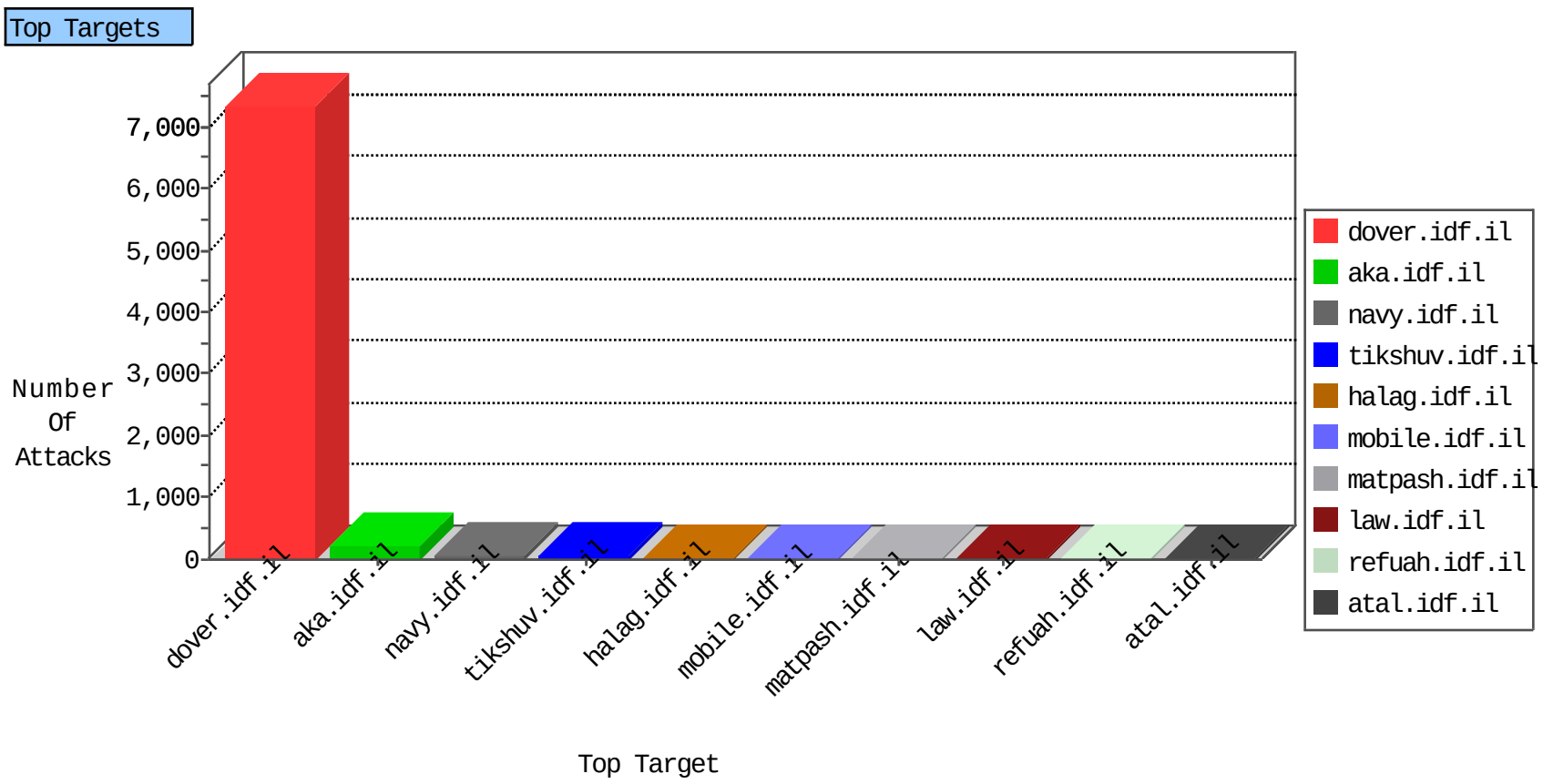
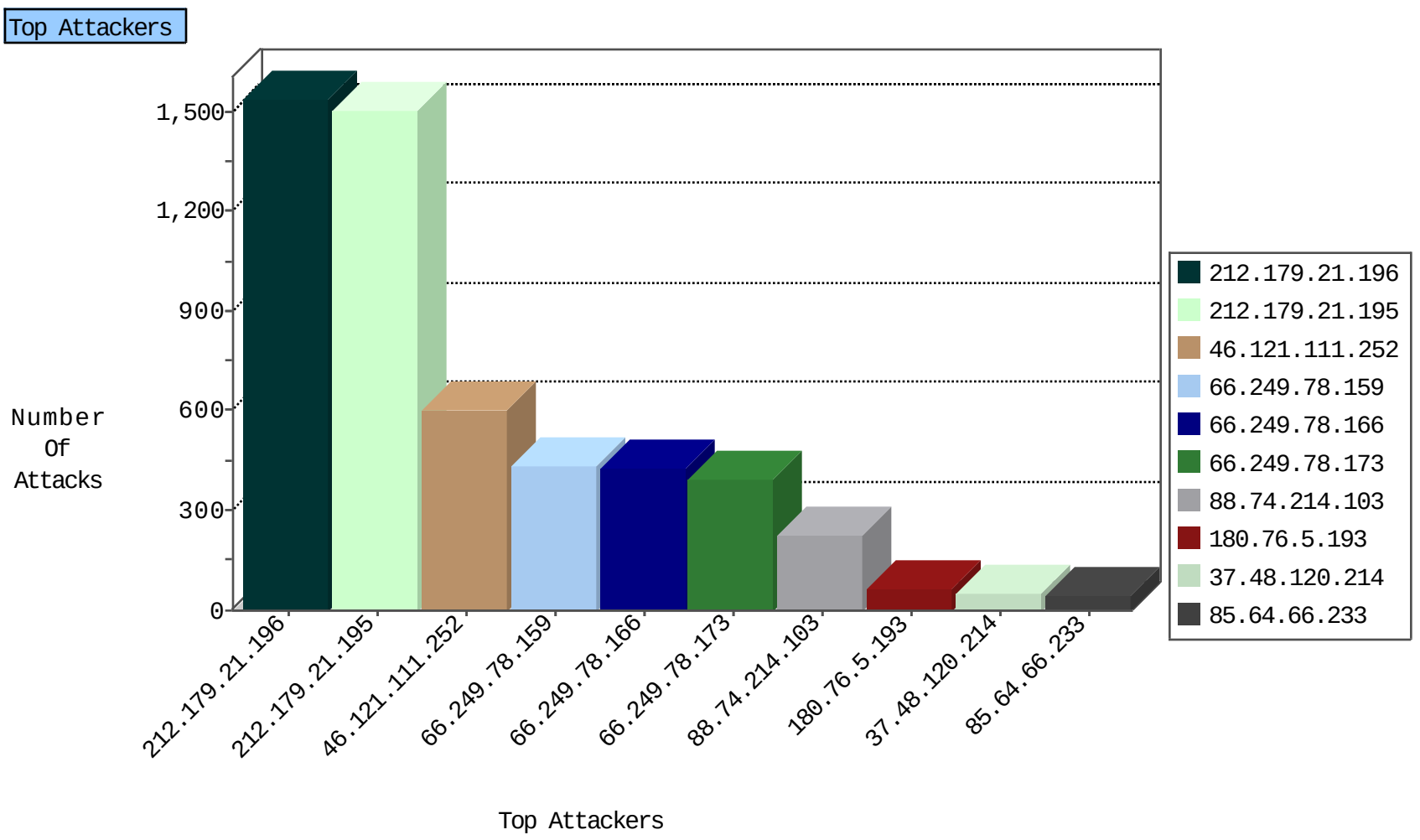
05-01-2015-13:03:05 to 05-01-2015-14:03:05

IDF Under Attack
05-01-2015-13:03:05

Top Targets



Top Attackers



05-01-2015-13:03:05 to 05-01-2015-14:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.66	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4256
66.249.64.64	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	888
66.249.64.4	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	90
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
87.68.226.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
66.249.81.199	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
212.179.21.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.216.41	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
66.249.81.196	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1
81.218.8.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
180.210.234.87	China	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

05-01-2015-13:03:05 to 05-01-2015-14:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	67
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.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
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
79.182.63.98	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.121.90.74	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.186.92.164	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.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
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.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

05-01-2015-13:03:05 to 05-01-2015-14:03:05

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	5
61.160.224.130	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.210.234.87	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.210.234.87	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.160.6.194	South Africa	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.92.202.251	Philippines	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
41.160.6.194	South Africa	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.40	Netherlands	147.237.77.74	law.idf.il	ET WEB_SERVER Muieblackcat scanner	1
202.71.25.29	India	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.200	United States	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.234.87	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.234.87	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.234.87	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.210.234.87	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.160.6.194	South Africa	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
119.92.202.251	Philippines	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
41.160.6.194	South Africa	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
86.174.116.244	United Kingdom	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.234.87	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
180.210.234.87	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1

05-01-2015-13:03:05 to 05-01-2015-14:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1540
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1504
46.121.111.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	606
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	334
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	330
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	292
88.74.214.103	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
85.64.66.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
46.117.43.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
83.149.8.9	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
176.106.227.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
79.182.145.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
2.54.144.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
87.68.64.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.64.26.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
46.19.85.44	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
95.86.66.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
2.54.137.103	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
84.229.0.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
213.151.35.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.228.173.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
77.125.73.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
79.180.181.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.57.81.41	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.86.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
212.117.157.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
84.228.27.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
93.172.5.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.75.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.121.133.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	20
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	9
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	8
157.55.39.91	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
157.55.39.106	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	6
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
2.54.137.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.137.103	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	3
84.228.119.73	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.173.17.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.106	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	2
157.55.39.90	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	2
66.249.69.86	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
66.249.64.98	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/30012011masaiyot.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.13	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.247.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	1
79.182.96.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.67.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
31.13.100.115	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8350-he	Block	1
141.212.122.34	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.140	Block	1
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58562&docid=35711	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.19	Block	1
84.228.237.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1404-he/atal.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-index03.stm	Block	1
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	1
66.249.64.2	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13229-en/dover.aspx forcerecrawl: 0	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
89.248.171.40	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/muieblackcat	Block	1
80.162.72.66	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.67.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	1
188.165.15.110	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim	Block	1