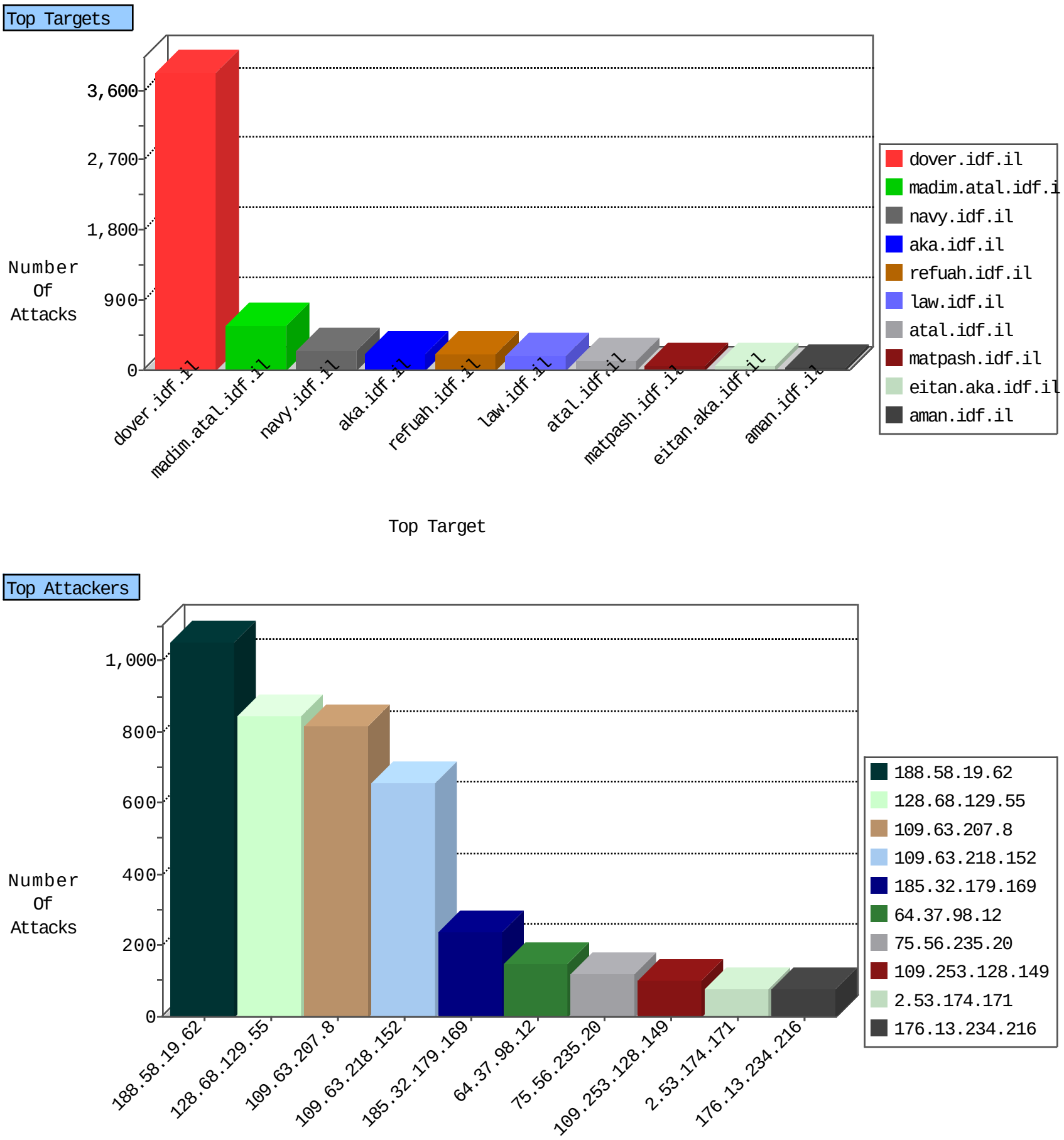
09-07-2016-12:04:08 to 09-07-2016-13:04:08

IDF Under Attack Daily Report



09-07-2016-12:04:08 to 09-07-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.192.169.103	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2842
109.63.207.8	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	447
84.229.8.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
128.68.129.55	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
93.158.203.199	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
172.91.186.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.216.55	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
109.63.218.152	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-07-2016-12:04:08 to 09-07-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.56.235.20	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	21
84.245.33.104	Netherlands	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
40.85.96.77	Ireland	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
103.238.138.4	Indonesia	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
110.4.46.108	Malaysia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	10
75.56.235.20	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
216.119.125.34	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.119.125.34	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
40.85.96.77	Ireland	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.97	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.58.230.159	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.45	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
84.245.33.104	Netherlands	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.63.228.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
192.99.167.90	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
103.238.138.4	Indonesia	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
103.238.138.4	Indonesia	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
187.17.96.33	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.68.17.195	Israel	147.237.77.176	matpash.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	2
62.212.73.211	Netherlands	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.234.159.250	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
81.177.24.40	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
50.63.197.11	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-07-2016-12:04:08 to 09-07-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
75.56.235.20	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	87
61.220.26.201	147.237.77.216	Taiwan	dover.idf.il	SQL Injection - Select From	37
216.119.125.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	32
103.238.138.4	147.237.77.176	Indonesia	matpash.idf.il	SQL Injection - Select From	27
40.85.96.77	147.237.76.42	Ireland	refuah.idf.il	SQL Injection - Select From	24
110.4.46.108	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	20
84.245.33.104	147.237.76.42	Netherlands	refuah.idf.il	SQL Injection - Select From	18
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	17
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	16
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	15
216.58.230.159	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
192.99.167.90	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	14
23.91.70.43	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	13
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	13
23.91.70.45	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
50.63.197.11	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
187.17.96.33	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	2
62.210.97.57	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

09-07-2016-12:04:08 to 09-07-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.58.19.62	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1055
128.68.129.55	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	841
109.63.207.8	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	812
109.63.218.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	659
176.192.169.103	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
176.195.114.193	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
94.23.98.79	France	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	39
87.69.36.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	36
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
79.177.241.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
79.46.4.211	Italy	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
209.197.16.156	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
209.197.16.156	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
209.197.16.156	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
83.168.250.50	Sweden	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.25.74.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
209.197.16.156	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
185.127.10.35	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.67.25.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.117.207.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
2.55.63.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
98.19.222.133	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.19.86.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.53.160.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.106.54.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.222.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.178.210.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.63.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	6
2.55.145.77	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.63.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.55.145.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.55.145.77	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.175	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5

09-07-2016-12:04:08 to 09-07-2016-13:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
109.253.128.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
2.53.174.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
176.13.234.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.53.22.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
5.29.193.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.193.40	Block	19
2.53.175.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.229.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
141.226.218.48	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
176.13.5.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.147.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
194.90.26.70	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
79.181.13.224	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
66.249.88.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.142.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.88.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.183.44.223	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.44.223	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
77.139.80.115	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
176.13.18.79	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
79.183.44.223	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.149.225	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
180.76.15.136	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.86.121	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ref.20.8afc=["","",1473239557,"http://www.google.co.il/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahukewju39lk8_zoahvrk8akhezrckmqfggamaa&url=http://www.idf.il/1038-he/dover.aspx&usg=afqjcnfk2ypxtlz4pscjbjznljo41rasvw"];	Block	1
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed URL from 45.79.71.122	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.49.110	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/klali.aspx	Block	1
5.29.193.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
207.46.13.76	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
109.67.25.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.206	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.202.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.121	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 60000; in URL	Block	1
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
31.154.41.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.103	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
178.62.224.34	Netherlands	147.237.76.200	eitan.aka.idf.il	Multiple Untraceable SSL Sessions from 178.62.224.34 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
109.67.49.7	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Malformed HTTP Header Line 2	Block	1
79.183.44.223	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/	Block	1
5.29.193.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
188.24.146.229	Romania	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
150.70.173.40	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1

09-07-2016-12:04:08 to 09-07-2016-13:04:08