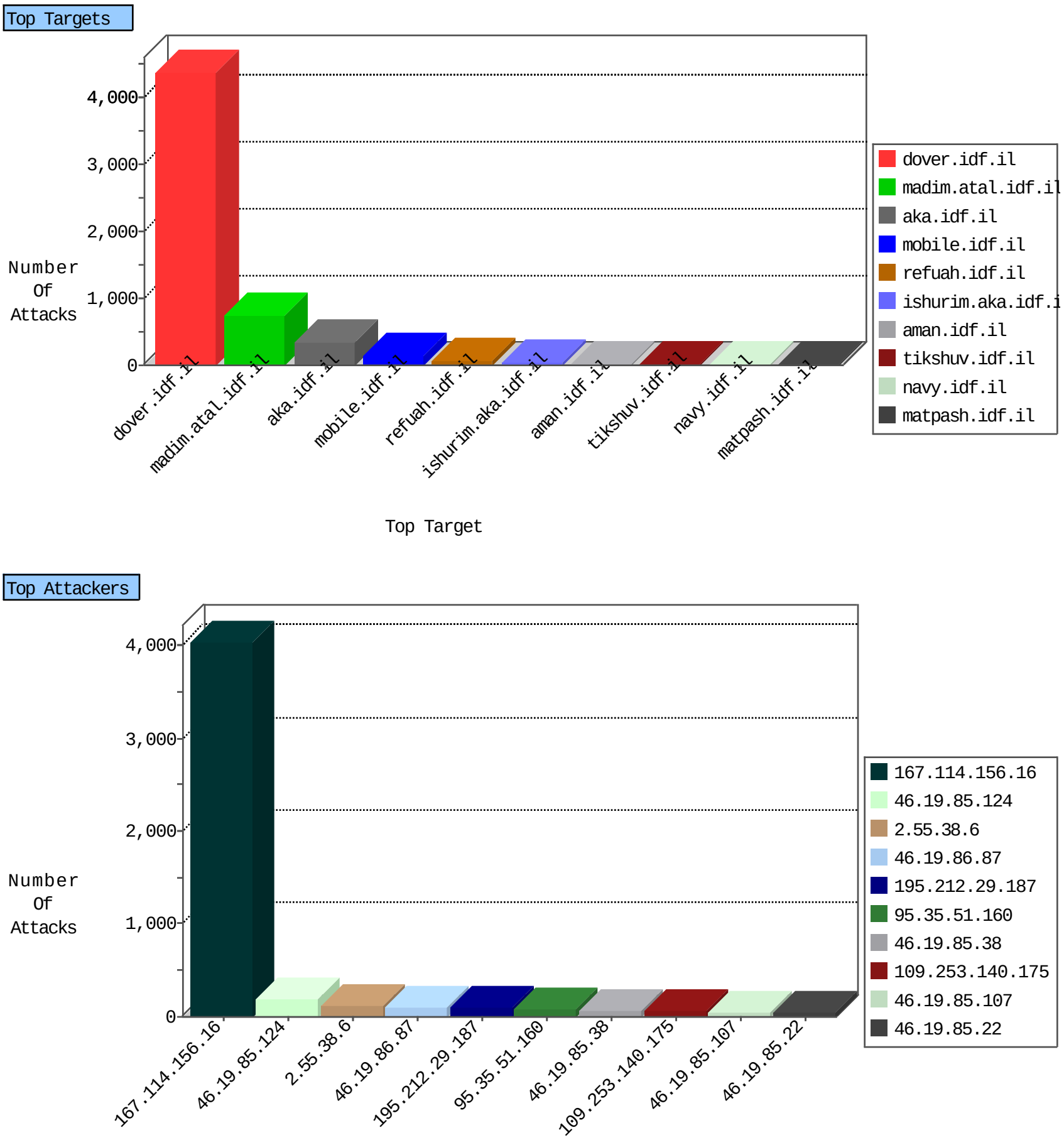
04-17-2016-16:04:04 to 04-17-2016-17:04:04

IDF Under Attack Daily Report



04-17-2016-16:04:04 to 04-17-2016-17:04:04

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	4034
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.228.76	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	2
185.94.111.1	Russian Federation	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
198.20.87.98	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
104.244.194.2	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1

04-17-2016-16:04:04 to 04-17-2016-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.32.63	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.32.63	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
171.96.176.226	Thailand	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
171.96.176.226	Thailand	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

04-17-2016-16:04:04 to 04-17-2016-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
73.187.117.50	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	2
85.131.208.140	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.8.45.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.16.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.14.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.243.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
73.187.117.50	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
73.187.117.50	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
87.71.56.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.187.117.50	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
87.69.62.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.187.117.50	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.176.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.181.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.106.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.105.20.127	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
73.187.117.50	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
73.187.117.50	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
87.69.149.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-17-2016-16:04:04 to 04-17-2016-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.212.29.187	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	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	26
2.55.35.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.147.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.37.243.87	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.253.226.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.228.162.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.253.226.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
37.26.146.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.147.131	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.172.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
193.43.245.250	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
41.37.243.87	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
5.22.130.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.37.243.87	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.102.195.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.209.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.246.250	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
109.67.253.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.101	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.61.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.182.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.105.231	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.55.136.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.8	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.26.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.106.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.101.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
117.41.235.233	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.65.111.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
95.35.51.160	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
2.53.190.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	5
94.230.86.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.55.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.64.247.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

04-17-2016-16:04:04 to 04-17-2016-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	194
2.55.38.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
95.35.51.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.140.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
176.13.1.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.19.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.55.35.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
132.69.245.173	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 132.69.245.173	Block	5
109.253.226.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.150.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.61.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
80.246.133.65	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.17.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/5/71725.pdf‍	Block	2
84.94.74.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
81.111.195.163	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.177.105.231	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
5.29.249.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Unknown HTTP Request Method ìˆ Ø,jÒÓ[[#23]]ŠùÍ[[#19]]w_'E/[[#0]]ã5•[[#17]]›¬ŒL9[[#14]] in URL š#[[#17]]a±Ù¼‰qqך'v[[#19]]j	Block	1
2.53.173.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9366-he/refuah.aspx	Block	1
84.108.51.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	NULL Character in Method ÿkú³Âz)Z,¢žh[[#0]]”[[#5]]LÍ[[#7]]	Block	1
80.246.130.45	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.61.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method ìˆ Ø,jÒÓ[[#23]]ŠùÍ[[#19]]w_'E/[[#0]]ã5•[[#17]]›¬ŒL9[[#14]]	Block	1
66.249.66.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
103.249.38.215	India	147.237.77.74	law.idf.il	PHP Attempt	Block	1
81.111.195.163	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
185.32.179.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.4.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.3.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/miluim/miluimnikpail/general.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
2.53.174.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.226.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/5/71725.pdf‍	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/miluim-over.jpg	Block	1
47.54.80.127	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
212.235.79.242	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	1
84.228.162.82	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

04-17-2016-16:04:04 to 04-17-2016-17:04:04