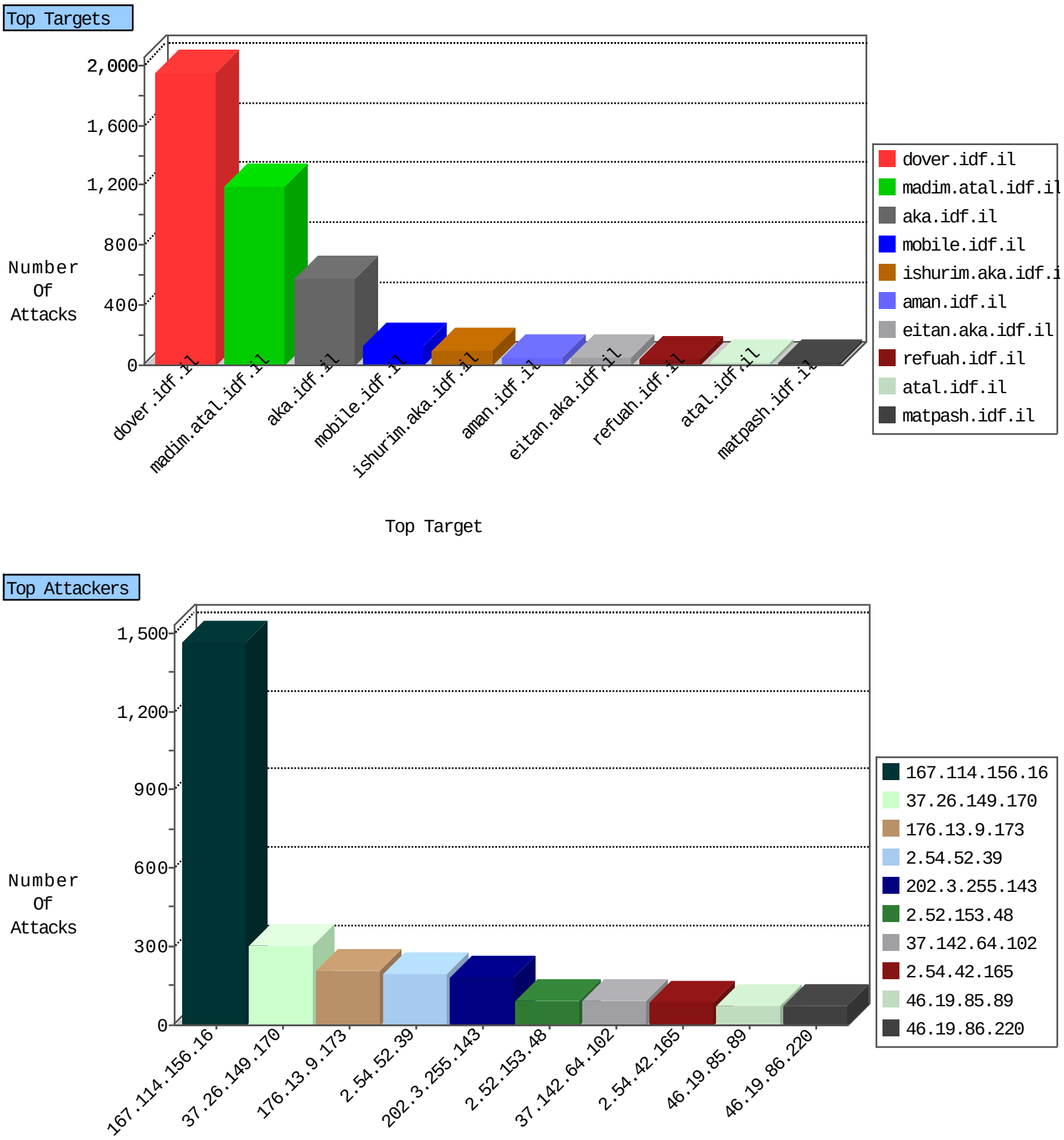
01-17-2016-11:04:00 to 01-17-2016-12:04:00

IDF Under Attack Daily Report



01-17-2016-11:04:00 to 01-17-2016-12:04:00

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	3284
212.179.8.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
84.109.13.208	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
47.32.30.199	Canada	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
222.174.5.17	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
146.185.239.100	Russian Federation	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
85.203.17.170	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
24.19.110.22	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
199.255.214.83	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
115.239.228.10	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Http	drop	1
171.41.52.48	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
58.153.169.134	Hong Kong	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
85.203.17.44	Netherlands	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1

01-17-2016-11:04:00 to 01-17-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.75	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-17-2016-11:04:00 to 01-17-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	147
193.104.41.54	147.237.0.35	Moldova, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
176.13.13.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.43.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.84.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.75	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1
182.18.160.216	147.237.0.19	India	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.230.93.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

01-17-2016-11:04:00 to 01-17-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.118.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
176.13.17.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
87.68.35.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.2.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.250	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
157.55.39.60	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	13
46.19.86.152	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
207.46.13.24	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.129.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.130.238	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.2.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
40.77.167.52	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
40.77.167.18	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.219.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.172.106	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.2.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.18.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.216.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.199.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
195.182.33.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.147.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
195.182.33.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
188.120.152.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.136.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
94.230.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

01-17-2016-11:04:00 to 01-17-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	134
2.54.52.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
37.142.64.102	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (403) in Session from 37.142.64.102	Block	91
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
2.54.42.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
2.54.52.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
2.52.153.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.149.170	Block	51
176.13.9.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
2.54.157.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
176.13.20.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
176.13.13.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.201.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
2.54.42.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.10.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.192.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
87.68.35.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	5
2.54.173.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.44.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.115.252.2	Block	3
46.19.86.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.213.112	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	3
176.13.6.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.184.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/1/	Block	3
79.180.48.94	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.2.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
176.13.6.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
77.127.165.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.188.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.247.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.188.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.242.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
212.29.203.226	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 212.29.203.226	Block	1
46.19.86.71	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
149.78.161.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.154.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1

01-17-2016-11:04:00 to 01-17-2016-12:04:00