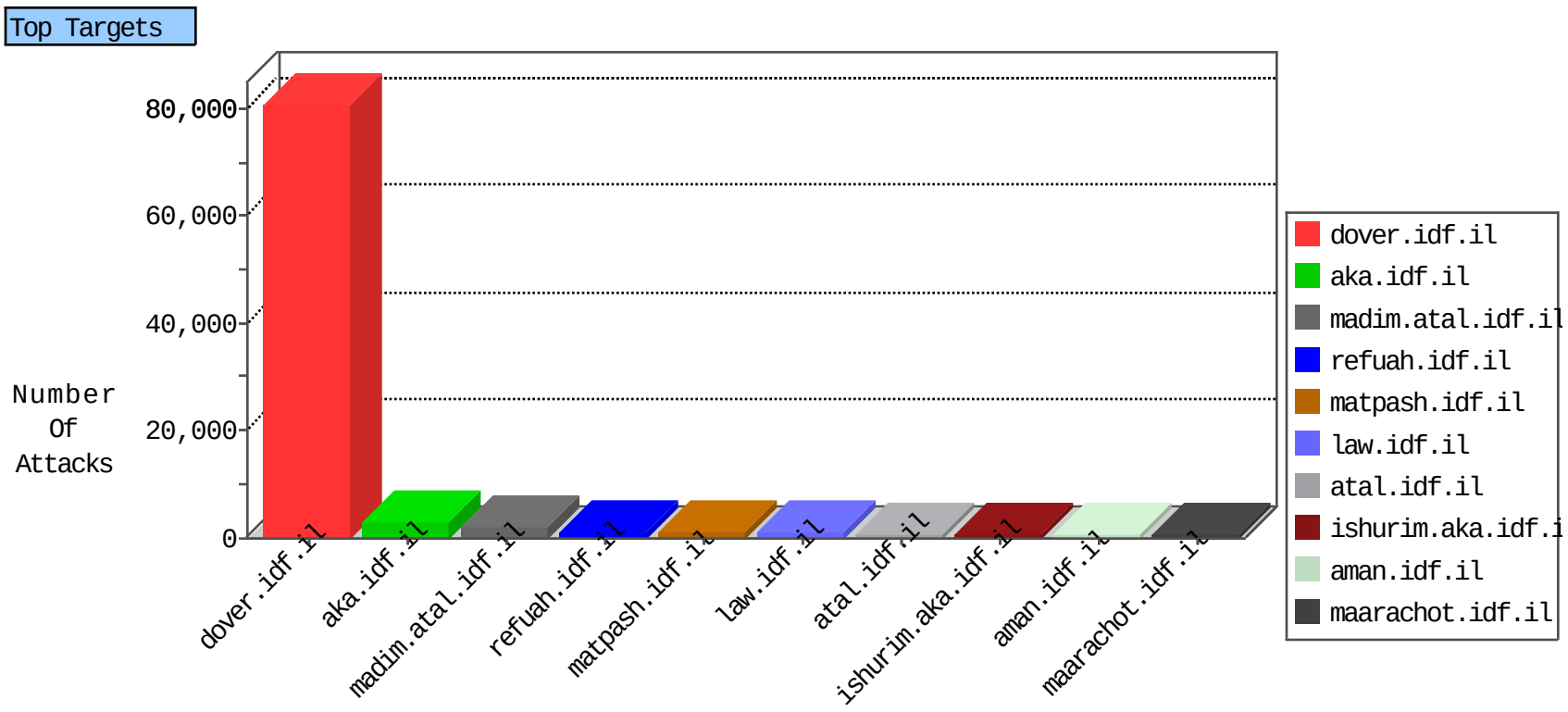
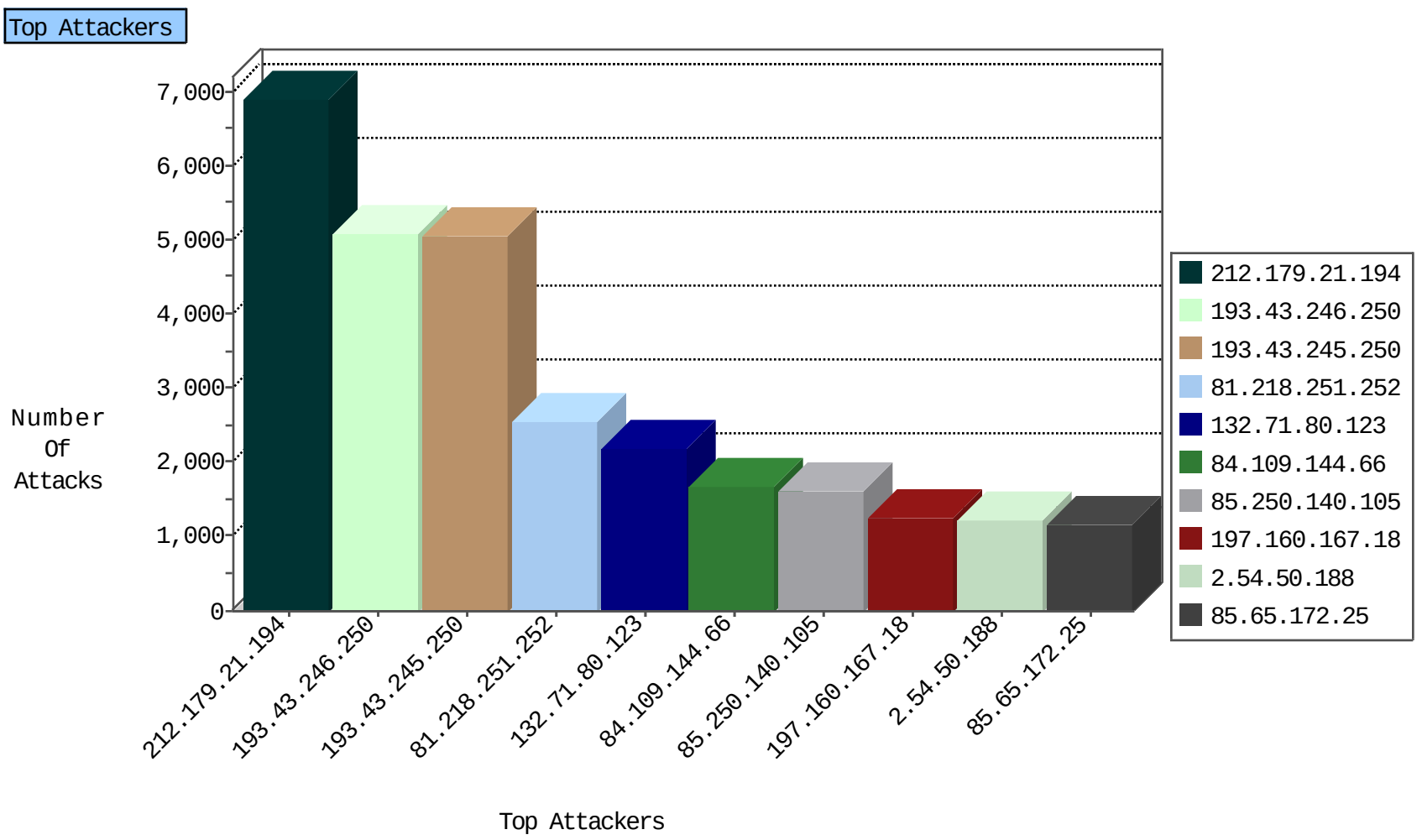
06-14-2015-00:00:01 to 06-15-2015-00:00:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



06-14-2015-00:00:01 to 06-15-2015-00:00:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3330
79.177.123.218	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2974
5.29.200.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2648
212.179.246.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1897
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1530
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1338
66.249.64.224	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	693
109.64.9.167	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	570
77.125.73.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	544
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	541
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	406
213.57.186.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	390
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	372
220.181.108.122	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	348
77.125.117.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	336
46.117.174.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	322
212.143.186.38	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	317
5.29.171.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	293
79.181.57.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	282
220.181.108.171	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	277
212.143.186.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	224
5.29.197.230	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
31.210.180.155	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	180
2.52.57.100	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
46.116.130.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
220.181.108.162	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	149
213.57.46.100	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
84.110.86.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
94.159.151.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
213.57.105.37	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	131
80.178.194.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
192.54.144.229	France	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	125
87.68.217.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
79.182.224.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
2.54.134.163	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
147.235.236.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
79.183.103.203	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	94
80.12.35.164	France	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
85.65.139.9	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
109.65.17.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
37.142.3.112	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.120.104.229	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
79.182.254.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
79.178.20.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
109.64.234.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
94.159.208.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
132.65.44.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
149.78.48.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80

06-14-2015-00:00:01 to 06-15-2015-00:00:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.59.19.32	France	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	292
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	287
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	256
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	152
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	106
199.203.53.3	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	90
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	48
118.193.200.137	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
205.134.224.235	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	30
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	26
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
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	9
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	7
79.177.123.218	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
94.230.89.81	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	6
212.199.218.50	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
91.230.121.131	Ukraine	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
104.236.231.233		147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	5
46.19.85.235	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
82.80.31.234	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.181.21.61	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4

06-14-2015-00:00:01 to 06-15-2015-00:00:01

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	99
2.52.184.5	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	95
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	59
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	59
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	56
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	55
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	55
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	55
2.52.34.82	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	55
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	40
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	34
46.19.85.72	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
37.8.87.236	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	22
209.66.70.253	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	17
209.66.70.253	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	9
197.160.167.18	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI	7
212.161.5.178	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	7
191.190.88.199	Brazil	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
41.225.226.46	Tunisia	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
66.249.64.112	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
84.21.142.230	United Kingdom	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.29	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.130	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.130	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
199.203.59.121	Israel	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
178.89.191.77	Kazakstan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
161.69.31.20	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.132	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
66.249.65.51	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2

06-14-2015-00:00:01 to 06-15-2015-00:00:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6734
193.43.246.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5072
193.43.245.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5052
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2526
132.71.80.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2203
84.109.144.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1690
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1561
2.54.50.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1181
85.65.172.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1153
213.151.54.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1085
91.197.46.32	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1070
168.235.196.199		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	942
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	804
109.160.219.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	774
2.54.184.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	739
109.67.115.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	727
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	678
95.86.123.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	615
82.145.208.93	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	554
95.86.116.223	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	525
82.166.131.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	494
197.160.167.18	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	491
213.151.60.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	469
98.201.70.129	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	440
46.120.104.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	394
73.128.9.242	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	393
95.86.96.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	382
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	372
79.177.109.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	369
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	356
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	342
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
91.230.26.130	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	300
85.250.189.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	298
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	296
46.210.193.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	283
109.110.118.146	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
46.19.86.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	242
37.220.234.251	Hungary	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	240
85.64.206.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
84.229.183.119	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	223
93.173.152.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	183
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	173
46.19.86.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	172
93.37.19.180	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	154
2.54.137.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	152

06-14-2015-00:00:01 to 06-15-2015-00:00:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.49.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.49.6	Block	471
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.117	Block	388
176.12.148.106	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.106	Block	350
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	263
109.253.143.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
183.60.243.190	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 183.60.243.190	Block	148
109.253.157.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	145
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.161	Block	100
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.84	Block	99
109.253.149.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
176.12.136.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	39
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
183.60.243.190	China	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 183.60.243.190	Block	27
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
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
5.102.105.187	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	22
79.182.225.37	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	18
183.60.243.190	China	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	18
95.86.121.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	17
109.253.136.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	16
5.29.78.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
195.95.183.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
109.253.129.186	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	15
212.199.142.58	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	14
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.89	Block	14
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
46.116.178.88	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	13
77.125.215.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
200.53.156.172	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
95.86.124.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
79.177.123.62	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	12
2.54.18.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
85.250.200.1	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.250.200.1	Block	10
81.218.21.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
77.125.107.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	9
5.144.57.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
79.179.102.123	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
2.54.30.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
37.26.147.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
46.19.86.99	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.99	Block	8
164.138.116.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
94.230.86.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
31.204.128.94	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 31.204.128.94	Block	7
164.138.114.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	7
87.69.171.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
213.57.14.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.182.121.184	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	7

06-14-2015-00:00:01 to 06-15-2015-00:00:01