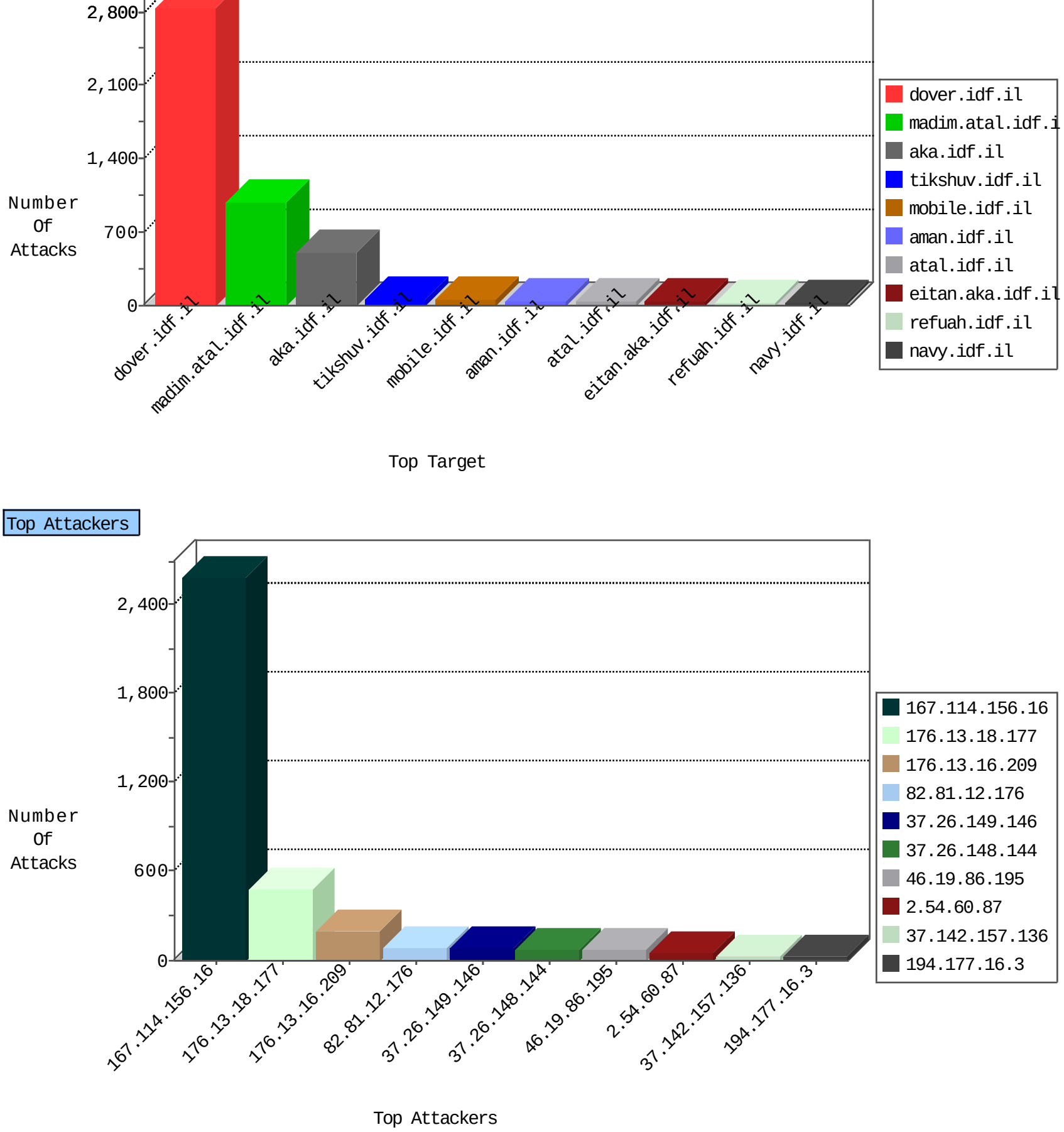
03-13-2016-15:04:04 to 03-13-2016-16:04:04

IDF Under Attack Daily Report



03-13-2016-15:04:04 to 03-13-2016-16:04:04

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	DOS-Tool-SwitchbladG	dest-reset	3768
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	88
79.181.33.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
2.54.7.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
94.230.84.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.86.79	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
85.64.249.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.160.172.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
80.246.136.21	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
31.168.205.126	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.65.169.138	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

03-13-2016-15:04:04 to 03-13-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
70.89.127.78	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
195.234.228.90	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
109.67.141.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
74.63.228.226	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
84.111.82.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
217.70.44.165	Sweden	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
97.88.198.223	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

03-13-2016-15:04:04 to 03-13-2016-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.124.109.87	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	6
70.89.127.78	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	2
68.180.229.221	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.106.92.65	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.126.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.55.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.54.83.98	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
2.54.128.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.98.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.237.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.158.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.47.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.207.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.112.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.248.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.11.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.142.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.224.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.121.136.51	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
109.226.44.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.3.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.97.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.141	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
212.199.218.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.230.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-13-2016-15:04:04 to 03-13-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	136
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	89
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	68
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	68
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
2.54.162.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.210.60	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.54.162.131	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	13
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.183.18.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.7.87	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.165.136	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.174.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.163.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.186.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.183.235	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.142.183.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
188.120.154.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.138.83.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
2.52.173.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.247.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.142.157.136	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.17.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.157.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.49.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.195.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.186.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.33.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.165.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.18.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.157.136	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.54.254.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.106.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.195.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.105.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.131.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
79.181.33.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.33.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.246.133.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

03-13-2016-15:04:04 to 03-13-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	279
176.13.16.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	193
37.26.149.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
2.54.60.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
2.54.145.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
69.195.124.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.195.124.113	Block	5
176.13.4.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.149.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.235.124.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.186.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.210.187.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/שכר/default.aspx	Block	2
2.54.129.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.238	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
188.162.166.56	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'	Block	2
37.26.147.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.12.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.235.103.203	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.69.67.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.67.209	Block	2
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.41.17	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
81.218.70.243	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
69.195.124.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
2.54.60.87	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend in madim.atal.idf.il/mobile/login.aspx	Block	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.115.177.202	Block	1
46.210.142.133	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.249	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
89.138.235.127	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
207.241.229.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
79.181.218.129	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
213.57.130.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
82.166.53.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.75.249.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	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
173.252.90.240	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
94.159.166.220	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.164.105	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
212.143.122.2	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.183.190.249	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.69	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.116.28.206 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1

03-13-2016-15:04:04 to 03-13-2016-16:04:04