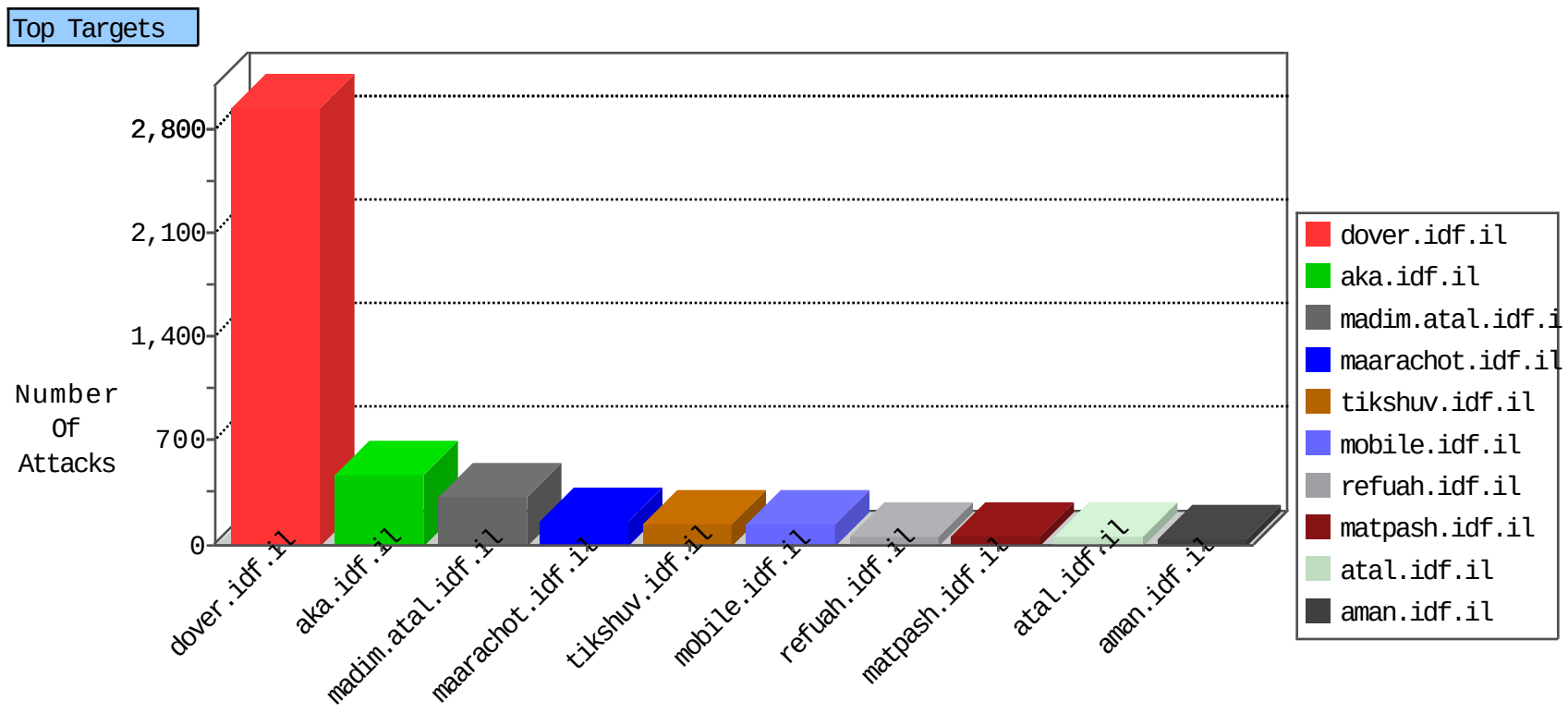
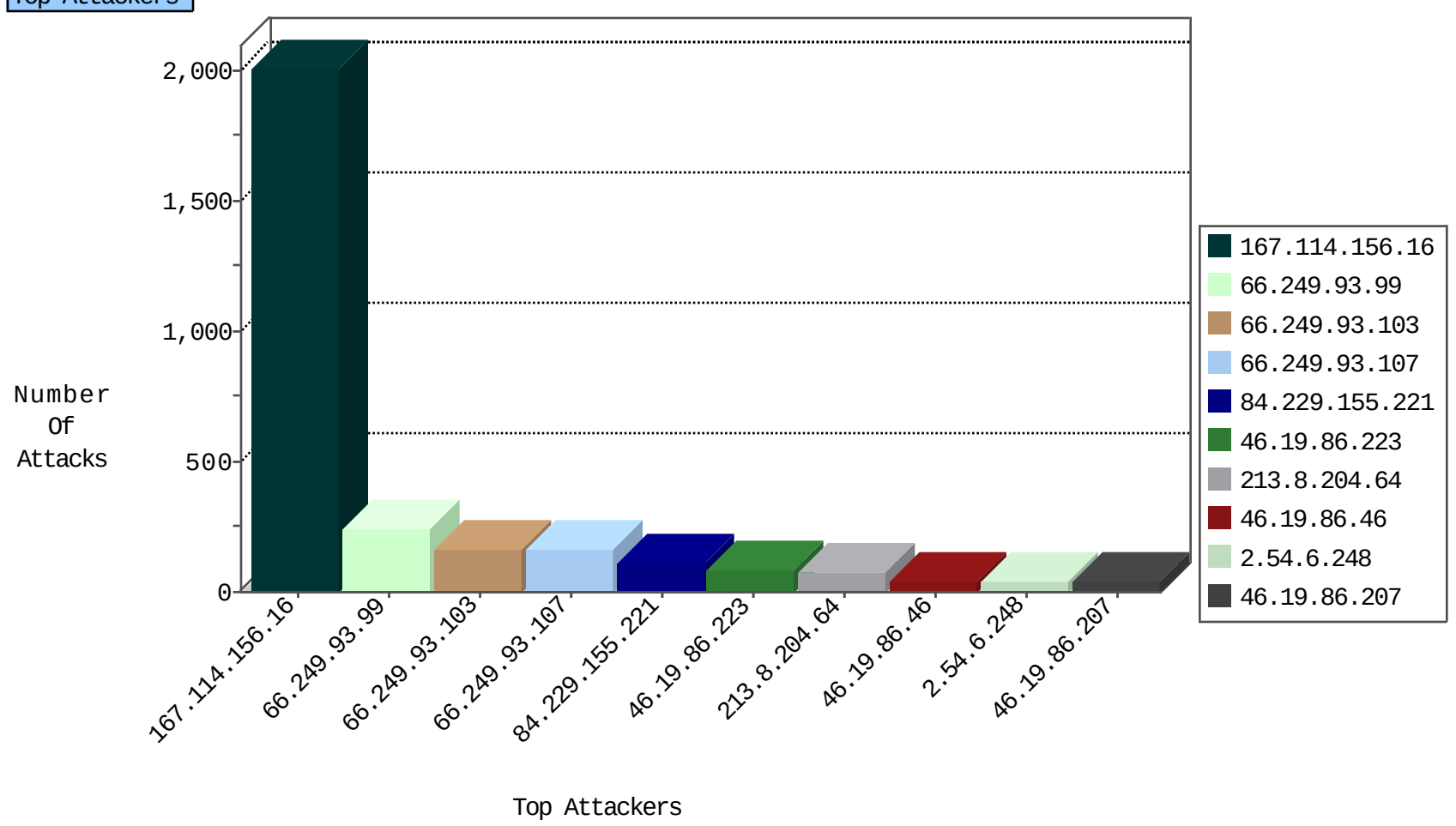
01-03-2016-15:04:01 to 01-03-2016-16:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-03-2016-15:04:01 to 01-03-2016-16:04:01

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	DOS-Tool-SwitchbladG	dest-reset	3252
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.180.210.227	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.210.227	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.134.8	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
208.67.1.60	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Udp	drop	1
173.195.0.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

01-03-2016-15:04:01 to 01-03-2016-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-03-2016-15:04:01 to 01-03-2016-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.116.212.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.89.70.205	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.177.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.54	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
185.130.5.224	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
169.0.8.7	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.4.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.165.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.110.33.83	147.237.0.19	China	madim.atal.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1

01-03-2016-15:04:01 to 01-03-2016-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.99	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	80
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	80
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	79
66.249.93.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
66.249.93.103	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	54
66.249.93.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	54
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	53
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
66.249.93.107	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
132.64.31.80	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
62.0.200.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
107.167.107.175	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
46.19.85.5	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.147.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.183.68.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
217.132.131.205	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
89.139.143.164	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.183.52.102	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
85.65.247.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.8.90.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.22.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.128.48.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
194.56.215.218	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.13.5.210	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.26.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
81.218.66.107	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.182.187.52	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.182.187.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.6.0.15	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.178.160.54	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.46	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
85.130.218.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.12.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.107	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.46	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

01-03-2016-15:04:01 to 01-03-2016-16:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.155.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
213.8.204.64	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
2.54.6.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
2.54.44.107	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
84.229.155.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.223	Block	13
2.54.31.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.5.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
85.64.6.196	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.6.196	Block	6
93.87.146.250		147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.204.27	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.204.27	Block	4
93.87.146.250		147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 93.87.146.250	Block	4
2.54.131.58	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 2.54.131.58	Block	3
185.32.179.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.39.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.192	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 37.26.146.192	None	3
2.54.166.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.27	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
37.26.148.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.218.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.13.36	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
80.179.18.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.179.18.61	Block	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/milnet	Block	2
84.108.219.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.20.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.180.132.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.166.184.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.20.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.168.113.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.35	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	2
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Illegal HTTP Version (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12H143	Block	1
83.130.109.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
193.34.56.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
109.66.207.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.134.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.219.50.236	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.246.137.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
179.188.17.23	Brazil	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
168.144.92.208	Canada	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/	None	1

01-03-2016-15:04:01 to 01-03-2016-16:04:01