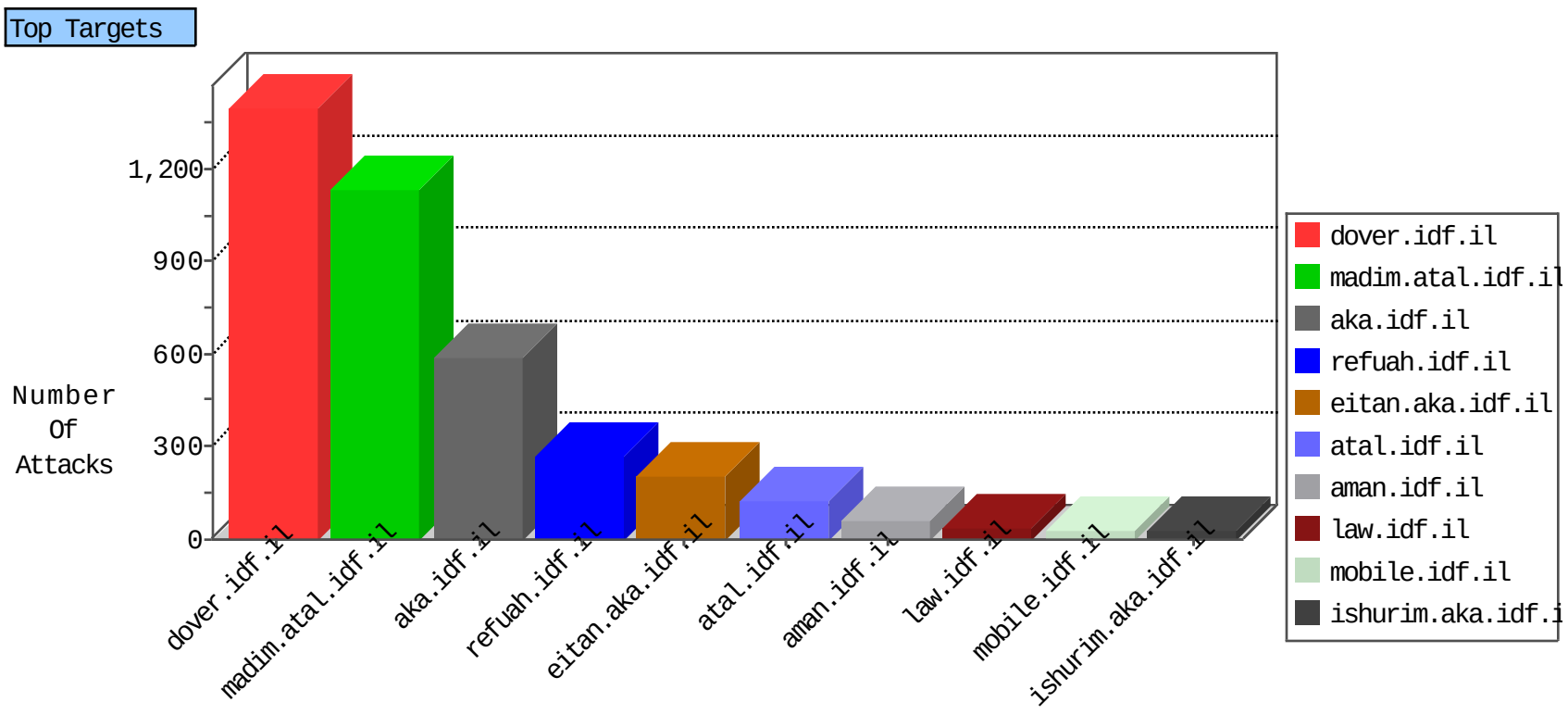
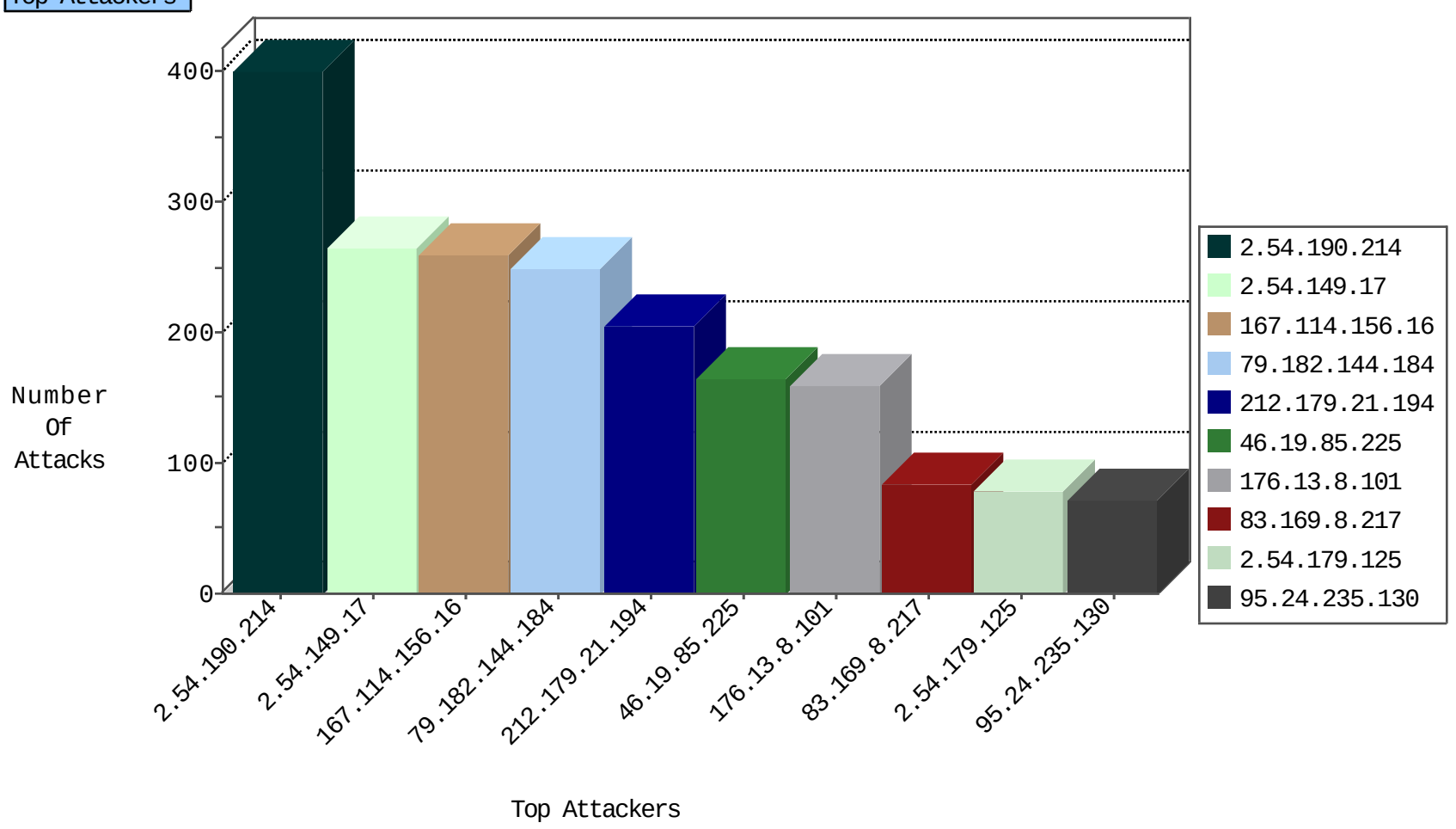
11-23-2015-17:04:01 to 11-23-2015-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-23-2015-17:04:01 to 11-23-2015-18:04:01

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	HTTP-POST-Segmented-DoS	dest-reset	8986
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1495
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	77
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	23
109.65.25.165	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.65.214.190	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
115.230.124.164	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
109.65.25.165	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
84.109.64.175	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
104.192.0.226	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.201	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

11-23-2015-17:04:01 to 11-23-2015-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.169.8.217	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	9
94.73.145.90	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
83.169.8.217	Germany	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
66.240.213.93	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
66.240.213.93	United States	147.237.77.243	mobile.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.130	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-23-2015-17:04:01 to 11-23-2015-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
83.169.8.217	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	71
94.73.145.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.240.213.93	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.144.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.234.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.243.16.106	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.204.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.76.148	Poland	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
84.109.64.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.24.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
79.178.202.10	147.237.0.34	Israel	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
176.13.6.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.118.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.39.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.1.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
77.109.38.223	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
192.95.12.59	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

11-23-2015-17:04:01 to 11-23-2015-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.144.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	242
2.54.179.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
95.24.235.130	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
66.87.82.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
94.242.206.183	Luxembourg	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.66.76	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
94.230.85.236	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.79.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
193.138.219.228	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
78.149.18.236	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
88.2.72.136	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.52.2.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
78.149.18.236	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
113.199.208.243	Nepal	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
213.57.61.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
89.139.37.160	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
100.100.108.31		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.57.61.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
64.79.85.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.31.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.102	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
207.46.13.17	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.129.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
100.100.12.14		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	192
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	123
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.8.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.190.214	Block	89
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.13.8.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
176.13.8.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.149.17	Block	34
176.13.2.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.12.144.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.12.141.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.120.126.32		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
79.180.5.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.141.26	Block	5
2.54.1.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
213.57.53.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.51.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
84.111.38.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
176.12.142.43	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.142.43	None	2
84.111.124.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
2.52.160.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.69.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.45.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.76.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
85.64.9.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.20.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.181.147.218	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
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.251.113	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.69.41.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.221.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx+x–x˜x™x‘xª xžx©x?x‘x™ x?x x•x©	Block	1
66.249.78.15	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/m/templates/getfile/getfile.aspx	Block	1
149.88.41.6	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.181.227	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	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
183.79.222.179	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1