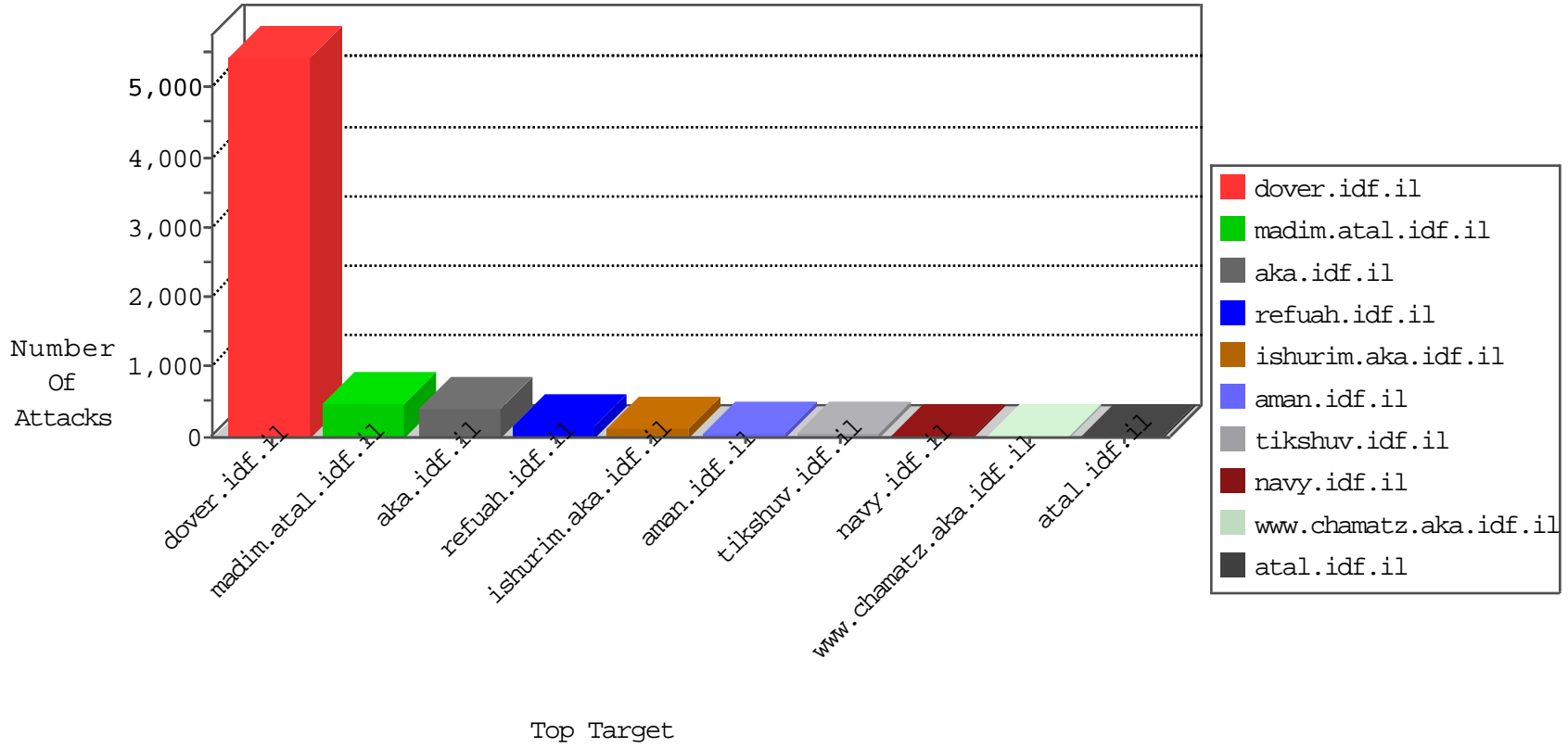


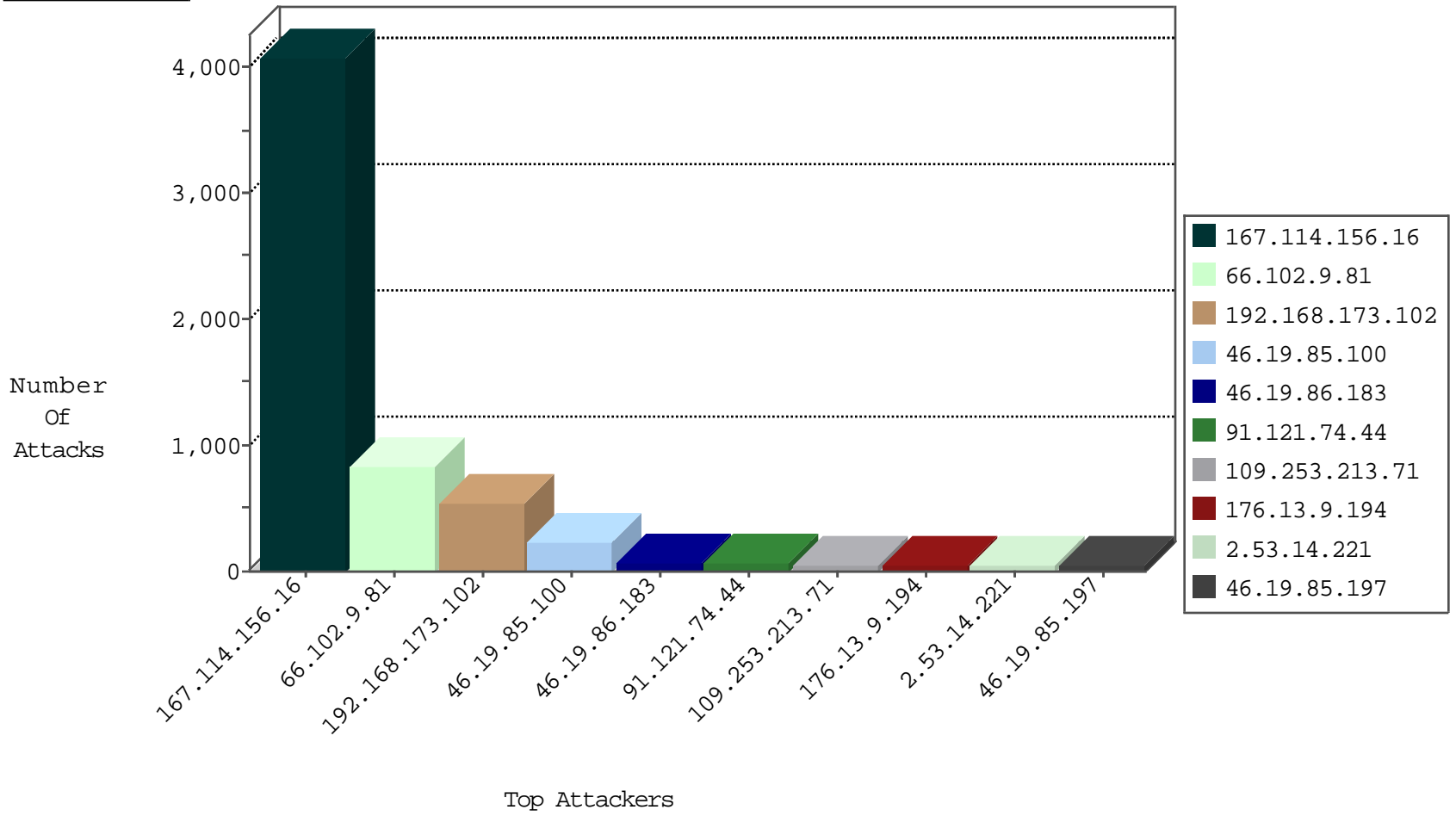
IDF Under Attack Daily Report



Top Targets



Top Attackers



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_Tp_Web_In	drop	4069
79.180.218.67	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.145.115.61	Russian Federation	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
107.150.46.37	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	2
37.145.115.61	Russian Federation	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
184.105.139.126	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.74	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.78	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.126	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.105	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.98	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.44.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
149.88.80.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.236.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
2.53.21.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.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
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
120.156.4.171	Australia	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	822
80.246.137.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.198.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.164.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.6	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
31.168.173.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.160.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.156.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
2.54.150.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.179	Canada	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
87.70.79.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.127.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.47.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.6	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.189.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.254.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.121.194	147.237.76.86	Singapore	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.22.129.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
89.138.110.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

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	346
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	192
91.121.74.44	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
176.13.9.194	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.136	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
107.167.104.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
46.19.85.137	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	23
80.246.130.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
109.253.219.10	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.53.14.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
2.53.14.221	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.4.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.27.82.30	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.25.22.226	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.30	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.27.82.30	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.55.35.187	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.179.195.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.211.145	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.14.221	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.67.11.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.177.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.53.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.16.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.184.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.186.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.230.158	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.241.229.223	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
217.132.32.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.164.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.47.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.52.196	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.186	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
109.253.196.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-10-2016-09:04:07 to 04-10-2016-10:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.195.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	221
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.213.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
109.67.135.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	23
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.53.1.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
199.203.226.21	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	4
176.13.15.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	3
213.8.204.33	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
2.53.60.87	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
5.102.207.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.29.202.206	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.203.226.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/sip_storage/files/3/	Block	2
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
46.19.86.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.219.32	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.4.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
46.19.85.9	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	2
87.71.121.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.163	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
107.170.74.206	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.167/	Block	1
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.217	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
199.203.226.21	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 199.203.226.21	Block	1
169.229.3.90	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/rec.dat	Block	1
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
91.104.107.152	Hungary	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
80.246.130.199	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
192.114.91.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.12	Block	1
109.65.247.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
82.166.125.198	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
92.126.5.174	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt'a=0	Block	1
37.26.146.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
81.218.40.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
85.65.116.235	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
68.180.231.43	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
203.127.96.250	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1