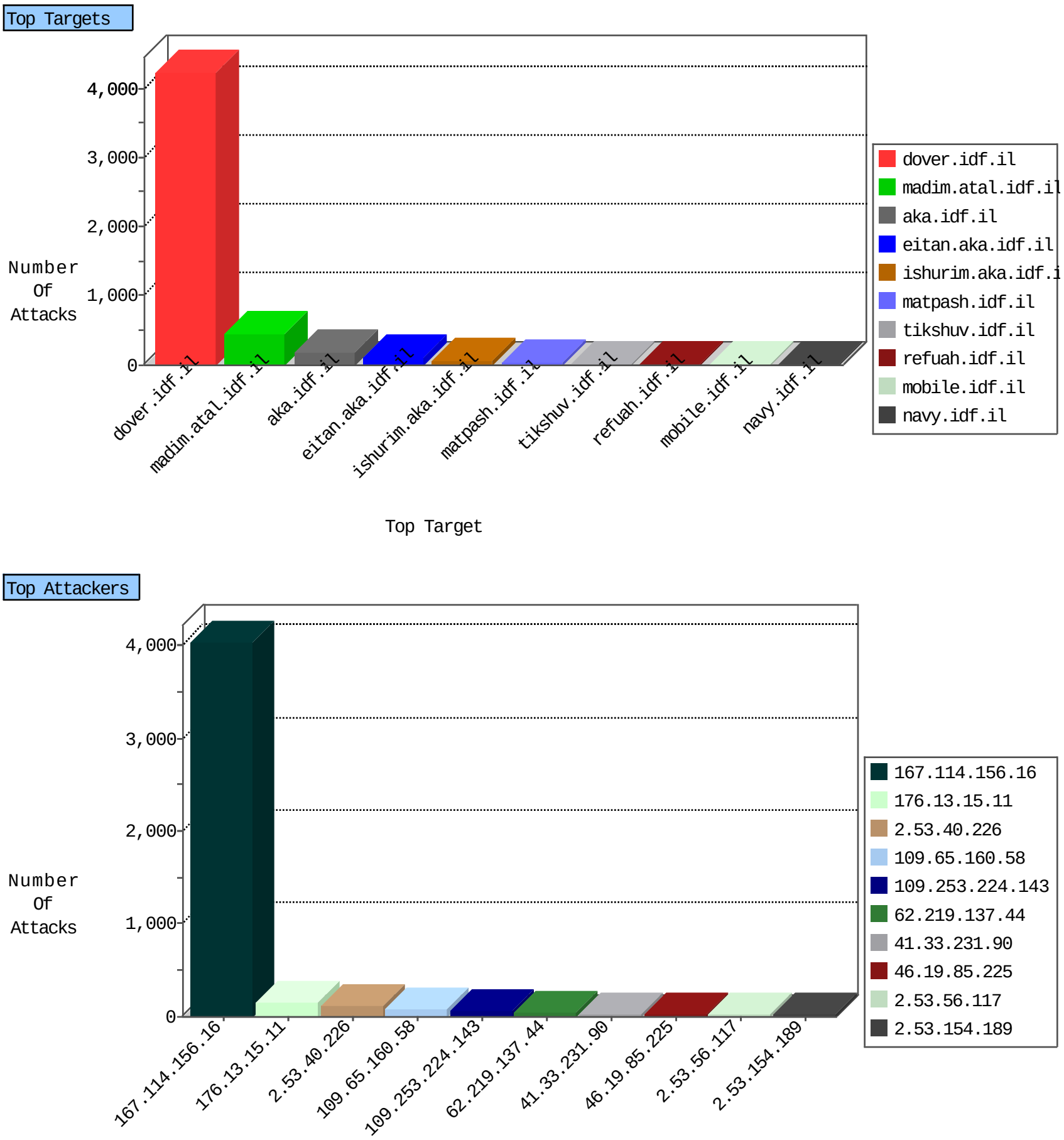
04-18-2016-09:04:00 to 04-18-2016-10:04:00

IDF Under Attack Daily Report



04-18-2016-09:04:00 to 04-18-2016-10:04:00

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	4033
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
82.145.209.40	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
82.145.218.133	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
184.105.139.114	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.207	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.231	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.0.33	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
184.105.139.126	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-09:04:00 to 04-18-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.53.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
69.197.177.50	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
69.197.177.50	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.50	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-18-2016-09:04:00 to 04-18-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
78.39.158.87	147.237.8.27	Iran, Islamic Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
212.129.15.245	147.237.76.196	France	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.8	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
184.80.10.136	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
87.68.29.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.254.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.112.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
204.152.218.49	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.8	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
109.65.237.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
96.237.50.37	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

04-18-2016-09:04:00 to 04-18-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.160.58	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.53.154.189	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
91.199.100.249	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.172.158.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.147.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.225	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.225	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.128.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.200.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
176.13.2.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.114.23.18	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.3.144.11	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.22.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.229.27.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.24	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.237.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.30.25.116	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.70.109	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.203.92.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.182.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.4.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.222.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.70.93.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.21.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.2.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.12.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.12.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.14.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.137.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.201.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.153.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.202.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.50.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-18-2016-09:04:00 to 04-18-2016-10:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.178.176.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.223.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	149
2.53.40.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
109.253.224.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
2.53.56.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
109.253.224.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
109.253.134.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
109.253.224.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
109.253.224.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
109.253.224.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.224.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.224.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.53.169.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.21.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
176.13.2.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.133.108	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
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	2
95.35.84.54	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 95.35.84.54 (Open Mode)	None	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
203.127.96.215	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.15.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Cookie Tampering on token: Login	None	1
93.139.78.120	Croatia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
208.113.248.195	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
192.116.190.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
157.55.39.83	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/pirsumim.asp	Block	1
80.246.133.195	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.181.78	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.117.113.18	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.208.16.10	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.137.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
95.35.84.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.64.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
37.46.39.132	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
204.3.219.103	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
191.252.44.242	Brazil	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
2.53.24.14	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
95.35.84.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
197.248.146.10	Kenya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.178.176.98	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.178.176.98	Block	1
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
176.13.2.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.139.78.120	Croatia	147.237.72.166	aka.idf.il	PHP Attempt	Block	1

04-18-2016-09:04:00 to 04-18-2016-10:04:00