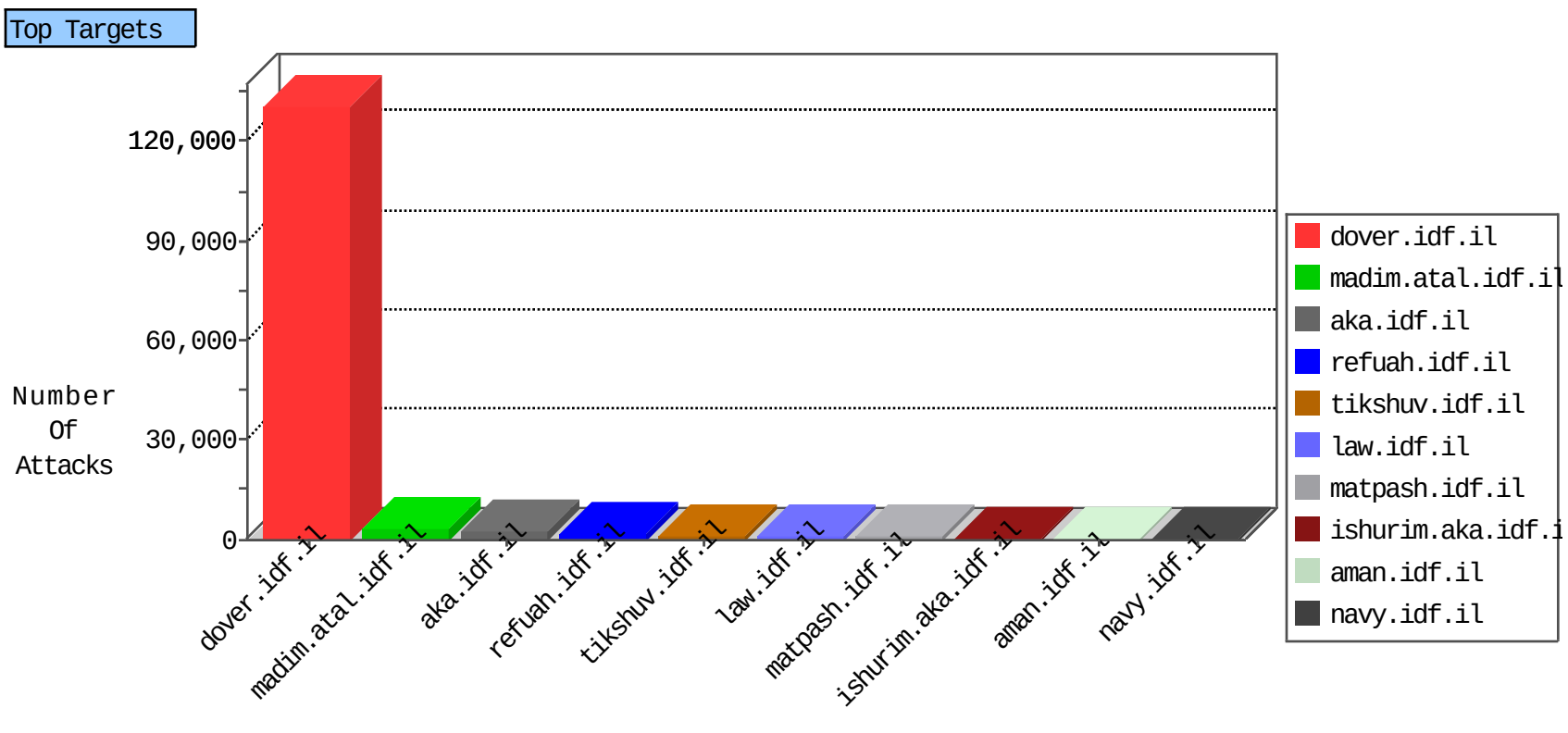
05-28-2015-00:00:05 to 05-29-2015-00:00:05

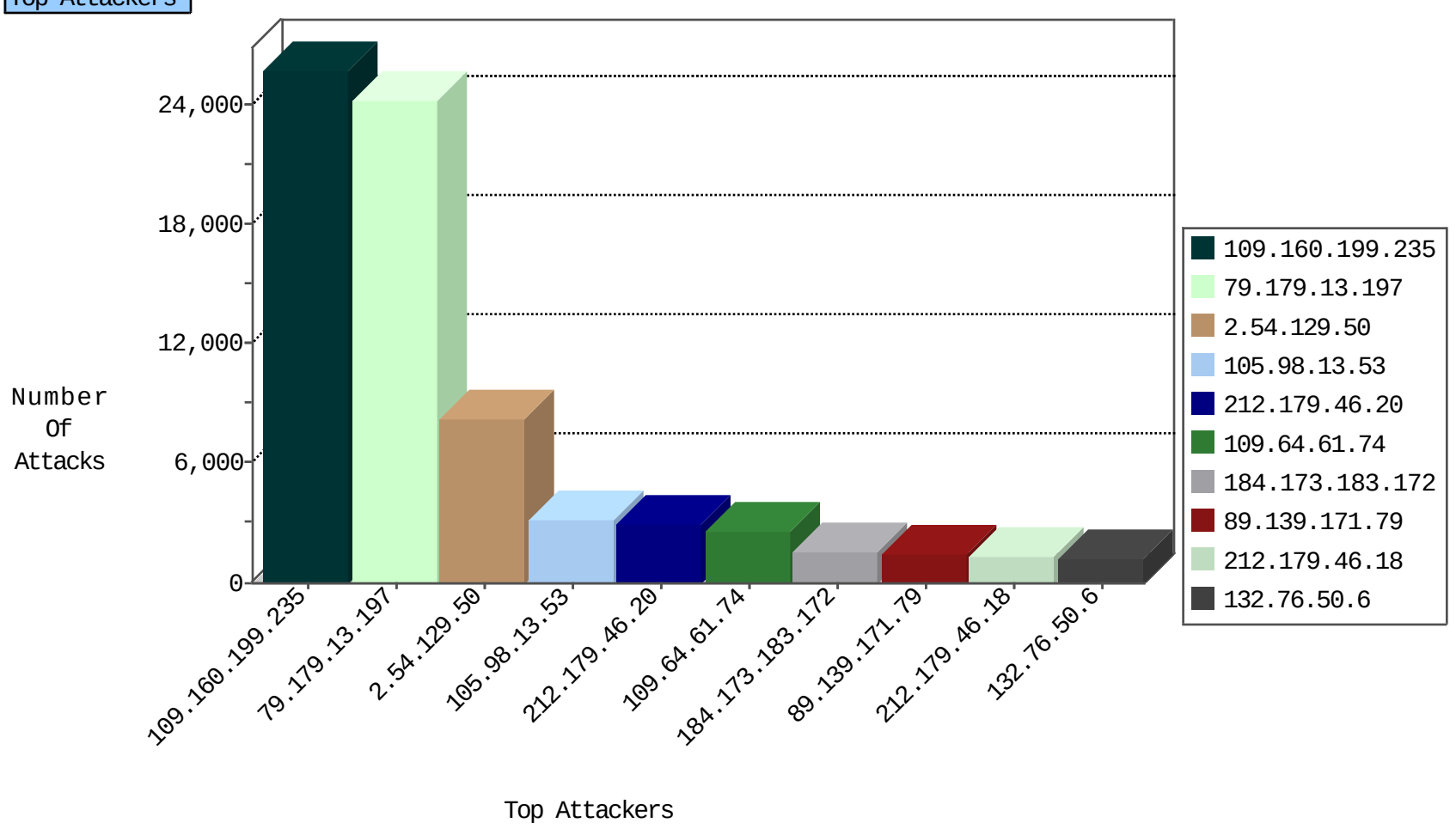
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-28-2015-00:00:05 to 05-29-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
81.218.126.226	Israel	147.237.76.42	refuah.idf.il	TCP Scan (vertical)	drop	125764
66.249.64.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5943
81.218.126.226	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	5550
79.177.19.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2694
79.181.66.58	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	2501
149.78.155.29	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	540
93.173.253.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	472
5.28.188.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	440
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	378
149.88.31.172	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	374
132.72.225.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	344
84.228.173.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	341
176.12.151.215	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
149.78.195.132	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	242
24.186.213.217	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	236
46.116.205.204	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
85.250.10.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	215
46.121.248.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
5.29.242.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	207
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	201
87.69.110.138	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.29.13.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
149.78.139.231	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
84.228.144.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
5.28.158.84	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	129
185.32.178.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
85.250.130.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
77.125.139.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
85.65.194.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
149.78.81.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
37.142.111.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.121.60.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
109.186.25.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
77.126.75.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
2.54.31.123	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
185.32.176.13	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.85.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.85.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	83
80.246.138.146	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
109.67.20.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
109.65.158.212	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
46.19.85.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
109.253.157.196	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74

05-28-2015-00:00:05 to 05-29-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	517
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	399
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	277
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	238
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	200
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	119
31.168.143.10	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	67
74.222.5.196	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
203.151.234.15	Thailand	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	30
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	29
194.90.186.65	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	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
89.139.171.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	20
62.90.221.127	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
212.143.3.44	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
84.111.156.183	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
85.64.200.198	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
87.69.79.112	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
84.94.60.40	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
87.68.249.94	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
112.111.188.127	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
109.64.180.163	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
109.186.156.78	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
82.80.128.9	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
80.178.28.172	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
213.57.177.48	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
89.139.166.243	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
178.234.221.250	Russian Federation	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
5.29.79.135	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
79.178.197.231	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	9
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	8
87.69.28.83	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.116.210.160	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
80.178.207.58	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
85.65.39.195	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
109.67.100.244	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
2.54.151.132	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.223	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
79.179.6.57	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
147.236.113.1	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
213.57.53.187	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
5.102.232.177	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
46.185.242.130	Jordan	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	7
176.12.144.138	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
157.55.39.220	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	6
37.26.148.140	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6

05-28-2015-00:00:05 to 05-29-2015-00:00:05

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	196
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Select From	188
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	176
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	119
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	110
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	100
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	95
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	95
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	95
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	95
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	94
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	94
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	94
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	94
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	81
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	81
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	81
81.162.98.252	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	47
81.162.98.252	Ukraine	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie	47
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	42
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	16
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	16
31.168.143.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	10
185.32.178.185	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
66.249.69.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
84.94.223.15	Israel	147.237.0.35	akaws.idf.il	WEB-FRONTPAGE /_vti_bin/ access	5
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - POST parameter	4
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Union Select (POST)	4
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Select From (POST)	4
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
105.98.13.53	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Union (POST)	4
89.139.171.79	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
43.255.188.130	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.25	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
79.182.136.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
46.162.116.221	Sweden	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.156	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.21	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
85.250.150.84	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.166.20.62	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
37.142.184.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.210.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.186.130.130	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

05-28-2015-00:00:05 to 05-29-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.160.199.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25702
79.179.13.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24223
2.54.129.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8225
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2878
109.64.61.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2534
89.139.171.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1380
105.98.13.53	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1345
212.179.46.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1289
132.76.50.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1259
212.179.46.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1236
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1150
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1009
2.54.167.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	995
2.54.38.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	987
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	879
95.86.88.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	798
164.138.125.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	788
91.240.235.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	653
162.198.18.243	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	550
79.178.141.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	536
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
2.54.155.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	464
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	453
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	450
37.26.146.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	449
82.80.17.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	431
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	425
8.37.224.254	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	384
89.139.166.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	367
194.114.146.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	358
153.107.192.208	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
63.141.204.184	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	350
46.121.218.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	311
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	311
95.86.89.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	306
5.2.219.77	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	304
108.53.97.47	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	294
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	289
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
164.138.116.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
93.173.28.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	271
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	264
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	253
2.54.183.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	252
66.87.80.62	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	229
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
41.33.232.65	Egypt	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	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	208
84.94.32.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	203
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	202

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.81	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.81	Block	749
2.54.31.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	697
2.54.32.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	466
79.177.103.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	380
176.12.148.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.96	Block	329
109.253.149.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.149.45	Block	294
5.29.113.21	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.113.21	Block	232
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	177
79.181.33.3	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.181.33.3	Block	123
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	69
109.186.146.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	42
176.12.148.68	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.68	Block	24
109.253.149.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
109.253.137.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	21
188.120.153.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	21
31.168.217.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
79.176.19.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
79.177.25.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
37.142.13.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
84.228.113.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	15
212.179.214.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
176.12.139.65	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
83.130.115.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
93.172.22.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
79.178.61.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
93.173.146.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.120.195.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
83.130.116.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
84.110.53.109	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.110.53.109	Block	10
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	9
109.253.136.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
80.246.138.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
95.86.115.162	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.115.162	Block	9
84.228.110.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
188.120.148.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
2.54.166.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
164.138.125.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
95.86.67.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	8
80.179.115.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.179.115.9	Block	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
207.46.13.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	8
37.26.147.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
192.117.13.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
213.151.40.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
85.250.63.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	7
80.179.126.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
2.54.186.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.12.140.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6

05-28-2015-00:00:05 to 05-29-2015-00:00:05