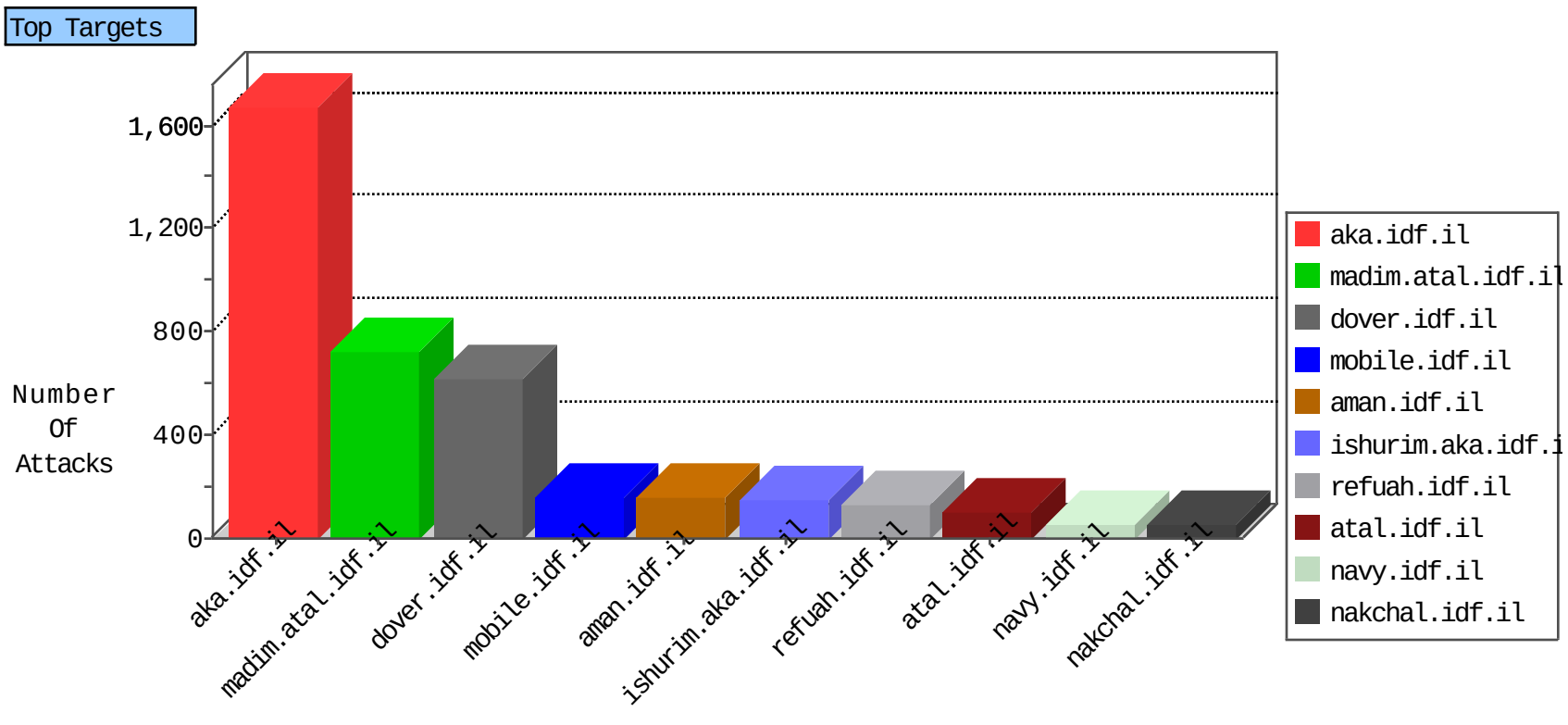
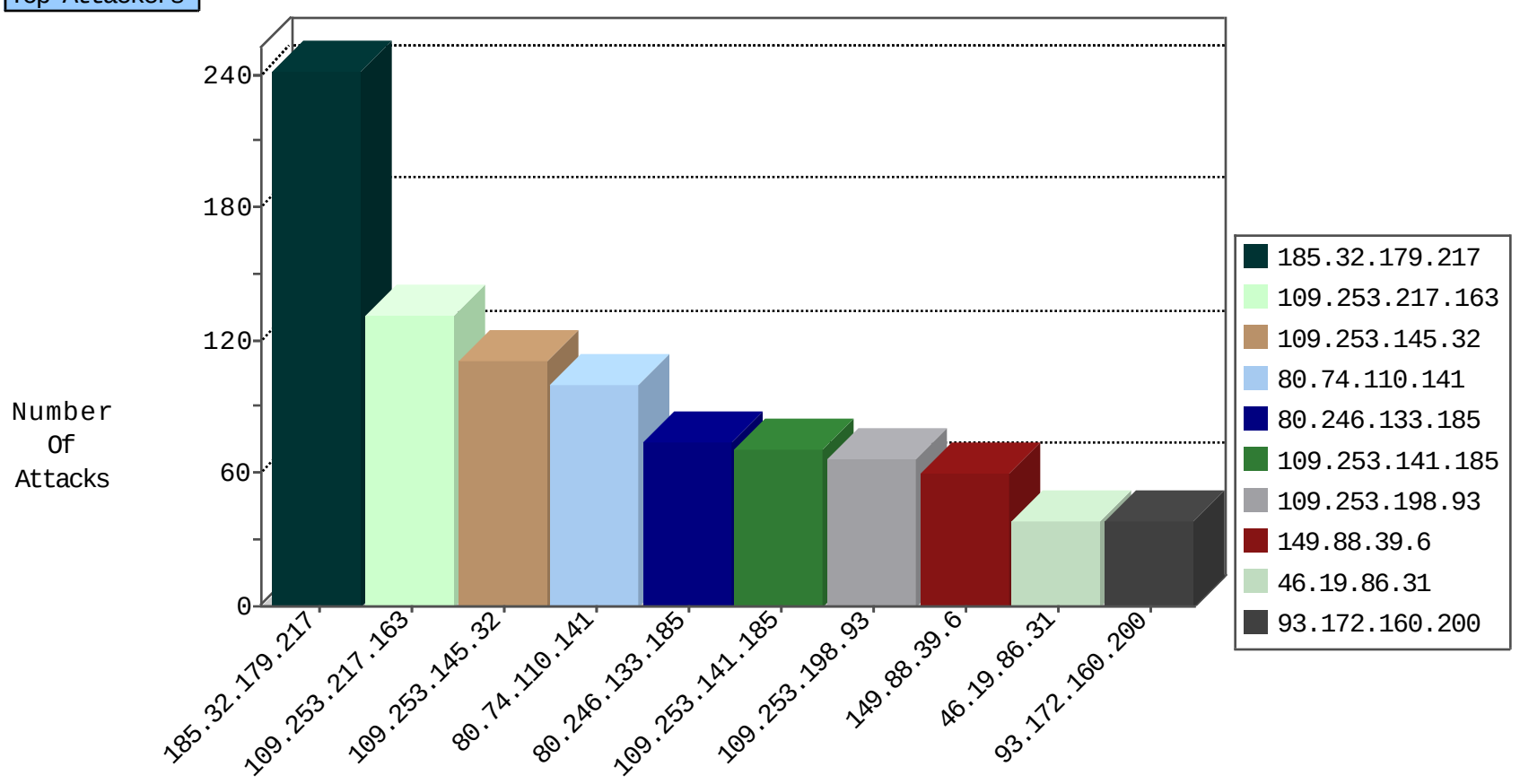
01-31-2016-17:04:06 to 01-31-2016-18:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-31-2016-17:04:06 to 01-31-2016-18:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.68	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	86
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	49
109.65.7.75	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
66.249.78.95	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
185.53.44.157	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
95.100.174.66	Europe	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.213	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

01-31-2016-17:04:06 to 01-31-2016-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-31-2016-17:04:06 to 01-31-2016-18:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
174.37.194.144	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
134.191.232.68	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
46.120.142.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
174.37.194.144	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.138.102.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sA (2)	1
84.109.82.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.131.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.130.6.191	147.237.77.121	United States	e.navy.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.151.53.217	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.160.181.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.28.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.124.121.194	147.237.76.201	Australia	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.206.201.94	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.109.163.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.140.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.11.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.154.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.216.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.218.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.218.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.215.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.131.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.54.250.106	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1

01-31-2016-17:04:06 to 01-31-2016-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
80.74.110.141	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	67
149.88.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
80.74.110.141	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	30
149.88.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
109.253.141.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
109.253.141.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
109.253.145.32	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
87.68.163.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
109.253.223.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
93.172.160.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
93.172.160.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
109.253.212.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.31	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
176.13.15.237	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
176.13.15.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
109.253.217.163	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
89.138.91.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
109.253.141.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.210.227.119	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	15
87.68.163.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.86.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.138.92	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
84.228.121.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
5.168.203.40	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
213.16.115.22	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.138.92	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.32.208.195	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
109.253.216.11	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.147.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.147.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.198.93	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
90.177.38.140	Czech Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.177.135.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.177.135.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
90.177.38.140	Czech Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.226.46.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.149.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.145.32	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.217.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.145.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.217	Block	67
109.253.198.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
80.246.140.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.130.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.54.144.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
109.253.147.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.210.154.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.52.15.83	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	18
31.154.94.21	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.94.21	Block	17
176.13.13.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 185.32.179.217	Block	8
80.246.139.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.64.191.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	5
2.54.49.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	3
37.26.149.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.253.197.111	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
79.180.186.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.143.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.233.179	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.204.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.158.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.107.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/home/home.asp	Block	2
109.253.156.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.179.115.198	Block	2
79.179.206.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
179.188.17.56	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.19.86.252	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.123.118.77	United Kingdom	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
95.86.116.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/userdetails.aspx	Block	1
220.134.189.104	Taiwan	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
79.183.105.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.65.52.222	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
31.154.232.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/resources/images/master/favicon.png	Block	1
87.69.196.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.96.187.74	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Ãª[[#28]]Ã»Ã²Âš[[#15]]	Block	1
50.116.75.183	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
2.54.179.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.32.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1