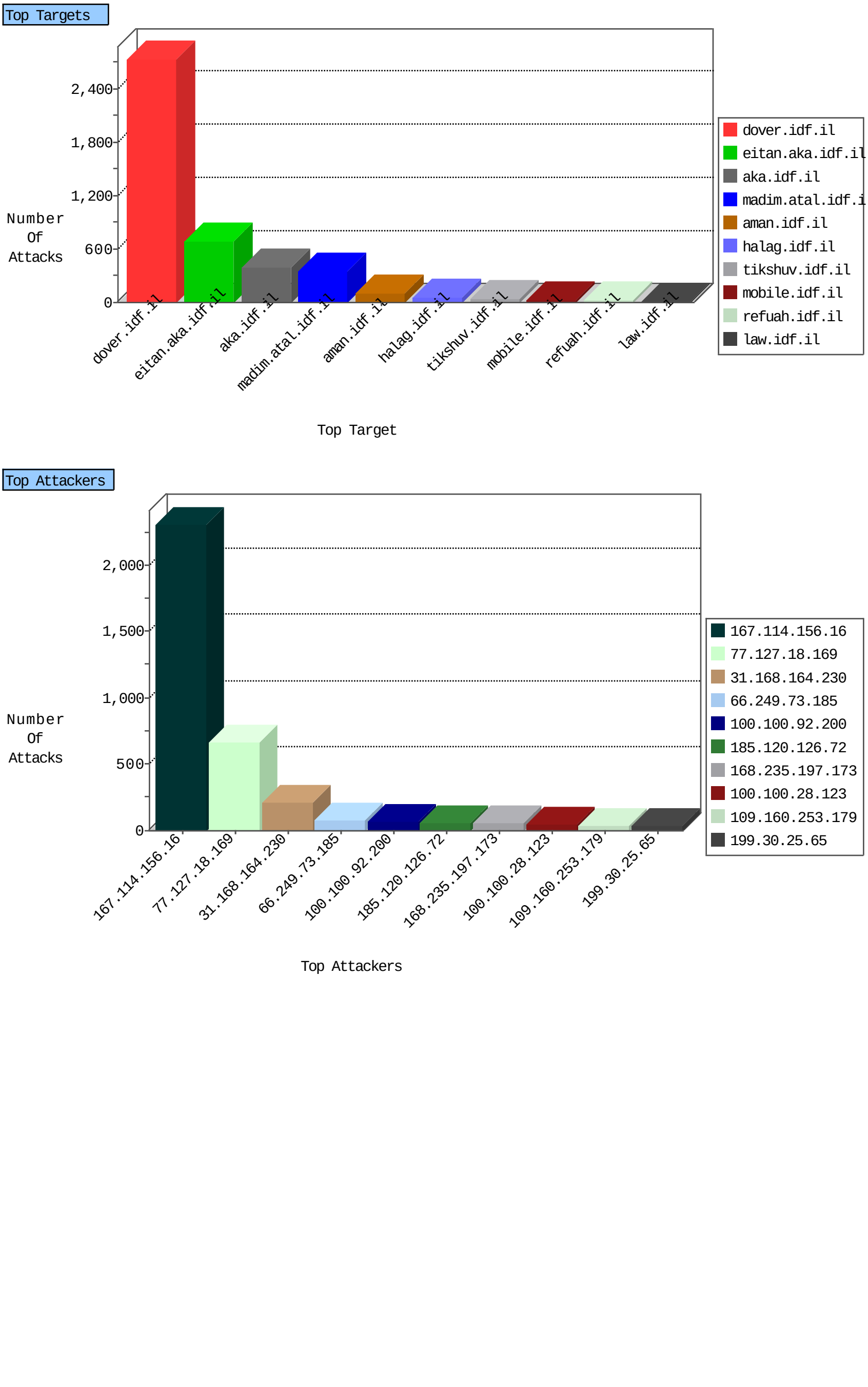
11-27-2015-16:04:09 to 11-27-2015-17:04:09

IDF Under Attack Daily Report



11-27-2015-16:04:09 to 11-27-2015-17:04:09

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	3374
168.235.197.173	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
45.63.17.42		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
14.219.42.45	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
168.235.197.173	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1

11-27-2015-16:04:09 to 11-27-2015-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.15.115	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-27-2015-16:04:09 to 11-27-2015-17:04:09

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
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.76.199	Australia	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
116.24.250.31	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.76.199	Australia	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
113.240.250.155	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
112.65.201.60	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
211.85.193.212	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.64.147.37	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
116.24.250.31	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
220.245.240.26	147.237.76.199	Australia	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
116.24.250.31	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
112.65.201.60	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
112.65.201.60	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.176	China	test.ncore.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
74.208.229.197	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

11-27-2015-16:04:09 to 11-27-2015-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.18.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	585
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
168.235.197.173	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
199.30.25.65	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
100.100.92.200		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
100.100.92.200		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
100.100.32.148		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
100.100.28.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
100.100.36.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
100.100.50.124		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
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
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
185.120.126.72		147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
100.100.121.93		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.125.75		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
100.100.108.53		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.52.146		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.6.99		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
185.3.144.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.120.126.48		147.237.72.156	aman.idf.il	drop	SAM rule	drop	8
89.138.240.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.19.86.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
89.138.240.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.97.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.30.25.242	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.20.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.37.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.38.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.56.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.82.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
87.69.26.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.142.167	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.180.129.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.26.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.130.212.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.176.146.177	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.247.36.89	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
85.65.54.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.164.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
31.168.164.230	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.164.230	Block	84
77.127.18.169	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.18.169	Block	84
185.120.126.72		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
109.160.253.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
31.168.164.230	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 31.168.164.230	Block	26
79.178.53.51	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.53.51	Block	18
2.54.23.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.26.146.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
199.30.24.247	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
87.68.154.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.192.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
195.154.146.225	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.146.225	Block	2
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	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17175.jpg	Block	2
46.116.15.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.240.79.29	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
80.242.120.103	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.181.153.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.160.224.60	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
5.29.148.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.127.214.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
188.120.148.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
176.106.226.210	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
85.65.195.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.183.140.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
46.120.140.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
79.178.53.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
37.26.146.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
109.160.224.60	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
8.37.70.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1511-en/dover.aspx&usg=alkjrhh53cy6n5sgifjineobbo-i6kcwdg	Block	1
95.86.107.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.14.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
176.240.79.29	Turkey	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
84.108.136.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.112	United States	147.237.77.234	halag.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
79.181.105.179	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.181.105.179	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on /	Block	1
188.120.148.196	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
109.64.142.167	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.73.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
176.106.226.210	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 176.106.226.210	Block	1