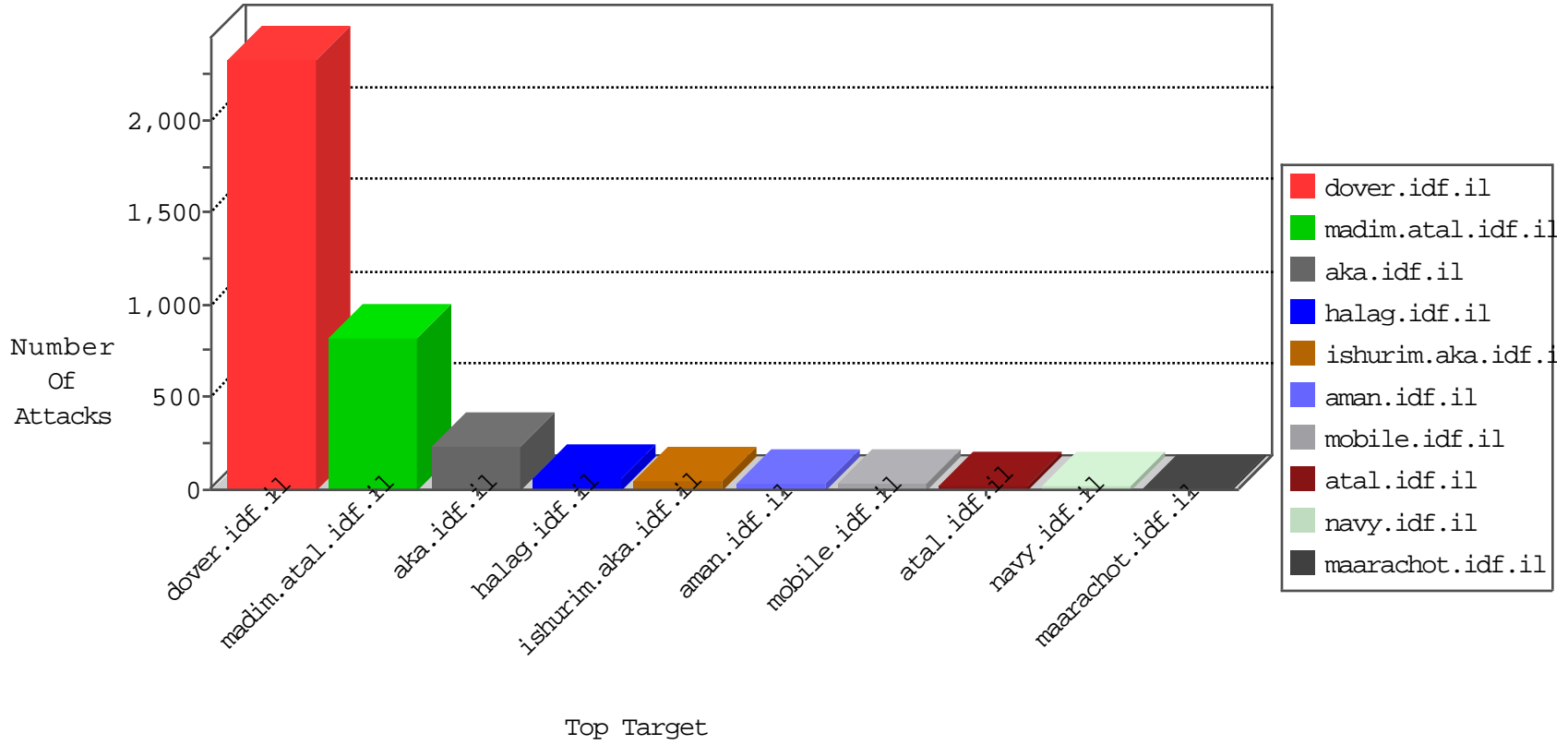


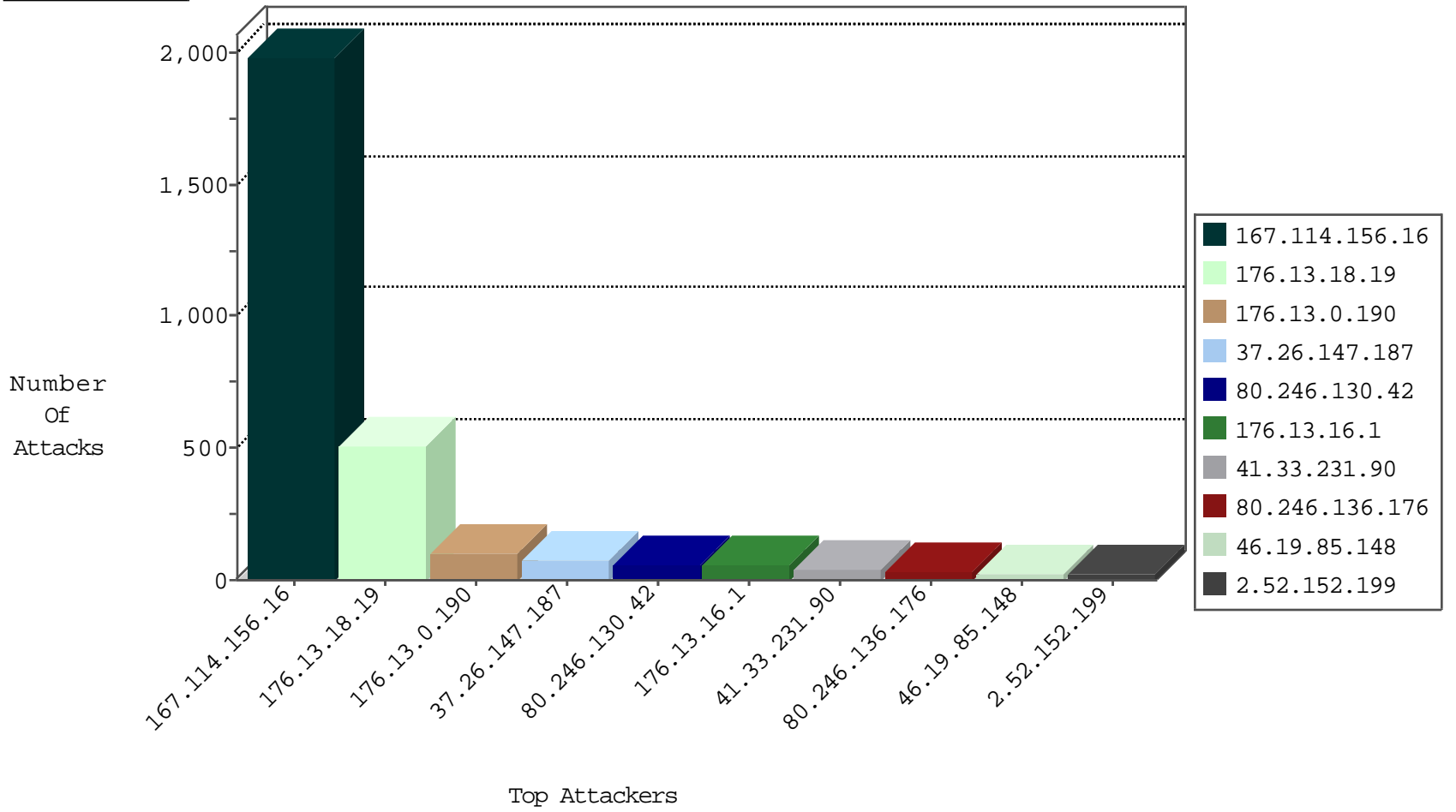
# IDF Under Attack Daily Report



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	3397
208.67.1.60	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.213	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	forward	1
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.93.151	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-08:04:09 to 01-07-2016-09:04:09

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	3
66.249.93.222	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
149.88.202.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.41.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.208.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.202.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.21.107.124	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
173.199.74.136	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.172.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.253.136.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.218.246.103	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.28.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.214.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.21.107.124	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
79.183.223.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.21.107.124	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
64.231.207.9	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.115.58.160	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.42	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
212.235.103.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
80.178.218.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.116.81.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.52.152.199	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.185.236	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.13.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.61	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.13.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.159.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.168	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
194.90.89.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.21.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.13.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.130.89	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.154.4.191	Belarus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	292
176.13.18.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
176.13.18.19	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.18.19	Block	102
176.13.0.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
176.13.16.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.136.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.146.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.0.190	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.0.190	Block	10
109.253.147.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
186.202.153.185	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.153.185	Block	5
84.228.54.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.54.138	Block	4
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.228.54.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
109.253.201.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.146.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.121.135.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.31.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
116.25.107.110	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	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
84.108.76.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.79.220.248	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
2.54.153.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.253	United States	147.237.77.176	matpash.idf.il	Multiple Illegal URL Path Encoding from 157.55.39.253	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1133-he/dover.aspx	Block	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	1
46.19.85.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
186.202.153.185	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
80.246.139.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.146.160	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
2.54.56.225	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
109.64.21.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
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	1
40.77.167.5	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
184.105.139.67	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
84.228.16.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.16.97	Block	1
2.54.184.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1