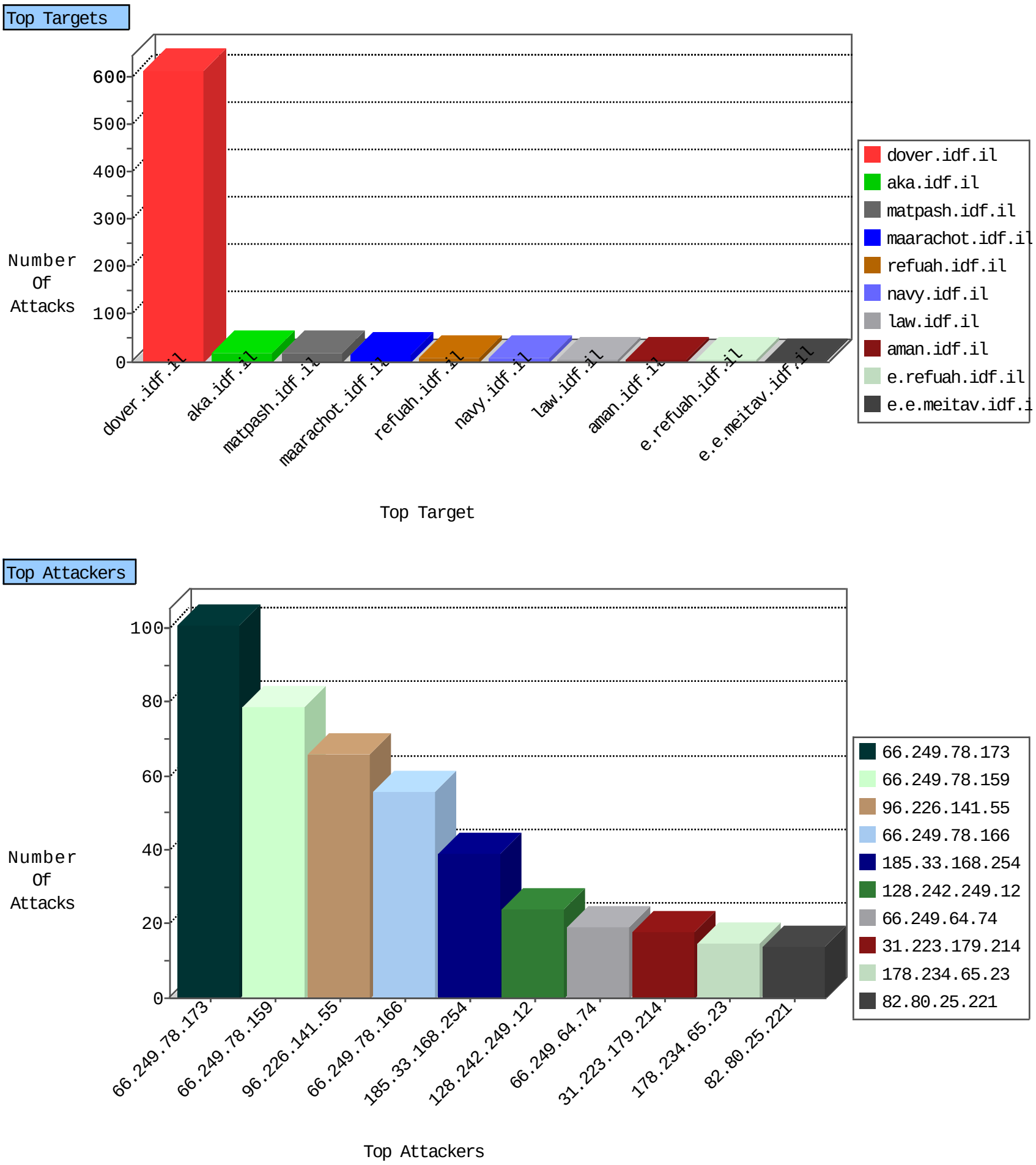
04-16-2015-04:03:08 to 04-16-2015-05:03:08

IDF Under Attack
04-16-2015-04:03:08



04-16-2015-04:03:08 to 04-16-2015-05:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2198
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	438
66.249.79.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	66
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9

04-16-2015-04:03:08 to 04-16-2015-05:03:08

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	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	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	147.237.76.176	test.ncore.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	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
94.23.6.131	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
96.44.189.101	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

04-16-2015-04:03:08 to 04-16-2015-05:03:08

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	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
103.27.236.108	Vietnam	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
103.27.236.108	Vietnam	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
103.6.87.143	India	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
103.6.87.143	India	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
106.187.90.86	Japan	147.237.76.148	gqcenter.aka.idf.il	GPL SCAN superscan echo	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.158.233.62	Norway	147.237.76.42	refuah.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
103.27.236.108	Vietnam	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
103.6.87.143	India	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
103.6.87.143	India	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
103.6.87.143	India	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

04-16-2015-04:03:08 to 04-16-2015-05:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	98
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
96.226.141.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
178.234.65.23	Russian Federation	147.237.77.170	maarachot.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	14
31.223.179.214	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
189.20.220.92	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
173.216.108.169	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
65.55.218.46	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.10.99.200	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
191.181.108.194	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
119.56.115.47	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
91.121.75.9	France	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	5
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	5
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
107.72.164.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.186.4.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
75.110.192.214	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.78	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
91.121.75.46	France	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	4
70.39.187.108	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	4
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.186.32.218	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
106.241.54.5	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
125.175.81.14	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.67.96.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
185.33.168.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
109.186.32.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
91.121.78.198	France	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	3
72.69.250.183	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
162.234.26.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.23	Israel	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
69.171.237.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.0.34.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
68.197.45.0	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.78	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.79.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
188.165.15.43	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.133	Block	1
119.73.170.114	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.79.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8386-he/navy.aspx	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
188.165.15.117	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19484-he/idfgdover.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/navy/navy6.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0227-2.stm	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyusÃ–â€¢ Ã–â€˜Ã–â€"Ã–Â¨Ã–â€¢	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
66.249.79.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8701-he/navy.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19075-he/dover.aspx	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	1
66.249.79.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
207.46.13.138	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
66.249.65.14	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
157.55.39.206	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx,	Block	1
66.249.79.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/default.asp	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx	Block	1
66.249.79.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/templates/homepage/homepage.aspx	Block	1
213.158.233.62	Norway	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/cgi-bin/hello	Block	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170//	Block	1
178.234.65.23	Russian Federation	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 178.234.65.23	Block	1
66.249.79.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9825-he/refuah.aspx	Block	1
207.46.13.78	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/iturim/asp/results.asp	None	1