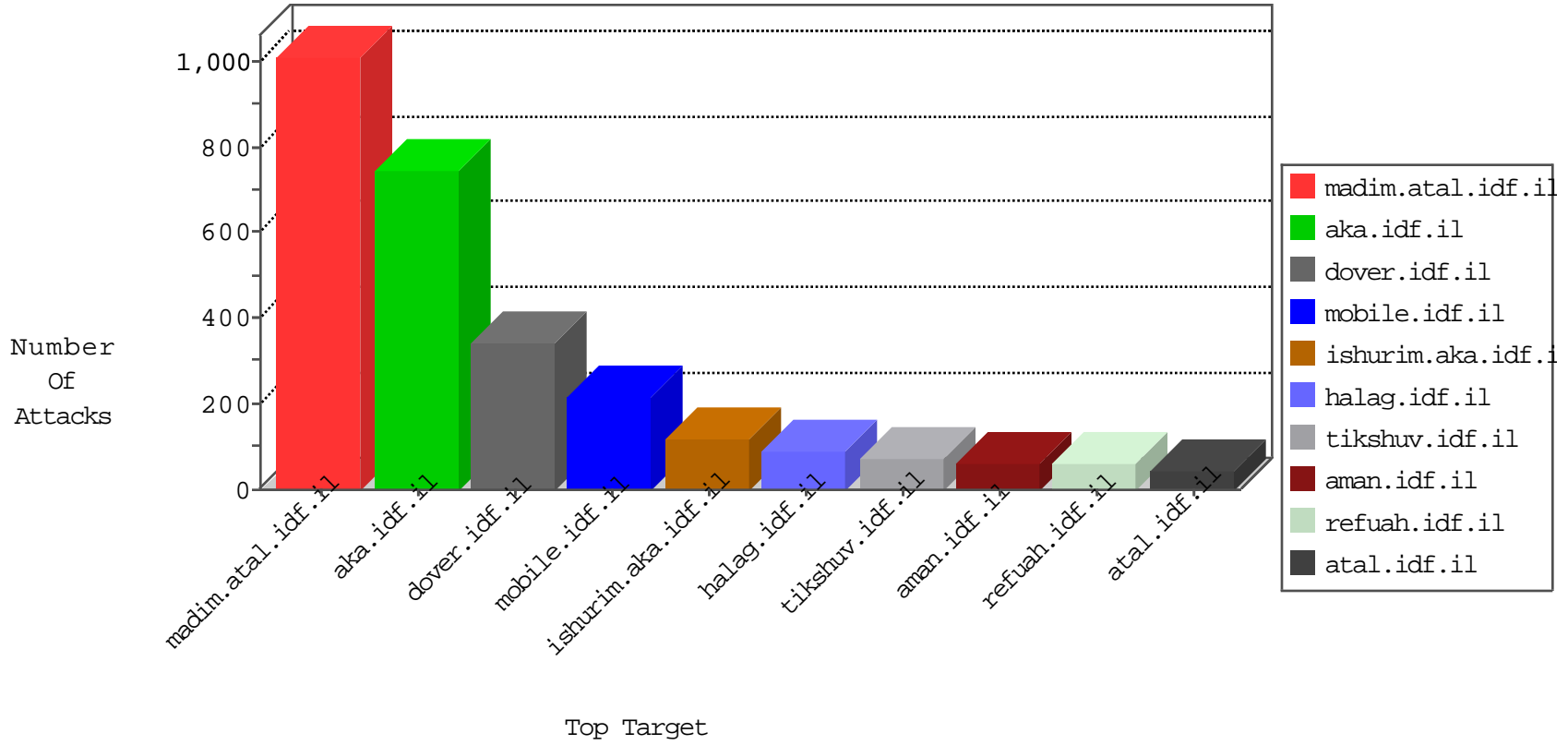


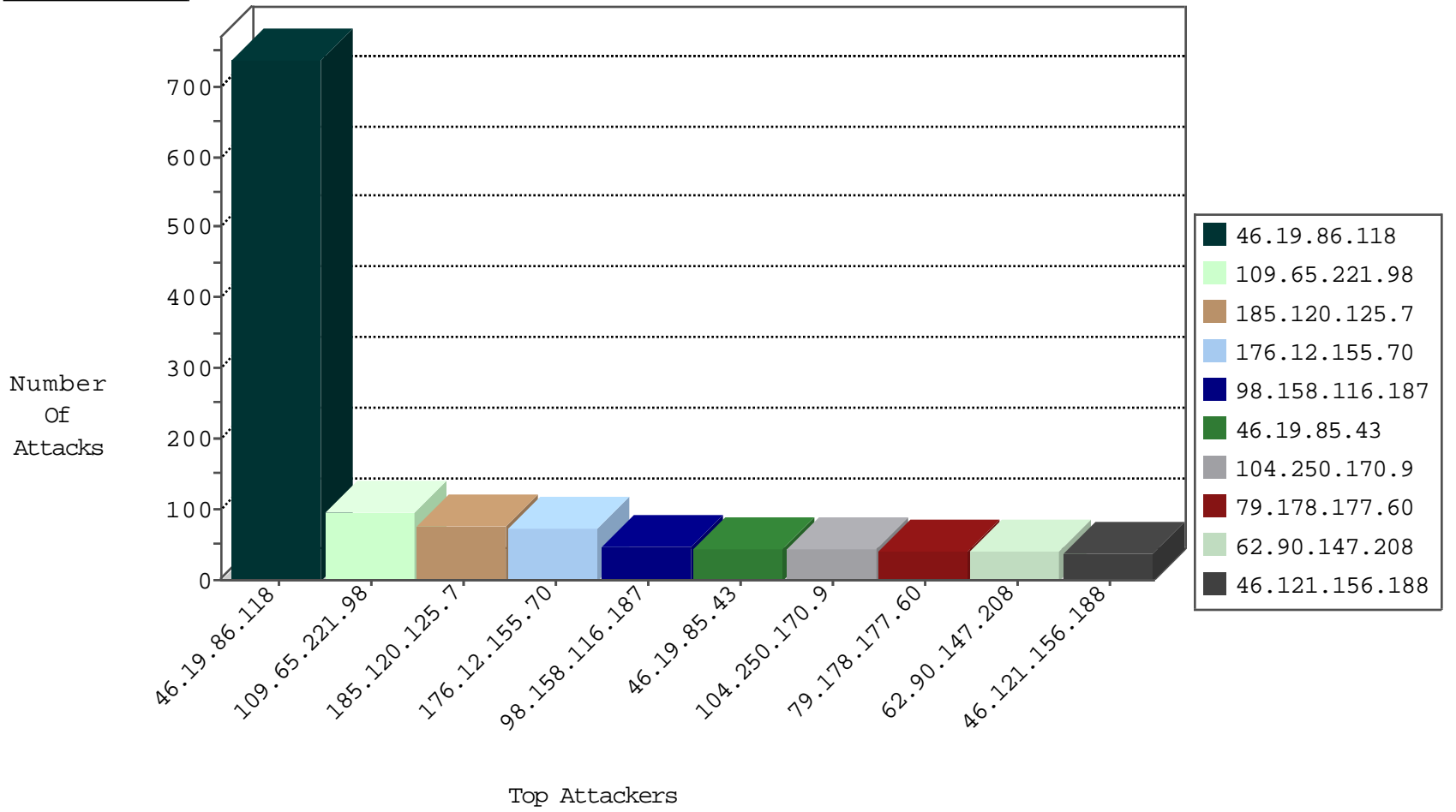
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
178.239.62.139	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
178.239.62.139	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
178.239.62.139	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.165	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
178.239.62.139	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.56.148.27		147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
45.56.148.27		147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
45.56.148.27		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.44.135.196	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
79.179.11.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.176.206.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.62.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.214.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.228.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.158.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.250.170.9	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.250.170.9	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.138.111.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.142.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.154.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.177.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
77.127.239.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.218.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
109.67.128.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.250.170.9	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	1
104.250.170.9	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
104.250.170.9	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.67.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
79.178.177.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
46.19.85.43	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.121.156.188	Israel	147.237.72.166	aka.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	30
46.19.86.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
98.158.116.187	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
62.90.147.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
5.29.27.79	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
62.90.147.208	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	19
46.28.142.4	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
2.52.129.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
98.158.116.187	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
93.173.180.161	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.67.42.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.110.111.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
37.26.146.226	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.32.179.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
188.120.151.103	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.125.151.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.155.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.154.193	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.155.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
77.125.151.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	10
109.67.166.99	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.145	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.12.155.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.120.148.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
191.232.136.148	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.1.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.67.69.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.224	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.25.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.149.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.168.132.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.233.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.116.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.98.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-01-2016-17:04:03 to 02-01-2016-18:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.69.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.35.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.17.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.118	Block	503
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.118	Block	123
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
109.65.221.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
176.12.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
79.180.176.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.139.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
79.178.37.126	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.187.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.12.155.112	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
79.179.39.162	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.39.162	Block	5
46.19.86.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.12.154.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.64.200.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.66.184.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
105.154.210.228	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.24.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.129.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
105.154.210.228	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.154.210.228	Block	3
80.246.137.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.110.113	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.155.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.163.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.154.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.181.123.65	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.12.155.90	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
149.88.23.165	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
77.125.120.117	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.54.1.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
61.153.237.242	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
185.100.86.86		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.230.114	Bulgaria	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
5.29.169.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
79.178.177.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
92.176.147.122	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1