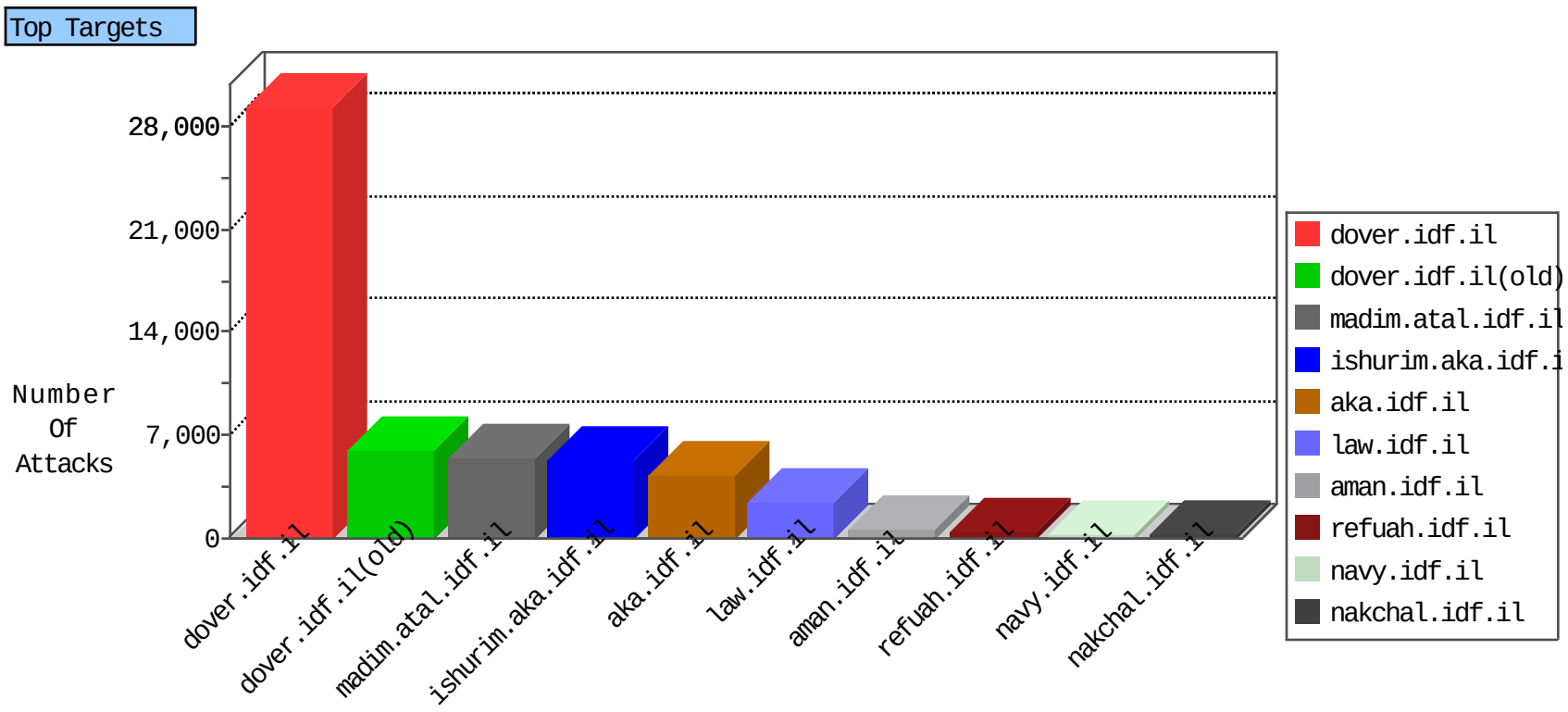
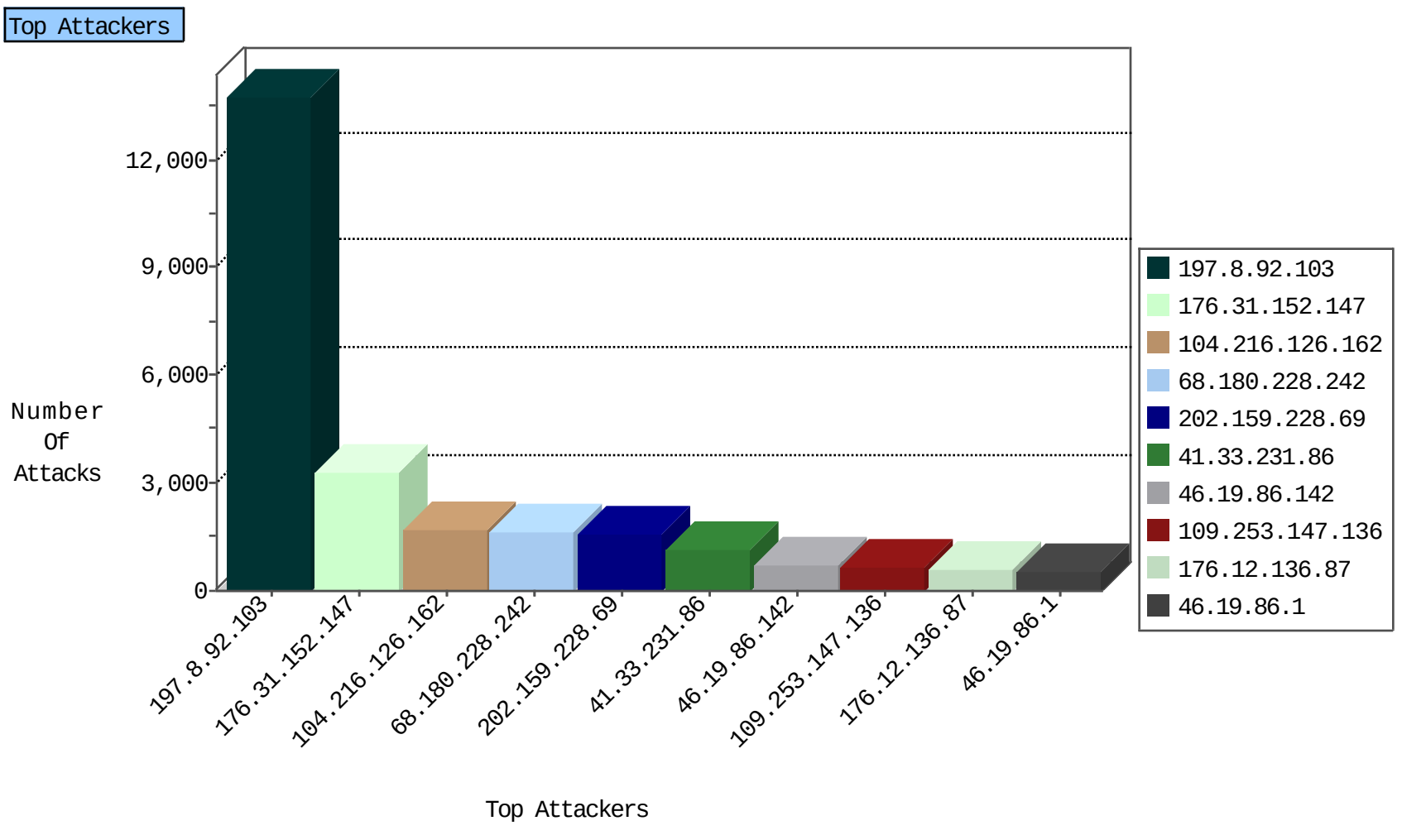
12-23-2014-00:00:00 to 12-24-2014-00:00:00

IDF Under Attack
Daily Report





12-23-2014-00:00:00 to 12-24-2014-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
99.59.38.233	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	214537
65.128.50.218	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	129982
50.151.250.99	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	115414
77.247.178.126	Netherlands	147.237.76.30	himush.idf.il	TCP handshake violation, first packet not syn	drop	111049
188.25.63.15	Romania	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	65908
212.78.197.210	Netherlands	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	65440
65.183.150.93	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	60952
72.229.242.240	United States	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	49150
64.235.150.197	United States	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	32424
77.247.178.126	Netherlands	147.237.76.31	nakchal.idf.il	TCP handshake violation, first packet not syn	drop	31610
203.87.77.94	Australia	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	19391
74.65.201.178	United States	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	17123
77.247.178.126	Netherlands	147.237.76.200	eitan.aka.idf.il	TCP handshake violation, first packet not syn	drop	9628
68.180.228.117	United States	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	7728
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7004
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	606
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	556
176.31.152.147	France	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	459
92.241.47.112	Jordan	147.237.77.216	dover.idf.il	HTTP-MISC-DosTool-SlowHeader	forward	336
176.31.152.147	France	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	309
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	306
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	202
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	160
82.102.141.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	150
132.64.67.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	108
104.216.126.162		147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	102
84.108.106.123	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	95
212.199.236.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	91
46.116.81.57	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
82.102.141.197	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
92.241.47.112	Jordan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	68
190.27.248.162	Colombia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	44
82.102.141.216	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	24
82.102.141.193	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	22
92.241.47.112	Jordan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	18
82.102.141.198	Israel	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	16
82.102.141.217	Israel	147.237.77.243	mobile.idf.il	Invalid TCP Flags	drop	15
82.102.141.199	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	11
82.102.141.216	Israel	147.237.77.243	mobile.idf.il	Invalid TCP Flags	drop	8
82.102.141.204	Israel	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	8
82.102.141.200	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	7
82.102.141.195	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	6
76.114.183.28	United States	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	6
82.102.141.197	Israel	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	5
66.249.64.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4
82.102.141.215	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4
82.102.141.197	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4
82.102.141.210	Israel	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	4
82.102.141.223	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4

12-23-2014-00:00:00 to 12-24-2014-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.69.187	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	89
66.249.75.131	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	81
66.249.75.115	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	80
66.249.75.147	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	61
132.72.138.1	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	56
66.249.69.155	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	52
66.249.69.171	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	39
66.249.75.133	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	19
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
82.81.193.82	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	17
66.249.75.117	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	16
207.46.13.70	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	15
84.94.182.136	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	13
66.249.75.101	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	13
77.125.92.58	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	13
212.179.46.20	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	13
188.165.15.98	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	12
188.165.15.235	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
188.165.15.240	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
188.165.15.90	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
207.46.13.79	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
157.55.39.162	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
207.46.13.108	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	11
188.165.15.193	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	10
94.178.50.225	Ukraine	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
87.69.36.196	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	10
5.29.213.164	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
188.165.15.64	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
109.65.60.130	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
188.165.15.202	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	9
207.46.13.48	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
157.55.39.79	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
212.179.21.194	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
188.165.15.198	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
199.203.63.126	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
87.68.48.78	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
188.165.15.127	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	8
188.165.15.29	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.228.140.43	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
68.180.228.118	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
37.26.147.180	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
188.165.15.231	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
188.165.15.13	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	7
87.68.63.163	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.165.15.233	France	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6
192.118.30.102	Israel	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
68.180.229.36	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6
157.55.39.181	United States	147.237.77.74	law.idf.il	C1000157: HTTP: Access to GetFile.aspx	Block	6

12-23-2014-00:00:00 to 12-24-2014-00:00:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	132
185.32.179.118	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
82.221.102.193	Iceland	147.237.0.19	madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	11
109.186.72.37	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
190.27.248.162	Colombia	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	7
5.135.144.86	France	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	5
62.152.27.30	Cyprus	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	4
202.159.228.69	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
107.167.110.60	United States	147.237.72.156	aman.idf.il	Tehila - Perl LWP with fake user agent	4
2.54.154.176	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
208.80.155.189	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	3
200.168.14.181	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
109.253.147.136	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.177.111.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.50.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.157.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.20.242	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.44.131.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.116	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
79.183.101.170	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.181.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.233.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.118	United Kingdom	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.253.147.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.160.224.128	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
134.191.232.70	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.155.65	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.174.93.106	Netherlands	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
212.38.181.118	United Kingdom	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
212.38.181.118	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
212.38.181.116	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.19.86.168	Israel	147.237.72.166	aka.idf.il	ET DOS SSL Bomb DoS Attempt	2
212.38.181.116	United Kingdom	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.160.224.128	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
37.60.46.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
189.15.197.135	Brazil	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
46.19.85.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.160.224.128	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
46.120.211.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.136.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.135.111.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.152.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.116	United Kingdom	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.12.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.116	United Kingdom	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
77.127.113.107	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
5.29.161.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.118	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2

12-23-2014-00:00:00 to 12-24-2014-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.8.92.103	Tunisia	147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP protocol name in request	Block HTTP Non Compliant	monitor	3431
202.159.228.69	India	147.237.77.216	dover.idf.il		drop	drop	1530
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)		drop	drop	1346
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1119
68.180.228.118	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	484
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	442
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	439
188.165.15.13	France	147.237.77.74	law.idf.il	SAM rule	drop	drop	383
190.27.248.162	Colombia	147.237.77.216	dover.idf.il		drop	drop	371
62.152.27.30	Cyprus	147.237.77.216	dover.idf.il		drop	drop	309
200.168.14.181	Brazil	147.237.77.216	dover.idf.il		drop	drop	304
66.249.69.155	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	264
92.241.47.112	Jordan	147.237.77.216	dover.idf.il		drop	drop	234
66.249.69.171	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	220
176.31.152.147	France	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	203
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Invalid HTTP End Of Line in request	Block HTTP Non Compliant	monitor	187
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Illegal start l in request	Block HTTP Non Compliant	monitor	165
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence	monitor	149
68.180.228.242	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence		147
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	141
213.151.38.209	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	139
104.216.126.162		147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	136
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	127
216.155.132.114	United States	147.237.77.216	dover.idf.il		drop	drop	125
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Invalid HTTP End Of Line in request	Block HTTP Non Compliant	monitor	122
132.64.205.145	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	107
87.69.225.64	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	84
157.55.39.1	United States	147.237.72.14	dover.idf.il(old)		drop	drop	82
46.236.24.52	United Kingdom	147.237.72.14	dover.idf.il(old)		drop	drop	81
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Illegal start l in request	Block HTTP Non Compliant	monitor	80
168.235.195.98		147.237.72.166	aka.idf.il		drop	drop	80
195.230.4.43	Bulgaria	147.237.77.216	dover.idf.il		drop	drop	79
79.178.199.106	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
192.230.140.109	United States	147.237.77.216	dover.idf.il		drop	drop	78
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP protocol name in request	Block HTTP Non Compliant	monitor	77
194.90.134.253	Israel	147.237.77.216	dover.idf.il		drop	drop	75
157.55.39.84	United States	147.237.72.14	dover.idf.il(old)		drop	drop	72
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	71
87.69.225.64	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	69
157.55.39.67	United States	147.237.72.14	dover.idf.il(old)		drop	drop	66
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP protocol name in request	Block HTTP Non Compliant	monitor	62
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	60
190.128.143.82	Paraguay	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	60
157.55.39.152	United States	147.237.72.14	dover.idf.il(old)		drop	drop	60
46.118.112.49	Ukraine	147.237.72.14	dover.idf.il(old)		drop	drop	59
82.102.141.221	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	59
5.22.129.198	Israel	147.237.72.167	ishurim.aka.idf.i		drop	drop	59
213.151.42.231	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	54
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	illegal header format detected: Invalid HTTP End Of Line in request	Block HTTP Non Compliant	monitor	54
78.154.170.6	Ukraine	147.237.72.14	dover.idf.il(old)		drop	drop	53

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
197.8.92.103	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	3431
197.8.92.103	Tunisia	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	3431
197.8.92.103	Tunisia	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	3431
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	705
109.253.147.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	665
176.12.136.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	586
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	543
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	422
84.228.36.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	391
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	366
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	339
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	314
46.116.81.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	299
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	289
84.108.31.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	275
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.216	Block	263
80.246.141.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	247
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	239
80.246.139.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	218
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	199
185.32.179.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	176
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	154
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	151
109.253.145.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	150
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Abnormally Long Header Line	Block	141
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	128
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	127
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.254	Block	123
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	110
176.31.152.147	France	147.237.77.216	dover.idf.il	Distributed Malformed HTTP Header Line	Block	110
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	95
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	91
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	90
82.102.141.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
2.54.164.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	70
66.249.78.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.160	Block	62
66.249.78.153	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	58
162.248.48.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	57
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	56
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	54
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Abnormally Long Header Line	Block	53
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	48
207.241.226.130	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	44
77.125.99.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	43
80.246.133.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	42
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	42
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	40