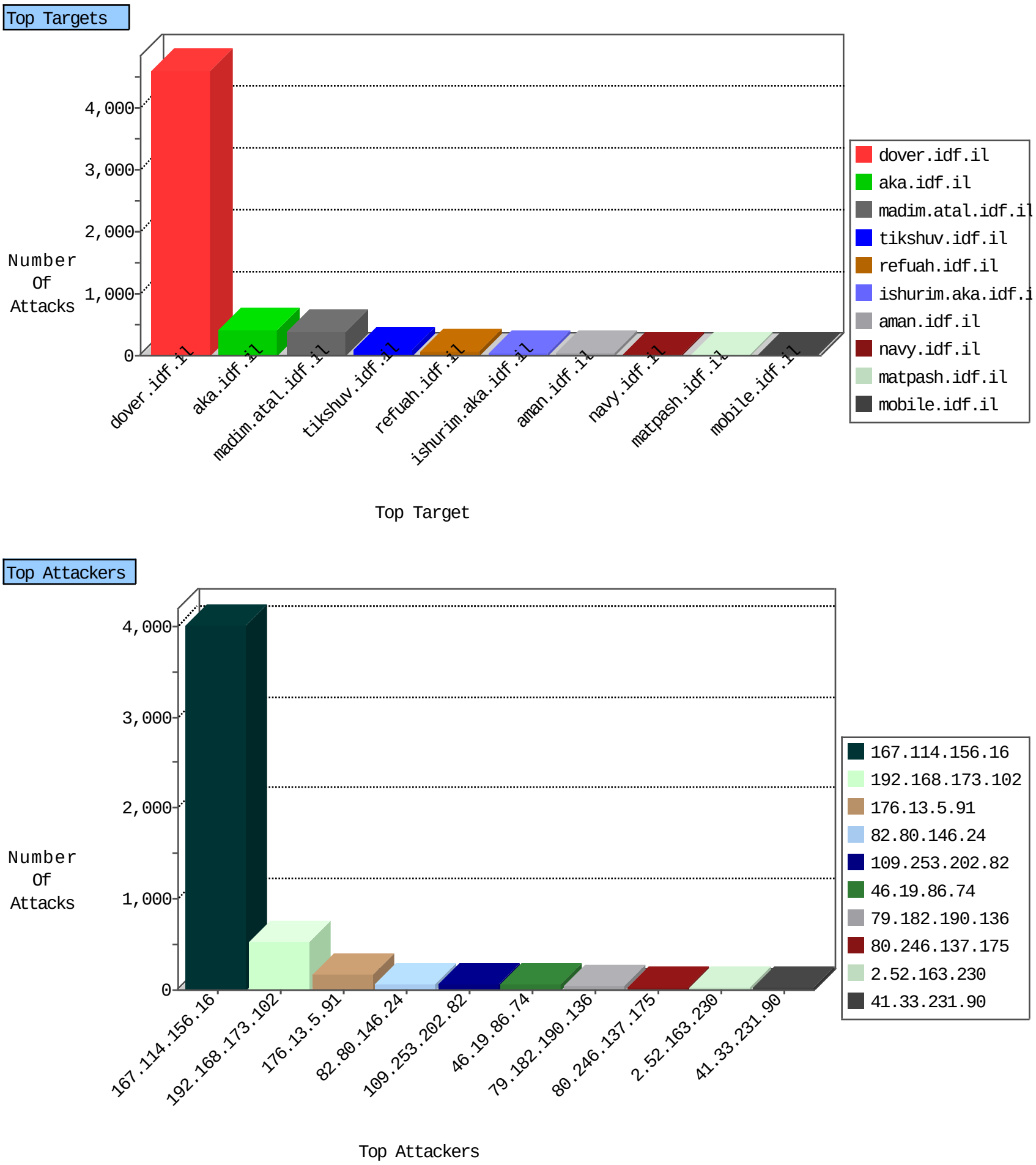
04-10-2016-12:04:05 to 04-10-2016-13:04:05

IDF Under Attack Daily Report



04-10-2016-12:04:05 to 04-10-2016-13:04:05

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	4023
46.19.86.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1110
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
79.180.63.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.64.204.115	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.64.204.115	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
109.64.204.115	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
69.30.226.99	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
74.91.18.44	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
69.30.198.147	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
107.150.32.62	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
74.91.20.195	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
69.30.198.149	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
173.208.197.254	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
153.254.134.223	Japan	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
91.15.198.93	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
216.72.40.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
165.225.76.105	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.15.198.93	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
128.139.21.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.15.198.93	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

04-10-2016-12:04:05 to 04-10-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.137.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
77.125.95.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.181.211.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
83.149.126.98	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
83.149.126.98	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-12:04:05 to 04-10-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.127	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
46.117.213.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.218.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.135.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
109.226.48.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.176	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.10.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
206.190.136.245	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
110.32.136.143	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.6.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.176	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
93.172.8.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.118.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.72.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-12:04:05 to 04-10-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	348
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	185
82.80.146.24	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
46.19.86.180	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	21
31.168.151.101	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	19
82.80.146.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.52.163.230	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.154	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
37.26.148.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.117.199.57	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.163.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.158.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
147.236.238.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.138.147	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.159.62	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.207.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.81.43.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.34	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.146.24	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.199.57	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
217.78.57.193	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.199.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.78.57.193	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	4
5.22.135.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.193.240	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.186	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
192.116.231.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.184.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.88	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
176.228.204.30	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
217.78.57.193	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
207.232.55.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.188.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.6.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.163.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-10-2016-12:04:05 to 04-10-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	176
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.137.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.182.190.136	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	26
176.13.9.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.182.190.136	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.182.190.136	Block	6
2.53.59.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.116.232.69	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	5
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	4
84.109.132.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.132.138	Block	4
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.165.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
62.159.77.165	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.159.77.165	Block	2
37.26.148.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.214.111	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.130.218	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
132.72.172.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	2
80.246.136.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
74.91.18.44	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
173.208.197.254	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
84.109.132.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/send_but.png	Block	1
192.114.7.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.142.37	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
86.158.202.158	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
217.78.57.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
192.114.91.247	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.62.91	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	1
79.179.21.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
37.26.149.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.150.32.62	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
69.30.198.147	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
192.114.163.81	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
54.153.33.233	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
141.212.122.129	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.50.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19815-he/idfgdover.aspx	Block	1

04-10-2016-12:04:05 to 04-10-2016-13:04:05