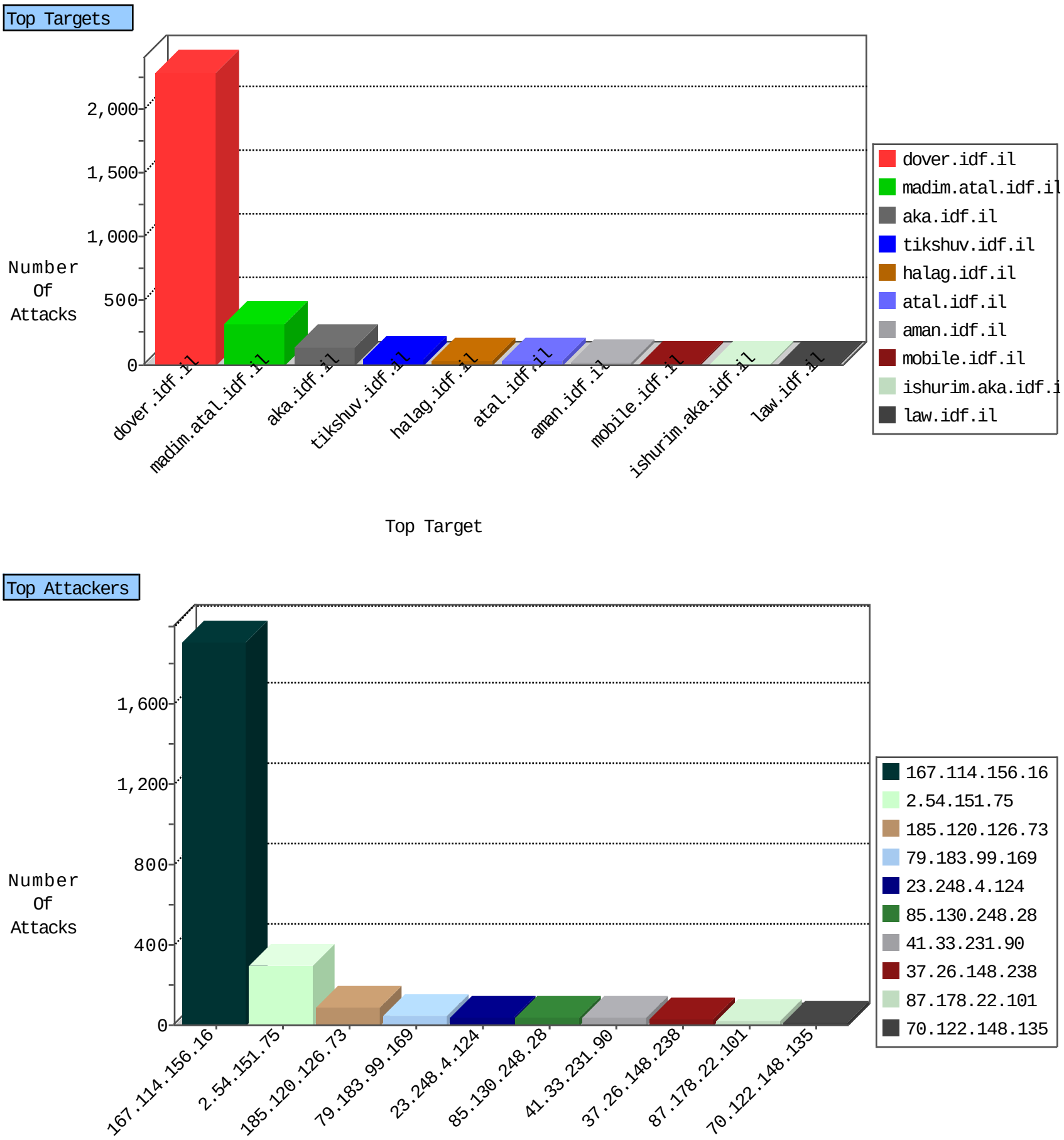
01-07-2016-00:04:03 to 01-07-2016-01:04:03

IDF Under Attack
Daily Report



01-07-2016-00:04:03 to 01-07-2016-01:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3294
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1546
159.203.67.223	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
37.26.148.201	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.174.4	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.249.93.182	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
46.166.188.68	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.102.9.21	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

01-07-2016-00:04:03 to 01-07-2016-01:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Netherlands	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-07-2016-00:04:03 to 01-07-2016-01:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
151.80.121.200	147.237.77.233	Italy	atal.idf.il	ET SCAN Potential SSH Scan	1
151.80.121.200	147.237.77.179	Italy	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
151.80.121.200	147.237.76.201	Italy	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.80.121.200	147.237.0.35	Italy	akaws.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.15	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
173.199.74.136	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.60.36.203	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.101.85.198	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
151.80.121.200	147.237.77.234	Italy	halag.idf.il	ET SCAN Potential SSH Scan	1
50.23.96.210	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
151.80.121.200	147.237.77.216	Italy	dover.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.80.121.200	147.237.77.74	Italy	law.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.80.121.200	147.237.8.27	Italy	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.80.121.200	147.237.0.15	Italy	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.15	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.60.36.203	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.23.96.210	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-07-2016-00:04:03 to 01-07-2016-01:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
23.248.4.124	Canada	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
85.130.248.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
79.183.99.169	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.178.22.101	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
79.183.99.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
81.109.59.88	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.3.147.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.33.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.10.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
70.122.148.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.61.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.210.193.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.118.58	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
70.122.148.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.199.57.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
65.55.210.155	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
65.55.210.155	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.215.192.130	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.180	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.197.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.242.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.207.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.116.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.234.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.1.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.177.114.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.64.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.137.120	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

01-07-2016-00:04:03 to 01-07-2016-01:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	197
2.54.151.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.151.75	Block	60
2.54.151.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.151.75	Block	42
85.64.33.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.197.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.210.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.i	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/1133-22461-he/dover.aspx.	Block	2
79.180.1.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
176.13.0.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.146.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.19.94	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
212.150.214.90	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
157.55.39.11	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
109.253.131.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
5.28.168.188	Israel	147.237.77.216	dover.idf.il	NULL Character in URL _hÂ¼â€?×‘Ã¼* +ÃžsÂ´>Âš.×,×?×šÂ¬[[#4]]nwe[[#16]]Â¬~m×ƒs×“iqoâ€œ [[#21]][[#3]][[#3]][[#0]][[#26]]o[[#26]]Ö³Â³e	Block	1
2.54.151.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
207.46.13.133	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
180.76.15.19	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
70.122.148.135	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.137.214	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	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
5.28.168.188	Israel	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.199.57.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.130.101.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
175.44.8.123	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-en/dover	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.253.141.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
23.248.4.124	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
185.106.92.36		147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1748	Block	1
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	1
5.28.168.188	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	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
66.249.79.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1111-7791-he/nakhal.aspx	Block	1
37.142.64.109	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
212.47.227.72	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.86.68.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.99.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.106.92.36		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20140-he/idfgdover.aspx	Block	1
148.251.21.227	Germany	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.66.27.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.168.188	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
2.52.61.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

01-07-2016-00:04:03 to 01-07-2016-01:04:03