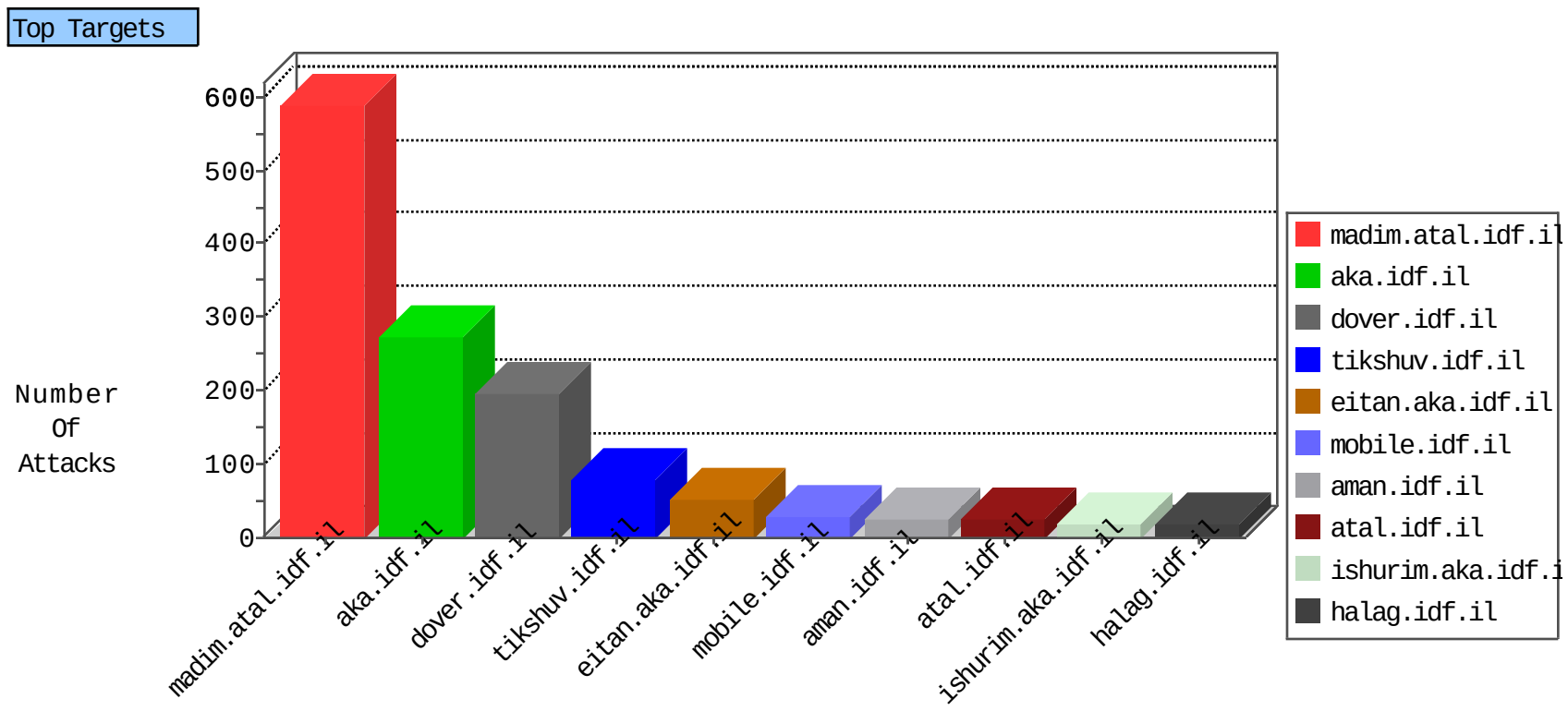
03-06-2016-13:04:03 to 03-06-2016-14:04:03

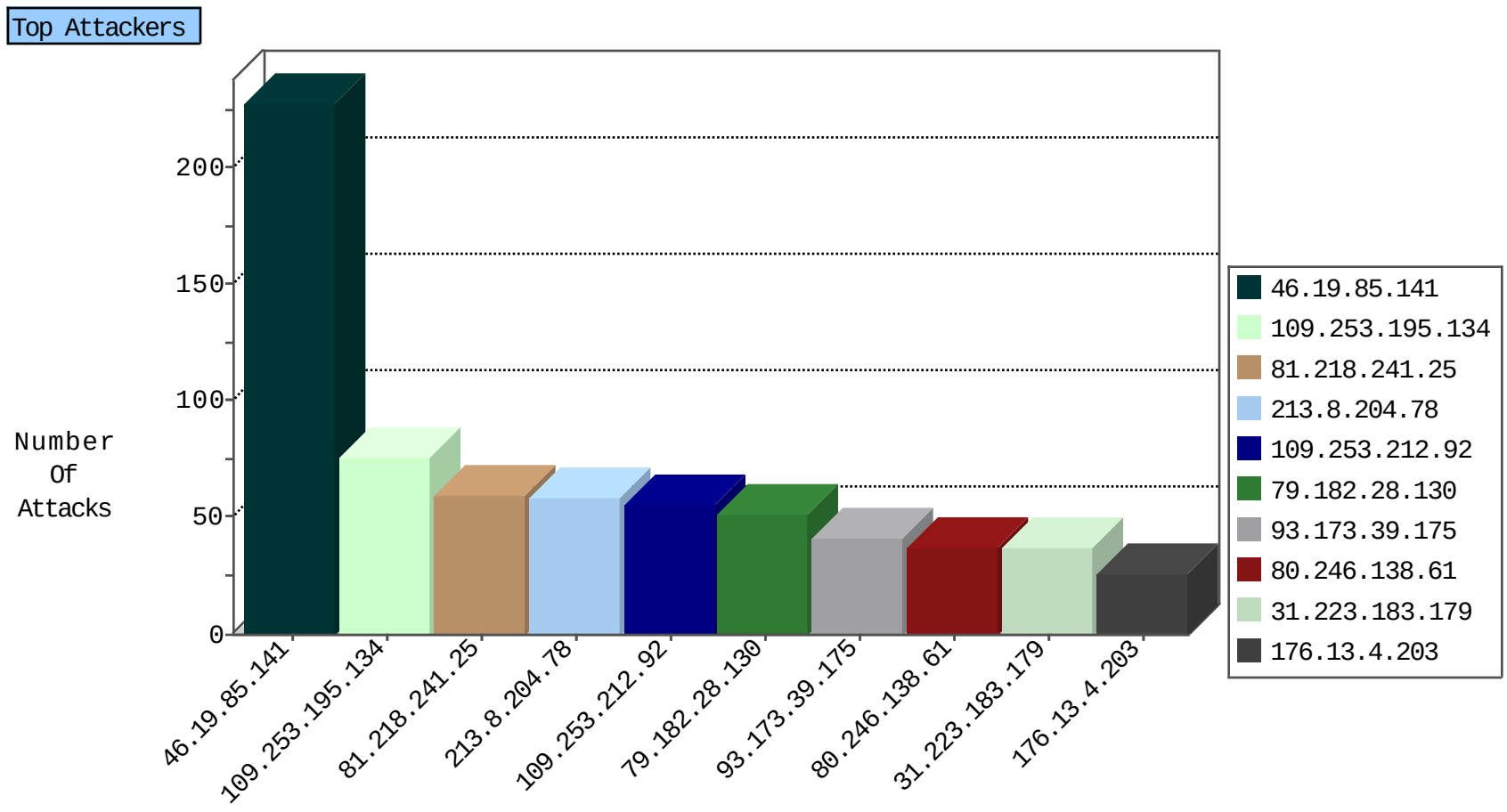
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
82.145.209.96	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
84.108.236.54	Israel	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
194.69.127.150	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.132	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
194.69.127.148	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.132	Netherlands	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
64.21.147.6	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
108.186.168.25	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
79.178.152.72	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.253.201.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
176.13.23.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.19.85.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.172.143	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
78.46.50.246	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.26.149.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.5.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.50.95.89	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
114.33.250.151	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.186.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.232.154	147.237.77.216	Israel	dover.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
176.13.8.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.196.117.70	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
109.253.206.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.231.192.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.77.176	Hong Kong	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.28.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
213.8.204.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	45
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
213.8.204.78	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
31.223.183.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.142.193.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
109.253.195.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.191.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.9.50	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.228.9.48	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
31.223.183.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.52.8.10	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.223.183.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.158.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
96.47.68.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.247.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.146.6.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.8.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.71.10.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.37	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.193.84	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.181.106.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.223.183.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
83.130.118.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
95.35.65.183	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
31.223.183.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.186	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.223.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.183	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.104	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
83.130.100.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.44.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.8.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.85.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.170.103	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.39.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.18.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.57.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.140.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.17.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.26.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.175.47	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	3

03-06-2016-13:04:03 to 03-06-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	227
109.253.195.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
109.253.212.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
93.173.39.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.138.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.4.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.170.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
80.246.137.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.136.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.5.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.89.217.230		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.89.217.231		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.64.222.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/	Block	5
185.89.217.228		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.89.217.227		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.89.217.233		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.89.217.224		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.138.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.225		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.141.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.81.177	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
185.89.217.234		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.136.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.195.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.235		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.226		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.167.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method anguage: in URL he-il,en-us	Block	1
141.212.122.129	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /x	Block	1
87.70.6.192	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
213.8.204.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
84.108.112.101	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
192.117.170.194	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.64.70	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
24.3.252.222	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
92.115.108.254	Moldova, Republic of	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
87.70.6.192	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
46.116.205.204	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.116.205.204 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
207.232.21.105	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to tech.atal.idf.il/style/shared/960.css	Block	1
37.46.38.192	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed PHP Attempt	Block	1
94.230.93.50	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
66.249.75.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/brothers/skira/default.asp	Block	1
87.70.6.192	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-06-2016-13:04:03 to 03-06-2016-14:04:03