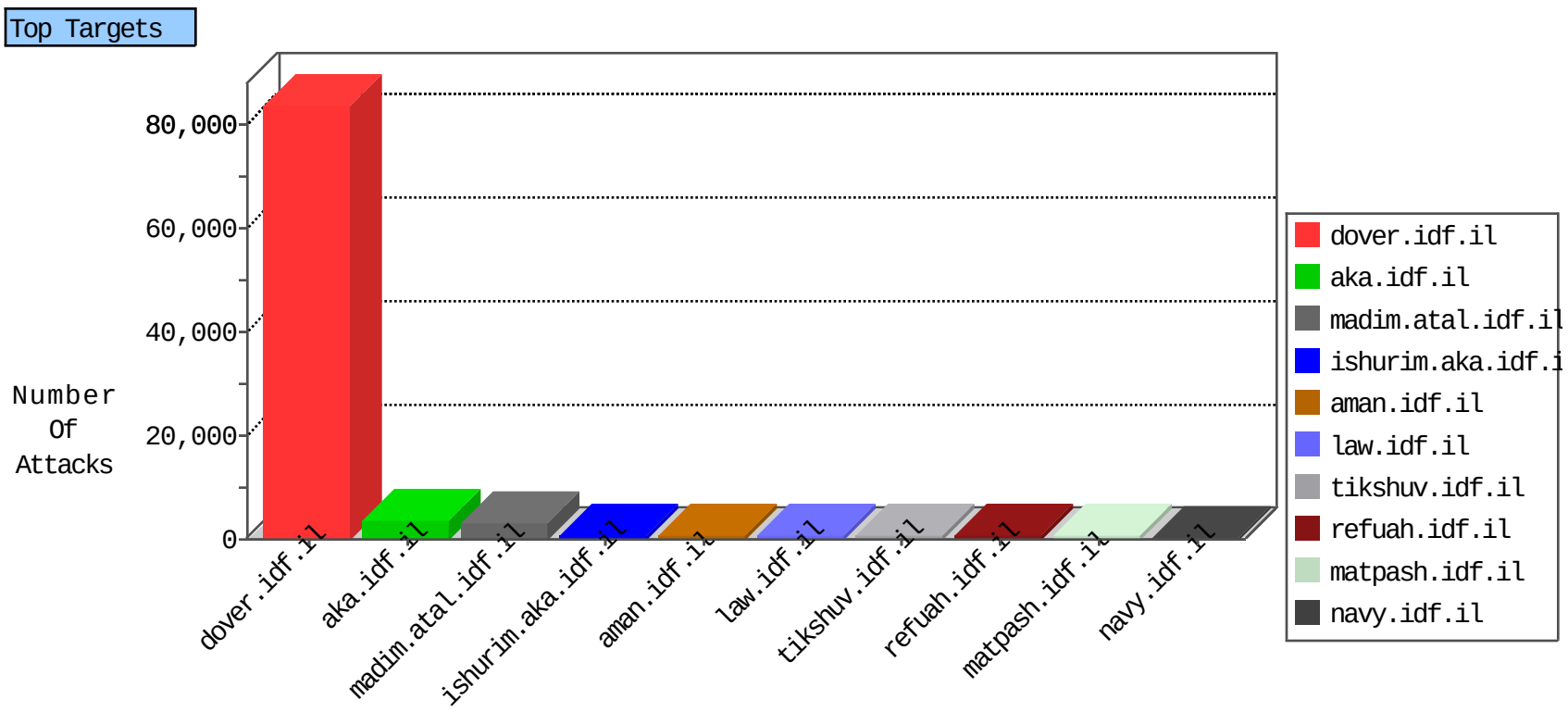
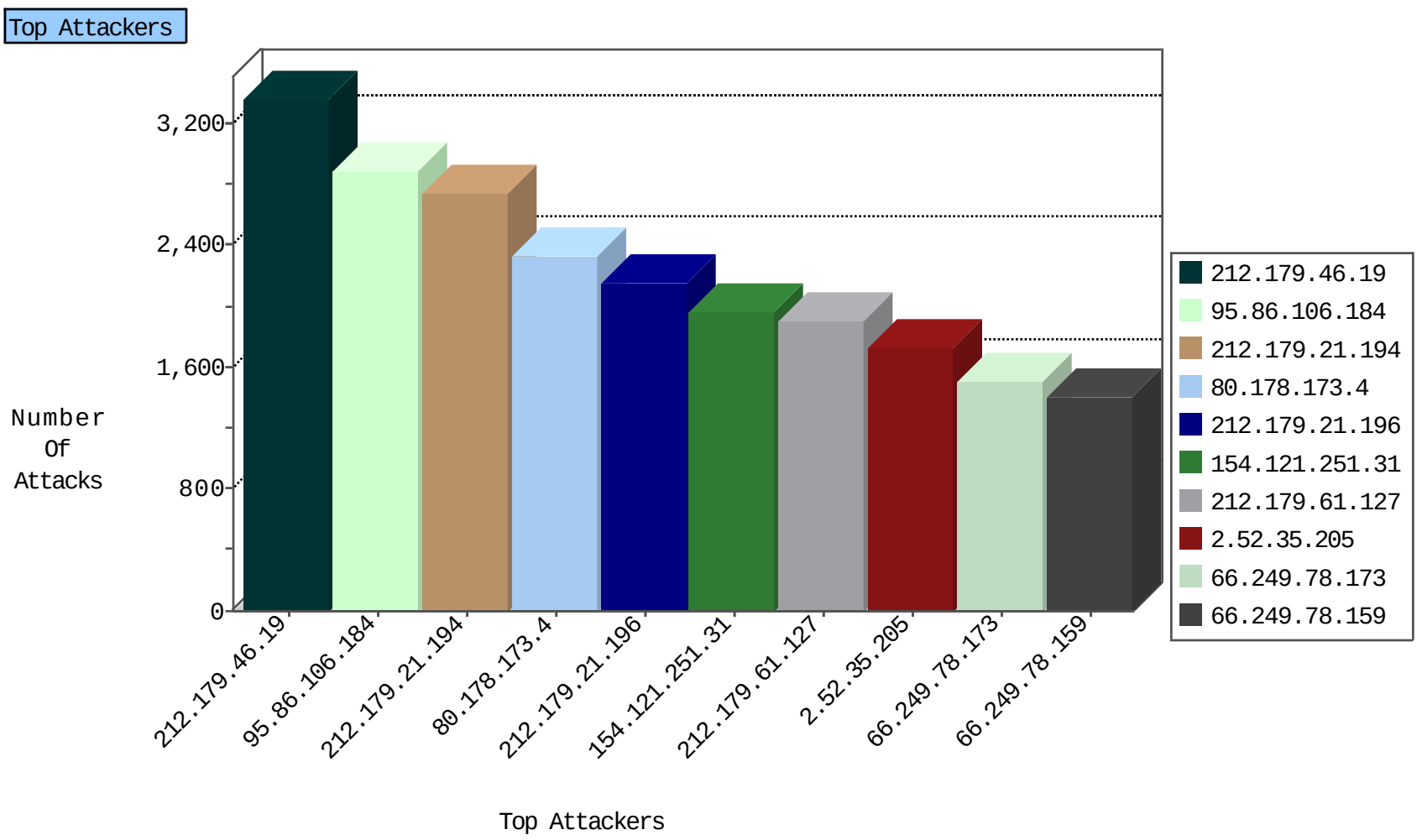
05-04-2015-00:00:07 to 05-05-2015-00:00:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2015-00:00:07 to 05-05-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	20269
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	19790
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8969
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3066
220.181.108.99	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3064
213.57.118.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2980
212.179.46.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2733
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2643
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1068
5.29.151.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	830
84.108.251.133	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	740
89.139.24.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	500
212.179.46.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
81.218.51.66	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	464
84.108.156.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	330
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	328
31.210.187.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
85.64.125.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
77.125.1.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	300
84.109.17.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	254
46.116.3.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
66.249.93.245	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	201
84.111.189.130	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
220.181.108.80	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	166
220.181.108.104	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	163
220.181.108.117	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	161
77.126.190.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
37.142.129.150	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	147
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	144
37.60.44.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	142
220.181.108.174	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	141
46.121.89.18	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	140
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
5.29.171.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
109.66.172.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	114
109.67.81.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
149.88.93.170	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	107
79.176.20.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
154.121.251.31		147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	105
84.110.82.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
220.181.108.94	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	94
2.54.40.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.178.8.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
89.138.215.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
37.142.221.208	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.48.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84

05-04-2015-00:00:07 to 05-05-2015-00:00:07

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	307
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	279
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	240
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	138
93.186.16.154	South Africa	147.237.77.216	dover.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	123
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	113
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	88
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	84
81.218.116.129	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	81
115.235.170.1	China	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	33
37.60.46.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	32
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
37.60.44.107	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
95.86.106.7	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
95.86.108.102	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
213.151.44.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
93.173.230.10	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
80.179.31.209	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
94.230.86.184	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.28.137.52	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
95.86.122.88	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
95.86.97.7	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.22.129.194	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
37.142.140.19	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.151.49.171	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
154.121.251.203		147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	5
86.134.190.155	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.54.26.31	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
201.197.102.10	Costa Rica	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.51	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
213.55.107.96	Ethiopia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
31.44.129.25	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
82.166.202.245	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

05-04-2015-00:00:07 to 05-05-2015-00:00:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
154.121.251.31		147.237.77.216	dover.idf.il	SQL Injection - Select From	167
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	149
154.121.251.31		147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	126
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	121
154.121.251.31		147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	105
154.121.251.31		147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	102
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	95
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	88
154.121.251.31		147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	87
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	87
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	87
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	83
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	62
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	62
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	62
154.121.251.31		147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	62
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	62
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	62
154.121.251.31		147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	62
156.17.187.240	Poland	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	50
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-IIS Directory transversal attempt	43
154.121.251.31		147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	42
46.116.164.218	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	42
154.121.251.31		147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	21
154.121.251.31		147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	13
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	9
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	7
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
154.121.251.203		147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	6
195.110.35.13	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
109.65.106.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
154.121.251.203		147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	5
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	4
154.121.251.31		147.237.77.216	dover.idf.il	SQL Injection - Union (POST)	3
66.249.64.193	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
154.121.251.31		147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - POST parameter	3
46.120.168.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
154.121.251.31		147.237.77.216	dover.idf.il	SQL Injection - Union Select (POST)	3
154.121.251.31		147.237.77.216	dover.idf.il	SQL Injection - Select From (POST)	3
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
112.175.184.11	Korea, Republic of	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	2
109.65.122.143	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.99.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.62.216	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.2.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.162	Japan	147.237.8.46	e.chinuch.idf.i	ET SCAN Potential SSH Scan	2

05-04-2015-00:00:07 to 05-05-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3363
95.86.106.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2886
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2731
80.178.173.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2333
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2149
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1864
2.52.35.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1684
192.115.62.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1354
77.42.252.199	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1309
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1247
212.76.96.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1223
105.46.152.193		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1208
82.205.75.35	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1175
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1118
164.138.119.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	902
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	864
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	746
81.218.71.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	707
2.52.184.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	682
46.19.86.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	663
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	575
81.218.126.226	Israel	147.237.77.216	dover.idf.i		SQL Injection	monitor	557
109.67.57.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	469
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	447
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	409
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	386
213.151.42.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	383
66.249.78.159	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	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	341
153.107.192.208	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	333
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	324
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	314
212.28.230.202	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	310
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	309
213.151.35.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	308
79.177.22.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	307
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	272
212.179.46.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262
95.86.79.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	251
66.87.117.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	246
148.177.129.211	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	236
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	235
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	232
176.12.144.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	223
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	221
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	214
2.54.60.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	207

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.129.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1014
5.29.193.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	684
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	528
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	504
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	497
109.253.140.86	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.86	Block	414
109.253.143.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	357
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 195.160.240.11	Block	195
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.38	Block	148
213.57.96.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
2.54.189.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	110
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	101
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	65
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	57
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	50
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.188	Block	48
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	44
154.121.251.203		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 154.121.251.203	Block	44
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	42
154.121.251.203		147.237.77.216	dover.idf.il	Multiple Admin Blocking from 154.121.251.203	Block	41
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	34
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	30
142.54.174.178	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 142.54.174.178	Block	28
80.246.136.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	23
212.76.113.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	23
80.246.140.146	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.140.146	Block	23
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	23
46.229.164.111	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	21
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	21
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	21
157.55.39.107	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.107	Block	18
62.219.153.212	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	18
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.123.8.135	Block	18
79.176.111.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	17
46.121.245.189	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.245.189	Block	16
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	15
80.246.136.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
79.182.126.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
213.151.59.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
80.246.130.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.216	Block	12
46.229.164.102	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	11
213.57.188.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
213.8.129.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	11
77.127.172.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
31.44.141.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
87.68.253.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	10
79.176.123.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10

05-04-2015-00:00:07 to 05-05-2015-00:00:07