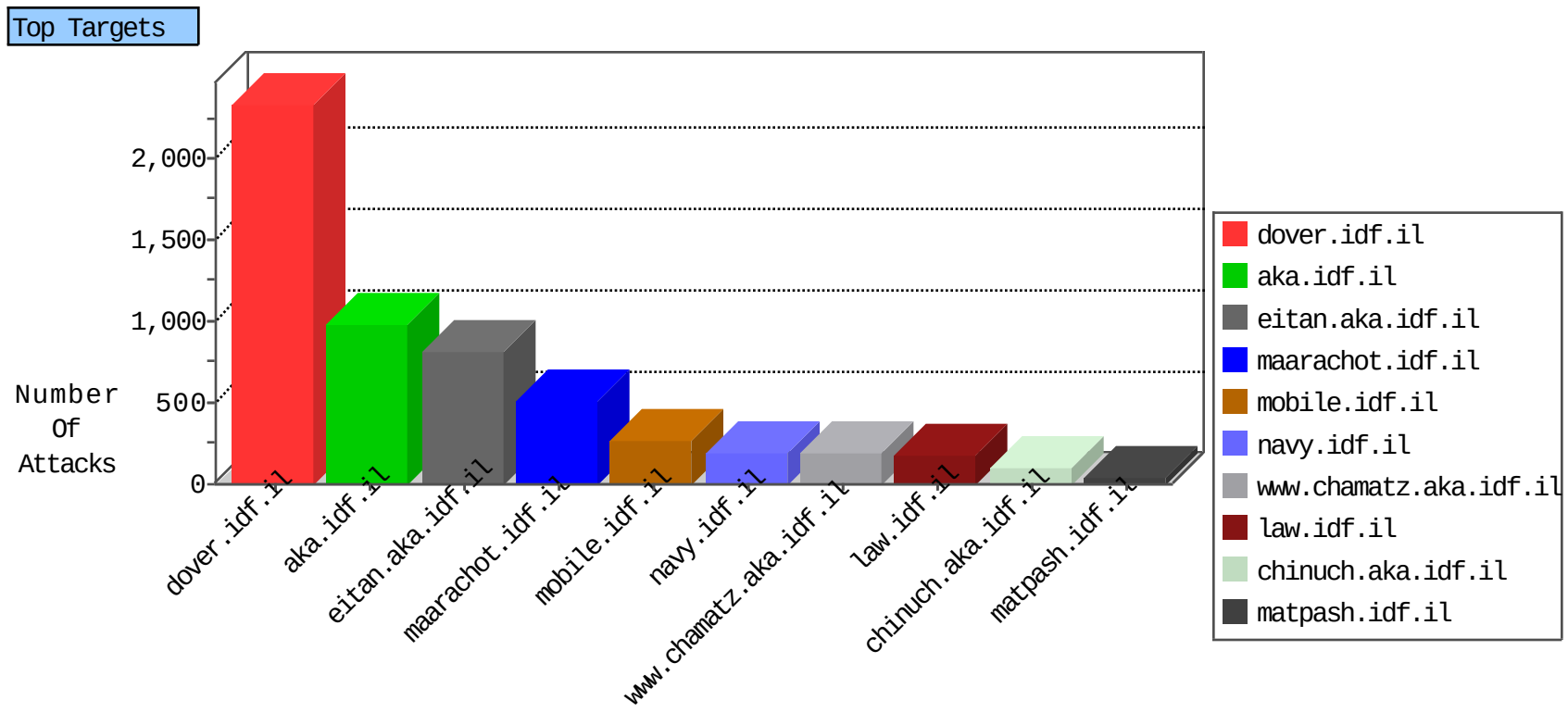
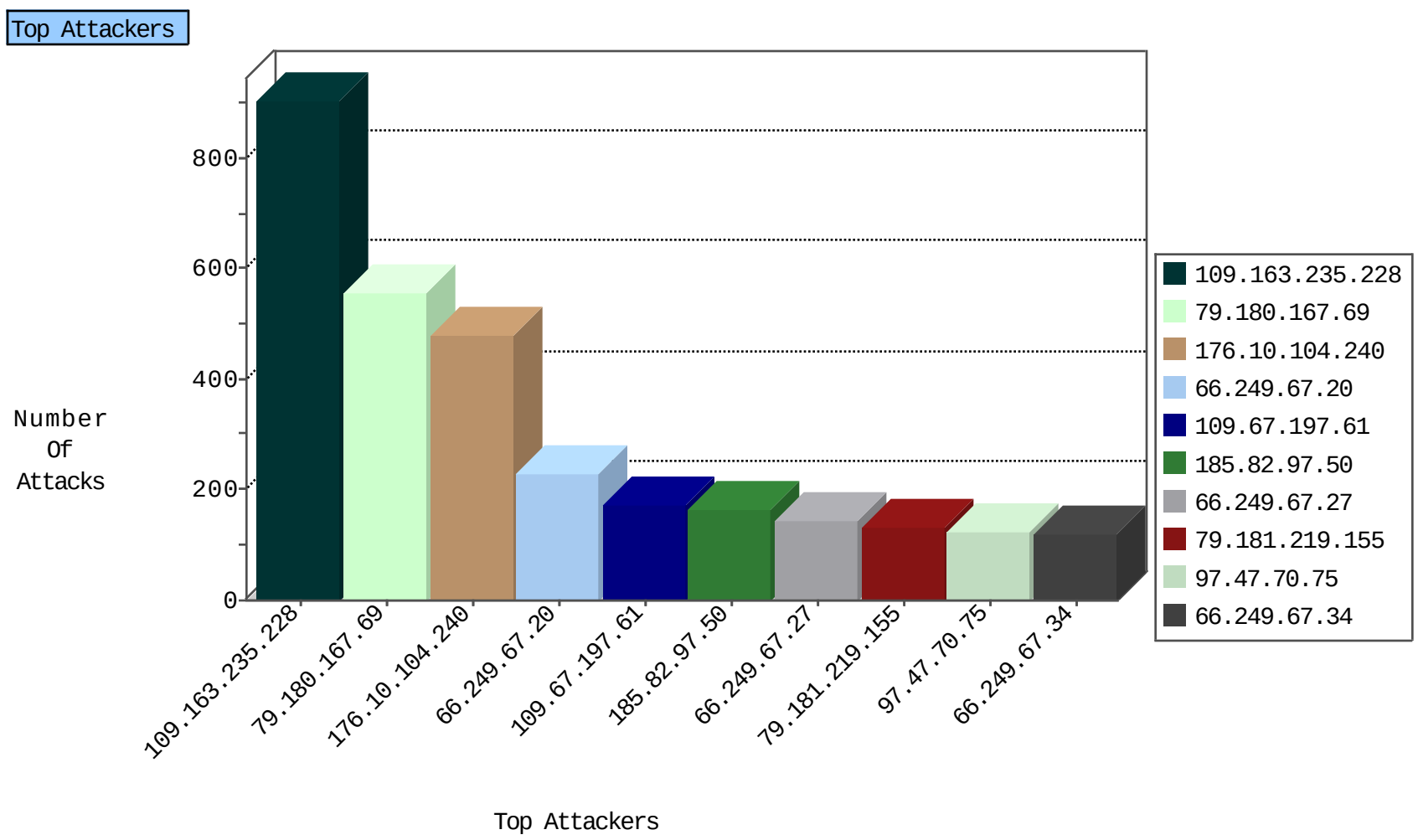
11-01-2015-01:04:04 to 11-01-2015-02:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-01-2015-01:04:04 to 11-01-2015-02:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	19933
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	18801
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	16571
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14155
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8846
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7953
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4775
109.163.235.228	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3885
97.47.70.75	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2785
173.252.89.56	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2042
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1962
31.171.194.182	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1619
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1604
176.10.104.240	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1456
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1387
64.233.172.155	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1223
66.249.65.22	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1159
78.40.176.243	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1071
37.26.146.251	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	852
66.249.75.2	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	633
66.249.75.52	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	547
64.233.172.163	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	515
185.82.97.50		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	451
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	380
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	273
173.63.97.48	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	261
63.230.162.251	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	256
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	232
66.249.75.44	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	127
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	59
66.102.8.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
46.19.86.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	38
66.249.75.106	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	34
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	28
46.19.85.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
66.102.8.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
97.47.70.75	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.121.77.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
109.64.107.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
85.65.8.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
46.116.148.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
149.78.195.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.64.107.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
64.233.172.171	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
176.10.104.240	Switzerland	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5
109.64.107.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
69.161.99.220	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.142.64.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.228.165.100	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

11-01-2015-01:04:04 to 11-01-2015-02:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.101.165	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
105.156.49.244	Morocco	147.237.77.216	dover.idf.il	C067: HTTP: attempt to access .config page	Block	2

11-01-2015-01:04:04 to 11-01-2015-02:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.75.68	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
111.93.198.54	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -f -sS	1
104.238.152.55	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 2048	1
104.192.0.20	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
193.107.16.206	147.237.8.27	Russian Federation	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
14.215.130.20	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
169.57.5.20	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
111.93.198.54	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.152.55	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 4096	1
104.238.152.55	147.237.77.205		prisha.idf.il	ET SCAN NMAP -f -sS	1
41.67.78.4	147.237.0.33	Egypt	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
186.46.61.122	147.237.76.30	Ecuador	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.93.198.54	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 2048	1

11-01-2015-01:04:04 to 11-01-2015-02:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.180.167.69	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	348
109.163.235.228	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	171
185.82.97.50		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
97.47.70.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
176.10.104.240	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	70
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
173.63.97.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
176.10.99.206	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	52
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
2.54.155.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
176.10.104.240	Switzerland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
95.86.104.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.181.219.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
176.13.9.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
95.221.254.71	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
31.171.194.182	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
95.86.73.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
79.180.167.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
78.40.176.243	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
194.228.20.175	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
24.131.6.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
63.230.162.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.130.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
173.174.203.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
84.226.110.21	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
98.80.223.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.10.104.240	Switzerland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.107.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.116.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
47.16.240.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	224
176.10.104.240	Switzerland	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
79.180.167.69	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	165
109.67.197.61	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.67.197.61	Block	150
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	105
79.181.219.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Distributed NULL Character in Parameter Value	Block	60
46.116.236.218	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	59
80.246.136.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.163.235.228	Block	30
46.117.181.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
82.166.120.183	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	30
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Distributed Double URL Encoding	Block	30
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
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	30
66.249.75.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	15
149.88.67.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	15
176.10.104.240	Switzerland	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/eitan.aspx	None	15
68.64.169.226	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
109.67.197.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1640.jpg	Block	15
79.137.225.218	Russian Federation	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/a2billing/customer/iridium_threed.php	Block	15
213.61.149.100	Germany	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
82.166.120.183	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 82.166.120.183	Block	15
176.12.144.40	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.163.235.228	Block	15
47.16.240.234	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$txtSearch in www.idf.il/1283-en/dover.aspx	Block	15
213.61.149.100	Germany	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/1.1	Block	15
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
176.10.104.240	Switzerland	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name <w	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat_id in www.aka.idf.il/iturim/asp/results.asp	None	15
5.28.183.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
176.12.144.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparTeuda' in www.aka.idf.il/main/sachar/default.aspx	None	15
66.249.64.139	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	15
109.163.235.228	Romania	147.237.72.166	aka.idf.il	Illegal Parameter Encoding search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	None	15
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
23.94.170.143	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	15
82.166.120.183	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	15
207.46.13.5	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	15