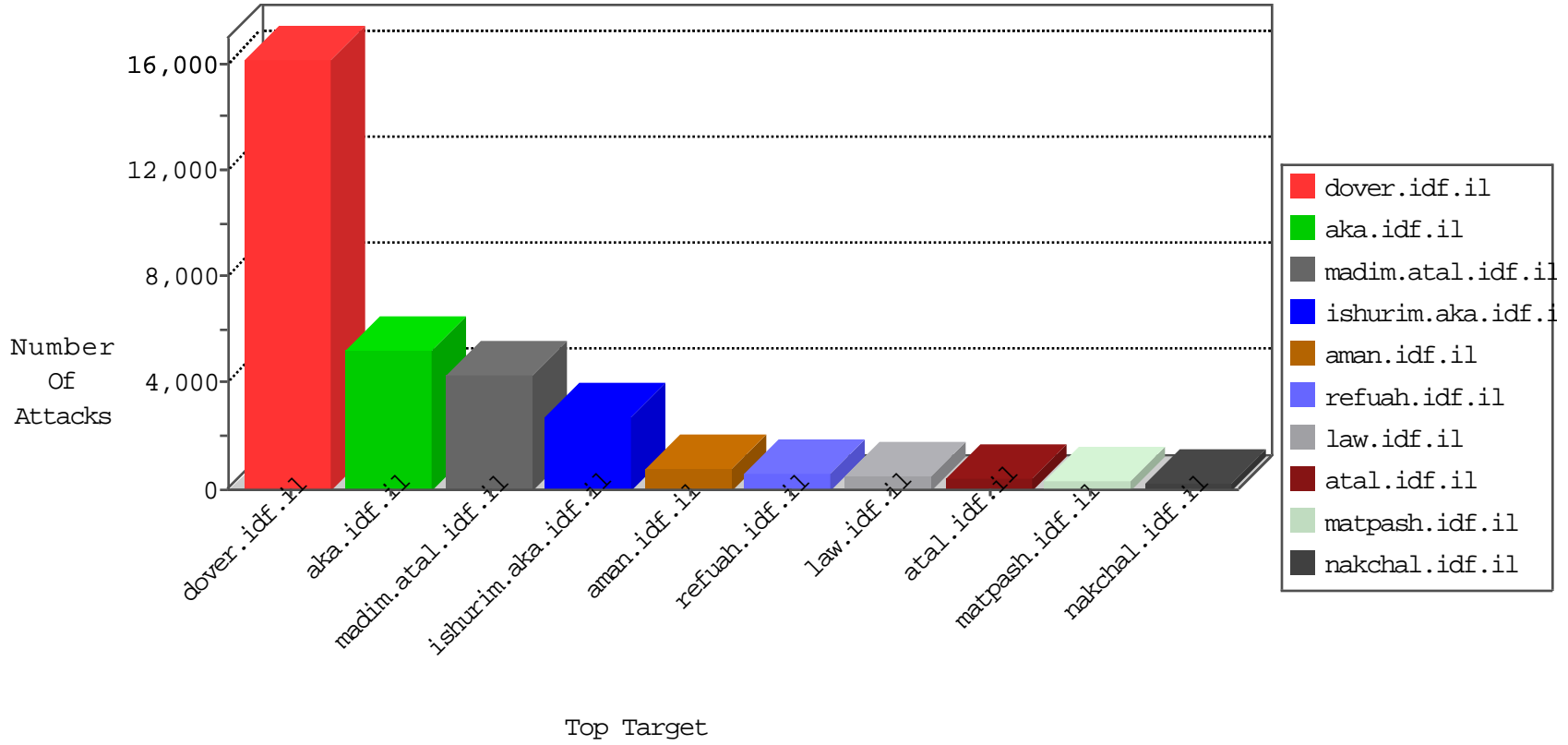


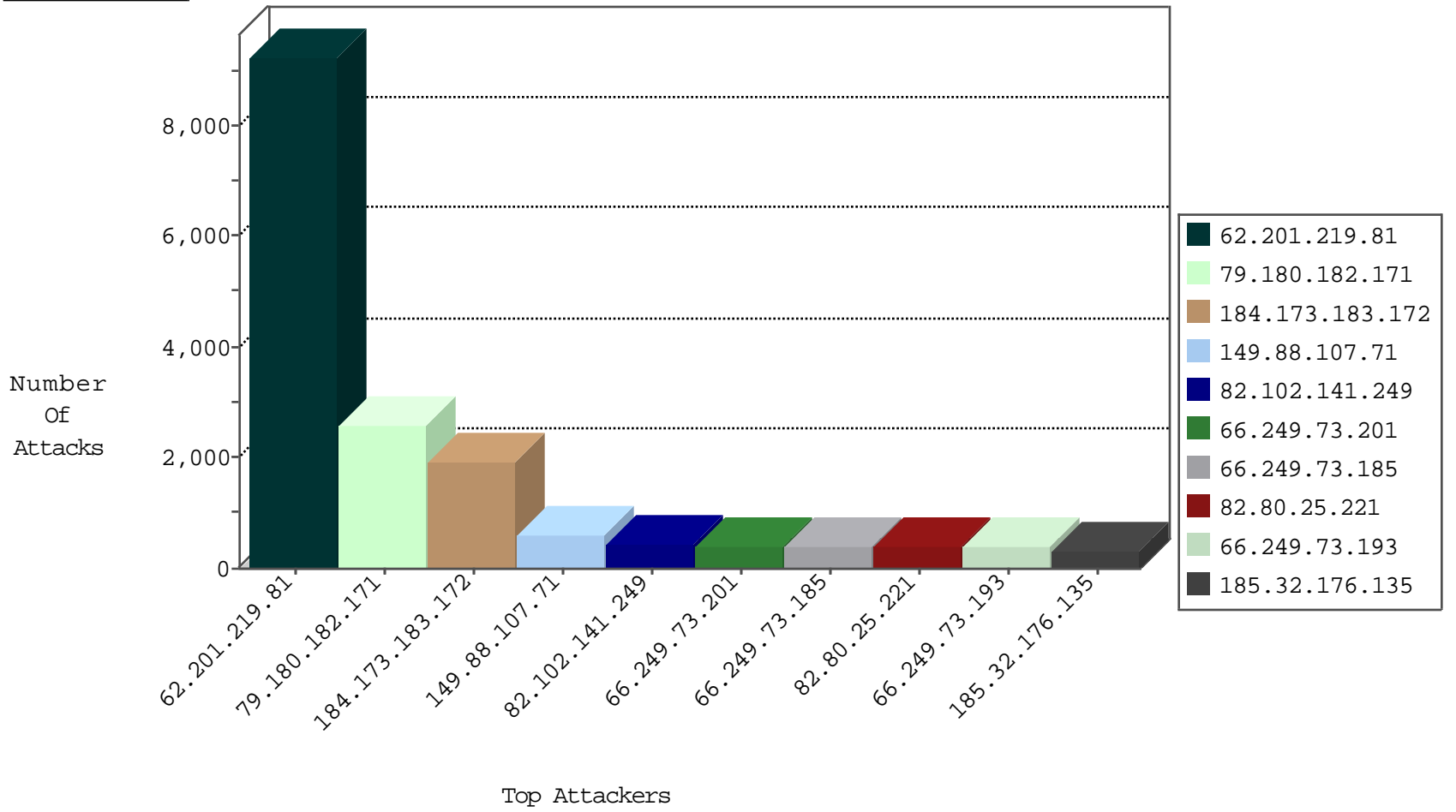
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	31985
66.249.67.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	28953
66.249.79.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	27787
66.249.79.42	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	27528
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	19534
66.249.81.156	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	15414
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	14478
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	14084
66.249.93.191	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12429
66.249.79.138	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10836
66.249.67.108	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9658
82.145.220.193	Europe	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9386
66.249.67.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8907
66.249.79.34	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8397
66.249.81.164	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	6967
66.249.81.179	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6777
66.249.83.251	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6726
66.249.81.184	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6376
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6196
66.249.81.168	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4187
46.217.122.182	Macedonia, the Former Yugoslav Republic of	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3877
66.249.78.147	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	3687
66.249.79.157	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3473
66.249.81.212	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3239
66.249.64.6	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2963
66.249.81.209	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2326
66.249.78.74	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2102
108.171.128.166	United Kingdom	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1974
66.249.79.5	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1897
194.78.243.137	Belgium	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1864
31.186.228.26	United Kingdom	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1805
66.249.64.183	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1759
207.46.13.129	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1736
66.249.78.242	United States	147.237.0.17	m.my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1695
66.249.81.240	United States	147.237.0.17	m.my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1502
149.78.167.6	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	1015
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1014
66.249.64.10	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	812
72.14.199.124	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	798
66.102.6.253	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	783
66.249.81.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	728
66.249.78.79	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	708
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	644
79.178.151.140	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	522
79.181.30.204	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	279
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	233
149.78.202.125	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Client	dest-reset	209
95.86.127.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	199
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	186
5.29.180.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	184

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	1053
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	265
79.180.182.171	Israel	147.237.72.166	aka.idf.il	C091: HTTP: Access to - admin.asp	Block	244
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	206
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	192
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	164
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	124
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	68
212.143.3.44	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	42
85.250.128.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	27
194.90.176.233	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
79.180.182.171	Israel	147.237.72.166	aka.idf.il	C023: HTTP: administrator in URI	Permit	17
194.177.16.3	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
109.186.184.53	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.62	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.216.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.180.182.171	Israel	147.237.72.166	aka.idf.il	C003: HTTP: phpMyAdmin access	Block	6
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	6
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
93.42.3.54	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.100.2	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
110.148.113.203	Australia	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.177.15.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.205	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
93.172.165.214	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.143	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
109.64.199.65	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
85.130.133.122	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.39	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
60.241.77.198	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
79.177.24.107	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	3
212.143.43.173	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
79.180.182.171	Israel	147.237.72.166	aka.idf.il	Admin login page scan - Haviij	191
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	108
79.180.182.171	Israel	147.237.72.166	aka.idf.il	SERVER-WEBAPP adminlogin access	31
46.19.86.88	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
79.180.182.171	Israel	147.237.72.166	aka.idf.il	SERVER-WEBAPP admin.php access	23
79.180.182.171	Israel	147.237.72.166	aka.idf.il	SERVER-WEBAPP login.htm access	11
81.218.155.10	Israel	147.237.76.31	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
66.249.81.188	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	7
77.127.226.24	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	6
109.67.11.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
36.81.87.23	Indonesia	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
109.64.132.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
93.173.33.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
115.28.48.188	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
89.234.68.87	Ireland	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
194.90.37.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.33.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.188.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.75.118	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.118.68	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
151.80.88.241	Italy	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
115.28.48.188	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
50.250.226.178	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
115.28.48.188	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
46.121.119.239	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.110.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
109.66.62.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
194.90.254.244	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.192.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.234.68.85	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
46.116.247.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.179.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
122.228.207.77	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
46.105.100.54	France	147.237.76.42	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.143.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.105.100.54	France	147.237.76.42	refuah.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
62.201.219.81	Iraq	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
115.28.48.188	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
192.114.86.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.28.48.188	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
85.64.202.4	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.48.209	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
62.201.219.81	Iraq	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8792
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	385
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	342
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	332
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	324
85.130.242.114	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	240
109.67.143.62	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	185
109.67.14.153	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	111
69.41.14.215	United States	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	88
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
109.253.144.145	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
76.109.47.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
69.41.14.158	United States	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	57
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
46.19.86.108	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	53
77.171.50.176	Netherlands	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
46.19.85.28	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	49
82.102.141.221	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
5.102.254.93	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	47
132.66.23.62	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	46
132.3.21.78	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
79.181.51.121	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
31.168.69.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
46.19.85.32	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	43
132.76.50.6	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
166.192.122.85	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
195.77.90.138	Spain	147.237.72.166	aka.idf.il	SAM rule	drop	drop	40
62.90.110.122	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
176.12.151.201	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
176.12.137.191	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
97.88.212.188	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
83.130.114.76	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.147.110	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.65.173.121	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	32
109.253.131.62	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.137.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.145.84	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
94.118.96.3	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.39	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
79.180.182.171	Israel	147.237.72.156	aman.idf.il	SAM rule	drop	drop	30
109.253.157.59	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
79.180.182.171	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	30
80.178.146.194	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
79.176.132.235	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
93.172.208.235	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	28
216.239.45.74	United States	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.182.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.182.171	Block	1063
149.88.107.71	United States	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.107.71	Block	589
79.180.182.171	Israel	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 79.180.182.171	Block	533
79.180.182.171	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	391
82.102.141.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	378
185.32.176.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	281
77.127.189.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	230
62.201.219.81	Iraq	147.237.77.216	dover.idf.il	Multiple Malformed URL from 62.201.219.81	Block	221
62.201.219.81	Iraq	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 62.201.219.81	Block	221
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	197
2.54.134.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
109.253.157.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	145
2.54.42.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
109.253.132.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	108
176.12.151.132	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.151.132	Block	106
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
82.102.141.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
109.253.132.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
109.253.134.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
109.253.132.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
109.253.131.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
109.253.138.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	62
109.253.139.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.138.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	55
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	54
80.246.138.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
37.26.147.162	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.162	Block	52
50.75.153.195	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.75.153.195	Block	49
109.253.142.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
109.253.147.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
176.12.146.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
109.253.157.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
176.12.141.18	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.141.18	Block	35
79.181.126.107	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	31
2.54.190.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	26
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	25
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	24
89.138.67.62	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 89.138.67.62	Block	24
109.253.128.97	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.128.97	Block	23
37.142.100.31	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	21
79.181.51.121	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	18
87.69.87.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	17
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	16
80.178.138.130	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	14