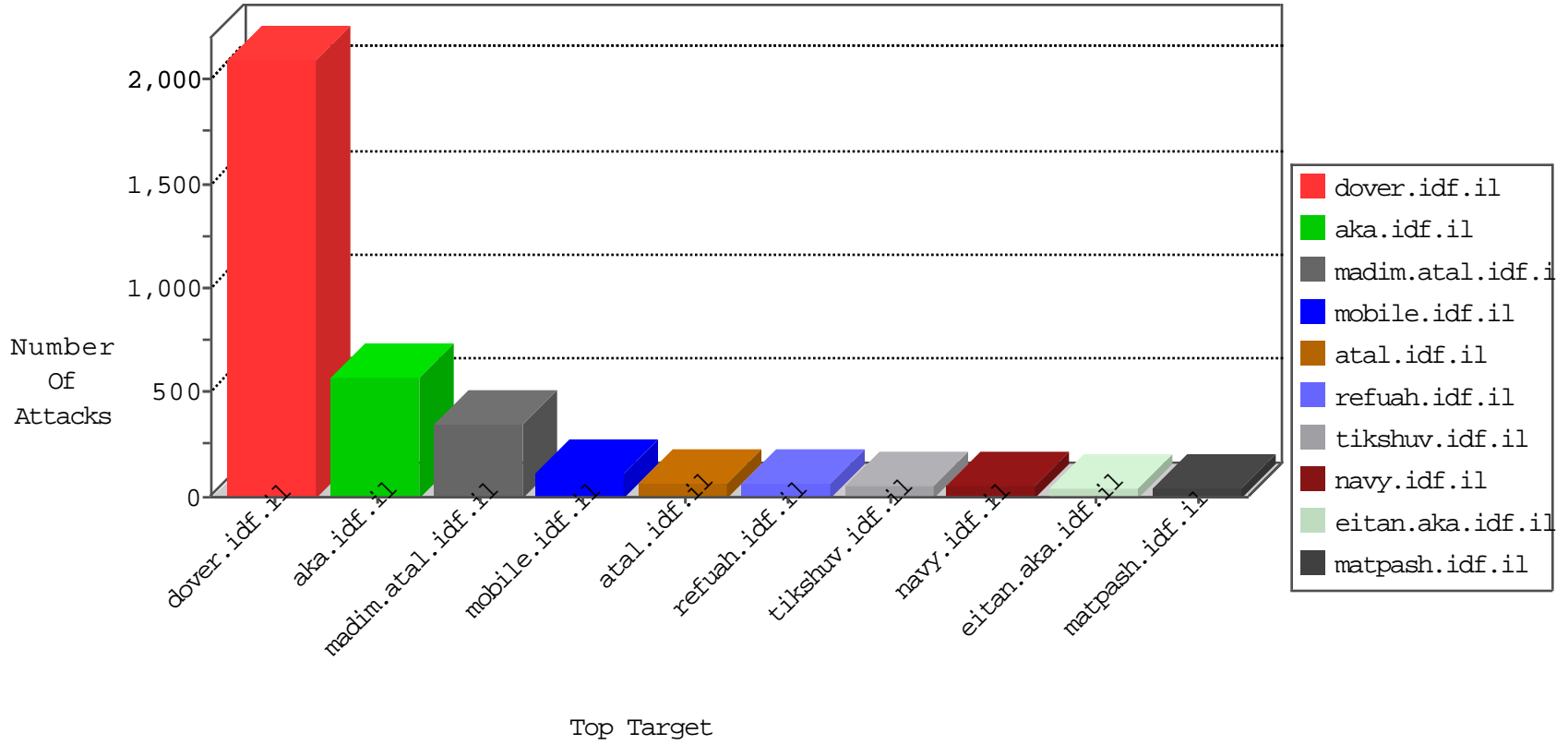


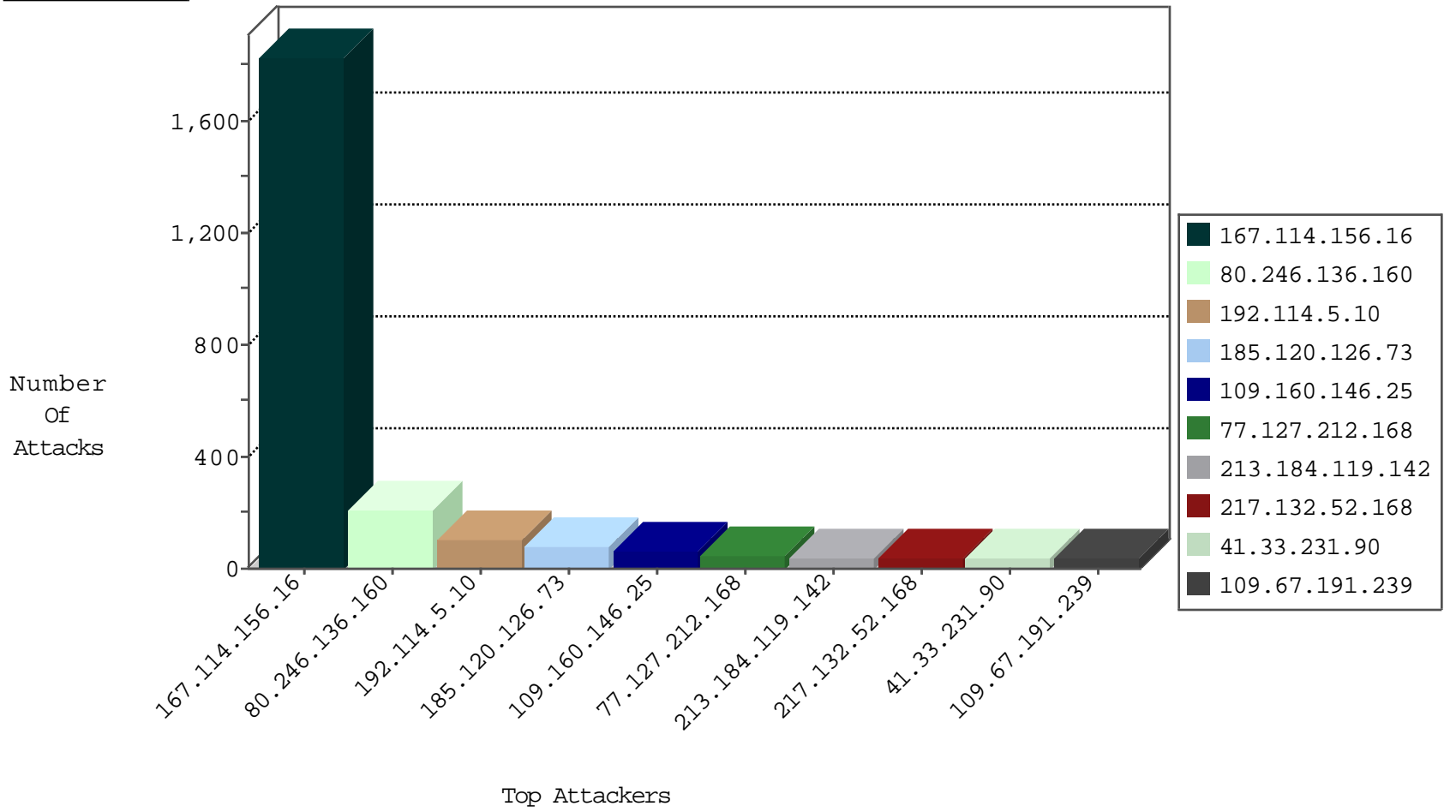
# IDF Under Attack Daily Report



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	3199
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	82
84.108.148.96	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.110.144.5	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.174.4	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-06-2016-20:04:00 to 01-06-2016-21:04:00

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	3
80.246.136.160	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
46.19.86.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
141.135.125.156	147.237.76.34	Belgium	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.75.199.201	147.237.76.42	China	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
89.248.162.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.9.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
186.112.188.79	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.188.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.162.131	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
109.160.146.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
77.127.212.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
213.184.119.142	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	39
217.132.52.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
82.166.148.146	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
213.8.204.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
79.179.48.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
84.228.94.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
41.218.250.155	Ghana	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.11	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.102.254.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.120.126.42		147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
212.116.169.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.160.130.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.11	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.203.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.194.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.127.2.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.46.39.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.144.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.112.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.116.112.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.112.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.111.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.1.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.230.69.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.202.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.144.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.186.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.218.250.155	Ghana	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.130.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.147.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.8.204.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.8.204.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.141.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.218.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.65.26.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.187.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
192.114.5.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
109.67.191.239	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.191.239	Block	33
176.13.8.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
89.138.54.64	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.160	Block	11
77.125.81.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.160.146.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
176.13.17.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.76.103.183	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	4
159.203.67.223	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 159.203.67.223	Block	4
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.128.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.89.185	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.20.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/controls/atuda/Å	Block	2
46.120.233.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.201.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
213.57.171.84	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
37.26.149.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.67.127.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	2
85.65.246.240	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.102.253.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.186.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.69.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
95.86.92.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/&sa=u&ved=0ahukewjoz9jt7jxkahwgxhqkhc kmc6ggfeggumae&usg=afqjcnhcvyyg7wlcg-yhd5_ammzoyodtwa	Block	1
109.253.197.137	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.111.165.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyius	Block	1
213.151.39.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20978-he/dover.aspx&sa=u&ved=0ahukewitwtys6px kahuffa8khl3aueqfggymac&usg=afqjcnfpecc5tshxnzefnkaohgjycbchiq	Block	1
79.180.203.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.218.250.155	Ghana	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.127.57.212	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
2.54.14.236	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyius/forum/asp/showforum.asp	Block	1
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.52.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.149.104.121	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
79.176.108.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
176.13.19.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.112.186	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.112.186	Block	1
213.151.39.169	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1787-he/dover.aspx&sa=u&ved=0ahukewj-gf-r7jxkahukvh okhsbeafeqfggimaa&usg=afqjcnhnolb7hxmsifzaz_gv3prewsrfqa	Block	1
46.121.209.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1