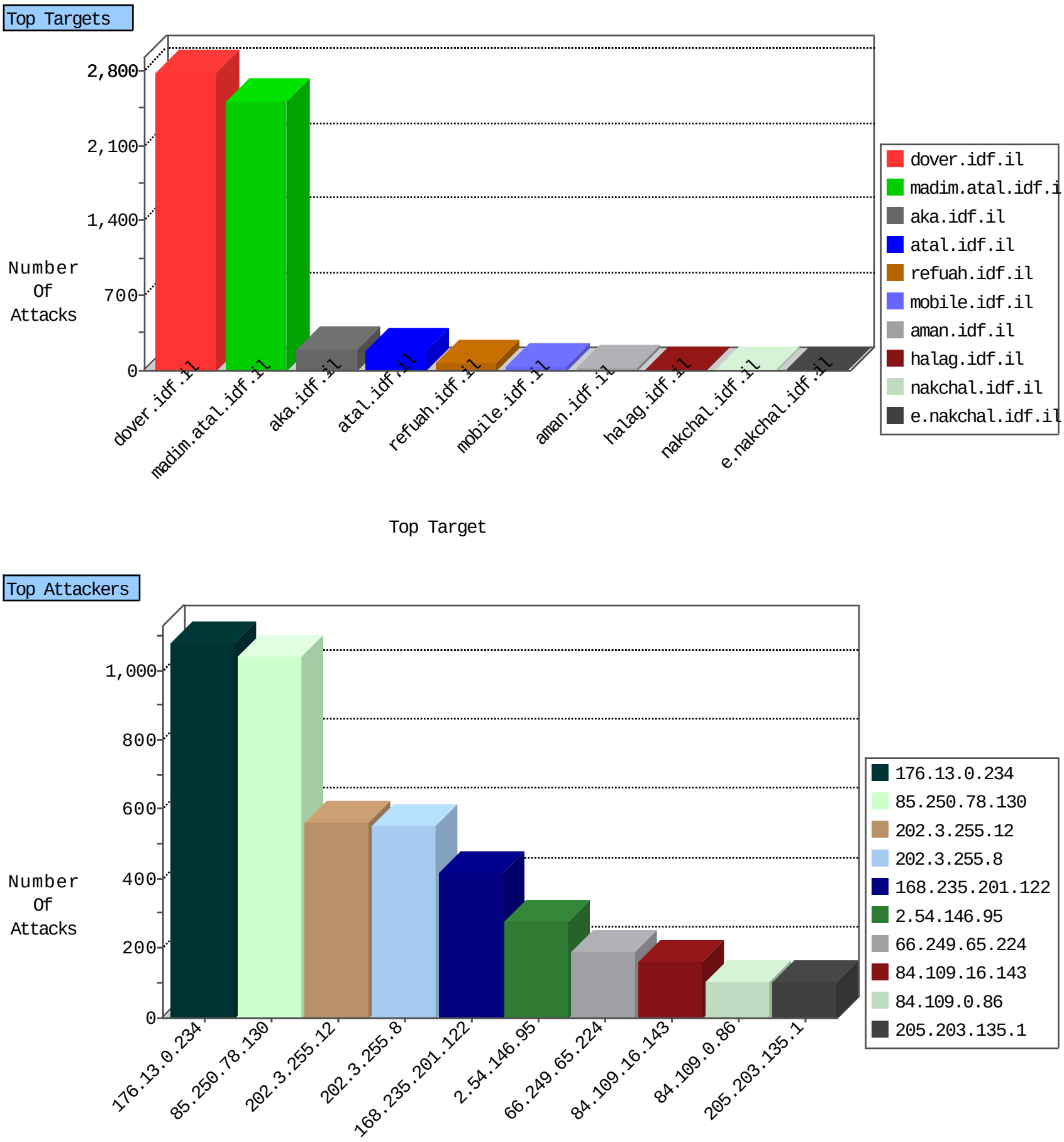
11-20-2015-20:04:08 to 11-20-2015-21:04:08

IDF Under Attack Daily Report



11-20-2015-20:04:08 to 11-20-2015-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	124
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
213.8.246.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
100.100.1.176		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
82.80.52.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.86.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
87.68.60.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
79.177.118.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
85.250.245.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.85.61	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
168.235.201.122	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
93.173.229.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
91.208.115.34	Ukraine	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

11-20-2015-20:04:08 to 11-20-2015-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.109.159	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	1

11-20-2015-20:04:08 to 11-20-2015-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	528
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	518
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
94.26.1.188	147.237.77.234	Bulgaria	halag.idf.il	ET SCAN Potential SSH Scan	2
94.26.1.188	147.237.77.170	Bulgaria	maarachot.idf.il	ET SCAN Potential SSH Scan	2
94.26.1.188	147.237.77.205	Bulgaria	prisha.idf.il	ET SCAN Potential SSH Scan	2
94.26.1.188	147.237.76.177	Bulgaria	ncore.idf.il	ET SCAN Potential SSH Scan	2
94.26.1.188	147.237.76.148	Bulgaria	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.76.31	Bulgaria	nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.77.212	Bulgaria	e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.72.14	Bulgaria	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
79.181.108.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.26.1.188	147.237.76.201	Bulgaria	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.76.199	Bulgaria	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
120.72.118.85	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
94.26.1.188	147.237.76.196	Bulgaria	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
104.243.16.106	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.26.1.188	147.237.76.176	Bulgaria	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.77.235	Bulgaria	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.76.38	Bulgaria	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.77.226	Bulgaria	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.72.166	Bulgaria	aka.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.0.33	Turkey	idf.il	ET SCAN NMAP -sS window 1024	1
94.26.1.188	147.237.77.178	Bulgaria	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
208.115.113.89	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.26.1.188	147.237.77.61	Bulgaria	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
94.26.1.188	147.237.76.200	Bulgaria	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
123.203.92.38	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.26.1.188	147.237.76.198	Bulgaria	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
120.72.118.85	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.26.1.188	147.237.77.243	Bulgaria	mobile.idf.il	ET SCAN Potential SSH Scan	1

11-20-2015-20:04:08 to 11-20-2015-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.201.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	415
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	182
84.109.16.143	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	160
84.109.0.86	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	105
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
70.199.77.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
107.161.8.130	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
185.3.146.210	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	41
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.117.126.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.120.137.220	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
84.110.108.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
213.57.132.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
131.137.245.208	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.165	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.121.114.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.1.176		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.57.132.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.46.249		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
220.255.97.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.180.122.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.250	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
87.68.60.74	Israel	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
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.81.128.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.99.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
207.46.13.47	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.161.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

11-20-2015-20:04:08 to 11-20-2015-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.78.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	698
176.13.0.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	682
176.13.0.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	232
85.250.78.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
176.13.0.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	168
2.54.146.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
85.250.78.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	136
2.54.146.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
85.65.13.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
31.154.152.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.146.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	8
5.135.144.131	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.135.144.131	Block	5
109.186.64.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.85	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
46.120.50.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.168.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.109.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.142.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.143.136.199	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	3
79.177.151.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.143.142.135	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
79.181.136.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
46.120.99.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.108.102.179	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.152.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.185.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.187.243	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 93.172.187.243	None	2
176.13.2.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.149.250	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
149.88.206.107	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.117.126.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.110.108.116	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
185.3.146.210	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.51	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size338x0/sip_storage	Block	1
136.243.92.10	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
85.250.131.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=4c9363f30438899f.1448044116.1.1448044116.1448044116.;	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
79.178.192.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.12.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	1

11-20-2015-20:04:08 to 11-20-2015-21:04:08