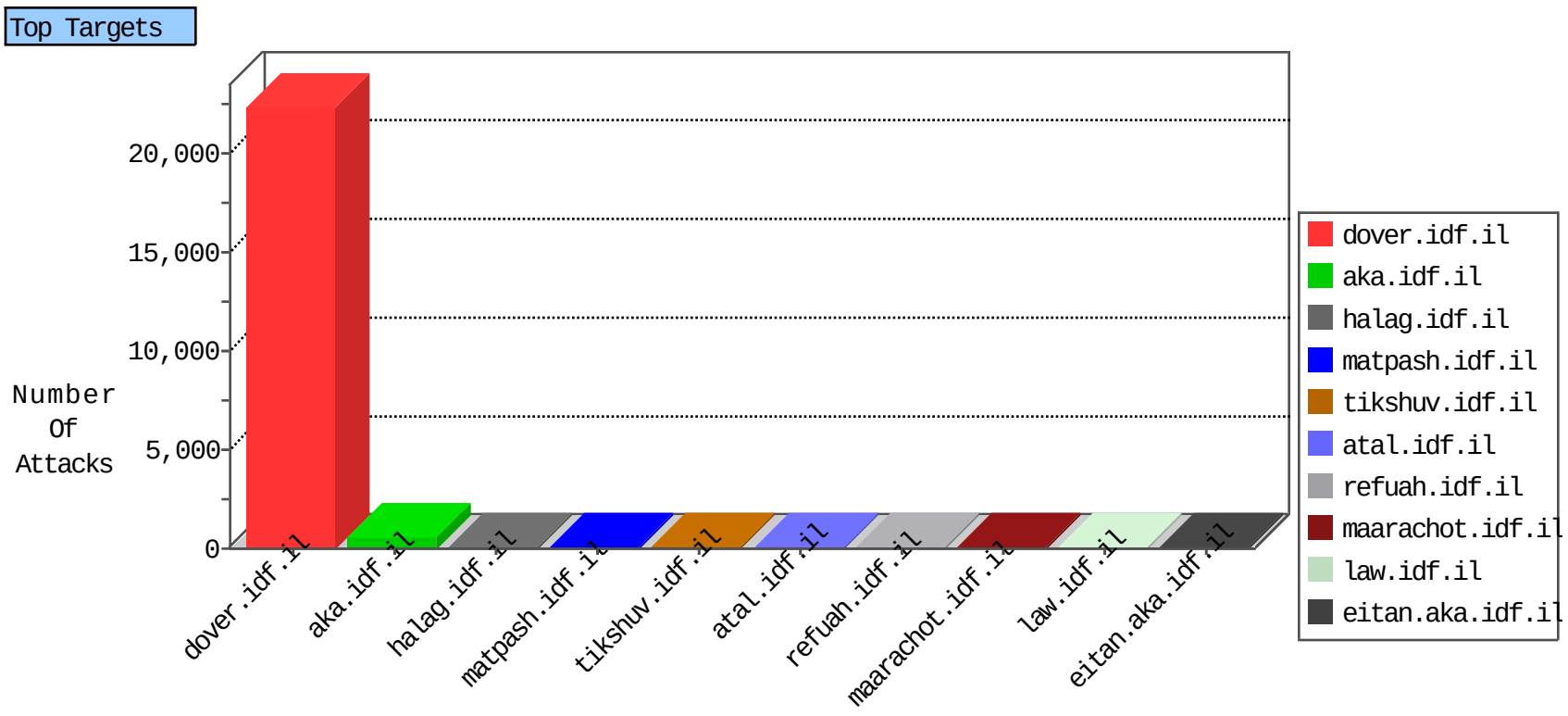
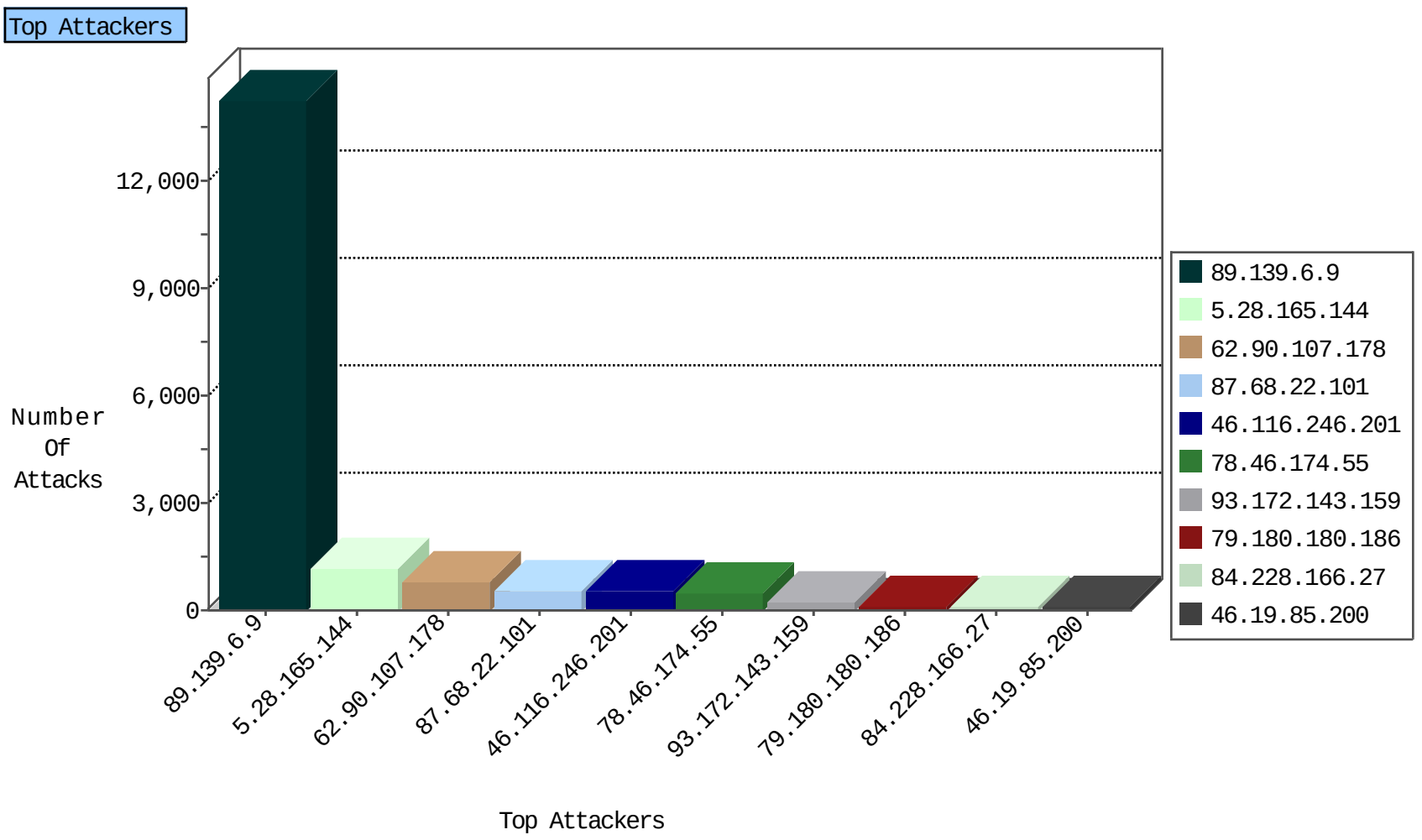
04-17-2015-19:03:02 to 04-17-2015-20:03:02

IDF Under Attack
04-17-2015-19:03:02

Top Targets



Top Attackers



04-17-2015-19:03:02 to 04-17-2015-20:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.66.80.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
180.182.183.236	Korea, Republic of	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
185.11.146.164	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
79.170.49.99	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.99	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-17-2015-19:03:02 to 04-17-2015-20:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.111.240.252	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.117.19.161	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.66.80.127	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.188.75	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
119.30.32.34	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.65.91.19	Israel	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	147.237.76.86	navy.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
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
190.230.224.68	Argentina	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.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
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
23.235.228.162	United States	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.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
46.19.85.41	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-17-2015-19:03:02 to 04-17-2015-20:03:02

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
46.121.99.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.157	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.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
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
107.170.7.139	United States	147.237.77.243	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
43.255.191.162	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
98.143.148.107	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
87.229.23.170	Hungary	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
109.66.24.253	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.254.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1
43.255.191.162	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
98.143.148.107	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
87.229.23.170	Hungary	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
87.69.205.232	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.162	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
79.178.148.224	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.162	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.254.221	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1

04-17-2015-19:03:02 to 04-17-2015-20:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.6.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14237
5.28.165.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1177
62.90.107.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	801
87.68.22.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
46.116.246.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	504
93.172.143.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	217
79.180.180.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111
84.228.166.27	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
46.19.85.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	91
46.19.85.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
217.66.238.9	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
89.138.238.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
66.249.67.157	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
5.22.129.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
176.12.150.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
109.253.157.6	Israel	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
176.12.140.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
37.142.58.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
79.179.58.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
85.65.7.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.85.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.253.158.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.253.158.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.186.181.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
46.19.86.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
176.12.140.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
79.180.179.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
24.203.59.13	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
46.121.99.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
176.12.143.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
181.141.13.151	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.253.147.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.253.136.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.19.85.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
82.80.164.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.150.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
109.253.143.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
2.52.170.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
109.253.136.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26

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	Distributed Abnormally Long Request	Block	225
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	225
79.178.0.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
41.79.76.33	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
192.99.32.47	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
148.251.124.155	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
5.153.10.228	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
178.18.124.109	United Kingdom	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.66.183.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
85.158.203.121	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
50.193.224.117	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
85.250.21.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
172.56.30.57	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
79.170.44.141	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
69.16.243.169	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
89.138.87.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
79.180.166.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
209.91.107.250	Canada	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.18.124.109	United Kingdom	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
5.153.10.228	Netherlands	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
109.66.80.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
85.65.111.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.176.11.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
91.200.12.27	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/3079.pdf/trackback/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	1
79.181.183.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il./webresource.axd	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
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	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
85.158.203.121	Netherlands	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
50.193.224.117	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.177.167.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
72.71.172.158	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter b6e681f8 in www.aka.idf.il/main/home/default.aspx	None	1
107.170.7.139	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on //	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
84.108.248.152	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
23.235.228.162	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
188.165.15.206	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.129.224	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1

04-17-2015-19:03:02 to 04-17-2015-20:03:02