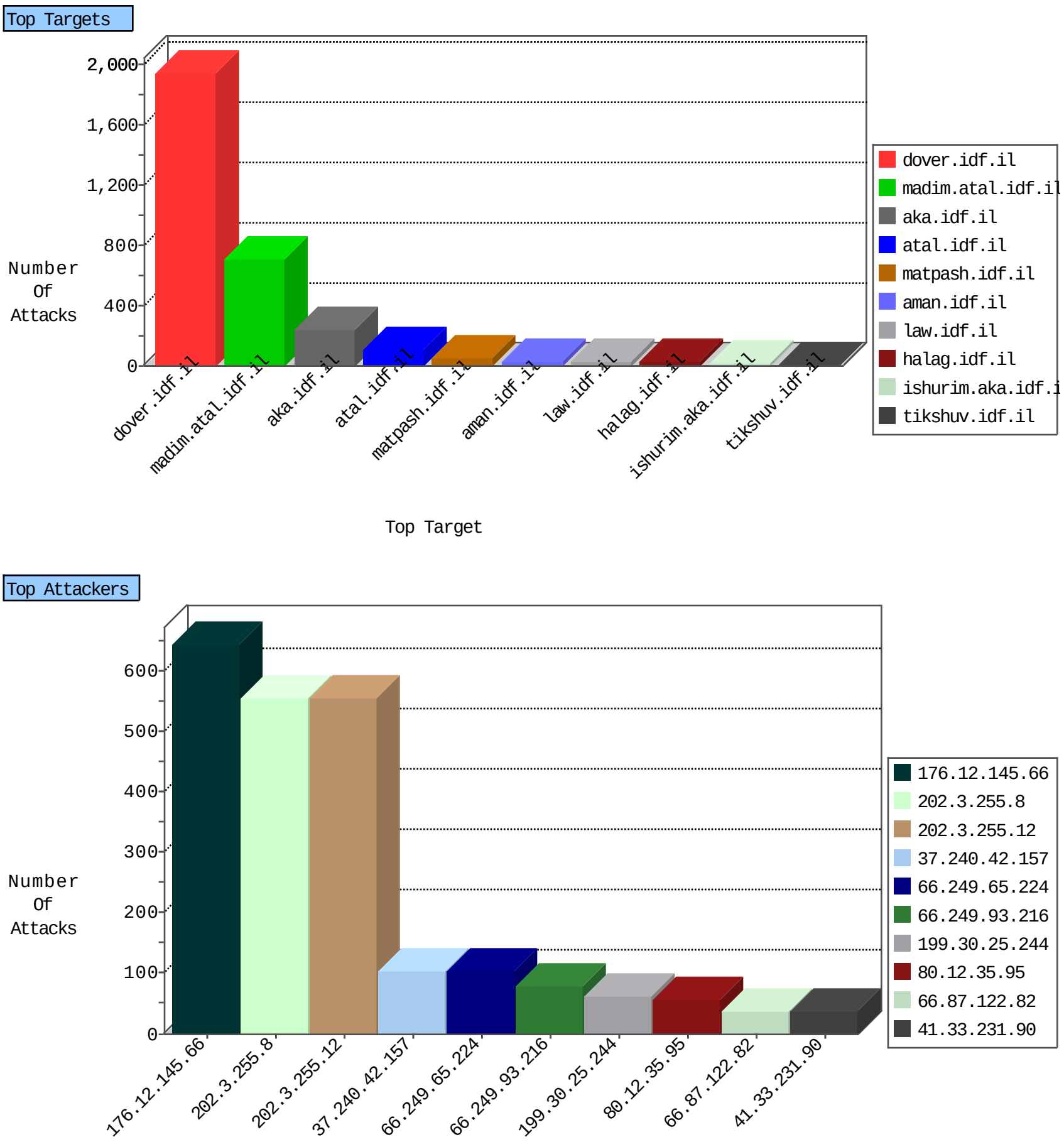
11-20-2015-18:04:02 to 11-20-2015-19:04:02

IDF Under Attack Daily Report



11-20-2015-18:04:02 to 11-20-2015-19:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.216	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5732
66.249.93.224	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4510
66.249.93.220	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1337
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.149.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.228.209.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
188.120.148.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-20-2015-18:04:02 to 11-20-2015-19:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
192.116.130.156	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-20-2015-18:04:02 to 11-20-2015-19:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	520
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	518
176.12.145.66	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
222.186.190.71	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.202	Ukraine	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.31.244.14	147.237.77.212	Iran, Islamic Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
74.117.209.135	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.190.71	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.214.128.12	147.237.76.42	Romania	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
81.31.244.14	147.237.77.212	Iran, Islamic Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
74.117.209.136	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

11-20-2015-18:04:02 to 11-20-2015-19:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.240.42.157	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
199.30.25.244	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.93.216	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	52
80.12.35.95	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.87.122.82	United States	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
202.3.255.12	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	34
100.100.127.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
2.54.154.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
199.36.184.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
200.115.154.235	Panama	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.87.66.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.158.108.255	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
178.135.117.70	Lebanon	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
199.30.24.241	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.188.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
89.138.205.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.188.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
89.139.185.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
178.135.117.68	Lebanon	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
89.139.185.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
199.16.156.124	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.12.35.95	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.12.35.95	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
100.100.102.129		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.178.194.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.189.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.202.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.62.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.207.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.236.140.91	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.159.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.5.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.33.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.25.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.17.111.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
100.100.26.228		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

11-20-2015-18:04:02 to 11-20-2015-19:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.145.66	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.145.66	Block	346
176.12.145.66	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.12.145.66	Block	180
176.12.145.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
80.246.136.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	19
89.138.28.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	11
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	9
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
85.64.19.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.43.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.19.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.50.183	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	2
2.52.42.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.65.51	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	2
46.120.236.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
183.79.220.209	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.220.209	Block	2
2.54.38.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.173.253.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
79.181.152.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.188.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.228.10.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
5.29.19.134	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
66.249.65.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/klali.aspx	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
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	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14276-he/dover.aspx	Block	1
46.117.7.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.206.3	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.66.20.217	Block	1
8.37.230.44	Anonymous Proxy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shael, idfspokeperson	Block	1
178.135.117.68	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
149.88.206.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
207.253.84.7	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
79.177.118.88	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.52.43.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
84.95.207.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.239.211.141	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
77.127.158.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.162.34.45	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/]	Block	1

11-20-2015-18:04:02 to 11-20-2015-19:04:02