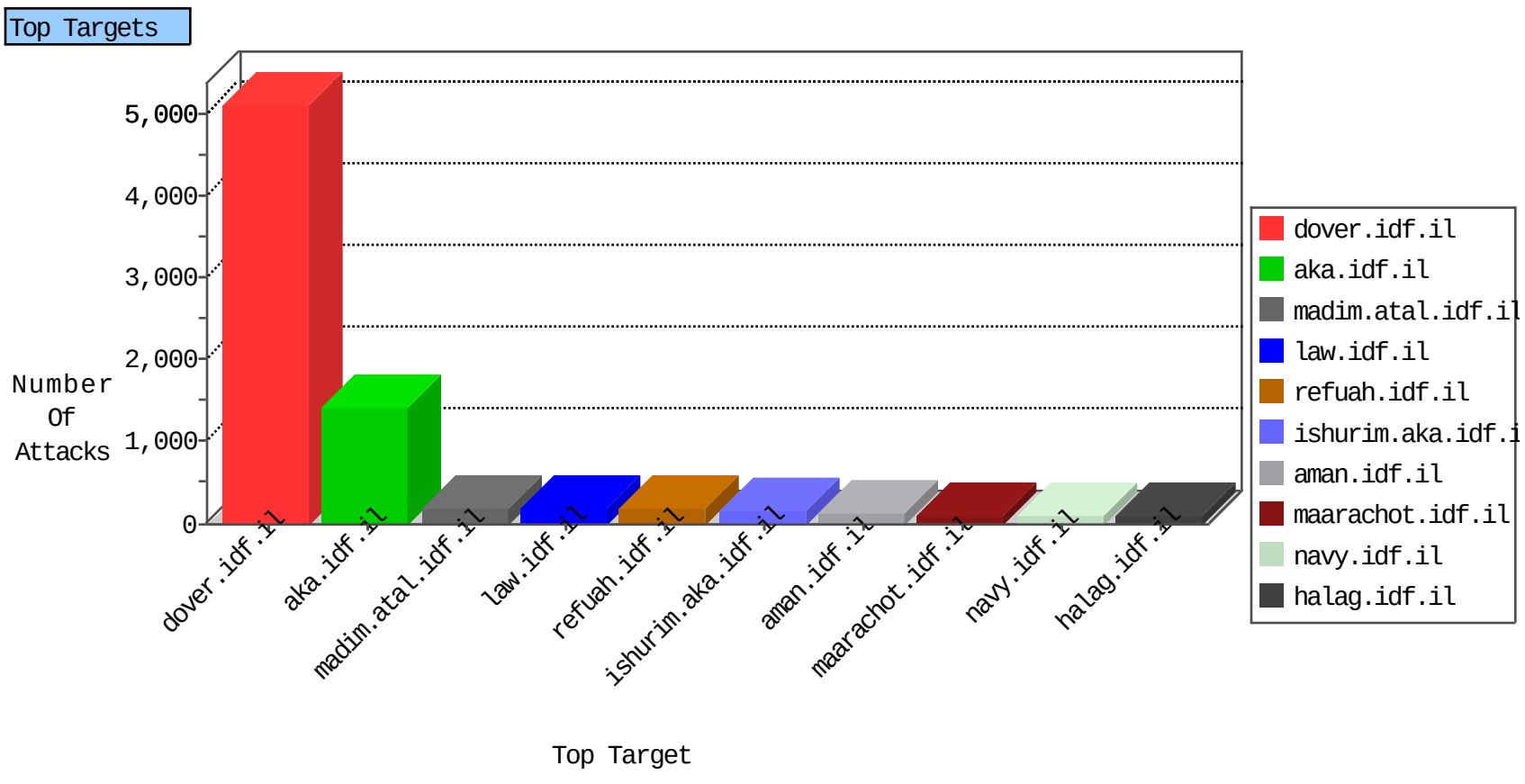
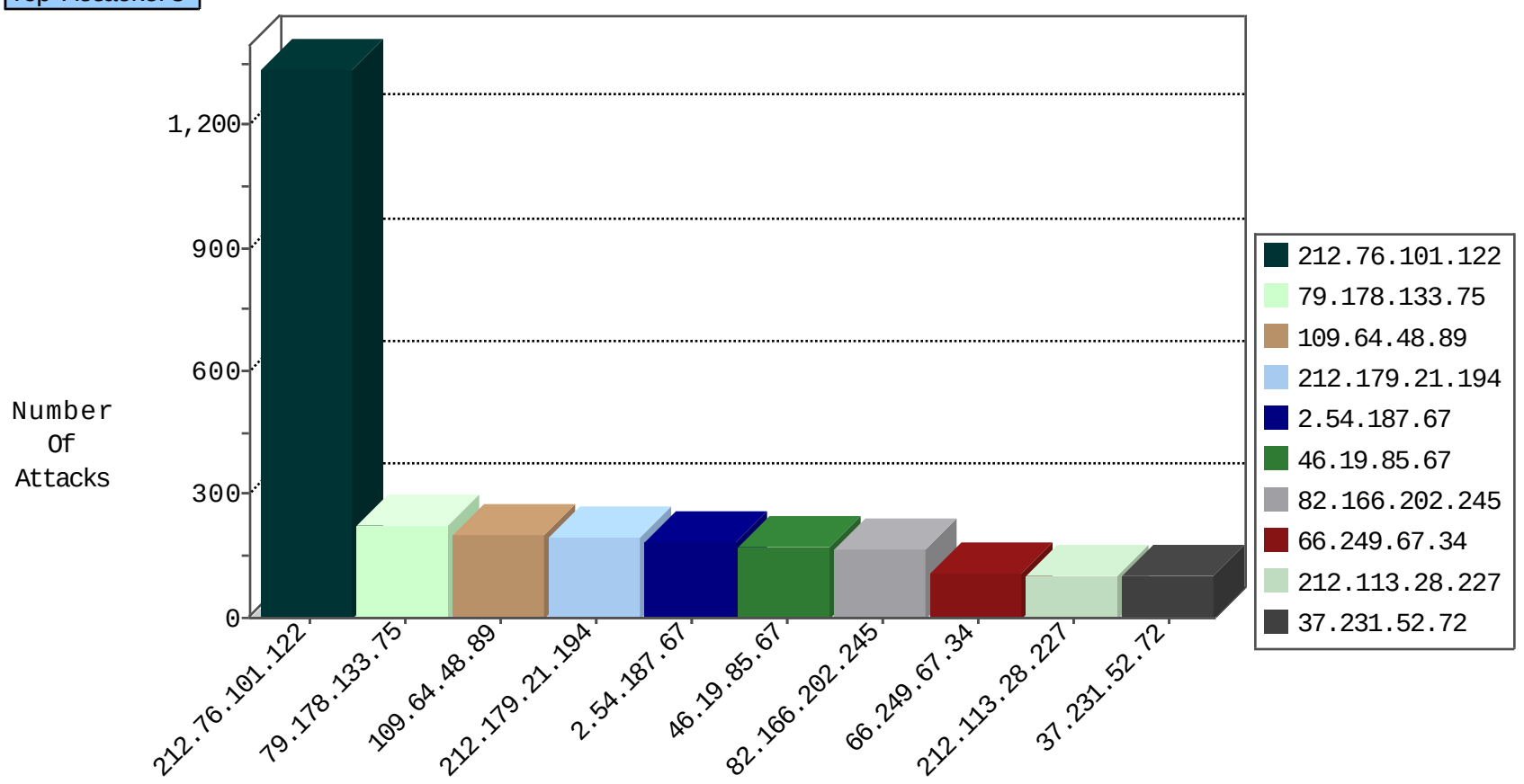
10-28-2015-14:04:09 to 10-28-2015-15:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-28-2015-14:04:09 to 10-28-2015-15:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	TCP handshake violation, first packet not syn	drop	49450
89.138.228.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6096
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4812
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4129
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2724
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2575
66.249.67.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1571
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1413
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	992
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	622
66.249.74.91	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	506
37.26.146.169	Israel	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	494
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	394
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	338
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	323
66.249.64.151	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	321
66.249.67.25	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	318
151.80.31.112	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	302
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	295
212.25.84.200	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
79.180.172.95	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	94
46.19.86.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	51
2.54.183.213	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	47
84.108.60.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
66.249.74.81	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	27
2.54.20.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
5.22.129.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
46.19.86.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
212.235.8.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
82.166.202.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
212.117.136.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
2.54.39.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
62.90.131.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
85.65.23.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
66.249.74.93	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	11
82.166.81.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
82.166.81.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.65.32.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
194.90.107.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.178.185.67	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
66.249.69.16	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	6
109.67.111.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.150.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.111.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
85.64.69.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.111.223	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6

10-28-2015-14:04:09 to 10-28-2015-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.135.63.82	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
93.89.16.110	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
66.135.63.82	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
93.89.16.110	Turkey	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

10-28-2015-14:04:09 to 10-28-2015-15:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.135.63.82	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
93.89.16.110	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	5
77.125.127.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.166.77.147	147.237.76.196	Austria	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
194.166.77.147	147.237.0.34	Austria	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.185.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.150.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.99.190.204	147.237.77.74	Latvia	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.34.160	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.139.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.166.77.147	147.237.76.200	Austria	eitan.aka.idf.i	ET SCAN Potential SSH Scan	1
77.126.151.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.166.77.147	147.237.76.197	Austria	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.159	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
194.166.77.147	147.237.76.176	Austria	test.ncore.idf.i	ET SCAN Potential SSH Scan	1
66.102.8.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.136.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.186.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.61.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.31.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.7.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.166.77.147	147.237.76.198	Austria	e.yohalan.idf.i	ET SCAN Potential SSH Scan	1

10-28-2015-14:04:09 to 10-28-2015-15:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1337
2.54.187.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
212.113.28.227	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
37.231.52.72	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
176.13.3.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
82.166.202.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
37.187.7.74	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
77.42.241.106	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
148.177.129.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
79.181.27.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.69.16	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
37.26.148.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
82.166.202.245	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	30
66.249.69.128	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.160.240.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
145.228.59.67	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.120.231.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
196.14.16.66	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
64.21.147.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
82.166.81.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
83.83.27.65	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.77.49.231	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.126.236.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
85.65.23.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.178.185.67	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.39.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
213.204.101.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.58.175		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	19
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
194.90.107.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.142.168.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
109.65.32.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.22.129.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.13.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.133.75	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	112
79.178.133.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	112
109.64.48.89	Israel	147.237.0.19	madim.atal.idf.i	PHP Attempt	Block	100
109.64.48.89	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/ajax/updatestatus.php	Block	100
82.166.202.245	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	83
212.199.97.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.97.194	Block	70
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	57
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	43
37.77.49.231	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	42
84.228.235.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	42
85.65.176.25	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	42
85.65.176.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	42
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	Block	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
2.54.43.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	29
149.78.48.122	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.67	Block	28
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	28
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.67	Block	28
176.12.143.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.67	Block	28
217.194.199.74	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.67	Block	28
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	25
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	15
97.88.213.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	15
62.219.209.229	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
185.45.192.227	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/__	Block	15
5.22.129.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
2.54.27.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
79.180.199.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	15
109.66.81.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
62.128.48.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15
185.45.192.227	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/__	Block	15
2.54.51.82	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	14
207.244.67.20	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lohsangiyus	Block	14
176.13.8.56	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
192.188.230.2	United States	147.237.76.86	navy.idf.il	Malformed URL	Block	14
85.65.192.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
82.80.85.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	14
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	14
151.80.31.123	Italy	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	14
66.249.67.79	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	14