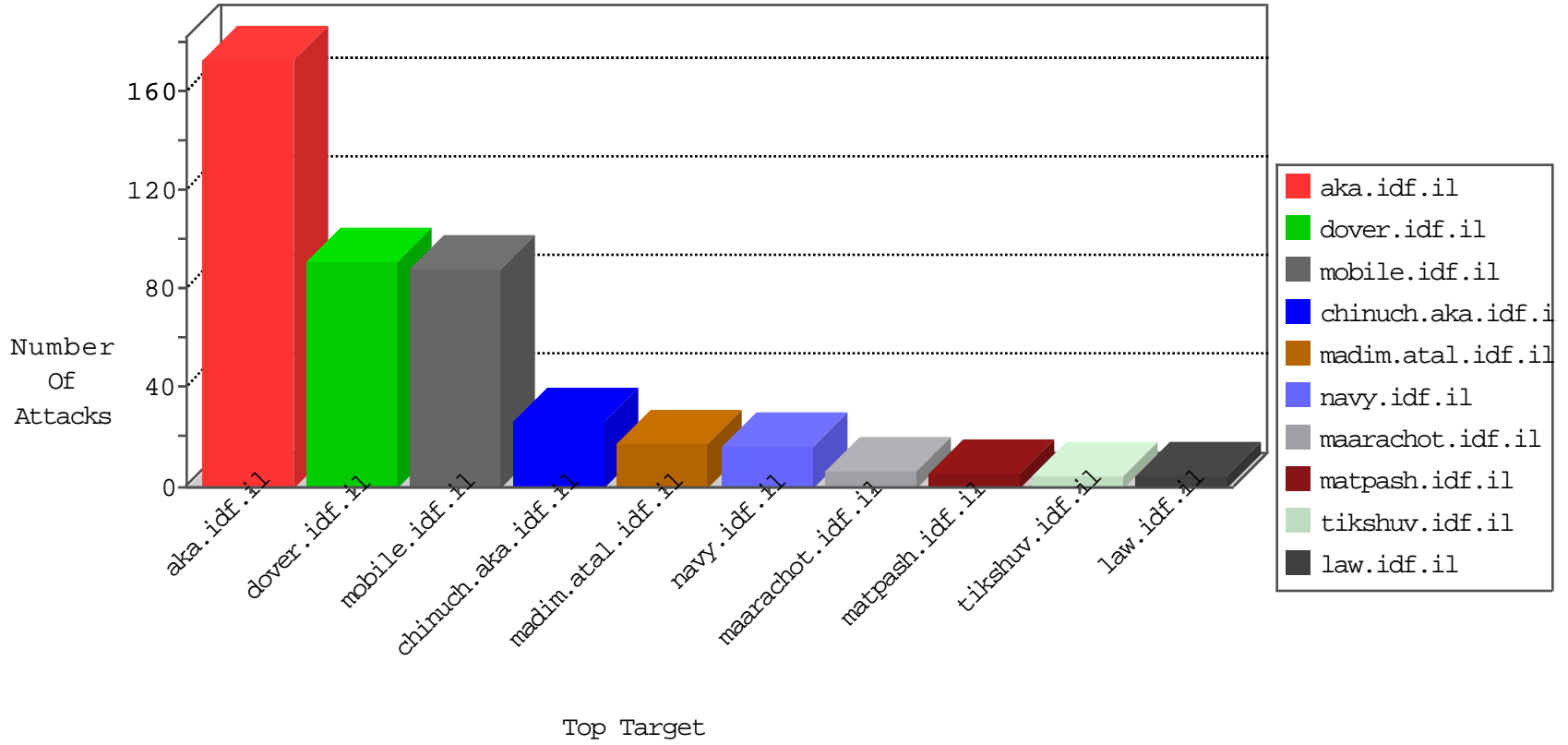


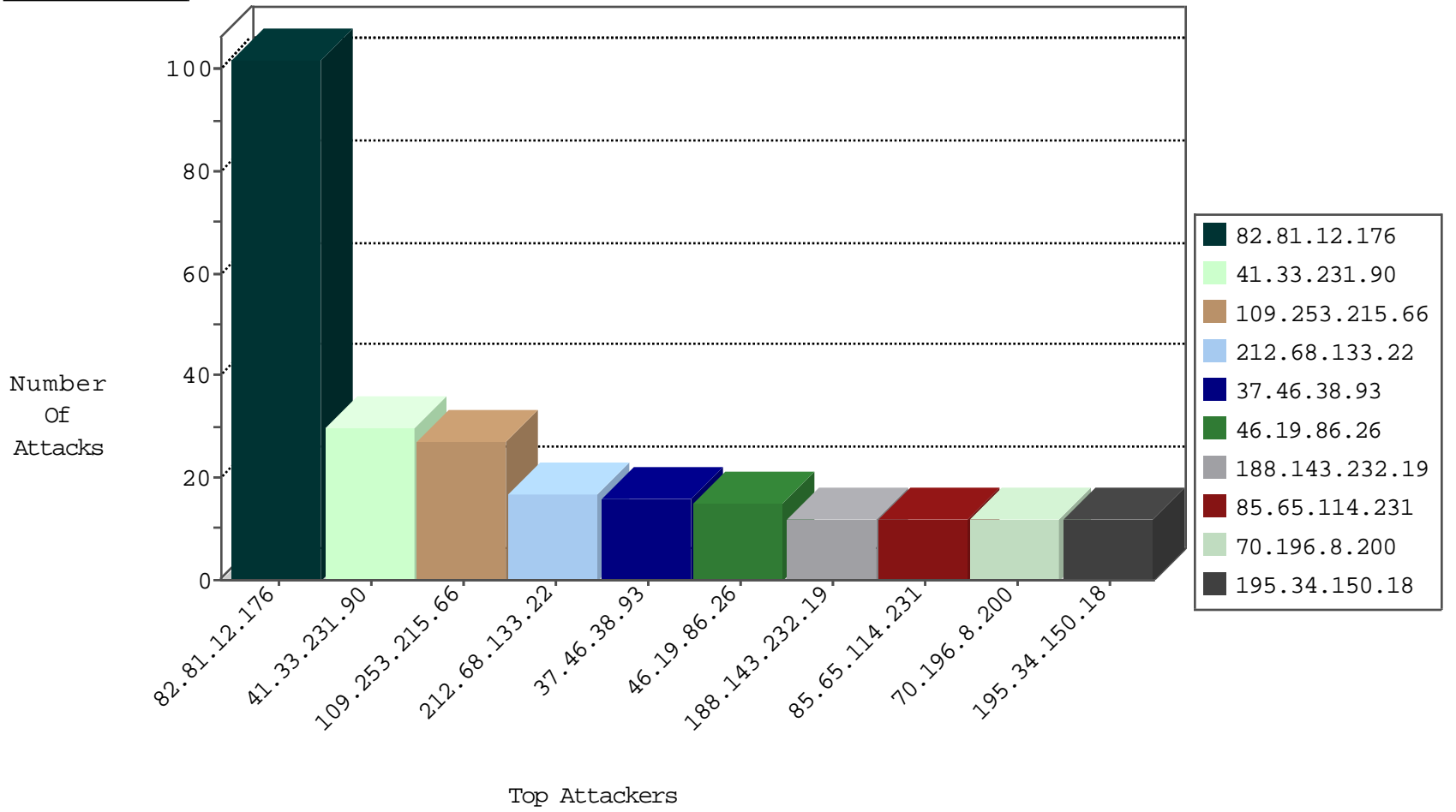
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	102
198.55.103.19	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.201.39.194	United States	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
54.213.43.131	United States	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
54.213.115.23	United States	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	1
54.191.233.78	United States	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.186.34.171	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.34.171	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
210.93.50.130	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.175.213	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.175.162	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.186.34.171	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
210.93.50.130	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
210.93.50.130	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
128.199.175.175	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.215.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
70.196.8.200	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
217.132.15.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.44.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.181.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.114.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.38.93	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.68.133.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.197.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.219.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.114.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.25.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.131.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.162.16.100	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
85.64.246.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
54.162.16.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.116.168.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
191.232.136.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.64.246.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.169	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.65.133	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.38.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
151.252.97.244	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.13.112.119	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.231.124.73	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.32.232.112	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.143.232.19	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.29.252.2	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.178	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.13.112.119	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
93.186.182.35	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.252.2	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.176.17.88	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
212.179.219.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.32.232.112	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.147.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.13.112.119	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.116.168.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

01-31-2016-02:04:04 to 01-31-2016-03:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.208	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.68.133.22	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 212.68.133.22	Block	8
37.46.38.93	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 37.46.38.93	Block	6
176.13.16.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.215.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
188.143.232.19	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	3
31.210.186.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.44.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.19	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	2
109.253.215.66	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.19	Russian Federation	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	2
185.32.179.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.68.133.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
85.64.246.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.143.232.19	Russian Federation	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	2
217.132.15.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
54.201.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method	Block	1
157.55.39.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/dover.aspx-title=chief	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 107.178.194.87	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
54.213.115.23	United States	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	1
40.77.167.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	1
69.121.14.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
191.232.136.6	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/matak/pages/economy.aspx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.201.39.194	United States	147.237.76.147	chinuch.aka.idf.il	NULL Character in Method	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
212.68.133.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
188.143.232.19	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/1111-he/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
141.212.122.209	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
77.127.24.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
191.232.136.117	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.141	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/894-he	Block	1
54.213.43.131	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
176.13.21.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.137.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/l.he/scroller/jquery.jcarousel.css	Block	1
66.249.64.186	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
151.252.97.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
54.191.233.78	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
2.54.25.84	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.25.84 (Unknown SSL Session)	None	1
84.229.129.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
191.232.136.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
54.213.43.131	United States	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	1