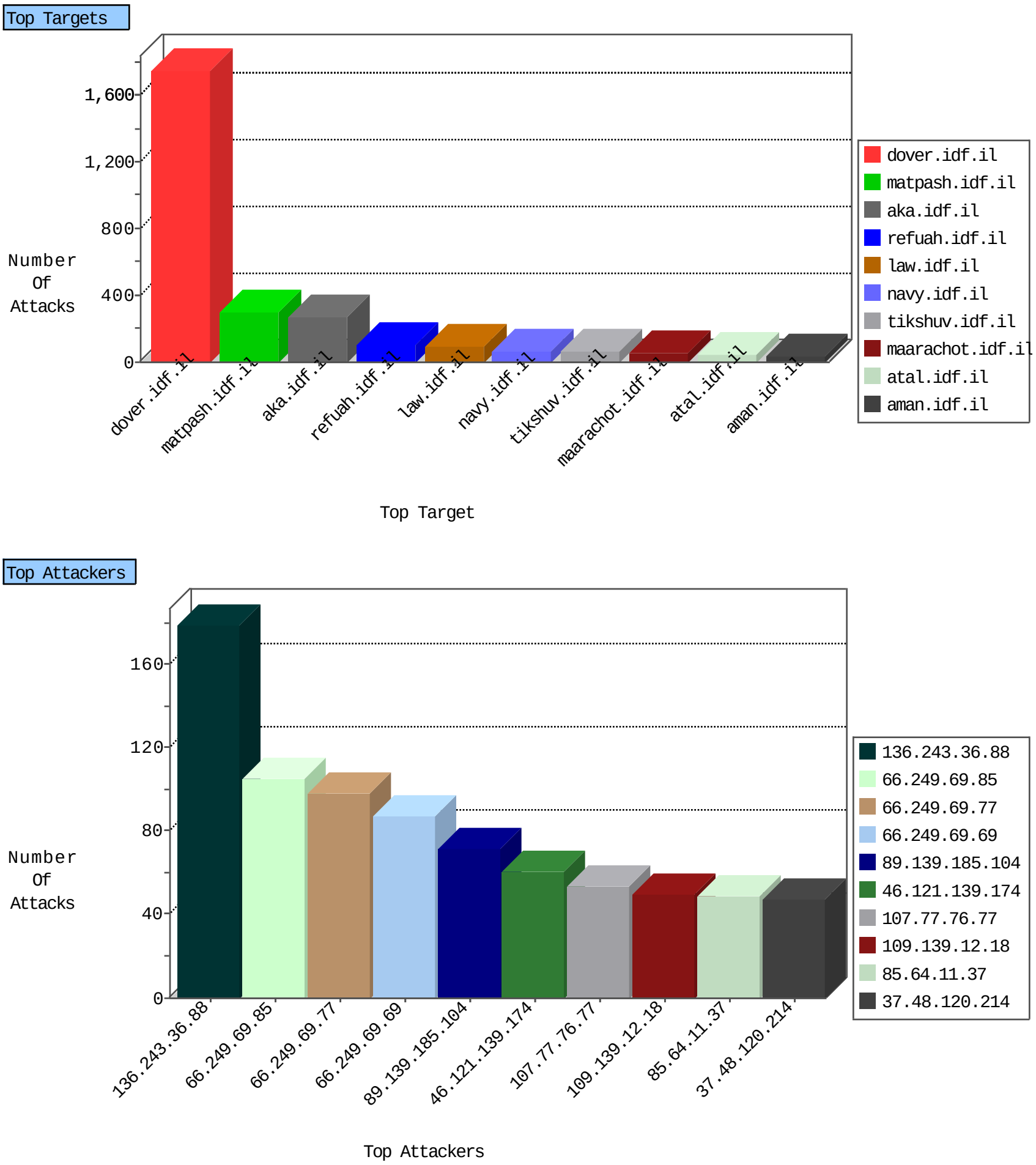
04-10-2015-23:03:09 to 04-11-2015-00:03:09

IDF Under Attack
04-10-2015-23:03:09



04-10-2015-23:03:09 to 04-11-2015-00:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.85.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2587
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	105
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	98
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	87
85.64.121.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	32
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	23
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	17
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.64.83	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	11
66.249.93.162	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.93.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
130.133.8.114	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.69.97	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	8
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	8
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
5.29.99.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6

04-10-2015-23:03:09 to 04-11-2015-00:03:09

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	25
212.34.12.166	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
2.52.59.84	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
178.8.197.222	Germany	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.52.56.54	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.164.226	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.87.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
192.116.188.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.64.9.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-23:03:09 to 04-11-2015-00:03:09

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	25
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
77.126.31.191	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
119.97.231.102	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 3072	1
119.97.231.102	China	147.237.76.30	himush.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
94.102.56.231	Netherlands	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
119.97.231.102	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
193.107.17.72	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.131.168	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
91.217.90.49	Ukraine	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
80.178.163.185	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

04-10-2015-23:03:09 to 04-11-2015-00:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
136.243.36.88	Germany	147.237.72.166	aka.idf.il	SAM rule	drop	drop	178
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
46.121.139.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
107.77.76.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
109.139.12.18	Belgium	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
85.64.11.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
95.105.233.90	Slovakia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.186.154.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
83.163.161.84	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.85.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
85.250.57.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
84.108.236.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
87.61.224.197	Denmark	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
41.141.18.153	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
37.231.129.223	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.67.86.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
134.134.139.74	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.253.135.68	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.135.179	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
134.134.137.75	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.116.127.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
185.21.120.29	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
212.34.12.121	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
84.229.174.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
109.253.145.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
134.134.137.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.141.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
85.250.86.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.149.182	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
85.64.121.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.253.139.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
75.74.223.253	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
109.253.140.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
134.134.139.78	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
85.250.133.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.142.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.65.108.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
70.94.201.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8

04-10-2015-23:03:09 to 04-11-2015-00:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	3
79.178.163.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	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
188.138.17.205	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
77.237.138.51	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
84.108.69.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
65.49.17.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org	Block	1
198.185.18.207	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&quot	Block	1
84.109.105.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
69.12.66.241	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
79.180.162.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
201.173.186.88	Mexico	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1506-en/dover.aspx	Block	1
87.69.231.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/englishlocales.stm	Block	1
80.178.163.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.67.69	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for list.ips.gov.il/	Block	1
77.93.59.1	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
190.72.37.195	Venezuela	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
80.230.125.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
2.54.174.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-10-2015-23:03:09 to 04-11-2015-00:03:09