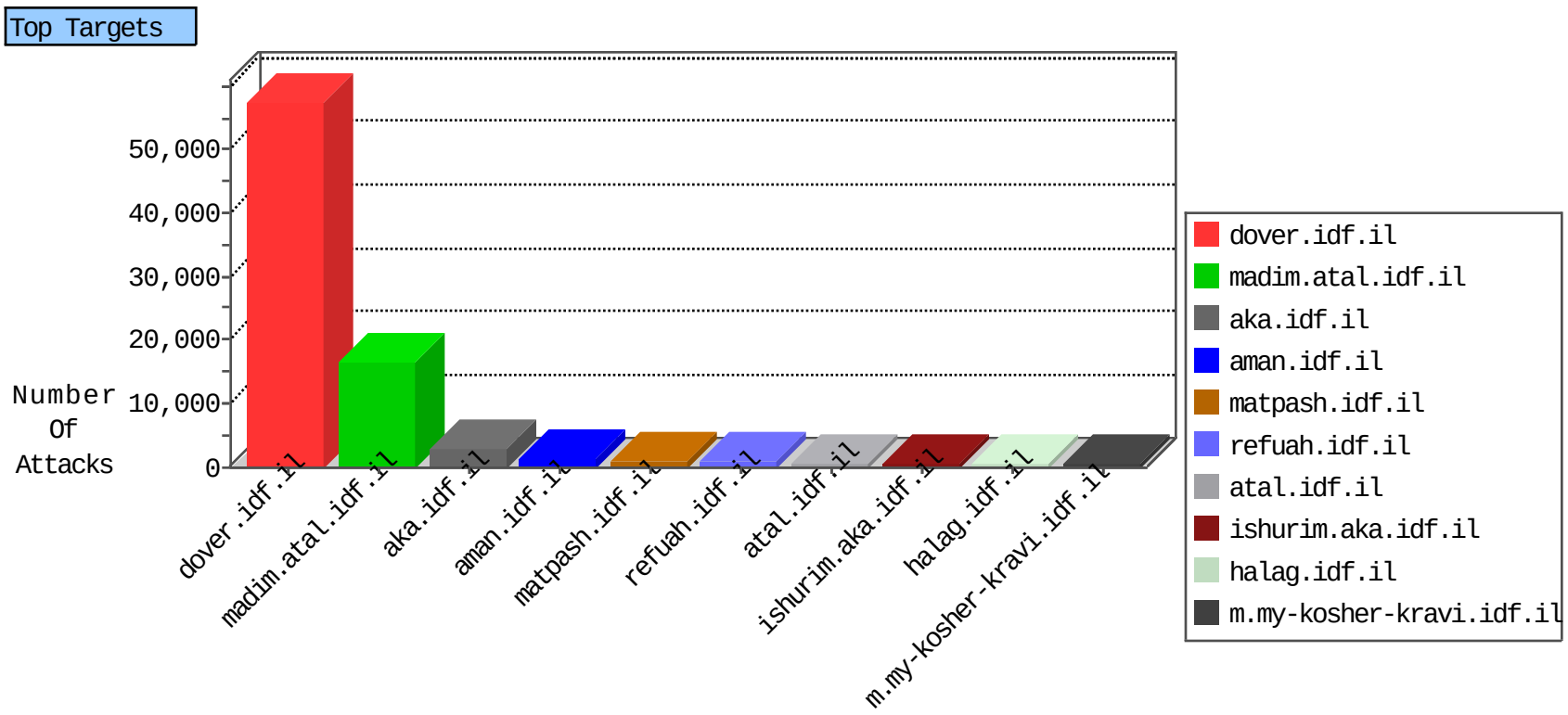
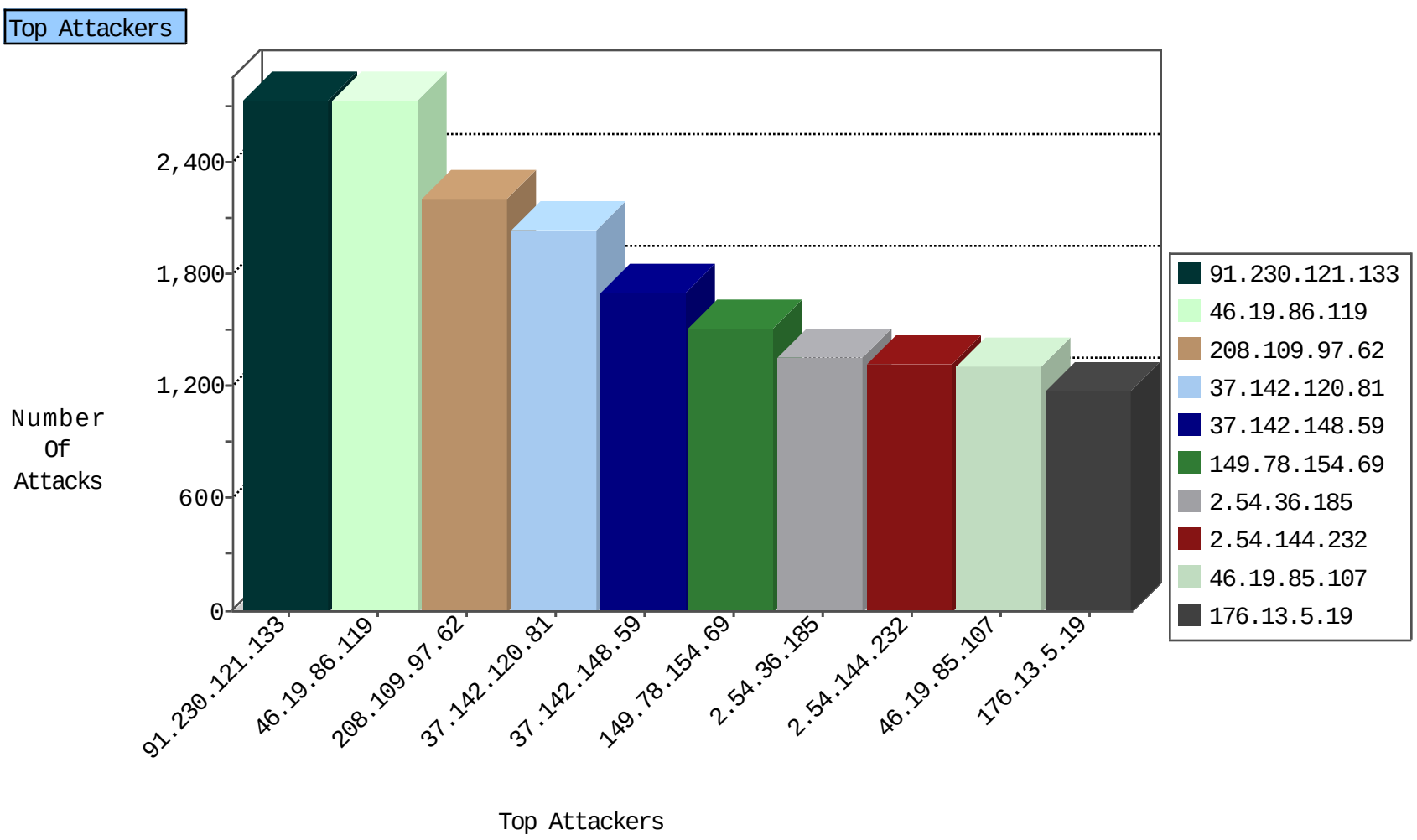
08-17-2015-00:00:05 to 08-18-2015-00:00:05

IDF Under Attack Daily Report





08-17-2015-00:00:05 to 08-18-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4791
66.249.67.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4277
37.48.86.168	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2846
84.109.124.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1194
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	962
148.251.231.197	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	923
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	636
77.126.2.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	621
84.228.102.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	536
149.78.253.225	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	462
109.65.178.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	449
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	449
79.180.202.99	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	342
213.8.241.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	323
79.178.98.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	262
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	260
79.179.51.239	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	254
109.65.108.33	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
192.114.91.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	244
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	243
93.172.51.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
212.179.44.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	235
84.228.248.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
84.229.100.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	209
185.32.179.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	203
85.250.83.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
213.57.209.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
84.111.190.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
109.66.173.117	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
79.183.125.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.102.205.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
84.228.88.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
84.109.190.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
85.130.133.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
5.29.93.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	151
89.138.56.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
2.54.139.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	143
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	139
81.218.51.66	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	138
87.69.17.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
5.29.117.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
46.121.122.15	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	123
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	119
37.26.147.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	116
79.177.203.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
79.182.174.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
87.69.203.130	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
91.227.71.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	96
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92

08-17-2015-00:00:05 to 08-18-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.166.23.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	32
159.253.145.150	United States	147.237.77.233	atal.idf.il	C095: Suspicious Addresses MFA	Permit	29
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
192.151.159.82	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	16
77.127.200.9	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	14
79.181.129.86	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
194.90.178.37	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
37.75.215.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
213.139.52.127	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
2.52.52.179	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
77.125.164.141	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
147.236.238.41	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
84.95.215.113	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
24.191.107.49	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
192.117.113.18	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.228.244.22	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
195.200.205.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.116.113.90	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.178.53.189	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
148.251.231.197	Germany	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	4
158.112.85.164	Norway	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
213.8.115.122	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.127	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
211.59.8.170	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.117.185.14	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
212.117.143.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	3
62.90.144.38	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
197.0.118.0	Tunisia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
123.1.192.208	Hong Kong	147.237.72.166	aka.idf.il	8479: HTTP: Suspicious HTTP Request	Block	3
79.180.55.11	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
109.64.60.69	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
62.219.114.144	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
41.82.61.180	Senegal	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
79.178.22.32	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.181	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	3
46.19.85.185	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
188.161.184.71	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
79.178.143.190	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
212.143.220.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.64.60.69	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
87.117.204.115	United Kingdom	147.237.77.216	dover.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
62.90.255.56	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
2.52.26.26	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
71.146.4.201	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
84.111.30.145	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	2

08-17-2015-00:00:05 to 08-18-2015-00:00:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	398
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	296
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SQL Injection - Select From	143
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	101
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie	98
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	91
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	91
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI	88
37.8.74.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	67
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	64
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	54
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP cart32.exe access	47
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	43
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	40
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER SQL Injection Select Sleep Time Delay	32
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	22
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	19
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	19
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	GPL EXPLOIT .cnf access	18
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-IIS .cnf access	18
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	17
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	16
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	16
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	16
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	16
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	16
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP cat%20 access	14
148.251.231.197	Germany	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	14
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP faxsurvey access	14
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP ndcgi.exe access	13
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	12
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	10
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	9
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	8
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	8
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	8
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP mod-plsql administration access	8
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP mailnews.cgi access	7
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-IIS Directory transversal attempt	6
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP webalizer access	6
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	GPL WEB_SERVER webalizer access	6
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	6
87.117.204.115	United Kingdom	147.237.77.216	dover.idf.il	ET SCAN FHScan core User-Agent Detect	5
66.249.67.23	United States	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	5
148.251.231.197	Germany	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	5
45.114.11.46		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	4
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP /cgi-bin/ access	4
148.251.231.197	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER safe_mode PHP config option in uri	4
148.251.231.197	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER disable_functions PHP config option in uri	4
148.251.231.197	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	4

08-17-2015-00:00:05 to 08-18-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.142.120.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2039
37.142.148.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1702
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1517
208.109.97.62	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1386
2.54.144.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1325
185.4.252.171	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1169
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	848
208.109.97.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	730
2.54.145.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	634
46.19.85.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	566
46.19.86.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	531
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	516
38.111.147.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	503
82.166.22.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	448
70.39.186.125	Satellite Provider	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	446
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	439
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	434
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	432
66.249.67.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	388
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	368
176.13.22.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	366
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	365
66.249.67.59	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	348
149.78.21.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	338
66.249.67.53	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	316
82.80.176.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	316
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
176.13.19.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	292
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	289
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	281
62.201.211.78	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	252
2.54.48.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	241
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
207.46.13.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
141.0.15.184	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
31.154.167.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
207.46.13.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	175
31.154.92.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	175
207.46.13.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	173
76.204.214.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	173
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	164
107.167.108.90	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
85.65.104.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
188.165.15.19	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
148.251.231.197	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
108.24.155.49	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	151
185.13.195.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	150

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2735
2.54.36.185	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.36.185	Block	1352
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1300
176.13.5.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1174
37.26.147.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1143
37.26.149.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	969
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	812
176.13.22.96	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.22.96	Block	770
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	708
2.54.4.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	619
2.54.182.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	583
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	518
2.54.30.69	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.30.69	Block	496
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	444
2.54.173.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	388
176.12.145.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	360
176.13.16.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	356
112.134.179.43	Sri Lanka	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 112.134.179.43	Block	322
2.54.14.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	232
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
2.52.165.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
176.12.139.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.198	Block	198
176.13.22.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	124
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	112
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	68
176.12.138.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.112.144	Block	64
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	64
79.179.61.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	44
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	36
148.251.231.197	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.231.197	Block	36
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	32
81.17.16.253	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	28
2.54.15.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
176.13.7.166	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	28
213.139.52.127	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	20
46.117.217.214	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	20
213.139.52.127	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	20
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (403)	Block	20
85.64.81.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.81.58	Block	20
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
176.13.10.173	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	20
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	20
85.64.81.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	20
109.65.54.112	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	20