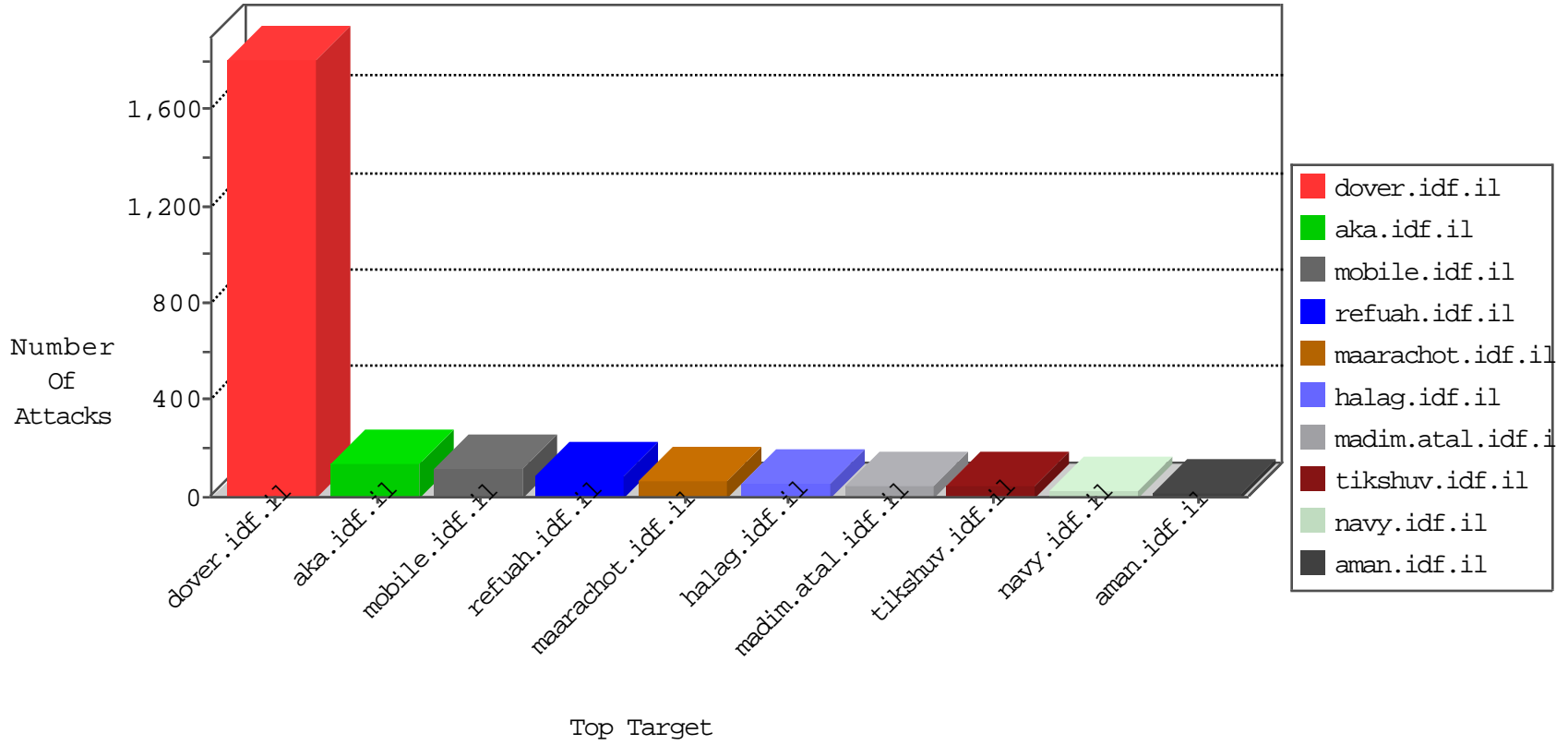


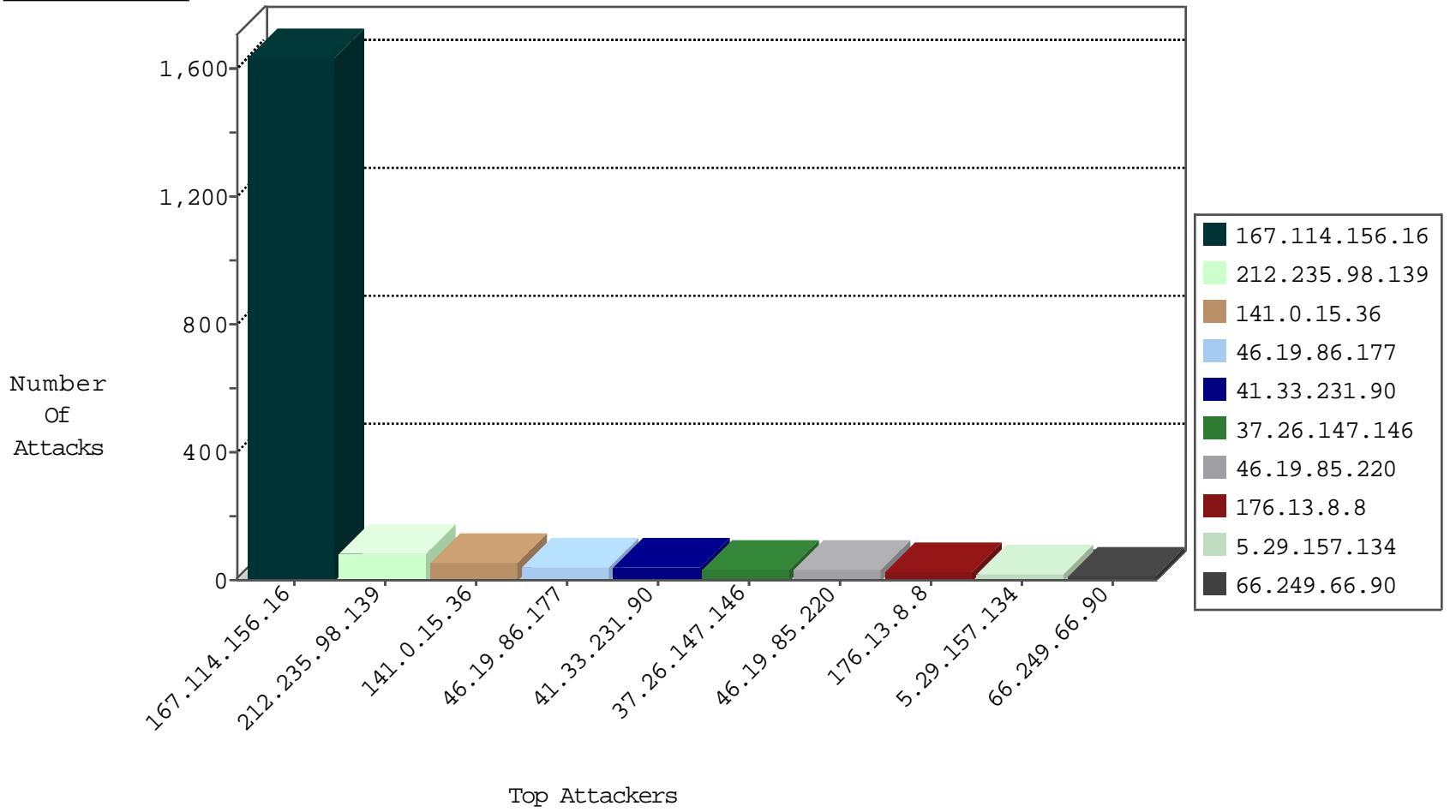
IDF Under Attack Daily Report



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	3025
82.80.217.70	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.182.8.181	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

01-03-2016-07:04:01 to 01-03-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.200.205	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

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
61.216.2.14	147.237.77.121	Taiwan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
212.199.145.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.197.114	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.132.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.37.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.216.2.14	147.237.77.216	Taiwan	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.216.2.14	147.237.76.38	Taiwan	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.85.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.197.114	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 3072	1
84.228.14.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.188.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	82
141.0.15.36	Europe	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	56
46.19.86.177	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.147.146	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
46.19.85.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
176.13.8.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.29.157.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
79.179.56.51	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
80.246.130.250	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.40.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.145.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.137.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.149.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.27.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.199.251.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
147.235.8.70	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
85.64.68.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.146	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
122.248.98.158	Myanmar	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.11.233	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.144.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.103.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.150.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.127.113	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.26.148.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.35.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
212.29.252.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
212.199.251.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	7
176.13.8.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
85.250.216.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.61.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
104.155.236.4	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.155.236.4	Block	4
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
5.29.157.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.40.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.149.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
176.13.7.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.137.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
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
2.54.146.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.211.182	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.69.211.182	Block	2
2.54.179.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.41.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.147.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.218.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.149.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
2.54.60.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.130.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.220	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	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
2.54.145.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.223.254.34	Austria	147.237.77.233	atal.idf.il	Unauthorized URL Access to /robots.txt	Block	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.png	Block	1
109.65.116.245	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.120.13.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
40.77.167.5	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
213.8.204.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.108.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/kkkkkkk=b866a561kkkkkkk_b866a561	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
2.54.26.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.140.73	Israel	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/1133-22461-he/dover.aspx.	Block	1
46.19.85.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.9.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchfText in www.idf.il/1065-he/dover.aspx	Block	1
61.216.2.14	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.66.127.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.208.197	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1