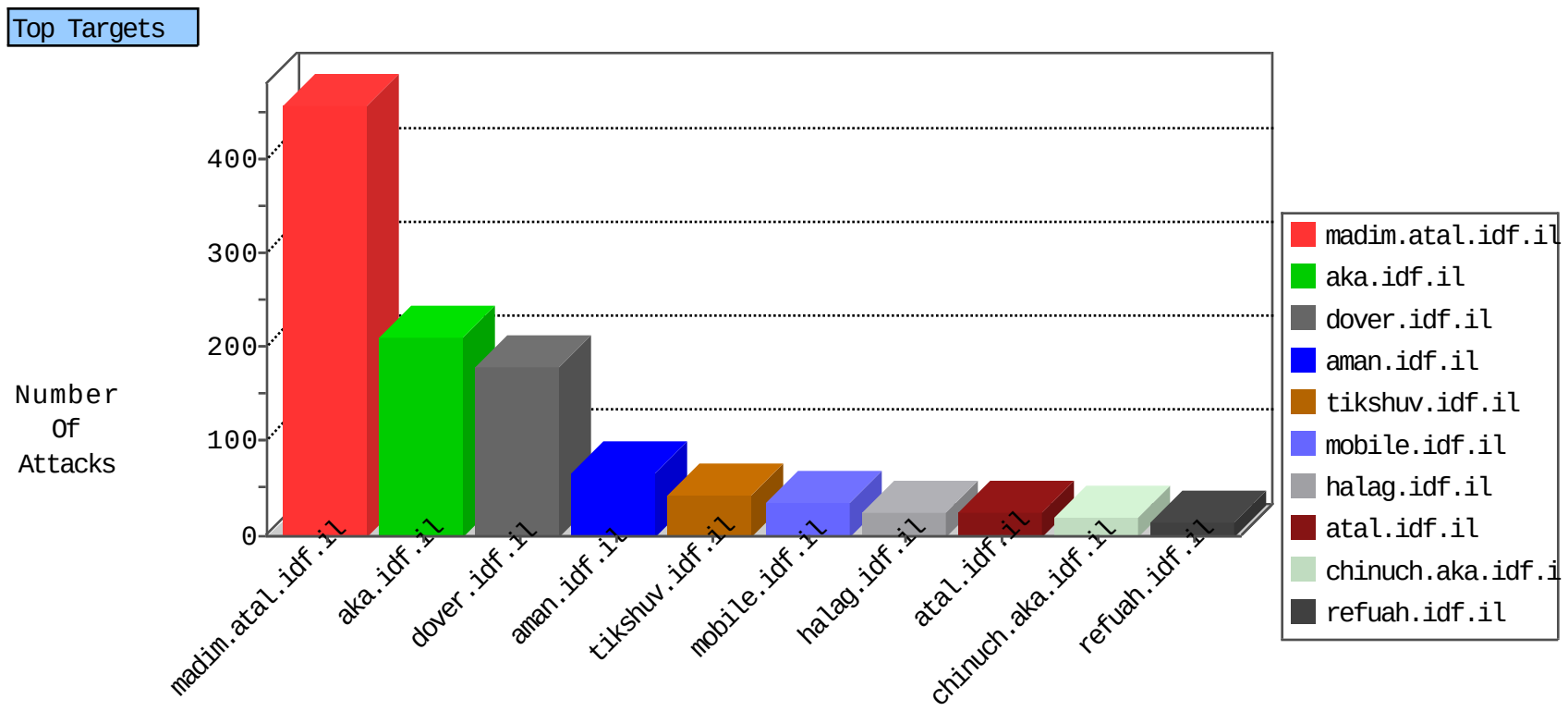
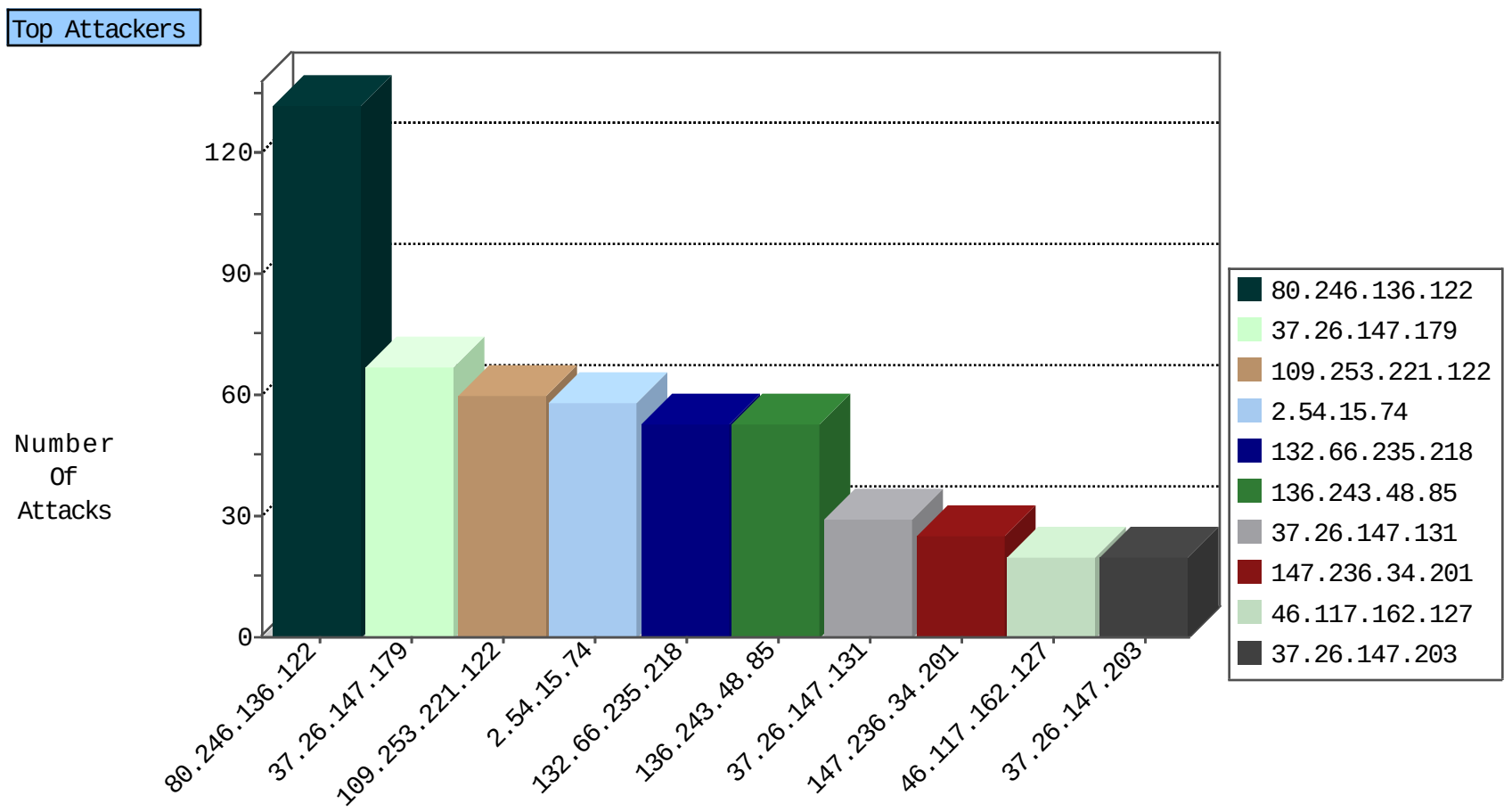
03-09-2016-16:04:07 to 03-09-2016-17:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-16:04:07 to 03-09-2016-17:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.209.166	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
136.243.48.85	Germany	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
136.243.48.85	Germany	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
5.29.93.253	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1
31.168.23.114	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
81.218.208.168	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

03-09-2016-16:04:07 to 03-09-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.102.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
87.70.75.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.147.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
176.13.6.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.9.87.111	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
31.168.18.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.239.205.207	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
37.142.161.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.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
173.208.136.170	United States	147.237.76.200	eitan.aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
173.208.136.170	United States	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-09-2016-16:04:07 to 03-09-2016-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.48.193	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.145.38	147.237.72.166	Germany	aka.idf.il	ET SCAN NMAP -sS window 4096	1
40.113.118.99	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
213.8.129.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.129.8.145	147.237.76.147	France	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.1.202	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
2.54.131.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.238	147.237.76.148		gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
132.73.196.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.132.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.103.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.237.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.221.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.23.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.238	147.237.76.202		e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.16.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.91.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.54.83.98	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-09-2016-16:04:07 to 03-09-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
136.243.48.85	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
46.117.162.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
79.176.0.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
132.66.235.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.236.34.201	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.48.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.111.49.2	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
85.130.223.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
170.252.72.61	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
132.66.235.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
5.29.212.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
87.71.67.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.136.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.223.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.155.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.34.201	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.179.21.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.24.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.54	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.55	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
147.236.34.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
136.243.48.85	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.223.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.10.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.29.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.144.59.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.96.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.21.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.18.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.131.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.251.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.63.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.14.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.138.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.145.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.214.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.121.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.135.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.6.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-16:04:07 to 03-09-2016-17:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.61	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.168.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.40.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-16:04:07 to 03-09-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
109.253.221.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.54.15.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
37.26.147.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.147.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.253.207.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.7.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.213.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
176.13.1.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.253.203.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.122.66	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
2.52.33.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.170.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.216.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.6.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.161.208	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.70.71.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
82.109.66.147	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.143.38.222	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
176.13.9.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
46.117.153.0	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.161.117.91	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
193.90.12.89	Norway	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
80.179.197.116	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
82.109.66.149	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.52.33.14	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.120.63.191	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
147.236.34.201	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	1
46.117.162.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
5.29.212.105	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.241.229.224	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.241.229.224	Block	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
176.13.1.59	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.49.2	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.118.10.10	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
156.207.66.59		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
46.210.145.89	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.146.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/pc	Block	1
207.241.229.224	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
66.249.93.48	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
124.6.181.98	Philippines	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-09-2016-16:04:07 to 03-09-2016-17:04:07