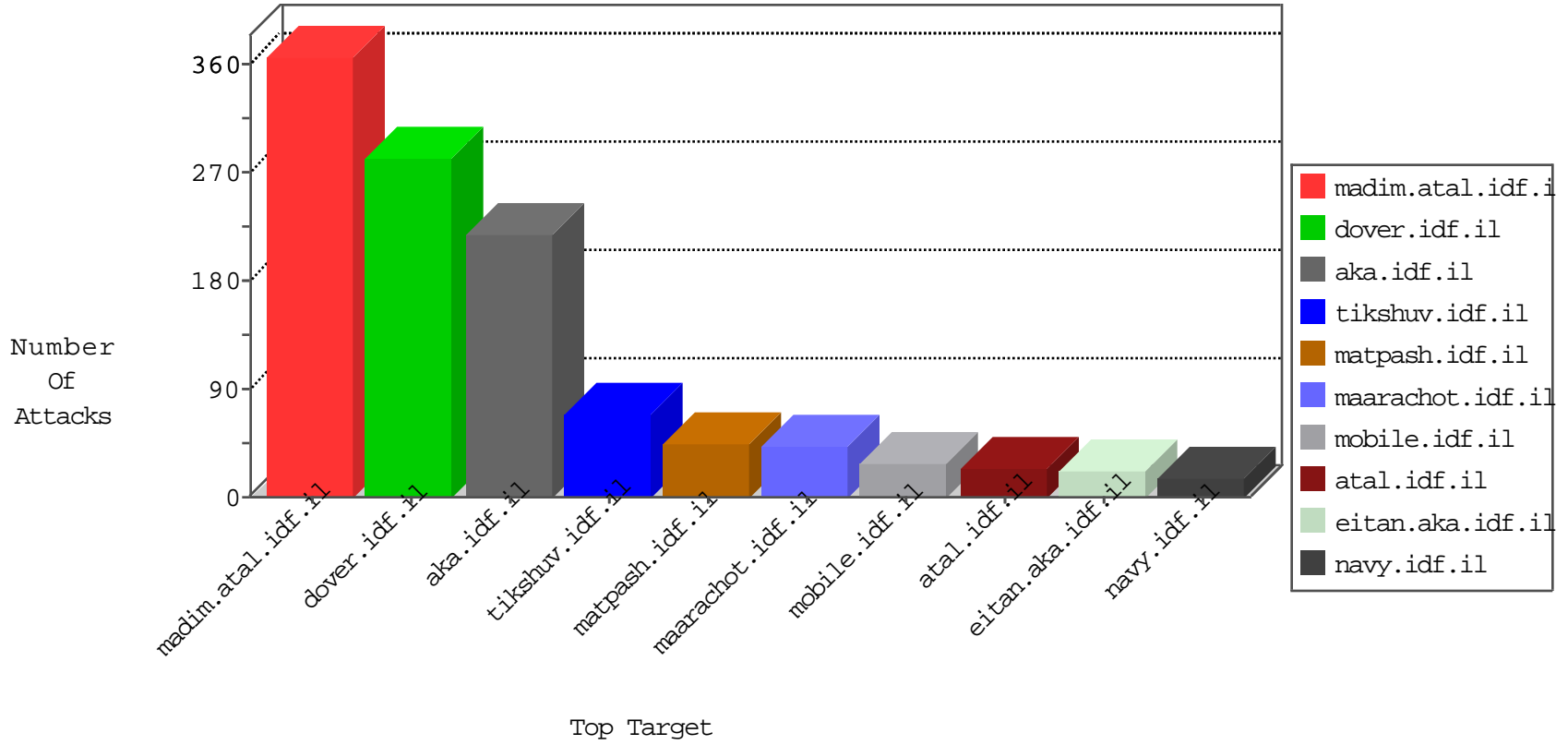


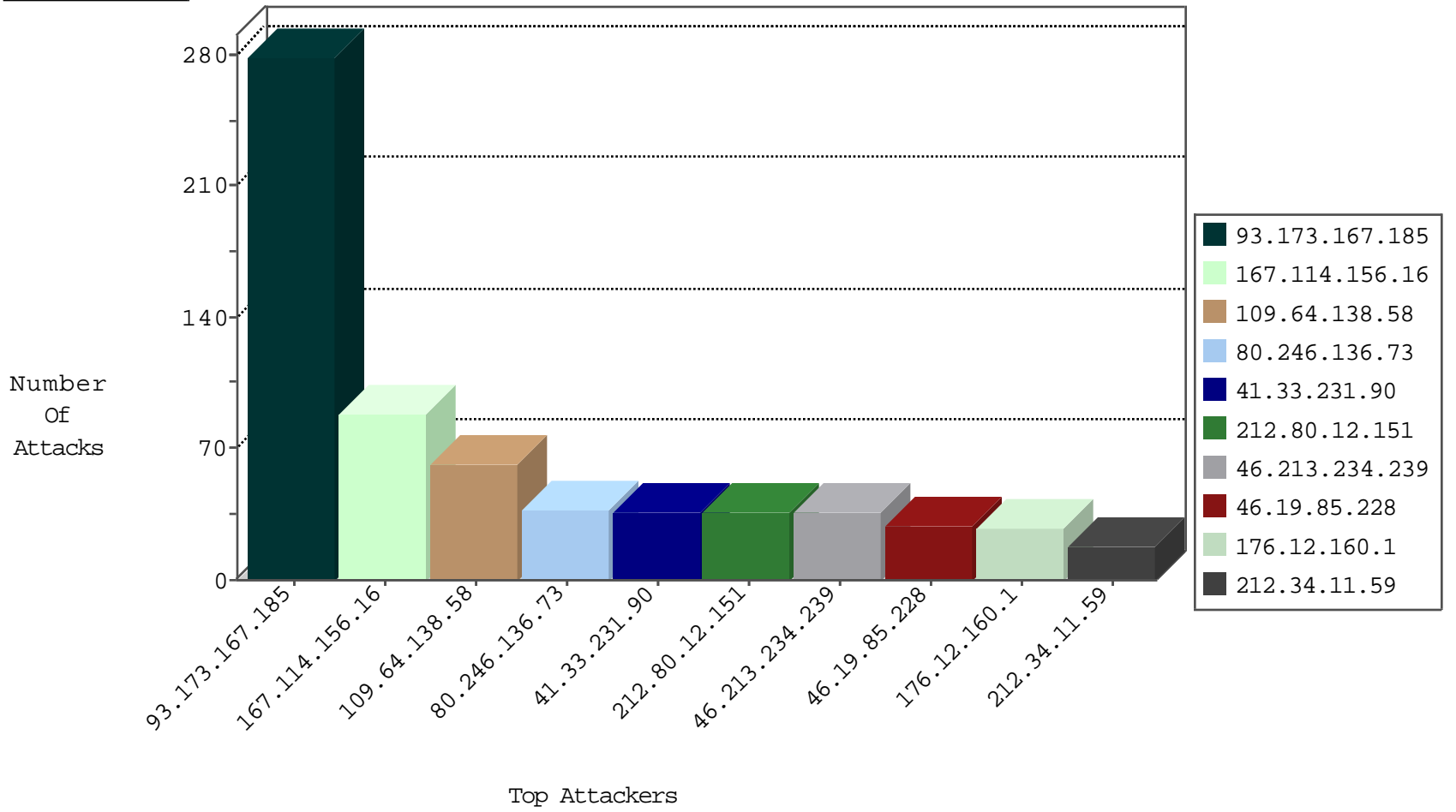
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3472
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2514
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
216.185.58.80	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
1.36.247.100	Hong Kong	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
188.165.201.164	France	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.60	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.76	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
173.208.136.170	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
142.54.168.140	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1

01-09-2016-13:04:09 to 01-09-2016-14:04:09

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.29	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.143.165.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.198	United States	e.yohanan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	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	36
176.12.160.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.213.234.239	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.213.234.239	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
212.80.12.151	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
212.80.12.151	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.128.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.157.158	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.22.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.139.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.89.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
84.228.53.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.60.96	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.53.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
109.64.53.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.159.166.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.241.49	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.3.144.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.59.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.88.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.22.129.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
194.90.39.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
101.226.69.246	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
198.100.144.55	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.16	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
101.226.69.246	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
207.46.13.32	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
101.226.69.246	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.175	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.13	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
101.226.69.246	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
87.69.17.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.127.130.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.120.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.23.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.193.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.198.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.251	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.57.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.132.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.132.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3

01-09-2016-13:04:09 to 01-09-2016-14:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.28.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.167.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
93.173.167.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.64.138.58	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
93.173.167.185	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 93.173.167.185	Block	29
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
80.246.136.73	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.73	Block	21
80.246.136.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
87.69.78.155	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.78.155	Block	9
37.142.64.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
212.34.11.59	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.59	Block	5
212.34.11.59	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.59	Block	5
109.66.120.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	4
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.34.11.59	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 212.34.11.59	Block	3
79.176.169.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	2
37.142.221.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.33.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
89.138.80.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
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	2
2.225.191.203	Italy	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1362-en/cogat.astx	Block	2
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout2.css	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.75	Block	1
87.69.63.226	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
79.182.116.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.174.101.91	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/xmlrpc.php	Block	1
5.135.66.213	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi	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
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1731	Block	1
212.34.11.59	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=5690d6ba51fe6e22000;_pk_id.20.8afc=882985ee9474082a.1452097654.3.1452332736.1452332736.;_pk_ses.20.8afc=*	Block	1
88.105.141.202	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
198.100.144.55	Canada	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
176.58.120.214	United Kingdom	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
83.169.10.185	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
109.201.135.183	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
78.47.17.5	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/text.css	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
46.19.86.24	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-5090-en/patzar.aspx15/i-got-a-bacon-omelette-to-dayt-up-a-rubsing-hist	Block	1
80.40.134.104	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
5.144.60.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.145	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1