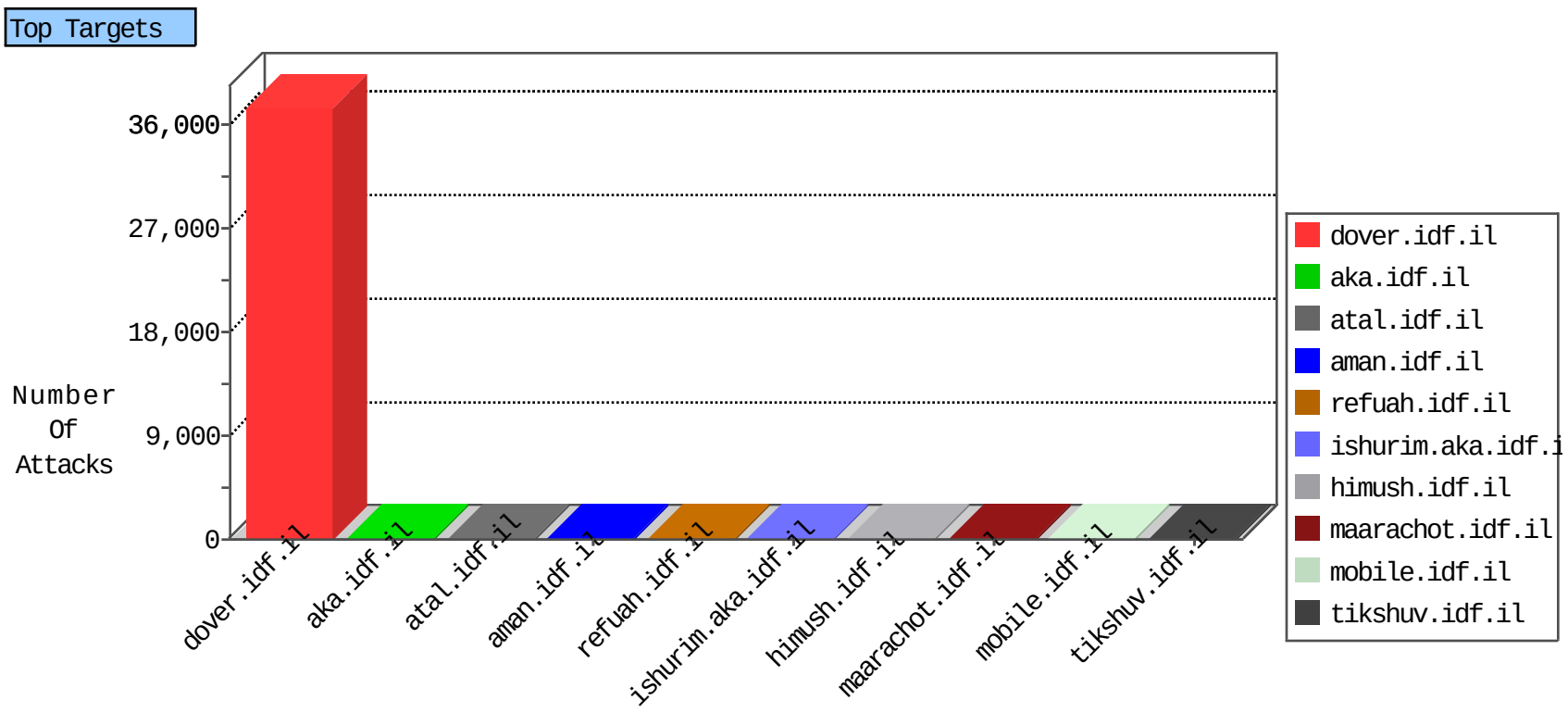
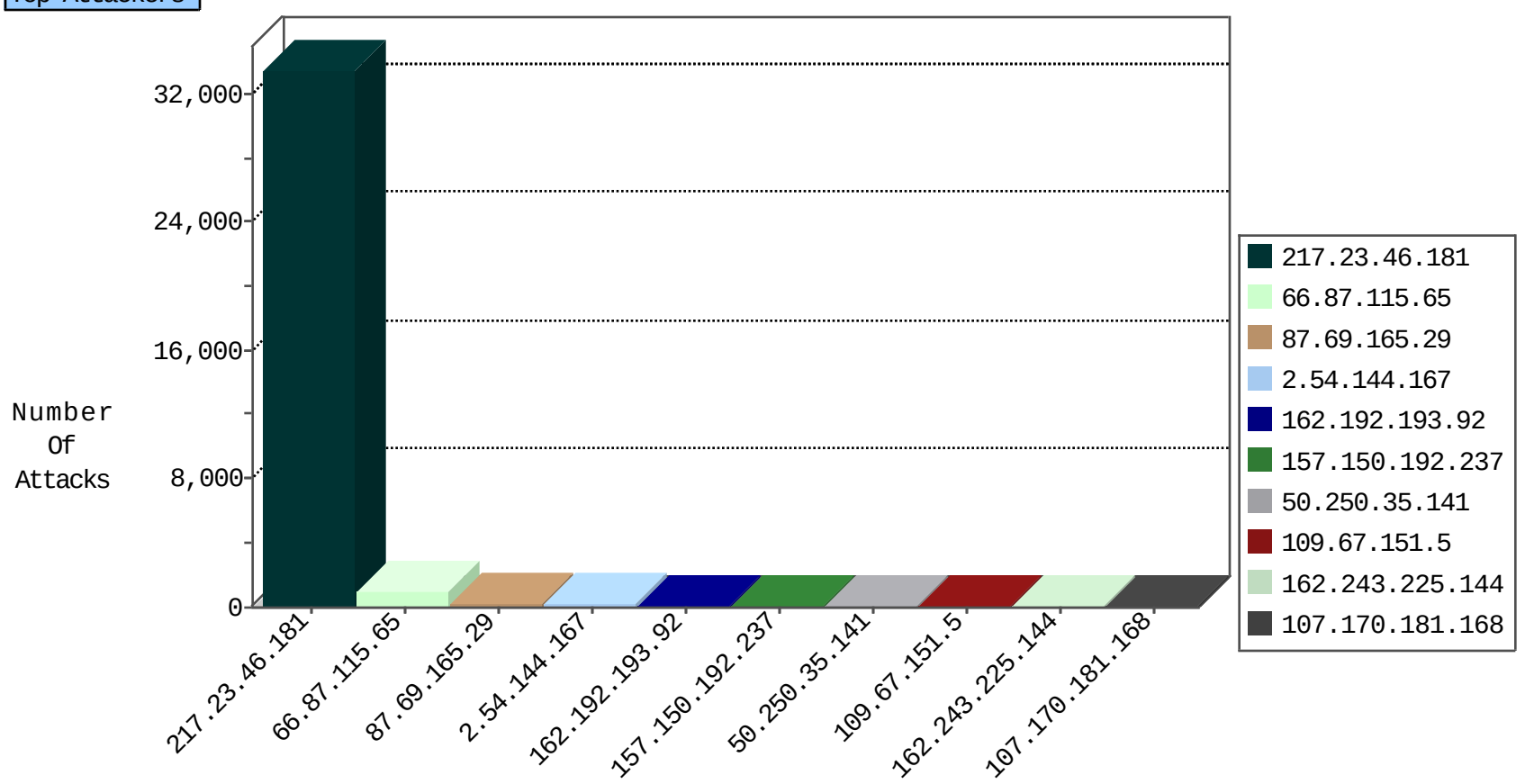
05-05-2015-20:03:06 to 05-05-2015-21:03:06

IDF Under Attack
05-05-2015-20:03:06

Top Targets



Top Attackers



05-05-2015-20:03:06 to 05-05-2015-21:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
77.127.151.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
79.179.124.94	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
109.64.27.54	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	48
46.117.120.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
2.54.1.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	5
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	DOS-HOIC-TCP-80-gbo	forward	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
46.116.254.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
146.185.239.100	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
2.54.175.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.216.37	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

05-05-2015-20:03:06 to 05-05-2015-21:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.67.151.5	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
61.186.249.141	China	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
77.125.121.109	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
79.179.52.74	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
2.52.133.91	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
79.179.96.104	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.116	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
94.28.252.52	Russian Federation	147.237.72.166	aka.idf.il	3617: HTTP: Paros Proxy HTTP Request	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
84.108.4.28	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1

05-05-2015-20:03:06 to 05-05-2015-21:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
2.52.131.238	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
37.142.105.184	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.175.255.61	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.75.56.43		147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
92.47.29.12	Kazakstan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
222.186.21.202	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.202	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.202	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.175.255.61	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.131	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.157.41.55	Pakistan	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.42.221	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.200.133	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.202	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.202	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.202	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	ET DROP Dshield Block Listed Source	1

05-05-2015-20:03:06 to 05-05-2015-21:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
217.23.46.181	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32897
66.87.115.65	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	935
87.69.165.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	188
2.54.144.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	178
217.23.46.181	Jordan	147.237.77.216	dover.idf.i		drop	drop	144
162.192.193.92	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
157.150.192.237	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
50.250.35.141	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	110
162.243.225.144	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	93
109.67.151.5	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	80
217.23.46.181	Jordan	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	68
107.170.181.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
217.23.46.181	Jordan	147.237.77.216	dover.idf.i	SAM rule	drop	drop	61
217.23.46.181	Jordan	147.237.77.216	dover.idf.i		Bad TCP sequence	monitor	55
217.23.46.181	Jordan	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	55
178.136.217.31	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
84.44.208.82	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
176.12.144.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
37.142.166.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
46.117.102.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
64.233.173.161	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
82.165.137.121	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
107.22.39.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
64.233.173.156	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
87.68.244.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
175.156.72.250	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
149.255.192.33	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
84.26.33.126	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
176.12.139.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.85.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
84.111.103.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
79.178.32.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
77.126.21.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
54.224.145.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
81.152.215.22	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
204.101.237.139	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
2.52.171.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
86.108.12.24	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
41.131.194.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
193.43.245.250	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
213.151.55.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
212.183.128.253	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
192.116.95.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 217.23.46.181	Block	98
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	88
62.219.155.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.181.117.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.149.36	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
213.151.59.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.67	Block	2
217.23.46.181	Jordan	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	2
79.181.19.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
213.57.250.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.163.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.117.34.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
170.74.56.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
80.246.130.169	Israel	147.237.76.42	refuah.idf.i	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
77.127.69.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.65.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.103.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.110.2.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
208.221.239.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
79.179.52.74	Israel	147.237.76.42	refuah.idf.i	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluiml	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1134-9115-he/dover.aspx	Block	1
54.197.94.30	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.158.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.22.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.149.36	Israel	147.237.77.243	mobile.idf.i	Multiple Unauthorized URL Access from 176.12.149.36	Block	1
80.246.136.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.176.24.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/iturimp	Block	1
109.64.103.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
84.111.64.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
209.73.137.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
79.179.149.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter 55bffe68 in www.aka.idf.il/main/home/default.aspx	None	1
95.86.74.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.177.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.42.110	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
79.176.104.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
109.67.151.5	Israel	147.237.76.42	refuah.idf.i	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1