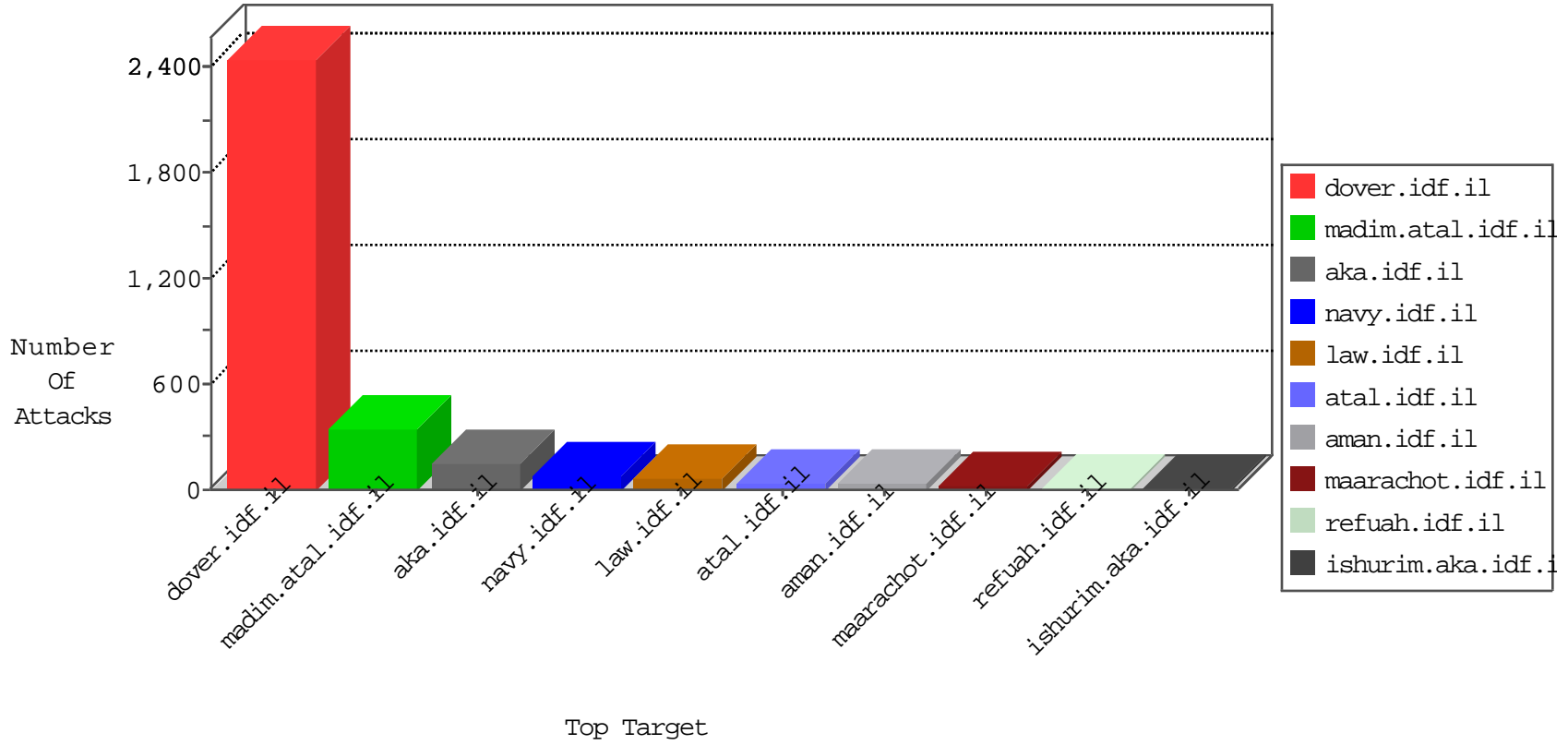


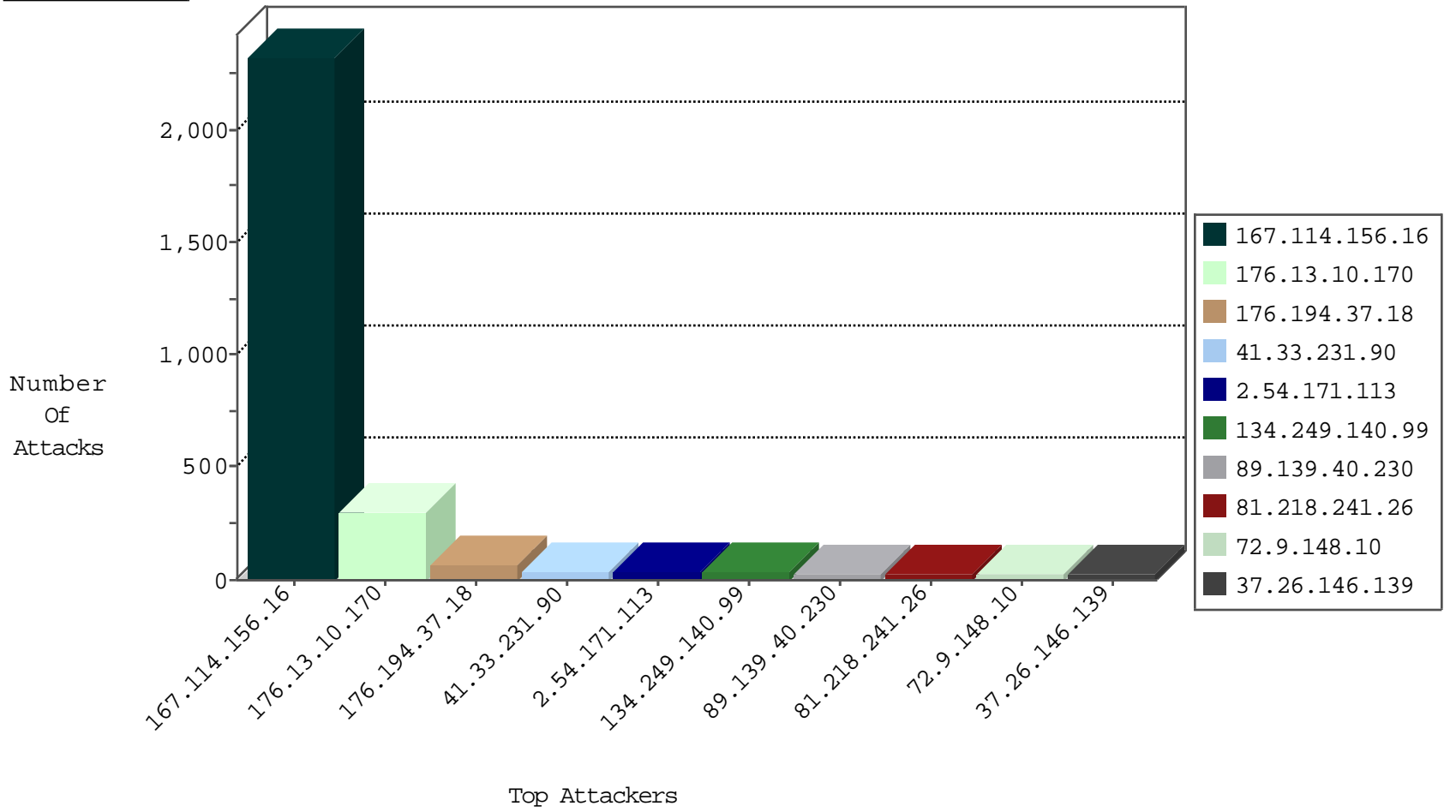
# IDF Under Attack Daily Report



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	3592
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
176.194.37.18	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
178.70.212.72	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
39.84.23.168	China	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Top	drop	2
176.194.37.18	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.247	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1
167.88.7.251	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-trafl	drop	1

12-07-2015-07:04:09 to 12-07-2015-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
124.130.51.99	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.63.116.27	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.72.167	United States	ishurim.aka.idf.i	ET DROP Dshield Block Listed Source	1
194.114.146.227	147.237.72.167	Israel	ishurim.aka.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.202.248.121	147.237.77.205	Germany	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
119.167.153.187	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
52.91.92.227	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.116.27	147.237.72.156		aman.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.194.37.18	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.139.40.230	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.139	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.131	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
24.52.235.227	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	8
46.19.85.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.182	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.186.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.232.5.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.84.248.173	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.41.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
24.52.235.227	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.10.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.130.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.27.105.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.132.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.14.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.109.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.25.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.25.69.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.178.198.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.137	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
202.180.34.186	Japan	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
207.46.13.186	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
79.180.106.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.112	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
202.180.34.186	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
134.249.140.99	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
5.28.137.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.106.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.15	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.125.119.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.2.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.15	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
202.180.34.186	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
173.252.46.103	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.10.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.10.170	Block	201
176.13.10.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
2.54.171.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
134.249.140.99	Ukraine	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 134.249.140.99	Block	7
134.249.140.99	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 134.249.140.99	Block	7
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
134.249.140.99	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 134.249.140.99	Block	3
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.37.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
134.249.140.99	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 134.249.140.99	Block	3
134.249.140.99	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
39.41.210.231	Pakistan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
2.52.132.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
81.17.31.222	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.112	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.120.139.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.249.140.99	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
39.41.210.231	Pakistan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
134.249.140.99	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1
64.71.32.33	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/blog/wp-admin/	Block	1
85.250.242.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.113.198.103	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
134.249.140.99	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.19.86.182	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.179.129.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
37.26.146.172	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx	Block	1
149.88.60.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
87.69.33.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_campaign in www.aka.idf.il/main/giyus/	None	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.52.134.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
134.249.140.99	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.69.74	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/ajaxpage.aspx	Block	1
134.249.140.99	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1