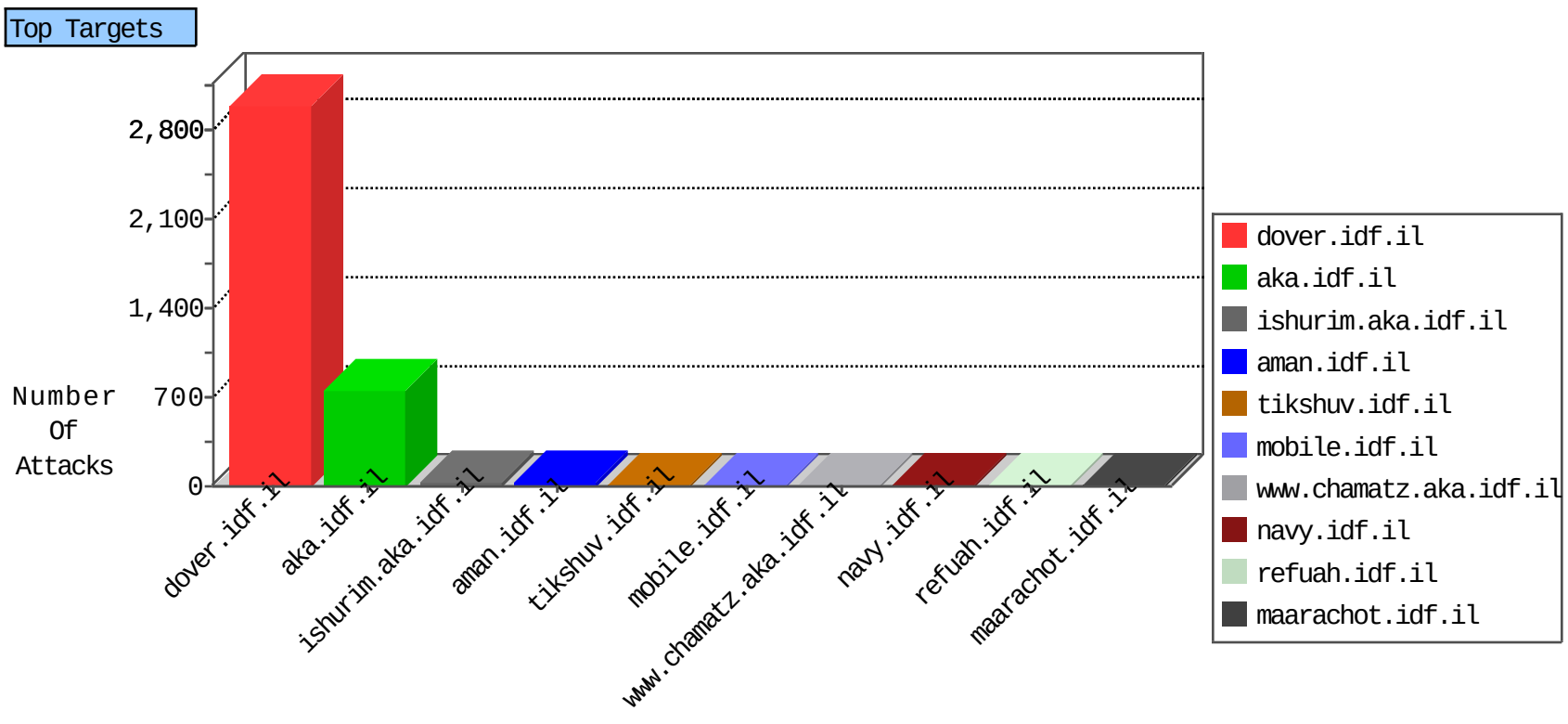
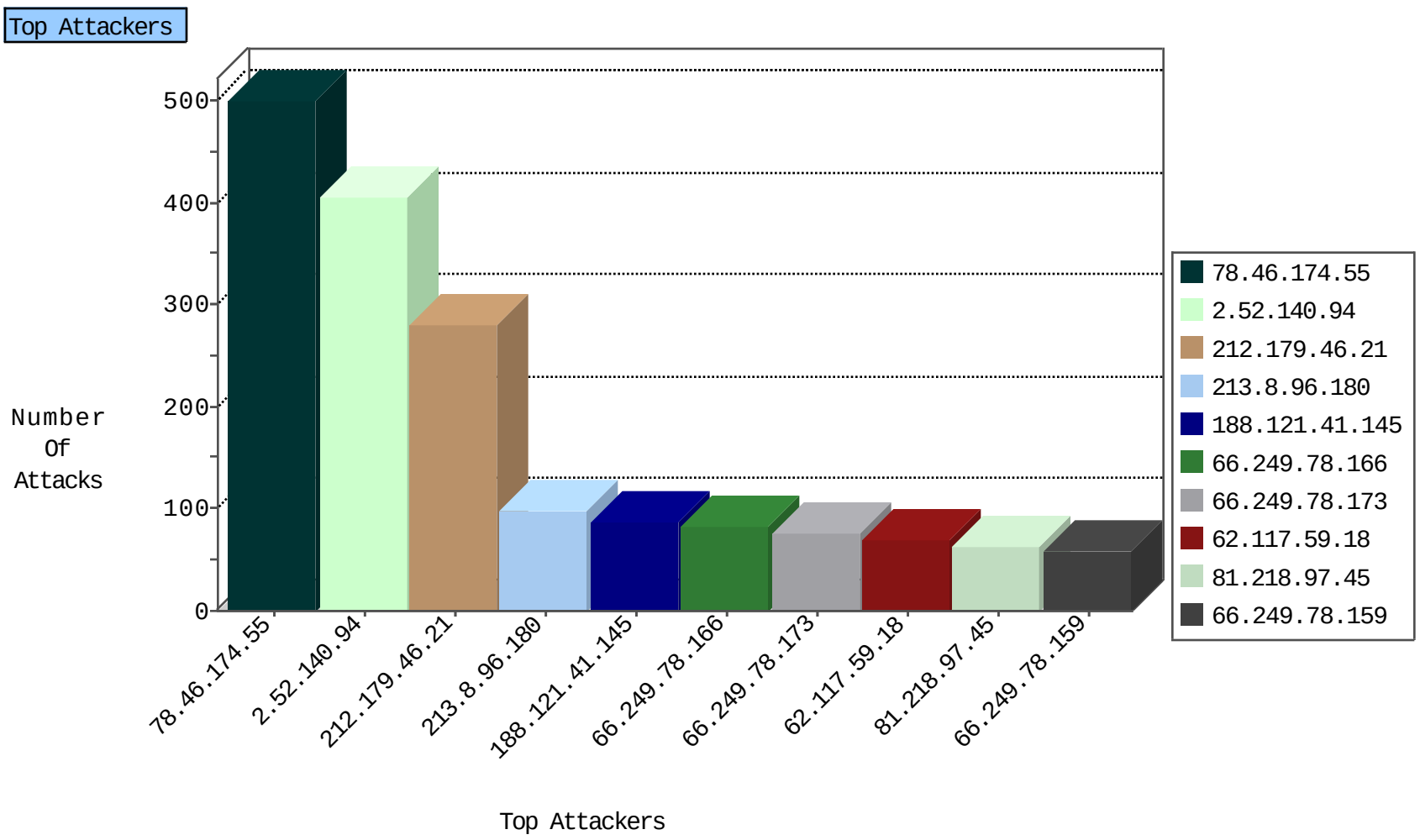
05-07-2015-12:03:05 to 05-07-2015-13:03:05

IDF Under Attack
05-07-2015-12:03:05





05-07-2015-12:03:05 to 05-07-2015-13:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	165
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
109.65.129.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
66.249.78.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.94.96.33	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
172.19.1.127		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
10.0.0.8		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.65.75.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
213.8.96.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.68.153.241	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
109.67.147.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.46.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
123.59.62.253	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
37.26.146.246	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

05-07-2015-12:03:05 to 05-07-2015-13:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
59.9.253.225	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	21
109.186.118.169	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
77.125.94.154	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
84.111.138.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
109.134.89.35	Belgium	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-12:03:05 to 05-07-2015-13:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.75.5	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	Germany	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.203	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
121.88.5.177	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.89	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
121.88.5.177	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.253.136.181	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.140.113	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.229.227	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.240.162	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
199.203.47.233	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
192.116.81.105	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.160.128	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.114	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
121.88.5.177	Korea, Republic of	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.244	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.186.173.39	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.240.162	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
92.47.29.12	Kazakstan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
207.232.27.5	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.108	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

05-07-2015-12:03:05 to 05-07-2015-13:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.140.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	394
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	280
213.8.96.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	94
62.117.59.18	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
81.218.97.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
45.48.96.151		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
109.253.158.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
132.66.167.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
46.120.190.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
118.241.234.224	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
2.54.43.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.253.141.128	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.137.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
82.145.219.85	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
62.0.34.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
109.186.118.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
217.164.22.187	United Arab Emirates	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
2.54.130.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
2.52.173.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.218.158.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
79.179.140.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
213.151.48.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.116.182.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
146.185.58.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
192.117.138.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
62.128.45.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.179.185.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.26.147.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
87.69.234.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
85.250.43.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.95.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.121.73.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.177.4.154	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
31.168.199.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
41.191.99.42	Ghana	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
80.178.11.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
84.94.96.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	342
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	41
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	40
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	40
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	38
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	34
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 188.121.41.145	Block	23
109.186.184.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnaviga ton.asp	Block	20
79.181.167.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	3
94.159.131.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.64.44.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
79.182.24.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
84.108.220.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.115.130.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
207.46.13.130	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.178.31.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1392-he/refuah.aspx	Block	1
109.253.147.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.120.241.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 202.112.50.77	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
95.86.81.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
212.14.228.106	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/937-he/refuah.aspx	Block	1
125.209.235.174	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.44.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnaviga ton.asp	Block	1
46.120.243.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/×ª/main/giyus	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
176.12.146.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
109.65.143.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/binladen2.stm	Block	1
213.57.196.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Illegal HTTP Version ×″×–×™× ×•×š ×•×″× ×• ×¢×¨&body=http://www.aka.idf.il/chinuch/home/default.asp?catId =42142&docId= HTTP/1.1	Block	1
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/klali/null	Block	1
89.77.24.21	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
54.160.234.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	1
78.47.8.52	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1

05-07-2015-12:03:05 to 05-07-2015-13:03:05