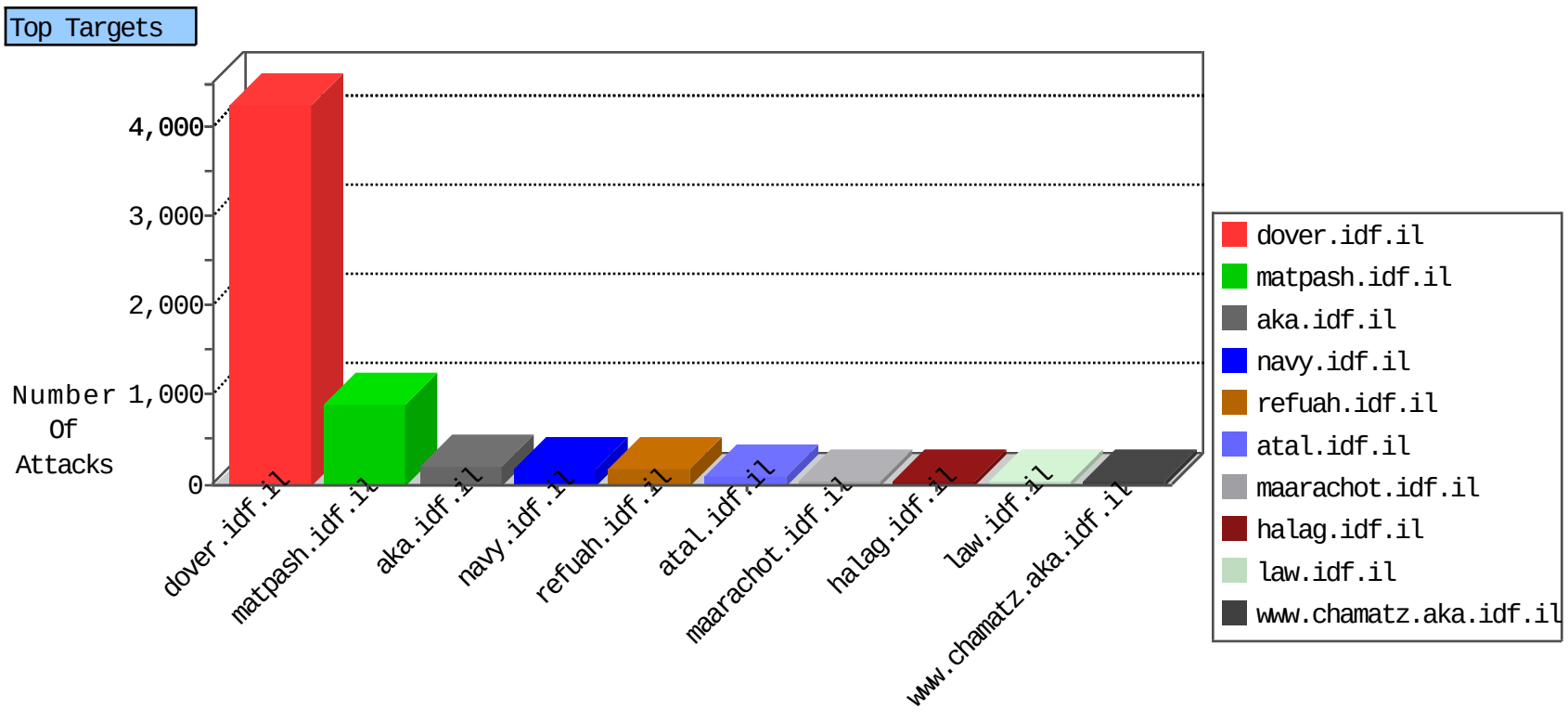
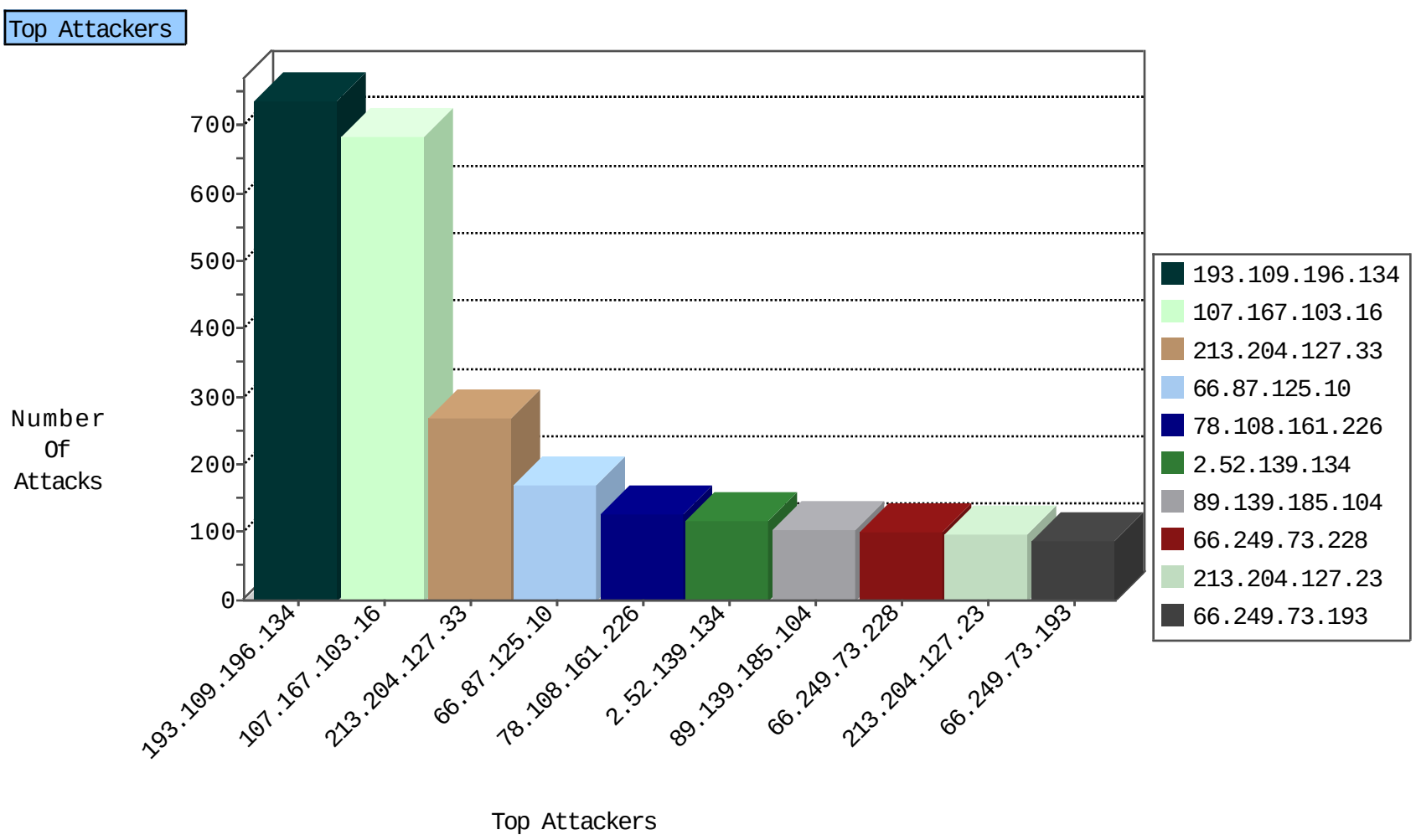
04-09-2015-20:03:05 to 04-09-2015-21:03:05

IDF Under Attack
04-09-2015-20:03:05

Top Targets



Top Attackers



04-09-2015-20:03:05 to 04-09-2015-21:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	102
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	89
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	85
79.180.15.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	64
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	55
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	54
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	44
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	38
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	38
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	34
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	33
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
84.110.213.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
37.142.162.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
107.167.103.16	United States	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	15
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.93.243	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.73.223	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.75.103	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.78.213	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
192.168.1.107		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6

04-09-2015-20:03:05 to 04-09-2015-21:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.137.216.152	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.32.203.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
93.120.27.62	Romania	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.96.154.140	Turkey	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	1
93.120.27.62	Romania	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.231	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-09-2015-20:03:05 to 04-09-2015-21:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
37.237.152.85	Iraq	147.237.77.216	dover.idf.il	ET SCAN WhatWeb Web Application Fingerprint Scanner Default User-Agent Detected	2
109.64.164.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.146.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.204.127.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
175.139.219.194	Malaysia	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.72.228.72	Indonesia	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
213.26.203.138	Italy	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	Indonesia	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
175.139.219.194	Malaysia	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
128.199.254.26	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.69.94.13	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
114.112.90.54	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.190.60	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	Indonesia	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2015-20:03:05 to 04-09-2015-21:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
193.109.196.134	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	738
107.167.103.16	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	670
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	258
66.87.125.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	171
2.52.139.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	103
213.204.127.23	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
37.228.105.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
84.228.247.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
147.21.8.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
37.26.146.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
105.210.11.21	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.67.177.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
46.19.85.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
46.43.75.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
84.137.216.152	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
2.54.173.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
46.19.86.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	35
78.108.161.226	Lebanon	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	34
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	34
93.173.128.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.64.164.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
197.46.231.40	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
92.225.8.69	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.141.110	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.210.225.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
93.172.51.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
176.12.148.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
50.87.144.145	United States	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
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.237.152.85	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
176.12.142.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
41.233.89.26	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
77.250.91.19	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.126	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.230.22.45	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
77.127.3.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
165.123.49.218	United States	147.237.77.216	dover.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
62.173.9.233	Malta	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	16
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15

04-09-2015-20:03:05 to 04-09-2015-21:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	2
37.26.147.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.59.29.19	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
159.20.182.223	Italy	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
62.173.9.233	Malta	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giy.com	Block	1
84.228.14.5	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
41.238.223.217	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
176.12.141.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1
87.69.28.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
46.19.85.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
176.12.145.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
37.26.147.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
93.173.33.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-en/idfgdover.aspx	Block	1
46.19.85.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
188.120.148.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
93.173.155.150	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5	Block	1
46.19.85.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method .NET_SessionId=3bxeb23tgkoq0255yc5gy245 in URL	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/c	Block	1
84.137.216.152	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

04-09-2015-20:03:05 to 04-09-2015-21:03:05