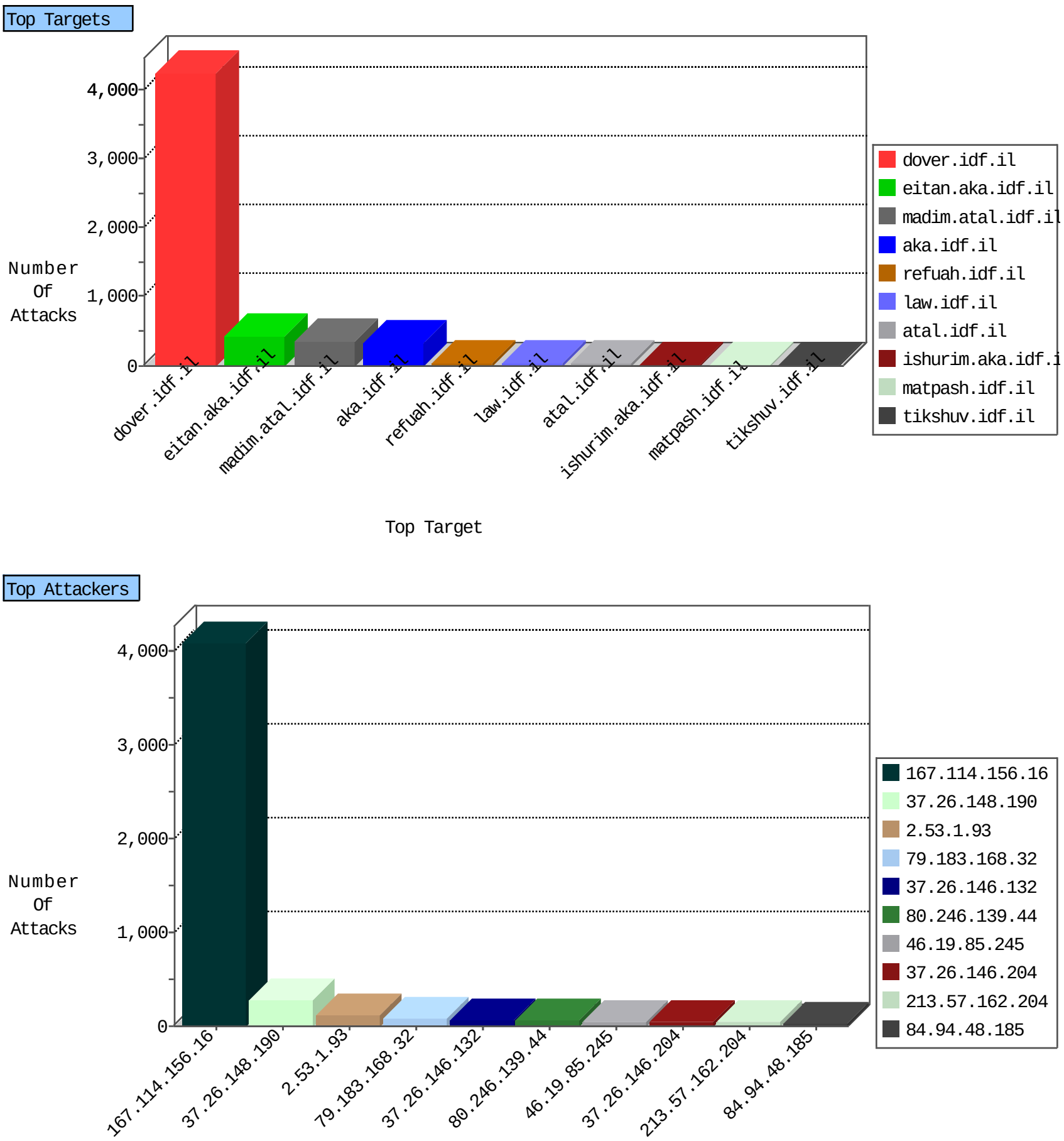
04-18-2016-13:04:00 to 04-18-2016-14:04:00

IDF Under Attack Daily Report



04-18-2016-13:04:00 to 04-18-2016-14:04:00

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	Block_Ip_Web_In	drop	4082
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
82.102.135.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.145.211.4	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
107.150.32.61	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
173.208.197.254	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
69.197.185.22	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
159.122.220.135	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
71.6.158.166	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
159.122.220.135	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-13:04:00 to 04-18-2016-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-18-2016-13:04:00 to 04-18-2016-14:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.6.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.181.123.161	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.62.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.77.226	Latvia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.118.99.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.12.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.217.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.112.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.178.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.168.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.228.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-18-2016-13:04:00 to 04-18-2016-14:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	273
79.183.168.32	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
84.94.48.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
85.64.86.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
149.50.72.53	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.162.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.6	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
84.108.26.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.238.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.214	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.94.188.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
141.0.15.209	Norway	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.180	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.121.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.181.27.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.162.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.238.109	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.154.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.162.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.121.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.228.165.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.0.238.109	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.229.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.133.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.162.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
62.0.238.109	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.180	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.166.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.26.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.168.112.36	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.203.215.1	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.39.236	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.26.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.138.192.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.108.26.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.26.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-18-2016-13:04:00 to 04-18-2016-14:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.1.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
37.26.146.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
80.246.139.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
37.26.146.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
109.253.218.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.148.27.130	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 80.148.27.130	Block	4
213.8.204.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	4
80.246.130.97	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.121.26.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.227.71.250	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	3
2.53.166.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.132	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.232.41.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
213.57.107.187	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.107.187	Block	2
131.253.25.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/shared/datepicker.css	None	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	1
89.139.143.207	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.177.217.143	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
46.19.85.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
173.208.197.254	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
93.173.43.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	None	1
2.53.160.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
213.57.107.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	1
199.203.136.130	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.79.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/109496.pdf	Block	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
89.234.68.70	Ireland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.180.57.42	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
175.44.14.95	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
109.64.37.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/sa_swfobject.js	None	1
217.132.159.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.159.36	Block	1
207.232.41.2	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.232.41.2	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/shared/clientscripts/clientscripts.js	None	1
89.234.68.70	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
175.44.14.95	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.14.95	Block	1
109.65.10.173	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/421-2258-he/patzar.aspx	Block	1
31.168.23.60	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter wb48617274 in www.eitan.aka.idf.il/style/1.he/960.css	None	1
2.55.189.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.65.171.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9696-he/refuah.aspx	Block	1
149.50.125.61	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

04-18-2016-13:04:00 to 04-18-2016-14:04:00