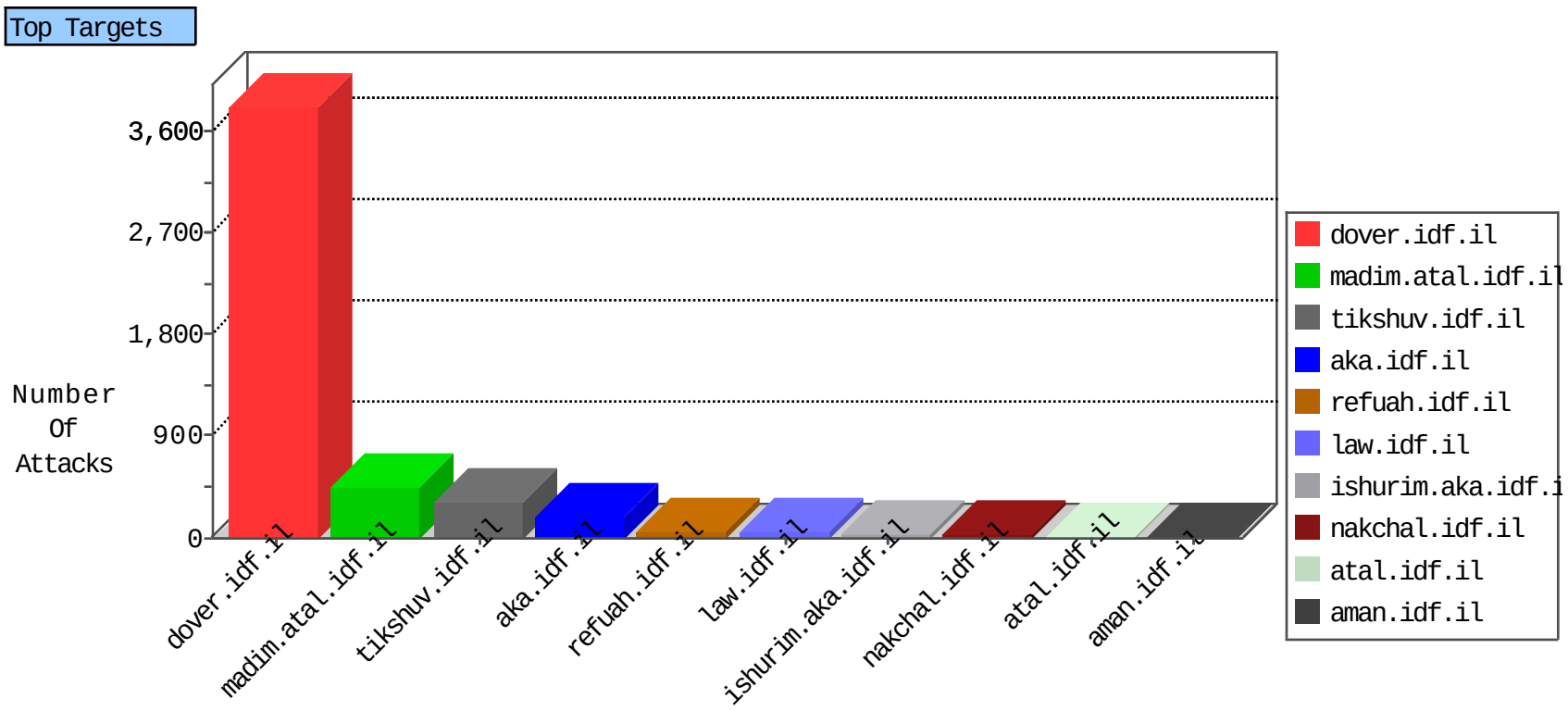
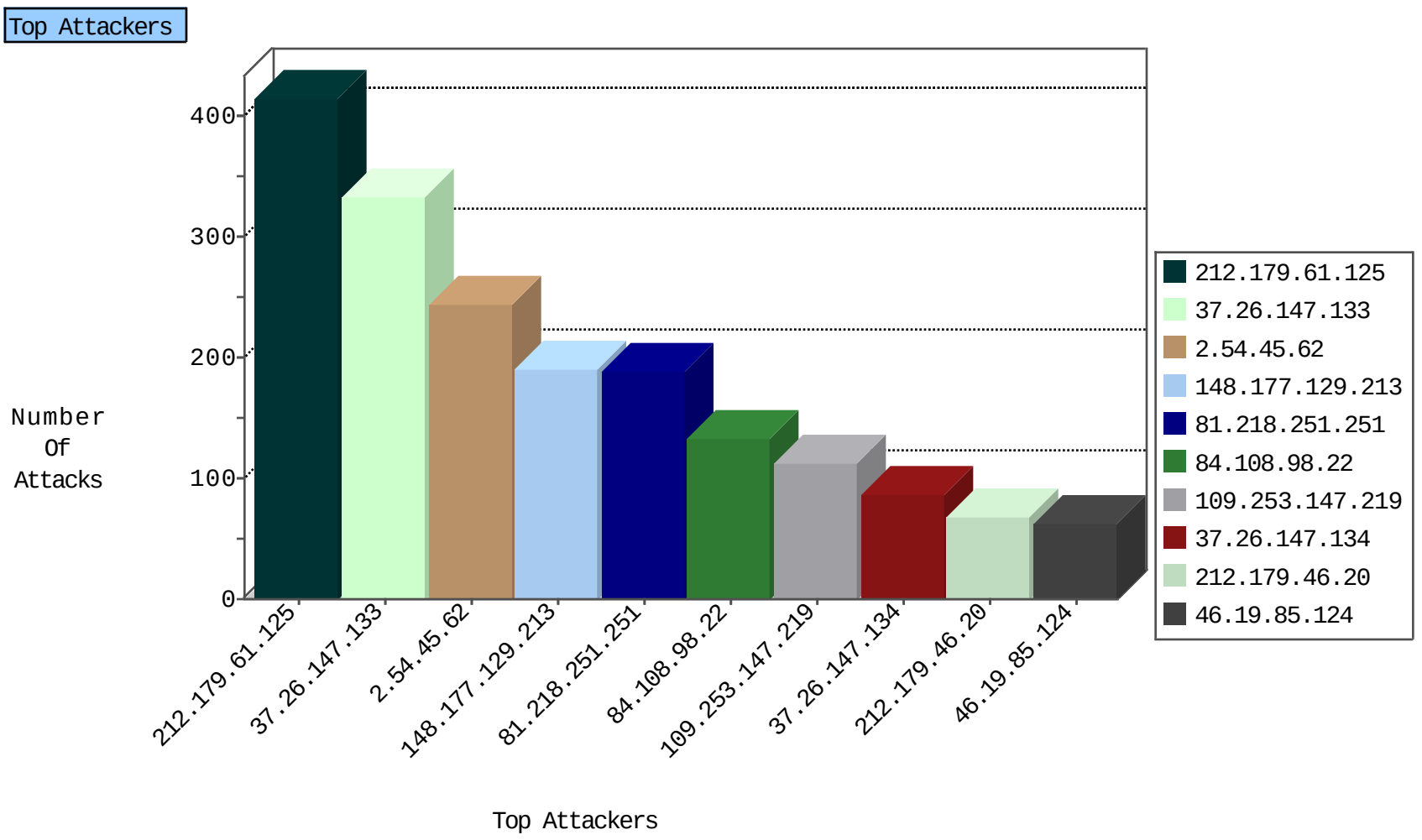
05-06-2015-11:03:02 to 05-06-2015-12:03:02

IDF Under Attack
05-06-2015-11:03:02

Top Targets



Top Attackers



05-06-2015-11:03:02 to 05-06-2015-12:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4017
157.55.39.204	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	523
46.19.85.134	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
2.54.187.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.64.51.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.186.34.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
80.178.147.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
82.102.141.253	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4
41.223.163.75	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
213.57.62.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
140.9.0.60	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
217.66.244.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.95.251.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.61.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
219.73.64.65	Hong Kong	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
188.162.64.70	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.147.205	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
213.8.242.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.145.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-11:03:02 to 05-06-2015-12:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	28
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
112.111.189.8	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
45.97.125.114		147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
84.157.174.218	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
213.57.190.247	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.46.39.146	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
149.78.174.142	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.31	nakchal.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
93.172.190.218	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
185.32.176.194	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
109.160.189.67	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-11:03:02 to 05-06-2015-12:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
212.179.61.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
84.109.192.147	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
79.178.0.138	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.244	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.249.73.225	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
142.59.15.141	Canada	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
128.140.230.75	Romania	147.237.0.15	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
109.64.42.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
85.65.127.165	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.75.26	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.69.94.13	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.182.74	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.244	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
79.176.144.107	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.244	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.219.149.53	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
203.59.90.68	Australia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.185	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
132.68.50.73	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.138.60	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.147.180.56	Saudi Arabia	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

05-06-2015-11:03:02 to 05-06-2015-12:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	413
2.54.45.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	244
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
84.108.98.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	133
37.26.147.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
46.19.85.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
46.19.86.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.160.189.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
91.231.92.29	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
41.223.163.75	Sudan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
77.127.26.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
62.90.192.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
82.166.229.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
31.186.228.65	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	24
213.57.109.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
84.157.174.218	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
79.181.49.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
149.88.206.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
2.52.23.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.26	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.31	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	20
134.191.232.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
178.63.165.188	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
77.125.248.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
31.186.228.91	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.68	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	18
109.186.34.142	Israel	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	18
62.0.103.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.186.34.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
31.186.228.93	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
109.186.2.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
31.186.228.86	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	14
167.220.196.80	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.96	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	14
213.151.37.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
209.88.198.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	333
109.253.147.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	113
62.81.85.102	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.81.85.102	Block	18
84.228.253.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
62.90.202.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.111.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.29.28.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
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	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
62.219.239.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	2
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	2
109.253.147.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
212.199.11.78	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.199.11.78	Block	2
213.57.190.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
115.252.188.136	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/8	Block	1
46.120.120.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.154.10.131	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/scriptresource.axd	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
188.95.227.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.24.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.46.39.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
80.246.130.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
2.54.48.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
173.192.138.226	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.73.225	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
61.49.45.43	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
149.88.91.170	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/webresource.axd	None	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-2.stm	Block	1
157.55.39.122	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
207.176.85.10	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
2.54.158.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.141.8	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/general	Block	1
174.129.64.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/may/19.stm	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
216.223.27.56	United States	147.237.77.74	law.idf.il	Distributed URL is Above Root Directory	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.146.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
203.133.169.221	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
89.138.79.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
79.180.33.135	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
188.165.15.230	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1