	Israel	147.237.72.167	ishurim.aka.idf.il	ET DOS SSL Bomb DoS Attempt	2
74.208.155.85	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
79.178.164.36	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.16.72	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
202.77.120.66	Indonesia	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.64.166.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.107.35	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.195.208	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
74.208.155.85	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
88.95.57.26	Norway	147.237.77.216	dover.idf.il	SAM rule	drop	drop	10935
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)		drop	drop	934
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	904
93.172.52.44	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	584
88.95.57.26	Norway	147.237.77.216	dover.idf.il		drop	drop	462
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	437
68.180.228.118	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	312
95.86.112.233	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	297
212.179.140.133	Israel	147.237.76.31	nakchal.idf.il	SAM rule	drop	drop	180
84.41.108.220	Slovenia	147.237.72.14	dover.idf.il(old)		drop	drop	179
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence		142
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence	monitor	141
66.249.78.82	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	126
213.151.42.231	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	113
197.8.100.62	Tunisia	147.237.77.216	dover.idf.il		drop	drop	106
84.95.211.33	Israel	147.237.72.166	aka.idf.il		drop	drop	103
188.165.15.187	France	147.237.77.74	law.idf.il	SAM rule	drop	drop	102
192.114.180.34	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	97
66.249.78.109	United States	147.237.72.14	dover.idf.il(old)		drop	drop	94
66.249.78.102	United States	147.237.72.14	dover.idf.il(old)		drop	drop	94
66.249.78.116	United States	147.237.72.14	dover.idf.il(old)		drop	drop	92
77.75.77.17	Czech Republic	147.237.72.14	dover.idf.il(old)		drop	drop	84
192.115.248.2	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	84
197.8.100.62	Tunisia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	66
157.55.39.211	United States	147.237.72.14	dover.idf.il(old)		drop	drop	63
80.215.160.85	France	147.237.72.166	aka.idf.il		drop	drop	63
74.81.89.139	United States	147.237.72.14	dover.idf.il(old)		drop	drop	60
62.90.159.249	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	59
192.114.87.2	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	57
81.218.77.163	Israel	147.237.77.216	dover.idf.il		drop	drop	56
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
208.93.0.48	United States	147.237.72.14	dover.idf.il(old)		drop	drop	55
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		55
212.179.140.133	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	54
212.179.140.133	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	54
213.244.82.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il		drop	drop	52
194.90.105.94	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	52
192.114.87.2	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	51
192.114.180.34	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence		51
109.65.106.193	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	49
46.116.139.166	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	49
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	48
157.55.39.1	United States	147.237.72.14	dover.idf.il(old)		drop	drop	48
109.65.106.193	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence		47
188.143.232.111	Russian Federation	147.237.72.14	dover.idf.il(old)		drop	drop	47
62.219.111.152	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
198.204.249.34	United States	147.237.72.166	aka.idf.il		drop	drop	42
157.55.39.95	United States	147.237.72.14	dover.idf.il(old)		drop	drop	42
23.236.125.249	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	41
197.8.196.178	Tunisia	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
197.8.100.62	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	2658
2.54.32.19	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.32.19	Block	661
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	521
2.54.130.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	346
38.111.147.84	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	322
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	314
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	298
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.43.210.235	Block	272
176.12.137.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
109.253.135.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
207.241.226.64	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	148
176.12.143.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
38.111.147.84	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	130
176.12.145.32	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.32	Block	119
176.12.150.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	111
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 5.43.210.235	Block	104
5.43.210.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	98
176.12.138.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
88.95.57.26	Norway	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	91
66.249.79.73	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//edim/yoman/enlarge.asp	Block	79
95.86.82.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	78
80.246.136.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.220	Block	70
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	70
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	65
66.249.79.81	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//edim/yoman/enlarge.asp	Block	65
176.12.144.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
88.95.57.26	Norway	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 88.95.57.26	Block	63
109.253.146.155	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.146.155	Block	62
95.86.119.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	62
176.12.144.17	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.144.17	Block	60
66.249.79.65	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//edim/yoman/enlarge.asp	Block	60
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	59
176.12.148.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
95.86.69.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	44
176.12.142.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	39
213.151.43.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	36
198.24.146.194	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/994-8613-he/navy.aspx.aspx	Block	36
81.218.68.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	35
93.173.7.27	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	33
212.150.112.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	30
82.102.141.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	28
77.125.7.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	25
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	24
132.70.66.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	24
85.250.125.120	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.125.120	Block	23
46.117.57.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	22
188.143.232.111	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.111	Block	22
74.6.254.141	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/.vjcxuyusv8e	Block	21