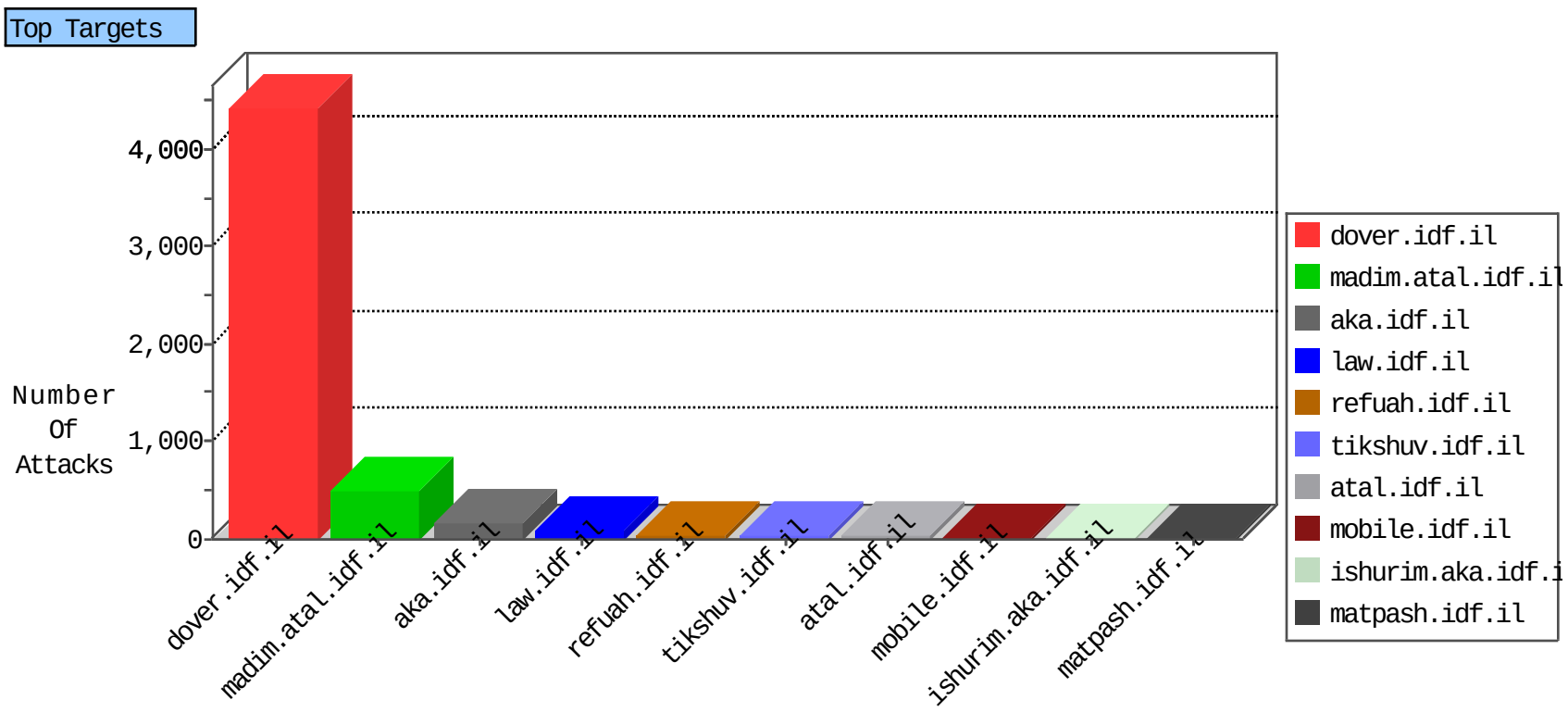
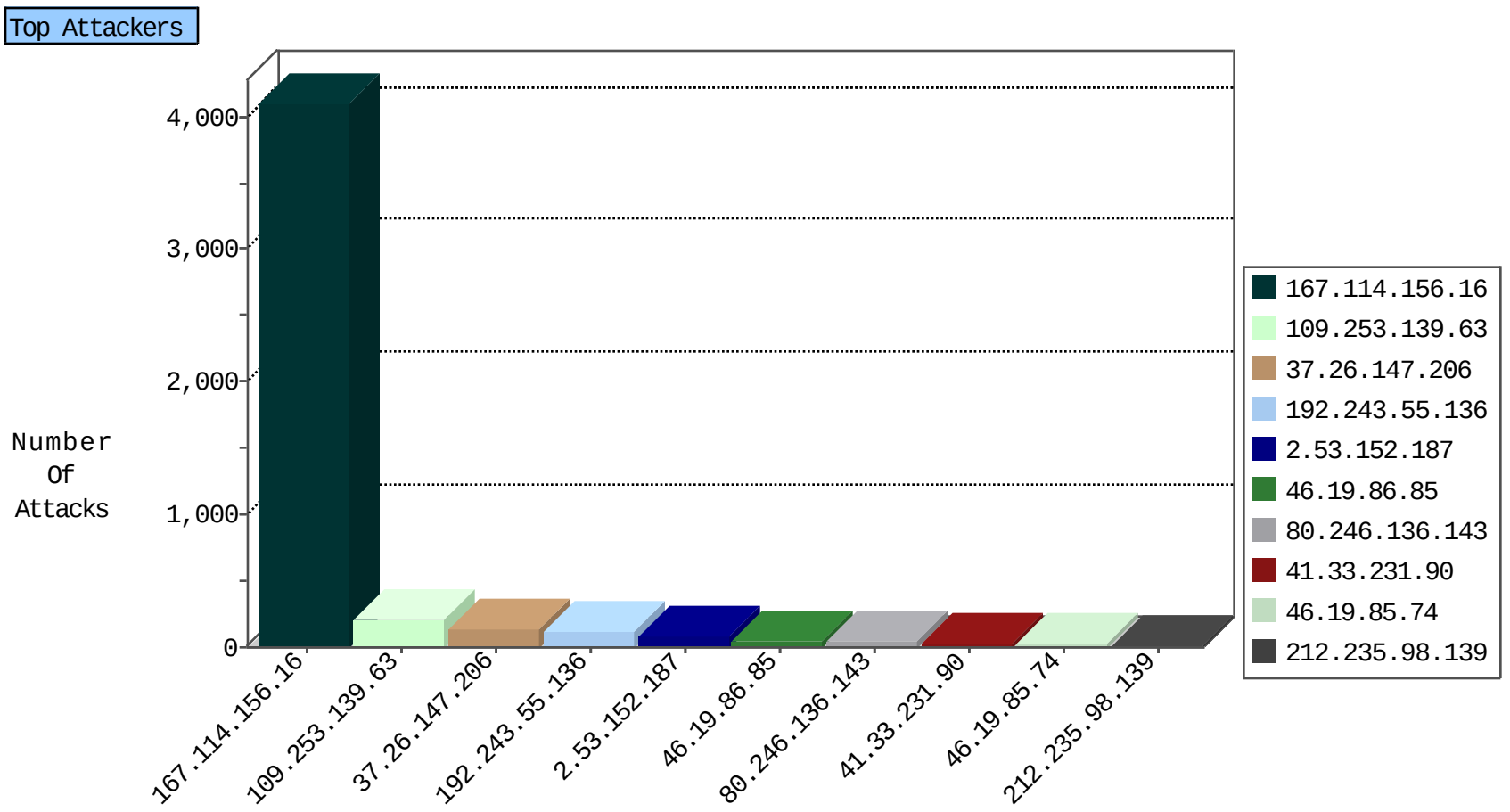
04-12-2016-15:04:01 to 04-12-2016-16:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-12-2016-15:04:01 to 04-12-2016-16:04:01

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	4095
109.253.199.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	917
93.173.15.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	895
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	573
120.132.50.135	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
87.71.81.39	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
182.31.41.82	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
104.148.71.133	United States	147.237.77.179	e.mazi.idf.il	JLM_Under_Attack_Con_Http	drop	2
62.219.77.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
82.80.86.86	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
168.235.207.176	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
2.55.169.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.65.133.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
31.168.170.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
121.185.50.97	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
219.167.231.51	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
109.253.132.117	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.188.77.109	Mauritania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.135.102.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
222.186.31.188	China	147.237.0.16	my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.120.125.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-12-2016-15:04:01 to 04-12-2016-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.129.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
85.65.99.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.143.54.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.116.15.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.138.109.210	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
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.215	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
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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-15:04:01 to 04-12-2016-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.197.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.143.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.187.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.9.179.239	147.237.77.19	Tunisia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.158	147.237.77.216	Israel	dover.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
177.158.141.105	147.237.72.14	Brazil	dover.idf.il(old	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.88.63.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.16.11.211	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.76.34	Turkey	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.16.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.96.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.77.227	Latvia	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.131.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.145.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
166.62.88.241	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
109.56.212.184	147.237.77.216	Denmark	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.8.50	Canada	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.102.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-12-2016-15:04:01 to 04-12-2016-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.85.251	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
89.138.161.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
176.13.9.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.46.13.74	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	10
80.246.136.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.235.69.34	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.246.136.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.132.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
46.19.86.164	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.218.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.202.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
185.24.207.59	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.53.161.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.69.37.88	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.24.207.59	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.111.217.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
132.70.66.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.136.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.233.202.36	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.3.147.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	5
89.139.235.138	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.235.138	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
185.24.207.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.143.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.218.126.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4

04-12-2016-15:04:01 to 04-12-2016-16:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.139.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	198
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
2.53.152.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.34.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
199.30.24.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
192.116.55.146	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	3
91.135.102.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.126.59	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	3
195.160.242.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	3
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	3
2.53.179.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.53.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.3.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.16.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.208	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.7.167	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.158.152.52	Block	2
79.177.183.69	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
65.55.210.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.52	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.162	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.160.242.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
89.139.235.138	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
178.162.209.109	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.162.209.109	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
109.56.212.184	Denmark	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.95	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
54.255.167.37	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
213.8.10.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.253.225.193	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.126.238.100	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.mag.idf.il/657-en/patzar.aspx	Block	1
2.53.131.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/size220x0/sip_storage	Block	1
178.162.209.109	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17946-en/dover.aspx'	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15558-en/dover.aspx.	Block	1

04-12-2016-15:04:01 to 04-12-2016-16:04:01