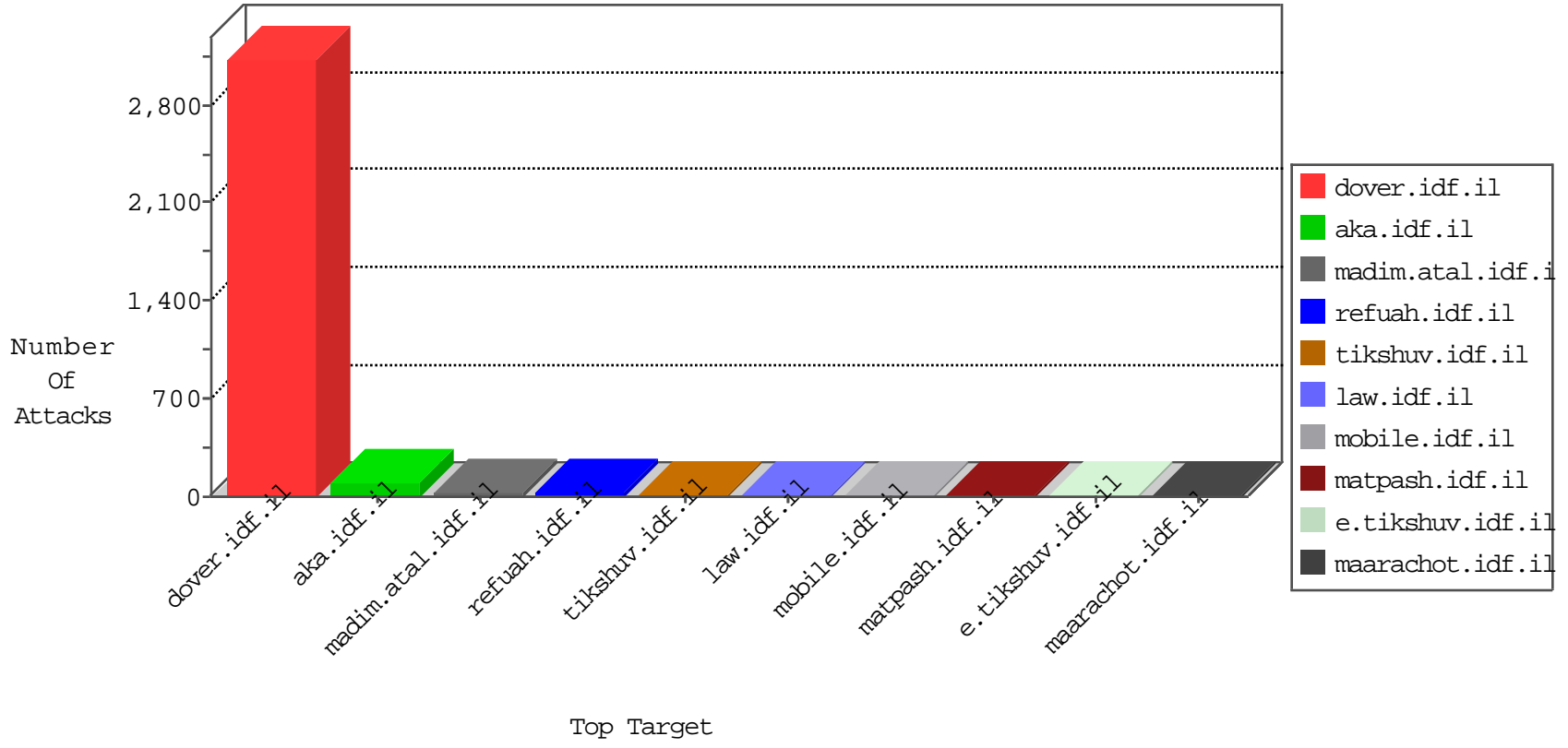


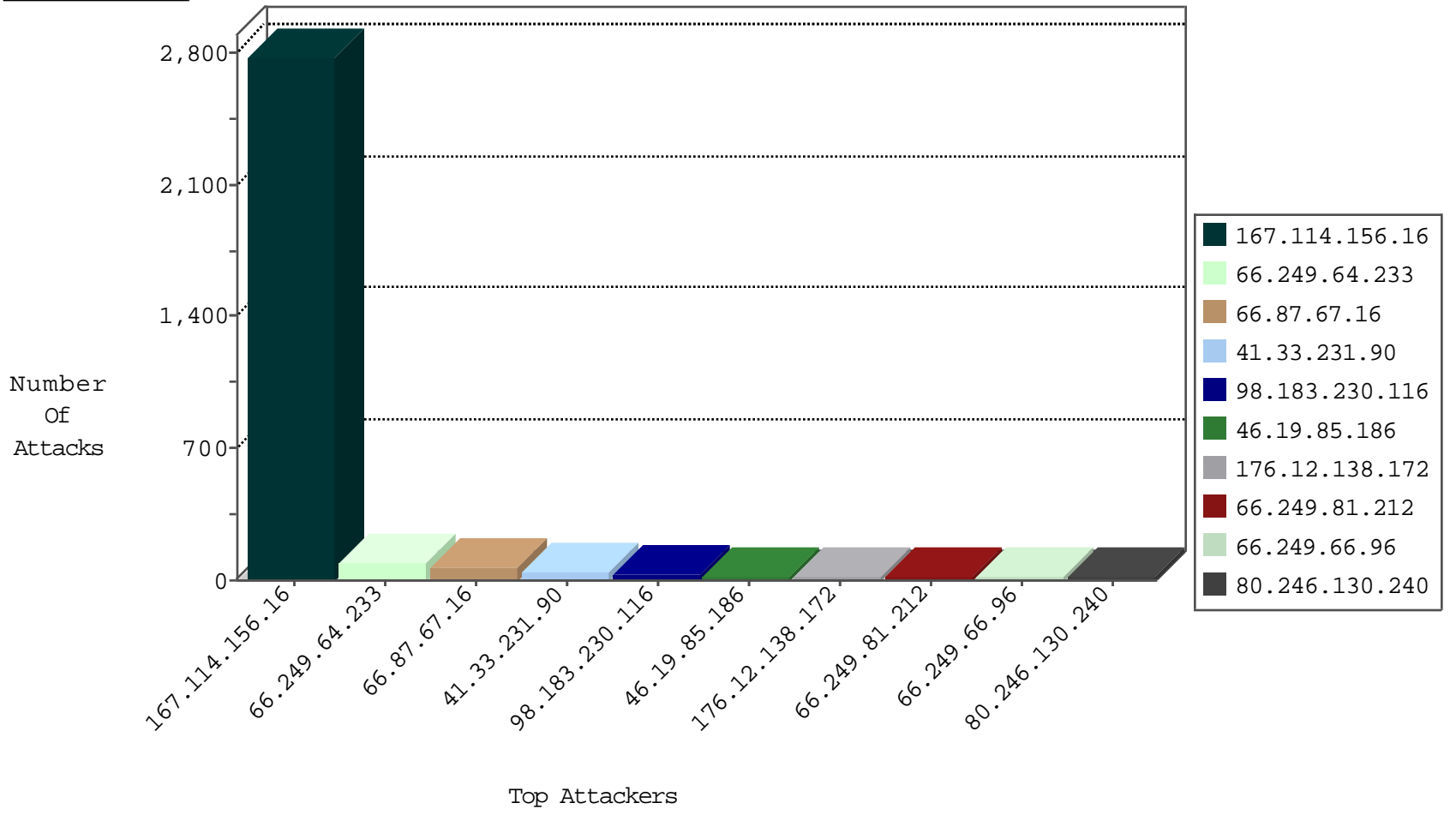
IDF Under Attack Daily Report



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	3438
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
111.200.254.3	China	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
173.242.125.211	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
112.68.181.216	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
104.192.0.226	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
173.242.125.211	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

11-25-2015-06:04:03 to 11-25-2015-07:04:03

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
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.223	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.96	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
92.227.134.93	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.55	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.38.250.31	147.237.72.167	Greece	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
54.183.246.95	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.134	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
14.136.116.175	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.254.90.133	147.237.8.50	Mexico	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.55	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.38.250.31	147.237.72.167	Greece	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.134	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
46.228.207.18	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.134	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
189.254.90.133	147.237.8.50	Mexico	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
189.254.90.133	147.237.8.50	Mexico	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
66.87.67.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
98.183.230.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.130.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.186	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
68.194.113.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.206.220.13	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.100.85.183		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.146.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.167	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.60.232.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.183.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
100.100.3.224		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.110.32.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.8		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.143.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.55.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.82		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.232.110.28	United Kingdom	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.28	United Kingdom	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.246.136.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
183.79.221.117	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
8.37.71.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.168.3.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
87.69.163.129	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.109	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.148	ggcenter.aka.idf.il	drop		drop	2
31.210.186.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.46.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.36	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
184.105.247.223	United States	147.237.0.33	idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.138.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
37.59.232.247	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
37.59.232.247	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.59.232.247	Block	5
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
84.228.116.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.55.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
128.232.110.29	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.142.68.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	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
74.82.47.4	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
5.28.172.177	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.12.142.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	1
109.67.205.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	1
37.59.232.247	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/plugins/content/plugin_googlemap2_proxy.php	Block	1
199.30.24.187	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/common/includes/globaltopbar/resources/images/border.jpg	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
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.142.68.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.177	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.182.118.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.172.177	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.13.22.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/kamiljenin.aspx	Block	1
109.67.205.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
86.97.126.107	United Arab Emirates	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
37.142.68.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17558.jpg	Block	1
5.22.131.148	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
157.55.39.169	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.66.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	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
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/20_10_03_strike_eng.asf	Block	1
37.142.68.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1