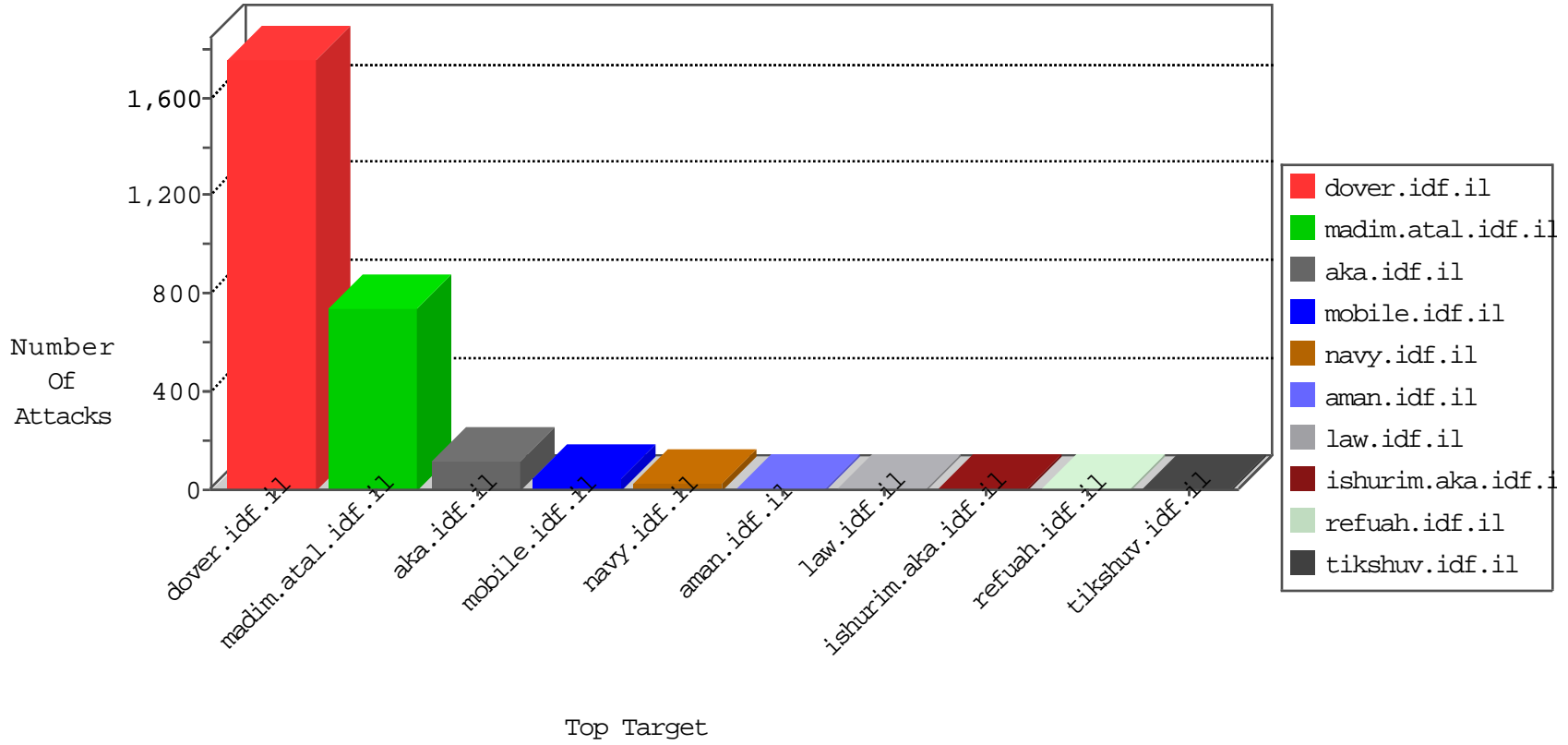


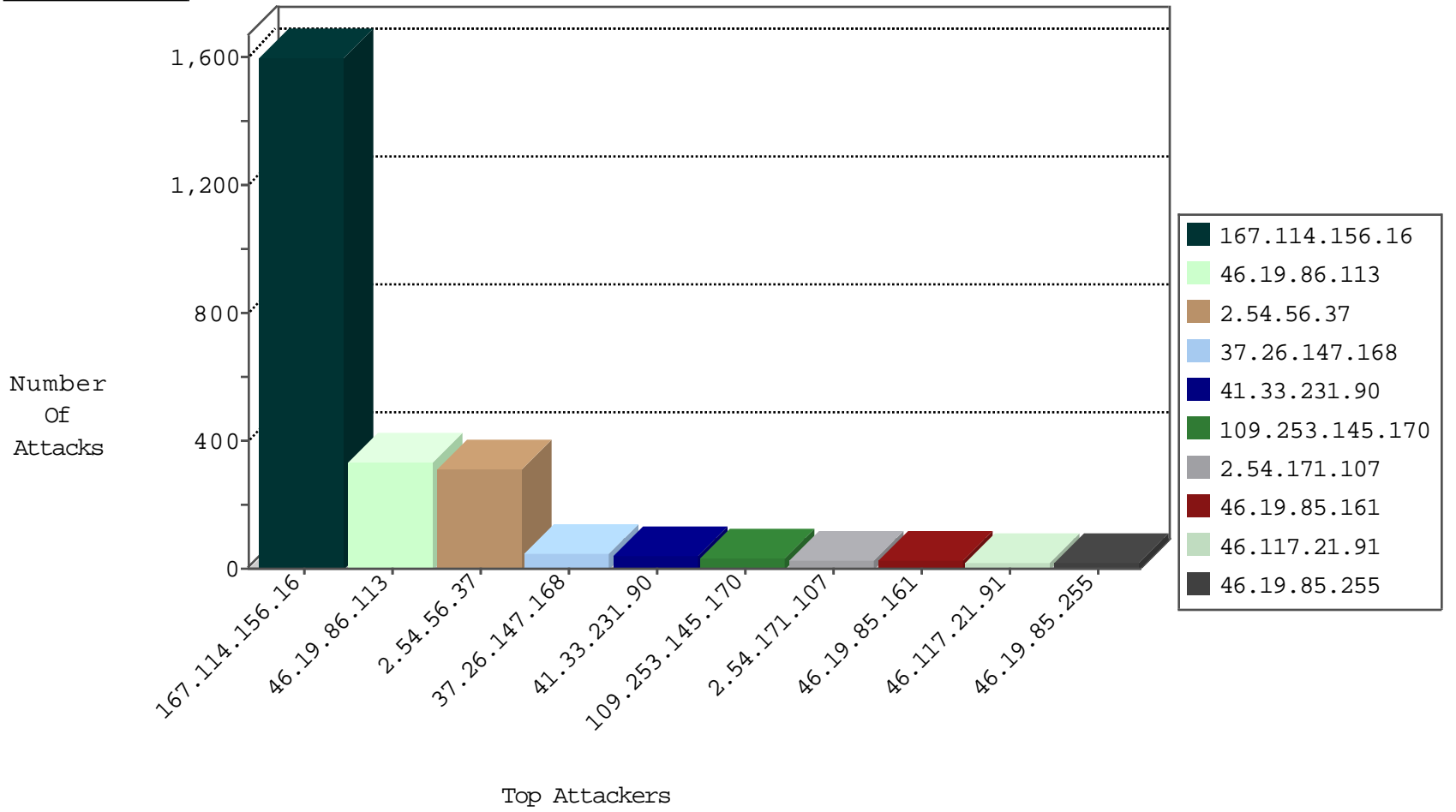
IDF Under Attack Daily Report



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	3001
222.186.13.29	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
23.95.248.111	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
107.150.55.210	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
142.54.160.210	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

01-11-2016-07:04:00 to 01-11-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.103.60	United Kingdom	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	4
162.242.245.138	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
112.16.76.209	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.0.33	China	idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
5.102.252.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.138.125.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.242.245.138	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
146.185.250.2	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.214.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.242.245.138	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	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	34
2.54.171.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.85.255	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.69.221.35	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.104.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.10.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.207.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.155.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.7.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.46.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.186.168.135	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.255.253.40	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.9.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.44.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.179.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.108.158.145	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.4.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.153	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.154	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.251	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
94.230.86.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
172.56.12.179	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
132.76.10.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.86.25	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	2
46.19.85.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
132.76.10.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.88.147.2	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.172	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
132.76.10.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.66.215.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.56.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.113	Block	174
2.54.56.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.113	Block	58
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
109.253.145.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.117.21.91	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.117.21.91	Block	19
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	9
2.54.26.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.56.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	7
79.177.104.142	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	3
2.52.191.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	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
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
109.65.105.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.13.194.167	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
91.135.102.170	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	1
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	1
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.67.225.10	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.168.226.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
50.63.197.85	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.135	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	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
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	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
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.71.247.36	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
62.219.121.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.252.90.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
207.46.13.10	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/xžx?x™x" x@x-xžx•xŸ.aspx	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.196.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.201.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.67.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.198.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
176.13.10.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59333	Block	1
46.117.21.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-23081-he/dover.asp	Block	1
40.77.167.76	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
109.253.211.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1