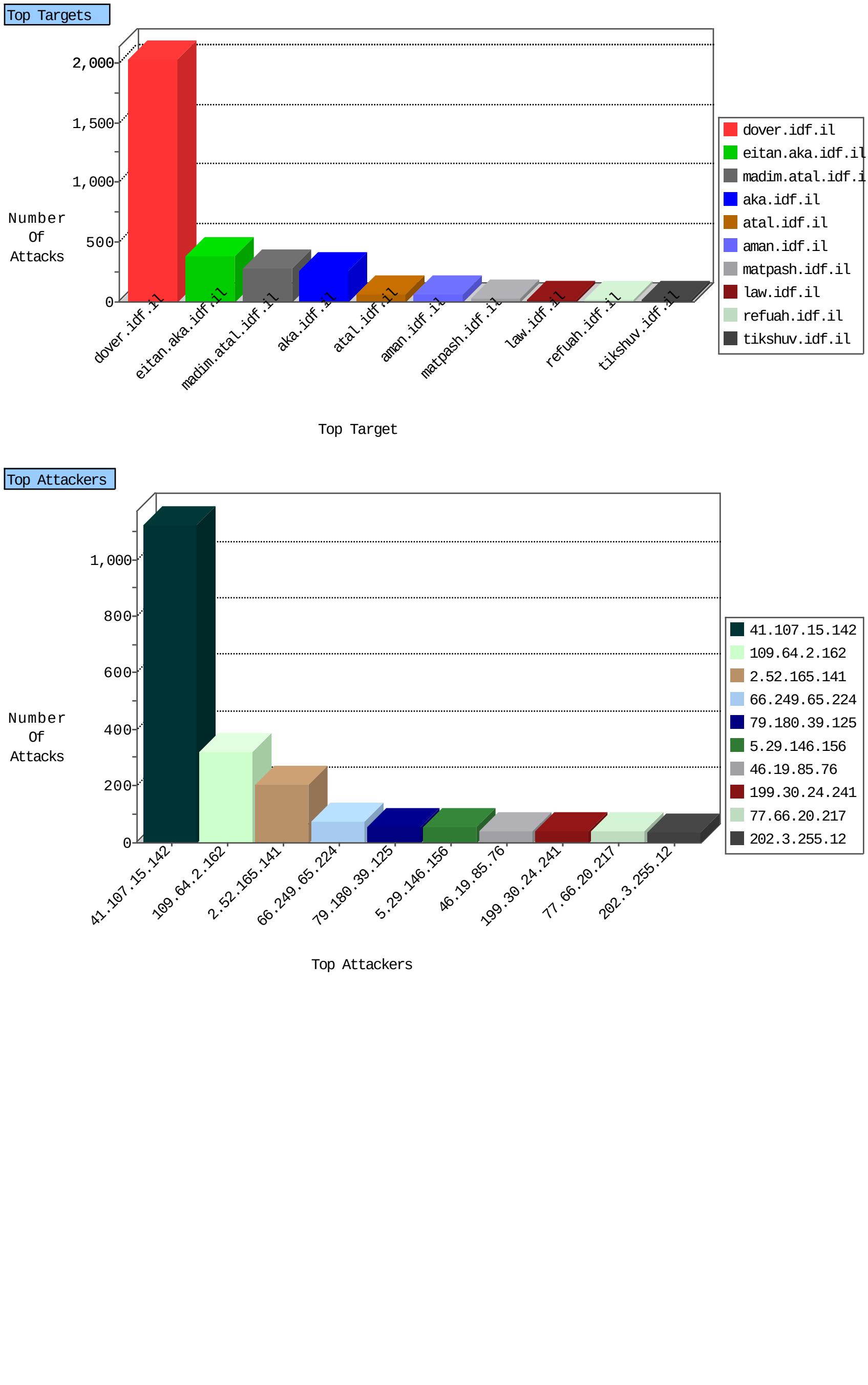
11-20-2015-17:04:04 to 11-20-2015-18:04:04

IDF Under Attack Daily Report



11-20-2015-17:04:04 to 11-20-2015-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.39		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	128
84.108.97.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
204.93.154.198	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	11
93.172.60.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
77.125.138.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.183.111.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.22.134.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.163.148.203	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.163.148.203	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

11-20-2015-17:04:04 to 11-20-2015-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.31.44.3	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	12
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	2
5.10.68.254	Netherlands	147.237.76.42	refuah.idf.i	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
84.184.221.178	Germany	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
5.10.68.254	Netherlands	147.237.76.42	refuah.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	1
178.214.84.54	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

11-20-2015-17:04:04 to 11-20-2015-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.107.15.142	147.237.77.216	Algeria	dover.idf.il	Admin login page scan - Havij	24
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
41.107.15.142	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP adminlogin access	7
41.107.15.142	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	4
41.107.15.142	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
178.214.84.54	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL Injection - Select From	1

11-20-2015-17:04:04 to 11-20-2015-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	726
109.64.2.162	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	321
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
79.180.39.125	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
5.29.146.156	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
199.30.24.241	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
131.253.25.164	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.125.113.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.6.242.153	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
173.68.98.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.178.135.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.120.17.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
131.253.25.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.166.69.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
100.100.26.20		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.225.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.54.25.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
76.10.175.66	Canada	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
100.100.49.23		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
100.100.10.227		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
46.121.254.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.201.169.254	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
83.168.248.11	Sweden	147.237.77.233	atal.idf.il	drop	SAM rule	drop	8
188.227.239.94	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.125.20	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
41.185.31.40	South Africa	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
46.19.86.42	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.61.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
107.212.12.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
123.136.106.58	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.220	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.15		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.26.20		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6

11-20-2015-17:04:04 to 11-20-2015-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.107.15.142	Block	213
2.52.165.141	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.165.141	Block	119
2.52.165.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.107.15.142	Block	77
41.107.15.142	Algeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	54
176.13.12.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
5.29.177.176	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.177.176	Block	19
79.182.39.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	11
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	6
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	5
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.66.20.217	Block	4
2.52.53.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.163.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.12.148.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.211.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.160.196.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
87.69.41.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
79.180.20.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.146.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.176.195.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
178.214.84.54	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.229.133.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.25.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.9.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.40.146	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1
79.178.182.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.73.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
173.68.98.15	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1038-en/dover.aspx parameter ctl00$ContentPlaceHolder1$txtEmail	Block	1
109.65.178.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.47.112	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/programmer.asp	Block	1
206.248.183.163	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
84.108.63.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
62.25.16.234	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
37.59.62.43	France	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
109.64.153.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/19-25.09.10.aspx	Block	1
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1

11-20-2015-17:04:04 to 11-20-2015-18:04:04