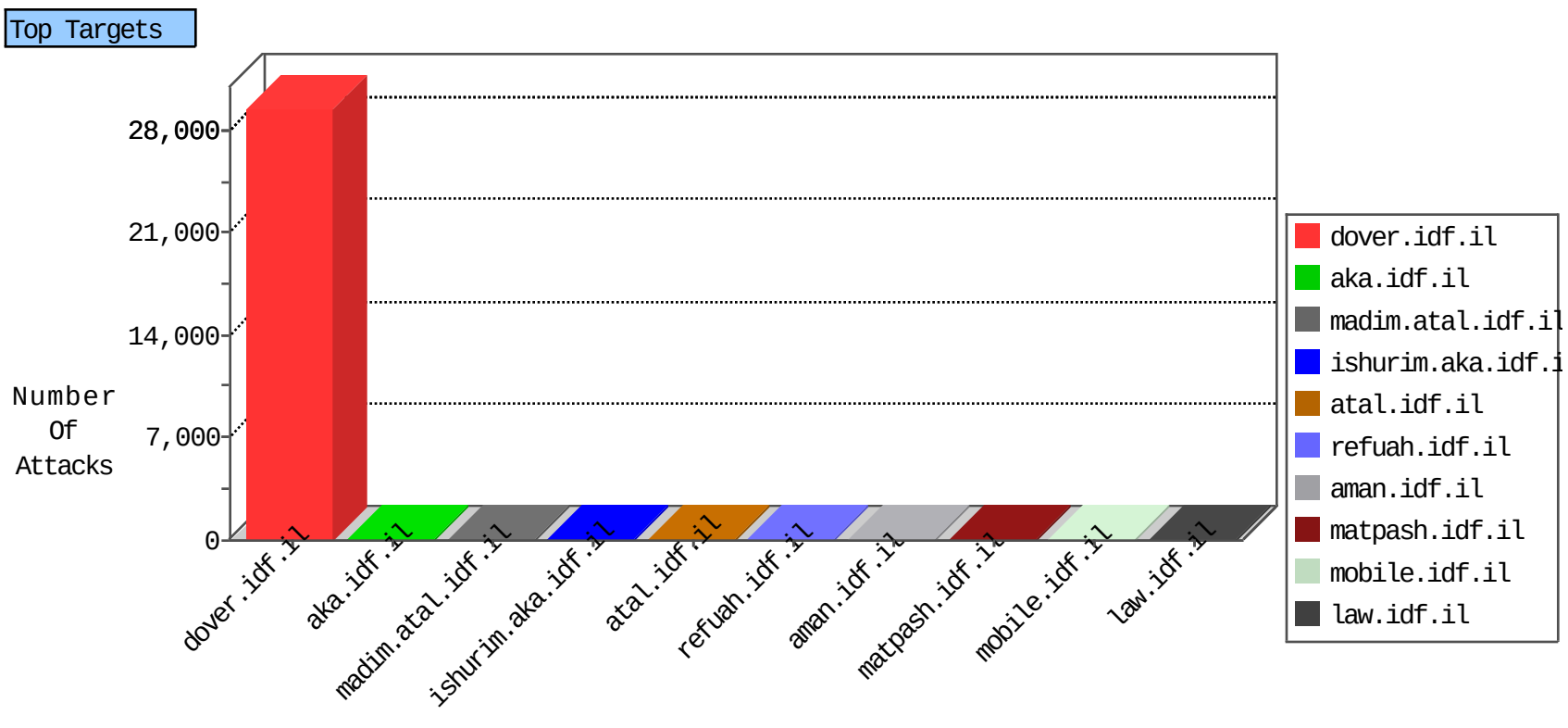
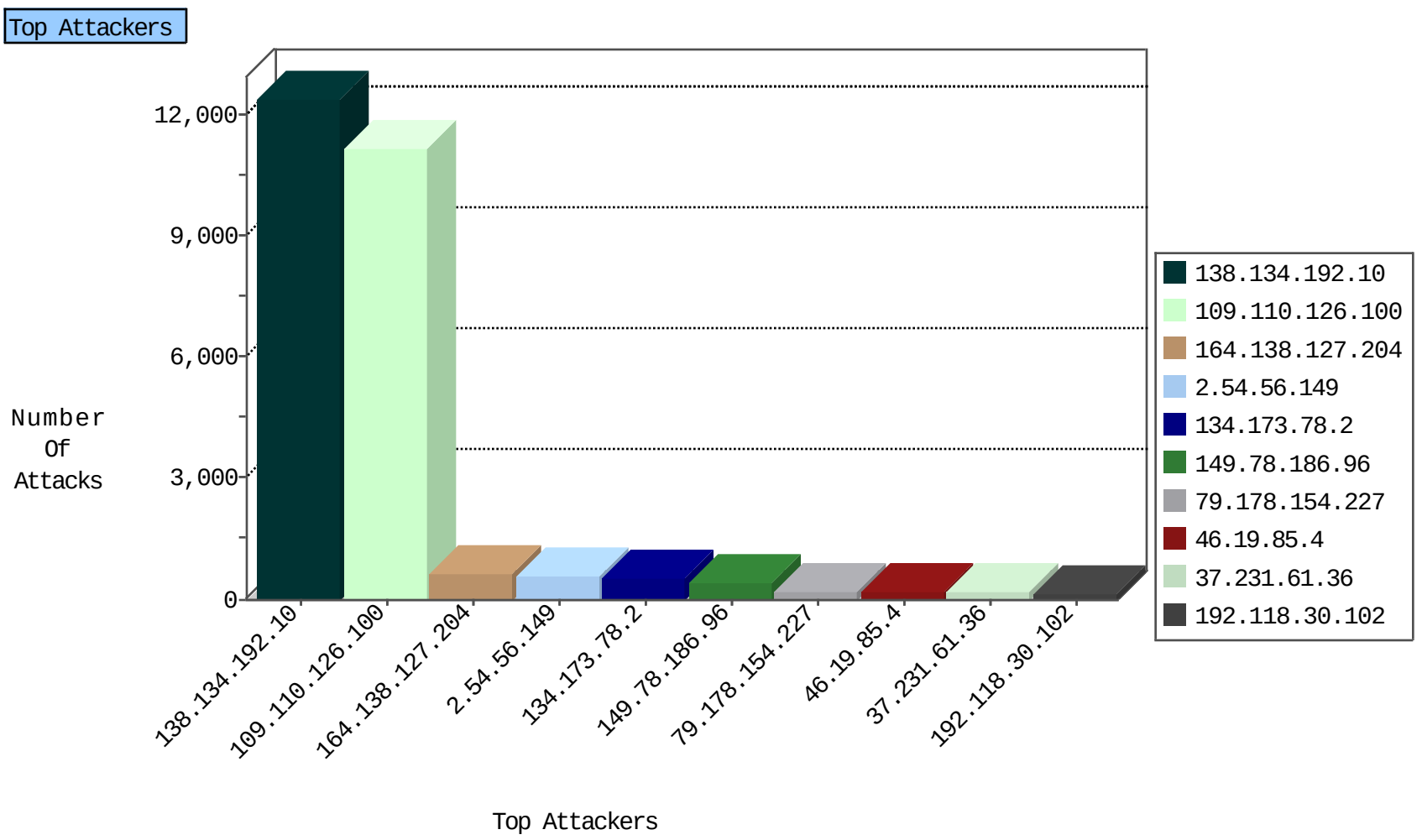
04-17-2015-09:03:03 to 04-17-2015-10:03:03

IDF Under Attack
04-17-2015-09:03:03

Top Targets



Top Attackers



04-17-2015-09:03:03 to 04-17-2015-10:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.110.126.100	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4422
66.249.67.34	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2885
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2858
108.211.78.223	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2516
66.249.67.157	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1073
138.134.192.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	517
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	510
84.108.65.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
66.249.67.31	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	148
109.110.126.100	Lebanon	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	6
109.110.126.100	Lebanon	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	4
106.244.87.198	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	4
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
149.88.148.206	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.102.141.251	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
192.118.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-17-2015-09:03:03 to 04-17-2015-10:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.179.39.236	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.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
93.120.27.62	Romania	147.237.76.39	mobile.meitav.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	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
79.183.9.160	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.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
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
37.8.56.190	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.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
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-09:03:03 to 04-17-2015-10:03:03

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	6
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
62.99.63.236	Spain	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.168.120.33	United States	147.237.76.31	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.7.57.198	Switzerland	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.68.196.123	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
186.115.220.210	Colombia	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
149.78.238.249	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.186.217	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
186.115.220.210	Colombia	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

04-17-2015-09:03:03 to 04-17-2015-10:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
138.134.192.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12361
109.110.126.100	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10963
164.138.127.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	615
2.54.56.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
134.173.78.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	548
149.78.186.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	437
79.178.154.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	214
46.19.85.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	175
37.231.61.36	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
104.131.228.99		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	106
109.110.126.100	Lebanon	147.237.77.216	dover.idf.i		drop	drop	100
46.19.85.96	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
46.19.86.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
36.68.8.168	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
2.54.37.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
192.118.30.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
69.166.47.139	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
31.44.141.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
79.180.120.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
2.54.33.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
176.12.146.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
212.179.91.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
176.12.146.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
46.19.86.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
77.245.3.103	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
79.177.127.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.120.24.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
176.12.150.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
79.183.9.160	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	33
80.74.103.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
84.109.83.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
93.34.198.144	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.86.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.253.149.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.86.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
83.42.128.170	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
109.110.126.100	Lebanon	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	22
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
207.46.13.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
176.12.144.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
46.19.86.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.65.158.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.238.249	United States	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.238.249	Block	60
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	3
79.182.189.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	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	3
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0106-3.stm	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/204-he/sb_item_lev1	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.63	Israel	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in chimush.atal.idf.il/938-he/himush.aspx	None	1
87.69.131.116	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.181.209.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.13	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//scriptresource.axd	Block	1
176.12.139.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.135.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.130.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
46.19.85.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.140	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0430-1.stm	Block	1
95.86.116.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.189.175	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.189.175	Block	1
31.13.112.116	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/sip_storage/files	Block	1
66.249.78.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/webresource.axd	Block	1
180.76.4.96	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
80.246.130.96	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.120.190.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general.aspx	Block	1
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.178	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.211	None	1
66.249.65.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
109.110.126.100	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.13.112.120	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/sip_storage/files/1	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/september/26.stm	Block	1
180.76.6.21	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-9403-he/cogat.aspx	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
80.246.137.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
61.14.146.240	Asia/Pacific Region	147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
79.179.39.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.179	Block	1
66.249.65.15	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.253.128.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.9.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1
31.168.199.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-he/refuah.aspx	Block	1

04-17-2015-09:03:03 to 04-17-2015-10:03:03