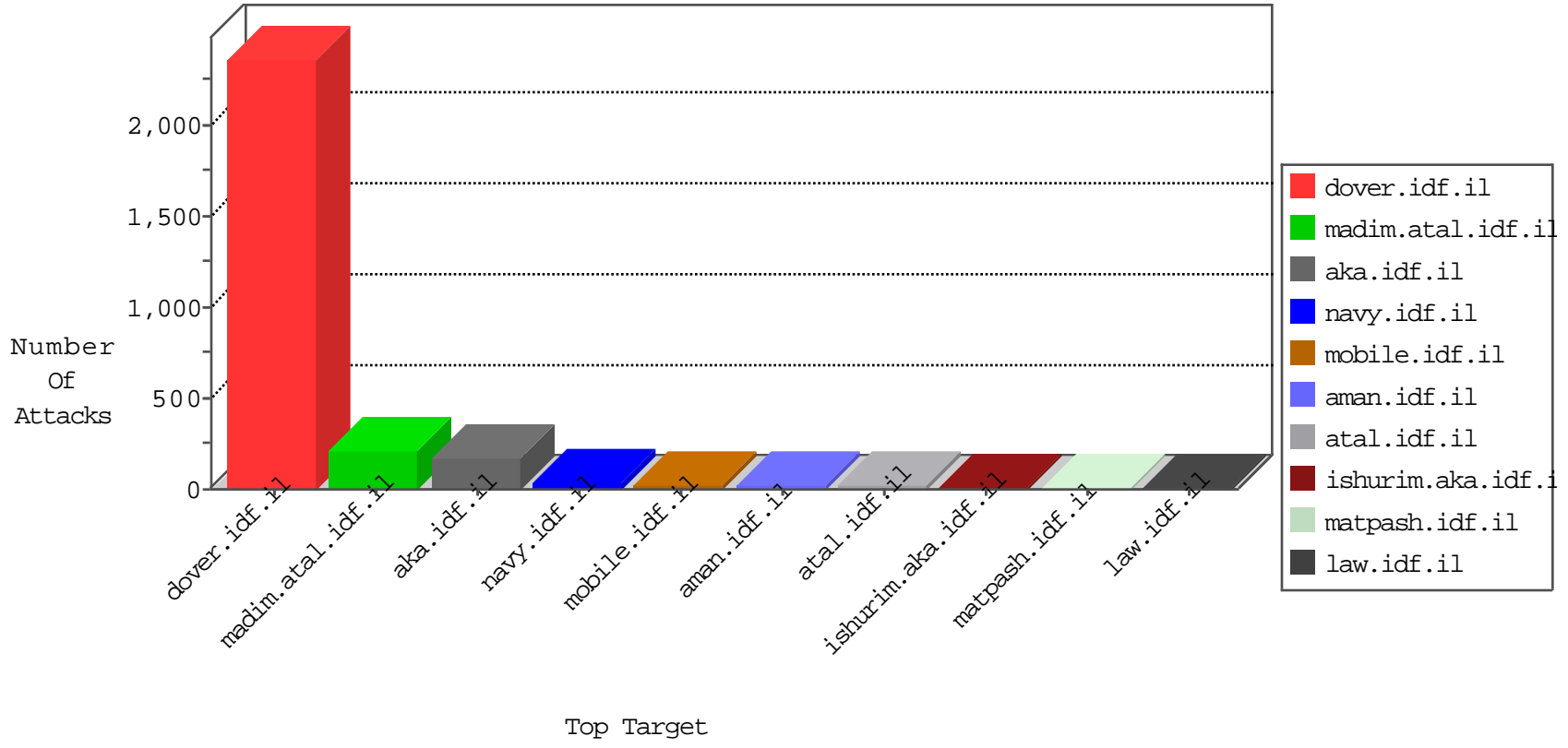


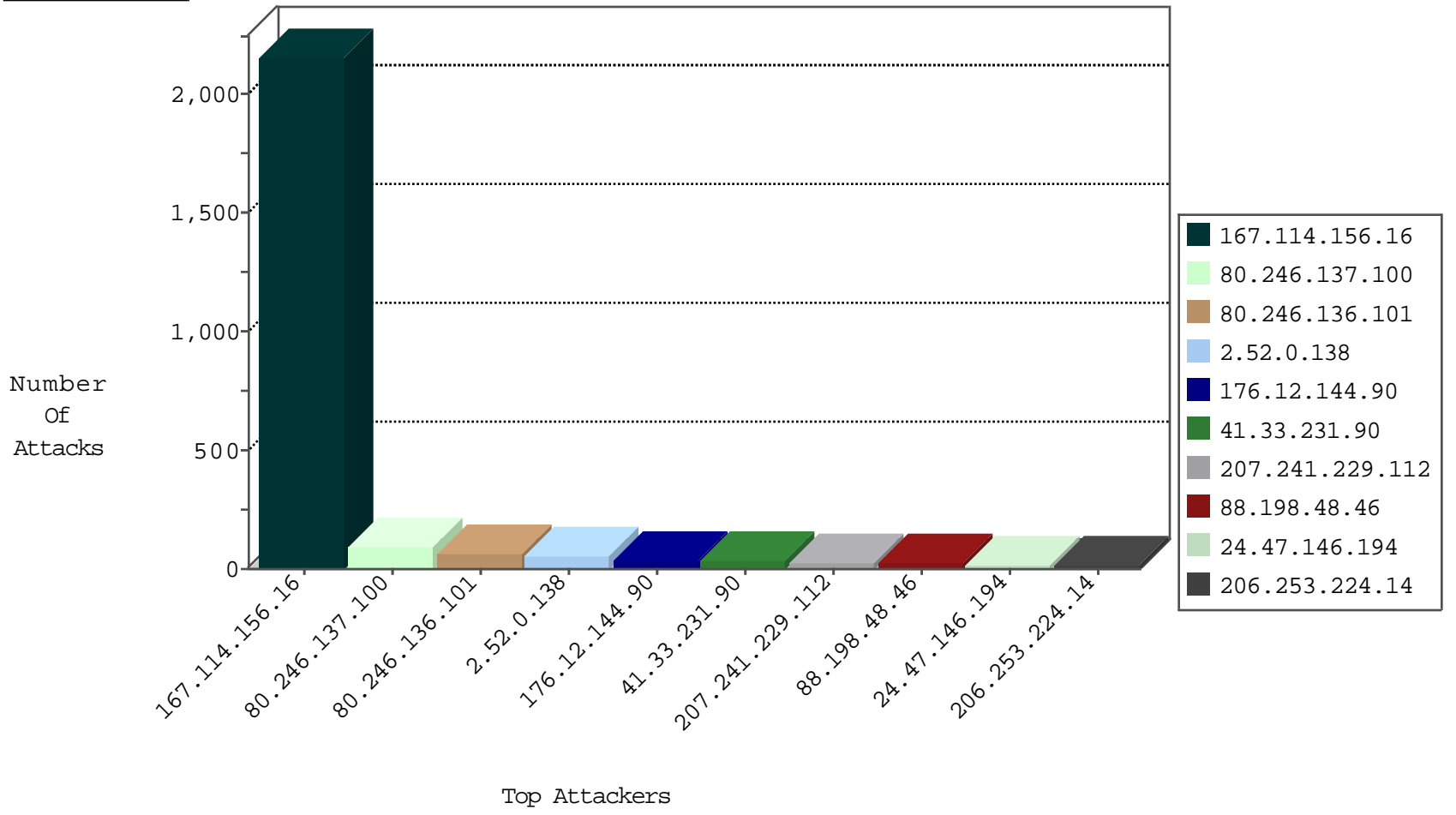
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3350
176.12.144.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
79.180.172.105	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
124.180.206.40	Australia	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
112.2.233.232	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.143.245	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
74.84.136.105	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
149.202.48.240	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.126.230.71	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.0.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.229.112	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
80.246.137.100	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
24.47.146.194	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
1.129.96.158	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.23.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
71.11.17.227	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.50	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.165.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.19.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.110.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
176.12.141.255	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.20.197	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.241.229.112	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.253.159.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.137.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.17.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.184	United States	147.237.72.166	aka.idf.il	drop		drop	3
109.66.153.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	United States	147.237.72.166	aka.idf.il	drop		drop	3
46.19.85.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.48.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.160.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
206.253.224.14	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
2.54.190.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
206.253.224.14	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
80.246.130.184	Israel	147.237.0.34	tikshuv.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
206.253.224.14	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.88.110.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
24.47.146.194	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
206.253.224.14	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
80.246.136.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
176.12.144.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
80.246.136.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
80.246.137.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
185.120.126.34		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.245.119.25	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.245.119.25	Block	5
80.245.119.25	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
2.54.63.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.20.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	2
188.165.89.85	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 88.198.48.46	Block	2
80.246.136.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.22.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.111	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
24.47.146.194	United States	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
80.246.136.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9827-he/refuah.aspx	Block	1
176.13.12.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.213.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rmd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
84.108.123.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.13.23.162	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.13.23.162	Block	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
24.47.146.194	United States	147.237.72.166	aka.idf.il	Multiple signatures from 24.47.146.194	Block	1
207.46.13.144	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
93.172.153.167	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
195.154.146.225	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
70.39.157.197	United States	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$btnSearch in www.aka.idf.il/main/giyus/login.aspx	None	1
109.253.213.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.213.109	None	1
85.250.188.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.152.90	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
206.253.224.14	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
176.228.149.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.230	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1