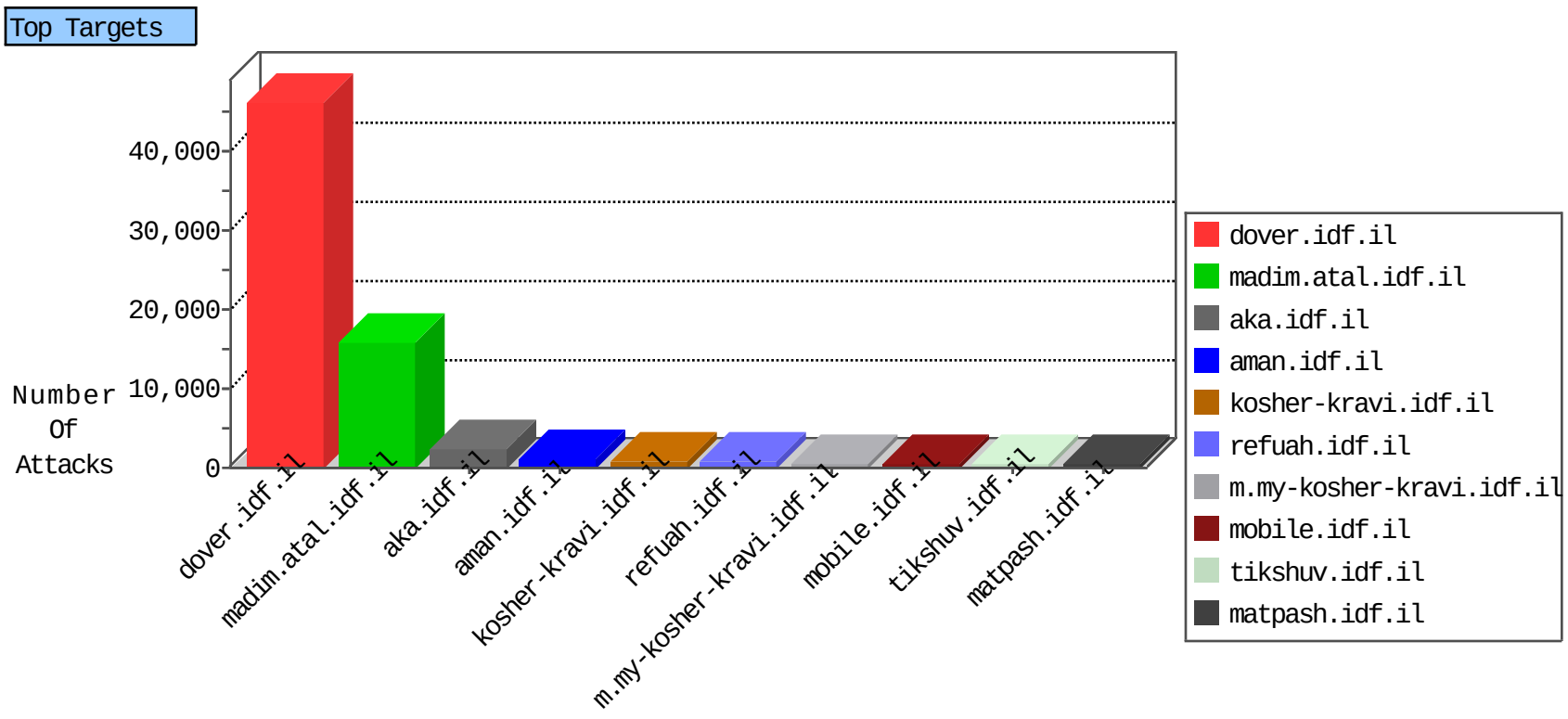
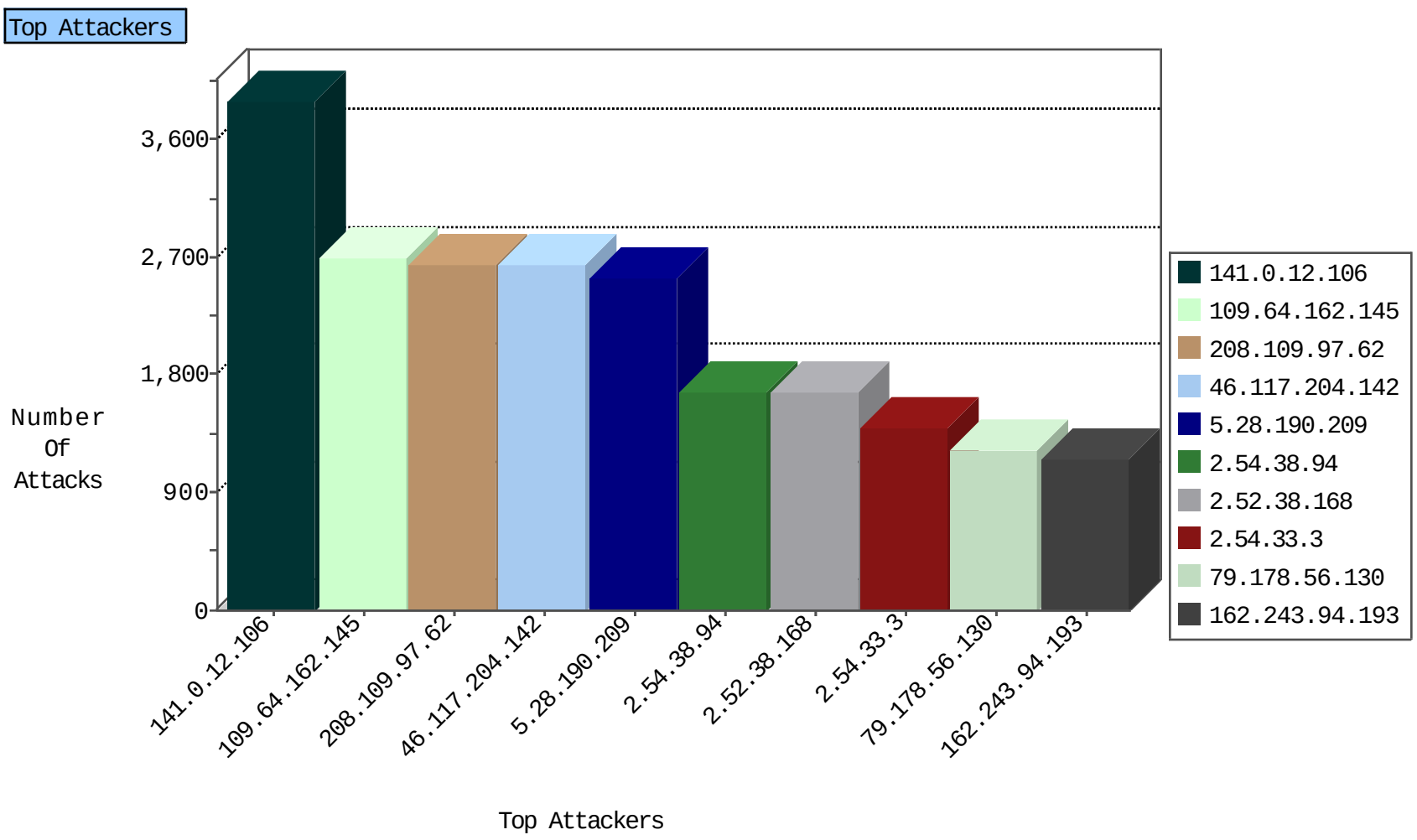
08-29-2015-00:00:03 to 08-30-2015-00:00:03

IDF Under Attack Daily Report





08-29-2015-00:00:03 to 08-30-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
5.109.102.52	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	63600
66.249.64.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20428
66.249.64.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19339
78.146.30.87	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	13501
176.223.83.64	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11077
188.132.72.167	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11026
95.128.56.36	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9101
176.223.85.133	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5107
37.231.31.177	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	915
109.64.71.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	776
66.249.64.148	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	630
141.0.12.106	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	471
85.64.240.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	399
37.142.255.22	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
82.166.23.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
79.178.56.130	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
213.57.159.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
79.178.182.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	185
46.19.85.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
85.64.66.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.29.5.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
93.173.191.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
46.120.84.148	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
86.111.149.198	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	125
82.166.23.54	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
5.29.86.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
62.219.126.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
176.106.227.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81
220.181.108.122	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	79
85.65.112.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
109.67.55.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
185.44.195.252	Turkey	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	52
2.54.53.30	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	50
46.117.109.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	44
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	34
84.94.178.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
46.210.162.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
109.64.56.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
2.54.53.30	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
141.0.12.106	Norway	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	14
173.32.5.152	Canada	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	14
5.22.129.0	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.168.14.111		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
12.51.210.253	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
82.145.209.32	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
5.22.129.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
154.121.5.234		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
99.101.65.118	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
46.19.86.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6

08-29-2015-00:00:03 to 08-30-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.66.163.23	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	40
46.116.41.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	36
85.250.7.96	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	27
103.224.249.239	Hong Kong	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
46.120.90.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	23
85.65.244.126	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	23
77.127.109.147	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	20
213.57.237.15	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	20
31.154.92.189	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	19
46.116.103.106	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	18
79.183.21.173	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	18
5.22.129.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	17
84.228.132.126	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	17
82.166.23.32	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	17
84.109.49.172	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	16
84.108.71.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	15
109.64.123.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	15
109.66.195.83	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	15
109.64.51.92	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	14
212.199.107.106	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
149.88.215.215	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
149.78.22.51	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
213.57.187.124	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
31.168.172.138	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
95.185.66.50	Romania	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
85.64.157.242	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	13
87.69.81.159	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
149.88.190.178	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
79.179.17.27	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
85.65.48.47	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
79.178.142.135	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
103.224.249.239	Hong Kong	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
5.22.129.173	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
79.180.204.88	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
31.154.92.6	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
109.186.166.40	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
79.177.5.65	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
79.182.225.37	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
109.66.192.147	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
60.241.102.135	Australia	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
149.78.174.204	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
85.64.203.77	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
79.183.107.15	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
46.117.71.251	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
46.19.85.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
27.123.171.53	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
149.78.60.22	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
77.126.237.115	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
185.22.224.96	United Kingdom	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
93.172.75.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7

08-29-2015-00:00:03 to 08-30-2015-00:00:03

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	92
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	40
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	40
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	40
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	35
79.177.213.214	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	16
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	14
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	SQL generic convert injection attempt - GET parameter	12
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	7
82.212.78.168	Jordan	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	5
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
185.44.195.252	Turkey	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	3
185.44.195.252	Turkey	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	3
174.50.38.157	United States	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	3
93.174.93.100	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	3
93.174.93.100	Netherlands	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
83.71.247.34	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
185.44.195.252	Turkey	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	3
185.44.195.252	Turkey	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	3
93.174.93.100	Netherlands	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	3
174.50.38.157	United States	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	3
108.45.93.68	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
59.46.193.114	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	2
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
134.191.232.72	Israel	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
95.106.119.24	Russian Federation	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
218.24.171.223	China	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	2
61.149.161.186	China	147.237.76.199	e.nakchal.idf.il	GPL SCAN nmap TCP	2
198.36.50.80	United States	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
95.106.119.24	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
87.111.128.2	Spain	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
94.102.49.102	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
104.238.177.65		147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
93.174.93.100	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
174.50.38.157	United States	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.168	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
198.36.50.80	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
87.111.128.2	Spain	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.153	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
99.224.176.169	Canada	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
174.50.38.157	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
198.36.50.80	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2

08-29-2015-00:00:03 to 08-30-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
141.0.12.106	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3878
208.109.97.62	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1786
46.19.86.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1125
162.243.94.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1041
90.148.7.34	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	990
85.113.111.57	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	936
62.209.14.202	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	847
82.145.220.240	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	831
208.109.97.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	694
12.51.210.253	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	637
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	580
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	476
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	472
2.54.168.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	453
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	440
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	400
109.186.118.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	395
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	351
5.109.101.230	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	348
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	319
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
188.132.72.167	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	296
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	292
5.108.144.191	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
37.231.216.77	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
46.152.13.17	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	248
37.239.8.99	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	242
31.154.158.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
141.0.15.115	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220
5.255.253.19	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	219
54.244.22.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	197
63.141.217.135	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
37.121.124.137	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
38.111.147.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
46.152.190.223	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
79.178.110.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
37.237.201.10	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	174
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	169
164.138.122.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	166
5.108.128.195	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	166
208.109.97.62	United States	147.237.77.216	dover.idf.il		drop	drop	164
37.231.31.177	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	163
37.231.104.17	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	163
176.223.83.64	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
205.203.135.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
37.231.173.31	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	149
192.0.80.165	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	145
5.102.254.106	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	144

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.162.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2699
46.117.204.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2608
5.28.190.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.190.209	Block	2537
2.54.38.94	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.38.94	Block	1667
2.52.38.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1644
2.54.33.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1398
79.178.56.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.56.130	Block	1200
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.234	Block	570
172.240.89.250	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 172.240.89.250	Block	468
109.253.144.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	336
85.64.0.101	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	311
37.26.146.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	288
203.143.28.33	Sri Lanka	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	228
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	228
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	228
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.188	Block	204
172.240.89.250	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Admin Blocking from 172.240.89.250	Block	156
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	144
192.187.124.251	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	138
109.186.141.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
74.6.254.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 74.6.254.91	Block	102
162.243.94.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.94.193	Block	90
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	84
37.142.219.215	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 37.142.219.215	Block	84
84.228.214.101	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.228.214.101	Block	72
109.253.144.82	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.144.82	Block	66
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	48
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	42
46.120.84.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.84.148	Block	42
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	36
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
46.121.136.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	30
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	30
31.131.16.162	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 31.131.16.162	Block	30
173.208.152.60	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.208.152.60	Block	30
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	24
109.67.34.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.34.62	Block	24
109.253.137.7	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	24
37.26.146.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	24
176.12.136.193	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	24
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	24
77.127.170.117	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	24
79.180.146.142	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	24
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	18
2.52.38.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.38.168	Block	18
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	18
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	18
41.238.221.54	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	18
77.126.237.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	18

08-29-2015-00:00:03 to 08-30-2015-00:00:03