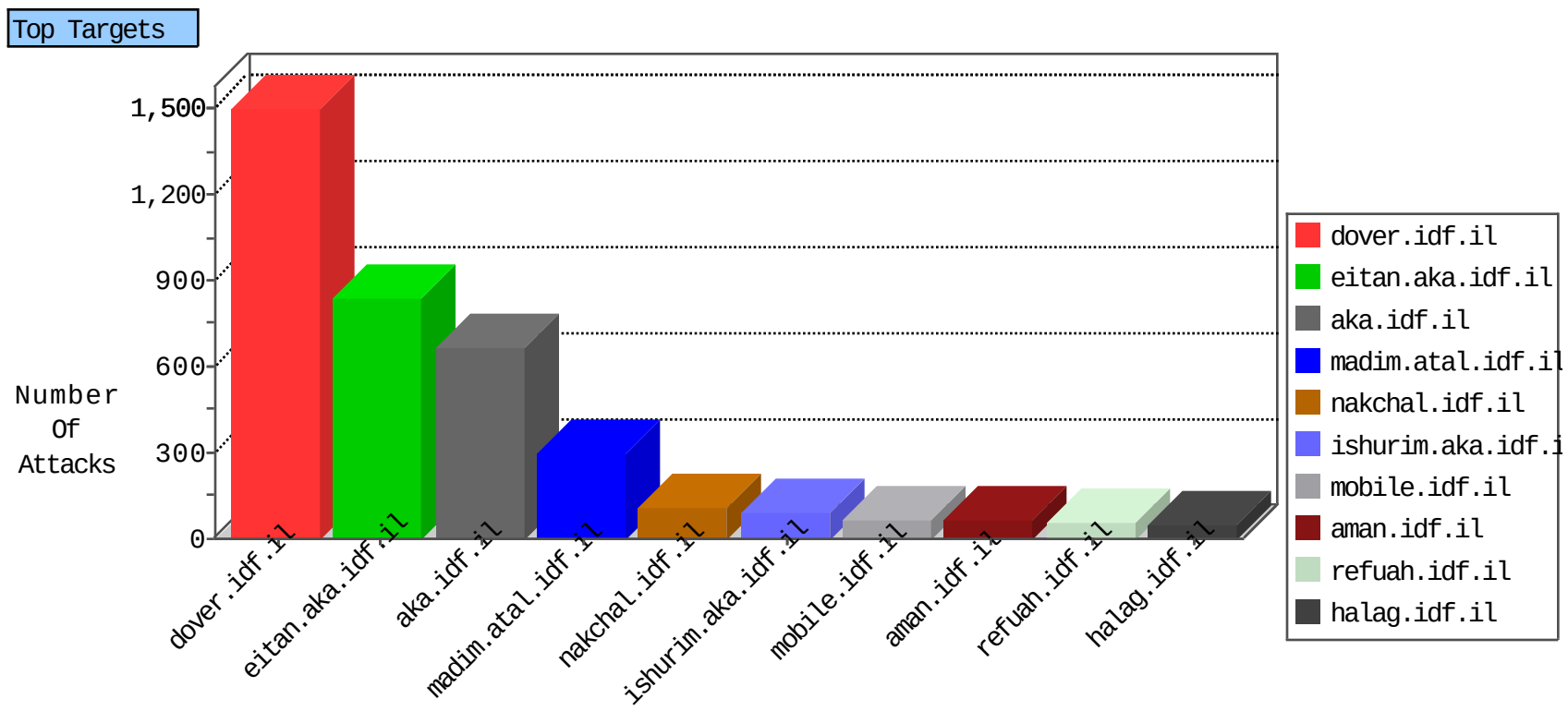
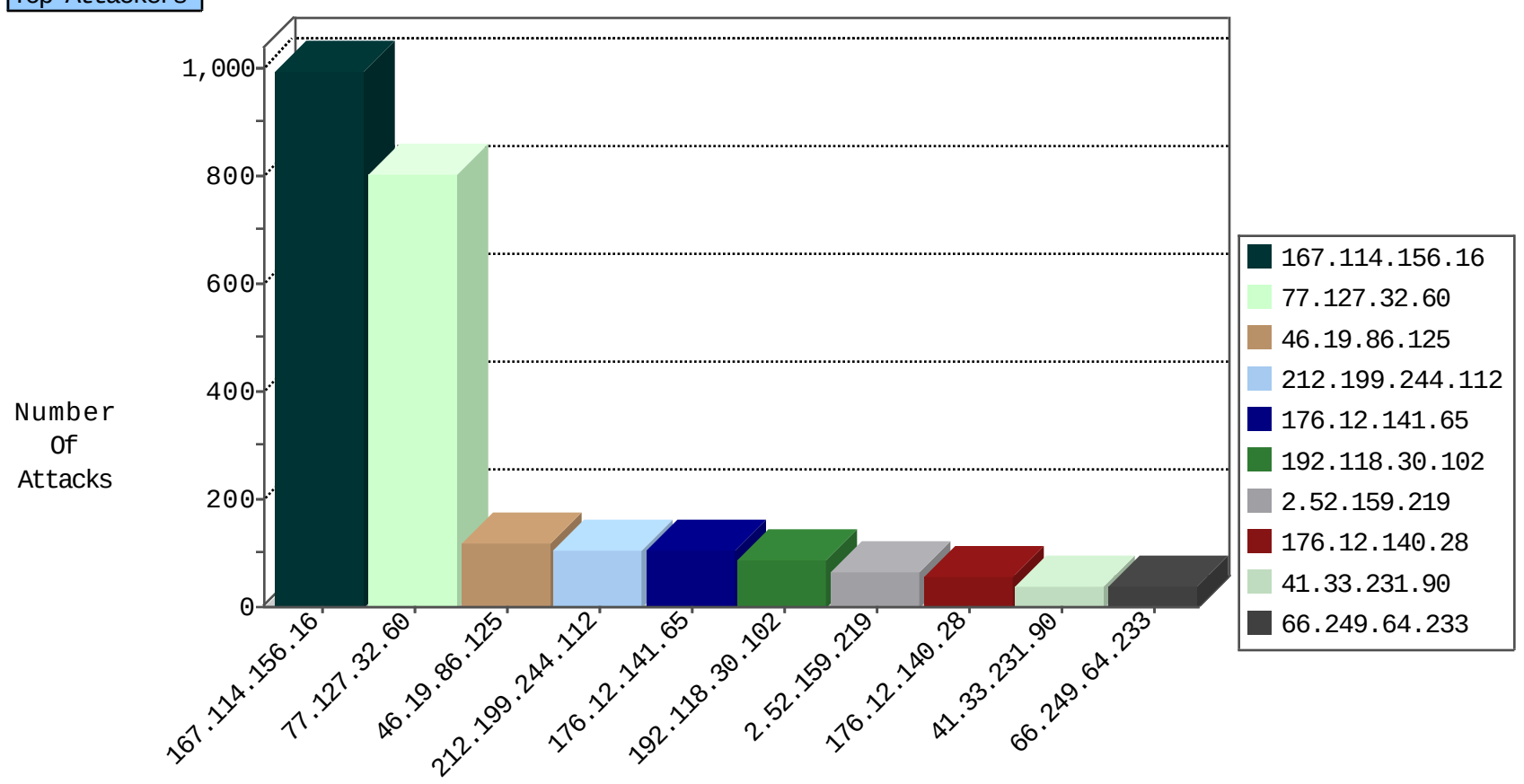
11-23-2015-14:04:04 to 11-23-2015-15:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-23-2015-14:04:04 to 11-23-2015-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	595
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	248
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	27
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.21.133	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
183.60.205.93	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
180.26.1.115	Japan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-23-2015-14:04:04 to 11-23-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
37.46.35.121	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
132.72.70.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
151.80.31.139	Italy	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-23-2015-14:04:04 to 11-23-2015-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
210.50.197.154	147.237.77.226	Australia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
128.139.251.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.18.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.221.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.66.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.241.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.142.96	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.154.91.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.30.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.190.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.185.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.147.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.215.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.117.209.136	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.76.42	Poland	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

11-23-2015-14:04:04 to 11-23-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	944
77.127.32.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	690
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.43.203		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
79.179.28.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
91.221.58.28	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.116.122.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.133.12	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
84.95.202.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
89.138.215.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.139.187.110	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
140.101.116.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.95	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	13
100.100.60.154		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
2.54.183.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
64.233.172.206	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.218	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
119.188.70.23	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.139.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.177.192.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.131.65.159	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
199.30.25.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.60.9.171	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.3.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.12.142.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.149.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.60.154		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

11-23-2015-14:04:04 to 11-23-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.32.60	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
212.199.244.112	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
176.12.141.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
2.52.159.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
176.12.140.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.52.34.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.1.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.12.141.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
176.12.151.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	8
46.116.122.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.125.241.184	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
87.69.235.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.54.30.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.215.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.20.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.136.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.176.60.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.42.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.182.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sacar	Block	2
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/70908.pdf	Block	1
176.12.137.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.200.12.220	Turkey	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
80.246.136.252	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 80.246.136.252	Block	1
50.195.116.61	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
79.180.207.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.52.2.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.19.86.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.111.38.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
176.12.144.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.183.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.133.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
213.151.39.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
141.212.122.96	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
46.117.251.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.52.56.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.117.151	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1

11-23-2015-14:04:04 to 11-23-2015-15:04:04