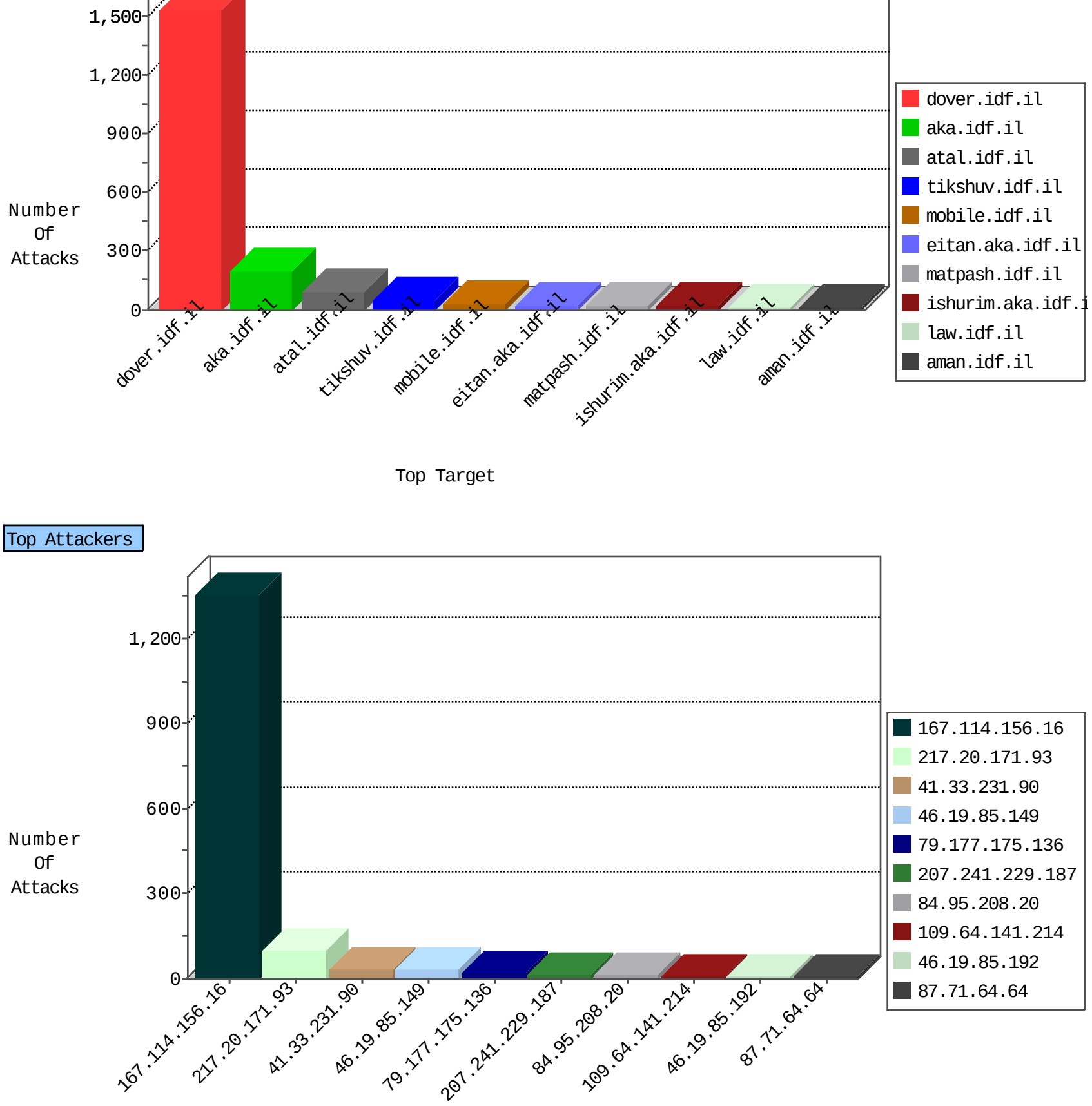
04-15-2016-10:04:07 to 04-15-2016-11:04:07

IDF Under Attack Daily Report



04-15-2016-10:04:07 to 04-15-2016-11:04:07

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	Block_Ip_Web_In	drop	1346
79.180.198.74	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.180.198.74	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.118	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-10:04:07 to 04-15-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.76	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
109.66.23.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
63.141.229.34	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
46.117.162.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
63.141.229.34	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.147.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-10:04:07 to 04-15-2016-11:04:07

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
165.138.213.4	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
161.123.171.88	147.237.77.216	South Africa	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.44.133.108	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
161.123.171.88	147.237.76.201	South Africa	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.102.168.255	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
161.123.171.88	147.237.76.148	South Africa	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
161.123.171.88	147.237.8.27	South Africa	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
161.123.171.88	147.237.0.35	South Africa	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.52.55.64	147.237.76.38	Philippines	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.13.70.132	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
165.138.213.4	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
161.123.171.88	147.237.77.227	South Africa	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
161.123.171.88	147.237.77.212	South Africa	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.44.133.108	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
161.123.171.88	147.237.76.196	South Africa	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.28.147.180	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
161.123.171.88	147.237.8.28	South Africa	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.123.171.88	147.237.8.14	South Africa	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.123.171.88	147.237.0.33	South Africa	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.77.74	Japan	law.idf.il	ET SCAN NMAP -sS window 1024	1

04-15-2016-10:04:07 to 04-15-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
217.20.171.93	Ukraine	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.229.187	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
109.64.141.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.64.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.53.181.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.177.175.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.177.175.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.20.171.93	Ukraine	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.64.118.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.65.110.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.220	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.154.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.101	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.20.171.93	Ukraine	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.80.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.131.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.30.24.149	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
69.164.203.71	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
66.102.6.135	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.240.235	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.121.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.197.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.10.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.240.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.126.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.144.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.157.87.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.180.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.31.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.130.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.20.171.93	Ukraine	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
2.55.134.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-15-2016-10:04:07 to 04-15-2016-11:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.37.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.228.30.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.252.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.112.192	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-15-2016-10:04:07 to 04-15-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	4
87.69.31.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
219.74.166.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.20.171.93	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	2
62.90.143.125	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.90.143.125	Block	2
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.148.111	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.64.118.177	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
219.74.166.227	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.32.179.140	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
120.42.78.247	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
38.111.147.83	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
220.255.103.33	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.20.171.93	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.64.118.177	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
203.127.96.248	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.242.36.176	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
114.98.80.58	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
217.20.171.93	Ukraine	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.66.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
123.158.68.200	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
38.111.147.83	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 38.111.147.83	Block	1
220.255.146.48	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/צה	Block	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.55.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
115.212.19.208	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
219.74.180.185	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
217.20.171.93	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	1
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
40.77.167.52	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/sitemap/	Block	1
218.58.40.222	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
93.157.87.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
78.95.65.132	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.241.229.48	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
62.90.143.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/1636646he/	Block	1
178.62.223.104	Netherlands	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/piwik.php	Block	1
217.20.171.93	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	1
203.127.96.232	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1

04-15-2016-10:04:07 to 04-15-2016-11:04:07